Camilla J. Hollanti

Order-Theoretic Methods for Space-Time Coding: Symmetric and Asymmetric Designs

Turku Centre *for* Computer Science

TUCS Dissertations
No 111, November 2008

Order-Theoretic Methods for Space-Time Coding: Symmetric and Asymmetric Designs

Camilla J. Hollanti

To be presented, with the permission of the Faculty of Mathematics and Natural Sciencies of the University of Turku, for public criticism in Auditorium II on January 9, 2009, at 12 noon.

University of Turku
Department of Mathematics
FI-20014 Turku, Finland

2009

Supervisor

Docent Jyrki Lahtonen
Department of Mathematics
University of Turku
FI-20014 Turku
Finland

Reviewers

Professor P. Vijay Kumar
Department of Electrical Communication Engineering
Indian Institute of Science
Bangalore-560012
India

Professor Frédérique Oggier
School of Physical and Mathematical Sciences
Nanyang Technological University
SPMS-04-01, 21 Nanyang Link
Singapore 637371

Opponent

Professor Olav Tirkkonen
Communications Laboratory
Department of Communications and Networking
Helsinki University of Technology
PO Box 3000, FI-02015 TKK
Finland

ISBN 978-952-12-2214-4
ISSN 1239-1883

To Krister,

for all the love and teasing I have got. And for the patience he has got.

To my Mom and Dad,

for being the best family one can ever hope for.

Acknowledgments

I want to express my deepest gratitude to my supervisor Docent Jyrki Lahtonen. Without his novel ideas, great intuition, and remarkable problem solving ability in addition to many enlightening discussions we have had, my research would have never got this far. I also want to thank the other members of our space-time research group, Dr. Roope Vehkalahti and Dr. Kalle Ranto, who provided me with all the help and support I could ever wish for and carefully read through this thesis. I consider myself really lucky to have been able to enjoy such unique team spirit. Without Roope my knowledge in algebraic number theory and class field theory would be a lot poorer. Kalle was always there when I needed some mental support, objective opinions or simulations to be done quickly. Especially, I thank Roope for his help with the most crucial code construction in Publication V.

Special thanks go to Professor Kumar and Dr. Oggier for the preliminary examination of the thesis. I thank Dr. Kibble for the language corrections.

During the past year I have had an excellent collaborator, Hsiao-feng Francis Lu from the National Chiao Tung University, Taiwan. Francis has made a great effort to many of the papers in this thesis to get ready and to be of good quality, not to mention the fact that he has been constantly teaching me new things in the field of electrical engineering and information theory. I am thankful for all the help from him and I am sure that our fruitful collaboration will continue in future. A thank you is also due to all the other collaborators for sharing their ideas and insights with me. Especially, I would like to thank Emanuele Viterbo, Lajos Rónyai, and Raj Kumar for what they have done for me.

In 2005, I spent half a year in the Department of Algebra at the Charles' University in Prague, Czech Republic. Chtěla bych poděkovat mým hostitelům za príjemný pobyt, který jsem měla na Univerzitě Karlově. I also thank professors Emanuele Viterbo, Sujatha Ramdorai, and Vijay Kumar for the memorable visits I had in Italy and India.

I would like to thank Professor Emeritus Tauno Metsänkylä for awakening me in his courses to see the beauty of algebraic number theory.

I thank the EWM for bringing hope and unforgettable moments to my life, both scientifically and personally.

I thank the whole staff of the Department of Mathematics and the Turku Centre for Computer Science for creating a pleasant working environment.

Turku Centre for Computer Science provided the fundamental financial means for my research. The Department of Mathematics at the University of Turku, the Finnish Cultural Foundation, the Magnus Ehrnrooth Foundation, the Turku University Foundation, the Finnish Academy of Science and Letters, the Institute of the Rolf Nevanlinna Foundation, the Finnish Foundation for Technology Promotion, the Nokia Foundation, the Finnish Concordia Fund, and any other foundation I might have forgotten are also gratefully acknowledged for their generous research and travel grants.

Finally, I thank my family, all my friends, and especially Krister for putting up with me and being there for me during this process. I bet they all know pretty well who Jyrki is.

Turku
November 2008 Camilla Hollanti

List of original publications

This thesis is based on the following original publications:

I. Hollanti, C., Lahtonen, J., and Lu, H.-F. (2008). Maximal orders in the design of dense space-time lattice codes.
IEEE Transactions on Information Theory, **54**(10), pp. 4493–4510.

II. Hollanti, C., Lahtonen, J., Ranto, K., and Vehkalahti, R. (2008). On the densest MIMO lattices from cyclic division algebras.
IEEE Transactions on Information Theory, in press.
Available at: http://arxiv.org/abs/cs.IT/0703052.

III. Hollanti, C. and Ranto, K. (2008). Maximal orders in space-time coding: Construction and decoding. *Proceedings of 2008 International Symposium of Information Theory and Its Applications (ISITA)*, Auckland, New Zealand, pp. 1459–1463.

IV. Hollanti, C., Lahtonen, J., Ranto, K., Vehkalahti, R., and Viterbo, E. (2008). On the algebraic structure of the Silver code: A 2×2 Perfect space-time code with non-vanishing determinant.
Proceedings of 2008 IEEE Information Theory Workshop (ITW), Porto, Portugal, pp. 91–94.

V. Hollanti, C. and Lu, H.-F. (2008). Construction methods for asymmetric and multi-block space-time codes.
IEEE Transactions on Information Theory, in press.

VI. Lu, H.-F. and Hollanti, C. (2008). Optimal diversity-multiplexing tradeoff and code constructions of constrained asymmetric MIMO systems. *IEEE Transactions on Information Theory*, submitted.

Contents

I Research Summary **3**

1 Introduction **5**

2 Algebraic preliminaries **9**
2.1 Algebraic number fields 9
2.2 Rings of integers and prime ideals 11
2.3 Central simple algebras 13
2.4 Cyclic division algebras 14
2.5 Orders and discriminants 16
2.6 The Brauer group and Hasse invariants 18
2.7 Local theory of orders 19

3 Coding-theoretic preliminaries **23**
3.1 The MIMO channel model 23
3.2 Code design criteria for space-time codes 24
3.3 Spatial diversity and multiplexing 27

4 Space-time codes from cyclic division algebras **31**
4.1 Lattices: normalized minimum determinant and density 32
4.2 Lattices from matrix representations of orders 34
4.3 Discriminant vs. density 37
4.4 Discriminant bounds for symmetric and asymmetric constructions 39
4.4.1 Symmetric codes 41
4.4.2 Asymmetric codes 48

5 Conclusions and future prospects **57**

List of abbreviations **59**

II Original Publications **67**

Part I

Research Summary

Chapter 1

Introduction

Radio broadcasting was perhaps the first successful wireless application. Other important examples of wireless applications have been, and still are, television broadcasting and satellite communication. However, the establishment of the first generation cellular phones back in the early 1980s has undoubtedly been the main initiator of the adrenaline boosting research race we are experiencing in wireless communications today.

Wireless transmission in the modern world is a challenging task. Huge buildings, slow and fast moving vehicles, and even the flora and fauna cause the signals to get reflected and distorted. Predicting the channel statistics which describe such fading caused by the environment is difficult, hence it is important to design codes that are able to fight against not just certain type of fading, but against, *any* types of fading. In addition to fading, the presence of thermal noise at the receiver makes the extraction of the transmitted message from the received signal even more difficult.

In this thesis, a *code* can be thought of as a finite set of matrices with complex entries, with the purpose of *encoding* the information bits in such a way that revealing the original message becomes feasible, even in the presence of fading and noise.

About a decade ago, it was noticed that by increasing the number of antennas at both the transmitting and receiving end of a wireless channel and by sending multiple copies of the data stream, the quality of the transmission can be significantly improved. The notion of a code matrix for the coded modulation scheme was introduced by Guey *et al.* in [10], where its design criteria were also established. The *space-time (ST) code* which spreads the transmitted signal in both space (antennas) and time (consecutive channel uses for the same information) in this way was invented by Tarokh, Seshadri, and Calderbank [51] in 1998. Their original construction was based on trellis codes. However, block codes were easier to implement, and the first explicit space-time block code (STBC) construction for this *multiple-input multiple-output (MIMO)* scenario was given by Alamouti [2]

later in 1998. Alamouti's construction was actually an example of a *multiple-input single-output (MISO)* code which are nowadays commonly used in telecommunications technology. MIMO systems significantly increase the channel capacity and link robustness of wireless communications, and have been widely adopted in many future wireless communication standards such as WiMAX (Worldwide Interoperability for Microwave Access), and 3GPP LTE (3rd Generation Partnership Project, Long Term Evolution).

Five years ago, Sethuraman *et al.* [48] showed that the transmission rate of a space-time code, i.e. how many bits of information can be transmitted in each channel use, can be increased by using *cyclic division algebras (CDAs)*. Division algebras were already in use prior to this, albeit seldom, due to the full diversity they provide. In addition to diversity gain, CDAs can also provide multiplexing gain [48]; Zheng and Tse showed in their landmark paper [58] that there exists a fundamental *diversity-multiplexing trade-off (DMT)*: diversity can be increased at the cost of reduced multiplexing, and vice versa. Sethuraman *et al.* took advantage of transcendental elements in order to achieve full diversity. However, this caused the minimum determinant of the code matrices to vanish when increasing the code size, i.e. when taking a bigger set of matrices. As the coding gain is directly proportional to the minimum determinant, this result was not welcome. In 2003, Belfiore and Rekaya [4] suggested that, instead of using transcendental elements and the whole algebra, one could use a certain subring that would guarantee a non-vanishing minimum determinant (NVD). Codes having this NVD property have raised a vast amount of interest, especially after Elia *et al.* [8] showed that the NVD property is a sufficient condition for a CDA-based code to achieve the optimal DMT. The most famous example of such DMT optimal codes are, by no doubt, the Perfect codes by Oggier *et al.* [43]. Later on, the construction of Perfect codes was generalized to an arbitrary number of antennas by Elia *et al.* [9].

One crucial observation still remained to be made. In 2006 we pointed out that the subring almost exclusively used in the construction of CDA-based space-time codes, later on referred to as the *natural order*, is not the optimal one [13] in terms of coding gain. Also the fact that this subring is actually an example of an algebraic object called *order* was revealed only then. We proved that if we use a *maximal order* instead, we can increase the size of the code within the given energy limits without any penalty in the coding gain. In other words, maximal orders allow us to increase the code *density*. A counterpart of this observation can be found in the traditional theory of error correcting codes.

The notion of maximal orders in the context of space-time codes was introduced in [13], and the first results in this direction were given for the MISO case in Publication I. In Publication II we proposed a systematic construction of codes from maximal orders for nTx+nRx antennas for any n, and gave explicit examples for all practical values of n. It was also shown that one should pick algebras which have maximal orders with the smallest possible discriminant, as these give the highest density for the code. Our explicit constructions for 2×2 and 3×3

systems have been shown to outperform the Perfect codes of the same size, despite the fact that the Perfect codes were considered unbeatable. The only penalty is the loss of orthogonality. Using a non-orthogonal code does introduce some practical problems. For instance, bit labeling becomes more complicated, as we cannot use the traditional Gray mapping for this purpose. Maintaining a codebook or sphere encoding is necessary in order to take full advantage of the density of the code. Suboptimal decoders may be required to reduce decoding complexity. Nevertheless, Kumar and Caire [32] have shown in their recent paper that using sphere encoding and a suboptimal decoder for maximal order codes still results in excellent performance. Our work in [24, 17] also deals with the decoding issues.

The general construction of ST codes from maximal orders with minimal discriminants was considered more thoroughly in Roope Vehkalahti's dissertation [55] in 2008. Here one can also find interesting bounds for the coding gain, revealing that orthogonal codes can never achieve the density provided by non-orthogonal codes.

Until recently, most of the research in algebraic space-time coding concentrated on the *symmetric scenario*, where the number of transmitting and receive antennas are equal. Often the portable receiving device, e.g. a mobile phone, laptop or a portable digital TV, is so small in physical size that only very few antennas fit inside. In this case, it is more practical to consider the *asymmetric scenario*, where we have more transmit antennas than receive antennas. In Publication V some of the results of Publication II were generalized to the asymmetric scenario and different construction methods were proposed. The best construction was shown to outperform all potential challengers [25, 33].

In addition to the record breaking symmetric and asymmetric space-time constructions, we feel that bringing maximal orders into the field as well as clarifying and explicitly laying out the notions of normalized minimum determinant and density should help the ST audience to design better codes and to compare different codes in algebraic terms rather than by simulations only. The methods and results in this thesis, at least to some extent, also apply to e.g. distributed and multi-user space-time coding. Especially the asymmetric methods can be exploited in the multi-user scenario.

Part I of this thesis is dedicated to explaining the required theory and summarizing the results from the original publications, that will form Part II. As most of the material in Part I can also be found in the publications, our aim is to give an overview of the theory and results without too many technicalities, and to introduce some down-to-earth examples. Part I consists of five chapters. After this introductory Chapter 1, Chapter 2 provides some algebraic preliminaries, introducing the reader to cyclic division algebras and maximal orders. Unfortunately, the explicit construction of maximal or even natural orders is not at all simple. There exist algorithms for maximality testing and for constructing maximal orders, both of which heavily exploit the local properties of orders. Therefore, some local properties of orders are also provided at the end of Chapter 2. Chapter 3 gives an

insight to the coding theoretic aspects of our problems. Chapter 4 brings us to the use of cyclic division algebras and their orders as lattice space-time codes. It is shown that by using the proposed methods, one can construct codes that perform extremely well both at low and high signal-to-noise ratios (SNRs). We remark that the beginning of Section 4.4 contains some deeper algebra, hence a reader with a modest mathematical background can skip the beginning and pick the explicit bounds from the following subsections. The main results from Publications I, II, V, and VI are summarized in Chapter 4, omitting the proofs as they can be found in the original publications. Finally, Chapter 5 will leave the reader with conclusions and some future prospects.

The organization of Part II of this thesis follows the chronological submission order of the original papers. In Publication I, we construct explicit codes with full diversity and non-vanishing minimum determinants for the 4×1 MISO channel. The constructions have straightforward generalizations to any $n \times 1$ or $2n \times 1$ MISO system. Our work on MISO codes has its origins in [11, 12, 13]. Whilst carrying out the research for Publication I, we came to realize that there exist remarkable algebraic objects, namely maximal orders of crossed product algebras, with the aid of which we would be able to generalize the promising results to the $n \times n$ MIMO scheme as well. This led us to the work upon which Publication II is based. There, we consider the construction of cyclic division algebras that have maximal orders with minimal discriminants, and hence provide the largest possible coding gain. We also enhance the Rónyai-Ivanyos algorithm to better suit our purposes, as the original implementation of their algorithm tends to fall short of memory when the index of the algebra is larger than six. Publications III and IV are related to decoding, and have been added here only for the sake of completeness. In Publication II, only the symmetric $n \times n$ scenario was considered. The proposed codes are also DMT optimal for any number of receivers less than or equal to n but, unless n receivers are used, cannot be efficiently decoded. In Publication V, we move on to the asymmetric scenario and solve the problem of constructing sphere decodable codes with large coding gains for the asymmetric MIMO systems. Various construction methods for asymmetric ST codes are proposed. For one of these constructions, we are able to generalize the density results from Publication II to also hold in this more challenging asymmetric case. And once more, maximal orders will play a role. In Publication VI, non-minimum delay, DMT optimal codes are constructed for different asymmetric scenarios.

Publications I-VI appear also in the references list, and from now on we will mostly use the respective numbers in the references list when referring to these papers.

Chapter 2

Algebraic preliminaries

In this chapter, we will recall some preliminaries from algebraic number theory. Throughout this thesis, we will deal with algebraic number fields, Galois groups, algebras, discriminants, and many other algebraic objects. We will give the most crucial definitions in Sections 2.1 and 2.2. For further background information, the reader can refer to e.g. [31] or [50]. For those with a background in information theory, we also recommend the early chapters of [44]. Sections 2.4 to 2.7 are devoted to introducing in more detail the non-commutative algebraic and class field theoretic tools that were used in the original publications. Throughout the whole thesis, we denote the fields of integers, rationals, reals, and complex numbers by $\mathbb{Z}, \mathbb{Q}, \mathbb{R},$ and $\mathbb{C}$, respectively. The capital letters F, L and E will denote number fields.

2.1 Algebraic number fields

Let us start with the very basics of algebraic number theory.

A *number field* F is a finite extension of $\mathbb{Q}$. Let E/F be a finite extension of number fields, and let the *degree* of the extension be $[E:F] = n$ $(< \infty)$. Now E can be seen as an n-dimensional vector space over the field F. Hence, E has a basis $\{b_1, b_2, ..., b_n\}$ over F. The extension E/F is *algebraic*, i.e. each element $e \in E$ is algebraic. This means that there exists a polynomial with coefficients in F having e as a root. The (unique) minimal polynomial of e is the monic, irreducible polynomial

$$\mu_e(x) = x^m + f_1 x^{m-1} + \cdots + f_m \in F[x],$$

for which $\mu_e(e) = 0$. The integer $m = \deg \mu$ is called the *degree* of e over F and it always divides n.

A finite extension E/F of number fields is always *simple*, i.e. it can be written as $E = F(\alpha)$, where α is algebraic over F. The single generating element α (not unique) is called *primitive*. The degree of a primitive element is $n = [E:F]$. This

means that the elements of E can be written as polynomials $f(\alpha) \in F[\alpha]$ with $\deg f \leq n-1$.

Definition 2.1.1. Let S be an integral domain and R its subdomain, $R \subseteq S$. An element $\alpha \in S$ is called *integral* over R, if there exists a monic polynomial $f(x) \in R[x]$ for which $f(\alpha) = 0$. A complex number $\alpha \in \mathbb{C}$ that is integral over $\mathbb{Z}$ is called an *algebraic integer*.

Remark 2.1.2. Algebraic integers of a number field form a ring. In Chapter 3 we will see that this is not the case when we consider the set of integers of a division algebra (see Remark 3.2.4).

An algebraic number α is an algebraic integer if and only if its minimal polynomial (over $\mathbb{Q}$) $\mu_\alpha(x) \in \mathbb{Z}[x]$. The *ring of (algebraic) integers* of F is denoted by $\mathcal{O}_F$. The above statement can be generalized to any field extension E/F: an algebraic number $\alpha \in E$ is integral over F if and only if its minimal polynomial (over F) $\mu_\alpha(x) \in \mathcal{O}_F[x]$.

Remark 2.1.3. If $F = \mathbb{Q}$, $F = \mathbb{Q}(i)$ or $F = \mathbb{Q}(\omega)$, $\omega = \zeta_3 = \exp(2\pi i/3)$, and E is an extension of F, then $\mathcal{O}_E$ is a free $\mathcal{O}_F$-module that has rank equal to $n = [E : F]$. This property will be needed later when we consider the rate of a code design constructed from a cyclic division algebra (see Equation (3.6) and Section 4.2).

Definition 2.1.4. A finite extension E/F is *separable*, if for all $\alpha \in E$ the roots of the minimal polynomial $\mu_\alpha(x) \in F[x]$ are simple. A number field extension is always separable.

A finite extension E/F is *normal*, if E is the splitting field for some polynomial $f(x) \in F[x]$ over F, in other words E is the smallest extension of F, where $f(x)$ splits into linear factors.

Now suppose again that E/F is a number field extension and $[E : F] = n$. Consider the set of field homomorphisms $\sigma : E \to \mathbb{C}$ that are F-embeddings, i.e. homomorphisms that fix F, $\sigma(f) = f$ for every $f \in F$, and that map E isomorphically to $\sigma(E)$. Let us denote $E = F(\alpha)$, and let $\mu_\alpha(x) \in F[x]$ be the minimal polynomial of α over F. Let $\alpha_1 = \alpha, \alpha_2, ..., \alpha_n$ be the roots of $\mu_\alpha(x)$ in $\mathbb{C}$. Now the F-monomorphisms are completely described by

$$\sigma_k(\alpha) = \alpha_k. \tag{2.1}$$

Hence, there are exactly n F-embeddings (cf. Definition 2.1.4). The set of F-embeddings of E will be denoted by $\mathrm{Hom}_F(E, \mathbb{C})$.

Definition 2.1.5. An extension is *Galois* if it is both normal and separable. Equivalently, an extension E/F is Galois, if E is the splitting field of a separable polynomial with coefficients in F. Yet another equivalent way of stating this is that all the roots of $\mu_\alpha(x)$ belong to the field E, hence $\sigma(E) = E$ for all $\sigma \in \mathrm{Hom}_F(E, \mathbb{C})$.

Definition 2.1.6. In the case when the extension E/F is Galois, the set of F-embeddings forms a group, called the *Galois group* of E/F, and is denoted by $\mathrm{Gal}(E/F)$.

Definition 2.1.7. Let E/F be a number field extension with the set of embeddings $\mathrm{Hom}_F(E,\mathbb{C}) = \{\sigma_1,...,\sigma_n\}$ and let $e \in E$. The (relative) *norm* and *trace* of E/F are defined as

$$\mathrm{N}_{E/F}(e) = \prod_{i=1}^{n} \sigma_i(e) \text{ and } \mathrm{T}_{E/F}(e) = \sum_{i=1}^{n} \sigma_i(e),$$

respectively.

Definition 2.1.8. The *discriminant* of the basis $\{b_1, b_2, ..., b_n\}$ of a number field extension E/F is

$$d(b_1,...,b_n) = \det(\sigma_i(b_j))^2 = \det(\mathrm{T}_{E/F}(b_i b_j)) \quad (1 \le i, j \le n),$$

where $\mathrm{Hom}_F(E,\mathbb{C}) = \{\sigma_1, \sigma_2, ..., \sigma_n\}$.

Definition 2.1.9. The basis $\{b_1, b_2, ..., b_n\}$ is called *integral,* if it forms an $\mathscr{O}_F$-module basis for $\mathscr{O}_E$, i.e. if

1) $b_i \in \mathscr{O}_E$ for $i = 1,...,n,$ and
2) $\mathscr{O}_E = \mathscr{O}_F b_1 \oplus \cdots \oplus \mathscr{O}_F b_n$.

The discriminant of an integral basis is called the (relative) *discriminant of* E/F and denoted by $d(E/F)$. The discriminant of E/F is independent of the choice of the integral basis up to a unit factor. In the cases where $\mathscr{O}_F$ is not a principal ideal domain (PID), we cannot guarantee the existence of a relative integral basis (one example of such an extension is $\mathbb{Q}(\sqrt{-14}, \sqrt{-7})/\mathbb{Q}(\sqrt{-14})$), and the discriminant must be viewed as an ideal, rather than as a number. For the modifications required in this case or in the case when an integral basis is not known, see Definition 2.5.6.

2.2 Rings of integers and prime ideals

Let F be an algebraic number field and let $\mathscr{O} = \mathscr{O}_F$ be the (commutative) ring of integers of F. An ideal $\mathfrak{I}$ of $\mathscr{O}$ generated by $\alpha_1,...,\alpha_s$ is denoted by $\mathfrak{I} = \langle \alpha_1,...,\alpha_s \rangle$. We will write $\langle 0 \rangle = 0$ and $\langle 1 \rangle = 1$, whenever the meaning is clear from the context. Notice that $1 = \mathscr{O}$.

An ideal $\mathfrak{p} \subseteq \mathscr{O}$ is a *prime ideal,* if $\mathfrak{p} \neq \mathscr{O}$ and

$$a, b \in \mathscr{O}, \ \ ab \in \mathfrak{p} \ \Rightarrow \ a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}.$$

An ideal $\mathfrak{M}$ is *maximal,* if $\mathfrak{M} \neq \mathscr{O}$ and

$$\mathfrak{M} \subset \mathfrak{I} \subseteq \mathscr{O} \ \Rightarrow \ \mathfrak{I} = \mathscr{O}.$$

An ideal $\mathfrak{I} \neq \mathscr{O}$ is maximal if and only if the (finite) residue ring $\mathscr{O}/\mathfrak{I}$ is a field. Moreover, an ideal $\mathfrak{p} \neq \mathscr{O}$ is prime if and only if $\mathscr{O}/\mathfrak{p}$ is an integral domain, i.e. has no zero divisors. From this it follows that every maximal ideal in $\mathscr{O}$ is also a prime ideal in $\mathscr{O}$. The inverse claim is also true: every (proper) prime ideal $\mathfrak{p} \neq 0,1$ of $\mathscr{O}$ is maximal. The ring $\mathscr{O}$ is a Dedekind domain, from which it follows that every ideal $0,1 \neq \mathfrak{I} \subseteq \mathscr{O}$ has a representation as a product of prime ideals (see Equation (2.2)). This presentation is unique up to the ordering of the ideals.

Now let E/F be a number field extension, $[E:F] = n$, and $\mathfrak{p}$ a prime ideal of $\mathscr{O}_F$. We can write

$$\mathfrak{p}\mathscr{O}_E = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}, \tag{2.2}$$

where $\mathfrak{P}_1, ..., \mathfrak{P}_g$ are distinct prime ideals in $\mathscr{O}_E$. We say that the ideals $\mathfrak{P}_i$ *lie above* $\mathfrak{p}$. Each of the ideals $\mathfrak{P}_i$ is adjoined with a number $f_i = [\mathscr{O}_E/\mathfrak{P}_i : \mathscr{O}_F/\mathfrak{p}]$, called the inertial degree of $\mathfrak{P}_i$ over $\mathfrak{p}$. The exponent e_i is called the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$. The inertial degrees and ramification indices satisfy

$$\sum_{1=i}^{g} e_i f_i = n. \tag{2.3}$$

The relative norm of a prime ideal $\mathfrak{P} \subseteq \mathscr{O}_E$ lying above $\mathfrak{p} \subseteq \mathscr{O}_F$ is $\mathrm{N}_{E/F}(\mathfrak{P}) = \mathfrak{p}^f$, where f is the inertial degree. This extends multiplicatively as $N(\mathfrak{I}_1\mathfrak{I}_2) = N(\mathfrak{I}_1)N(\mathfrak{I}_2)$. For $a \in E$, $\mathrm{N}_{E/F}(a)\mathscr{O}_F = \mathrm{N}_{E/F}(a\mathscr{O}_E)$. That is, the ideal of $\mathscr{O}_F$ generated by the norm of a is equal to the norm of the ideal of $\mathscr{O}_E$ generated by a.

In the case when E/F is Galois, (2.2) gets a simpler form

$$\mathfrak{p}\mathscr{O}_E = (\prod_{i=1}^{g} \mathfrak{P}_i)^e,$$

where the prime ideals $\mathfrak{P}_i$ are the distinct conjugate ideals of $\mathfrak{P}_1$. That is, $\mathfrak{P}_i = \sigma_j(\mathfrak{P}_1)$ for some $\sigma_j \in \mathrm{Gal}(E/F)$. Each prime ideal $\mathfrak{P}_i$ has the same inertial degree $f_i = f$ and $N(\mathfrak{P}_i) = \mathfrak{p}^f$ for all $i = 1, ..., g$. Also the ramification indices $e_i = e$ coincide for all $\mathfrak{P}_i$. Equation (2.3) now takes the form

$$efg = n.$$

If $e > 1$, we say that $\mathfrak{p}$ *ramifies* in E/F. If $\mathfrak{p}$ ramifies, then $\mathfrak{p}|d(E/F)$. If $g > 1$, we say that $\mathfrak{p}$ *splits*. If $f > 1$, $\mathfrak{p}$ has *inertia*.

Lemma 2.2.1. *Let $F_2 \supseteq F_1 \supseteq F$ be a tower of finite extensions of $\mathbb{Q}$. Then*

$$d(F_2/F) = N_{F_1/F}(d(F_2/F_1))d(F_1/F)^{[F_2:F_1]}.$$

Proof. For the proof we refer the reader to [46, p.249]. □

Definition 2.2.2. Let $F/\mathbb{Q}$ be a finite extension of degree n. Let r_1 be the number of real embeddings $\sigma : F \to \mathbb{R}$ and r_2 the number of conjugate pairs of non-real embeddings $\sigma : F \to \mathbb{C}$. The 2-tuple (r_1, r_2) is called *the signature* of the field F.

Proposition 2.2.3. *Let $[F : \mathbb{Q}] = n$. Then*

$$r_1 + 2r_2 = n.$$

As mentioned above, the ramification of the prime ideals of F for a finite extension E/F of algebraic number fields is dictated by the discriminant $d(E/F)$, which is an ideal of $\mathcal{O}_F$. In 1977 Andrew Odlyzko [41] gave a lower bound $C_{(r_1,r_2)}$ for the discriminants of fields with signature (r_1, r_2). For small values of r_1 and r_2 there exists tables for $C_{(r_1,r_2)}$. Asymptotically, when n approaches infinity, we have

$$|d(F/\mathbb{Q})|^{1/n} \geq (60.8395...)^{r_1/n}(22.3816...)^{2r_2/n} - O(n^{-2/3}) = C_{(r_1,r_2)}. \qquad (2.4)$$

2.3 Central simple algebras

Let us next formally introduce the world of central simple algebras. We refer the interested reader to [27, 45] for a more detailed exposition of the theory of central simple algebras and their matrix representations.

An algebra $\mathcal{A}$ over a field F (or an F-algebra) is a (right) F-module and a ring such that the module $\mathcal{A}$ and the ring $\mathcal{A}$ have the same additive group $(\mathcal{A}, +, 0)$ and

$$(ab)f = a(bf) = (af)b$$

for $a, b \in \mathcal{A}$ and $f \in F$. The center $C = C(\mathcal{A}) = \{a \in \mathcal{A} \mid aa' = a'a \ \forall a' \in \mathcal{A}\}$ of an algebra $\mathcal{A}$ is the set of elements of $\mathcal{A}$ that commute with all elements of $\mathcal{A}$, and the image of F under the ring homomorphism $\mu : F \to \mathcal{A},\ f \mapsto 1f$, is $1F \subseteq C$.

Definition 2.3.1. An F-algebra $\mathcal{A}$ is called central, if $C = 1F$. An algebra $\mathcal{A}$ is called *simple* if it has no nontrivial ideals. An *F-central simple algebra* is a simple F-algebra that is finite dimensional over its center F.

Definition 2.3.2. We call the algebra $\mathcal{A}$ a *division algebra* if every non-zero element of $\mathcal{A}$ is invertible.

If $\mathcal{A}$ is a finite dimensional simple algebra over F, then $\mathcal{A} \cong \mathcal{M}_n(\mathcal{D})$, where $\mathcal{D}$ is a finite dimensional division algebra over F. The centers of $\mathcal{A}$ and $\mathcal{D}$ are isomorphic, i.e. the center C is a field. Hence, we can consider $\mathcal{A}$ as a central simple algebra over C. Later on we shall see that this class of finite dimensional central simple algebras has some beautiful properties that are especially welcome in the context of space-time code constructions.

Definition 2.3.3. Let M be a left $\mathcal{A}$-module and $x \in M$. We define a representation $v_M : A \to \mathrm{End}(M)$ of $\mathcal{A}$, where $a \in \mathcal{A}$ maps to a homomorphism $x \mapsto ax$.

Later on in Section 2.5, by restricting this map to an order $\Lambda \subseteq \mathscr{A}$, we also get a representation of an order. Moreover, if M is actually an $(\mathscr{A}, E)$-bimodule, then the image of v_M is in $\mathrm{End}_E(M)$. If then M is an n-dimensional (right) vector space over E, we get a representation of A as $n \times n$ matrices over E.

2.4 Cyclic division algebras

In this section, we concentrate on a special class of central simple algebras, namely cyclic division algebras. For a more detailed exposition, see [27, 45].

The main ingredients of a cyclic division algebra are

(i) a finite dimensional algebraic number field extension and its (cyclic) Galois group,
(ii) a so-called non-norm element coming from the base field.

Let us explain the above more precisely. In Publications II-IV we consider number field extensions E/F, where F denotes the base field and F^* (resp. E^*) denotes the set of the non-zero elements of F (resp. E). For the purposes of space-time coding, the most interesting cases are those where F is an imaginary quadratic field, usually either $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$. We assume that E/F is a cyclic field extension of degree n with Galois group $\mathrm{Gal}(E/F) = \langle\sigma\rangle = \{\sigma, \sigma^2, ..., \sigma^n = \mathrm{Id}_F\}$. Let $\mathscr{A} = (E/F, \sigma, \gamma)$ be the corresponding cyclic algebra of degree n (n is also called the *index* of $\mathscr{A}$), that is

$$\mathscr{A} = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E,$$

as a (right) vector space over E. Here $u \in \mathscr{A}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in F^*$. An element $a = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathscr{A}$ has the following left regular representation (see Definition 2.3.3) as

$$A = \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}. \tag{2.5}$$

We refer to this as the standard matrix representation of $\mathscr{A}$, and we identify the element $a \in \mathscr{A}$ with its representation (2.5). Taking e.g. a transpose A^T makes no difference for coding purposes.

Definition 2.4.1. The determinant (resp. trace) of the matrix A above is called the *reduced norm* (resp. *reduced trace*) of the element $a \in \mathscr{A}$ and is denoted by $nr_{\mathscr{A}/F}(a)$ (resp. $tr_{\mathscr{A}/F}(a)$). In short, we denote the norm and trace by $nr(a)$ and $tr(a)$, respectively, when the field is clear from the context.

Remark 2.4.2. The connection with the usual norm map $\mathrm{N}_{\mathscr{A}/F}(a)$ (resp. trace map $\mathrm{T}_{\mathscr{A}/F}(a)$) and the reduced norm $nr(a)$ (resp. reduced trace $tr(a)$) of an element $a \in \mathscr{A}$ is $\mathrm{N}_{\mathscr{A}/F}(a) = (nr(a))^n$ (resp. $\mathrm{T}_{\mathscr{A}/F}(a) = ntr(a)$), where n is the degree of E/F. Recall that $\mathrm{N}_{\mathscr{A}/F}(a)$ (resp. $\mathrm{T}_{\mathscr{A}/F}(a)$) is defined similarly as the reduced norm (resp. reduced trace), i.e. as the determinant (resp. trace) of the left multiplication matrix of a but with respect to a basis of $\mathscr{A}/F$ rather than of $\mathscr{A}/E$.

Theorem 2.4.3. *Let F be a number field. Every central simple F-algebra is cyclic.*

Proof. [45, Thm. 32.30, p. 280] □

The element γ is often called a *non-norm element* due to Theorem 2.4.5 by Albert [3, Theorem 11.12, p. 184]. It provides us with a condition under which a cyclic algebra is a division algebra. The original result was stated for $t = 1, 2, ..., n-1$, but is given in a simplified form after the next lemma.

Lemma 2.4.4. *Let $\gamma \in F^*$ and E/F be as above. Consider the set S of exponents $t \in \mathbb{Z}$ such that γ^t is a norm of an element of E. Then*

$$S = k\mathbb{Z}$$

for some $k|n$.

Proof. The mapping $f : t \mapsto \gamma^t$ is a homomorphism of groups from $(\mathbb{Z}, +)$ to $(F^*, \cdot)$. Because $H = \mathrm{N}_{E/F}(E^*)$ is a subgroup of F^*, and $S = f^{-1}(H)$, we immediately see that S is a subgroup of $(\mathbb{Z}, +)$. From basic algebra it now follows that S is cyclic, i.e. $S = k\mathbb{Z}$ for some $k \in \mathbb{Z}$. On the other hand, as $\gamma \in F^*$ we get that $\gamma^n = \mathrm{N}_{E/F}(\gamma)$, and hence $n \in S$. Therefore $k|n$. □

Proposition 2.4.5 (Norm condition). *The cyclic algebra $\mathscr{A} = (E/F, \sigma, \gamma)$ of degree n is a division algebra if and only if the smallest factor $t \in \mathbb{Z}_+$ of n such that γ^t is the norm of some element of E^* is n.*

Proof. We need to prove the equivalence of two conditions, the original stating that γ^t is not a norm for any t in the range $1, 2, ..., n-1$, and the relaxed version stating the same for those t in the same range that are also divisors of n. One implication is clear, and the other follows from the above lemma. Namely, if there are integers t in the range $1, 2, ..., n-1$ such that γ^t happens to be a norm, then the lemma tells us that the smallest such t must be a divisor of n. □

Remark 2.4.6. We can even relax the above conditions for t. The proof of the previous lemma shows that it actually suffices to check that $\gamma^{n/p}$ is not a norm for any prime divisor p of n. For example, when $n = 8$, it suffices to check that γ^4 is not a norm.

We conclude this section by defining the Jacobson radical which will be needed for investigating the algorithmic properties of maximal orders [15].

Definition 2.4.7. Let S denote an arbitrary ring with identity. An S-module is *simple*, if it is not the zero module and if it has no proper submodules.

Definition 2.4.8. Let again S denote an arbitrary ring with identity. The *Jacobson radical* of the ring S is the set

$$\mathrm{Rad}(S) = \{x \in S \mid xM = 0 \text{ for all simple left } S\text{-modules } M\}.$$

$\mathrm{Rad}(S)$ is a two-sided ideal in S containing every nilpotent (i.e. for which $\mathscr{I}^k = 0$ for some $k \in \mathbb{Z}_+$) one-sided ideal $\mathscr{I}$ of S. Also, $\mathrm{Rad}(S)$ can be characterized as the intersection of the maximal left ideals in S. If S is a finite dimensional algebra over a field or, more generally, left or right Artinian (i.e. satisfies the descending chain condition on (left or right) ideals), then $\mathrm{Rad}(S)$ is the maximal nilpotent ideal in S.

2.5 Orders and discriminants

In this section, our intention is to familiarize the reader with orders and their basic and most crucial properties. The original publications also contain most of the material of this section. The general theory of maximal orders can be found in [45].

Throughout the section, let us suppose that we have an F-central division algebra of index $n < \infty$, and that R is a Dedekind ring in F. For instance, we could have $F = \mathbb{Q}(i)$ and $R = \mathbb{Z}[i]$.

Definition 2.5.1. An *R-order* in the F-algebra $\mathscr{A}$ is a subring Λ of $\mathscr{A}$, having the same identity element as $\mathscr{A}$, and such that Λ is a finitely generated module over R and generates $\mathscr{A}$ as a linear space over F.

Definition 2.5.2. An order Λ is called *maximal*, if it is not properly contained in any other R-order.

Let us illustrate the above definition via some concrete examples.

Example 2.5.3. (a) Orders always exist: If $FM = \mathscr{A}$, i.e. M is a *full* R-lattice in $\mathscr{A}$, then the *left order* of M defined as $\mathscr{O}_l(M) = \{x \in \mathscr{A} \mid xM \subseteq M\}$ is an R-order in $\mathscr{A}$. The right order is defined in an analogous way. Left orders are used in [15] to demonstrate algorithmic properties of maximal orders.

(b) If R is the ring of integers $\mathscr{O}_F$ of the number field F, then the ring of integers $\mathscr{O}_E$ of the extension field E is the unique maximal order in E. For example, in the case of the cyclotomic field $E = \mathbb{Q}(\zeta)$, where $\zeta = \exp(2\pi i/k)$ is a primitive root of order k the maximal order is $\mathscr{O}_E = \mathbb{Z}[\zeta]$. In sharp contrast to the commutative case, a maximal order in a non-commutative algebra is usually not unique.

One of the most crucial properties of orders is stated below (see Section 4.2). For the proof, see [45, Theorem 10.1, p. 125].

Proposition 2.5.4. *Let Λ be an order in a cyclic division algebra $(E/F,\sigma,\gamma)$. Then for any non-zero element $a \in \Lambda$ its reduced norm $nr(a)$ and reduced trace $tr(a)$ are non-zero elements of the ring of integers $\mathcal{O}_F$ of the center F.*

Example 2.5.5. Let $\gamma \in F^*$ be an algebraic integer, i.e. $0 \neq \gamma \in \mathcal{O}_F$. If γ is not integral to start with, it is of the form $\frac{a}{b}$, where $a,b \in \mathcal{O}_F$. Now we can get an isomorphic algebra having an integral γ by multiplying by a 'norm element' $\mathrm{N}_{E/F}(b) = b^n$. By [27, Theorem 8.14, p. 481], the cyclic division algebras $(E/F,\sigma,\gamma)$ and $(E/F,\sigma,\gamma\mathrm{N}(b)) = (E/F,\sigma,ab^{n-1})$ are then isomorphic. So when considering the division algebras up to isomorphism, then without loss of generality we can assume that the non-norm element is actually an algebraic integer.

We immediately see that then the $\mathcal{O}_F$-module

$$\Lambda_{NAT} = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E,$$

where $\mathcal{O}_E$ is the ring of integers, is an $\mathcal{O}_F$-order in the cyclic algebra $(E/F,\sigma,\gamma)$. We refer to this $\mathcal{O}_F$-order as the *natural order*. It will also serve as a starting point when searching for maximal orders.

In any cyclic algebra, a maximal $\mathbb{Z}$-order is a maximal $\mathcal{O}_F$-order as well.

We remark that the term 'natural order' is somewhat misleading. While it is perhaps the first order that comes to mind, there is nothing canonical about it. Indeed, distinct realizations of a given division algebra as a cyclic algebra often lead to different natural orders. For instance, constructing the algebra of rational Hamiltonian quaternions from the cyclic extension $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ as opposed to the more common $\mathbb{Q}(i)/\mathbb{Q}$ leads to a different natural order.

Let us next define the discriminant of an order. Let $\mathcal{A} = (E/F,\sigma,\gamma)$ be a cyclic division algebra and $\Lambda \subset \mathcal{A}$ an order.

Definition 2.5.6. Let F be the center of $\mathcal{A}$ and $m = dim_F \mathcal{A}$. The *discriminant* of the R-order Λ is the ideal $d(\Lambda/R)$ in R generated by the set

$$\{\det(tr_{\mathcal{A}/F}(x_i x_j))_{i,j=1}^m \mid (x_1,...,x_m) \in \Lambda^m\}.$$

In the interesting cases of $F = \mathbb{Q}(i)$ (resp. $F = \mathbb{Q}(\sqrt{-3})$) the ring $R = \mathbb{Z}[i]$ (resp. $R = \mathbb{Z}[\omega]$, $\omega = (-1+\sqrt{-3})/2$) is a Euclidean domain, so in these cases (as well as in the case $R = \mathbb{Z}$) it makes sense to speak of the discriminant as an element of R rather than as an ideal. We simply pick a generator of the discriminant ideal, and call it the discriminant. Equivalently we can compute the discriminant as

$$d(\Lambda/R) = \det(tr(x_i x_j))_{i,j=1}^m,$$

where $\{x_1,\ldots,x_m\}$ is any R-basis of Λ. It can be readily seen that whenever $\Lambda \subseteq \Gamma$ are two R-orders, then $d(\Gamma/R)$ is a factor of $d(\Lambda/R)$. The index $[\Gamma:\Lambda]$ is related to discriminants by the following lemma.

Lemma 2.5.7.

$$[R : d(\Lambda/R)R] = [\Gamma : \Lambda]^2 [R : d(\Gamma/R)R]$$

Proof. [45, p. 66] □

We present the following basic formula for the discriminant of certain cyclotomic fields (see [30, Theorem 1.61, p. 42]), as it will be required later.

Example 2.5.8. Let $\zeta_\ell = \exp(2\pi i/2^\ell)$ be a complex primitive root of unity of order 2^ℓ, where $\ell \geq 2$ is an integer. Then $n = [\mathbb{Q}(\zeta_\ell) : \mathbb{Q}(i)] = 2^{\ell-2}$ and

$$d(\mathbb{Z}[\zeta_\ell]/\mathbb{Z}[i]) = (1+i)^{2n(\ell-2)}.$$

Remark 2.5.9. It turns out (cf. [45, Theorem 25.3, p. 218]) that all the maximal orders of a division algebra share the same discriminant, which we will refer to as the *discriminant of the division algebra*. In this sense a maximal order has the smallest possible discriminant among all orders within a given division algebra, as all the orders are contained in a maximal one.

For an easy reference we state the following result which follows from the definitions.

Lemma 2.5.10. *Let E/F be as above, assume that γ is an algebraic integer of F, and let Λ_{NAT} be the natural order of Example 2.5.5. If $d(E/F)$ is the $\mathcal{O}_F$-discriminant of $\mathcal{O}_E$ (often referred to as the relative discriminant of the extension E/F), then*

$$d(\Lambda_{NAT}/\mathcal{O}_F) = d(E/F)^n \gamma^{n(n-1)}.$$

Proof. [15, Lemma 5.4] or [55]. □

2.6 The Brauer group and Hasse invariants

In this section, we define two useful algebraic objects called, namely the Brauer group and the Hasse invariants of an algebra.

Let $\mathscr{A}$ and $\mathscr{B}$ be finite dimensional central simple algebras. We say $\mathscr{A}$ and $\mathscr{B}$ are *similar*, if for some positive integers m and n we have $\mathscr{M}_m(\mathscr{A}) \cong \mathscr{M}_n(\mathscr{B})$ as F-algebras. From the properties of the tensor product it follows that this similarity relation defines an equivalence relation. Any cyclic algebra (see Section 2.4) is a central simple F-algebra (cf. Definition 2.3.1) and Wedderburn's structure theorem [27, Theorem, p. 171] tells us that any central simple algebra is a matrix algebra over a central simple division algebra. Thus, it easily follows that within any similarity class there is a unique division algebra. The similarity classes $\{\mathscr{A}\}$ form a group under the multiplication rule

$$\{\mathscr{A}\}\{\mathscr{B}\} = \{\mathscr{A} \otimes_F \mathscr{B}\}.$$

This group is called the *Brauer group of* F and is denoted by $\mathrm{Br}(F)$. If F' is an extension field of F, and $\mathscr{A}$ is a central simple F-algebra, then the tensor product $\mathscr{A}' = \mathscr{A} \otimes_F F'$ is a central simple F'-algebra. We refer to this algebra as the algebra obtained from $\mathscr{A}$ by *extending the scalars to* F'.

A *prime* of F is an equivalence class of non-trivial valuations on F. Thus there is exactly one prime for each prime ideal in $\mathscr{O}_F$, for each real embedding $F \hookrightarrow \mathbb{R}$, and for each conjugate pair of non-real embeddings $F \hookrightarrow \mathbb{C}$. The corresponding primes are called *finite, real, and complex*, respectively. An element of F is said to be *positive* at the real prime corresponding to an embedding $F \hookrightarrow \mathbb{R}$ if it maps to a positive element of $\mathbb{R}$. A real prime of F is said to *split* in an extension E/F if every prime lying over it is real; otherwise it is said to *ramify* in E. A finite extensions F of $\mathbb{Q}$ only has finitely many infinite primes.

Let P be an infinite prime of F. By $\hat{F}_P$ we refer to the field of reals $\mathbb{R}$ or to the field of complex numbers $\mathbb{C}$, depending on whether the prime P is real or complex, respectively. If P is finite then $\hat{F}_P$ is just the familiar P-adic completion of the field F. All the fields $\hat{F}_P$, where P is any prime of F, are referred to as completions of F. The division algebras over $\hat{F}_P$ are easy to describe. They are all obtained as cyclic algebras of the form $\mathscr{A}(n,r) = (E/\hat{F}_P, \sigma, \pi^r)$, where E is the unique unramified extension of $\hat{F}_P$ of degree n, σ is the Frobenius automorphism, and π is the prime element of F_P. The quantity r/n is called the *Hasse invariant* of this algebra and n is referred to as the *local index*. It immediately follows from Proposition 2.4.5 that $\mathscr{A}(n,r)$ is a division algebra if and only if $(r,n) = 1$. For a description of the theory of Hasse invariants we refer the reader to [45, p. 266] or [40].

For a detailed exposition on the general properties of Brauer groups and Hasse invariants, we refer to [45, Chapters 3,7, and 8].

2.7 Local theory of orders

In [15] some facts from the local theory of orders are required in order to describe an algorithm for producing maximal orders. For the basic properties of localization the reader can turn to [27, Chapter 7] or [45, Chapters 1, 2]. In this section, we only briefly summarize some of the results that were needed in [15]. For the proofs of the results in this section, see [26] and [47] — these references have a nice collection of results which were originally taken from [45], but have been modified for our purposes. For the definition of the radical, see Definition 2.4.8.

We first recall the left order of an algebra.

Definition 2.7.1. Let us suppose that we have an F-central division algebra of index n and that R is a Dedekind ring in F. If M is a *full* R-lattice in $\mathscr{A}$, i.e. $FM = \mathscr{A}$, then the *left order* of M defined as $\mathscr{O}_l(M) = \{x \in \mathscr{A} \mid xM \subseteq M\}$ is an R-order in $\mathscr{A}$. The right order is defined in an analogous way.

The next proposition (see [47, proof of Theorem 3.2]) is useful when computing left orders.

Proposition 2.7.2. *Let $\mathscr{A}$ be a simple algebra over F and M a finitely generated $\mathcal{O}_F$-module such that $FM = \mathscr{A}$. Then there exists an element $s \in \mathcal{O}_F \setminus \{0\}$ such that $s \cdot 1 \in M$. Moreover, $\mathcal{O}_l(M) = \{b \in s^{-1}M \mid bM \leq M\} \leq s^{-1}M$.*

If R is a Dedekind domain with a quotient field F, and P is a prime ideal in R, then the ring of quotients $R_P = (R/P)^{-1}R \subset F$ is a discrete valuation ring. For the R-lattices M in $\mathscr{A}$ the localization at P is defined as $M_P = R_P M \subset \mathscr{A}$. M_P is an R_P-lattice. Moreover, if M is a full (cf. Example 2.5.3) R-lattice in $\mathscr{A}$, then M_P is a full R_P-lattice in $\mathscr{A}$. To be more specific, let us define the ring $\mathbb{Z}_p$.

Definition 2.7.3. For a rational prime p let $\mathbb{Z}_p$ denote the ring

$$\mathbb{Z}_p = \{\frac{r}{s} \in \mathbb{Q} \mid r,s \in \mathbb{Z},\ gcd(p,s) = 1\}.$$

$\mathbb{Z}_p$ is a discrete valuation ring with the unique maximal ideal $p\mathbb{Z}_p$. If Λ is a $\mathbb{Z}$-order we use the notation $\Lambda_p = \mathbb{Z}_p\Lambda$.

We remark that one should not confuse the localization R_P with the ring of integers $\hat{R}_P$ of the P-adic completion. We use the caret to indicate a complete structure. This is somewhat non-standard in the case of $\mathbb{Z}_p$ that is nearly universally used to denote the complete ring of p-adic integers. We use $\hat{\mathbb{Z}}_p$ for the complete ring.

In the following, we work inside an F-central division algebra $\mathscr{A}$, R being the ring of algebraic integers in F. The next statement illustrates a simple but useful connection between the orders Λ and Λ_P.

Proposition 2.7.4 (Proposition 2.8 [26]). *Let Λ be a R-order in $\mathscr{A}$. The map $f : x \mapsto x + P\Lambda_P$, $x \in \Lambda$ induces an isomorphism of the rings $\Lambda/P\Lambda \cong \Lambda_P/P\Lambda_P$.*

Proposition 2.7.5 (Proposition 3.1 [26]). *Let P be a prime ideal of the ring R. The residue class ring $\overline{\Lambda_P} = \Lambda_P/P\Lambda_P$ is an algebra with identity element over the residue class field $\overline{R_P} = R_P/PR_P$ and $dim_F \mathscr{A} = dim_{\overline{R_P}} \overline{\Lambda_P}$. If $\phi : \Lambda_P \to \overline{\Lambda_P}$ is the canonical epimorphism, then $P\Lambda_P \subseteq \mathrm{Rad}(\Lambda_P) = \phi^{-1}\mathrm{Rad}(\overline{\Lambda_P})$ and ϕ induces a ring isomorphism $\Lambda_P/\mathrm{Rad}(\Lambda_P) \cong \overline{\Lambda_P}/\mathrm{Rad}(\overline{\Lambda_P})$. As a consequence, a left (or right) ideal $\mathscr{I}$ of Λ_P is contained in $\mathrm{Rad}(\Lambda_P)$ if and only if there exists a positive integer t such that $\mathscr{I}^t \subseteq P\Lambda_P$.*

Combining the previous two results we get.

Corollary 2.7.6 (Corollary 9.4 [15]). *Let P be a prime ideal of the ring R. We then have*

$$\phi^{-1}(\mathrm{Rad}(\Lambda/P\Lambda)) = \psi^{-1}(\mathrm{Rad}(\Lambda_P)),$$

where ψ is the embedding $\Lambda \mapsto \Lambda_P$ and ϕ is the canonical epimorphism $\Lambda \to \Lambda/P\Lambda$.

The following facts establish some practical connections between the local and global properties of orders.

Proposition 2.7.7 (Theorem 2.3 [47]). *Let $\mathscr{A}$ be a simple algebra over F. Let P be a prime ideal of R, and Γ be an R-order in $\mathscr{A}$. Then*

(i) Γ_P is an R_P-order in $\mathscr{A}$.

(ii) Γ is a maximal R-order in $\mathscr{A}$ if and only if Γ_P is a maximal R_P-order in $\mathscr{A}$ for every prime ideal P of R.

(iii) $d(\Gamma/R)_P = d(\Gamma_P/R_P)$.

Corollary 2.7.8 (Corollary 9.6 [15]). *If P does not divide $d(\Lambda/R)$, then Λ_P is maximal R_P-order.*

Extremal orders and especially Proposition 2.7.13 below play a key role in the method for constructing maximal orders.

Definition 2.7.9. We say that Γ_P radically contains Λ_P if and only if $\Lambda_P \subseteq \Gamma_P$ and $\mathrm{Rad}(\Lambda_P) \subseteq \mathrm{Rad}(\Gamma_P)$. The orders maximal with respect to this partial ordering are called *extremal*. Maximal orders are obviously extremal.

Proposition 2.7.10 (Proposition 4.1 [26]). *An R_P-order Λ_P is extremal if and only if $\Lambda_P = \mathscr{O}_l(\mathrm{Rad}(\Lambda_P))$.*

Lemma 2.7.11 (Lemma 2.7 [26]). *Let P be a prime ideal of the ring R, Λ an R-order and suppose that $\mathscr{O}_l(\mathrm{Rad}(\Lambda_P)) \supset \Lambda_P$. Let I denote the inverse image of $\mathrm{Rad}(\Lambda_P)$ with respect to the embedding $\Lambda \mapsto \Lambda_P$. Then we have $I \supseteq P\Lambda$ and $\mathscr{O}_l(I) \supset \Lambda$.*

The previous corollary together with Corollary 2.7.6 gives us the following.

Lemma 2.7.12. *If $\mathscr{O}_l(\phi^{-1}(\mathrm{Rad}(\Lambda/P\Lambda)) = \Lambda$, the order Λ_P is extremal.*

Proposition 2.7.13 (Theorem 4.5 [26]). *Let $\Lambda_P \subset \Gamma_P$ be R_P-orders in $\mathscr{A}$. Suppose that Λ_P is extremal and that Γ_P is minimal among the R_P-orders properly containing Λ_P. Then there exists an ideal $\mathscr{J}$ of Λ_P minimal among those containing $\mathrm{Rad}(\Lambda_P)$ such that $\mathscr{O}_l(\mathscr{J}) \supseteq \Gamma_P$.*

Chapter 3

Coding-theoretic preliminaries

3.1 The MIMO channel model

A distinguishing characteristic of wireless channels is the fact that there are many different paths between the transmitter and the receiver. This means that, instead of simply receiving the transmitted signal, the receiver will get several different versions of the signal. All these multipath components are then added together at the receiver, which results in signal fading since the phase factors of distinct components have a tendency to cancel each other out. In addition to the faded signal, some other factors are added to the mix: thermal noise, interference from other users etc. These extra terms can adequately be modeled by Gaussian random variables. There are many different models which describe the fading effect due to multipath propagation, but in what follows we mostly restrict ourselves to the Rayleigh fading model. Good handbooks for wireless communications and space-time coding are [54] and [28], among others. First, let us give a formal definition for a space-time (ST) code. We restrict ourselves to square matrices; the generalization to rectangular matrices is straightforward.

Definition 3.1.1. A *space-time code* $\mathscr{C}$, sometimes also referred to as a *MIMO* code, is a finite collection of complex matrices

$$X = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} \in \mathscr{C} \subset \mathscr{M}_n(\mathbb{C}).$$

The rows represent different transmit antennas, i.e. *space*. The different *time* slots are represented by the columns. The first transmit antenna sends x_{1j} in the jth time slot, the second antenna sends x_{2j}, etc.

Rayleigh fading is a statistical model for the effect of a propagation environment on a radio signal, such as that used by wireless devices. The model assumes

that the signal will fade according to a Rayleigh distribution, and experience has shown that it describes the effects of the heavily built-up urban environment on the transmitted signal reasonably well. We use a somewhat simplified channel model which is sufficient for the purposes of this thesis.

Let us denote by n_t (resp. n_r) the number of transmitting (Tx) (resp. receiving (Rx)) antennas. We assume the coherent $n_t \times n_r$ MIMO channel with perfect channel state information (CSI) available at the receiver. Let X be a codeword matrix coming from a space-time code $\mathscr{C} \subset \mathscr{M}_n(\mathbb{C})$. We assume that the quasi-static interval, i.e. the coherence time during which the channel remains constant, and the block length n are equal. We only consider square matrices and hence further assume that $n_t = n$. Now the transmitted signal is received in the form

$$Y = \sqrt{\rho}HX + N \in \mathscr{M}_{n_r \times n}(\mathbb{C}), \tag{3.1}$$

where $H \in \mathscr{M}_{n_r \times n}(\mathbb{C})$ is the channel response matrix and $N \in \mathscr{M}_{n_r \times n}(\mathbb{C})$ is the noise matrix. The entries of both H and N are independent identically distributed (i.i.d.) zero-mean complex circular Gaussian random variables with unit variance. Let $||X||_F$ denote the Frobenius norm of X (corresponds to the squared Euclidean norm of the vectorized matrix, i.e. the sum of the squares of all the matrix elements). We assume the code $\mathscr{C}$ satisfies the overall power constraint

$$\frac{1}{|\mathscr{C}|} \sum_{X \in \mathscr{C}} ||X||_F^2 = n. \tag{3.2}$$

We then easily see that the parameter ρ represents the average signal to noise ratio (SNR) at the receive antennas.

3.2 Code design criteria for space-time codes

Let us assume that the receiver has to decide (based on the Euclidean metric) knowing the channel, whether X or X' was transmitted. Let $X^\dagger$ denote the hermitian transpose of X. The probability $P_e = P(X \to X')$ that the receiver makes an error between X and X' gives us a clue of the criteria we need for designing good codes. At high SNR values ρ the right hand side of the below inequality gives a good approximation to the pairwise error probability.

$$P_e \leq \frac{1}{(\det((X-X')(X-X')^\dagger))^{n_r} \rho^{n_t n_r}}. \tag{3.3}$$

From the above pairwise error probability (PEP) point of view [51], the performance of a space-time code is dependent on two parameters: *diversity gain* and *coding gain*. At high SNRs, a log-log plot of the corresponding error rates is a straight line. Roughly speaking, the diversity gain is the slope of the asymptote. Although two codes with the same diversity gain achieve the same asymptotic

slope, they can still differ in the horizontal shift of their asymptotes. The coding gain of a space-time code is an approximate measure of the offset of the asymptote. Together with (3.3), this leads us to the natural code design criteria given below.

The diversity gain is the minimum of the rank of the difference matrix $X - X'$ taken over all distinct code matrices $X, X' \in \mathscr{C}$, and it is also called the *rank* of the code $\mathscr{C}$. When $\mathscr{C}$ is a full-rank code, the coding gain is proportional to the determinant of the matrix $(X - X')(X - X')^\dagger$. The minimum of this determinant taken over all distinct code matrices is called the *minimum determinant* or coding gain of the code $\mathscr{C}$. If the coding gain is bounded away from zero, even in the limit as the size of the code approaches infinity, then the ST code is said to have the *non-vanishing determinant* (NVD) property [4]. For non-zero square matrices, having full-rank coincides with being invertible.

The goal is to design sets of full-rank matrices with large and preferably non-vanishing minimum determinants.

These design criteria, to some extent, depend on the premise that the receiver will know the channel response matrix, but the transmitter will not. If the transmitter also has this piece of information, then other methods are used. For example, in modern cell phone networks, the user's equipment reports its measured channel coefficients back to the base station, and the MIMO transmission aimed at that particular phone may then be adapted accordingly. Nevertheless, the situations where the transmitter is denied this information occur. In broadcast applications there are several recipients of the same signal, and such tuning is useless. Also, in the case of a rapidly moving cellular phone, e.g. one on a fast train, the channel conditions may vary so rapidly that the received information will become outdated so quickly that it is practically useless. The situation changes quite a lot of if the receiver does not know the channel. The code design for this *non-coherent* channel has a whole theory of its own.

Remark 3.2.1. The term 'diversity' has multiple meanings in wireless communications. Henceforth, diversity will refer to (spatial) diversity, as defined below in (3.10).

Remark 3.2.2. When we discuss the coding gain of a finite code we always suppose that the code is scaled so that the overall energy constraint in (3.2) is met. This normalization allows us to reasonably compare two finite codes of the same size.

The next example introduces the reader to the first explicit space-time code designed for the 2×1 MIMO channel, namely the Alamouti code [2].

Example 3.2.3. The Hamiltonian quaternions form a neat set for illustrating the above. Let $i^2 = j^2 = k^2 = -1$, and $ij = k$. If a, b, c, and d range over $\mathbb{R}$, we

define the set **H** of Hamiltonian quaternions as the one containing the elements $q = a + bi + cj + dk$. This set becomes a ring by extending the above multiplication rules linearly. It might be helpful for the reader to notice that $\mathbf{H} \simeq \mathbb{C} \oplus \mathbb{C}j$. The conjugate quaternion $\overline{q} = a - bi - cj - dk$ tells us that $q\overline{q} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R} \setminus \{0\}$, whenever $q \neq 0$. Thus, the quaternions form a division algebra.

The quaternions can be conveniently represented either by complex 2×2 matrices or by real 4×4 matrices with respect to a suitable basis. We now write $z_1 = a + bi$ and $z_2 = c + di$ and let z^* denote the complex conjugate of z. The complex matrix takes the form

$$q = \begin{pmatrix} z_1 & -z_2^* \\ z_2 & z_1^* \end{pmatrix} \tag{3.4}$$

with respect to the basis $\{1, j\}$. We identify the element q with its matrix representation q and recycle the same notation.

The Alamouti code [2] is now obtained by selecting complex integer vectors (z_1, z_2), i.e. the *Lipschitz quaternions*, and mapping them to codewords of the 2-antenna ST-code as in (3.4) above. The rank criterion is automatically met, and the minimum determinant of q is the squared minimum Euclidean distance.

Remark 3.2.4. In Remark 2.1.2 it was noted that the set of integral elements does not form a ring in the non-commutative case. As an easy counter-example one can use the ring of Lipschitz quaternions

$$\mathscr{L} = \{q = a + bi + cj + dk \in \mathbf{H} \mid a, b, c, d \in \mathbb{Z}\}$$

from the above example. For instance, consider the polynomial $f(x) = x^2 + 1$ having integral coefficients. The element $t = \frac{3i+4j}{5}$ is one of the (infinitely many) roots of the polynomial $f(x)$, and hence may be called integral. However, if we try to adjoin t to the ring $\mathscr{L}$, we end up with a set that will also contain the element it. The reduced trace $tr(it) \in \mathbb{Q}$ is not an integer, hence we cannot have an order that would contain both the Lipschitz quaternions and t.

Remark 3.2.5. Proposition 2.5.4 provides us with a tool for producing codes satisfying the NVD property. See Proposition 4.2.6 for a more thorough explanation. In the above example, the Alamouti code corresponds to the natural order of the cyclic division algebra $(\mathbb{Q}(i)/\mathbb{Q}, \sigma = {}^*, \gamma = -1)$ (cf. Section 2.4 and Example 2.5.5), hence, according to Proposition 2.5.4, $\det(q) \in \mathbb{Z}$ and $\det(q) \geq 1$ for all $0 \neq q \in \mathbf{H}$.

The *data rate* R in bits per channel use (bpcu) is given by

$$R = \frac{1}{n}\log_2(|\mathscr{C}|), \tag{3.5}$$

where $|\mathscr{C}|$ is the code size and n is the number of channel uses. The data rate should not be confused with the *rate of a code design* (in short, the *code rate*) defined as the ratio,

$$\frac{k}{n}, \tag{3.6}$$

of the number k of transmitted (complex) information symbols, e.g. quadrature amplitude modulation (QAM) symbols matching Gaussian integers, to the decoding delay n. If this ratio is equal to the delay, then the code is said to have a *full rate*.

Remark 3.2.6. If one intends to use n_r receive antennas and perform sphere decoding or some other simple decoding method at the receiver, then *the code rate should not exceed* n_r, i.e. we must have $\frac{k}{n} \leq n_r$. In order to achieve as high a rate as possible while enabling sphere decoding, one should choose the rate $\frac{k}{n} = n_r$. See [18, 38] for a more detailed justification of this claim.

The contents of the following section are mainly taken from [28], [54], and [38].

3.3 Spatial diversity and multiplexing

The Rayleigh fading channel model (3.1) describes sudden declines in power. As discussed earlier, this fading is due to the destructive addition of multipath signals in the propagation media. Also interference from other users may complicate the situation. The received power can thus change significantly. On the other hand, the power of the thermal noise at the receiver does not usually change very much. As a result, if the signal undergoes significant fading, the effective SNR at the receiver may drop dramatically. In practice, for a fixed rate there is a minimum SNR for which the receiver can still reliably detect and decode the transmitted signal. For a SNR below this threshold, recovering the signal reliably is impossible. This event is referred to as an *outage*. The outage probability can be calculated based on the statistical model describing the channel, or one can measure the actual real-life channel.

The main idea behind diversity is to provide the receiver with different replicas of the transmitted signal. If the multiple antennas used are far enough apart from each other, then the paths between different pairs of antennas can be considered as independent. In this way it is less probable that all the copies of the transmitted signal would significantly fade simultaneously. As a result the outage probability will be lower than for a system with a lower diversity.

More technically, diversity (or diversity gain) can be defined as the slope of the error probability curve in terms of the received SNR in a log-log scale.

Multiple transmit antennas can also be utilized to achieve goals other than diversity. For instance, a higher capacity and, as a result, a higher transmission rate

are possible by increasing the number of transmit antennas. Let us, for the sake of simplicity, assume a symmetric MIMO channel equipped with equal numbers of transmit and receive antennas. Then, in a rich scattering environment the capacity increases linearly with the number of transmit antennas without increasing the transmission power. This results in the possibility of transmitting at a higher rate by using spatial multiplexing. In general, one can transmit up to $\min\{n_t, n_r\}$ symbols in one time slot (see the remark below). For example, if $n_t \geq n_r$, one can send n_r symbols and achieve a diversity gain of $n_t - n_r + 1$. On the other hand, the maximum spatial diversity while transmitting only one symbol per time slot is $n_t n_r$. Therefore, we can benefit from a MIMO channel in two ways: (i) we can increase the diversity of the system, and (ii) we can increase the number of transmitted symbols.

Remark 3.3.1. The received signal belongs to a t-dimensional complex vector space, where $t = 2n_r n$. From this it is clear that the receiver cannot decode a lattice (see Section 4.1) that has rank $> t$, because the infimum of the euclidean distance of points in such a lattice is zero. This gives us a natural upper bound for the multiplexing gain.

Remark 3.3.2. The capacity of a MIMO channel increases by raising the SNR. Since the transmission rate relates to capacity, it is reasonable to hope that the rate can be increased as the SNR increases. This motivates the formal definition of (spatial) multiplexing gain (3.7).

Let us next give the formal definition of the diversity-multiplexing tradeoff.

When the channel matrix H is known completely to the receiver but not to the transmitter, Telatar [53] first showed that the ergodic channel capacity of such an $n_t \times n_r$ MIMO channel approximates to $\min\{n_t, n_r\} \log_2 \mathrm{SNR}$ at high SNR regime, regardless of the relation between n_t and n_r. Furthermore, it was shown that such a capacity can be achieved by using i.i.d. complex Gaussian random vectors $\underline{x}$ having a covariance matrix $K_X = \frac{\mathrm{SNR}}{n_t} I_{n_t}$. On the other hand, assuming that the transmitter communicates at a rate of

$$R \;=\; r \log_2 \mathrm{SNR} \qquad \text{(bits/channel use)}, \tag{3.7}$$

where r, $0 \leq r \leq \min\{n_t, n_r\}$, is termed the *multiplexing gain*, Zheng and Tse [58] proved that given r, the smallest bit error probability that can be achieved by any coding scheme is given by

$$P_{\mathrm{e,min}}(\mathrm{SNR}) \;\doteq\; \mathrm{SNR}^{-d^*(r)}, \tag{3.8}$$

where by $\doteq$ we mean the exponential equality defined by

$$\lim_{\mathrm{SNR}\to\infty} \frac{\log P_{\mathrm{e,min}}(\mathrm{SNR})}{\log \mathrm{SNR}} \;=\; -d^*(r). \tag{3.9}$$

The negative exponent $d^*(r)$ is termed *diversity gain*, and is given by a piecewise-linear function connecting the points

$$\big\{(r,(n_t-r)(n_r-r)) \;:\; r=0,1,...,\min\{n_t,n_r\}\big\}. \tag{3.10}$$

Particularly, for the MISO case we get

$$d^*_{MISO}(r) = n_t(1-r), \quad 0 \le r \le 1. \tag{3.11}$$

Here, $d^*(r)$ indicates an optimal tradeoff between the multiplexing gain r and the diversity gain, and is thus also termed the *diversity-multiplexing tradeoff* (DMT) of a Rayleigh fading channel. It is also proved in [58] that $d^*(r)$ can be achieved by using i.i.d. length-n_t complex Gaussian random vectors, provided that the asymmetric MIMO Rayleigh fading channel is quasi-static and the channel matrix H remains fixed for T channel uses with $T \ge n_t + n_r - 1$.

Invigorated by this remarkable result, a considerable amount of research activity has been devoted to constructing coding schemes [5, 7, 29, 8, 52] to achieve the optimal tradeoff $d^*(r)$ in (3.10). In particular, Elia *et al.* [8] have provided a sufficient condition for having deterministic DMT optimal codes. Furthermore, they have proposed an algebraic construction of $n_t \times n_t$ code matrices meeting this sufficient condition for all $n_t \ge 2$ and $T \ge n_t$, using a cyclic division algebra with degree n_t^2 over its center $\mathbb{Q}(i)$, where $i=\sqrt{-1}$. One step further was taken in [16], where Hollanti *et al.* showed that, with the aid of maximal orders, the CDA-based DMT-achieving constructions can be further improved in terms of density. A denser code provides a better error performance even at low and moderate SNRs, whereas DMT optimality is an asymptotic measure.

Remark 3.3.3. The relationship of the above spatial multiplexing gain to the transmission rate is similar to that of the diversity gain to the probability of error in (3.9). In other words, multiplexing gain measures how far the rate R is from capacity.

Let us quickly go back to Example 3.2.3 before moving on to the next section.

Example 3.3.4. The Alamouti code is DMT-achieving for the 2×1 MISO case, but fails to do so in the 2×2 MIMO case, as it is rate-one and hence not fully multiplexing.

Let us now assume a 2×1 channel and take look at the received signal when an Alamouti codeword q is transmitted. It takes the form

$$(y_1\; y_2) = (h_1\; h_2)\begin{pmatrix} z_1 & -z_2^* \\ z_2 & z_1^* \end{pmatrix} + (n_1\; n_2)$$

and can be rewritten as

$$\begin{pmatrix} y_1 \\ y_2^* \end{pmatrix} = \begin{pmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{pmatrix}\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2^* \end{pmatrix}. \tag{3.12}$$

Let us denote by H the matrix in (3.12) containing the channel coefficients. The columns of H are orthogonal to each other and have the same Euclidean norms. Thus, when we multiply (3.12) from the left by $H^{\dagger}$, the received vector takes the new form

$$\begin{pmatrix} y_1' \\ y_2' \end{pmatrix} = \begin{pmatrix} |h_1|^2+|h_2|^2 & 0 \\ 0 & |h_1|^2+|h_2|^2 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} + \begin{pmatrix} n_1' \\ n_2' \end{pmatrix}, \tag{3.13}$$

where n_1', n_2' remain i.i.d.. The channel now actually corresponds to two parallel SISO channels and hence (see [44, Section 3.4.1, p. 33]) the error probability is asymptotically given by

$$P_{e,Alamouti} \approx \mathsf{SNR}^{-2(1-r)}.$$

By setting $n_t = 2$ in Equation (3.11), we can conclude that the Alamouti code is optimal in terms of the DMT of a 2×1 channel.

Chapter 4

Space-time codes from cyclic division algebras

In this chapter, we will introduce cyclic division algebras and their orders as a tool for space-time coding. We begin by mentioning that it was a long and rocky path to discovering that cyclic algebras could be used and that indeed we were dealing with objects called orders.

When we began this work, our intention was just to produce ST codes for the 4×1 MISO system [14]. As specified by the code design criteria, we wanted these codes to have full rank and a minimum determinant as large as possible. Already in [14] we managed to build codes with the NVD property. The tools at hand at that time were not very sophisticated, so this took a lot more effort than was necessary. Thanks to Sethuraman *et al.* [48], cyclic division algebras were finally introduced in 2003 and the first ST codes were built using them. The use of CDAs enabled full multiplexing as they produced full lattices. For the first time, the code matrix was fully packed with no wasted space. These codes, however, did not enjoy the NVD property as transcendental elements were used instead of algebraic numbers.

Later in 2003, Belfiore and Rekaya [4] pointed out that one should use a specific subring instead of the whole algebra in order to guarantee a non-vanishing determinant. Whilst working on [14] we realized that there exists something called order, and the above mentioned subring as well as our example rings in [14] are occurrences of such orders. We also managed to prove with some ad hoc methods that the densest code in [14] corresponds to a maximal order. This led us to further investigate orders and their properties [16]. It was noticed that by using a maximal order within a given CDA, we obtain the densest possible codes. If the algebra is not fixed, then we first pick an algebra that has maximal orders with a minimal discriminant, as these are the densest among all the maximal orders within *any* CDA [15] (see the framed statements at the end of Sections 4.1 and 4.3). This observation provided us with codes that are already very close to the outage bound [32]. With practical numbers of antennas there is hardly any gap between the per-

formance of a maximal order code and the outage bound, even at low SNRs.

Achieving promising results with the symmetric (#Tx antennas = #Rx antennas) ST codes motivated us to try the same with the asymmetric (#Tx antennas > #Rx antennas) space-time (AST) codes as well. In [19] we generalized the density results from [15] to the asymmetric scenario. The situation was now more complicated as rather that only having two principal options for the center of the algebra, as in the symmetric scenario (see Corollaries 4.3.2 and 4.3.4), the center could be almost any field of a suitable degree. When we started this work, we did not even know how to construct AST codes with a suitable rate and the NVD property. One way to construct AST codes was proposed in [25], but we were not aware of this work until we had independently discovered the same method and noticed that the performance it provided was not satisfactory. Also the block structure we introduced in [22] was independently discovered in [57] in the context of amplify-and-forward relay codes.

Finally in [22, 23, 19] different construction methods for asymmetric codes were proposed, one of them based on maximal orders. Not surprisingly, the codes from maximal orders outperformed all competing codes. Later on, both transmit antenna selection (TAS) [21, 38] and the situation where one wants to effectively use all the transmit antennas [18, 20] were considered, and optimal constructions with excellent error performance were given.

4.1 Lattices: normalized minimum determinant and density

We define a *lattice* to be a discrete finitely generated free abelian subgroup L of a real or complex finite dimensional vector space, called the ambient space. In the space-time (ST) setting a natural ambient space is the space $\mathscr{M}_n(\mathbb{C})$ of complex $n \times n$ matrices. The *Gram matrix* is defined as

$$G(L) = \left(\Re(\mathrm{Tr}(x_i x_j^\dagger))\right)_{1 \leq i,j \leq k}, \tag{4.1}$$

where Tr is the matrix trace, and $x_i \in \mathscr{M}_n(\mathbb{C})$, $i = 1, \ldots, k$, form a $\mathbb{Z}$-basis of L. The rank k of the lattice is upper bounded by $2n^2$. We remark that we need to take the real part of the trace in the Gram matrix, as the matrices $x_i x_j^\dagger$ are not necessary real for $i \neq j$. The Gram matrix has a positive determinant equal to the squared measure of the fundamental parallelotope $m(L)^2$. A change of basis does not affect the measure $m(L)$.

Any lattice L with the NVD property can be scaled, i.e. multiplied by a real constant t, either to satisfy $\det_{min}(L) = \min_{M \in L \setminus \{0\}} \{\det(M)\} = 1$ or to satisfy $m(L) = 1$. This is because $\det_{min}(tL) = t^n \det_{min}(L)$ and $m(tL) = t^k m(L)$. As the minimum determinant determines the asymptotic pairwise error probability, this gives rise to natural numerical measures for the quality of a lattice.

Definition 4.1.1. We shall denote by $\delta(L)$ the *normalized minimum determinant* of the lattice L, i.e. here we first scale L to have a unit size fundamental parallelotope. Dually we denote by $\rho(L) = 1/m(L)$ the *normalized density* of the lattice L, having first scaled the lattice to have unit minimum determinant, and only then computing the quantity $1/m(L)$. In other words, we define

$$\delta(L) = \frac{\det_{min}(L)}{m(L)^{n/k}},$$

$$\rho(L) = \frac{(\det_{min}(L))^{k/n}}{m(L)}.$$

There are two different point of views one can adopt related to the density. Firstly, assume that both of the lattices we consider have a unit minimum determinant. Now a denser code means that we can pack more codewords within a same space as compared to a lattice having a lower density. That is, the data rate (3.5) is improved. Secondly, if instead of increasing the rate we normalize the lattices to have a unit measure, then according to the above definition the (normalized) minimum determinant of the denser lattice is bigger than that of the other lattice.

Definition 4.1.2. A *MIMO code* or *space-time code* refers to the infinite code $\mathscr{C}_\infty$ which is a lattice in $\mathscr{M}_n(\mathbb{C})$.

In this thesis, we consider only codes that are subsets in an infinite complex lattice. Then, for an infinite code lattice $\mathscr{C}_\infty$ in Section 3.2, we can just look at non-zero matrices instead of the differences, as the difference of two lattice points is again a point in the same lattice.

Remark 4.1.3. The minimum determinant defined here is actually the square root of the minimum determinant defined in Section 3.2.

Remark 4.1.4. When comparing the minimum determinants of different codes, one should always use the normalized minimum determinant. Otherwise the notion of minimum determinant would be somewhat meaningless, as for example $\det_{min}(2L) = 2^n \det_{min}(L)$. Therefore we need the above normalization. According to Definition 4.1.1 and Section 3.2, we can refer to $\delta(L)^2$ as the coding gain of the corresponding MIMO code.

Remark 4.1.5. To avoid confusion let us mention that from now on, when we talk about the minimum determinant we always mean the minimum determinant $\det_{min}(L)$ of the infinite code lattice $L = \mathscr{C}_\infty$. For our purposes it suffices to consider infinite lattices, thus we can ignore the side effects caused by the finiteness of the actual code.

According to Definition 4.1.1, the above can be formalized as follows:

Proposition 4.1.6. *The coding gain of a lattice L equals*

$$\delta(L)^2 = \rho(L)^{2n/k}.$$

Now we can conclude this section by stating:

Maximizing the coding gain is equivalent to maximizing the density of the corresponding lattice.

We emphasize that this is one of the main contributions of this work, as we have now produced a well-defined criterion for maximizing the coding gain. Later on in Section 4.4, we will see that the previously known methods for code construction are insufficient, if one hopes to achieve maximal coding gains. Indeed, in Section 4.4 it will be shown that there exists a 2×2 MIMO code having $\delta(L) = 0.562$ as opposed to the Golden code that has $\delta(L) = 0.447$.

4.2 Lattices from matrix representations of orders

Why do we want to use cyclic division algebras and their orders to construct ST codes? Firstly, division algebras have no zero divisors, so the rank criterion (cf. Section 3.2) is automatically met. The cyclic representation is moreover simple to deal with. Secondly, orders help us to increase the coding gain by providing us with the NVD property. When we choose the center carefully, a discrete set of determinants is guaranteed.

Some authors have made the assumption that the so-called linear dispersion encoding is used. Therein a fixed subset of a complex alphabet lattice (such as QAM or HEX, corresponding to Gaussian or hexagonal lattice, respectively) is chosen, and sequences of symbols from that subset are then turned into lattice points by the simple process of using them as coefficients of a fixed basis (as a module over a ring generated by the alphabet) of the actual lattice. From our point of view this approach places undue emphasis on the encoding process, so we largely ignore this aspect. Therefore questions like whether our lattices are 'information lossless' (cf. [49],[43]) are meaningless, because that concept is defined only under the assumption of linear dispersion encoding.

This change means that we often need to resort to the use of a codebook, and thus the complexity of encoding is higher. But, consequently, we are also free to do optimal spherical shaping. In other words, we choose our finite codebook to consist of shortest vectors (not necessarily all of them) of the lattice or of a coset of the lattice, and thus minimize the transmission power.

Our lattices of $n \times n$ matrices are of rank $2n^2$. This implies that if we impose a constraint on the transmission power and require that $\mathrm{Tr}(XX^\dagger) \leq P$ for all the matrices X in a codebook, then the number of signals X meeting this constraint grows

like $O(P^{n^2})$ as a function of maximal transmission power P. Thus, they automatically share this property with the full-rate linear dispersion codes. Therefore, we are entitled to use Theorem 3 from [8] and conclude that, also for the maximal order codes, the NVD property implies DMT-optimality.

Again let E/F be a cyclic Galois extension with $\mathrm{Gal}(E/F) = \langle\sigma\rangle$ (cf. Section 2.4).

Definition 4.2.1. Let $a = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \Lambda \subset \mathscr{A} = (E/F, \sigma, \gamma)$, where Λ is a maximal order. The basic form of a cyclic division algebra based space-time code coming from a maximal order is

$$\mathscr{C} \subset \mathscr{C}_\infty = \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix} \right\}, \qquad (4.2)$$

where $\gamma \in F$ is a suitable non-norm element. Here, the above infinite code lattice $\mathscr{C}_\infty$ can be identified with the standard matrix representation of the order Λ. Notice that as opposed to the natural order, the elements $x_i \in E$ in (4.2) are not necessarily integral!

If we denote the basis of E over F by $\{1, e_1, ..., e_{n-1}\}$, then the elements x_i, $i = 0, ..., n-1$, in the above matrix take the form $x_i = \sum_{k=0}^{n-1} f_k e_k$, where $f_k \in F$ for all $k = 0, ..., n-1$. Hence $k = n^2$ information symbols, e.g. Gaussian or Eisensteinian integers corresponding to QAM and HEX signaling respectively, are transmitted inside the matrix (n per channel use). This is equal to saying that the design has a full rate $\frac{k}{n} = \frac{n^2}{n} = n$ (cf. (3.6)).

Remark 4.2.2. We recall that the natural order only exists, when γ is an algebraic integer. In this case an immediate consequence of Lemma 2.5.7 is that Λ_{NAT} has a finite index in the maximal order Λ. In particular, as lattices, Λ_{NAT} and Λ share the same rank.

A full rate is guaranteed when using full lattices, i.e. lattices that have rank equal to $2n^2$. For the asymmetric scenario, however, full lattices are out of the question, at least if we wish to preserve the ability to perform simple decoding, e.g. sphere decoding, at the receiver (cf. Remark 3.2.6). In this case, we need to modify the dimension of the algebra and the degrees of the extensions appropriately, or we can choose a certain subset of the corresponding symmetric code [19]. In particular, a two-dimensional center is now out of our reach. Taking into account that for the use of the famous QAM and HEX modulation alphabets we need $\mathbb{Q}(i) \subseteq \mathscr{A}$ or $\mathbb{Q}(\omega) \subseteq \mathscr{A}$, it can be seen that the set of possible centers stretches significantly when compared to the symmetric scenario.

Remark 4.2.3. There exist practical methods for picking the right non-norm element, so this is not a hard task. It may be impossible to find a unit γ. In this case, we can either suffer from an antenna energy imbalance, or we can try to force the γ to have a unit modulus by dividing it by some suitable element with the same absolute value [9]. The latter option means a loss in the minimum determinant (as we will not have an order anymore) but, due to the additive way in which we form the codeword from the basis matrices, it will still be non-vanishing. This loss is often compensated by an improved error performance [19].

Albeit there is no question of energy balance being important, one ought to be careful and notice that sometimes a unit non-norm element may still lead to higher average energy requirements. This is due to the fact that sometimes we cannot simply replace a non-unit γ with a unit one without having to change the whole algebra. It is well possible that despite a unit γ this change in the algebra will result in a higher average energy.

The shaping of the code is also important [43]. The closer the code is to being orthogonal, the easier the encoding, decoding and bit labeling will be. However, restricting to orthogonal codes only would prevent us from achieving the best possible coding gains. Hence, we do not make this restriction, and instead of simple encoding we will use a codebook or sphere encoding (see [32]) to guarantee optimal spherical shaping.

We remark that the energy and shaping discussion is of very technical nature, hence a reader with no sufficient background can safely ignore this remark.

A division algebra may be represented as a cyclic algebra in many ways as demonstrated by the following example.

Example 4.2.4. The division algebra $\mathscr{GA}$ used in [5] to construct the Golden code is the cyclic division algebra with $F = \mathbb{Q}(i)$, $E = \mathbb{Q}(i, \sqrt{5})$, $\gamma = i$, when the F-automorphism σ is determined by $\sigma(\sqrt{5}) = -\sqrt{5}$. We also note that in addition to this representation $\mathscr{GA}$ can be given another construction as a cyclic algebra. As $u^2 = i$ we immediately see that $F(u)$ is a subfield of $\mathscr{GA}$ that is isomorphic to the eighth cyclotomic field $E' = \mathbb{Q}(\zeta)$, where $\zeta = (1+i)/\sqrt{2}$. The relation $u\sqrt{5} = -\sqrt{5}u$ read differently means that we can view u as the complex number ζ and $\sqrt{5}$ as the auxiliary generator $u' = \sqrt{5}$. We thus see that the cyclic algebra

$$E' \oplus u'E' = (E'/F, \sigma', \gamma')$$

is isomorphic to the Golden algebra. Here σ' is the F-automorphism of E' determined by $\zeta \mapsto -\zeta$ and $\gamma' = u'^2 = 5$.

Remark 4.2.5. We remark that two different, algebraically isomorphic constructions may still yield codes with significant differences in performance. In addition to the minimum determinant, the shape of the code lattice also plays a key role.

When research into CDA-based ST codes began, transcendental elements were used as non-norm elements and thus the resulting codes did not have the NVD

property [48]. Later on, it was noticed, [4], that by choosing the elements in the codeword matrix (2.5) to be algebraic integers instead of transcendental elements, i.e. by using a certain subring of an algebra with an integral non-norm element, one could obtain codes with the NVD property. Soon after this, it was pointed out in [13, 14] that these subrings are examples of *orders*, and that some further optimization can still be done by exploiting the algebraic properties of orders [16, 15].

The reason for concentrating on orders when constructing MIMO lattices is summarized in the following proposition. This is simply Proposition 2.5.4 rephrased to fit the language of MIMO-lattices. We often identify an order (and its subsets) with its standard matrix representation.

Proposition 4.2.6. *Let Λ be an order in a cyclic division algebra $(E/F, \sigma, \gamma)$. Then for any non-zero element $a \in \Lambda$ its reduced norm $nr(a)$ is a non-zero element of the ring of integers $\mathcal{O}_F$ of the center F. In particular, if F is $\mathbb{Q}$ or an imaginary quadratic number field, then the minimum determinant of the lattice Λ is equal to one.*

Note that if γ is not an algebraic integer, then Λ fails to be closed under multiplication. This may adversely affect the minimum determinant of the resulting matrix lattice, as elements not belonging to an order may have non-integral (and hence small) norms.

The power of orders in ST code construction is based on two things:

1) They yield codes that satisfy the NVD property, and

2) they provide us with a tool called a discriminant which reveals the algebra and order that will result in the best coding gain.

4.3 Discriminant vs. density

The definition of the discriminant closely resembles that of the Gram matrix of a lattice, so the following results are not very surprising. Nevertheless, they are extremely important in our hunt for denser lattice codes.

For explicit code constructions, see Example 4.4.16.

Lemma 4.3.1. *Assume that F is an imaginary quadratic number field and that 1 and θ form a $\mathbb{Z}$-basis of its ring of integers R. Assume further that the order Λ is a free R-module (an assumption automatically satisfied when R is a principal ideal domain). Then the measure of the fundamental parallelotope equals*

$$m(\Lambda) = |\Im\theta|^{n^2} |d(\Lambda/R)|.$$

Proof. [15, Lemma 5.1] □

In the cases $F=\mathbb{Q}(i)$ and $F=\mathbb{Q}(\sqrt{-3})$, we have $\theta=i$ and $\theta=(-1+\sqrt{-3})/2$ respectively, so we immediately get the following two corollaries.

Corollary 4.3.2. *Let $F=\mathbb{Q}(i), R=\mathbb{Z}[i]$, and assume that $\Lambda\subset(E/F,\sigma,\gamma)$ is an R-order. Then the measure of the fundamental parallelotope equals*

$$m(\Lambda)=|d(\Lambda/\mathbb{Z}[i])|.$$

Example 4.3.3. When we scale the Golden code [5] to have a unit minimum determinant, all 8 elements of its $\mathbb{Z}$-basis will have length $5^{1/4}$ and the measure of the fundamental parallelotope is thus 25. This is also a consequence of the fact that the $\mathbb{Z}[i]$-discriminant of the natural order of the Golden algebra is equal to 25. As was observed in [13], the natural order happens to be maximal in this case. Therefore the Golden code cannot be improved upon by enlarging the order within $\mathscr{GA}$.

Corollary 4.3.4. *Let $\omega=(-1+\sqrt{-3})/2$, $F=\mathbb{Q}(\omega)$, $R=\mathbb{Z}[\omega]$, and assume that $\Lambda\subset(E/F,\sigma,\gamma)$ is an R-order. Then the measure of the fundamental parallelotope equals*

$$m(\Lambda)=(\sqrt{3}/2)^{n^2}|d(\Lambda/\mathbb{Z}[\omega])|.$$

The upshot of this is that in both cases we have the following:

Maximizing the density of the code is equivalent to minimizing the discriminant.

Thus, in order to get the densest MIMO-codes we need to look for division algebras that have a maximal order with as small a discriminant as possible. If we, for one reason or another, want to stick with a specific algebra, then we should at least use a maximal order.

Example 4.3.5. Let us use the notation from Example 2.5.8. In [29], Kiran and Rajan have shown that the family of cyclic algebras $\mathscr{A}_\ell=(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(i),\sigma(\zeta_\ell)=\zeta_\ell^5,2+i)$, with $\ell\geq 3$, consists entirely of division algebras. Let $\Lambda_{NAT,\ell}$ be the natural order of the algebra $\mathscr{A}_\ell$. We can conclude from Lemma 2.5.10, Proposition 2.5.8, and Corollary 4.3.2 that

$$d(\Lambda_{NAT,\ell}/\mathbb{Z}[i])=(2+i)^{n(n-1)}(1+i)^{2n^2(\ell-2)},$$

and that

$$m(\Lambda_{NAT,\ell})^2=2^{2n^2(\ell-2)}5^{n(n-1)}.$$

For instance, in the 2 antenna case $\ell=3,n=2$, we have $m(\Lambda_{NAT,\ell})=80$, and thus the Golden code is denser than the corresponding lattice $\mathscr{A}_3$ of the same minimum determinant. However, the natural order of $\mathscr{A}_3$ is not maximal. We will return to this example later on.

To conclude the section, we include the following simple but interesting result on orders which explains why using a principal one-sided (left or right) ideal instead of the entire order will not change the density of the code. For the proof, see [15, Lemma 10.1].

Lemma 4.3.6. *Let Λ be an order in a cyclic division algebra of index n over an imaginary quadratic number field. Let $x \in \Lambda$ be any non-zero element. Then the normalized minimum determinants of the two lattices coincide:*

$$\delta(\Lambda x) = \delta(\Lambda).$$

4.4 Discriminant bounds for symmetric and asymmetric constructions

In this section, we present a fundamental lower bound for the discriminant. With the aid of this bound we are able to give upper bounds for the code density in both the symmetric and asymmetric case. In the symmetric case the bound was derived by R. Vehkalahti, [15, 55], and generalized to the asymmetric case in [18]. Most of the contents of this section can be found in [15, 18]. The main goal of this section is to motivate the use of maximal orders and to give an insight into the main results in [15, 18, 14].

Again let F be an algebraic number field that is finite dimensional over $\mathbb{Q}$, $\mathscr{O}_F$ its ring of integers, P a prime ideal of $\mathscr{O}_F$ and $\hat{F}_P$ the completion. In what follows we discuss the size of ideals of $\mathscr{O}_F$. By this we mean that ideals are ordered by the absolute values of their norms to $\mathbb{Q}$, so e.g. in the case $\mathscr{O}_F = \mathbb{Z}[i]$ we say that the prime ideal generated by $2+i$ is smaller than the prime ideal generated by 3 as they have norms 5 and 9, respectively.

The following relatively deep result from class field theory was the key to deriving the discriminant bound. Assume that the field F is totally complex. Then we have the *fundamental exact sequence of Brauer groups* (see e.g. [45] or [40])

$$0 \longrightarrow \mathrm{Br}(F) \longrightarrow \oplus \mathrm{Br}(\hat{F}_P) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0. \tag{4.3}$$

Here the first nontrivial map is obtained by mapping the similarity class of a central division F-algebra $\mathscr{D}$ to a vector consisting of the similarity classes of all simple algebras $\mathscr{D}_P$ obtained from $\mathscr{D}$ by extending the scalars from F to $\hat{F}_P$, where P ranges over all prime ideals of $\mathscr{O}_F$. Observe that $\mathscr{D}_P$ is not necessarily a division algebra, but by Wedderburn's theorem [27, p. 203] it can be written in the form

$$\mathscr{D}_P = \mathscr{M}_{\kappa_P}(\mathscr{A}_P),$$

where $\mathscr{A}_P$ is a division algebra with a center $\hat{F}_P$, and κ_P is a natural number called the *local capacity*. The second nontrivial map of the fundamental exact sequence

is then simply the sum of the Hasse invariants of the division algebras $\mathscr{A}_P$ representing elements of the Brauer groups $\mathrm{Br}(\hat{F}_P)$.

Albeit implicitly, this exact sequence tells us that, for all but finitely many primes P, the resulting algebra $\mathscr{D}_P$ is actually in the trivial similarity class of $\hat{F}_P$-algebras. In other words, $\mathscr{D}_P$ is isomorphic to a matrix algebra over $\hat{F}_P$. More importantly, the sequence tells us that the sum of the nontrivial Hasse invariants of any central division algebras must be an integer. Furthermore, this is the only constraint for the Hasse invariants, i.e. any combination of Hasse invariants a/m_P such that only finitely many of them are non-zero, and such that their sum is an integer, is realized as a collection of the Hasse invariants of some central division algebra $\mathscr{D}$ over F.

Let us now suppose that for a given number field F, we would like to produce a division algebra $\mathscr{A}$ of a given index n, having F as its center and having the smallest possible discriminant. We proceed to show that while we cannot give an explicit description of the algebra $\mathscr{A}$ in all cases, we can derive an explicit formula for its discriminant.

Theorem 4.4.1. *Assume that the field F is totally complex and that $P_1,\dots,P_n$ are some prime ideals of $\mathscr{O}_F$. Assume further that a sequence of rational numbers $a_1/m_{P_1},\dots,a_n/m_{P_n}$ satisfies*

$$\sum_{i=1}^{n}\frac{a_i}{m_{P_i}} \equiv 0 \qquad (mod \quad 1),$$

$1 \le a_i \le m_{P_i}$, and $(a_i, m_{P_i}) = 1$.

Then there exists a central division F-algebra $\mathscr{A}$ that has local indices m_{P_i} and the least common multiple (LCM) of the numbers $\{m_{P_i}\}$ as an index.

If Λ is a maximal $\mathscr{O}_F$-order in $\mathscr{A}$, then the discriminant of Λ satisfies

$$d(\Lambda/\mathscr{O}_F) = \prod_{i=1}^{n} P_i^{(m_{P_i}-1)\frac{[\mathscr{A}:F]}{m_{P_i}}}.$$

Proof. [15, Theorem 6.11] □

At this point it is clear that the discriminant $d(\Lambda)$ of a division algebra only depends on its local indices m_{P_i}.

We now have an optimization problem to solve: given the center F and an integer n, we should decide how to choose the local indices and the Hasse invariants so that the LCM of the local indices is n, the sum of the Hasse invariants is an integer, and the resulting discriminant is as small as possible. We immediately observe that at least two of the Hasse invariants must be non-integral.

Observe that the exponent $d(P)$ of the prime ideal P in the discriminant formula is

$$d(P) = (m_P - 1)\frac{[\mathscr{A}:F]}{m_P} = n^2\left(1 - \frac{1}{m_P}\right).$$

As for the nontrivial Hasse invariants $n \geq m_P \geq 2$, we see that $n^2/2 \leq d(P) \leq n(n-1)$. Therefore the nontrivial exponents are roughly of the same size. For example, when $n = 6$, $d(P)$ will be either 18, 24 or 30 according to whether m_P is 2, 3 or 6, respectively. Not surprisingly, it turns out that the optimal choice is to have only two non-zero Hasse invariants and to associate these with the two smallest prime ideals of $\mathcal{O}_F$.

Theorem 4.4.2 (Main Theorem). *Assume that F is a totally complex number field, and that P_1 and P_2 are the two smallest prime ideals in $\mathcal{O}_F$. Then the smallest possible discriminant of all central division algebras over F of index n is*

$$(P_1 P_2)^{n(n-1)}.$$

Proof. [15, Theorem 6.12] □

We remark that in the most interesting (for the symmetric MIMO) cases $n = 2$ and $n = 3$, the proof of Theorem 4.4.2 is more or less an immediate corollary of Theorem 4.4.1. We also remark that the division algebra which achieves our bound is by no means unique; any pair of Hasse invariants $a/n, (n-a)/n$, where $0 < a < n$, and $(a,n) = 1$, leads to a division algebra with the same discriminant.

4.4.1 Symmetric codes

The smallest primes of the ring $\mathbb{Z}[i]$ are $1+i$ and $2 \pm i$. They have norms 2 and 5, respectively. The smallest primes of the ring $\mathbb{Z}[\omega]$ are $\sqrt{-3}$ and 2 with respective norms 3 and 4. Together with Corollaries 4.3.2 and 4.3.4 we have arrived at the following bounds.

Corollary 4.4.3 (Discriminant bound). *Let Λ be an order of a central division algebra of index n over the field $\mathbb{Q}(i)$. Then the measure of a fundamental parallelotope of the corresponding lattice is*

$$m(\Lambda) \geq 10^{n(n-1)/2}.$$

Corollary 4.4.4 (Discriminant bound). *Let Λ be an order of a central division algebra of index n over the field $\mathbb{Q}(\omega)$, $\omega = (-1+\sqrt{-3})/2$. Then the measure of a fundamental parallelotope of the corresponding lattice is*

$$m(\Lambda) \geq (\sqrt{3}/2)^{n^2} 12^{n(n-1)/2}.$$

Corollary 4.4.5 (Density bounds). *From the above corollaries we also obtain the corresponding density bounds. Let Λ be an order of a central division algebra of*

index n over the field (1) $\mathbb{Q}(i)$ or (2) $\mathbb{Q}(\omega)$. Then the normalized density $\rho(\Lambda)$ of the corresponding lattice satisfies the inequality

$$(1) \quad \rho(\Lambda) \leq 10^{n(1-n)/2} \quad \textit{or}$$
$$(2) \quad \rho(\Lambda) \leq (2/\sqrt{3})^{n^2} 12^{n(1-n)/2},$$

respectively.

Remark 4.4.6. The Golden algebra reviewed in Example 4.2.4 has its nontrivial Hasse invariants corresponding to the primes $2+i$ and $2-i$ and hence cannot be an algebra which achieves the bound of Theorem 4.4.2.

A clue for finding the optimal division algebra is hidden in the alternative description of the Golden algebra given in Example 4.2.4. It turns out that in the case $F = \mathbb{Q}(i)$, $E = \mathbb{Q}(\zeta)$ instead of using $\gamma' = 5$ as in the case of the Golden algebra we can use its prime factor $\gamma = 2+i$.

Proposition 4.4.7. *The maximal orders of the cyclic division algebra*

$$\mathscr{A}_3 = (\mathbb{Q}(\zeta)/\mathbb{Q}(i), \sigma, 2+i)$$

of Example 4.3.5 achieve the bound of Theorem 4.4.2.

Proof. [15, Proposition 7.3] □

Remark 4.4.8. By Corollary 4.3.2, we see that the fundamental parallelotope of the maximal order in Proposition 4.4.7 has measure 10. Thus this code has 2.5 times the density of the Golden code.

Remark 4.4.9. The algebra $\mathscr{A}_3$ has the drawback that the parameter γ is quite large. This leads to an antenna power imbalance in both space and time domains. To some extent these problems can be alleviated by conjugating the matrix lattice by a suitable diagonal matrix (a trick used in [56] and elsewhere). One of the motifs underlying the Perfect codes [43] is the requirement that the variable γ should have a unit modulus. To meet this requirement we proceed to give a different construction for this algebra. In [15, 32] it was shown that the *Golden+ code* based on a maximal order of the algebra $\mathscr{GA}+$ below outperforms the Golden code. Prior to our result, this was not thought to be possible [42].

Theorem 4.4.10. *Let λ be the square root of the complex number $2+i$ belonging to the first quadrant of the complex plane. The cyclic algebra*

$$\mathscr{GA}+ = (\mathbb{Q}(\lambda)/\mathbb{Q}(i), \sigma, i),$$

where the automorphism σ is determined by $\sigma(\lambda) = -\lambda$, is a division algebra. The maximal orders of $\mathscr{GA}+$ achieve the bound of Theorem 4.4.2. Furthermore, the algebras $\mathscr{GA}+$ and $\mathscr{A}_3$ of Theorem 4.4.7 are isomorphic.

Proof. [15, Theorem 7.4] □

We refer to the algebra $\mathscr{GA}+$ as the *Golden+ algebra*. This is partly motivated by the higher density and partly by the close relationship between the algebra $\mathscr{A}_3$ and the Golden algebra. After all, the algebra $\mathscr{A}_3$ is obtained when in the alternative description of the Golden algebra (cf. Example 4.2.4) the variable $\gamma = 5$ is replaced with its prime factor $2+i$. In [15, Section IX-C] we have also provided an alternative proof for Theorem 4.4.10 by explicitly producing a maximal order within $\mathscr{GA}+$ and verifying that it has the prescribed discriminant. It is immediate from the discussion in the early parts of this section that in this case there is only one cyclic division algebra (up to isomorphism) with that discriminant.

It turns out that all algebras $\mathscr{A}_\ell$ in the Kiran & Rajan family of Example 4.3.5 have maximal orders achieving the discriminant bound. The following observation is the key to proving this.

Lemma 4.4.11. *Let F be either one of the fields $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$, and let P_1 and P_2 be the two smallest ideals of its ring of integers R. Let $\mathscr{D}$ be a central division algebra over F, and let Λ be any R-order in $\mathscr{D}$. If the discriminant $d(\Lambda/\mathscr{O}_F)$ is divisible by no prime other than P_1 and P_2, then any maximal order Γ of $\mathscr{D}$ achieves the discriminant bound of Theorem 4.4.2.*

Proof. [15, Lemma 7.5] □

Corollary 4.4.12. *Let $\ell > 2$ be an integer. The maximal orders of the cyclic division algebra $\mathscr{A}_\ell = (\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(i), \sigma, 2+i)$ from Example 4.3.5 achieve the discriminant bound.*

Proof. Proposition 2.5.8 and Lemma 2.5.10 indicate that the only prime factors of the discriminant of the natural order in $\mathscr{A}_\ell$ are $1+i$ and $2+i$. The claim then follows from Lemma 4.4.11. □

Example 4.4.13. Let $F = \mathbb{Q}(\sqrt{-3})$, so that $\mathscr{O}_F = \mathbb{Z}[\omega]$. In this case, the two smallest prime ideals are generated by 2 and $1-\omega$ and have norms 4 and 3 respectively. By Theorem 4.4.2 the minimal discriminant is $4(1-\omega)^2$ when $n = 2$. As the absolute value of $1-\omega$ is $\sqrt{3}$, an application of the formula in Corollary 4.3.4 shows that the lattice L of the code achieving this bound has $m(L) = 27/4$. In [16] we show that a maximal order of the cyclic algebra $(E/F, \sigma(i) = -i, \gamma = \sqrt{-3})$, where $E = \mathbb{Q}(i, \sqrt{-3})$, achieves this bound.

As noted in [15], maximal orders can provide significant density gains without compromising either the coding gain or the transmission power. We demonstrate this using the following example.

Example 4.4.14. Consider again the family of cyclic division algebras $\mathscr{A}_\ell$ of index $n = 2^{\ell-2}$ from Example 4.3.5. If Λ_ℓ is a maximal order of $\mathscr{A}_\ell$, then according to Corollary 4.4.12

$$d(\Lambda_\ell/\mathbb{Z}[i]) = (1+i)^{n(n-1)}(2+i)^{n(n-1)}.$$

On the other hand, by Example 4.3.5 we know that

$$d(\Lambda_{NAT,\ell}/\mathbb{Z}[i]) = (1+i)^{2n^2(\ell-2)}(2+i)^{n(n-1)}.$$

Hence, by Lemma 2.5.7 we may conclude that the natural order is of index

$$[\Lambda_\ell : \Lambda_{NAT,\ell}] = 2^{((2\ell-5)n+1)n/2}.$$

In the cases $\ell = 3,4,5$ this index thus equals 2^3, 2^{26} and 2^{164}, respectively.

Remark 4.4.15. It has now become evident that the natural orders of the algebras $\mathscr{A}_\ell$ of Example 4.3.5 are very far from being maximal. In other words, by using a maximal order as opposed to the natural order of $\mathscr{A}_\ell$, one can send 1.5, 6.5, or 20.5 more bits per channel use without compromising either the transmission power or the minimum determinant in the respective cases of 2, 4, and 8 antennas. Hence the problem of actually finding these maximal orders, rather than simply knowing that they exist, becomes relevant.

In Section IV of [15], we describe briefly how maximal orders can be constructed in general. A more detailed version of the algorithm can be found in [26].

In practice, however, it is less time consuming to compute the maximal orders with the aid of the MAGMA software [1] (see [24]). The implementation of the algorithm in the software package is due to Willem van de Graaf and makes use of an algorithm proposed in [26]. MAGMA is a commercial computer program, but has a free 20-second online calculator that is convenient enough for the smallest cases.

Next we give two explicit code constructions tying together the above concepts.

Example 4.4.16. The Golden division algebra [5] mentioned in Example 4.2.4 is the cyclic division algebra $\mathscr{GA} = (E/F, \sigma, \gamma)$, where $E = \mathbb{Q}(i, \sqrt{5})$, $F = \mathbb{Q}(i)$, $\gamma = i$, $n = 2$, and $\sigma(\sqrt{5}) = -\sqrt{5}$. The natural order Λ of $\mathscr{GA}$ is already maximal [13]. The ring of algebraic integers is $\mathscr{O}_E = \mathbb{Z}[i][\theta]$, when we denote the golden ratio by $\theta = \frac{1+\sqrt{5}}{2}$. The authors of [5] further optimize the code by using an ideal $(\alpha) = (1+i-i\theta)$, and the Golden code is then explicitly defined as

$$GC = \left\{ \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha x_0 & i\sigma(\alpha)\sigma(x_1) \\ \alpha x_1 & \sigma(\alpha)\sigma(x_0) \end{pmatrix} \;\middle|\; x_0, x_1 \in \mathscr{O}_E \right\}.$$

The factor $1/5$ is added to get $\rho(GC) = 1$. Without this factor, we have $\det_{min}(GC) = 1$, and therefore $\delta(GC) = 1/\sqrt{5}$ (cf. Definition 4.1.1). Notice that the ideal α does not have an impact on the normalized measures (cf. Lemma 4.3.6).

The Golden plus division algebra [15], for its part, is the cyclic division algebra $\mathcal{GA}+ = (\mathbb{Q}(\lambda)/\mathbb{Q}(i), \sigma, i)$ (cf. Theorem 4.4.10), where λ is the square root of the complex number $2+i$ belonging to the first quadrant of the complex plane. The automorphism σ is determined by $\sigma(\lambda) = -\lambda$.

In order to give a concrete description of the maximal order used for the Golden+ code (GC+), we describe it in terms of its $\mathbb{Z}[i]$-basis. The maximal order Λ consists of the matrices $aM_1 + bM_2 + cM_3 + dM_4$, where a, b, c, d are arbitrary Gaussian integers and $M_i, i = 1, 2, 3, 4$, are the following matrices.

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix},$$

$$M_3 = \frac{1}{2}\begin{pmatrix} i+i\lambda & i-\lambda \\ -1+i\lambda & i-i\lambda \end{pmatrix}, \qquad M_4 = \frac{1}{2}\begin{pmatrix} -1-i\lambda & i+i\lambda \\ -1+\lambda & -1+i\lambda \end{pmatrix}.$$

One of the ingredients in the construction of the Perfect codes was the use of ideals in improving the shape of the code lattices. A way of doing that is to choose an element x of the maximal order in such way that the left (or right) ideal $x\Lambda$ is contained in the natural order. By moving the code inside the natural order we then, to some extent, recover the layered structure of the natural order. Hence, we also recover some of the advantages of the inherent orthogonality between layers.

In the case of the Golden+ algebra we can use the element $(1-\lambda)^3$ from the ring of integers $\mathcal{O}_E$ of the larger field $E = \mathbb{Q}(\sqrt{2+i})$ as a multiplier. Thus, by denoting

$$M = \begin{pmatrix} (1-\lambda)^3 & 0 \\ 0 & (1+\lambda)^3 \end{pmatrix},$$

we get the ideal $\mathcal{I}$ consisting of matrices of the form

$$aMM_1 + bMM_2 + cMM_3 + dMM_4, \tag{4.4}$$

where the coefficients a, b, c, d are Gaussian integers and the matrices $M_j, j = 1, 2, 3, 4$ are as above. This ideal is a subset of the natural order $\mathcal{O}_E \oplus u\mathcal{O}_E$.

For the Golden+ code consisting of codewords of the form (4.4), we have $\delta(GC+) = 1/\sqrt[4]{10}$ (see Definition 4.1.1). Once more, according to Lemma 4.3.6, the ideal does not change the normalized measures.

We conclude the treatment of symmetric codes by the following remark on Perfect codes and their performance as compared to the denser maximal order codes.

Remark 4.4.17. The Perfect codes are based on the natural orders (or their ideals to be more specific) of the corresponding algebras. For the two- and three-antenna codes, the natural order happens to be a maximal order as well. This is not the case with the four- and six-antenna codes, where the natural order is properly contained in a maximal one. Even in the two- and three-antenna cases, the maximal order in use does not achieve the discriminant bound, as already noted in Remark 4.4.6 for

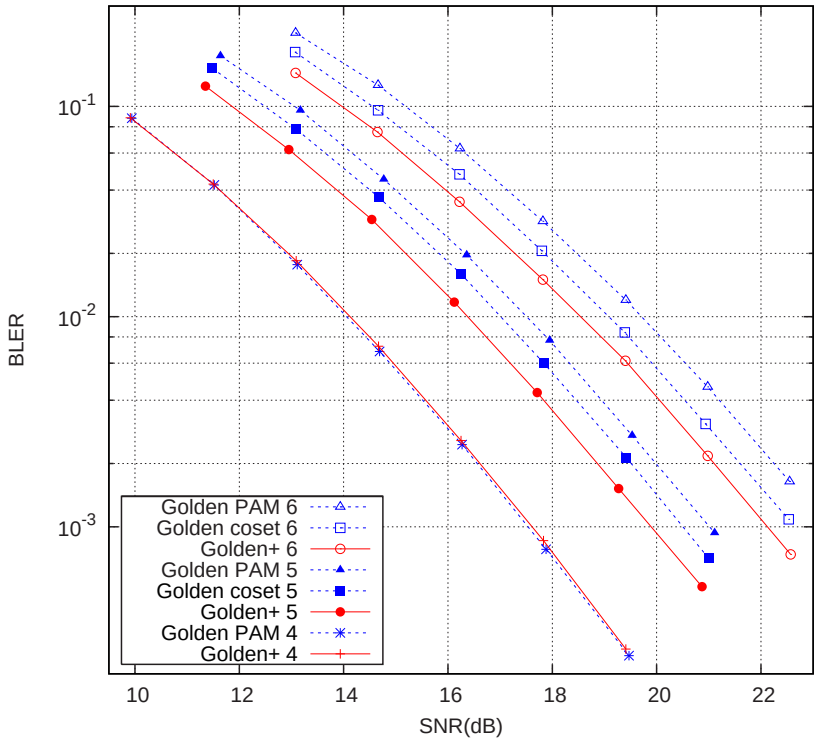


Figure 4.1: Block error rates of the Golden and Golden+ codes at 4, 5, and 6 bpcu.

the Golden code. The consequences of this fact are demonstrated in Figures 4.1 and 4.2.

In both figures, the *x*-axis describes the SNR, and the block error rate (i.e. the probability of decoder deciding in favor of a matrix $X' \neq X$, when X was transmitted) is depicted on the *y*-axis. Thus, with a fixed data rate, the lower the position of the curve in the picture, the better the performance of the corresponding code.

The Golden+ code constructions (cf. Theorem 4.4.10) in Figure 4.1 are based on spherical shaping. In other words, on selecting the prescribed number of lowest energy matrices, i.e. shortest codewords, from a chosen additive coset of a certain ideal of the Golden+ algebra (see [15] for details). In order to reach a target bandwidth utilization of 4, 5 or 6 bpcu we thus selected 256, 1024 or 4096 matrices. In this sense, we have done some coset optimization for the Golden+ codes, but make no claims as to having found the best coset. For the rival Golden code from [43], the coset corresponding to assigning the value of $(1+i)/2$ to all Gaussian integers stands out. With this assignment, the code will consist of 256 matrices all having the minimal energy, thus the Golden code also naturally admits spherical shaping at 4 bpcu. Therefore, pulse amplitude modulation (PAM) can be used to good effect. We began by doing some simulations using a PAM-type rule for larger

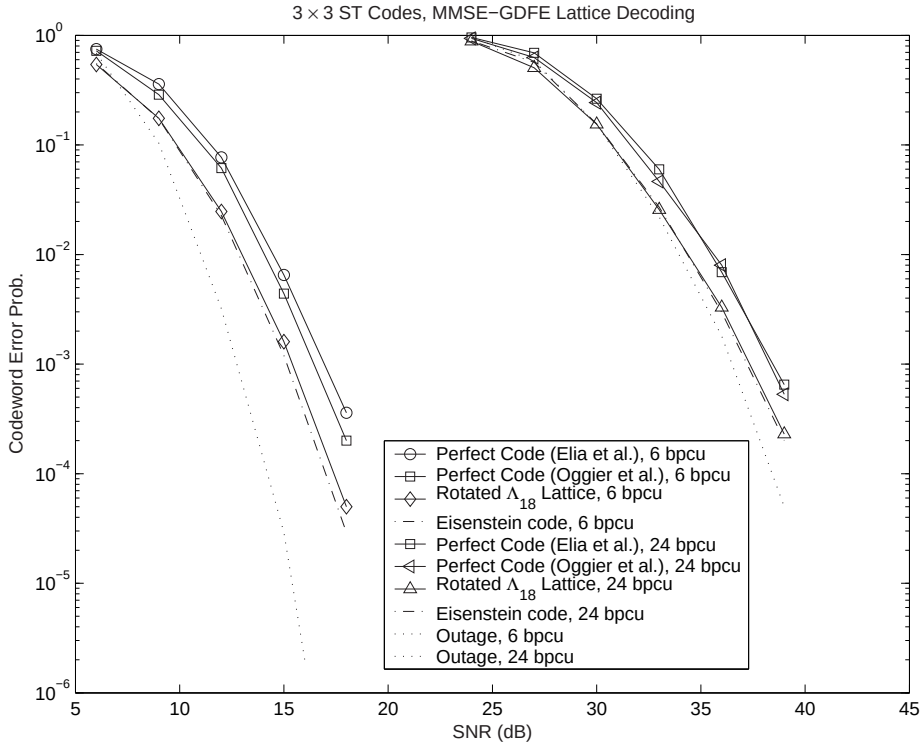


Figure 4.2: Block error rates of different 3×3 MIMO codes at 6 and 24 bpcu.

subsets of the Golden code. The desired bandwidth efficiency was achieved by arbitrarily selecting a suitable number of coefficients of the basis matrices from the set $\{-3/2, -1/2, 1/2, 3/2\}$. This is a natural choice, well suited for example to the sphere decoding algorithm. While we ended up having a tie in terms of the block error rate at 4.0 bpcu, the Golden code lost to the Golden+ code by about 0.9 dB at the rates 5 and 6 bpcu (see Figure 4.1). In the interest of a fair comparison, we then tried coset optimization for the Golden code as well. This narrowed down the gap to about 0.3 dB. However, the resulting subsets of the Golden code no longer had a structure that would be suited to PAM. In other words, both the rival codes must resort to the use of a codebook. Alternatively, sphere encoding could be used [32].

In Figure 4.2 we depict the performance of different 3×3 MIMO codes. Again, we see that the codes optimized in terms of density (named Eisenstein codes, see [15] for the algebra in use) win over the Perfect codes. The denser maximal order codes even slightly outperform or have tie with the structured lattice code based on the Leech lattice Λ_{18} [32].

4.4.2 Asymmetric codes

Let us now move on to the asymmetric situation. The discriminant bound in Theorem 4.4.2 can be applied directly in the asymmetric case, as it does not make any assumptions on the degree of the center. As opposed to the very simple density bounds obtained in Corollary 4.4.5 for the symmetric codes, deriving such explicit bounds becomes much more challenging in the asymmetric case. The reason for this is that, whereas the centers used for symmetric codes always have degree two, the centers in use for asymmetric codes will have degree at least four. Moreover taking into account the fact that there are typically only two centers, $\mathbb{Q}(i)$ and $\mathbb{Q}(\omega)$ (corresponding to the QAM or HEX signaling, respectively), used for symmetric codes, it can readily be seen that the set of possible centers has now stretched considerably. In the simple, and possibly also the most interesting, case of 4Tx and 2Rx antennas, the center has degree four over $\mathbb{Q}$. Now the requirement (again for signaling reasons) is that the algebra will contain $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$ as a subfield, hence allowing the center to be almost anything. Any field of the form $\mathbb{Q}(i,\alpha)$ with $\alpha \in \mathscr{A}$ of degree two over $\mathbb{Q}(i)$ meets this requirement, giving an indication of the variety of different possibilities. In what follows, we summarize the main results from [18].

The above symmetric $n \times n$ codes can also be used in the asymmetric scenario, as they are DMT optimal for any number of receivers $n_r \leq n$, but there is no simple decoding method when $n_r < n$; e.g. a sphere decoder cannot be used. Hence, one needs to think of other construction methods in order to also enable simple decoding. There are different construction methods that one can choose from. According to our experience and simulations, there is no universal method which one should always use, but the best method depends on the algebra and the SNR range. The different methods we have proposed in [18, 38] are

1) the trivial puncturing method (TPM),
2) the block diagonal method (BDM),
3) the subfield construction method (SCM),
4) the smart puncturing method (SPM), and
5) the transmit antenna selection method (TAS).

Method 1 was independently proposed in [25], and a structure similar to Method 2 was independently considered in [57] in the amplify-and-forward cooperative setting. The structure in Method 2 is very similar to that of a multi-block code [35, 36], and it did turn out that the density results obtained in [18] for Method 2 also hold for multi-block codes. Method 4 is a somewhat trivial generalization of Method 3, allowing the use of any number of receivers $n_r < n_t$, while Method 2 and 3 always require $n_t = kn_r$ for some integer k. None of the Methods 1-4 are known to yield DMT optimal codes, but it has been conjectured [34] that Method 2 would be DMT optimal in the special case of minimal delay, i.e. square matrices. The codes proposed in [38] are DMT optimal, but they have non-minimum delay. That

means that the lattices in use have quite a high dimension, hence complicating the decoding process. One ought to remember also that the DMT is an asymptotical measure, and hence when dealing with a low or moderate (finite) SNR, the performance order of different codes has to be confirmed by computer simulations. Of course the determinant criterion also has asymptotic nature. However, only few of the simulations we have carried out during the past few years have violated the order determined by the normalized minimum determinants. The normalized minimum determinant thus seems to give us a good way to compare different codes without simulations, even at low SNRs.

Let us next take a closer look to the block diagonal method. The proofs for the propositions and corollaries in this section can be found in [18]. Consider an extension tower $F \subseteq L \subseteq E$ with the degrees $[E:L] = n_r, [L:F] = m$ and with the Galois groups $\mathrm{Gal}(E/F) = \langle \tau \rangle$, $\mathrm{Gal}(E/L) = \langle \sigma = \tau^m \rangle$. Let

$$\mathscr{B} = (E/L, \sigma, \gamma) = E \oplus uE \oplus \cdots \oplus u^{n_r-1}E$$

be an index n_r division algebra, where the center L is fixed by $\sigma = \tau^m$. We denote by $\#\mathrm{Tx} = n_t = n_r m$.

If one has a symmetric, index $n_t = n_r m$ CDA-based STBC, the algebra $\mathscr{B}$ can be constructed by just picking a suitable intermediate field $L \subseteq E$ of the appropriate degree as the new center.

An element $b = x_0 + \cdots + u^{n_r-1}x_{n_r-1},\ x_i \in E,\ i = 0,...,n_r-1$ of the algebra $\mathscr{B}$ has the standard representation as an $n_r \times n_r$ matrix $B = (b_{ij})_{1 \le i,j \le n_r}$ as given in Sections 2.4 and 4.2.

However, we can 'afford' an $n_t \times n_t$ packing as we are using n_t transmit antennas. This can be achieved by using the isomorphism τ. Let us denote by $\tau^k(\mathscr{B}) = (E/L, \sigma, \tau^k(\gamma)),\ k = 0,...,m-1$ the m isomorphic copies of $\mathscr{B}$ and the respective matrix representations by

$$\tau^k(B) = (\tau^k(b_{ij}))_{1 \le i,j \le n_r},\ k = 0,...,m-1. \tag{4.5}$$

The next proposition shows that by using these copies as diagonal blocks we obtain an infinite lattice with non-vanishing determinant.

Proposition 4.4.18 (BDM). *Let $b \in \Lambda \subseteq \mathscr{B}$ and $F = \mathbb{Q}(d)$, where $d \in \{i, \omega\}$. Assume that $\gamma \in \mathscr{O}_L$. The block diagonal lattice*

$$\mathscr{C}(\Lambda) = \left\{ M = \begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & \tau(B) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \tau^{m-1}(B) \end{pmatrix} \right\}$$

built from (4.5) has a non-vanishing determinant $\det(M) = \prod_{i=0}^{m-1} \det(\tau^i(B)) \in \mathbb{Z}[d]$. *Thus, the minimum determinant is equal to one for all m. The code rate equals $n_r^2 m / n_r m = n_r$.*

Proof. See [18, Proposition 5.1]. □

Now the natural question is how should one choose a suitable division algebra. In [8] and [37] several systematic methods for constructing extensions E/L are provided. All of these methods make use of cyclotomic fields. Next we will show that, as in the symmetric case, maximizing the code density (i.e. minimizing the volume of the fundamental parallelotope, see [15]) with a given minimum determinant is equivalent to minimizing a certain discriminant. Later in this section we shall show that this also holds for the multi-block codes from [35].

As a generalization to Lemma 4.3.1, we give the following proposition.

Proposition 4.4.19. *Assume that F is an imaginary quadratic number field and that $\{1, v\}$ forms a $\mathbb{Z}$-basis of its ring of integers $\mathscr{O}_F$. Let $n_r = [E : L]$, $m = [L : F]$, $n_t = n_r m$, and $s = |\Im v|^{mn_r^2}$. If the order $\mathscr{C}(\Lambda)$ defined as in Proposition 4.4.18 is a free $\mathscr{O}_F$-module (which is always the case if $\mathscr{O}_F$ is a PID), then the measure of the fundamental parallelotope equals*

$$\begin{aligned} m(\mathscr{C}(\Lambda)) &= s|d(\Lambda/\mathscr{O}_F)| && (4.6)\\ &= s|d(\mathscr{O}_L/\mathscr{O}_F)^{n_r^2} N_{L/F} d(\Lambda/\mathscr{O}_L)| && (4.7)\\ &= s|d(\mathscr{O}_L/\mathscr{O}_F)^{n_r^2} \prod_{i=0}^{m-1} \tau^i(d(\Lambda/\mathscr{O}_L))|. && (4.8) \end{aligned}$$

Proof. See [18, Proposition 5.3]. □

Corollary 4.4.20. *In the case $F = \mathbb{Q}(i)$ the volume equals*

$$m(\mathscr{C}(\Lambda)) = |d(\Lambda/\mathbb{Z}[i])|.$$

Corollary 4.4.21. *In the case $F = \mathbb{Q}(\omega)$ we get*

$$m(\mathscr{C}(\Lambda)) = (\frac{\sqrt{3}}{2})^{mn_r^2} |d(\Lambda/\mathbb{Z}[\omega])|.$$

Now we can conclude (cf. (4.7)) that the extensions $E/L, L/F$ and the order $\Lambda \subseteq \mathscr{B}$ should be chosen in such a way that the discriminants $d(\mathscr{O}_L/\mathscr{O}_F)$ and $d(\Lambda/\mathscr{O}_L)$ are as small as possible. By choosing a maximal order within a given division algebra we can minimize the norm of $d(\Lambda/\mathscr{O}_L)$ (cf. Remark 2.5.9). As, in practice, an imaginary quadratic number field F is contained in L, we know that L is totally complex. In that case the fact that

$$d(\Lambda/\mathscr{O}_L) \geq (P_1 P_2)^{n_r(n_r-1)}, \tag{4.9}$$

where P_1 and P_2 are prime ideals $\in \mathscr{O}_L$ with the smallest norms (to $\mathbb{Q}$) helps us in picking a good algebra (for the proof, see [15, Theorem 3.2]). However, one must realize that optimization with respect to $d(\mathscr{O}_L/\mathscr{O}_F)$ may result in a loss in $d(\Lambda/\mathscr{O}_L)$ and vice versa.

Keeping the above notation, we have now arrived at the following theorem.

Theorem 4.4.22 (Density bound for lattices from the BDM). *For the density of the lattice $\mathscr{C}(\Lambda), \Lambda \subseteq \mathscr{A}$ it holds that*

$$\rho(\mathscr{C}(\Lambda)) = \frac{1}{m(\mathscr{C}(\Lambda))} \leq s^{-1} |d(\mathscr{O}_L/\mathscr{O}_F)|^{-n_r^2} |N_{L/F}(P_1P_2)|^{n_r(1-n_r)}. \tag{4.10}$$

Proof. See [18, Theorem 5.6]. □

Remark 4.4.23. We emphasize that, as opposed to Corollaries 4.4.3 and 4.4.4 (cf. [15]), here we do not automatically achieve nice, explicit lower bounds for $m(\mathscr{C}(\Lambda))$. This is a consequence of the fact that the center L can now be any field containing $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$, and thus determining the smallest ideals P_1 and P_2 or even the minimal $d(\mathscr{O}_L/\mathscr{O}_F)$ is not at all straightforward. An exact lower bound is hard to derive in the general case as the calculation of minimal number field discriminants is known to be a tricky problem. The reader may ponder over the fact that tables for minimal discriminants do exist in literature (though only for certain degrees, see e.g. [6]) so why not use them. We want to emphasize that these tables cannot be adapted here, as the fields in question do not necessarily contain the desired subfield $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$. Also it may be the case that P_1 and P_2 actually take smaller values in a field that is not included in the table. However, in the smallest (and perhaps the most practical) case of 4Tx+2Rx antennas, we are able to give an explicit and even achievable upper bound for the density. We believe that the best one can do in the other cases is to take advantage of the known bounds of a more general nature, such as Odlyzko's bound [41]. We could also continue calculations by hand in order to get exact bounds, but whether this is worth the effort is questionable.

The n_tTx+n_rRx antenna AST code from Proposition 4.4.18 can be transformed into an n_rTx+n_rRx antenna multi-block code [35] by rearranging the blocks as shown below:

$$\begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & \tau(B) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \tau^{m-1}(B) \end{pmatrix} \leftrightarrow \begin{pmatrix} B & \cdots & \tau^{m-1}(B) \end{pmatrix}. \tag{4.11}$$

As the Gram matrices of an AST lattice and a multi-block ST lattice coincide, Lemma 4.4.19 also holds for multi-block ST codes with the same parameters. Let the notation be as above.

Proposition 4.4.24. *Let $b \in \Lambda \subseteq \mathscr{B}$ and $F = \mathbb{Q}(d)$, where $d \in \{i, \omega\}$. Assume that $\gamma \in \mathscr{O}_L$. As the lattice*

$$\mathscr{C}'(\Lambda) = \left\{ M = \left(B, \tau(B), \ldots, \tau^{m-1}(B) \right) \right\}$$

built from (4.5) satisfies the generalized non-vanishing determinant property (cf. [35],[29]), it is optimal with respect to the DMT for all numbers of fading blocks

m. Again, as in Proposition 4.4.18, $|\prod_{i=0}^{m-1}\det(\tau^i(B))| \geq 1$. *The code rate equals* $n_r^2 m/n_r m = n_r$.

Proof. For the proof, see [35]. □

Proposition 4.4.25. *The Gram determinants (cf.* (4.1)*) of the lattices* $\mathscr{C}(\Lambda)$ *and* $\mathscr{C}'(\Lambda)$ *coincide:*

$$\det G(\mathscr{C}(\Lambda)) = \det G(\mathscr{C}'(\Lambda)).$$

Proof. This is obvious. □

Corollary 4.4.26. *The lattices* $\mathscr{C}(\Lambda)$ *and* $\mathscr{C}'(\Lambda)$ *share the same density, i.e. Proposition 4.4.19 also holds for the multi-block scheme.*

Proposition 4.4.27 (Density Bound for $n_t = 4$**,** $F = \mathbb{Q}(i)$**).** *Let* $m = n_r = 2$*, i.e.* $n_t = 4$*. For the density of the lattice* $\mathscr{C}(\Lambda)$ *it holds that*

$$\rho(\mathscr{C}(\Lambda)) = 1/m(\mathscr{C}(\Lambda)) \leq \frac{1}{2^2 \cdot 3^6} \approx 0.00034. \tag{4.12}$$

Proof. See [18, Proposition 5.10]. □

The following example introduces an explicit code construction achieving the density bound. The density upper bound is achieved e.g. by the maximal order of the algebra $\mathscr{I}\mathscr{A}$, see the example and Table 4.1 below.

Example 4.4.28. We obtain a rate-2 AST code $\mathscr{I}\mathscr{A}_1$ by introducing the another algebra $\mathscr{I}\mathscr{A} = (E/L, \sigma = \tau^2, \gamma = \sqrt{-3})$, where $F = \mathbb{Q}(i)$, $L = \mathbb{Q}(i, \sqrt{3})$, $E = L(a = \sqrt{1+i})$, and $\tau : \sqrt{3} \mapsto -\sqrt{3}, \sqrt{1+i} \mapsto -\sqrt{1+i}$. If we order the $\mathbb{Z}$-basis of the natural order of $\mathscr{I}\mathscr{A}$ as

$$\{e_i\}_{1\leq i\leq 16} = \{1, u, i, \gamma, a, ui, u\gamma, ua, i\gamma, ia, a\gamma, ui\gamma, uia, ua\gamma, ia\gamma, uia\gamma\},$$

then (according to the MAGMA software [1]) the maximal order $\Lambda_{MAX} \subseteq \mathscr{I}\mathscr{A}$ has a $\mathbb{Z}$-basis

$$\Big\{\frac{1}{2}(e_1+e_2+e_3+e_6),\ \frac{1}{2}(e_2+e_6+e_9+e_{12}+e_{14}+e_{16}),$$

$$\frac{1}{2}(e_3+e_6+e_7+e_9+e_{14}+e_{15}),\ \frac{1}{2}(e_4+e_6+e_7+e_9+e_{12}\ ),$$

$$\frac{1}{2}(e_5+e_8+e_{10}+e_{13}),\ e_6,\ e_7,\ \frac{1}{2}(e_8+e_{13}+e_{15}+e_{16}),$$

$$e_9,\ \frac{1}{2}(e_{10}+e_{13}+e_{14}+e_{15}),\ \frac{1}{2}(e_{11}+e_{14}+e_{15}+e_{16}),$$

$$e_{12},\ e_{13},\ e_{14},\ e_{15},\ e_{16}\Big\}.$$

Now the codebook $\mathscr{C} \subseteq \Lambda_{MAX}$ (cf. Definition 2.3.3 and (2.5) for the matrix representation) of an arbitrary size can be produced as

$$\mathscr{C} \subseteq \{M \in \Lambda_{MAX} \mid ||M|| \leq P\},$$

where again $||\cdot||$ denotes the Frobenius norm, and P is some desired energy limit.

For the natural order of $\mathscr{IA}$, we have $\delta(\Lambda_{NAT}) = 2^{-5/2} \cdot 3^{-3/2} \approx 0.0340$. The maximal order of $\mathscr{IA}$ has $\delta(\Lambda_{MAX}) = \frac{1}{3\sqrt{2}\sqrt{3}} \approx 0.1361$ (cf. Definition 4.1.1).

For the explicit constructions of the other example algebras in Table 4.1, see [18].

Table 4.1: Normalized minimum determinant $\delta(\mathscr{C}(\Lambda))$ and normalized density $\rho(\mathscr{C}(\Lambda)) = 1/m(\mathscr{C}(\Lambda))$ of natural and maximal orders of different algebras.

	$\mathscr{QA}$	$\mathscr{CA}$	$\mathscr{IA}$	$\mathscr{PA}$
	Λ_{NAT}	Λ_{NAT}	Λ_{NAT}	Λ_{NAT}
δ	**0.0894**	0.0361	0.0340	0.0298
ρ	$5^{-6} =$ $6.4 \cdot 10^{-5}$	$2^{-16} \cdot 3^{-2} =$ $1.7 \cdot 10^{-6}$	$2^{-10} \cdot 3^{-6} =$ $1.4 \cdot 10^{-6}$	$3^{-4} \cdot 5^{-6} =$ $7.9 \cdot 10^{-7}$
	$\mathscr{IA}$	$\mathscr{CA}$	$\mathscr{QA}$	$\mathscr{PA}$
	Λ_{MAX}	Λ_{MAX}	Λ_{MAX}	Λ_{MAX}
δ	**0.1361**	0.1214	0.0894	0.0894
ρ	$2^{-2} \cdot 3^{-6} =$ $\mathbf{3.4 \cdot 10^{-4}}$	$2^{-9} \cdot 3^{-2} =$ $2.2 \cdot 10^{-4}$	$5^{-6} =$ $6.4 \cdot 10^{-5}$	$5^{-6} =$ $6.4 \cdot 10^{-5}$

We conclude the treatment of asymmetric codes by the following remark on the DMT-optimal TAS codes and simulation results. The asymmetric codes based on the algebras $\mathscr{IA}$ and $\mathscr{QA}$ clearly outperform the best previously known asymmetric codes. For a thorough description of our simulation results, see [18, Section VII].

Remark 4.4.29. The above asymmetric codes are not necessarily DMT optimal. We have derived lower bounds for their DMTs, but these do not coincide with the optimal DMT. Nevertheless, they are only lower bounds and the upper bounds are not known to us. We conjecture that they do not achieve the optimal DMT. On the other hand, we believe that the block diagonal method produces DMT optimal codes, if we require minimum delay. The TAS codes [38] based on transmit

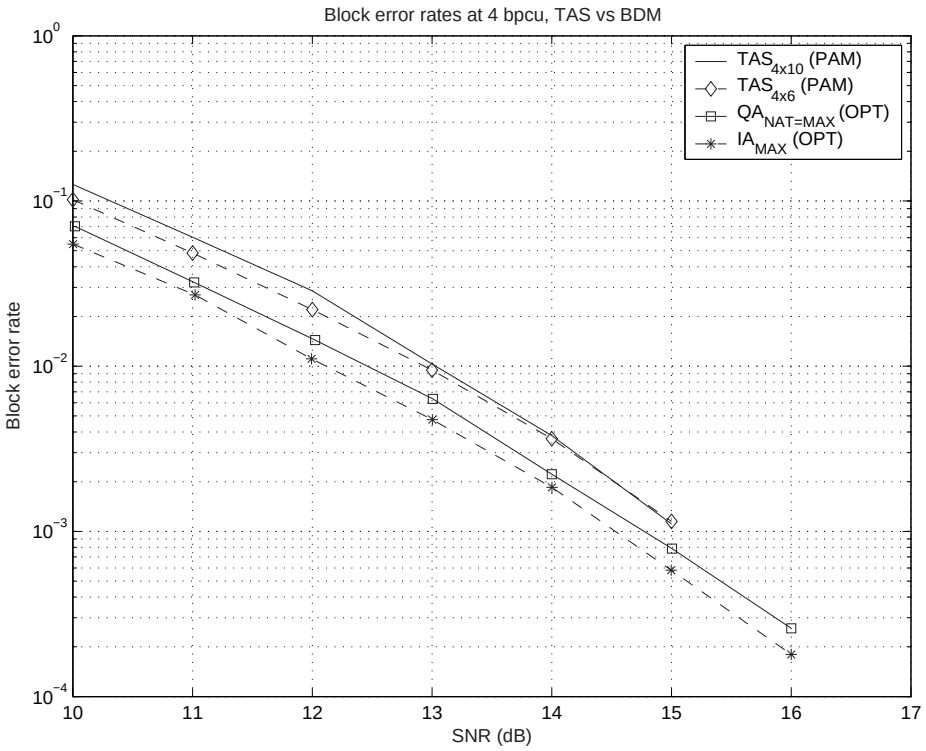


Figure 4.3: Block error rates at 4 bpcu of different BDM and TAS codes, when using a codebook for BDM and 2-PAM for TAS.

antenna selection are DMT-optimal. However, as Figures 4.3 and 4.4 show, quite large SNRs are required before the power of the DMT kicks in. At low or moderate SNRs, one is probably better off using some other construction method, such as the BDM.

Figure 4.3 shows that when we take advantage of the spherical shape of the maximal orders, they clearly outperform the TAS codes at low and moderate SNRs. For the TAS codes making a codebook is so complex due to the high dimension of the lattice, that we simply used the PAM signaling in both Figure 4.3 and 4.4. Figure 4.4 indicates that when we use the PAM signaling also for the maximal order codes, the gap between the TAS codes and $\mathcal{2A}$ becomes somewhat smaller. In particular, the algebra $\mathcal{IA}$ loses all of its benefits now, as it is highly non-orthogonal. The maximal order of the algebra $\mathcal{2A}$ happens to also be the natural order, so the loss is smaller and $\mathcal{2A}$ still wins over the TAS codes at SNRs up to 15.

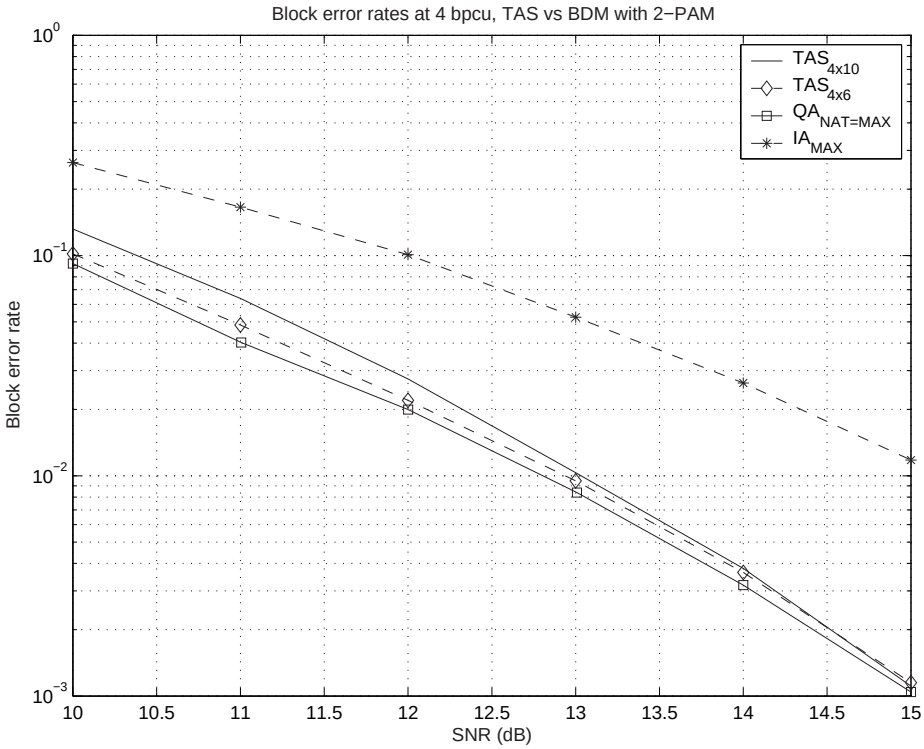


Figure 4.4: Block error rates at 4 bpcu of different BDM and TAS codes with 2-PAM.

Chapter 5

Conclusions and future prospects

In this thesis, we have presented various methods for constructing space-time block codes from division algebras and their orders. The key contribution, as compared to the rest of the work in the field, was the introduction of maximal orders of cyclic division algebras in the context of ST coding. Both symmetric and asymmetric scenarios were considered, and explicit, DMT optimal constructions with a non-vanishing determinant were provided.

As a main design criterion, we adopted the maximization of the coding gain. In other words, our aim was to produce code lattices that are as dense as possible, hence maximizing the normalized (non-vanishing) minimum determinant. Computer simulations were used to demonstrate the robustness of the proposed methods. The simulations further indicated that, for practical numbers of antennas and SNRs, the best of the newly proposed codes outperform all previously known codes in terms of block error performance. We confess that the optimization to encode may also be a drawback in scenarios where rate adaptation is needed.

Taking also into consideration the work in Vehkalahti's dissertation [55], we would like to encourage the ST audience to further exploit maximal orders and the notion of density. Natural orders are already widely used — even when they are not orthogonal. While orthogonality can be a very good reason for using a natural order, in the skewed case there is no point in using a natural order instead of a maximal one.

We have started to extend our theory to multi-user settings as well, see [39] for the promising preliminary results. In the future, it would be interesting to know whether, in general, denser lattices can be produced by means other than maximal orders. It would be also worth a try to implement the algorithm for constructing maximal orders more efficiently, taking use of the module bases rather than the $\mathbb{Z}$-bases as in the MAGMA software.

One may have noticed that in the asymmetric case, density analysis was provided only for the lattices constructed using the block-diagonal method. We aim to consider the other methods in the immediate future. We anticipate that for the

subfield construction method this should be fairly easy, whereas for the smart puncturing method giving a universal density analysis probably turns out to be impossible. The TAS codes were designed with the DMT optimality in mind, so giving a density analysis for them makes little sense.

List of abbreviations

(A)ST = (asymmetric) space time
(A)STBC = (asymmetric) space time block code
BDM = block diagonal method
BLER = block error rate
bpcu = bits per channel use
CDA = cyclic division algebra
DMT = diversity-multiplexing gain tradeoff
HEX = hexagonal constellations
i.i.d. = independent, identically distributed
MIMO = multiple-input multiple-output
MISO = multiple-input single-output
MU-MIMO = multi-user MIMO
NVD = non-vanishing determinant
PAM = pulse amplitude modulation
PAPR = peak-to-average power ratio
PEP = pairwise error probability
PID = principal ideal domain
QAM = quadrature amplitude modulation
SCM = subfield construction method
SNR = signal to noise ratio
SPM = smart puncturing method
TAS = transmit antenna selection
TPM = trivial puncturing method

Bibliography

[1] MAGMA Computational Algebra System, University of Sydney, Sydney, Australia, *http://magma.maths.usyd.edu.au/magma/htmlhelp/text835.htm#8121*.

[2] ALAMOUTI, S. M. A simple transmitter diversity scheme for wireless communications. *IEEE J. Select. Areas Commun.* (Oct. 1998), 1451–1458.

[3] ALBERT, A. A. *Structure of Algebras*. American Mathematical Society, New York, 1939.

[4] BELFIORE, J.-C., AND REKAYA, G. Quaternionic lattices for space-time coding. In *Proc. IEEE Information Theory Workshop* (Paris, 31 March - 4 April 2003).

[5] BELFIORE, J.-C., REKAYA, G., AND E.VITERBO. The Golden code: A 2×2 full-rate space-time code with non-vanishing determinants. In *Proc. 2004 IEEE Int. Symp. Inform. Theory* (Chicago, IL, June 27-July 2 2004), p. 308.

[6] COHEN, H., Y DIAZ, F. D., AND OLIVIER, M. A table of totally complex number fields of small discriminants. *Algorithmic number theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., 1423, Springer, Berlin.* (1998), 381–391.

[7] EL GAMAL, H., CAIRE, G., AND DAMEN, M. Lattice coding and decoding achieve the optimal diversity-multilpexing tradeoff of MIMO channels. *IEEE Trans. Inf. Theory 50*, 6 (Jun. 2004), 968–985.

[8] ELIA, P., KUMAR, K. R., PAWAR, S. A., KUMAR, P. V., AND LU, H.-F. Explicit construction of space-time block codes achieving the diversity-multiplexing gain tradeoff. *IEEE Trans. Inf. Theory 52*, 9 (Sep. 2006), 3869–3884.

[9] ELIA, P., SETHURAMAN, B. A., AND KUMAR, P. V. Perfect space-time codes for any number of antennas. *IEEE Trans. Inf. Theory 53*, 11 (2007), 3853–3868.

[10] GUEY, J.-C., FITZ, M. P., BELL, M. R., AND KUO, W.-Y. Signal design for transmitter diversity wireless communication systems over rayleigh fading channels. In *Proc. IEEE VTC'96* (1996), pp. 136–140.

[11] HILTUNEN, J., HOLLANTI, C., AND LAHTONEN, J. Four antenna space-time lattice constellations from division algebras. In *Proc. 2004 IEEE Int. Symp. Inform. Theory* (Chicago, IL, June 27-July 2 2004).

[12] HILTUNEN, J., HOLLANTI, C., AND LAHTONEN, J. Dense full-diversity matrix lattices for four antenna MISO channel. In *Proc. 2005 IEEE Int. Symp. Inform. Theory* (Adelaide, Australia, Sep. 4-9 2005), pp. 1290–1294.

[13] HOLLANTI, C., AND LAHTONEN, J. A new tool: Constructing STBCs from maximal orders in central simple algebras. In *Proc. 2006 IEEE Inform. Theory Workshop* (Punta del Este, Uruguay, Mar. 13-17 2006).

[14] HOLLANTI, C., LAHTONEN, J., AND LU, H.-F. Maximal orders in the design of dense space-time lattice codes. *IEEE Trans. Inf. Theory 54*, 10 (2008), 4493–4510.

[15] HOLLANTI, C., LAHTONEN, J., RANTO, K., AND VEHKALAHTI, R. On the densest MIMO lattices from cyclic division algebras. *IEEE Trans. on Inform. Theory* (in press), 2008. *http://arxiv.org/abs/cs.IT/0703052.*

[16] HOLLANTI, C., LAHTONEN, J., RANTO, K., AND VEHKALAHTI, R. Optimal matrix lattices for MIMO codes from division algebras. In *Proc. 2006 IEEE Int. Symp. Inform. Theory* (Seattle, WA, Jul. 2006), pp. 783 – 787.

[17] HOLLANTI, C., LAHTONEN, J., RANTO, K., VEHKALAHTI, R., AND VITERBO, E. On the algebraic structure of the Silver code: A 2x2 Perfect space-time code with non-vanishing determinant. In *Proc. 2008 IEEE Inf. Theory Workshop* (Porto, Portugal, May 2008), pp. 91–94.

[18] HOLLANTI, C., AND LU, H.-F. Construction methods for asymmetric and multi-block space-time codes. *IEEE Trans. Inf. Theory*. In press, 2008.

[19] HOLLANTI, C., AND LU, H.-F. Normalized minimum determinant calculation for multi-block and asymmetric space-time codes. In *Proc. Applied Algebra, Algebraic Algorithms and Error Correcting Codes (AAECC-17)* (Bangalore, India, 2007), pp. 227 – 236.

[20] HOLLANTI, C., AND LU, H.-F. Constructing asymmetric space-time codes with the smart puncturing method. In *Proc. 2008 IEEE Int. Symp. Inform. Theory* (Toronto, ON, Jul. 2008). Full version submitted to *IEEE Trans. Inf. Theory, Jun. 2008*.

[21] HOLLANTI, C., AND LU, H.-F. On the construction of DMT-optimal AST codes with transmit antenna selection. In *Proc. 2008 IEEE Int. Symp. Inform. Theory* (Toronto, ON, Jul. 2008). Full version submitted to *IEEE Trans. Inf. Theory, Apr. 2008*.

[22] HOLLANTI, C., AND RANTO, K. Asymmetric space-time block codes for MIMO systems. In *Proc. 2007 IEEE Inform. Theory Workshop* (Solstrand, Norway, Jul. 2007), pp. 101–105.

[23] HOLLANTI, C., AND RANTO, K. On MIDO space-time block codes. In *Proc. 2007 IEEE Int. Symp. Inform. Theory* (Nice, France, Jun. 2007).

[24] HOLLANTI, C., AND RANTO, K. Maximal orders in space-time coding: Construction and decoding. In *Proc. 2008 Int. Symp. Inf. Theory and its Appl.* (New Zealand, Dec. 2008), pp. 1459–1463.

[25] HOTTINEN, A., HONG, Y., VITERBO, E., MEHLFÜHRER, C., AND MECKLENBRÄUKER, C. F. A comparison of high rate algebraic and non-orthogonal stbcs. In *Proc. 2007 ITG/IEEE Workshop on Smart Antennas WSA* (Vienna, Austria, Feb. 2007).

[26] IVANYOS, G., AND RÓNYAI, L. On the complexity of finding maximal orders in semisimple algebras over Q. *Computational Complexity 3* (1993), 245–261.

[27] JACOBSON, N. *Basic Algebra II*. W. H. Freeman and Company, San Francisco, 1980.

[28] JAFARKHANI, H. *Space-Time Coding: Theory and Practice*. Cambridge University Press, Cambridge, 2005.

[29] KIRAN, T., AND RAJAN, B. S. STBC-schemes with non-vanishing determinant for certain number of transmit antennas. *IEEE Trans. Inf. Theory 51*, 8 (Aug. 2005), 2984–2992.

[30] KOCH, H. *Algebraic Number Theory*. Springer, Berlin, 1997.

[31] KOCH, H. *Number Theory, Algebraic Numbers and Functions*. American Mathematical Society, New York, 2000.

[32] KUMAR, K. R., AND CAIRE, G. Space-time codes from structured lattices. *IEEE Trans. Inf. Theory* (in press), 2008. *http://arxiv.org/abs/0804.1811*.

[33] LIU, J., AND CALDERBANK, A. R. The Icosian code and the E_8 lattice: A new 4×4 space-time code with nonvanishing determinant. In *Proc. 2006 IEEE Int. Symp. Inform. Theory* (Seattle, WA, Jul. 2006), pp. 1006–1010.

[34] LU, H.-F. Personal communication.

[35] LU, H.-F. Explicit constructions of multi-block space-time codes that achieve the diversity-multiplexing tradeoff. In *Proc. 2006 IEEE Int. Symp. Inform. Theory* (Seattle, WA, Jul. 2006), pp. 1149–1153.

[36] LU, H.-F. Explicit constructions of multi-block space-time codes that achieve the diversity-multiplexing tradeoff. *IEEE Trans. Inf. Theory 54*, 8 (2008), 3790–3796.

[37] LU, H.-F., ELIA, P., KUMAR, K. R., PAWAR, S. A., AND KUMAR, P. V. Space-time codes meeting the diversity-multiplexing gain tradeoff with low signalling complexity. In *the 39th Annual CISS 2005 Conference on Information Sciences and* (2005).

[38] LU, H.-F., AND HOLLANTI, C. Optimal diversity multiplexing tradeoff and code constructions of constrained asymmetric MIMO systems. *IEEE Trans. on Inform. Theory*, submitted, May 2008.

[39] LU, H.-F., VEHKALAHTI, R., HOLLANTI, C., LAHTONEN, J., HONG, Y., AND VITERBO, E. New space-time code construcions for two-user multiple access channels. Submitted to *IEEE J. on Special Topics in Signal Processing: Managing Complexity in Multi-user MIMO Systems*, Sep. 2008.

[40] MILNE, J. S. Class field theory. Lecture notes for a course given at the University of Michigan, Ann Arbor, *http://www.jmilne.org/math/coursenotes/*.

[41] ODLYZKO, A. M. Lower bounds for discriminants of number fields II. *Tohoku Math. J.*, 29 (1977), 209–216.

[42] OGGIER, F. On the optimality of the Golden code. *Information Theory Workshop, 2006. ITW '06 Chengdu. IEEE* (Oct. 2006), 468–472.

[43] OGGIER, F., REKAYA, G., BELFIORE, J.-C., AND VITERBO, E. Perfect space-time block codes. *IEEE Trans. Inf. Theory 52*, 9 (Sept. 2006), 3885–3902.

[44] OGGIER, F. E., BELFIORE, J.-C., AND VITERBO, E. Cyclic division algebras: A tool for space-time coding. *Foundations and Trends in Communications and Information Theory 4*, 1 (2007), 1–95.

[45] REINER, I. *Maximal Orders*. Academic Press, New York, 1975.

[46] RIBENBOIM, P. *Classical Theory of Algebraic Numbers*. Springer, New York, 2001.

[47] RÓNYAI, L. Algorithmic properties of maximal orders in simple algebras over Q. *Computational Complexity 2* (1992), 225–243.

[48] SETHURAMAN, B. A., RAJAN, B. S., AND SHASHIDHAR, V. Full-diversity, high-rate space-time block codes from division algebras. *IEEE Trans. Inf. Theory 49*, 10 (Oct. 2003), 2596– 2616.

[49] SHASHIDHAR, V., RAJAN, B. S., AND SETHURAMAN, B. A. Information-lossless STBCs from crossed-product algebras. *IEEE Trans. Inf. Theory 52* (2006), 3913–3935.

[50] STEWART, I., AND TALL, D. *Algebraic number theory*. Chapman and Hall, London, 1979.

[51] TAROKH, V., SESHADRI, N., AND CALDERBANK, A. R. Space-time codes for high data rate wireless communication: Performance criterion and code construction. *IEEE Trans. Inf. Theory 44* (Mar. 1998), 744–765.

[52] TAVILDAR, S., AND VISWANATH, P. Approximately universal codes over slow fading channels. *IEEE Trans. Inf. Theory 52*, 7 (Jul. 2006), 3233– 3258.

[53] TELATAR, E. Capacity of multi-antenna Gaussian channels. *Europ. Trans. Telecomm. 10*, 6 (Nov.-Dec. 1999), 585–595.

[54] TSE, D., AND VISWANATH, P. *Fundamentals of Wireless Communications*. Cambridge University Press, Cambridge, 2005.

[55] VEHKALAHTI, R. *Class Field Theoretic Methods in the Design of Lattice Signal Constellations*. PhD thesis, 2008. *TUCS Dissertations Series*, no. 100, *https://oa.doria.fi/handle/10024/36604*.

[56] WANG, G., AND XIA, X.-G. On optimal multi-layer cyclotomic space-time code designs. *IEEE Trans. Inf. Theory 51*, 3 (Mar. 2005), 1102–1135.

[57] YANG, S., AND BELFIORE, J.-C. Optimal space-time codes for the MIMO amplify-and-forward cooperative channel. *IEEE Trans. Inf. Theory 53*, 2 (Feb. 2007), 647–663.

[58] ZHENG, L., AND TSE, D. Diversity and multiplexing: A fundamental trade-off in multiple antenna channels. *IEEE Trans. Inf. Theory 49*, 5 (May 2003), 1073–1096.

Part II

Original Publications

Publication I

Hollanti, C., Lahtonen, J., and Lu, H.-F. (2008). Maximal orders in the design of dense space-time lattice codes. *IEEE Transactions on Information Theory*, **54**(10), pp. 4493–4510.

Maximal Orders in the Design of Dense Space-Time Lattice Codes

Camilla Hollanti, Jyrki Lahtonen, *Member IEEE*, and Hsiao-feng (Francis) Lu

***Abstract*— We construct explicit rate-one, full-diversity, geometrically dense matrix lattices with large, non-vanishing determinants (NVD) for four transmit antenna multiple-input single-output (MISO) space-time (ST) applications. The constructions are based on the theory of rings of algebraic integers and related subrings of the Hamiltonian quaternions and can be extended to a larger number of Tx antennas. The usage of ideals guarantees a non-vanishing determinant larger than one and an easy way to present the exact proofs for the minimum determinants. The idea of finding denser sublattices within a given division algebra is then generalized to a multiple-input multiple-output (MIMO) case with an arbitrary number of Tx antennas by using the theory of cyclic division algebras (CDA) and maximal orders. It is also shown that the explicit constructions in this paper all have a simple decoding method based on sphere decoding. Related to the decoding complexity, the notion of sensitivity is introduced, and experimental evidence indicating a connection between sensitivity, decoding complexity and performance is provided. Simulations in a quasi-static Rayleigh fading channel show that our dense quaternionic constructions outperform both the earlier rectangular lattices and the rotated ABBA lattice as well as the DAST lattice. We also show that our quaternionic lattice is better than the DAST lattice in terms of the diversity-multiplexing gain tradeoff.**

***Index Terms*— Cyclic division algebras, dense lattices, maximal orders, multiple-input multiple-output (MIMO) channels, multiple-input single-output (MISO) channels, number fields, quaternions, space-time block codes (STBCs), sphere decoding.**

I. Introduction and background

Multiple-antenna wireless communication promises very high data rates, in particular when we have perfect channel state information (CSI) available at the receiver. In [1] the design criteria for such systems were developed and further on the evolution of ST codes took two directions: trellis codes and block codes. Our work concentrates on the latter branch.

The very first ST block code for two transmit antennas was the *Alamouti code* [2] representing multiplication in the ring of quaternions. As the quaternions form a division algebra, such matrices must be invertible, i.e. the resulting STBC meets the rank criterion. Matrix representations of other division algebras have been proposed as STBCs at least in [3]-[15], and (though without explicitly saying so) [16]. The most recent work [6]-[16] has concentrated on adding multiplexing gain, i.e. multiple input-multiple output (MIMO) applications, and/or combining it with a good minimum determinant. In this work, we do not specifically seek any multiplexing gains, but want to improve upon e.g. the diagonal algebraic space time (DAST) lattices introduced in [5] by using non-commutative division algebras. Other efforts to improve the DAST lattices and ideas alike can be found in [17]-[19].

The main contributions of this work are:

- We give energy efficient MISO lattice codes with simple decoding that win over e.g. the rotated ABBA [20] and the DAST lattice codes in terms of the block error rate (BLER) performance.
- It is shown that by using a non-rectangular lattice one can gain major energy savings without significant increasement in decoding complexity. The usage of ideals moreover guarantees a non-vanishing determinant > 1 and an easy way to present the exact proofs for the minimum determinants.
- In addition to the explicit MISO constructions, we present a general method for finding dense sublattices within a given CDA in a MIMO setting. This is tempting as it has been shown in [15] that CDA-based square ST codes with NVD achieve the diversity-multiplexing gain tradeoff (DMT) introduced in [21]. When a CDA is chosen the next step is to choose a corresponding lattice or, what amounts to the same thing, choose an order within the algebra. Most authors, among which e.g. [11], [15], and [16], have gone with the so-called natural order (see Section III-B, Example 3.2). In a CDA based construction, the density of a sublattice is lumped together with the concept of maximality of an order. The idea is that one can, on some occasions, use several cosets of the natural order without sacrificing anything in terms of the minimum determinant. So the study of maximal orders is easily motivated by an analogy from the theory of error correcting codes: why one would use a particular code of a given minimum distance and length, if a larger code with the same parameters is available.
- Furthermore, related to the decoding complexity, the notion of sensitivity is introduced for the first time, and evidence of its practical appearance is provided. Also the DMT behavior of our codes will be given.

At first, we are interested in the coherent MISO case with perfect CSI available at the receiver. The received signal $\mathbf{y} \in \mathbb{C}^n$ has the form

$$\mathbf{y} = \mathbf{h}X + \mathbf{n},$$

where $X \in \mathbb{C}^{m\times n}$ is the transmitted codeword drawn from a ST code $\mathcal{C}$, $\mathbf{h} \in \mathbb{C}^m$ is the Rayleigh fading channel response and the components of the noise vector $\mathbf{n} \in \mathbb{C}^n$ are i.i.d. complex Gaussian random variables.

A *lattice* is a discrete finitely generated free abelian subgroup of a real or complex finite dimensional vector space V, also called the ambient space. Thus, if L is a k-dimensional lattice, there exists a finite set of vectors $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k\} \subset V$ such that $\mathcal{B}$ is linearly independent over the integers and that

$$L = \{\sum_{i=1}^{k} z_i\mathbf{b}_i \mid z_i \in \mathbb{Z}, \mathbf{b_i} \in V \text{ for all } i = 1, 2, \ldots, k\}.$$

In the space-time setting a natural ambient space is the space $\mathbb{C}^{n\times n}$ of complex $n \times n$ matrices. When a code is a subset of a lattice L in this ambient space, the *rank criterion* [22] states that any non-zero matrix in L must be invertible. This follows from the fact that the difference of any two matrices from L is again in L.

The receiver and the decoder, however, (recall that we work in the MISO setting) observe vector lattices instead of matrix lattices. When the channel state is $\mathbf{h}$, the receiver expects to see the lattice $\mathbf{h}L$. If $\mathbf{h} \neq 0$ and L meets the rank criterion, then $\mathbf{h}L$ is, indeed, a free abelian group of the same rank as L. However, it is well possible that $\mathbf{h}L$ is not a lattice, as its generators may be linearly dependent over the reals — the lattice is said to *collapse*, whenever this happens.

From the pairwise error probability (PEP) point of view [22], the performance of a space-time code is dependent on two parameters: *diversity gain* and *coding gain*. Diversity gain is the minimum of the rank of the difference matrix $X - X'$ taken over all distinct code matrices $X, X' \in \mathcal{C}$, also called the *rank* of the code $\mathcal{C}$. When $\mathcal{C}$ is full-rank, the coding gain is proportional to the determinant of

C. Hollanti is with the Laboratory of Discrete Mathematics for Information Technology, Turku Centre for Computer Science, Joukahaisenkatu 3-5 B, FIN-20520 Turku, Finland.

C. Hollanti & J. Lahtonen are with the Department of Mathematics, FIN-20014 University of Turku, Finland. (e-mails: {cajoho, lahtonen}@utu.fi)

H.-f. Lu is with Department of Communications Engineering, National Chiao Tung University, Hsinchu 300, Taiwan. (e-mail: francislu@ieee.org)

the matrix $(X-X')(X-X')^H$, where X^H denotes the transpose conjugate of the matrix X. The minimum of this determinant taken over all distinct code matrices is called the *minimum determinant* of the code $\mathcal{C}$ and denoted by $\delta_{\mathcal{C}}$. If $\delta_{\mathcal{C}}$ is bounded away from zero even in the limit as SNR $\to \infty$, the ST code is said to have the *non-vanishing determinant* property [8]. As mentioned above, for non-zero square matrices being full-rank coincides with being invertible.

The *data rate* R in symbols per channel use is given by

$$R = \frac{1}{n}\log_{|S|}(|\mathcal{C}|),$$

where $|S|$ and $|\mathcal{C}|$ are the sizes of the symbol set and code respectively. This is not to be confused with the *rate of a code design* (shortly, *code rate*) defined as the ratio of the number of transmitted information symbols to the decoding delay (equivalently, block length) of these symbols at the receiver for any given number of transmit antennas using any complex signal constellations. If this ratio is equal to the delay, the code is said to have *full rate*.

The paper is organized as follows: basic definitions of algebraic number theory and explicit MISO lattice constructions are provided in Section II. As a (MIMO) generalization for the idea of finding denser lattices within a given division algebra, the theory of cyclic algebras and maximal orders is briefly introduced in Section III. In Section IV, we consider the decoding of the nested sequence of quaternionic lattices from Section II. A variety of results on decoding complexity is established in Section IV, where also the notion of sensitivity is taken into account. Simulation results are discussed in Section V along with energy considerations. Finally in Section VI, the DMT analysis of the proposed codes will be given.

This work has been partly published in a conference, see [3] and [4]. For more background we refer to [22]-[29].

II. Rings of algebraic numbers, quaternions and lattice constructions

We shall denote the sets of integers, rationals, reals, and complex numbers by $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ respectively.

Let us recall the set

$$\mathbb{H} = \{a_1 + a_2 i + a_3 j + a_4 k \mid a_t \in \mathbb{R}\ \forall t\},$$

where $i^2 = j^2 = k^2 = -1,\ ij = k$, as the ring of *Hamiltonian quaternions*. Note that $\mathbb{H} \simeq \mathbb{C} \oplus \mathbb{C}j$, when the imaginary unit is identified with i. A special interest lies on the subsets

$$\mathbb{H}_{\mathcal{L}} = \{a_1 + a_2 i + a_3 j + a_4 k \mid a_t \in \mathbb{Z}\ \forall t\} \subseteq \mathbb{H} \text{ and}$$

$$\mathbb{H}_{\mathcal{H}} = \{a_1\rho + a_2 i + a_3 j + a_4 k \mid a_t \in \mathbb{Z}\ \forall t,\ \rho = \frac{1}{2}(1+i+j+k)\} \subseteq \mathbb{H}$$

called the *Lipschitz'* and *Hurwitz' integral quaternions* respectively.

We shall use extension rings of the Gaussian integers

$$\mathcal{G} = \{a + bi \mid a, b \in \mathbb{Z}\}$$

inside a given division algebra. It would be easy to adapt the construction to use the slightly denser hexagonal ring of the Eisensteinian integers

$$\mathcal{E} = \{a + b\omega \mid a, b \in \mathbb{Z}\},$$

where $\omega^3 = 1$, as a basic alphabet. However, the Gaussian integers nicely fit with the popular 16-QAM and QPSK alphabets. Natural examples of such rings are the rings of algebraic integers inside an extension field of the quotient fields of $\mathcal{G}$, as well as their counterparts inside the quaternions. To that end we need division algebras $\mathcal{A}$ that are also 4-dimensional vectors spaces over the field $\mathbb{Q}(i)$.

A. Base lattice constructions

Let now $\zeta = e^{\pi i/8}$ (resp. $\xi = e^{\pi i/4} = (1+i)/\sqrt{2}$) be a primitive 16^{th} (resp. 8^{th}) root of unity. Our main examples of suitable division algebras are the number field

$$\mathbf{L} = \mathbb{Q}(\zeta),$$

and the following subskewfield

$$\mathbf{H} = \mathbb{Q}(\xi) \oplus j\mathbb{Q}(\xi) \subseteq \mathbb{H}$$

of the Hamiltonian quaternions. Note that as $zj = jz^*$ for all complex numbers z, and as the field $\mathbb{Q}(\xi)$ is stable under the usual complex conjugation $(^*)$, the set $\mathbf{H}$ is, indeed, a subskewfield of the quaternions.

As always, multiplication (from the left) by a non-zero element of a division algebra $\mathcal{A}$ is an invertible $\mathbb{Q}(i)$-linear mapping (with $\mathbb{Q}(i)$ acting from the right). Therefore its matrix with respect to a chosen $\mathbb{Q}(i)$-basis $\mathcal{B}$ of $\mathcal{A}$ is also invertible. Our example division algebras $\mathbf{L}$ and $\mathbf{H}$ have the sets $\mathcal{B}_L = \{1, \zeta, \zeta^2, \zeta^3\}$ and $\mathcal{B}_H = \{1, \xi, j, j\xi\}$ as natural $\mathbb{Q}(i)$-bases. Thus we immediately arrive at the following matrix representations of our division algebras.

Proposition 2.1: Let the variables c_1, c_2, c_3, c_4 range over all the elements of $\mathbb{Q}(i)$. The division algebras $\mathbf{L}$ and $\mathbf{H}$ can be identified via an isomorphism ϕ with the following rings of matrices

$$\mathbf{L} = \left\{ M_L = M_L(c_1,c_2,c_3,c_4) = \begin{pmatrix} c_1 & ic_4 & ic_3 & ic_2 \\ c_2 & c_1 & ic_4 & ic_3 \\ c_3 & c_2 & c_1 & ic_4 \\ c_4 & c_3 & c_2 & c_1 \end{pmatrix} \right\}$$

and

$$\mathbf{H} = \left\{ M = M(c_1,c_2,c_3,c_4) = \begin{pmatrix} c_1 & ic_2 & -c_3^* & -c_4^* \\ c_2 & c_1 & ic_4^* & -c_3^* \\ c_3 & ic_4 & c_1^* & c_2^* \\ c_4 & c_3 & -ic_2^* & c_1^* \end{pmatrix} \right\}.$$

The isomorphism ϕ from $\mathbf{L}$ into the matrix ring is determined by $\mathbb{Q}(i)$-linearity and the fact that ζ corresponds to the choice $c_2 = 1, c_1 = c_3 = c_4 = 0$. The isomorphism ϕ from $\mathbf{H}$ into the matrix ring is determined by $\mathbb{Q}(i)$-linearity and the facts that ξ corresponds to the choice $c_2 = 1$, $c_1 = c_3 = c_4 = 0$, and j corresponds to the choice $c_3 = 1$, $c_1 = c_2 = c_4 = 0$. In particular, the determinants of these matrices are non-zero whenever at least one of the coefficients c_1, c_2, c_3, c_4 is non-zero. ■

In order to get ST lattices and useful bounds for the minimum determinant, we need to identify suitable subrings S of these two algebras. Actually, we would like these rings to be free right $\mathcal{G}$-modules of rank 4. This is due to the fact that then the determinants of the matrices of Proposition 2.1 that belong to the subring $\phi(S)$ must be elements of the ring $\mathcal{G}$. We repeat the well-known reason for this for the sake of completeness: the determinant of the matrix representing the multiplication by a fixed element $x \in S$ does not depend on the choice of the basis $\mathcal{B}$ and thus we may assume that it is a $\mathcal{G}$-module basis. However, in that case $x\mathcal{B} \subseteq S$, so the matrix will have entries in $\mathcal{G}$ as all the elements of S are $\mathcal{G}$-linear combinations of $\mathcal{B}$. The claim follows.

In the case of the field $\mathbf{L}$ we are only interested in its ring of integers $\mathcal{O}_L = \mathbb{Z}[\zeta]$ that is a free $\mathcal{G}$-module with the basis $\mathcal{B}_L$. In this case the ring $\phi(\mathcal{O}_L)$ consists of those matrices of $\mathbf{L}$ that have all the coefficients $c_1, c_2, c_3, c_4 \in \mathcal{G}$. Similarly, the $\mathcal{G}$-module

$$\mathcal{L} = \mathcal{G} \oplus \xi\mathcal{G} \oplus j\mathcal{G} \oplus j\xi\mathcal{G}$$

spanned by our earlier basis $\mathcal{B}_H$ is a ring of the required type. We call this the ring of *Lipschitz' integers of* $\mathbf{H}$. Again $\phi(\mathcal{L})$ consists of

those matrices of $\mathbf{H}$ that have all the coefficients $c_1, c_2, c_3, c_4 \in \mathcal{G}$. While $\mathcal{O}_L$ is known to be maximal among the rings satisfying our requirements, the same is not true about $\mathcal{L}$. The ring $\mathbb{H}_{\mathcal{H}}$ also has an extension of the prescribed type inside $\mathbf{H}$, called the ring of *Hurwitz' integers of* $\mathbf{H}$. This ring, denoted by

$$\mathcal{H} = \rho\mathcal{G} \oplus \rho\xi\mathcal{G} \oplus j\mathcal{G} \oplus j\xi\mathcal{G},$$

is the right $\mathcal{G}$-module generated by the basis $\mathcal{B}_{Hur} = \{\rho, \rho\xi, j, j\xi\}$, where again $\rho = (1+i+j+k)/2$. The fact that $\mathcal{H}$ is a subring can easily be verified by straightforward computations, e.g. $\xi\rho = \rho\xi - j\xi$. For future use we express the ring $\mathcal{H}$ in terms of the basis $\mathcal{B}_H$ of Proposition 2.1. It is not difficult to see that the element

$$q = c_1 + \xi c_2 + jc_3 + j\xi c_4 \in \mathbf{H}$$

is an element of $\mathcal{H}$, if and only if the coefficients c_t satisfy the requirements $(1+i)c_t \in \mathcal{G}$ for all $t = 1, 2, 3, 4$ and $c_1 + c_3, c_2 + c_4 \in \mathcal{G}$. As the ideal generated by $1+i$ has index two in $\mathcal{G}$, we see that $\mathcal{L}$ is an additive, index four subgroup in $\mathcal{H}$. We summarize these findings in Proposition 2.2. The bound on the minimum determinant is a consequence of the fact that all the elements of $\mathcal{G}$ have a norm at least one.

Proposition 2.2: The following rings of matrices form ST lattices with minimum determinant equal to one.

$$L_1 = \{M_L(c_1, c_2, c_3, c_4) \mid c_1, c_2, c_3, c_4 \in \mathcal{G}\},$$

$$L_2 = \{M(c_1, c_2, c_3, c_4) \mid c_1, c_2, c_3, c_4 \in \mathcal{G}\},$$

$$L_3 = \{M(c_1, c_2, c_3, c_4) \mid c_1, c_2, c_3, c_4 \in \frac{1+i}{2}\mathcal{G},$$

$$c_1 + c_3 \in \mathcal{G}, c_2 + c_4 \in \mathcal{G}\}.$$

■

Remark 2.1: The lattice L_1 is quite similar to the DAST lattice in the sense that all of its matrices can be simultaneously diagonalized. See more details in Section IV-B. The lattice L_2, for its part, is a more developed case from the so-called *quasi-orthogonal* STBC suggested e.g. in [30]. The matrix $M(c_1, c_2, c_3, c_4)$ of Proposition 2.1 can also be found as an example in the landmark paper [6], but no optimization has been done there by using, for example, ideals as we shall do here.

A drawback shared by the lattices L_1 and L_2 is that in the ambient space of the transmitter they are isometric to the rectangular lattice $\mathbb{Z}^8$. The rectangular shape does carry the advantage that the sets of information carrying coefficients of the basis matrices are simple and all identical which is useful in e.g. sphere decoding. But, on the other hand, this shape is very wasteful in terms of transmission power. Geometrically denser sublattices of $\mathbb{Z}^8$, e.g. the checkerboard lattice

$$D_8 = \left\{ (x_1, ..., x_8) \in \mathbb{Z}^8 \;\middle|\; \sum_{i=1}^{8} x_i \equiv 0 \pmod 2 \right\}$$

and the diamond lattice

$$E_8 = \left\{ (x_1, ..., x_8) \in \mathbb{Z}^8 \;\middle|\; x_i \equiv x_j \pmod 2,\ \sum_{i=1}^{8} x_i \equiv 0 \pmod 4 \right\},$$

are well-known (cf. e.g. [31]). However, we must be careful in picking the copies of the sublattices, as it is the minimum determinant we want to keep an eye on (see Remark 2.3).

B. Dense sublattices inside the base lattice L_2

As our earlier simulations [3],[4] have shown that L_2 outperforms L_1, we concentrate on finding good sublattices of L_2. The units of the ring L_2 are exactly the non-zero matrices whose determinants have the minimal absolute value of one. Thus a natural way to find a sublattice with a better minimum determinant is to take the lattice $\phi(\mathcal{I})$, where $\mathcal{I} \subset S$ is a proper ideal. This idea has appeared at least in [3], [4], and [8]. Even earlier, ideals of rings of algebraic integers were used in [27] to produce dense lattices. Let us first record the following simple fact.

Lemma 2.3: Let A and B be diagonalizable complex square matrices of the same size. Assume that they commute and that their eigenvalues are all real and non-negative. Then

$$\det(A + B) \geq \det A + \det B$$

with a strict inequality if both A and B are invertible.

Proof: As A and B commute, they can be simultaneously diagonalized. Hence, we can reduce the claim to the case of diagonal matrices with non-negative real entries. In that case the claim is obvious. ■

In Proposition 2.4 we give a construction isometric to the checkerboard lattice D_8

Proposition 2.4: Let $\mathcal{I}$ be the prime ideal of the ring $\mathcal{G}$ generated by $1+i$. Define

$$\mathcal{I}_{\mathcal{L}} = \{(c_1 + \xi c_2) + j(c_3 + \xi c_4) \in \mathcal{L} \mid c_1 + c_2 + c_3 + c_4 \in \mathcal{I}\}.$$

Then $\mathcal{I}_{\mathcal{L}}$ is an ideal of index two in $\mathcal{L}$. The corresponding lattice

$$L_4 = \{M(c_1, c_2, c_3, c_4) \in L_2 \mid c_1 + c_2 + c_3 + c_4 \in \mathcal{I}\}$$

is an index 2 sublattice in L_2. Furthermore, the absolute value of $\det(MM^H),\ M \in L_4 \setminus \{0\}$, is then at least 4.

Proof: It is straightforward to check that $\mathcal{I}_{\mathcal{L}}$ is stable under (left or right) multiplication with the quaternions ξ and j, so $\mathcal{I}_{\mathcal{L}}$ is an ideal in $\mathcal{L}$.

Let us consider a matrix $M \in L_4$ and write it in the block form

$$M = \begin{pmatrix} A & -B^H \\ B & A^H \end{pmatrix}.$$

We see that

$$MM^H = \begin{pmatrix} AA^H + BB^H & 0 \\ 0 & AA^H + BB^H \end{pmatrix},$$

and

$$AA^H + BB^H = \begin{pmatrix} \alpha & k^* \\ k & \alpha \end{pmatrix},$$

where $\alpha = \sum_{j=1}^{4} |c_j|^2$ is a non-negative integer and $k = -ic_1c_2^* + c_2c_1^* - ic_3c_4^* + c_4c_3^*$ is a Gaussian integer with the property $k^* = ik$. We are to prove that $\det MM^H = \left(\alpha^2 - |k|^2\right)^2 \geq 4$. Assume first that $c_3 = c_4 = 0$, i.e. the block $B = 0$. Then $\det(A)$ is the relative norm

$$\det(A) = N_{\mathbb{Q}(i)}^{\mathbb{Q}(\xi)}(c_1 + \xi c_2),$$

which is a Gaussian integer. As $c_1 + \xi c_2$ is a non-zero element of the ideal $\mathcal{I}$, we conclude that $\det(A)$ is a non-zero non-unit. Therefore $\det(A)\det(A^H) \geq 2$, and the claim follows.

Let us then assume that both A and B are non-zero. Then $\det(A)$ and $\det(B)$ are non-zero Gaussian integers and have a norm at least one. The matrices A, A^H, B, B^H all commute, so by Lemma 2.3 we get

$$\det(MM^H) > \det(AA^H)^2 + \det(BB^H)^2 \geq 2.$$

As $\det(MM^H) = \left(\alpha^2 - |k|^2\right)^2$ is a square of a rational integer, it must be at least 4. ∎

Remark 2.2: It is easy to see that in the previous proposition $a + bi \in \mathcal{I}$, if and only if $a + b$ is an even integer. Thus geometrically the matrix lattice L_4 is, indeed, isometric to D_8.

We proceed to describe two more interesting sublattices of L_2 with even better minimum determinants. To that end we use the ring $\mathcal{H}$ (or the lattice L_3). The first sublattice is isometric to the direct sum $D_4 \perp D_4$ [31] of two 4-dimensional checkerboard lattices.

Proposition 2.5: Let again $\mathcal{I}$ be the ideal $(1+i)\mathcal{G}$. The lattice

$$L_5 = \{M(c_1, c_2, c_3, c_4) \in L_2 \mid c_1 + c_3, c_2 + c_4 \in \mathcal{I}\}$$

has a minimum determinant equal to 16. The index of L_4 in L_2 is 4.

Proof: The coefficients c_1 and c_3 can be chosen arbitrarily within $\mathcal{G}$. The the ideal $\mathcal{I}$ has index 2 in $\mathcal{G}$, and the coefficients c_2 and c_4 now must belong to the cosets $c_1 + \mathcal{I}$ and $c_3 + \mathcal{I}$ respectively. Whence, the index of L_5 in L_2 is 4. The matrices A in the lattice L_5 are of the form $A = (1+i)M$, where M is a matrix in the lattice L_3 of Proposition 2.2. Thus $\det(AA^H) = 16\det(MM^H)$ and the claim follows from Proposition 2.2. ∎

The diamond lattice E_8 can be described in terms of the Gaussian integers as (cf. [32])

$$E_8 = \frac{1}{1+i}\{(c_1, c_2, c_3, c_4) \in \mathcal{G}^4 \mid c_1 + \mathcal{I} = c_t + \mathcal{I},$$

$$t = 2, 3, 4, \ \sum_{t=1}^{4} c_t \in 2\mathcal{G}\}.$$

By our identification of quadruples $(c_1, c_2, c_3, c_4) \in \mathcal{G}^4$ and the elements of $\mathbf{H}$ it is straightforward to verify that $(1+i)E_8$ has $\{2, (1+i)+(1+i)\xi, (1+i)\xi+(1+i)j, 1+\xi+j+j\xi\} \subseteq \mathcal{L}$ as a $\mathcal{G}$-basis, whence the set $\{1+i, 1+\xi, \xi+j, \rho+\rho\xi\} \subseteq \mathcal{H}$ is a $\mathcal{G}$-basis for E_8. By another simple computation we see that $E_8 = \mathcal{H}(1+\xi)$, i.e. E_8 is the left ideal of the ring $\mathcal{H}$ generated by $1+\xi$.

Proposition 2.6: The lattice

$$L_6 = \{M(c_1, c_2, c_3, c_4) \in L_2 \mid \ c_1 + \mathcal{I} = c_t + \mathcal{I},$$

$$t = 2, 3, 4, \ \sum_{t=1}^{4} c_t \in 2\mathcal{G}\}$$

is an index 16 sublattice of L_2. Furthermore, the minimum determinant of L_6 is 64.

Proof: Let $M_I = M(1, 1, 0, 0)$ be the matrix $\phi(1+\xi)$ under the isomorphism of Proposition 2.1. We see that $\det(M_I M_I^H) = 4$. By the preceding discussion any matrix A of the lattice L_6 has the form $A = MM_I(1+i)$, where M is a matrix in L_3. As in the proof of Proposition 2.5, we see that $\det AA^H = 16\det(M_I M_I^H)\det(MM^H)$. The claim on the minimum determinant now follows from Proposition 2.2. We see that the coefficient c_1 can be chosen arbitrarily within $\mathcal{G}$. The coefficients c_2 and c_3 then must belong to the coset $c_1 + \mathcal{I}$, and c_4 must be chosen such that $c_1 + c_2 + c_3 + c_4 \in 2\mathcal{G} = \mathcal{I}^2$. As $\mathcal{I}$ has index two in $\mathcal{G}$, we see that the index of L_6 in L_2 is 16 as claimed. ∎

Remark 2.3: We have now produced a *nested sequence of lattices*

$$2\mathbb{Z}^8 = 2L_2 \subseteq L_6 \subseteq L_5 \subseteq L_4 \subseteq L_2 = \mathbb{Z}^8 (\subseteq L_3). \qquad (1)$$

We concentrate on the lattices that are sandwiched between $2\mathbb{Z}^8$ and $\mathbb{Z}^8$. It is worthwhile to note that these lattices are in a bijective correspondence with a binary linear code of length 8 by projection modulo 2, see Table I above. As it happens, within this sequence of lattices the minimum Hamming distance of the binary linear code and the minimum determinant of the lattice are somewhat related.

TABLE I
LATTICES FROM A CODING THEORETICAL POINT OF VIEW

$L_2 \leftrightarrow$ The 8-dimensional rectangular grid $\mathbb{Z}^8$
$\leftrightarrow$ no coding
$\downarrow$
$L_4 \leftrightarrow$ The checkerboard lattice D_8
$\leftrightarrow$ overall parity check code of length 8
$\downarrow$
$L_5 \leftrightarrow$ The lattice $D_4 \perp D_4$
$\leftrightarrow$ two blocks of the overall parity check code of length 4
$\downarrow$
$L_6 \leftrightarrow$ The diamond lattice E_8
$\leftrightarrow$ extended Hamming-code of length 8

Thereupon it is natural to ask that what if we simply concatenate the use of L_2 with a good binary code (extended over several L_2-blocks, if needed), and be done with it. While the binary linear codes appearing above are the first ones that come to one's mind, we want to caution the unwary end-user. Namely, it is possible that there are high weight units in the ring in question. If such binary words are included, then the minimum determinant of the corresponding lattice is equal to 1, i.e. no coding gain will take place. E.g. the unit $(1-\xi^3)/(1-\xi) = 1 + \xi + \xi^2 = (1+i) + \xi$ of the ring $\mathcal{L}$ corresponds to the matrix $M(1+i, 1, 0, 0)$ of determinant 1, and thus we must not allow such words of weight 3. If the lattice L_1 were used, the situation would be even worse, as then we have units like $(1-\zeta^7)/(1-\zeta)$ in the ring $\mathcal{O}_L$ that would be mapped to a word of Hamming weight 7. A construction based on ideals provides a mechanism to avoid this problem caused by high weight units.

III. CYCLIC ALGEBRAS AND ORDERS

In Section II we produced a nested sequence (1) of quaternionic lattices with the property that as the lattice gets denser after rescaling the increased minimum determinant back to one, the BLER perfomance gets better. As the sequence (1) lies within a specific division algebra, an obvious question evokes how to generalize this idea. The theory of cyclic division algebras and their maximal orders offer us an answer. When designing square ST matrix lattices for MIMO use, cyclic division algebras are of utmost interest as it has been shown in [15] that a non-vanishing determinant is a sufficient condition for full-rate CDA based STBC-designs to achieve the upper bound on the optimal DMT, hence proving that the upper bound itself is the optimal DMT for any number of transmitters and receivers. Given the number of transmitters n, we pick a suitable cyclic division algebra of index n (more on this in a forthcoming paper, see Section VII and [33]. See also [15]). The matrix representation of the algebra, with some constraints on the elements, will then correspond to the base lattice, similarly as did the lattice L_2 in Section II. Now in order to make the lattice denser, we choose the elements in the matrices from an order. The natural first choice for an order is the one corresponding to the ring of algebraic integers of the maximal subfield inside the algebra. The densest possible sublattice is the one where the elements come from a maximal order.

All algebras considered here are finite dimensional associative algebras over a field.

A. Cyclic algebras

The basic theory of cyclic algebras and their representations as matrices are thoroughly considered in [[34], Chapter 8.5] and [6]. We are only going to recapitulate the essential facts here.

In the following, we consider number field extensions E/F, where F denotes the base field. F^* (resp. E^*) denotes the set of non-zero elements of F (resp. E). Let E/F be a cyclic field extension of degree n with the Galois group $Gal(E/F) = \langle\sigma\rangle$, where σ is the generator of the cyclic group. Let $\mathcal{A} = (E/F, \sigma, \gamma)$ be the corresponding cyclic algebra of *index* n, that is,

$$\mathcal{A} = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E,$$

with $u \in \mathcal{A}$ such that $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in F^*$. An element $a = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{A}$ has the following representation as a matrix $A =$

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}. \quad (2)$$

Let us compute the third column as an example:

$$\begin{aligned} u^2 \mapsto au^2 &= x_0u^2 + ux_1u^2 + \cdots + u^{n-1}x_{n-1}u^2 \\ &= u\sigma(x_0)u + u^2\sigma(x_1)u + \cdots + \gamma\sigma(x_{n-1})u \\ &= u^2\sigma^2(x_0) + u^3\sigma^2(x_1) + \cdots + u\gamma\sigma^2(x_{n-1}), \end{aligned}$$

and hence as the third column we get the vector

$$(\gamma\sigma^2(x_{n-2}), \gamma\sigma^2(x_{n-1}), \sigma^2(x_0), \ldots, \sigma^2(x_{n-3}))^T.$$

Let us denote the ring of algebraic integers of E by $\mathcal{O}_E$. A basic, rate-n MIMO STBC $\mathcal{C}$ is usually defined as $\mathcal{C} =$

$$\left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix} \;\middle|\; x_i \in \mathcal{O}_E \right\}. \quad (3)$$

Further optimization might be carried out by using e.g. ideals. If we denote the basis of E over $\mathcal{O}_F$ by $\{1, e_1, ..., e_{n-1}\}$, then the elements $x_i,\ i = 0, ..., n-1$ in (3) take the form $x_i = \sum_{k=0}^{n-1} f_k e_k$, where $f_k \in \mathcal{O}_F$ for all $k = 0, ..., n-1$. Hence n complex symbols are transmitted per channel use, i.e. the design has rate n. In literature this is often referred to as having a *full rate*.

Definition 3.1: An algebra $\mathcal{A}$ is called *simple* if it has no nontrivial ideals. An F-algebra $\mathcal{A}$ is *central* if its center $Z(A) = \{a \in \mathcal{A} | aa' = a'a\ \forall a' \in \mathcal{A}\} = F$.

Definition 3.2: An ideal $\mathcal{I}$ is called *nilpotent* if $\mathcal{I}^k = 0$ for some $k \in \mathbb{Z}_+$. An algebra $\mathcal{A}$ is *semisimple* if it has no nontrivial nilpotent ideals. Any finite dimensional semisimple algebra over a field is a finite and unique direct sum of simple algebras.

Definition 3.3: The determinant (resp. trace) of the matrix A is called the *reduced norm* (resp. *reduced trace*) of an element $a \in \mathcal{A}$ and is denoted by $nr(a)$ (resp. $tr(a)$).

Remark 3.1: The connection with the usual norm map $N_{A/F}(a)$ (resp. trace map $T_{A/F}(a)$) and the reduced norm $nr(a)$ (resp. reduced trace $tr(a)$) of an element $a \in \mathcal{A}$ is $N_{A/F}(a) = (nr(a))^n$ (resp. $T_{A/F}(a) = ntr(a)$), where n is the degree of E/F.

In Section II we have attested that the algebra $\mathbf{H}$ is a division algebra. The next old result due to A. A. Albert [[35], Chapter V.9] provides us with a condition for when an algebra is indeed a division algebra.

Proposition 3.1: The algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ of index n is a division algebra, if and only if the smallest factor $t \in \mathbb{Z}_+$ of n such that γ^t is the norm of some element in E^*, is n. ■

B. Orders

We are now ready to present some of the basic definitions and results from the theory of maximal orders. The general theory of maximal orders can be found in [36].

Let S denote a Noetherian integral domain with a quotient field F, and let $\mathcal{A}$ be a finite dimensional F-algebra.

Definition 3.4: An *S-order* in the F-algebra $\mathcal{A}$ is a subring Λ of $\mathcal{A}$, having the same identity element as $\mathcal{A}$, and such that Λ is a finitely generated module over S and generates $\mathcal{A}$ as a linear space over F.

As usual, an S-order in $\mathcal{A}$ is said to be *maximal*, if it is not properly contained in any other S-order in $\mathcal{A}$. If the integral closure $\overline{S}$ of S in $\mathcal{A}$ happens to be an S-order in $\mathcal{A}$, then $\overline{S}$ is automatically the unique maximal S-order in $\mathcal{A}$.

Let us illustrate the above definition by the following example.

Example 3.1: (a) Orders always exist: If M is a full S-lattice in $\mathcal{A}$, i.e. $FM = \mathcal{A}$, then the *left order* of M defined as $\mathcal{O}_l(M) = \{x \in \mathcal{A} \mid xM \subseteq M\}$ is an S-order in $\mathcal{A}$. The right order is defined in an analogous way.

(b) If $\mathcal{A} = \mathcal{M}_n(F)$, the algebra of all $n \times n$ matrices over F, then $\Lambda = \mathcal{M}_n(S)$ is an S-order in $\mathcal{A}$.

(c) Let $a \in \mathcal{A}$ be integral over S, that is, a is a zero of a monic polynomial over S. Then the ring $S[a]$ is an S-order in the F-algebra $F[a]$.

(d) Let S be a Dedekind domain, and let E be a finite separable extension of F. Denote by $\overline{S}$ the integral closure of S in E. Then $\overline{S}$ is an S-order in E. In particular, taking $S = \mathbb{Z}$, we see that the ring of algebraic integers of E is a $\mathbb{Z}$-order in E.

Hereafter, F will be an algebraic number field and S a Dedekind ring with F as a field of fractions.

Proposition 3.2: Let $\mathcal{A}$ be a finite dimensional semisimple algebra over F and Λ be a $\mathbb{Z}$-order in $\mathcal{A}$. Let $\mathcal{O}_F$ stand for the ring of algebraic integers of F. Then $\Gamma = \mathcal{O}_F\Lambda$ is an $\mathcal{O}_F$-order containing Λ. As a consequence, a maximal $\mathbb{Z}$-order in $\mathcal{A}$ is a maximal $\mathcal{O}_F$-order as well. ■

The following proposition provides us with a useful tool for finding a maximal order within a given algebra.

Proposition 3.3: Let Λ be an S-order in $\mathcal{A}$. For each $a \in \Lambda$ we have $nr(a) \in S$ and $tr(a) \in S$. ■

Proposition 3.4: Let Γ be a subring of $\mathcal{A}$ containing S, such that $F\Gamma = \mathcal{A}$, and suppose that each $a \in \Gamma$ is integral over S. Then Γ is an S-order in $\mathcal{A}$. Conversely, every S-order in $\mathcal{A}$ has these properties. ■

Corollary 3.5: Every S-order in $\mathcal{A}$ is contained in a maximal S-order in $\mathcal{A}$. There exists at least one maximal S-order in $\mathcal{A}$. ■

Remark 3.2: As the previous corollary indicates, a maximal order of an algebra is not necessarily unique.

Remark 3.3: The algebra $\mathbf{H}$ can also be viewed as a cyclic division algebra. As it is a subring of the Hamiltonian quaternions, its center consists of the intersection $\mathbf{H} \cap \mathbb{R} = \mathbb{Q}(\sqrt{2})$. Also $\mathbb{Q}(\xi)$ is an example of a splitting field of $\mathbf{H}$. In the notation above we have an obvious isomorphism

$$\mathbf{H} \simeq (\mathbb{Q}(\xi)/\mathbb{Q}(\sqrt{2}), \sigma, -1),$$

where σ is the usual complex conjugation.

Remark 3.4: In principle, the lattices from Section II could also be used as MIMO codes, but when we pack $\mathbf{H}$ in the form of (2), $\delta_{\mathcal{C}}$ becomes vanishing and the DMT cannot be achieved.

One extremely well-performing CDA based code taking advantage of a maximal order is the celebrated *Golden code* [8] (also independently found in [9]) treated in the following example.

Example 3.2: In any cyclic algebra where the element γ happens to be an algebraic integer, we have the following *natural order*

$$\Lambda = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E,$$

where $\mathcal{O}_E$ is the ring of integers of the field E. We note that $\mathcal{O}_E$ is the unique maximal order in E. In the so-called *Golden Division Algebra* (GDA) [8], i.e. the cyclic algebra $(E/F, \sigma, \gamma)$ obtained from the data $E = \mathbb{Q}(i, \sqrt{5})$, $F = \mathbb{Q}(i)$, $\gamma = i$, $n = 2$, $\sigma(\sqrt{5}) = -\sqrt{5}$, the natural order Λ is already maximal [37]. The ring of algebraic integers $\mathcal{O}_E = \mathbb{Z}[i][\theta]$, when we denote the golden ratio by $\theta = \frac{1+\sqrt{5}}{2}$. The authors of [8] further optimize the code by using an ideal $(\alpha) = (1 + i - i\theta)$, and the Golden code is then defind as

$$\mathcal{GC} = \left\{ \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha x_0 & i\sigma(\alpha)\sigma(x_1) \\ \alpha x_1 & \sigma(\alpha)\sigma(x_0) \end{pmatrix} \;\middle|\; x_0, x_1 \in \mathcal{O}_E \right\}. \quad (4)$$

The Golden code achieves the DMT as the element $\gamma = i$ is not in the image of the norm map. For the proof, see [8].

Remark 3.5: We feel that in [8], the usage of a maximal order is just a coincidence, as in this case it coincides with the natural order which is generally used in ST code designs (cf. (3)). At least the authors do not mention maximal orders. As far as we know, but our constructions (see also [33]) there does not exist any designs using a maximal order other than the natural one.

Next we prove that the lattice L_6 is optimal within the cyclic division algebra $\mathbf{H}$ in the sense that the diamond lattice $E_8 = \mathcal{H}(1+\xi)$ corresponds to a proper ideal of a maximal order in $\mathbf{H}$.

Proposition 3.6: The ring

$$\mathcal{H} = \{q = c_1 + \xi c_2 + jc_3 + j\xi c_4 \in \mathbf{H} \mid c_1, \ldots, c_4 \in \mathbb{Q}(i),$$
$$(1+i)c_t \in \mathcal{G}\ \forall t, c_1 + c_3, c_2 + c_4 \in \mathcal{G}\}$$

is a maximal $\mathbb{Z}$-order of the division algebra $\mathbf{H}$.

Proof: Clearly the $\mathbb{Q}$-span of $\mathcal{H}$ is the whole algebra $\mathbf{H}$, and we have seen that $\mathcal{H}$ is a ring, so it is an order of $\mathbf{H}$. Furthermore, if Λ is any order of $\mathbf{H}$, then so is $\Lambda[\sqrt{2}] = \Lambda \cdot \mathbb{Z}[\sqrt{2}]$, as the element $\sqrt{2}$ is in the center of $\mathbf{H}$ (cf. Proposition 3.2). Therefore it suffices to show that $\mathcal{H}$ is a maximal $\mathbb{Z}[\sqrt{2}]$-order. In what follows, we will call rational numbers in the coset $(1/2) + \mathbb{Z}$ half-integers. Assume for contradiction that we could extend the order $\mathcal{H}$ into a larger order $\Gamma = \mathcal{H}[q]$ by adjoining the quaternion $q = a_1 + a_2 j$, where the coefficients

$$a_t = m_{t,0} + m_{t,1}\xi + m_{t,2}\xi^2 + m_{t,3}\xi^3, \quad m_{t,\ell} \in \mathbb{Q} \text{ for all } t, \ell$$

are elements of the field $\mathbb{Q}(\xi)$. As $\xi - \xi^3 = \sqrt{2}$, and $\xi^* = -\xi^3$, we see that

$$tr(q) = a_1 + a_1^* = 2m_{1,0} + \sqrt{2}(m_{1,1} - m_{1,3}).$$

By Proposition 3.3 this must be an element of $\mathbb{Z}[\sqrt{2}]$, so we may conclude that $m_{1,0}$ must be an integer or a half-integer, and that $m_{1,1} - m_{1,3}$ must be an integer. Similarly

$$tr(q\xi) = -2m_{1,3} + \sqrt{2}(m_{1,0} - m_{1,2})$$

must be an element of $\mathbb{Z}[\sqrt{2}]$. We may thus conclude that all the coefficients $m_{1,\ell},\ \ell = 0, 1, 2, 3$ are integers or half-integers, and that the pairs $m_{1,0}, m_{1,2}$ (resp. $m_{1,1}, m_{1,3}$) must be of the same type, i.e. either both are integers or both are half-integers. A similar study of $tr(qj)$ and $tr(qj\xi)$ shows that the same conclusions also hold for the coefficients $m_{2,\ell},\ \ell = 0, 1, 2, 3$. Because $\mathbb{Z}[\xi] \subseteq \mathcal{H}$, replacing q with any quaternion of the form $q - \nu$, where $\nu \in \mathbb{Z}[\xi]$ will not change the resulting order Γ. Thus we may assume that the coefficients $m_{1,\ell},\ \ell = 0, 1, 2, 3$ all belong to the set $\{0, 1/2\}$. Similarly, if needed, replacing q with $q - \nu' j$ for some $\nu' \in \mathbb{Z}[\xi]$ allows us to assume that the coefficients $m_{2,\ell},\ \ell = 0, 1, 2, 3$ also all belong to the set $\{0, 1/2\}$. Further replacements of q by $q - \rho$ or $q - \rho\xi$ then permit us to restrict ourselves to the case $m_{2,\ell} = 0$, for all $\ell = 0, 1, 2, 3$. If we are to get a proper extension of $\mathcal{H}$, we are left with the cases $q = (1+i)/2$, $q = \xi(1+i)/2$ and $q = (1+\xi)(1+i)/2$. We immediately see that none of these have reduced norms in $\mathbb{Z}[\sqrt{2}]$, so we have arrived at a contradiction. ∎

Remark 3.6: Another related well known maximal order is the icosian ring. It is a maximal order in another subalgebra of the Hamiltonian quaternions, namely

$$(\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(\sqrt{5}), \sigma, -1),$$

where σ is again the usual complex conjugation. This order made a recent appearance as a building block of a MIMO-code in a construction by Liu & Calderbank. We refer the interested reader to their work [38] or [31] for a detailed description of this order.

The icosian ring and our order share one feature that is worth mentioning. As 2×2 matrices they do not have the non-vanishing determinant property. Algebraically this is a consequence of the fact the respective centers, $\mathbb{Q}(\sqrt{5})$ or $\mathbb{Q}(\sqrt{2})$ both have arbitrarily small algebraic integers, e.g. the sequence consisting of powers of the units $(\sqrt{5}-1)/2$ (resp. $\sqrt{2}-1$) converges to zero. We shall return to this point in the next section, where a remedy is described.

IV. Decoding of the nested sequence of lattices

In this section, let us consider the coherent MIMO case where the receiver perfectly knows the channel coefficients. The received signal is

$$\mathbf{y} = B\mathbf{x} + \mathbf{n},$$

where $\mathbf{x} \in \mathbb{R}^m$, $\mathbf{y},\ \mathbf{n} \in \mathbb{R}^n$ denote the channel input, output and noise signals, and $B \in \mathbb{R}^{n \times m}$ is the Rayleigh fading channel response. The components of the noise vector $\mathbf{n}$ are i.i.d. complex Gaussian random variables. In the special case of a MISO channel ($n = 1$), the channel matrix takes a form of a vector $B = \mathbf{h} \in \mathbb{R}^m$ (cf. Section I).

The information vectors to be encoded into our code matrices are taken from the pulse amplitude modulation (PAM) signal set $\mathcal{X}$ of the size Q, i.e.,

$$\mathcal{X} = \{u = 2q - Q + 1 \ \mid \ q \in \mathbb{Z}_Q\}$$

with $\mathbb{Z}_Q = \{0, 1, ..., Q-1\}$.

Under this assumption, the optimal detector $g : \mathbf{y} \mapsto \hat{\mathbf{x}} \in \mathcal{X}^m$ that minimizes the average error probability

$$P(e) \triangleq P(\hat{\mathbf{x}} \neq \mathbf{x})$$

is the maximum-likelihood (ML) detector given by

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x} \in \mathbb{Z}_Q^m} \mid \mathbf{y} - \mathbf{B}\mathbf{x} \mid^2, \quad (5)$$

where the components of the noise $\mathbf{n}$ have a common variance equal to one.

A. Code controlled sphere decoding

The search in (5) for the *closest lattice point* to a given point $\mathbf{y}$ is known to be NP-hard in the general case where the lattice does not exhibit any particular structure. In [39], however, Pohst proposed an efficient strategy of enumerating all the lattice points within a

sphere $\mathcal{S}(\mathbf{y}, \sqrt{C_0})$ centered at $\mathbf{y}$ with a certain radius $\sqrt{C_0}$ that works for lattices of a moderate dimension. For background, see [40]-[43]. For finite PAM signals sphere decoders can also be visualized as a *bounded search* in a tree.

The complexity of sphere decoders critically depends on the preprocessing stage, the ordering in which the components are considered, and the initial choice of the sphere radius. We shall use the standard preprocessing and ordering that consists of the *Gram-Schmidt orthonormalization* $B = (Q, Q') \begin{pmatrix} R \\ 0 \end{pmatrix}$ of the columns of the channel matrix B (equivalently, QR *decomposition* on B) and the natural back-substitution component ordering given by $x_m, ..., x_1$. The matrix R is an $m \times m$ upper triangular matrix with positive diagonal elements, Q (resp. Q') is an $n \times m$ (resp. $n \times (n-m)$) unitary matrix, and 0 is an $(n-m) \times m$ zero matrix.

The condition $B\mathbf{x} \in \mathcal{S}(\mathbf{y}, \sqrt{C_0})$ can be written as

$$| \mathbf{y} - B\mathbf{x} |^2 \leq C_0 \tag{6}$$

which after applying the QR decomposition on B takes the form

$$| \mathbf{y}' - R\mathbf{x} |^2 \leq C_0', \tag{7}$$

where $\mathbf{y}' = Q^T\mathbf{y}$ and $C_0' = C_0 - |(Q')^T\mathbf{y}|^2$. Due to the upper triangular form of R, (7) implies the set of conditions

$$\sum_{j=i}^{m} \left| y_j' - \sum_{\ell=j}^{m} r_{j,\ell} x_\ell \right|^2 \leq C_0', \quad i = 1, ..., m. \tag{8}$$

The sphere decoding algorithm outputs the point $\hat{\mathbf{x}}$ for which the distance

$$d^2(\mathbf{y}, B\mathbf{x}) = \sum_{j=1}^{m} \left| y_j' - \sum_{\ell=j}^{m} r_{j,\ell} x_\ell \right|^2 \tag{9}$$

is minimum. See details in [43].

The decoding of the base lattice L_2 can be performed by using the algorithm below proposed in [43].

Algorithm II, Smart Implementation (Input C_0', $\mathbf{y}'$, R. Output $\hat{\mathbf{x}}$.)

STEP 1: (Initialization) Set $i := m$, $T_m := 0$, $\xi_m := 0$, and $d_c := C_0'$ (current sphere squared radius).

STEP 2: (DFE on x_i) Set $x_i := \lfloor (y_i' - \xi_i)/r_{i,i} \rceil$ and $\Delta_i := sign(y_i' - \xi_i - r_{i,i}x_i)$.

STEP 3: (Main step) If $d_c < T_i + | y_i' - \xi_i - r_{i,i}x_i |^2$, then go to STEP 4 (i.e., we are outside the sphere).

Else if $x_i \notin \mathbb{Z}_Q$ go to STEP 6 (i.e., we are inside the sphere but outside the signal set boundaries).

Else (i.e., we are inside the sphere and signal set boundaries) if $i > 1$, then {let $\xi_{i-1} := \sum_{j=i}^{m} r_{i-1,j}x_j$, $T_{i-1} := T_i + | y_i' - \xi_i - r_{i,i}x_i |^2$, $i := i - 1$, and go to STEP 2}.

Else (i=1) go to STEP 5.

STEP 4: If $i = m$, terminate, else set $i := i + 1$ and go to STEP 6.

STEP 5: (A valid point is found) Let $d_c := T_1 + | y_1' - \xi_1 - r_{1,1}x_1 |^2$, save $\hat{\mathbf{x}} := \mathbf{x}$. Then, let $i := i + 1$ and go to STEP 6.

STEP 6: (Schnorr-Euchner enumeration of level i) Let $x_i := x_i + \Delta_i$, $\Delta_i := -\Delta_i - sign(\Delta_i)$, and go to STEP 3.

Note that given the values $x_{i+1}, ..., x_m$, taking the ZF-DFE (zero-forcing decision-feedback equalization) on x_i avoids retesting other nodes at level i in case we fall outside the sphere. Setting $d_c = \infty$ would ensure that the first point found by the algorithm is the ZF-DFE point (or the Babai point) [43]. However, if the distance between the ZF-DFE point and the received signal is very large this choice may cause some inefficiency, especially for high dimensional lattices.

TABLE II
CCSD: ADDITIONAL CASE CONSIDERATIONS

CASE L_4	$\sum_{i=1}^{8} x_i \equiv 0 \pmod 2$
CASE L_5	$x_1 + x_2 \equiv x_5 + x_6$, $x_3 + x_4 \equiv x_7 + x_8 \pmod 2$
CASE L_6	$x_1 + x_2 \equiv x_3 + x_4 \equiv x_5 + x_6 \equiv x_7 + x_8$, $\sum_{2\mid i} x_i \equiv \sum_{2\nmid i} x_i \equiv 0 \pmod 2$

The decoding of the other three lattices in (1) also relies on this algorithm, but we need to run some additional parity checks. This simply means that in addition to the checks concerning the facts that we have to be both inside the sphere radius and inside the signal set boundaries, we also have to lie inside a given sublattice. This will be taken care of by a method we call *code controlled sphere decoding* (CCSD), that combines the algorithm above with certain case considerations. To this end, let us write the constraints on the elements c_i as *modulo* 2 *operations*. Denote by $\mathbf{x} = (x_1, x_2, ..., x_8) = (\Re c_1, \Im c_1, ..., \Re c_4, \Im c_4) \in \mathbb{R}^8$ the real vector corresponding to the channel input. Note that when exploiting these relations in the CCSD algorithm, we have to use different orderings for the basis matrices of the lattice in different cases in order to make the parity checks as simple as possible. Let us first order the basis matrices as $B_1 = M(1,0,0,0), B_2 = M(i,0,0,0), ..., B_7 = M(0,0,0,1), B_8 = M(0,0,0,i)$. Then when decoding e.g. the L_5 lattice, we reorder the basis matrices as $B_1, B_2, B_5, B_6, B_3, B_4, B_7, B_8$ in order to get the sum $c_1 + c_3$ as the sum of the first 4 components and the sum $c_2 + c_4$ as the sum of the last 4 components (cf. Proposition 2.5). The conditions for the Gaussian elements of Propositions 2.4-2.6 can clearly be translated into the following modulo 2 integer conditions, see for instance Remark 2.2. The additional parity check steps will hence be as shown in Table II above.

As the Alamouti scheme [2] has a very efficient decoding algorithm available, and our quaternionic lattices have an Alamouti-like block structure, it is natural to ask whether any of the benefits of Alamouti decoding will survive for our lattices. We shall see that the block structure allows us to decode the two blocks independently from each other. The following simple observation is the underlying geometric reason for our ability to do this.

Lemma 4.1: Let A and B be two $n \times n$ matrices with the property that the matrices A, B, A^H, B^H commute. Let $\mathbf{h} \in \mathbb{C}^{2n}$ be any (row) vector and write

$$M(A,B) = \begin{pmatrix} A & B \\ -B^H & A^H \end{pmatrix}.$$

Then the vectors $\mathbf{h}M(A,0)$ and $\mathbf{h}M(0,B)$ are orthogonal to each other when we identify $\mathbb{C}^{2n}$ with $\mathbb{R}^{4n}$ and use the usual inner product of a vector space over the real numbers.

Proof: With the identification $\mathbb{C}^{2n} = \mathbb{R}^{4n}$ the real inner product is the real part of the hermitian inner product $\langle\ ,\ \rangle$ of $\mathbb{C}^{2n}$. Write the vector $\mathbf{h}$ in the block form $\mathbf{h} = (h^{(1)}, h^{(2)})$, where the blocks

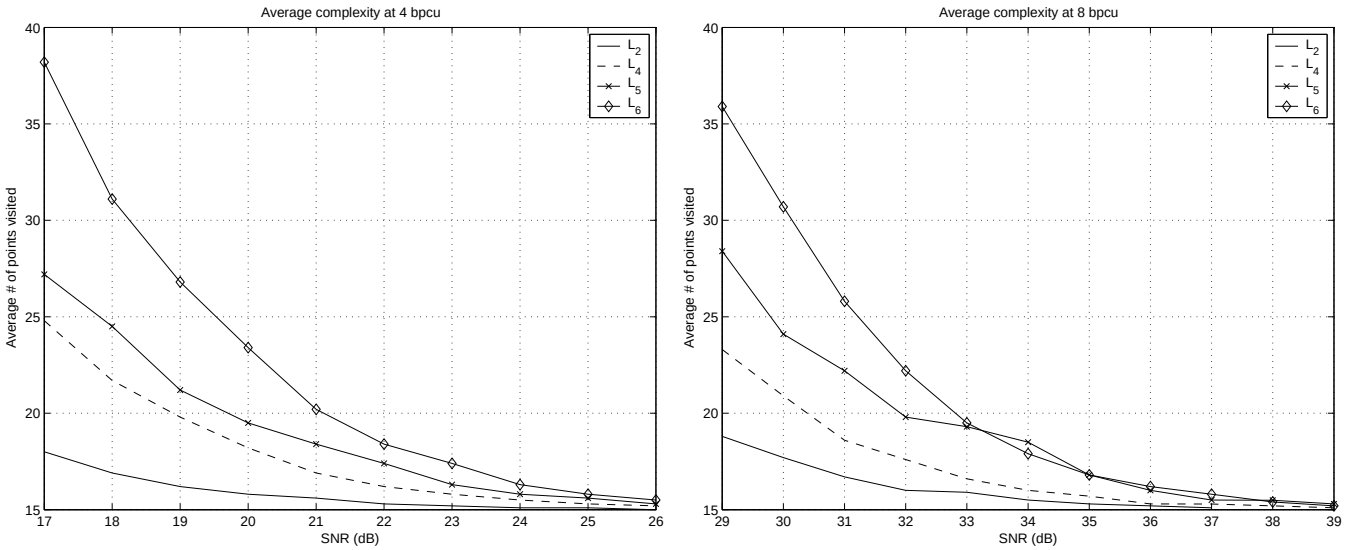


Fig. 1. Average complexity of 4 tx-antenna matrix lattices at rates (approximately) $R = 4$ and $R = 8$ bpcu.

$h^{(j)}, j = 1, 2$, are (row) vectors in $\mathbb{C}^n$. Then we can compute

$$\begin{aligned} & \langle \mathbf{h}M(A,0), \mathbf{h}M(0,B) \rangle \\ = \; & \langle \mathbf{h}M(A,0)M(0,B)^H, \mathbf{h} \rangle \\ = \; & \langle \mathbf{h}M(A,0)M(0,-B), \mathbf{h} \rangle \\ = \; & \langle \mathbf{h}M(0,-AB), \mathbf{h} \rangle \\ = \; & \langle h^{(2)}A^H B^H, h^{(1)} \rangle - \langle h^{(1)}AB, h^{(2)} \rangle. \end{aligned}$$

As $\langle \mathbf{u}M, \mathbf{v} \rangle = \langle \mathbf{v}M^H, \mathbf{u} \rangle^*$ for all vectors $\mathbf{u}, \mathbf{v}$ and matrices M, we see that the above hermitian inner product is pure imaginary. ∎

Corollary 4.2: Let A and B range over sets of $n \times n$-matrices. Let $\mathbf{h}$ and $\mathbf{r}$ be vectors in $\mathbb{C}^{2n}$. Then the Euclidean distance between $\mathbf{r}$ and $\mathbf{h}M(A,B)$ is minimized for the $A = A_0$ and $B = B_0$, when A_0 minimizes the Euclidean distance between $\mathbf{r}$ and $\mathbf{h}M(A,0)$ and B_0 minimizes the Euclidean distance between $\mathbf{r}$ and $\mathbf{h}M(0,B)$.

Proof: Write V_A (resp. V_B) for the real vector space spanned by the vectors $\mathbf{h}M(A,0)$ (resp. $\mathbf{h}M(0,B)$). These subspaces are orthogonal to each other in the sense of Lemma 4.1. Whence we can uniquely write $\mathbf{r} = r_A + r_B + r_\perp$, where $r_A \in V_A, r_B \in V_B$ and $r_\perp$ is in the (real) orthogonal complement of the direct sum $V_A \oplus V_B$. A similar decomposition for the vector $\mathbf{h}M(A,B)$ is $\mathbf{h}M(A,B) = h_A + h_B$, where $h_A = \mathbf{h}M(A,0) \in V_A$ and $h_B = \mathbf{h}M(0,B) \in V_B$. By the Pythagorean theorem

$$|\mathbf{r} - \mathbf{h}M(A,B)|^2 = |r_A - \mathbf{h}M(A,0)|^2 + |r_B - \mathbf{h}M(0,B)|^2 + |r_\perp|^2.$$

Furthermore, here

$$|r_A - \mathbf{h}M(A,0)|^2 = |\mathbf{r} - \mathbf{h}M(A,0)|^2 - |r_B|^2 - |r_\perp|^2,$$

so the quantities $|r_A - \mathbf{h}M(A,0)|^2$ and $|\mathbf{r} - \mathbf{h}M(A,0)|^2$ are minimized for the same choice of the matrix A. A similar argument applies to the B-components, so the claim follows. ∎

B. Complexity issues and collapsing lattices

The number of nodes in the search tree is used as a measure of complexity so that the implementation details or the physical environment do not affect it. We have analyzed many different kinds of situations concerning the change of complexity of the sphere decoder when moving in (1) from right to left.

In Fig. 1 we have plotted the average number of points visited by the algorithm in different cases at the rates approximately 4 and 8 bpcu. The SNR regions cover the block error rates between $\approx 10\% - 0.01\%$. As can be seen, in the low SNR end, the difference in complexity between the different lattices is clear but evens out when the SNR increases. For the sublattices L_4, L_5, and L_6 the algorithm visits $1.1 - 2.1$ times as many points as for the base lattice L_2. In the larger SNR end, the performance is fairly similar for all the lattices. E.g. at 4 and 8 bpcu, when all the lattices reach the bound of maximum 20 points visited, the block error rates of L_4, L_5, and L_6 are still as big as 5%, 2%, and 1% respectively.

Definition 4.1: In a MISO setting we say that a matrix lattice L of rank m *collapses at a channel realization* $\mathbf{h}$, if the receiver's version of the lattice $\mathbf{h}L$ spans a real vector space of dimension $< m$. We call the set of such channel realizations the critical set. We say that the *sensitivity* $s(L)$ (towards collapsing) of the lattice L is r, if the critical set is a union of finitely many subspaces of real dimension $\leq r$.

So we e.g. immediately see that a lattice residing in an orthogonal design will have zero sensitivity. While we have no precise results the thinking underlying the concept can be motivated as follows. When the infinite lattice collapses into a lower dimensional space, its linear structure is severely mutilated. For example the minimum Euclidean distance drops to zero — for any $\epsilon > 0$ there will be infinitely many other lattice points within a distance $< \epsilon$. Even when we restrict ourselves to a finite subset of the lattice, the coordinates of the nearby points may differ drastically. Thus even an ML-decoder will have problems, and an algorithm relying on the orderly linear structure of the lattice (like the sphere decoder) cannot work very efficiently. Similar problems are still there, when the actual channel realization $\mathbf{h}$ is close to a critical vector.

The sensitivity then enters the scene as a crude measure for the probability of this happening. It is easy to see that in a Rayleigh fading channel the probability of the channel vector $\mathbf{h}$ to be within ϵ of a critical vector behaves like $\mathcal{O}(\epsilon^{2n-s})$. Thus the lower the sensitivity, the lower the probability of the lattice becoming distorted by the channel.

We lead off by determining the sensitivity of the DAST-lattices.

Example 4.1: There exist 8-dimensional lattices [5] of 4×4

matrices of the form

$$M_{DAST} = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & -x_2 & x_3 & -x_4 \\ x_1 & x_2 & -x_3 & -x_4 \\ x_1 & -x_2 & -x_3 & x_4 \end{pmatrix}.$$

These matrices are simultaneously diagonalizable as they have common orthogonal eigenvectors $\mathbf{h}_1 = (1,1,1,1)$, $\mathbf{h}_2 = (1,-1,1,-1)$, $\mathbf{h}_3 = (1,1,-1,-1)$ and $\mathbf{h}_4 = (1,-1,-1,1)_4$. Write the channel vector in terms of this basis $\mathbf{h} = \sum_{j=1}^4 a_j \mathbf{h}_j$. If any of the coefficients vanishes, say $a_k = 0$, then the DAST-lattice collapses, because the receiver's version of the lattice will belong to the complex span of the other three eigenvectors $\mathbf{h}_j, j \neq k$. On the other hand, if all the coefficients $a_j \neq 0, j = 1,2,3,4$, this channel vector will not be critical. One way of seeing this is that applying the linear mapping determined by $\mathbf{h}_j \mapsto (1/a_j)\mathbf{h}_j$ to the receiver's lattice then recovers the original full rank lattice of vectors (x_1, x_2, x_3, x_4). Such a mapping obviously cannot affect the dimension of the space spanned by the vectors, so the lattice won't collapse.

We have shown that the sensitivity of the DAST-lattice is six.

We proceed to determine the sensitivities of the lattices L_1 of Proposition 2.2 and the ones within the nested sequence (1). Let us first consider L_1. Let

$$U = \begin{pmatrix} \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_4 \end{pmatrix}$$

be the 4×4 matrix with rows $\mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3, \mathbf{h}_4$ of the form $(1, \zeta^j, \zeta^{2j}, \zeta^{3j})$ for $j = 1, 5, 9, 13$. Recall that earlier we have used $\{1, \zeta, \zeta^2, \zeta^3\}$ as an integral basis, so the rows of U are the images of this ordered basis under the action of the Galois group G of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}(i)$. Now it happens that the matrix U is unitary (up to a constant factor) as $UU^* = 4I_4$. Let $z = c_1 + c_2\zeta + c_3\zeta^2 + c_4\zeta^3$ be an arbitrary algebraic integer of $\mathbb{Q}(\zeta)$, and $M(z) = M_L(c_1, c_2, c_3, c_4) \in L_1$ be the corresponding matrix of Proposition 2.2. According to the theory of algebraic numbers (and also trivially verified by hand) the rows of U are (left) eigenvectors of $M(z)$, and

$$UM(z)U^{-1} = \begin{pmatrix} z & 0 & 0 & 0 \\ 0 & \sigma_2(z) & 0 & 0 \\ 0 & 0 & \sigma_3(z) & 0 \\ 0 & 0 & 0 & \sigma_4(z) \end{pmatrix}$$

is a diagonal matrix with entries gotten by applying the elements of the Galois group $G = \{\sigma_1 = id, \sigma_2, \sigma_3, \sigma_4\}$ to the number z.

So all the matrices $M_L(c_1, c_2, c_3, c_4)$ are diagonalized by U. Therefore we might call the lattice L_1 'DAST-like', as it shares this property with the lattices from [5].

Proposition 4.3: The lattice L_1 has sensitivity six.

Proof: The situation is completely analogous to that of Example 4.1. The lattice L_1 will collapse, iff the channel realization belongs to any of the 4 complex vector spaces spanned by any three of the common eigenvectors. ∎

In order to study the quaternionic lattices we first observe that the 2×2-matrices A and B appearing as blocks of a matrix $M \in L_2$ all have $(1, \pm\xi)$ as their common (left) eigenvectors. The same holds for the adjoints A^*, B^* as they also appear as blocks of M^* that also happens to belong to the lattice L_2. From the proof of Proposition 2.4 we see that the matrix MM^*, $M = M(c_1, c_2, c_3, c_4)$, has eigenvalues $\alpha \pm |k|$ with respective (left) eigenvectors $(1, \pm\xi, 0, 0)$ and $(0, 0, 1, \pm\xi)$. Here $\alpha = \sum_{j=1}^4 |c_j|^2$ and $k = -ic_1c_2^* + c_2c_1^* - ic_3c_4^* + c_4c_3^*$. We make this more precise before we determine the sensitivity of the quaternionic lattices.

There is a connection between our MISO-code and the multi-block codes introduced by Belfiore in [45] and Lu in [44] that can be best explained with the notation of the present section. Consider the unitary matrix with the above basis vectors as columns

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ \xi & -\xi & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & \xi & -\xi \end{pmatrix}.$$

If we conjugate the matrices of the algebra $\mathbf{H}$ by U we get matrices of the form

$$\begin{pmatrix} x_1 & -x_2^* & 0 & 0 \\ x_2 & x_1^* & 0 & 0 \\ 0 & 0 & \tau(x_1) & -\tau(x_2) \\ 0 & 0 & \tau(x_2) & \tau(x_1)^* \end{pmatrix},$$

where the elements x_1, x_2 belong to the field $\mathbb{Q}(\xi) = \mathbb{Q}(i, \sqrt{2})$, and $\tau : \mathbb{Q}(\xi) \to \mathbb{Q}(\xi)$ is the automorphism determined by $\tau(i) = i$, $\tau(\sqrt{2}) = -\sqrt{2}$. Thus we see that our MISO-code is unitarily equivalent to a multi-block code with a structure similar to [44] — only our center is smaller.

The upshot here, as well as in [45], [44], and in the icosian construction from [38] is that while the individual diagonal blocks may have arbitrarily small determinants, when we use them together with their algebraic conjugates, the diagonal blocks together conspire to give a non-vanishing determinant. This is because the algebraic conjugates of small numbers are necessarily just large enough to compensate as the algebraic norms are known to be integers.

Another benefit enjoyed by our matrix representation of the algebra $\mathbf{H}$ over the above multi-block representation is that the signal constellation is better behaved. Surely the simple QAM-constellation of our matrices is to be preferred over the linear combinations of two rotated QAM-symbols of the multi-block representation.

This feature clearly begs to be generalized to a MIMO-setting. One such construction is the previously mentioned icosian construction of Liu & Calderbank [38], where they managed to add a multiplexing gain of 2 to a similar multi-block representation of the icosians. It turned out that the question of how to best do this in the spirit of the present article is somewhat delicate. The resulting codes will necessarily be asymmetric MIMO-codes, and we refer the reader to [46].

We return to the sensitivity of the quaternionic lattices. The following result is now easy to verify

Proposition 4.4: Let V_+ (resp. V_-) be the complex subspace of $\mathbb{C}^4$ generated by the vectors $(1, \xi, 0, 0)$ and $(0, 0, 1, \xi)$ (resp. by $(1, -\xi, 0, 0)$ and $(0, 0, 1, -\xi)$). The subspaces V_+ and V_- are orthogonal complements of each other in $\mathbb{C}^4$, so any channel vector can be uniquely written as

$$\mathbf{h} = \mathbf{h}_+ + \mathbf{h}_-,$$

where $\mathbf{h}_\pm \in V_\pm$ respectively. If $\mathbf{h}$ belongs to one of the subspaces V_+, V_-, the lattice $\mathbf{h}L_2$ collapses. Otherwise the lattice L_2 does not collapse. In particular the sensitivity of the lattices L_2, L_3, L_4, L_5, L_6 is four. ∎

Our simulations, indeed, show that the complexity of a sphere decoder increases sharply, when we approach the critical set. A comparison between the lattices L_1 and L_2 does not show a dramatic difference between the average complexities of a sphere decoder, but the difference becomes very apparent, when studying the high-complexity tails of the complexity distribution.

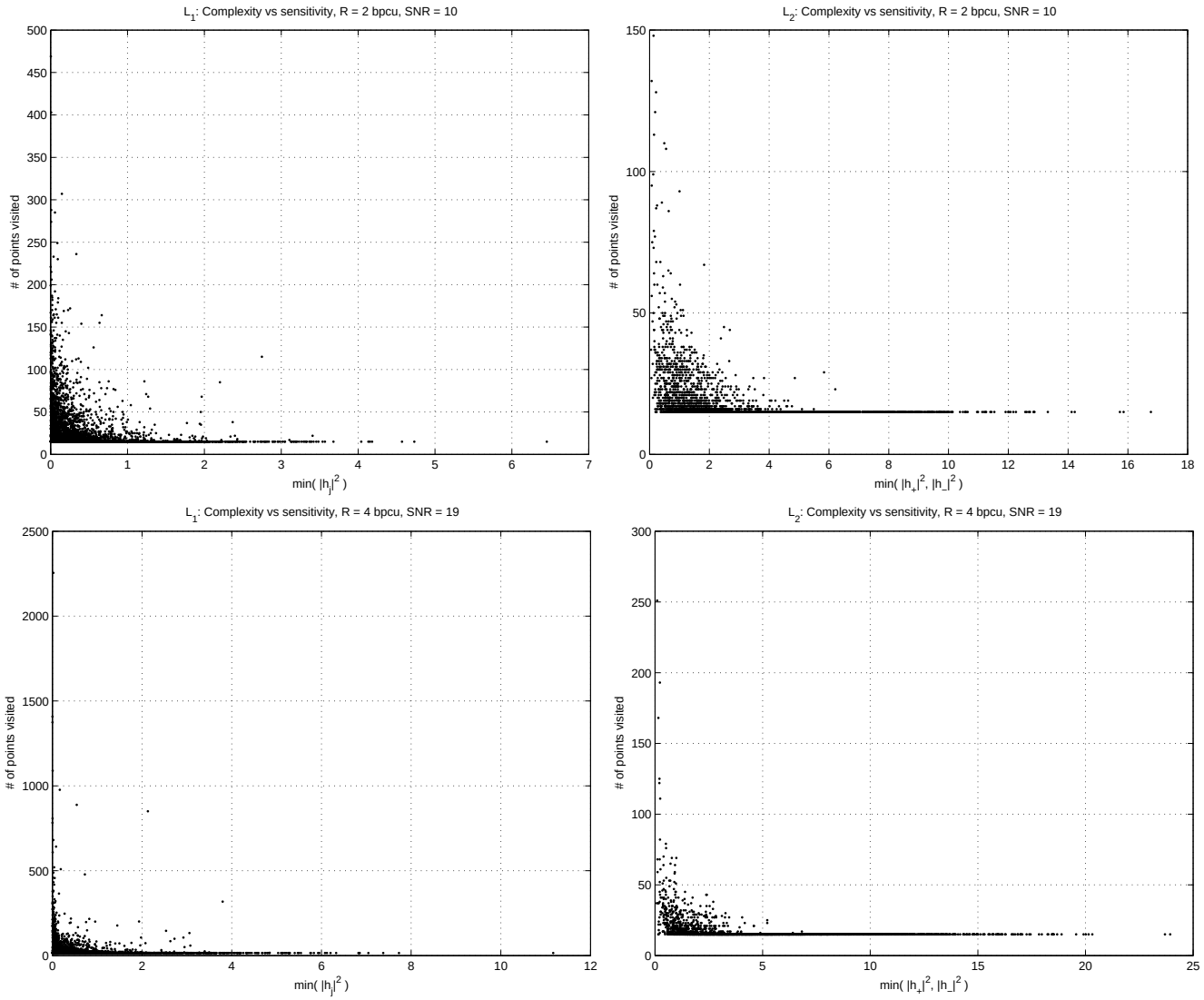


Fig. 2. The impact of sensitivity on complexity, L_1 ($\approx L_{DAST}$) vs L_2.

In Fig. 2 we have plotted the complexity distribution of 5000 transmissions for different data rates. On the horizontal axis the quantity $\min(\ |\mathbf{h}_i|^2\ )$ (resp. $\min(\ |\mathbf{h}_+|^2, |\mathbf{h}_-|^2\ )$) describes how close the lattice L_1 (resp. L_2) is to the situation where it would collapse. That is, how close to zero the minimum of the components $\mathbf{h}_i \in V_i,\ i = 1,2,3,4$, (resp. $\mathbf{h}_\pm \in V_\pm$) gets (cf. Remark 4.3 and Proposition 4.4). For both L_1 and L_2 the figure shows that the smaller the quantity, the higher the complexity. We can also conclude that the lattice L_1 nearly collapses a lot more often than the lattice L_2. In addition, the number of points visited by the sphere decoding algorithm is much higher for L_1 than for L_2. These are phenomena caused by the higher sensitivity of L_1. In Fig. 3 the scaled impact of sensitivity is depicted.

Note that as L_{DAST} has the same sensitivity as L_1, we can equally well analyze the behavior of the DAST lattice on the basis of Fig. 2 and Fig. 3.

V. Energy considerations and simulations

As a summary of Propositions 2.2–2.6 we get the following.

Proposition 5.1: (1) The lattice L_2 is isometric to the rectangular lattice $\mathbb{Z}^8$ and has a minimum determinant equal to 1.

(2) The lattice L_4 isometric to D_8 is an index two sublattice of L_2 and has a minimum determinant equal to 4.

(3) The lattice L_5 isometric to $D_4 \perp D_4$ is an index four sublattice of L_2 and has a minimum determinant equal to 16.

(4) The lattice L_6 isometric to E_8 is an index 16 sublattice of L_2 and has a minimum determinant equal to 64. ■

In order to compare these lattices we scale them to the same minimum determinant. When a real scaling factor ρ is used the minimum determinant is multiplied by ρ^2. As all the lattices have rank 8, the fundamental volume is then multiplied by ρ^8. Let us choose the units so that the fundamental volume of L_2 is $m(L_2) = 1$. Then after scaling $m(L_4) = 1/2$, $m(L_5) = 1/4$, and $m(L_6) = 1/4$. As the density of a lattice is inversely proportional to the fundamental volume, we thus expect the codes constructed within e.g. the lattices L_4 and L_6 to outperform the codes of the same size within L_2.

The exact average transmission power data in Fig. 4 is computed as follows. Given the size K of the code we choose a random set of K shortest vectors from each lattice. The average energy of the code

$$E_{av} = \frac{\sum_{x \in \mathcal{C}} \|x\|^2}{K}$$

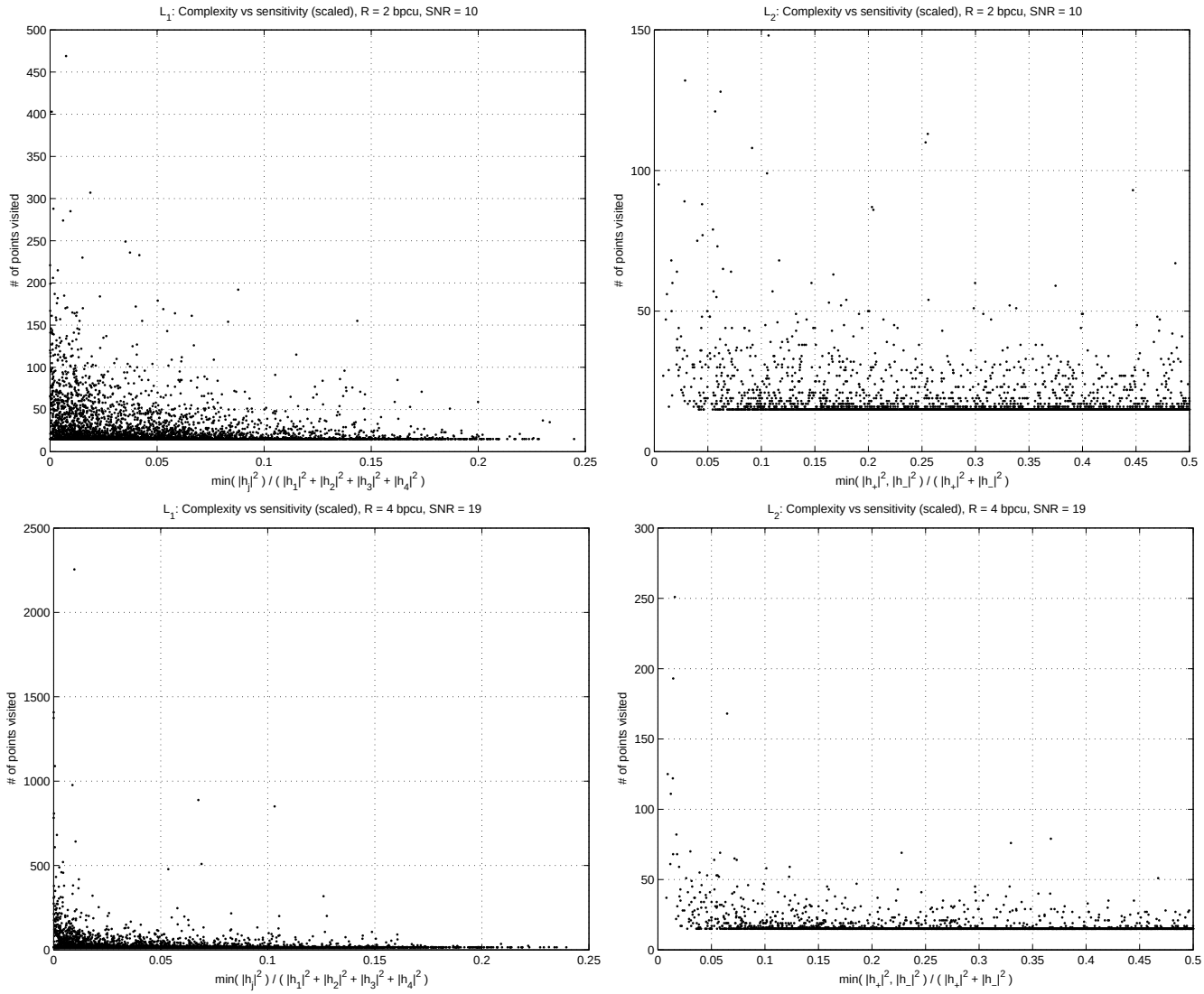


Fig. 3. The scaled impact of sensitivity on complexity, L_1 ($\approx L_{DAST}$) vs L_2.

is then computed with the aid of theta functions [31]. All the lattices were normalized to have minimum determinant equal to 1. When using the matrices $M(c_1, c_2, c_3, c_4)$ of Proposition 2.1, in some cases we are better off selecting the input vectors (c_1, c_2, c_3, c_4) from the coset $\frac{1}{2}(1+i, 1+i, 1+i, 1+i) + \mathcal{G}^4$ instead of letting them range over $\mathcal{G}^4$. Obviously such a translation does not change the minimum determinant of the code, but it sometimes results in significant energy savings. E.g. to get a code of size 256 it is clearly desirable to let the coefficients c_1, c_2, c_3, c_4 range over the QPSK-alphabet.

Fig. 5 shows the block error rates of the various competing lattice codes at the rates approximately 2, 4, 6, and 8 bpcu, i.e. all the codes contain roughly $2^8, 2^{16}, 2^{24}$ or 2^{32} matrices respectively. For the lattices L_1, L_2, L_{DAST}, and L_{ABBA} [20] this simply amounted to letting the coefficients c_1, c_2, c_3, c_4 take all the values in a QPSK-alphabet. Therefore, it would have been easy to obtain bit error rates as well. For the lattices L_4, L_5, L_6 the rate is not exact, see (10) below and the preceding explanation. Of course also the exact rate equal to a power of two could be achieved by just choosing a more or less random set of shortest lattice vectors. As there is no natural way to assign bit patterns to vectors of D_8, $D_4 \perp D_4$ or E_8, we chose to show the block error rates instead of the bit error rates.

The simulations were set up, here, so that the 95 per cent reliability range amounts to a relative error of about 3 per cent at the low SNR end and to about 10 per cent at the high SNR end (or to about 4000 and 400 error events respectively). One receiver was used for all the lattices.

When moving left in (1) the minimum determinant increaces while the BLER decreases at the same time. However, the other side of the coin is that improvements in the BLER performance cause a slightly more complex decoding process by increasing the number of points visited in the search tree. Still after this increasement, even the lattice L_6 admits a fairly low average complexity as compared to the lattices L_1 and L_{DAST} due to its lower sensitivity. In part of the pictures in Fig. 5, the order of the curves seems not to respect the above mentioned order, but this only happens because the rates are not exactly the same for all the lattices. E.g. at the rate ≈ 4 bpcu, the exact rates for L_2, L_4, L_5, and L_6 are $4, 3.75, 4.14$, and 4.17 bpcu respectively. Consequently, the lattice L_4 seems to perform better than what it actually does. Let us shortly explain how these rates follow: when picking the elements $x_1, ..., x_8$ from the set $\mathbb{Z}_Q$ (cf. Section IV (5) and the discussion after Algorithm II), the size of the code within the lattice L_i, $i = 2, 4, 5, 6$, will be $\frac{Q^8}{[L_2 : L_i]} =$

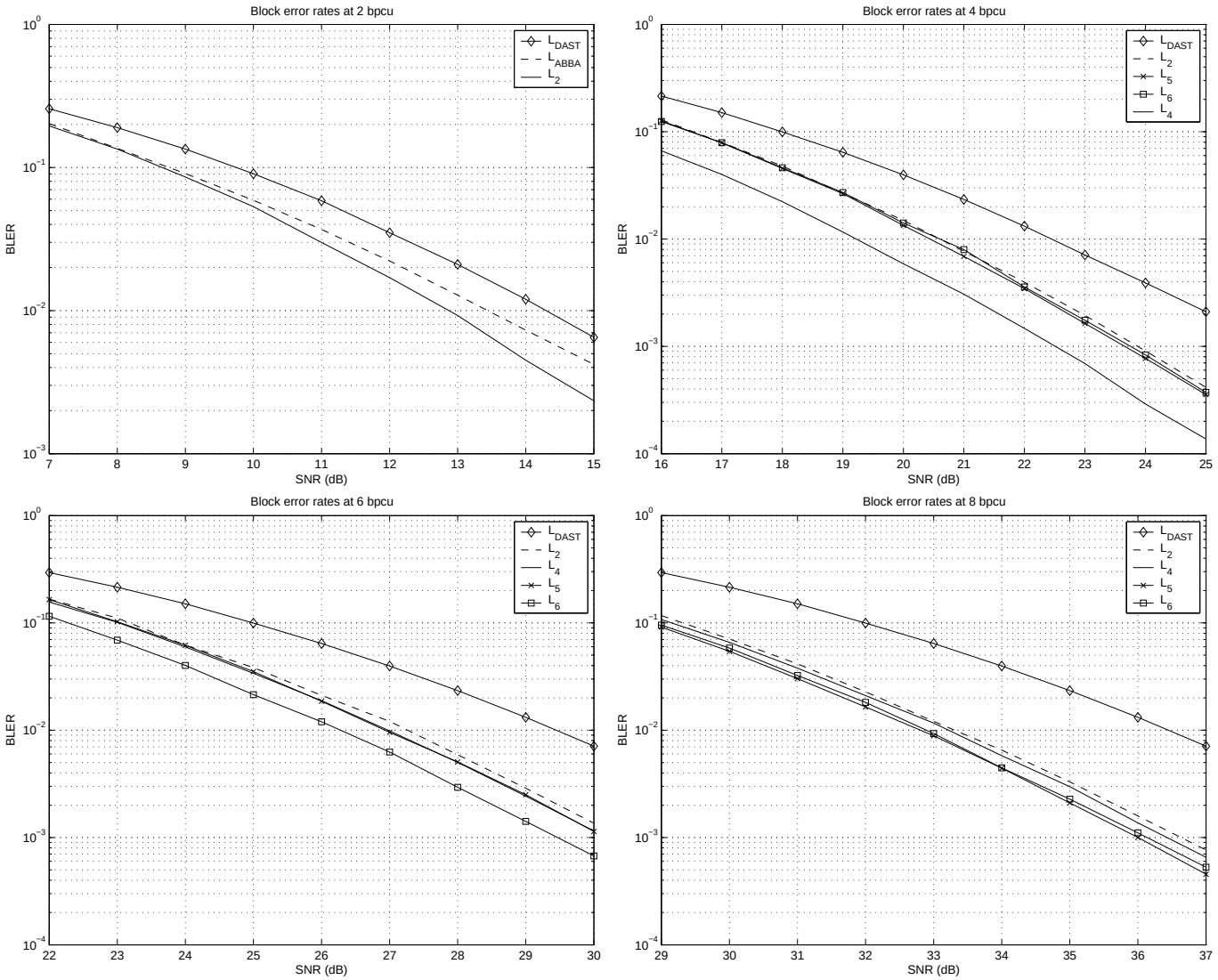


Fig. 5. Block error rates of 4 tx-antenna lattices at approximately 2.0, 4.0, 6.0, and 8.0 bpcu with one receiver.

$2^{\log \frac{Q^8}{[L_2:L_i]}}$, where $[L_2 : L_i]$ is the index of the sublattice L_i inside L_2 (cf. Proposition 5.1). Hence, the data rate in bits per channel use can be computed as

$$R = \frac{\log \frac{Q^8}{[L_2:L_i]}}{4}. \tag{10}$$

Now, for instance, to get as close to the rate $R = 4$ bpcu as possible, we have to choose $Q = 4, Q = 4, Q = 5$, and $Q = 6$ for the lattices L_2, L_4, L_5, and L_6 respectively. By substituting Q and the sublattice index in question to (10) we obtain the above rates.

Simulations at the rate 6 bpcu with one receiver show that the lattice L_6 wins by approximately 1 dB over the lattice L_2 and by at least 2.5 dB over L_{DAST}. At the rate 2 bpcu, the rotated ABBA lattice L_{ABBA} is already beaten by the L_2 lattice by a fraction of a dB. The difference between L_2 and L_{DAST} is even clearer: L_2 gains $1 - 2$ dB over L_{DAST}, depending on the SNR. At all data rates the lattice L_6 outperforms all the other lattices.

Prompted by the question of one of the reviewers, we make the following remark in case that the reader is familiar with the Icosian code [38] and ponders over whether and how it relates to the codes presented in this paper.

Remark 5.1: The Icosian lattice $L_{ICOSIAN}$ presented in [38] takes use of the Icosian ring (cf. Remark 3.6) and has a similar looking structure to the Golden code [11], where the matrix elements are replaced with Icosian Alamouti blocks

$$A = A(a_1, a_2, a_3, a_4) = \begin{pmatrix} a_1 + a_2 i & -a_3 + a_4 i \\ a_3 + a_4 i & a_1 - a_2 i \end{pmatrix}$$

and $B = B(b_1, b_2, b_3, b_4)$ respectively:

$$L_{ICOSIAN} = \left\{ \begin{pmatrix} A & K\overline{B} \\ B & \overline{A} \end{pmatrix} \;\middle|\; a_i, b_i \in \mathbb{Z}[(1+\sqrt{5})/2] \; \forall i \right\},$$

where $\overline{A}$ denotes the algebraic conjugate of A with respect to the mapping $\sqrt{5} \mapsto -\sqrt{5}$ and

$$K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

A code within this lattice is called *Icosian code*. Note that Jafarkhani's quasi-orthogonal code [30] in the simulations of [38] is exactly our base lattice L_2.

First of all, note that the Icosian code has code rate two, as the lattice is 16-dimensional over the reals. Hence, in order to enable

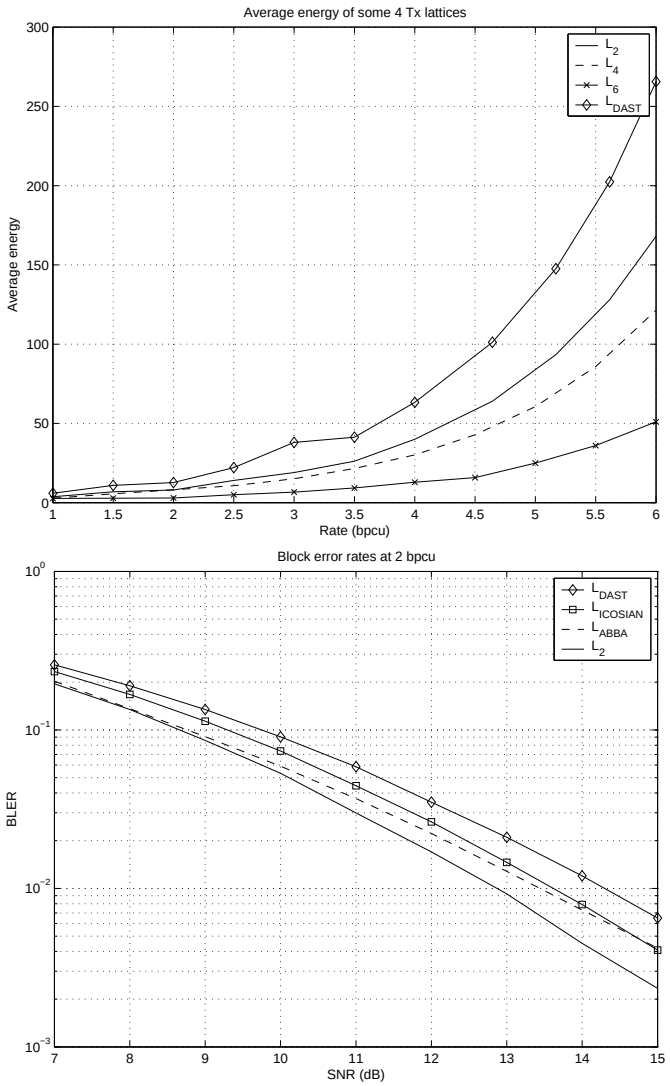


Fig. 4. Average energy (top) and block error rates of 4 Tx-antenna lattices at 2 bpcu with one receiver (bottom).

efficient linear decoding, at least two antennas are required at the receiving end. Taking this into consideration, there is no good way to make fair comparison between the Icosian lattice and the 8-dimensional lattices proposed in this paper. If the application at hand allows us to use one receiving antenna only, we either have to puncture $L_{ICOSIAN}$ (e.g. by setting $B = 0$) which will cause it to lose its benefits, or, we need to perform complex decoding process (e.g. a sphere decoder cannot be used).

However, if we still want to compare these codes with two receivers, our codes will of course lose due to the lower code rate as they are designed for MISO use only. Similar comparison could be done e.g. with the 4×4 Perfect code [11] and the Icosian code resulting to the loss of the Icosian code due to its lower rate (two vs. four). When using one receiver for the Icosian code by punctring the block B, it will lose to L_2 by 0.5-1 dB at 2 bpcu depending on the SNR as depicted in Figure 4. But, as noted above, in this way $L_{ICOSIAN}$ will of course lose its benefits (as we are not really using the whole Icosian ring) so this is not a comparison on which we should put too much value.

To conclude, the codes in this paper and the Icosian code are targeted into different types of applications: the first ones are aimed for systems with one receiving antenna, whereas the Icosian code naturally fits into systems with two receiving antennas.

VI. Diversity-multiplexing tradeoff analysis

This section contains the DMT analysis of the MISO codes constructed in this paper. We denote by n_t (resp. n_r) the number of transmitting (resp. receiving) antennas. For the rest of the notation, see [21].

Let us first consider the number field construction. Denote (cf. Proposition 2.2)

$$L_1 \;=\; \left\{ \begin{pmatrix} c_1 & ic_4 & ic_3 & ic_2 \\ c_2 & c_1 & ic_4 & ic_3 \\ c_3 & c_2 & c_1 & ic_4 \\ c_4 & c_3 & c_2 & c_1 \end{pmatrix}, c_i \in \mathcal{A} \right\},$$

where $\mathcal{A} \subset \mathbb{Z}[i]$ is some constellation set. This code is for the MISO system with $n_t = 4$ transmit and $n_r = 1$ receive antennas. Given the transmit code matrix $X \in L_1$, the received signal vector is

$$\underline{y}^T \;=\; \theta \underline{h}^T X + \underline{n}^T,$$

where $\underline{h} \sim \mathbb{CN}(\underline{0}, I_4)$.

Let r be the desired multiplexing gain; then we need

$$|L_1| \;\doteq\; \mathsf{SNR}^{4r} \;\doteq\; |\mathcal{A}|^4$$

and the above in turn gives

$$|\mathcal{A}| \;\doteq\; \mathsf{SNR}^{r}. \tag{11}$$

Hence we see for every $c_i \in \mathcal{A}$

$$\|c_i\|^2 \;\dot{\leq}\; \mathsf{SNR}^{r} \tag{12}$$

and

$$\theta^2 \;\doteq\; \mathsf{SNR}^{1-r}. \tag{13}$$

Let $\lambda := \|\underline{h}\|_F^2 = \mathsf{SNR}^{-\alpha}$ and let $\delta_1 \geq \cdots \geq \delta_4$ be the ordered eigenvalues of $XX^\dagger$; then the random Euclidean distance d_E is lower bounded by

$$d_E^2 \geq \theta^2 \lambda \delta_4 \doteq \frac{\theta^2 \lambda}{\prod_{i=1}^3 \delta_i} \;\dot{\geq}\; \mathsf{SNR}^{E_{L_1}} \tag{14}$$

where

$$E_{L_1} \;=\; 1 - r - \alpha - 3r = 1 - 4r - \alpha. \tag{15}$$

Now the DMT of this code is given by

$$d_{L_1}(r) \;\geq\; \inf_{E_{L_1} < 0} 4\alpha \;=\; 4(1-4r), \quad \text{for } 0 \leq r \leq \frac{1}{4}, \tag{16}$$

while the optimal tradeoff in this channel is actually

$$d^*(r) \;=\; 4(1-r) \quad \text{for } 0 \leq r \leq 1. \tag{17}$$

The quaternionic construction is

$$L_2 \;=\; \left\{ \begin{pmatrix} c_1 & ic_2 & -c_3^* & -c_4^* \\ c_2 & c_1 & ic_4^* & -c_3^* \\ c_3 & ic_4 & c_1^* & c_2^* \\ c_4 & c_3 & -ic_2^* & c_1^* \end{pmatrix}, c_i \in \mathcal{A} \right\}.$$

First of all, as pointed out in the proof of Proposition 2.4, the matrix $M \in L_2$ is of the following form:

$$M \;=\; \begin{pmatrix} A & -B^H \\ B & A^H \end{pmatrix}$$

and

$$MM^H = \begin{pmatrix} AA^H + B^HB & \mathbf{0} \\ \mathbf{0} & A^HA + BB^H \end{pmatrix} = \begin{pmatrix} AA^H + BB^H & \mathbf{0} \\ \mathbf{0} & AA^H + BB^H \end{pmatrix}$$

since $AB = BA$. Thus the ordered eigenvalues of MM^H satisfy $\delta_1 = \delta_2 \geq \delta_3 = \delta_4$ and in particular, $\delta_1 \geq \delta_3$ are the ordered eigenvalues of $AA^H + BB^H$. Secondly, note that MM^H satisfies the non-vanishing determinant property, and so does the matrix $AA^H + BB^H$. Now the bound for the random Euclidean distance is

$$d_E^2 \ \geq \ \theta^2\lambda\delta_4 \ \doteq \ \frac{\theta^2\lambda}{\delta_3} \dot{\geq} \mathsf{SNR}^{E_{L_2}}, \tag{18}$$

where

$$E_{L_2} \ = \ 1 - r - \alpha - r = 1 - 2r - \alpha. \tag{19}$$

Now the DMT of this code is given by

$$d_{L_2}(r) \ \geq \ \inf_{E_{L_2}<0} 4\alpha \ = \ 4(1-2r), \quad \text{for } 0 \leq r \leq \frac{1}{2}. \tag{20}$$

The same of course also holds for codes within the sublattices $L_4, L_5, L_6 \subseteq L_2$.

Remark 6.1: While our codes are not DMT optimal, it has to be noticed that without using a full-rate code the DMT cannot be achieved. Hence, if one wishes to enable efficient decoding process with one receiving antenna only (see the remark below), sacrifices in terms of the DMT have to be made. However, our quaternionic lattices L_2, L_4, L_5, L_6 admit higher DMT as e.g. the DAST lattice, as the DMT of the DAST lattice coincides with that of L_1.

Remark 6.2: One might ponder why not use e.g. the full-rate CDA based codes (cf. [6], [11]) as they are DMT optimal provided that they have non-vanishing determinant. The answer to this is in principle the same as the one provided in Remark 5.1. We could naturally do this, but considering that we only want to use one receiving antenna it should be clear that a full-rate code cannot be efficiently used. Indeed, using a full-rate code would destroy the lattice structure and cause exponential complexity at the receiver. To enable efficient decoding with one receiver we have to limit ourselves to rate-one codes, which exactly we have done in this paper. We want the reader to note that full-rate codes (e.g. the perfect codes [11]) are optimally suited for systems with $n_t = n_r > 1$, hence inapplicable to the purposes of this paper where we have $n_t = 4$ and $n_r = 1$.

VII. Conclusions and suggestions for further research

In this paper, we have presented new constructions of rate-one, full-diversity, and energy efficient 4×4 space-time codes with non-vanishing determinant by using the theory of rings of algebraic integers and their counterparts within the division rings of Lipschitz' and Hurwitz' integral quaternions. A comfortable, purely number theoretic way to improve space-time lattice constellations was introduced. The use of ideals provided us with denser lattices and an easy way to present the exact proofs for the minimum determinants. The constructions can be extended also to a larger number of transmit antennas, and they nicely fit with the popular Q^2-QAM and QPSK modulation alphabets. The idea of finding denser sublattices within a given division algebra was also generalized to a MIMO case with arbitrary number of Tx antennas by using the theory of cyclic division algebras and, as a novel method, their maximal orders. This is encouraging as the CDA based square ST constructions with NVD are known to achieve the DMT. We have also shown that the explicit constructions in this paper all have a simple decoding method based on sphere decoding. Related to the decoding complexity, the notion of sensitivity was introduced for the first time in this paper. The experimental results have given evidence about the relevance of this new notion.

Comparisons with the four antenna DAST block code have shown that our codes provide lower energy and block error rates due to their good minimum determinant, i.e. high density and lower sensitivity. At the moment, we are searching for well-performing MIMO codes arising from the theory of crossed product algebras and maximal orders of cyclic division algebras. We have noticed that also the discriminant of a maximal order plays an important role in code design. It is desirable to choose cyclic division algebras for which the discriminant of a maximal order is as small as possible [33]. By now, we are able to construct an explicit cyclic division algebra of an arbitrary index over $\mathbb{Q}(i)$ (or $\mathbb{Q}(\omega)$) that has a maximal order with minimal discriminant. Despite the fact that we have not yet fully analyzed the practical performance of codes arising from these constructions, the preliminary results have been very promising. Further details on this and on the algorithmic properties of maximal orders (see also [47]-[49]) will be given in a forthcoming paper [33].

VIII. Acknowledgments

The authors are grateful to graduate student Miia Mäki for partly implementing the sphere decoder that was used for the simulations. A thank-you is also due to anonymous reviewers for their insightful comments that greatly improved the quality of this paper.

C. Hollanti was supported in part by the Nokia Foundation, the Foundation of Technical Development, and the Foundation of the Rolf Nevanlinna Institute, Finland.

References

[1] J.-C. Guey, M. P. Fitz, M. R. Bell, and W. Y. Kuo, "Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels", in *Proc. IEEE Vehicular Technology Conf.*, 1996, pp. 136–140. Also in *IEEE Trans. Commun.*, vol. 47, pp. 527–537, April 1999.

[2] S. M. Alamouti, "A simple transmit diversity technique for wireless communication", *IEEE J. on Select. Areas in Commun.*, vol. 16, pp. 1451–1458, October 1998.

[3] J. Hiltunen, C. Hollanti, and J. Lahtonen, "Four antenna space-time lattice constellations from division algebras", in *Proc. IEEE ISIT 2004*, p. 338., Chicago, June 27 - July 2, 2004.

[4] J. Hiltunen, C. Hollanti, and J. Lahtonen, "Dense full-diversity matrix lattices for four antenna MISO channel", in *Proc. IEEE ISIT 2005*, pp. 1290–1294, Adelaide, September 4 - 9, 2005.

[5] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes", *IEEE Trans. Inf. Theory*, vol. 48, pp. 628–636, March 2002.

[6] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras", *IEEE Trans. Inf. Theory*, vol. 49, pp. 2596–2616, October 2003.

[7] J.-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding", in *Proc. ITW 2003*, Paris, France, March 31 - April 4, 2003.

[8] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "The Golden code: A 2x2 full-rate space-time code with non-vanishing determinants", in *Proc. IEEE ISIT 2004*, p. 308, Chicago, June 27 - July 2, 2004.

[9] H. Yao and G. W. Wornell, "Achieving the full MIMO diversity-multiplexing frontier with rotation-based space-time codes", in *Proc. Allerton Conf. Commun., contr., and Computing*, Oct. 2003.

[10] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "Algebraic 3x3, 4x4 and 6x6 space-time codes with non-vanishing determinants", in *Proc. IEEE ISITA 2004*, Parma, Italy, October 10 - 13, 2004.

[11] J.-C. Belfiore, F. Oggier, G. Rekaya, and E. Viterbo, "Perfect space-time block codes", *IEEE Trans. Inf. Theory*, vol. 52, pp. 3885–3902, September 2006.

[12] Kiran. T and B. S. Rajan, "STBC-schemes with non-vanishing determinant for certain number of transmit antennas", *IEEE Trans. Inf. Theory*, vol. 51, pp. 2984–2992, August 2005.

[13] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman "STBCs using capacity achieving designs from crossed-product division algebras", in *Proc. IEEE ICC 2004*, pp. 827–831, Paris, France, 20-24 June 2004.

[14] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman, "Information-lossless STBCs from crossed-product algebras", *IEEE Trans. Inf. Theory*, vol. 52, pp. 3913–3935, September 2006.
[15] P. Elia, K. R. Kumar, P. V. Kumar, H.-F. Lu, and S. A. Pawar, "Explicit space-time codes achieving the diversity-multiplexing gain tradeoff", *IEEE Trans. Inf. Theory*, vol. 52, pp. 3869–3884, September 2006.
[16] G. Wang and X.-G. Xia, "On optimal multi-layer cyclotomic space-time code designs", *IEEE Trans. Inf. Theory*, vol. 51, pp. 1102–1135, March 2005.
[17] M. O. Damen, H. E. Gamal, and N. C. Beaulieu, "Linear threaded algebraic space-time constellations", *IEEE Trans. Inf. Theory*, vol. 49, pp. 2372–2388, October 2003.
[18] M. O. Damen and H. E. Gamal, "Universal space-time coding", *IEEE Trans. Inf. Theory*, vol. 49, pp. 1097–1119, May 2003.
[19] P. Dayal and K. Varanasi, "Algebraic space-time codes with full diversity and low peak-to-mean power ratio", in *Proc. Commun. Th. Symp., IEEE GLOBECOM*, San Francisco, CA, Dec. 2003.
[20] O. Tirkkonen, A. Boariu, and A. Hottinen, "Minimal non-orthogonality rate 1 space-time block code for 3+ TX antennas", in *Proc. IEEE ISSSTA*, vol. 2, pp. 429–432, September 2000.
[21] L. Zheng and D. Tse, "Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels", *IEEE Trans. Inf. Theory*, vol. 49, pp. 1073–1096, May 2003.
[22] V. Tarokh, N. Seshadri, and A.R. Calderbank, "Space-time codes for high data rate wireless communications: Performance criterion and code construction", *IEEE Transactions on Information Theory*, vol. 44, pp. 744–765, March 1998.
[23] I. Stewart and D. Tall, *Algebraic Number Theory*, Chapman and Hall, London 1979.
[24] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs", *IEEE Transactions on Information Theory*, vol. 45, pp. 1456–1467, July 1999.
[25] O. Tirkkonen, "Optimizing space-time block codes by constellation rotations", in *Proceedings Finnish Wireless Communications Workshop FWCW'01*, pp. 59–60, October 2001.
[26] A. Hottinen and O. Tirkkonen, "Square-matrix embeddable space-time Block codes for complex signal constellations", *IEEE Trans. Inf. Theory*, vol. 48 (2), pp. 384–395, February 2002.
[27] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good lattice constellations for both rayleigh fading and gaussian channels", *IEEE Trans. Inf. Theory*, vol. 42, pp. 502–518, March 1996.
[28] B. Hassibi, B. M. Hochwald, A. Shokrollahi, and W. Sweldens, "Representation theory for high-rate multiple-antenna code design", *IEEE Trans. Inf. Theory*, vol. 47, pp. 2335–2364, September 2001.
[29] F. E. Oggier and E. Viterbo, "Algebraic number theory and code design for Rayleigh fading channels", *Foundations and Trends in Communications and Information Theory*, December 2004.
[30] H. Jafarkhani, "A quasi-orthogonal space-time block code", *IEEE WCNC*, vol. 1, pp. 42–45, September 2000.
[31] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Grundlehren der Mathematischen Wissenschaften #290, Springer-Verlag, New York 1988.
[32] D. Allcock, "New complex- and quaternion-hyperbolic reflection groups", *Duke Mathematical Journal*, vol. 103, pp. 303–333, June 2000.
[33] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, "Optimal matrix lattices for MIMO codes from division algebras", in *Proc. IEEE ISIT 2006*, pp. 783–787, Seattle, July 9 - 14, 2006. Full paper submitted to IEEE Trans. Inf. Theory, Dec. 2006. Available at http://arxiv.org/abs/cs.IT/0703052.
[34] N. Jacobson, *Basic Algebra II*, W. H. Freeman and Company, San Francisco 1980.
[35] A. A. Albert, *Structure of Algebras*, American Mathematical Society, New York City 1939.
[36] I. Reiner, *Maximal Orders*, Academic Press, London 1975.
[37] C. Hollanti and J. Lahtonen, "A new tool: Constructing STBCs from maximal orders in central simple algebras", in *Proc. IEEE ITW 2006*, pp. 322–326, Punta del Este, Uruguay, March 13-17, 2006.
[38] J. Liu and A. R. Calderbank, "The icosian code and the E_8 lattice: A new 4×4 space-time code with nonvanishing determinant", in *Proc. IEEE ISIT 2006*, Seattle, July 9 - 14, 2006.
[39] M. Pohst, "On the computation of lattice vectors of minimal length, successive minima and reduced basis with applications", *ACM SIGSAM*, vol. 15, pp. 37–44, 1981.
[40] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channel", *IEEE Transactions on Information Theory*, vol. 45, pp. 1639–1642, July 1999.
[41] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices", *IEEE Transactions on Information Theory*, vol. 48, pp. 2201–2214, August 2002.
[42] M. O. Damen, A. Chkeif, and J.-C. Belfiore, "Lattice codes decoder for space-time codes", *IEEE Commun. Lett.*, vol. 4, pp. 161–163, May 2000.
[43] M. O. Damen, H. El Gamal, and G. Caire, "On maximum-likelihood detection and the search for the closest lattice point", *IEEE Transactions on Information Theory*, vol. 49, pp. 2389–2402, October 2003.
[44] H.-f. (F.) Lu, "Explicit constructions of multi-block space-time codes that achieve the diversity-multiplexing tradeoff", in *Proc. IEEE ISIT 2006*, pp. 1149–1153, Seattle, 2006.
[45] S. Yang and J.-C. Belfiore, "Optimal space-time codes for the MIMO amplify-and-forward cooperative channel", *IEEE Trans. Inf. Theory*, vol. 53, pp. 647–663, Feb. 2007.
[46] C. Hollanti and H.-f. (F.) Lu, "Normalized minimum determinant calculation for multi-block and asymmetric space-time codes", *Applied Algebra, Algebraic Algorithms and Error Correcting Codes*, pp. 227–237, Springer-Verlag LNCS 4851, Berlin 2007.
[47] L. Rónyai, "Algorithmic properties of maximal orders in simple algebras over Q", *Computational Complexity 2*, pp. 225–243, 1992.
[48] G. Ivanyos and L. Rónyai, "On the complexity of finding maximal orders in algebras over Q", Computational Complexity 3, pp. 245–261, 1993.
[49] Web page: http://magma.maths.usyd.edu.au/magma/htmlhelp/text835.htm#8121.

Camilla Hollanti received the M.S. degree from University of Turku, Finland, in 2003 in pure mathematics, and is now working through her final year in the graduate school of Turku Centre for Computer Science to finish her doctoral degree in discrete mathematics.

Since June 2004, she has been with the Department of Mathematics, University of Turku, Finland. In 2005, she visited the Department of Algebra at Charles' University, Prague, Czech Republic, for six months. Her research is in the area of applications of algebraic number theory and class field theory in lattice space-time coding.

Hollanti is a recipient of several grants from various foundations, including the Finnish Cultural Foundation research grant in 2007 and the Finnish Academy of Science research grant in 2008. She has also won the prize for the best presentation in the EWM 2007 conference in Cambridge, UK.

Jyrki Lahtonen (M'96) received the M.S. degree from University of Turku, Turku, Finland, in 1986, and the Ph.D. degree from University of Notre Dame, Notre Dame, Indiana, U.S.A. in 1990 respectively, both in mathematics.

He was a postdoctoral research fellow at Mathematical Sciences Research Insitute, Berkeley, California in 1990. In January 1991, he joined the faculty of the Department of Mathematics at University of Turku. Since September 2006, he has held a part-time position as a visiting fellow at Nokia Research Center, Helsinki, Finland.

His research interests include sequences, finite fields and their applications into coding theory, and space-time codes.

Hsiao-feng (Francis) Lu (S'98-M'04) received the B.S. degree from Tatung University, Taipei, Taiwan, in 1993, and the M.S.E.E. and Ph.D. degrees from the University of Southern California (USC), Los Angeles, in 1999 and 2003, respectively, all in electrical engineering.

He was a postdoctoral research fellow at University of Waterloo, ON, Canada, during 2003-2004. In February 2004, he joined the faculty of the Department of Communications Engineering, National Chung-Cheng University, Chiayi, Taiwan, and was promoted to Associate Professor in August 2007. Since August 2008, he has been with the Department of Communications Engineering, National Chiao Tung University, Hsinchu, Taiwan. His research is in the area of space-time codes, MIMO systems, error correcting codes, wireless communication, optical fiber communication, and multi-user detection.

Dr. Lu is a recipient of several research awards, including the 2006 IEEE Information Society Taipei Chapter and IEEE Communications Society Taipei/Tainan Chapter Best Paper Award for Young Scholars, the 2007 Wu Da You Memorial award from Taiwan National Science Council, the 2007 IEEE Communication Society Asia Pacific Outstanding Young Researchers Award, and the 2008 Academia Sinica Research Award for Junior Research Investigators.

Publication II

Hollanti, C., Lahtonen, J., Ranto, K., and Vehkalahti, R. (2008). On the densest MIMO lattices from cyclic division algebras. *IEEE Transactions on Information Theory* (in press).

On the Densest MIMO Lattices from Cyclic Division Algebras

Camilla Hollanti, Jyrki Lahtonen, *Member, IEEE*, Kalle Ranto, and Roope Vehkalahti

***Abstract*— It is shown why the discriminant of a maximal order within a cyclic division algebra must be minimized in order to get the densest possible matrix lattices with a prescribed nonvanishing minimum determinant. Using results from class field theory, a lower bound to the minimum discriminant of a maximal order with a given center and index (= the number of Tx/Rx antennas) is derived. Also numerous examples of division algebras achieving the bound are given. For example, a matrix lattice with QAM coefficients that has 2.5 times as many codewords as the celebrated Golden code of the same minimum determinant is constructed. Also a general algorithm due to Ivanyos and Rónyai for finding maximal orders within a cyclic division algebra is described and enhancements to this algorithm are discussed. Also some general methods for finding cyclic division algebras of a prescribed index achieving the lower bound are proposed.**

***Index Terms*— Cyclic division algebras (CDAs), dense lattices, discriminants, Hasse invariants, maximal orders, multiple-input multiple-output (MIMO) channels, multiplexing, space-time block codes (STBCs).**

I. Overview

Multiple-antenna wireless communication promises very high data rates, in particular in the coherent case, where we have perfect channel state information (CSI) available at the receiver. In [1] the design criteria for such systems were developed, and further on the evolution of space-time (ST) codes took two directions: trellis codes and block codes. Our work concentrates on the latter branch. In this paper, we will be interested in the coherent and symmetric multiple input-multiple output (MIMO) case, where we have an equal number of transmit and receive antennas.

To motivate our work, we discuss certain properties of *lattices*. Below, we only give a short description, for a more detailed introduction to abstract lattices, see Section II.

A *lattice* is a discrete finitely generated free abelian subgroup Λ of a real or complex finite dimensional vector space $\mathbf{V}$, called the ambient space. In the space-time setting, a natural ambient space is the space $M_n(\mathbf{C})$ of complex $n \times n$ matrices. Due to the symmetric situation, we only consider full-rank lattices that have a basis $x_1, x_2, \ldots, x_{2n^2}$ consisting of matrices that are linearly independent over the field of real numbers. We can form a $2n^2 \times 2n^2$ matrix M having rows consisting of the real and imaginary parts of all the basis elements. It is well known that the measure, or hypervolume, $m(\Lambda)$ of the fundamental parallelotope of the lattice then equals the absolute value of $\det(M)$. Alternatively we may use the *Gram matrix*

$$G(\Lambda) = MM^T = \left(\Re tr(x_i x_j^\dagger)\right)_{1 \le i,j \le 2n^2},$$

where $x^\dagger$ indicates the complex conjugate transpose of the matrix x. The Gram matrix has a positive determinant equal to $m(\Lambda)^2$.

From the pairwise error probability (PEP) point of view [2], the performance of a space-time code is dependent on two parameters: *diversity gain* and *coding gain*. Diversity gain is the minimum of the rank of the difference matrix $X - X'$ taken over all distinct code matrices $X, X' \in \mathcal{C}$, also called the *rank* of the code $\mathcal{C}$. When $\mathcal{C}$ has a full rank, the coding gain is proportional to the determinant of $(X-X')(X-X')^\dagger$. The minimum of this determinant taken over all distinct code matrices is called the *minimum determinant* of the code $\mathcal{C}$. If it remains bounded away from zero even in the limit as the size of the constellation $\to \infty$, the ST code is said to have the *nonvanishing determinant* (NVD) property [3]. For nonzero square matrices, having a full rank coincides with being invertible.

Definition 1.1: The *data rate* R in bits per channel use is given by

$$R = \frac{1}{n}\log_2|\mathcal{C}|,$$

where $|\mathcal{C}|$ is the size of the code.

This is not to be confused with the *rate of a code design* (or code rate, in short), defined as the ratio k/n, where k is the number of information symbols k (coming from a complex signal alphabet, e.g. a QAM-alphabet) in a code matrix, and n is the decoding delay n of these symbols. If this ratio is equal to the delay (=block lengh), the code is said to have a *full rate*.

The very first space-time block code (STBC) for two transmit antennas was the *Alamouti code* [4] representing multiplication in the ring of quaternions. As the quaternions form a division algebra, such matrices must be invertible, i.e. the resulting STBC meets the rank criterion. Matrix representations of other division algebras have been proposed

This work was supported in part by the Nokia Foundation, the Foundation of Technical Development, Finland, the Foundation of the Rolf Nevanlinna Institute, Finland, and the Academy of Finland, grant #108238.

During this work, C. Hollanti and R. Vehkalahti were with the Laboratory of Discrete Mathematics for Information Technology, Turku Centre for Computer Science, Finland. Currently they are with the Department of Mathematics, FI-20014 University of Turku, Finland (e-mail: {cajoho, roiive}@utu.fi).

J. Lahtonen is with the Department of Mathematics, FI-20014 University of Turku, Finland (e-mail: lahtonen@utu.fi), and Nokia Research Center, Wireless Access Systems, FI-00045 Nokia Group, Finland (e-mail: jyrki.lahtonen@nokia.com).

During this work, K. Ranto was with the Department of Mathematics, FI-20014 University of Turku, Finland. Currently he is with the Nokia Corporation, Nokia Devices, P.O. Box 86, FI-24101 Salo, Finland (e-mail: kalle.ranto@nokia.com).

as STBCs at least in [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], and (though without explicitly saying so) in [15]. The work in [7]-[15] has concentrated on adding multiplexing gain, i.e. increasing the code rate (see Definition 1.1), and/or combining it with a good minimum determinant. It has been shown in [14] that CDA-based square ST codes with the NVD property achieve the diversity-multiplexing gain tradeoff (DMT) introduced in [16]. The codes proposed in this paper all fall into this category and are in that sense optimal. Furthermore, algebras with an imaginary quadratic field as a center yield lattices with a good minimum determinant, as the corresponding rings of integers have no short nonzero elements.

Some authors have made the assumption that the so-called linear dispersion encoding is used. Therein a fixed subset of a complex alphabet lattice (such as QAM or HEX) is chosen, and sequences of symbols from that subset are then turned into lattice points by the simple process of using them as coefficients of a fixed basis (as a module over a ring generated by the alphabet) of the actual lattice. From our point of view this approach places undue emphasis on the encoding process, so we largely ignore this aspect. Therefore questions like whether our lattices are 'information lossless' (cf. [13],[10]) are meaningless, because that concept is defined only under the assumption of linear dispersion encoding.

This change means that we often need to resort to the use of a codebook, and thus the complexity of encoding is higher. But, consequently, we are also free to do optimal spherical shaping. In other words, we choose our finite codebook to consist of shortest vectors (not necessarily all of them) of the lattice or of a coset of the lattice, and thus minimize the transmission power.

Our lattices of $n \times n$ matrices are of rank $2n^2$. This implies that if we impose a constraint on the transmission power and require that $tr(XX^\dagger) \leq P$ for all the matrices X in a codebook, then the number of signals X meeting this constraint grows like $O(P^{n^2})$ as a function of maximal transmission power P. Thus, they automatically share this property with the full-rate linear dispersion codes. Therefore, we are entitled to use Theorem 3 from [14] and conclude that, also for the maximal order codes, the NVD property implies DMT-optimality.

In this paper, yet another design criterion is brought into the playground, namely an explicit criterion for maximizing the density of the code. The field of ST coding seems to be lacking a general, precise notion for the density in the case of noncommutative structures. Normally, when studying density of the lattices, e.g. in [17], one is concerned with the relation of the squared minimum Euclidean distance $d^2(\Lambda)$ of the lattice and its relation to the fundamental volume $m(\Lambda)$. For rank N lattices, these scale by factors r^2 and r^N, respectively, when Λ is scaled by a factor r. Therefore, one often uses the ratio (also known as Hermite's parameter)

$$\gamma = \frac{d^2(\Lambda)}{m(\Lambda)^{2/N}}$$

that has the virtue of being invariant under scaling. In ST applications an appropriate density measure has the minimum squared determinant in the numerator instead of the minimum squared Euclidean distance. There are several alternative ways of normalizing the scale of a ST lattice code. One alternative is to scale the lattice to have a unit fundamental volume. This is the scaling used in e.g. [10]. It has the benefit that when unitary linear dispersion is used, then signal transmission power is the sum of the symbol powers. With this normalization one then naturally seeks to maximize the minimum determinant to minimize the PEP. Alternatively, we can normalize the lattices to have a unit minimum determinant instead. The motivation for this normalization comes from the fact that algebraic constructions produce lattices with determinants that are algebraic integers of a quadratic imaginary number field, hence ≥ 1. With this normalization, one then seeks to minimize the fundamental volume in order to be able to pack the maximum number of constellation points into a given power constrained region of the signal space, i.e. we maximize the data rate within a fixed 'power sphere'.

A third natural way of carrying out the minimum determinant vs. fundamental volume comparison of lattices would be to study the ratio

$$\gamma_{ST} = \frac{\min |\det(\Delta X \Delta X^\dagger)|^{1/n}}{m(\Lambda)^{2/2n^2}}$$

that is again invariant under scaling. Whichever normalization is adopted, the relative order of lattices will not change, so any one will do.

After a cyclic division algebra has been chosen, the next step is to choose a corresponding lattice, or what amounts to the same thing, to choose an order within the algebra. Most authors [15], [14] have gone with the so-called natural order (see Section IV for a definition). One of the points we want to emphasize in this article is to use the maximal orders instead. The idea is that one can sometimes use several cosets of the natural order without sacrificing anything in terms of the minimum determinant. So the study of maximal orders is clearly motivated by an analogy from the theory of error correcting codes: why one would use a particular code of a given minimum distance and length, if a larger code with the same parameters is available. The standard matrix representation of the natural order results in codes that have a so-called threaded layered structure [18]. When a maximal order is used, the code will then also extend 'between layers'. However, our simulations suggest that restoring the layered structure by replacing the maximal order with its smartly chosen ideal yields codes with better performance. For more details on this, see Section XII below. Earlier, we have successfully used maximal orders in a construction of some 4Tx antenna MISO lattices [5]. Maximal orders have turned out to be useful also in the design of certain asymmetric and multi-user space-time codes, more details to follow in the forthcoming papers [19] and [20].

In some cases the index of the natural order as a sublattice of a maximal order is quite large. For example in the cases of a family of cyclic algebras suggested in [11] one can theoretically increase the data rate by 1.5, 6.5 and 20.5 bits per channel use for 2, 4 and 8 antenna codes respectively. The lattice of a fully multiplexing 8Tx+8Rx antenna MIMO

code has dimension 128. The nearest vector problem in such high-dimensional lattices is used in some cryptographic applications, so it is safe to say that ML-based decoding, e.g. sphere decoding, of such lattices will have prohibitively high complexity. Thus, we emphasize that such increments of data rates are mostly theoretical in nature. These numbers, however, motivated us to look for methods for locating maximal orders. A general purpose algorithm for this task has been developed by Ivanyos and Rónyai [21]. A commercially available version of their algorithm is implemented by W. van de Graaf as part of the computer algebra system MAGMA [22]. It turned out that this general purpose algorithm was not able to handle the aforementioned algebras of index eight. To deal with these special cases we developed some enhancements to their algorithm.

Given that maximal orders provide the best codes in terms of minimum determinant vs. average power, we are left with the question: Which division algebra should we use? To continue the analogy from the theory of error-correcting codes we want to find the codes with the highest possible density. That is, with the smallest fundamental parallelotope. To that end we need a suitable tool for parameterizing the cyclic division algebras with a given center and index. Luckily, relatively deep results from class field theory provide us with the necessary tool of Hasse invariants. The measure of a fundamental parallelotope of a maximal order (that later on will be referred to as the discriminant of the division algebra) can be expressed in terms of Hasse invariants [23]. With these results at hand we then derive a lower bound to the discriminant. The proof of the lower bound is not constructive per se, but it does show that our lower bound is achievable. In the latter parts of this article we describe some techniques for constructing division algebras with a minimal discriminant.

It is worth mentioning that in [24] the authors have made a similar approach in the reduced case of commutative number fields.

While our interest in these problems is mostly theoretical, some of the densest lattices we have found also perform well in computer simulations. Our construction of the densest 2×2 matrix lattice improves upon the deservedly celebrated Golden code in block error rates by about 0.9 dB at data rates from 5 to 6 bpcu. The performance of both the rival codes can be further improved by coset optimization and this also cuts down the gap to about 0.3 dB. Observe that at the data rate of 4 bpcu we have a tie. This is easily explained by the fact that for codes of that size there is a particularly attractive choice for the coset of the Golden code — at that data rate the Golden code has spherical shaping! Our work could be viewed as a study of the further gains available, when the assumption of linear dispersion is dropped. Also as explained in [25], spherical encoding is a viable alternative to the use of a codebook when using our lattice.

This article places somewhat high demands on the reader's exposure to algebraic number theory and its machinery. Some readers may only be interested in the constructions, and with those readers in mind we have a coding theoretical main track outlined in the last paragraph of this section, so that such a reader can skip the heavy duty algebra to a large extent. On the other hand, many researchers working in this area are quite familiar with algebraic number fields. However, it would be pointless to attempt to give an overview of class field theory to even those readers. So we have adopted the policy of injecting hopefully clarifying examples into the sections, where the necessary tools and results from class field theory are presented. They form a poor substitute to a serious study of class field theory, but seek to serve the function of tying the concepts together with something the reader might already be familiar with.

The paper is organized as follows. The early sections II–V give an overview of the basic algebraic concepts and their relation to the density of MIMO-lattices. Section VI then introduces some deeper machinery and proves the general Discriminant Bound that is one of our main results. The specific instances of the discriminant bound that occur most often in practice are then collected into section VII. Section VIII, then gives the first examples of algebras achieving the discriminant bound. Then in section IX, we tackle the problem of finding maximal orders or, equivalently, of constructing the actual MIMO-lattices within the cyclic division algebras. Section X is dedicated to the study of the perfect codes in the context of our theory. The problem of locating the best CDAs is dissected in the longish section XI. We then wrap up with some simulation results and concluding remarks. The appendix contains certain results from algebraic number theory that are well known, but are not usually covered in an introductory course to the topic. They are needed in section XI are included mostly for easy reference. The appendix also contains a proof for the fact that in order to achieve the discriminant bound it is necessary to leave the domain of layered codes (that we refer to as natural orders).

A reader who does not want to spend much time on number theoretic details can follow a coding theoretical main track within the article. It begins with the introductory Sections II, IV and V. Main track reader can largely ignore the derivation of discriminant bound, but we recommend cherry-picking the most common instances of it from Section VII. After that a main track reader might just peruse the Tables III and IV from the end of Section X for numerical data pitting the perfect codes against the discriminant bound, and then finish off with Section XII.

II. Abstract lattice codes

In this section we define in more detail the *coding gain* and *normalized density* of an infinite MIMO-lattice. These measures are essential if we like to compare two MIMO-lattices.

Our take on MIMO codes is rather abstract and we define:

Definition 2.1: A MIMO code $\mathcal{C}$ is a full lattice in $M_n(\mathbf{C})$.

By *full* we mean that the lattice has a basis $x_1, x_2, \ldots, x_{2n^2}$ consisting of matrices in $M_n(\mathbf{C})$ that are linearly independent over the field of real numbers. As discussed in the previous section, we only consider MIMO lattices Λ, where Λ is full in $M_n(\mathbf{C})$.

The PEP oriented design criteria give us a natural measure related to the coding gain:

Definition 2.2: The minimum determinant $\det_{min}(\Lambda)$ of the lattice Λ is defined to be the infimum of the absolute values of the determinants of all non-zero matrices in the lattice.
Yet this definition is not very satisfactory. If we use the minimum determinant of a code lattice as a measure of the quality of the lattice, we will get nonsensical results. For example, the lattice 2Λ has a lot better minimum determinant than Λ. It is now evident that we need some kind of normalization.

We can flatten the matrices A of $M_n(\mathbf{C})$ to $2n^2$ vectors $\phi(A) \in \mathbf{R}^{2n^2}$ by first forming a vector of length n^2 out of the entries (e.g. row by row) and then replacing a complex number z with the pair of its real and imaginary parts $\Re z$ and $\Im z$. This mapping ϕ is clearly $\mathbf{R}$-linear and maps full $M_n(\mathbf{C})$ lattices to full $\mathbf{R}^{2n^2}$ lattices. We also have the equality $||A||_F = ||\phi(A)||_E$, where F and E denote the Frobenius and Euclidean norms, respectively. Therefore, ϕ is also an isometry.

We denote the measure (or hypervolume) of the fundamental parallelotope of the lattice $\phi(\Lambda)$ by $m(\Lambda)$ and we call it the *volume of the fundamental parallelotope of the lattice* Λ. If $x_1, \ldots, x_{2n^2}$ is a basis of Λ, we can form a matrix M by using the vectors $\phi(x_i)$ as column blocks. Then the *Gram matrix* of the lattice Λ is

$$G(\Lambda) = MM^T = \left(\Re tr(x_i x_j^\dagger)\right)_{1 \le i,j \le 2n^2}.$$

The Gram matrix has a positive determinant equal to $m(\Lambda)^2$.

Any full lattice Λ can be scaled (i.e. multiplied by a real constant r) to satisfy $m(\Lambda) = 1$. As the minimum determinant determines the asymptotic pairwise error probability (PEP), this gives rise to natural numerical measures for the quality of a lattice. We shall denote by $\delta(\Lambda)$ the *normalized minimum determinant* of the lattice Λ, i.e. here we first scale Λ to have a unit size fundamental parallelotope. A simple computation shows that

$$\delta(\Lambda) = \frac{\det_{min}(\Lambda)}{m(\Lambda)^{1/2n}}. \quad (1)$$

Definition 2.3: Let Λ be a full lattice in $M_n(\mathbf{C})$ having the NVD property. We then refer to $\delta(\Lambda)^2$ as the *coding gain* of the lattice Λ.
As explained in the introduction we can as well use the *normalized density* of the code

$$\rho(\Lambda) = \frac{\det_{min}(\Lambda)^{2n}}{m(\Lambda)}.$$

It is directly seen that $\delta(\Lambda) = (1/\rho(\Lambda))^{1/2n}$. Therefore both these measures are essentially the same thing and we will use them interchangeably. In numerical examples we usually choose to use the normalized minimum determinant for obvious reasons.

The rest of the paper can be seen either as a quest for constructing the best possible space time codes or as a mathematical study of normalized minimum determinant of matrix lattices.

III. Central simple algebras, orders and discriminants

The cyclic division algebras (Definition 3.4) are the main object of interest for us, but in order to fully understand these algebras we have to widen our view and consider a larger class of algebras. As we will see the class of *central simple algebras* (Definition 3.3) is a proper context for this theory.

In this section we give a short introduction to the theory of central simple algebras. The proofs for the following results can be found from a nice book by Irving Reiner [23].

In this section the reader can suppose that all the fields are algebraic number fields (see the appendix). The results are true also in the case where we consider P-adic fields, but these we will need only in Sections VI, VIII, IX and X. In order to understand our main results no P-adic theory is needed.

Definition 3.1: Let F be any field and assume that E/F is a cyclic Galois extension of degree n with the Galois group $\mathrm{Gal}(E/F) = \langle\sigma\rangle$. We can define an associative F-algebra

$$\mathcal{A} = (E/F, \sigma, \gamma) = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E,$$

where $u \in \mathcal{A}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in F^*$. We call this type of algebra *cyclic algebra*.

Definition 3.2: An algebra $\mathcal{A}$ is called *simple* if it has no non-trivial ideals. An F-algebra $\mathcal{A}$ is *central* if its center $Z(\mathcal{A}) = \{a \in \mathcal{A} \mid aa' = a'a \ \forall a' \in \mathcal{A}\} = F$.

Definition 3.3: A *central simple* F-algebra is a simple algebra which is finite dimensional over its center F.

Proposition 3.1: Every cyclic algebra is central simple.

Also the reverse is true if we are considering F-central simple algebras, where F is an algebraic number field.

Theorem 3.2: Let F be an algebraic number field. Every F-central simple algebra is cyclic.

Definition 3.4: A central simple F-algebra $\mathcal{A}$ is a division algebra, if every non-zero element of $\mathcal{A}$ is invertible.

We need a tool for identifying the division algebras among the cyclic algebras. The next proposition due to Albert [26, Theorem 11.12, p. 184] serves as a starting point.

Proposition 3.3 (Norm condition): The cyclic algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ of degree n is a division algebra if and only if none of the elements $\gamma^t, 0 < t < n$, are norms of some element of E^*.

This result is most often stated in the above way. We proceed to describe equivalent conditions that relax the conditions, as now the number of powers of γ to be tested drops quite a bit. The relaxed conditions simply combine Albert's result and the following trivial observation.

Lemma 3.4: Assume that E/F is a cyclic extension of number fields, so $\mathrm{Gal}(E/F) = \langle\sigma\rangle$ is cyclic of order n. Let $\gamma \in F^*$ be an arbitrary element of the smaller field. Consider the set S of such exponents t of γ that γ^t belongs to the norm group $N_{E/F}(E^*)$. Then S is an additive subgroup of $\mathbf{Z}$ and we have

$$S = k\mathbf{Z}$$

for some k that is a factor of n.

Proof: Consider the homomorphism $f : \mathbf{Z} \to F^*$ from the additive group of integers to the multiplicative group F^* given by the formula $f(t) = \gamma^t$. We can then deduce that the set $S = f^{-1}(N_{E/F}(E^*))$ is a subgroup of $(\mathbf{Z}, +)$. Elementary group theory then tells us that $S = k\mathbf{Z}$ for a unique non-negative integer k. Because $N_{E/F}(\gamma) = \gamma^n$ we see that $n \in S$. Therefore the generator k of S must divide n. ■

Proposition 3.5 (Norm condition): The cyclic algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ of degree n is a division algebra if and only if the smallest factor $t \in \mathbf{Z}_+$ of n such that γ^t is the norm of some element of E^* is n.

Proof: If there are integers $t, 0 < t < n$, such that γ^t is a norm, then Lemma 3.4 tells us that the smallest such t must be a factor of n. Therefore it is enough to test the factors of n as opposed to all the integers up to $n-1$. ■

To take full advantage of Lemma 3.4 we record the following ultimate version of the norm condition.

Proposition 3.6 (Norm condition): The cyclic algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ of degree n is a division algebra if and only if $\gamma^{n/p}$ is not the norm of some element of E^* for any prime divisor p of n.

Proof: Again, if γ^t is a norm for some proper divisor t of n, then some integer multiple of t is of the form n/p for some prime factor p of n, say $kt = n/p, k \in \mathbf{Z}, k > 0$, so it suffices to test the exponents of this prescribed form. For if γ^t were a norm, so would be $\gamma^{n/p} = \gamma^{kt} = (\gamma^t)^k$. ■

Due to the above proposition, the element γ is often referred to as the *non-norm element*.

Example 3.1: The division algebra $\mathcal{GA}$ used in [3] to construct the Golden code is a cyclic algebra with $F = \mathbf{Q}(i)$, $E = \mathbf{Q}(i, \sqrt{5})$, $\gamma = i$, when the F-automorphism σ is determined by $\sigma(\sqrt{5}) = -\sqrt{5}$. We also note that, in addition to this representation, $\mathcal{GA}$ can be given another construction as a cyclic algebra. As now $u^2 = i$ we immediately see that $F(u)$ is a subfield of $\mathcal{GA}$ that is isomorphic to the eighth cyclotomic field $E' = \mathbf{Q}(\zeta)$, where $\zeta = (1+i)/\sqrt{2}$. The relation $u\sqrt{5} = -\sqrt{5}u$ read differently means that we can view u as the complex number ζ and $\sqrt{5}$ as the auxiliary generator, call it $u' = \sqrt{5}$. We thus see that the cyclic algebra

$$E' \oplus u'E' = (E'/F, \sigma', \gamma')$$

is isomorphic to the Golden algebra. Here σ' is the F-automorphism of E' determined by $\zeta \mapsto -\zeta$ and $\gamma' = u'^2 = 5$.

A. Orders and discriminants of a division algebra

The main algebraic object in the design of code lattices from algebraic number fields is the ring of algebraic integers. In the division algebras the analogy of this concept is the maximal order. We begin with two examples.

Example 3.2: Suppose that E/F is a cyclic extension of algebraic number fields. Let $\mathcal{A} = (E/F, \sigma, \gamma)$ be a cyclic division algebra and let $\gamma \in F^*$ be an algebraic integer. We immediately see that the $\mathcal{O}_F$-module

$$\Lambda = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E,$$

where $\mathcal{O}_E$ is the ring of integers, is a subring in the cyclic algebra $(E/F, \sigma, \gamma)$. We refer to this ring as the *natural order*. Note also that if γ is not an algebraic integer, then Λ fails to be closed under multiplication.

We use the previous notation.

Definition 3.5: An $\mathcal{O}_F$-order Λ in $\mathcal{A}$ is a subring of $\mathcal{A}$, having the same identity element as $\mathcal{A}$, and such that Λ is a finitely generated module over $\mathcal{O}_F$ and generates $\mathcal{A}$ as a linear space over F.

Remark 3.1: We use the notation Λ interchangeably for both orders and lattices, as the orders we shall use are also lattices.

Proposition 3.7: Any F-central division algebra $\mathcal{A}$ has a maximal $\mathcal{O}_F$-order and any order inside $\mathcal{A}$ is contained in at least one maximal order.

The following example illustrates the fact that non-trivial maximal orders are not just some rare and abstract objects, but come up in the most common situations.

Example 3.3: In the algebra of rational Hamiltonian quaternions $\mathbf{H}(\mathbf{Q}) = (\mathbf{Q}(i)/\mathbf{Q}, \sigma, -1)$, where σ is the usual complex conjugation, standard notation is to denote the auxiliary generator by j instead of u, and to write $k = ij$. So $i^2 = j^2 = k^2 = -1$, and $ji = -ij$.

In this case the natural order $\Lambda = \mathbf{Z}[i, j, k]$ is known as the Lipschitz order. A maximal order known as Hurwitz order is $\Lambda_H = \mathbf{Z}\rho \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}k$, where $\rho = (1 + i + j + k)/2$.

See [5] for MISO codes constructed from the above quaternion orders.

In order to study the relation between the ring $\mathcal{O}_F$ and the $\mathcal{O}_F$-order Λ, it can be beneficial to consider the division algebra $\mathcal{A}$ as a subalgebra in a matrix algebra.

Theorem 3.8: Let $\mathcal{A}$ be a division algebra with center F. Every maximal subfield E of $\mathcal{A}$ contains F. Further, if $[\mathcal{A} : F] = n^2$, then

$$[E : F] = n.$$

Remark 3.2: It is clear that any division algebra contains at least one maximal subfield.

Let $\mathcal{A}$ be an F-central division algebra where $[\mathcal{A} : F] = n^2$ and suppose that E is a maximal subfield of $\mathcal{A}$. Then we can consider $\mathcal{A}$ as an n-dimensional right vector space and the left multiplication with an element c of $\mathcal{A}$ is an E-linear transformation of $\mathcal{A}$. Therefore, c can be seen as a matrix $C \in M_n(E)$. So described representation gives us an injective F-algebra homomorphism ψ from $\mathcal{A}$ to $M_n(E)$. To shorten the notation we often identify the algebra $\mathcal{A}$ and its matrix representation. We refer to maps ψ by calling them *maximal representations*. We refer the reader to [7, Chapter 6, Section A] for details of this map.

Definition 3.6: The determinant (resp. trace) of the matrix C above is called the *reduced norm* (resp. *reduced trace*) of the element $c \in \mathcal{A}$ and is denoted by $nr_{\mathcal{A}/F}(c)$ (resp. $tr_{\mathcal{A}/F}(c)$).

Remark 3.3: The connection with the usual norm map $N_{\mathcal{A}/F}(a)$ (resp. trace map $T_{\mathcal{A}/F}(a)$) and the reduced norm $nr(a)$ (resp. reduced trace $tr(a)$) of an element $a \in \mathcal{A}$ is $N_{\mathcal{A}/F}(a) = (nr(a))^n$ (resp. $T_{\mathcal{A}/F}(a) = ntr(a)$), where n is the degree of E/F.

Proposition 3.9: Let $\mathcal{A}$ be an F-central division algebra and a an element of $\mathcal{A}$. Then $nr(a)$ and $tr(a) \in F$.

Example 3.4: Suppose that E/F is a cyclic extension of algebraic number fields. Let $\mathcal{A} = (E/F, \sigma, \gamma)$ be a cyclic division algebra.

We can consider $\mathcal{A}$ as a right vector space over E and every element $a = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{A}$ has the following

representation as a matrix $\psi(a) = A$

$$= \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

Proposition 3.10: The norm and trace maps do not depend on the maximal representation.

Proposition 3.11: Let Λ be an $\mathcal{O}_F$-order in an F-central division algebra $\mathcal{A}$. Then for any element $a \in \Lambda$ its reduced norm $nr_{\mathcal{A}/F}(a)$ and reduced trace $tr_{\mathcal{A}/F}(a)$ are elements of the ring of integers $\mathcal{O}_F$ of the field F. If a is non-zero, then so is $nr_{\mathcal{A}/F}(a)$.

Now we are ready to define one of the main algebraic objects of this paper.

Definition 3.7: Let $\mathcal{A}$ be an F-central division algebra and $m = dim_F\mathcal{A}$. The *$\mathcal{O}_F$-discriminant* of the $\mathcal{O}_F$-order Λ is the ideal $d(\Lambda/\mathcal{O}_F)$ in $\mathcal{O}_F$ generated by the set

$$\{\det(tr_{\mathcal{A}/F}(x_ix_j))_{i,j=1}^m \mid (x_1, ..., x_m) \in \Lambda^m\}.$$

To shorten the notation, we denote $d(\Lambda/\mathcal{O}_F) = d(\Lambda)$, whenever there is no danger of confusion.

In the interesting cases of $F = \mathbf{Q}(i)$ (resp. $F = \mathbf{Q}(\sqrt{-3})$) the ring $R = \mathbf{Z}[i]$ (resp. $R = \mathbf{Z}[\omega]$, $\omega = (-1+\sqrt{-3})/2$) is a Euclidean domain, so in these cases (as well as in the case $R = \mathbf{Z}$) it makes sense to speak of the discriminant as an element of R rather than as an ideal. We simply pick a generator of the discriminant ideal, and call it the discriminant. Equivalently we can compute the discriminant as

$$d(\Lambda/R) = \det(tr(x_ix_j))_{i,j=1}^m,$$

where $\{x_1, \ldots, x_m\}$ is any R-basis of Λ. It is readily seen that whenever $\Lambda \subseteq \Gamma$ are two R-orders, then $d(\Gamma)$ is a factor of $d(\Lambda)$. The index $[\Gamma : \Lambda]$ is related to discriminants by the following lemma.

Lemma 3.12:

$$[R : d(\Lambda)R] = [\Gamma : \Lambda]^2[R : d(\Gamma)R]$$

Proposition 3.13: All the maximal orders of an F-central division algebra share the same discriminant.

Now we can define the following.

Definition 3.8: Let $\mathcal{A}$ be an F-central division algebra and let Λ be some maximal order in $\mathcal{A}$. Then we refer to $d(\Lambda/\mathcal{O}_F) = d_{\mathcal{A}}$ as the *discriminant of the algebra $\mathcal{A}$.*

We include as an easy reference (see [27, Theorem 1.61, p. 42]) the following formula for the discriminant of certain cyclotomic fields.

Proposition 3.14: Let $\zeta_\ell = \exp(2\pi i/2^\ell)$ be a complex primitive root of unity of order 2^ℓ, where $\ell \geq 2$ is an integer. Then $n = [\mathbf{Q}(\zeta_\ell) : \mathbf{Q}(i)] = 2^{\ell-2}$ and

$$d(\mathbf{Z}[\zeta_\ell]/\mathbf{Z}[i]) = (1+i)^{\ell(n/2)}.$$

IV. Order codes

Let F be a complex quadratic field. Again, we assume that E/F is a cyclic field extension of degree n with the Galois group $\mathrm{Gal}(E/F) = \langle\sigma\rangle$. Let $\mathcal{A} = (E/F, \sigma, \gamma)$ be a cyclic division algebra of index n. That is,

$$\mathcal{A} = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E,$$

as a (right) vector space over E. Further, let $u^n = \gamma$ be an algebraic integer, $\gamma \in \mathcal{O}_F$.

Let us now consider the map ψ described in Example 3.4 and identify the algebra $\mathcal{A}$ and its matrix representation.

In order to produce a MIMO lattice satisfying the NVD property, the authors of [3] restricted the coefficients $x_i \in E$ of u^j and the non-norm element to be algebraic integers, i.e. $\gamma \in \mathcal{O}_F,\ x_i \in \mathcal{O}_E$. As a result, we get a natural order

$$\Lambda_n = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus u^2\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E.$$

Proposition 3.11 and Lemma 13.2 then assure that $|\det(\psi(a))| \geq 1$, for every non-zero $a \in \Lambda_n$. It is also easily proved (Lemma 5.1) that the lattice $\psi(\Lambda_n)$ is full in $M_n(\mathbf{C})$. These properties show that Λ_n is a promising space-time code in terms of this paper.

However, these remarkable properties are not true only for natural orders. We could have chosen any $\mathcal{O}_F$-order (and any maximal representation ψ) and still maintain all the benefits of the natural order. In the following, we discuss the coding theoretic properties of $\mathcal{O}_F$-orders supposing always that we use some maximal representation ψ. As we are considering F-central division algebras, the reader can always suppose that we are using some cyclic generation and representation ψ attached to it. At this point, the volumes of fundamental parallelotopes of the orders could depend on the chosen map ψ. Let $\mathcal{A}$ be an F-central division algebra of index n and ψ some maximal representation.

Proposition 4.1: Let Λ be an $\mathcal{O}_F$-order in $\mathcal{A}$. Then

$$\det_{min}(\psi(\Lambda)) = 1.$$

Proof: This result is a direct corollary of Proposition 3.11 and Lemma 13.2. ∎

Corollary 4.2: Suppose we have an $\mathcal{O}_F$-order Λ in an F-central division algebra $\mathcal{A}$ of index n. Then

$$\delta(\psi(\Lambda)) = \left(\frac{1}{m(\psi(\Lambda))}\right)^{\frac{1}{2n}}$$

and

$$\rho(\psi(\Lambda)) = \frac{1}{m(\psi(\Lambda))}.$$

This reveals that in order to measure the normalized minimum determinant and density of an order, it is enough to determine the volume of the fundamental parallelotope.

Corollary 4.3: Let $\Lambda_1 \subseteq \Lambda_2$ be two $\mathcal{O}_F$-orders inside an F-central division algebra $\mathcal{A}$. Then

$$\delta(\psi(\Lambda_1)) \leq \delta(\psi(\Lambda_2)),$$

$$\rho(\psi(\Lambda_1)) \leq \rho(\psi(\Lambda_2))$$

and we have an equality if and only if $\Lambda_1 = \Lambda_2$.

Proposition 4.4: Suppose we have two maximal orders $\Lambda_1, \Lambda_2 \subseteq \mathcal{A}$. Then

$$\delta(\psi(\Lambda_1)) = \delta(\psi(\Lambda_2))$$

and

$$\rho(\psi(\Lambda_1)) = \rho(\psi(\Lambda_2))$$

Proof: The proof is postponed to Section V. ∎

It is now evident that in order to maximize the minimum determinant we have to use maximal orders as any other order is always contained in a maximal one having a better minimum determinant.

V. The coding gain and density of an order code

Previously, we have seen that the normalized minimum determinant and the density of an order code depend only on the volume of the fundamental parallelotope. In this section, we are going to show how this volume actually depends on the algebraic properties of the order.

The definition of the discriminant closely resembles that of the Gram matrix of a lattice, so the following results are not very surprising.

Lemma 5.1: Assume that F is an imaginary quadratic number field and that 1 and θ form a $\mathbf{Z}$-basis of its ring of integers R. Assume further that the order Λ is a free R-module (an assumption automatically satisfied, when R is a principal ideal domain). Let us further assume that ψ is some maximal representation. Then the measure of the fundamental parallelotope of the lattice $\psi(\Lambda)$ equals

$$m(\psi(\Lambda)) = |\Im\theta|^{n^2}|d(\Lambda/R)|.$$

Proof: Let $A = (a_{ij})$ be an $n \times n$ complex matrix. We flatten it out into a $2 \times 2n^2$ matrix $L(A)$ by first forming a vector of length n^2 out of the entries (e.g. row by row) and then replacing a complex number z by a diagonal two by two matrix with entries z and z^* (= the usual complex conjugate of z). If A and B are two square matrices with n rows we can easily verify the identities

$$L(A)L(B)^H = \begin{pmatrix} tr(AB^H) & 0 \\ 0 & tr(A^HB) \end{pmatrix} \qquad (2)$$

and

$$L(A)L(B^T)^T = \begin{pmatrix} tr(AB) & 0 \\ 0 & tr(AB)^* \end{pmatrix}. \qquad (3)$$

Next let $\mathcal{B} = \{x_1, x_2, \ldots, x_{n^2}\}$ be an R-basis for $\psi(\Lambda)$. We form the $2n^2 \times 2n^2$ matrix $L(\mathcal{B})$ by stacking the matrices $L(x_i)$ on top of each other. Similarly we get $R(\mathcal{B})$ by using the matrices $L(x_i^T)^T$ as 'column blocks'. Then by (3) the matrix $M = L(\mathcal{B})R(\mathcal{B})$ consists of two by two blocks of the form

$$L(x_i)L(x_j^T)^T = \begin{pmatrix} tr(x_ix_j) & 0 \\ 0 & tr(x_ix_j)^* \end{pmatrix}.$$

Clearly $\det R(\mathcal{B}) = \pm\det L(\mathcal{B})$, and $\det M = |d(\Lambda/R)|^2$, so we get

$$|d(\Lambda/R)| = |\det L(\mathcal{B})|.$$

Next we turn our attention to the Gram matrix. By our assumptions the set $\mathcal{B} \cup \theta\mathcal{B}$ is a $\mathbf{Z}$-basis for Λ. Let us denote

$$D = \begin{pmatrix} 1 & 1 \\ \theta & \theta^* \end{pmatrix}.$$

From the identities $\Re(xy^*) = (xy^* + x^*y)/2$ and

$$D\begin{pmatrix} x & 0 \\ 0 & x^* \end{pmatrix} = \begin{pmatrix} x & x^* \\ \theta x & \theta^* x^* \end{pmatrix}$$

together with (2) it follows that for any two $n \times n$ matrices A and B we have

$$\frac{1}{2}\left(DL(A)\right)\left(DL(B)\right)^H = \begin{pmatrix} \Re(tr(AB^H)) & \Re(tr(A(\theta B)^H) \\ \Re(tr(\theta AB^H)) & \Re(tr(\theta A(\theta B)^H)) \end{pmatrix}.$$

Therefore, if we denote by $D^{[n]}$ the $2n^2 \times 2n^2$ matrix having n^2 copies of D along the diagonal and zeros elsewhere, we get the following formula for the Gram matrix

$$G(\psi(\Lambda)) = \frac{1}{2}\left(D^{[n]}L(\mathcal{B})\right)\left(D^{[n]}L(\mathcal{B})\right)^H.$$

Thus,

$$m(\psi(\Lambda)) = \det G(\psi(\Lambda))^{1/2} = |\det L(\mathcal{B})|\left|\frac{1}{2}\det D\right|^{n^2}.$$

Our claim now follows from all these computations and the fact that $(\det D)/2 = (\theta^* - \theta)/2 = -\Im\theta$. ∎

We have now seen that the density of an order code does not depend on the representation. Thus, as we are only interested in the questions concerning the density, we will forget about the representation ψ and simply identify the order and its matrix representation. Now we also have a proof for Proposition 4.4, as all the maximal orders share the same discriminant.

In the cases of $F = \mathbf{Q}(i)$ and $F = \mathbf{Q}(\sqrt{-3})$, we have $\theta = i$ and $\theta = (-1 + \sqrt{-3})/2$, respectively. Thus, we immediately get the following two corollaries.

Corollary 5.2: Let $F = \mathbf{Q}(i), R = \mathbf{Z}[i]$, and assume that $\Lambda \subseteq (E/F, \sigma, \gamma)$ is an R-order. Then the measure of the fundamental parallelotope equals

$$m(\Lambda) = |d(\Lambda/\mathbf{Z}[i])|.$$

Example 5.1: When we scale the Golden code [3] to have a unit minimum determinant, all the 8 elements of its $\mathbf{Z}$-basis will have length $5^{1/4}$ and the measure of the fundamental parallelotope is thus 25. In view of all of the above this is also a consequence of the fact that the $\mathbf{Z}[i]$-discriminant of the natural order of the Golden algebra is equal to 25. As was observed in [28] the natural order happens to be maximal in this case, so the Golden code cannot be improved upon by enlarging the order within $\mathcal{GA}$.

Corollary 5.3: Let $\omega = (-1 + \sqrt{-3})/2$, $F = \mathbf{Q}(\omega)$, $R = \mathbf{Z}[\omega]$, and assume that $\Lambda \subset (E/F, \sigma, \gamma)$ is an R-order. Then the measure of the fundamental parallelotope equals

$$m(\Lambda) = (\sqrt{3}/2)^{n^2}|d(\Lambda/\mathbf{Z}[\omega])|.$$

The upshot is that in both cases **maximizing the density of the code, i.e. minimizing the fundamental parallelotope, is equivalent to minimizing the discriminant**. Thus, in order to get the densest MIMO-codes we need to look for division algebras that have a maximal order with as small a discriminant as possible.

For an easy reference we also include the following result.

Lemma 5.4: Let E/F be as above, assume that γ is an algebraic integer of F, and let Λ be the natural order of Example 3.2. If $d(E/F)$ is the $\mathcal{O}_F$-discriminant of $\mathcal{O}_E$ (often referred to as the relative discriminant of the extension E/F), then

$$d(\Lambda/\mathcal{O}_F) = d(E/F)^n\gamma^{n(n-1)}.$$

Proof: In the expansion

$$\Lambda = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E$$

we see that $u^i\mathcal{O}_E$ and $u^j\mathcal{O}_E$ are orthogonal to each other with respect to the bilinear form given by the reduced trace except in the cases where $i+j \equiv 0 \pmod n$. Assume that $i+j$ is divisible by n for some i,j in the range $0 \leq i,j < n$, and that $x_1,\ldots,x_n$ are elements of $\mathcal{O}_E$. Then the multiplication rules of the cyclic algebra together with Lemma 13.6 imply that

$$\begin{aligned}\det(tr(u^i x_k u^j x_\ell))_{k,\ell=1}^n &= \pm\det(u^{i+j}tr(x_k x_\ell))_{k,\ell=1}^n \\ &= \pm\gamma^\epsilon \det(tr(x_k x_\ell))_{k,\ell=1}^n,\end{aligned}$$

where the exponent ϵ is equal to zero or n according to whether $i+j$ equals zero or n. The former case occurs only once and the latter case occurs exactly $n-1$ times. The claimed formula then follows. ∎

Example 5.2: We use the notation from Proposition 3.14. In [11] Kiran and Rajan have shown that the family of cyclic algebras $\mathcal{A}_\ell = (\mathbf{Q}(\zeta_\ell)/\mathbf{Q}(i), \sigma(\zeta_\ell) = \zeta_\ell^5, 2+i)$, with $\ell \geq 3$, consists entirely of division algebras. Let $\Lambda_{nat,\ell}$ be the natural order of the algebra $\mathcal{A}_\ell$. We may now conclude from Lemma 5.4, Proposition 3.14, and Corollary 5.2 that

$$d(\Lambda_{\ell,nat}/\mathbf{Z}[i]) = (2+i)^{n(n-1)}(1+i)^{\ell(n/2)n},$$

and that

$$m(\Lambda_{nat,\ell})^2 = 2^{\ell(n/2)n}5^{n(n-1)}.$$

For instance, in the 2 antenna case $\ell = 3, n = 2$, we have $m(\Lambda_{nat,\ell}) = 40$, and thus the Golden code is denser than the corresponding lattice $\mathcal{A}_3$ of the same minimum determinant. However, the natural order of $\mathcal{A}_3$ is not maximal and we will return to this example later on.

VI. The Discriminant Bound

In the previous section, we studied the relation between the normalized minimum determinant of an order and its discriminant. In the case of a maximal order it thus depends on the discriminant of the algebra. It is now evident that there are some optimal algebras that have minimal discriminants. In order to describe and hopefully also identify these optimal algebras we need to gain a deeper understanding of the discriminant of an algebra.

In this section, we leave coding theory behind and only consider the discriminants of division algebras (and also all central simple algebras). The emphasis is on the problem of finding the minimal possible discriminant. In Section VII we return to our main track and apply our general results to get bounds for normalized minimum determinants and densities of codes from orders of division algebras.

Due to space limitations, we cannot perform a comparison to the commutative case or give a deep insight here. We refer the interested reader to [29] for a more thorough discussion on the discriminant bounds and the underlying principles.

For more details and for the proofs of this Section, we refer the reader to [23], especially to its Chapters 3, 7, and 8.

A. Localization and Hasse invariants of an algebra

We are mostly interested in such cyclic division algebras $\mathcal{A}$, where the center F is an algebraic number field. However, in order to understand these algebras, we also have to consider their localizations. These localizations force us out of the world of simple division algebras.

If F' is an extension field of F and $\mathcal{A}$ is a central simple F-algebra, then the tensor product $\mathcal{A}' = \mathcal{A} \otimes_F F'$ is a central simple F'-algebra. We refer to this algebra as the algebra obtained from $\mathcal{A}$ by *extending the scalars to* F'.

Definition 6.1: Let F be an algebraic number field that is finite dimensional over $\mathbf{Q}$ and let P be some prime of F. If $\mathcal{A}$ is an F-central simple algebra, then we call the algebra $\mathcal{A}_P = \hat{F}_P \otimes_F \mathcal{A}$ *the localization* of $\mathcal{A}$ at P.

Proposition 6.1: With the notation of the previous definition,

$$[\mathcal{A} : F] = [\mathcal{A}_P : \hat{F}_P].$$

A theorem of Wedderburn reduces the classification of central simple algebras to the case of division algebras.

Theorem 6.2 (Wedderburn): If $\mathcal{A}$ is an F-central simple algebra, then

$$\mathcal{A} \simeq M_n(\mathcal{D}),$$

where $\mathcal{D}$ is some F-central division algebra. The integer n and the algebra $\mathcal{D}$ are uniquely determined (up to isomorphism).

Definition 6.2: Let $\mathcal{A}$ be the algebra of the previous theorem. We call $\operatorname{index}[\mathcal{A}] = \sqrt{[\mathcal{D} : F]}$ *the index* of the algebra $\mathcal{A}$. We note that the index is always an integer.

Definition 6.3: Let $\mathcal{A}$ be an F-central simple algebra. We call

$$\sqrt{[\mathcal{A} : F]}$$

the *degree* of the algebra.

Remark 6.1: One should notice that an F-central simple algebra $\mathcal{A}$ is a division algebra if and only if $\operatorname{index}[\mathcal{A}] = \sqrt{[\mathcal{A} : F]}$.

Theorem 6.2 gives us that $\hat{F}_P \otimes_F \mathcal{A} \simeq M_s(\mathcal{D}_P)$, where $\mathcal{D}_P$ is some $\hat{F}_P$-central division algebra. This leads us to consider those division algebras, where $\hat{F}_P$ is some completion of F.

Let F be an algebraic number field that is finite dimensional over $\mathbf{Q}$ and let P be a finite prime of F.

Proposition 6.3: The cyclic algebra

$$\mathcal{A}(n,r) = (\hat{E}/\hat{F}_P, \sigma, \pi^r), \quad (r,n) = 1, \quad 0 \leq r < n,$$

where $\hat{E}$ is the unique unramified extension of $\hat{F}_P$ of degree n, σ is the Frobenius automorphism, and π is a prime element of $\hat{F}_P$, is a division algebra. The algebras $\mathcal{A}(n,r_1)$ and $\mathcal{A}(n,r_2)$ are isomorphic if and only if $r_1 = r_2$.

Theorem 6.4: Let $\mathcal{A}$ be a $\hat{F}_P$-central division algebra of index n. Then

$$\mathcal{A} \simeq \mathcal{A}(n,r)$$

for some r.

Definition 6.4: Let $\mathcal{A}$ be the $\hat{F}_P$-central division algebra of the previous theorem. We call the rational number $\operatorname{inv}[\mathcal{A}] = \frac{r}{n}$ the Hasse invariant of $\mathcal{A}$.

Now we are ready to define the following.

Definition 6.5: Suppose that F is an algebraic number field and P some prime of F. Let $\mathcal{A}$ be an F-central simple algebra and

$$\hat{F}_P \otimes_F \mathcal{A} = M_{\kappa_P}(\mathcal{D}_P),$$

where $\mathcal{D}_P$ is a $\hat{F}_P$-central division algebra. We refer to $inv[\mathcal{D}_P] = h_P = r_P/m_P$ as the Hasse invariant of $\mathcal{A}$ at P and to m_P as the *local index*. The integer κ_P is referred to as the *local capacity* (at P).

Remark 6.2: The fact that the local capacity and Hasse invariants are well defined follows from the uniqueness part of Theorem 6.2.

Note that $m_P = 1$ if and only if

$$\mathcal{A}_P \simeq M_{\kappa_P}(\hat{F}_P).$$

We say that a prime P is ramified in the algebra $\mathcal{A}$ if the corresponding local index is not 1.

Theorem 6.5: Let $\mathcal{A}$ be an F-central simple algebra. There exist only a finite set $\{P_1, \ldots, P_n\}$ of primes in F that have non-zero Hasse invariants and

$$\mathrm{index}[\mathcal{A}] = LCM\{m_{P_i}\}.$$

Corollary 6.6: Suppose that $\mathcal{A}$ is an F-central simple algebra of degree n. If $\mathcal{A}$ has such a local index m_P that

$$m_P = n,$$

then $\mathcal{A}$ is a division algebra.

B. The Brauer group

In order to get a better grip of the central simple algebras it is beneficial to consider them as elements in a group. This deceivingly simple step, taken by Richard Brauer, gives us a great insight on central simple algebras.

Proposition 6.7: Let $\mathcal{A}$ and $\mathcal{B}$ be F-central simple algebras. Then $\mathcal{A} \otimes_F \mathcal{B}$ is an F-central simple algebra.

Let us now consider the family of all F-central simple algebras. Two central simple F-algebras $\mathcal{A} = M_n(\mathcal{D}_\mathcal{A})$ and $\mathcal{B} = M_s(\mathcal{D}_\mathcal{B})$ are said to be *similar*, if $\mathcal{D}_\mathcal{A} \simeq \mathcal{D}_\mathcal{B}$. We denote the similarity class of a central simple algebra $\mathcal{A}$ by $[\mathcal{A}]$.

Similarity classes of F-central simple algebras form a group (under tensor product over F), called the *Brauer group* $\mathrm{Br}(F)$ of the field F. The identity element of $\mathrm{Br}(F)$ is the similarity class of F and the inverse of the element $[\mathcal{A}] \in \mathrm{Br}(F)$ is the similarity class of the *opposite algebra* $\mathcal{A}^{opp}$.

Theorem 6.8: Let F be an algebraic number field and suppose that $\mathcal{A}$ and $\mathcal{B}$ are F-central simple algebras. Then

$$\mathcal{A} \sim \mathcal{B} \Longleftrightarrow \mathcal{A}_P \sim \mathcal{B}_P \quad \forall\, P \in F.$$

This theorem now allows us to introduce the following map.

Lemma 6.9: Let $\mathcal{A}$ be an F-central simple algebra where F is an algebraic number field and P a prime in F. Then the map defined by

$$\mathcal{A} \longmapsto \hat{F}_P \otimes_F \mathcal{A},$$

is a group homomorphism from $\mathrm{Br}(F)$ to $\mathrm{Br}(\hat{F}_P)$.

The following theorem gives us a concrete view on the previous map.

Theorem 6.10: Suppose that L/F is a cyclic Galois extension, $\mathrm{Gal}(L/F) = \langle\sigma\rangle$ and $a \in F^*$. Let E be any field containing F, and let EL be the compositum of E and L in some larger field containing both E and L. We may write

$$H = \langle\sigma^k\rangle = \mathrm{Gal}(L/L \cap E) \simeq \mathrm{Gal}(EL/E),$$

where k is the least positive integer such that σ^k fixes $L \cap E$. Then

$$E \otimes_F (L/F, \sigma, a) \sim (EL/E, \sigma^k, a).$$

C. Proving the Discriminant Bound

The following relatively deep result from class field theory is the key for deriving the discriminant bound. Assume that the field F is totally complex. Then we have the *fundamental exact sequence of Brauer groups* (see e.g. [23, Equation 32.13, p. 277] or [30])

$$0 \longrightarrow \mathrm{Br}(F) \longrightarrow \oplus\, \mathrm{Br}(\hat{F}_P) \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow 0. \qquad (4)$$

Here the first nontrivial map is obtained by mapping the similarity class of a F-central simple algebra $\mathcal{A}$ to a vector consisting of the similarity classes of all the simple algebras $\mathcal{A}_P$ obtained from $\mathcal{A}$ by extending the scalars from F to $\hat{F}_P$, where P ranges over all the primes of $\mathcal{O}_F$. Note that the injectivity of this map is stated in Theorem 6.8. That such a mapping is well defined is due to Lemma 6.9 and Theorem 6.5.

The second nontrivial map of the fundamental exact sequence is then simply the sum of the Hasse invariants of the division algebras $\mathcal{A}_P$ representing elements of the Brauer groups $\mathrm{Br}(\hat{F}_P)$.

The sequence tells us that the sum of the nontrivial Hasse invariants of any central simple algebra must be an integer. Furthermore, this is the only constraint for the Hasse invariants, i.e. any combination of Hasse invariants (a/m_P) such that only finitely many of them are non-zero, and that they sum up to an integer, is realized as a collection of the Hasse invariants of some central simple algebra $\mathcal{A}$ over F.

Example 6.1: For example, when $F = \mathbf{Q}(i)$, the fundamental exact sequence tells us that there is a 16-dimensional division algebra D_1 over F with non-trivial Hasse invariants $1/4$ at the prime $P_1 = 1 + i$ and $3/4$ at the prime $P_2 = 3$. There is also another 16-dimensional division algebra D_2 with non-trivial Hasse invariants $1/4$ at P_1, $1/4$ at P_2 and $1/2$ at prime $P_3 = 2 + i$. Then $D_1 \otimes_F D_2$ has Hasse invariants $1/4 + 1/4 = 1/2$ at P_1, $3/4 + 1/4 = 1 \equiv 0$ at P_2 and $0 + 1/2 = 1/2$ at P_3. Wedderburn's theorem tells us that $D_1 \otimes_F D_2 \simeq \mathcal{M}_m(D_3)$ for a division algebra D_3. The nontrivial local indices of D_3 are both equal to 2, so we know that D_3 is a 4-dimensional F-algebra. A calculation of dimensions tells us that $m = 8$.

Let us now suppose that, with a given number field F, we would like to produce a division algebra $\mathcal{A}$ of a given index n, having F as its center and the smallest possible discriminant. We proceed to show that, while we cannot give an explicit description of the algebra $\mathcal{A}$ in all the cases, we can derive an explicit formula for its discriminant.

Theorem 6.11: Assume that the field F is totally complex and that $P_1, \ldots, P_n$ are some prime ideals of $\mathcal{O}_F$. Assume further that a sequence of rational numbers $a_1/m_{P_1}, \ldots, a_n/m_{P_n}$

satisfies

$$\sum_{i=1}^{n} \frac{a_i}{m_{P_i}} \equiv 0 \qquad (\text{mod} \quad 1),$$

$1 \leq a_i \leq m_{P_i}$, and $(a_i, m_{P_i}) = 1$.

Then there exists a central division F-algebra $\mathcal{A}$ that has local indices m_{P_i} and the least common multiple (LCM) of the numbers $\{m_{P_i}\}$ as an index.

If Λ is a maximal $\mathcal{O}_F$-order in $\mathcal{A}$, then the discriminant of Λ is

$$d(\Lambda/\mathcal{O}_F) = \prod_{i=1}^{n} P_i^{(m_{P_i}-1)\frac{[\mathcal{A}:F]}{m_{P_i}}}.$$

Proof: By exactness of the sequence (4) we know that there exists a central division algebra $\mathcal{A}$ over F which has local indices m_{P_i}. We also know that $\sqrt{[\mathcal{A}:F]} = LCM\{m_{P_i}\}$. By [23, Theorem 32.1] the discriminant then equals

$$d(\Lambda/R) = \left(\prod_{i=1}^{n} P_i^{(m_{P_i}-1)\kappa_{P_i}} \right)^{\sqrt{[\mathcal{A}:F]}}, \tag{5}$$

where κ_{P_i} is the local capacity.

A simple calculation of dimensions shows that

$$\kappa_P = \frac{\sqrt{[\mathcal{A}:F]}}{m_P}.$$

Substituting this into (5) we get the claim. ∎

At this point it is clear that the discriminant $d(\Lambda)$ of a division algebra only depends on its local indices m_{P_i}.

Now we have an optimization problem to solve. Given the center F and an integer n we should decide how to choose the local indices and the Hasse invariants so that the LCM of the local indices is n, the sum of the Hasse invariants is an integer, and that the resulting discriminant is as small as possible. We immediately observe that at least two of the Hasse invariants must be non-integral.

Observe that the exponent $d(P)$ of the prime ideal P in the discriminant formula is

$$d(P) = (m_P - 1)\frac{[\mathcal{A}:F]}{m_P} = n^2\left(1 - \frac{1}{m_P}\right).$$

As for the nontrivial Hasse invariants $n \geq m_P \geq 2$, we see that $n^2/2 \leq d(P) \leq n(n-1)$. Therefore the nontrivial exponents are roughly of the same size. For example, when $n = 6$, $d(P)$ will be either 18, 24 or 30 according to whether m_P is 2, 3 or 6. Not surprisingly, it turns out that the optimal choice is to have only two non-zero Hasse invariants and to associate these with the two smallest prime ideals of $\mathcal{O}_F$.

Theorem 6.12 (Main Theorem): Assume that F is a totally complex number field, and that P_1 and P_2 are the two smallest prime ideals in $\mathcal{O}_F$. Then the smallest possible discriminant of all central division algebras over F of index n is

$$(P_1 P_2)^{n(n-1)}.$$

Proof: By Theorem 6.11 the division algebra with Hasse invariants $1/n$ and $(n-1)/n$ at the primes P_1 and P_2 has the prescribed discriminant, so we only need to show that this is the smallest possible value. When there are only two non-trivial Hasse invariants, the two local indices are clearly equal to n, so we cannot do better than this with only two non-trivial Hasse invariants.

The next observation we make is that in order to minimize the discriminant one cannot have more than three nontrivial Hasse invariants. This is because for prime ideals P_1, P_2, P_3, P_4 (listed from the smallest to the largest) we always have

$$P_1^{d(P_1)} P_2^{d(P_2)} P_3^{d(P_3)} P_4^{d(P_4)} > (P_1 P_2)^{n(n-1)},$$

as the exponents $d(P_i) \geq n^2/2$ irrespective of the values of the Hasse invariants. A possibility is that some combination of three non-trivial Hasse invariants $(a_i/m_{P_i}), i = 1, 2, 3$ might yield a smaller discriminant. Let us study this in detail, and assume that a division algebra $\mathcal{D}$ has these 3 non-trivial Hasse invariants at the primes P_1, P_2, P_3 (not necessarily in increasing order).

If one of the local indices, say m_{P_1}, has only a single prime factor p, then $m_{P_1} = p^t, t > 0$. We write $m_{P_2} = p_2' p^a$ and $m_{P_3} = p_3' p^b$, where the integer factors p_2' and p_3' are coprime to p. Without loss of generality (swap P_2 and P_3, if necessary) we may assume that $a \leq b$. Let first q be any prime divisor of p_2' or p_3'. Then a_1/p^t is a q-adic integer. Because the sum of the three Hasse invariants is a rational integer, the q-adic triangle inequality shows that any power of q dividing either p_2' or p_3' must also divide the other. Therefore $p_2' = p_3'$. Let us next consider the p-adic values. By the p-adic triangle inequality we have either $t = b$, or $a = b > t$. In both cases we have $m_{P_3} = LCM(m_{P_1}, m_{P_2})$. Therefore $m_{P_3} = LCM(m_{P_1}, m_{P_2}, m_{P_3}) = n$.

We shall show that in this case the discriminant becomes smaller, if we assign the sum of the two Hasse invariants

$$a_1/m_{P_1} + a_2/m_{P_2} = a'/m'_{P'} \pmod 1$$

to the smaller prime P' of the two prime ideals P_1 and P_2. Let $\mathcal{D}'$ be the division algebra with only non-trivial Hasse invariants $a'/m'_{P'}$ at P' and a_3/m_{P_3} at P_3. Because $a'/m'_{P'} + a_3/m_{P_3}$ is an integer, we immediately see that $m'_{P'} = m_{P_3}$. Therefore the index n' of $\mathcal{D}'$ is $n' = m_{P_3} = n$. As $d(P_1) + d(P_2) > n(n-1) \geq d'(P')$, where $d'(P')$ is the exponent corresponding to the local index $m_{P'}$, $\mathcal{D}'$ will have a smaller discriminant than $\mathcal{D}$.

The remaining case is that all the three local indices have at least two distinct prime factors. In this case the three local indices are all ≥ 6. As then $d(P_1)+d(P_2)+d(P_3) > 2n(n-1)$, we see that the discriminant of the division algebra with these Hasse invariants also exceeds the stated lower bound. ∎

We remark that in the most interesting (for MIMO) cases $n = 2, 3, 4$, Theorem 6.12 is more or less an immediate corollary of Theorem 6.11. We also remark that the division algebra achieving our bound is by no means unique. For example, any pair of Hasse invariants $a/n, (n-a)/n$, where $0 < a < n$, and $(a, n) = 1$, leads to a division algebra with the same discriminant.

VII. Density bounds for order codes

In this section, we return to our original route and derive bounds and existence results for the coding gains and normal-

ized densities of order codes. After we have given the bounds, we proceed with examples of algebras achieving these bounds.

The smallest primes of the ring $\mathbf{Z}[i]$ are $1+i$ and $2\pm i$. They have norms 2 and 5 respectively. The smallest primes of the ring $\mathbf{Z}[\omega]$ are $\sqrt{-3}$ and 2 with respective norms 3 and 4. Together with Corollaries 5.2 and 5.3 we have arrived at the following bounds.

Corollary 7.1 (Discriminant bound): Let Λ be an order of a central division algebra of index n over the field $\mathbf{Q}(i)$. Then the measure of a fundamental parallelotope of the corresponding lattice satisfies

$$m(\Lambda) \geq 10^{n(n-1)/2}$$

and the normalized minimum determinant satisfy the inequality

$$\delta(\Lambda) \leq 1/10^{(n-1)/4}.$$

Furthermore, for every n, there exist cyclic division algebras with center $\mathbf{Q}(i)$, whose maximal orders achieve equality in both of these bounds.

Corollary 7.2 (Discriminant bound): Let Λ be an order of a central division algebra of index n over the field $\mathbf{Q}(\omega)$, $\omega = (-1+\sqrt{-3})/2$. Then the measure of the fundamental parallelotope of the corresponding lattice satisfies

$$m(\Lambda) \geq (\sqrt{3}/2)^{n^2} 12^{n(n-1)/2}$$

and the normalized minimum determinant satisfy the inequality

$$\delta(\Lambda) \leq (2/\sqrt{3})^{n/2}/12^{(n-1)/4}.$$

Furthermore, for every n there exist cyclic division algebras with center $\mathbf{Q}(\omega)$, whose maximal orders achieve equality in both of these bounds.

We remark that in [29], it was shown that using the center $\mathbf{Q}(\sqrt{-7})$ instead of the more common ones above, we get even denser maximal orders provided that $n > 4$. See also [31] related to this center.

The Golden algebra reviewed in Example 3.1 has its nontrivial Hasse invariants (both equal to $1/2$) at the primes $2+i$ and $2-i$ and hence cannot be an algebra achieving the bound of Theorem 6.12. A clue for finding the optimal division algebra is hidden in the alternative description of the Golden algebra given in Example 3.1. It turns out that in the case $F = \mathbf{Q}(i)$, $E = \mathbf{Q}(\zeta)$, instead of using $\gamma' = 5$ as in the case of the Golden algebra, we can use its prime factor $\gamma = 2+i$.

Proposition 7.3: The maximal orders of the cyclic division algebra $\mathcal{A}_3 = (\mathbf{Q}(\zeta)/\mathbf{Q}(i), \sigma, 2+i)$ of Example 5.2 achieve the bound of Theorem 6.12.

Proof: The algebra $\mathcal{A}_3$ is generated as a $\mathbf{Q}(i)$-algebra by the elements ζ and u subject to the relations $\zeta^2 = i$, $u^2 = 2+i$, and $u\zeta = -\zeta u$. The natural order $\mathbf{Z}[\zeta] \oplus u\mathbf{Z}[\zeta]$ is not maximal. Let us use the matrix representation of $\mathcal{A}_3$ as 2×2 matrices with entries in $\mathbf{Q}(\zeta)$, so elements of $\mathbf{Q}(i)$ are mapped to scalar matrices and ζ is mapped to a diagonal matrix with diagonal elements ζ and $-\zeta$. We observe that the matrix

$$w = \frac{1}{4}\begin{pmatrix} 2i-(1-i)\sqrt{2} & (2+i)(2i-(1+i)\sqrt{2}) \\ (1+i)(1+\sqrt{2}+i) & 2i+(1-i)\sqrt{2} \end{pmatrix}$$

is an element of $\mathcal{A}_3$. Straightforward calculations show that w satisfies the equations

$$w^2 = -i + iw \quad \text{and} \quad w\zeta = -1 + \zeta^3 - \zeta w.$$

From these relations it is obvious that the free $\mathbf{Z}[\zeta]$-module with basis elements 1 and w is an order Λ. Another straightforward computation shows that $d(\Lambda/\mathbf{Z}[i]) = -8+6i = (1+i)^2(2+i)^2$. As this is the bound of Theorem 6.12 we may conclude that Λ is a maximal order. ∎

By Corollary 5.2 we see that the fundamental parallelotope of the maximal order in Proposition 7.3 has measure 10. We compare this lattice to the Golden code, and scale both to have unit minimum determinant. In a power constraint subset of the signal space this lattice will then have approximately 2.5 times as many codewords as the Golden code.

The algebra $\mathcal{A}_3$ has the drawback that the parameter γ is quite large. This leads to an antenna power imbalance in both space and time domains. To some extent these problems can be alleviated by conjugating the matrix lattice by a suitable diagonal matrix (a trick used in at least [15]). One of the motifs underlying the perfect codes [10] is the requirement that the variable γ should have a unit modulus. To meet this requirement we proceed to give a different construction for this algebra.

Theorem 7.4: Let λ be the square root of the complex number $2+i$ belonging to the first quadrant of the complex plane. The cyclic algebra $\mathcal{GA}+ = (\mathbf{Q}(\lambda)/\mathbf{Q}(i), \sigma, i)$, where the automorphism σ is determined by $\sigma(\lambda) = -\lambda$, is a division algebra. The maximal orders of $\mathcal{GA}+$ achieve the bound of Theorem 6.12. Furthermore, the algebras $\mathcal{GA}+$ and $\mathcal{A}_3$ of Theorem 7.3 are isomorphic.

Proof: The algebra $\mathcal{GA}+$ is a central algebra $F\{u', \lambda\}$ over the field $F = \mathbf{Q}(i)$ defined by the relations $\lambda^2 = 2+i$, $u'^2 = i$, $u'\lambda = -\lambda u'$. Comparing these relations with the relations in the proof of Theorem 7.3 we get an isomorphism of F-algebras $f : \mathcal{GA}+ \to \mathcal{A}_3$ by declaring $f(u') = \zeta$, $f(\lambda) = u$ and extending this in the natural way. The other claims follow immediately from this isomorphism and Theorem 7.3. ∎

We refer to the algebra $\mathcal{GA}+$ as the *Golden+ algebra*. This is partly motivated by the higher density and partly by the close relation between the algebra $\mathcal{A}_3$ and the Golden algebra. After all, the algebra $\mathcal{A}_3$ comes out when in the alternative description of the Golden algebra (cf. Example 3.1) the variable $\gamma = 5$ is replaced with its prime factor $2+i$. In Section IX we will provide an alternative proof for Theorem 7.4 by explicitly producing a maximal order within $\mathcal{GA}+$ and verifying that it has the prescribed discriminant. It is immediate from the discussion in the early parts of this section that in this case there is only one cyclic division algebra (up to isomorphism) with that discriminant.

It turns out that all the algebras $\mathcal{A}_\ell$ in the Kiran & Rajan family of Example 5.2 have maximal orders achieving the discriminant bound. The following observation is the key to proving this.

Lemma 7.5: Let F be either one of the fields $\mathbf{Q}(i)$ or $\mathbf{Q}(\omega)$, and let P_1 and P_2 be two smallest ideals of its ring of integers

R. Let $\mathcal{D}$ be a central division algebra over F, and let Λ be any R-order in $\mathcal{D}$. If the discriminant $d(\Lambda)$ is divisible by no prime other than P_1 and P_2, then any maximal order Γ of $\mathcal{D}$ achieves the discriminant bound of Theorem 6.12.

Proof: We know that there exists a maximal order, say Γ_0 containing Λ. The discriminant of Γ_0 is then a factor of $d(\Lambda)$, so P_1 and P_2 are the only prime divisors of $d(\Gamma_0)$. From Theorem 6.11 we infer that the only nontrivial Hasse invariants of $\mathcal{D}$ occur at P_1 and P_2. As the sum of the two Hasse invariants is an integer, they have the same denominator. This must then be equal to the index of $\mathcal{D}$. The discriminant formula of Theorem 6.11 then shows that $d(\Gamma_0)$ equals the discriminant bound. Any other maximal order in $\mathcal{D}$ shares its discriminant with Γ_0. ■

Corollary 7.6: Let $\ell > 2$ be an integer. The maximal orders of the cyclic division algebra $\mathcal{A}_\ell = (\mathbf{Q}(\zeta_\ell)/\mathbf{Q}(i), \sigma, 2+i)$ from Example 5.2 achieve the discriminant bound.

Proof: Proposition 3.14 and Lemma 5.4 indicate that the only prime factors of the discriminant of the natural order in $\mathcal{A}_\ell$ are $1+i$ and $2+i$. The claim then follows from Lemma 7.5. ■

At this point we remark that the natural orders of the algebras $\mathcal{A}_\ell$ of Example 5.2 are very far from being maximal. We will study this in greater detail in Section IX.

Example 7.1: Let $F = \mathbf{Q}(\sqrt{-3})$, so $\mathcal{O}_F = \mathbf{Z}[\omega]$. In this case the two smallest prime ideals are generated by 2 and $1-\omega$ and they have norms 4 and 3 respectively. By Theorem 6.12 the minimal discriminant is $4(1-\omega)^2$ when $n = 2$. As the absolute value of $1-\omega$ is $\sqrt{3}$ an application of the formula in Corollary 5.3 shows that the lattice $\mathbf{L}$ of the code achieving this bound has $m(\mathbf{L}) = 27/4$. In [32] we showed that a maximal order of the cyclic algebra $(E/F, \sigma(i) = -i, \gamma = \sqrt{-3})$, where $E = \mathbf{Q}(i, \sqrt{-3})$, achieves this bound.

We remark that one of the codes suggested in [15] is the natural order of the algebra of Example 7.1. However, the authors there never mentioned the possibility of using a maximal order. Nor did they mention that their lattice actually is an order.

VIII. Example algebras achieving the Discriminant Bound

In the previous section, we proved the existence of extremely attractive MIMO codes with the best known coding gain and gave examples of algebras achieving the discriminant bounds.

In this section, we begin a systematic study of methods to construct the actual codes by giving an explicit construction of division algebras with minimal discriminants and unit non-norm elements. After the correct algebra is found we can use the existing algorithms to find the maximal order. We will return to this question in Section IX.

In the following, we concentrate on the cases where the center of the algebra is $\mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt{-3})$. When natural orders are used for the code construction, large non-norm elements may result in a power imbalance between transmit antennas. While this is not so clear, when we are using maximal orders, the test data we have collected suggests that a big non-norm element may negatively affect the performance of the code. Therefore, it is beneficial to aim at small non-norm elements. However, as noted in [10], we can choose a unit (by a unit we mean a unit of the ring F, separate this from an element having a unit modulus, see [33]) non-norm element only when $n < 7$. In what follows, we actually manage to build an optimal division algebra with a unit non-norm element in all the possible cases.

In Section XI, we relax the restriction on the size of γ and give a general construction for $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-3})$-central division algebras with a minimal discriminant.

One should notice that none of the natural orders of the algebras we shall construct will have a minimal discriminant. This, unfortunately, is not just a coincidence. Later on in Section XIII-B of Appendix, we prove that there are no natural orders reaching the bound of Theorem 6.12.

A. The center $\mathbf{Q}(i)$

TABLE I
$\mathbf{Q}(i)$-CENTRAL DIVISION ALGEBRAS WITH A UNIT γ

n	γ	f_n
2	i	$x^2 + (2+i)$
4	i	$x^4 + (2+i)$

In Table I we give a cyclic generation for algebras of degree 2 and 4 with minimal discriminants. Proposition 3.6 implies that 4 is the largest degree that we can hope to have a cyclic division algebra with a unit γ. There does not exist such an algebra of degree 3. The reason for this is that in every cyclic extension $E/\mathbf{Q}(i)$ of degree 3, all the units of $\mathbf{Q}(i)$ are third powers and therefore are in the image of the norm $N_{E/\mathbf{Q}(i)}$.

In the following we use the generic notation $\mathbf{Q}(i) = F$ and $E = F(a_n)$, where a_n is a zero of the polynomial f_n, and prove that the algebras in Table I are division algebras with minimal discriminants. We refer to these algebras with $\mathcal{D}_i$, where i represents the index of the algebra.

Algebra $\mathcal{D}_2$: The algebra $\mathcal{D}_2$ was previously shown to be a division algebra with a minimal discriminant.

Algebra $\mathcal{D}_4$: When considering $\mathcal{D}_4$ we first have to check whether it really is a division algebra. We note that $(2+i)$ is a totally ramified prime in E/F. Consequently the local extension $\hat{E}_{(2+i)}/\hat{F}_{(2+i)}$ is totally and tamely ramified cyclic extension of degree 4. We note that $\#(\mathcal{O}_{F_{(2+i)}}/(2+i)\mathcal{O}_{F_{(2+i)}}) = \#(\mathcal{O}_F/(2+i)) = 5$.

Proposition 3.6 states that $\mathcal{D}_4$ is a division algebra if i satisfies the norm condition, i.e. -1 is not a norm. While proving this we see at the same time that none of the elements $\{i, -1, -i\}$ is a norm. This demonstrates that the difference between Proposition 3.6 and its more stringent cousins is marginal.

Hasse Norm Theorem [23, Theorem 32.8] states that it is enough to show that the elements $\{i, -1, -i\}$ are not norms in the extension $\hat{E}_{(2+i)}/\hat{F}_{(2+i)}$. Elementary local theory [34, Proposition 7.19] states that if we have any complete residue

system $\{0,1,a,b,c\}$ of the group $\mathcal{O}_{\hat{F}_{(2+i)}}/(2+i)\mathcal{O}_{\hat{F}_{(2+i)}}$ and an arbitrary unit $e \in \hat{F}_{(2+i)}$ then

$$\hat{F}^*_{(2+i)} = \{1,a,b,c\} \times (1+(2+i)\mathcal{O}_{\hat{F}_{(2+i)}}) \times \langle e(2+i)\rangle. \quad (6)$$

The prime $(2+i)$ is tamely ramified in $\hat{E}_{(2+i)}/\hat{F}_{(2+i)}$ and therefore the local conductor is $(2+i)$ (see Lemma 13.7). The definition of the conductor now implies that $(1+(2+i)\mathcal{O}_{F_{2+i}}) \subseteq N_{\hat{E}_{(2+i)}/\hat{F}_{(2+i)}}(\hat{E}_{(2+i)})$. Because the prime $(2+i)$ is totally ramified, we have $e_1(2+i) \subseteq N_{\hat{E}_{(2+i)}/\hat{F}_{(2+i)}}(\hat{E}_{(2+i)})$ for some unit $e_1 \in \hat{F}_{(2+i)}$. The previous results now imply that $(1+(2+i)\mathcal{O}_{E_{(2+i)}}) \times \langle e_1(2+i)\rangle \subseteq N_{\hat{E}_{(2+i)}/\hat{F}_{(2+i)}}(\hat{E}_{(2+i)})$.

On the other hand one of the main theorems of local class field theory [30, Theorem 1.1] states that $\hat{F}^*_{(2+i)}/(N_{\hat{E}_{(2+i)}/\hat{F}_{(2+i)}}(\hat{E}^*_{2+i})) = \mathrm{Gal}(\hat{E}_{(2+i)}/\hat{F}_{(2+i)})$. By considering (6) we see that the elements $\{a,b,c\}$ are not norms. Because the elements $\{0,i,-1,-i,1\}$ form a complete residue system of the group $\mathcal{O}_{\hat{E}_{(2+i)}}/(2+i)\mathcal{O}_{\hat{E}_{(2+i)}}$ we find that none of the elements $\{i,-1,-i\}$ is a norm.

The discriminant of the extension E/F has only two prime divisors $(2+i)$ and $(1+i)$ and therefore also the discriminant of the natural order of $\mathcal{D}_4$ has only two prime divisors. According to Lemma 7.5 this implies that the discriminant of the algebra is minimal.

B. The center $\mathbf{Q}(\sqrt{-3})$

TABLE II
$\mathbf{Q}(\sqrt{-3})$-CENTRAL DIVISION ALGEBRAS WITH A UNIT γ

n	γ	f_n
2	$-\omega$	$x^2+\sqrt{-3}$
3	ω	x^3-2
6	$-\omega^2$	$x^6-3\sqrt{-3}x^4+4x^3-9x^2+12\sqrt{-3}x+3\sqrt{-3}+4$

In Table II we give cyclic generations for algebras of degrees $2,3$, and 6. The theorem of Albert 3.6 shows that 6 is the biggest degree we could hope to have a division algebra with a unit γ. We cannot have a division algebras of degrees 4 and 5 as tensoring these with a division algebra $\mathcal{G}_3$ (below) would give us division algebras of degrees 12 and 15 respectively with a unit γ.

We use the same generic notation as in the case of $\mathbf{Q}(i)$-central algebras expect that we refer to the algebras with $\mathcal{G}_i$, where i represents the index of the algebra.

Algebra $\mathcal{G}_2$: We use here the same methods that were used with the algebra $\mathcal{D}_4$. We remark that $P=(\sqrt{-3})$ is tamely ramified in the extension E/F. If we pass to the completion $\hat{E}_P/\hat{F}_P$ we get that the local conductor is P and that $\{-\omega,1,0\}$ is a complete set of representatives of the group $\mathcal{O}_{\hat{F}_P}/P$. As a result it is seen that $-\omega$ is not a norm in the extension $\hat{E}_P/\hat{F}_P$ and therefore it is not a norm in the extension E/F either. From this it follows that $\mathcal{G}_2$ is a division algebra.

By now it is obvious that the discriminant of the natural order of the algebra $\mathcal{G}_2$ has only two divisors $(\sqrt{-3})$ and (2), and hence the maximal order admits a minimal discriminant.

Algebra $\mathcal{G}_3$: The proof of this case is similar to that of $\mathcal{G}_2$ except that the tamely ramified prime P is 2, and that the suitable set of representatives is $\{1,\omega,\omega^2\}$.

Algebra $\mathcal{G}_6$: The algebra $\mathcal{G}_6$ we get as a tensor product from the algebras $\mathcal{G}_2$ and $\mathcal{G}_3$.

IX. Finding maximal orders

In the previous section, we gave examples of cyclic division algebras with minimal discriminants. One of the interesting features of these algebras is that none of the natural orders is maximal. However, we already saw that in the case of the Golden algebra the natural order is maximal. So clearly natural orders can be maximal. So what is the problem with our algebras? Why we did not construct such algebras that the natural orders would be maximal? The answer is simple: it is impossible. Natural orders can never reach our discriminant bounds. This underlines the fact that, with the previously known methods, the density of our maximal order codes is not achievable. The proof of this result can be found in Section XIII-B in the Appendix.

While these considerations reveal that we have, indeed, constructed something fundamentally new, they also reveal that we have a difficult problem to solve. How to construct maximal orders when the algebra is given? Luckily there exists an algorithm by Ivanyos and Rónyai that solves this problem. In the following we first introduce some algebraic results that will be needed in order to understand the algorithm. Then we present the algorithm and finally, in Section IX-D, we will give some enhancements to this algorithm in a certain special case.

A. The radical and extremal orders

Definition 9.1: Let S denote an arbitrary ring with identity. The *Jacobson radical* of the ring S is the set $\mathrm{Rad}(S) =$

$$\{x \in S \mid xM = 0 \text{ for all simple left } S\text{-modules } M\}.$$

$\mathrm{Rad}(S)$ is a two-sided ideal in S containing every nilpotent (i.e. for which $\mathcal{I}^k = 0$ for some $k \in \mathbf{Z}_+$) one-sided ideal $\mathcal{I}$ of S. Also, $\mathrm{Rad}(S)$ can be characterized as the intersection of the maximal left ideals in S. If S is a finite dimensional algebra over a field or, more generally, left or right Artinian then $\mathrm{Rad}(S)$ is the maximal nilpotent ideal in S.

Definition 9.2: Let us suppose that we have an F-central division algebra of index n and that R is a dedekind ring in F. If M is a *full* R-lattice in $\mathcal{A}$, i.e. $FM=\mathcal{A}$, then the *left order* of M defined as $\mathcal{O}_l(M)=\{x \in \mathcal{A} \mid xM \subseteq M\}$ is an R-order in $\mathcal{A}$. The right order is defined in an analogous way.

The next proposition (see [35, proof of Theorem 3.2]) is useful when computing left orders.

Proposition 9.1: Let $\mathcal{A}$ be a simple algebra over F and M a finitely generated $\mathcal{O}_F$-module such that $FM=\mathcal{A}$. Then there exists an element $s \in \mathcal{O}_F \setminus \{0\}$ such that $s \cdot 1 \in M$. Moreover, $\mathcal{O}_l(M)=\{b \in s^{-1}M \mid bM \leq M\} \leq s^{-1}M$.

Here we need some facts from the local theory of orders. For the basic properties of localization the reader can turn to [36, Chapter 7] or [23, Chapters 1, 2]. For the proofs for the rest of this section, see [21] and [35].

If R is a Dedekind domain with a quotient field F, and P is a prime ideal in R, then the ring of quotients $R_P = (R/P)^{-1}R \subset F$ is a discrete valuation ring. For the R-lattices M in $\mathcal{A}$ the localization at P is defined as $M_P = R_P M \subset \mathcal{A}$. M_P is an R_P-lattice. Moreover, if M is a full (cf. Example 9.2) R-lattice in $\mathcal{A}$, then M_P is a full R_P-lattice in $\mathcal{A}$. To be more specific, let us define the ring $\mathbf{Z}_p$.

Definition 9.3: For a rational prime p let $\mathbf{Z}_p$ denote the ring

$$\mathbf{Z}_p = \{\frac{r}{s} \in \mathbf{Q} \mid r, s \in \mathbf{Z},\ gcd(p, s) = 1\}.$$

$\mathbf{Z}_p$ is a discrete valuation ring with the unique maximal ideal $p\mathbf{Z}_p$. If Λ is a $\mathbf{Z}$-order we use the notation $\Lambda_p = \mathbf{Z}_p\Lambda$.

We remark that one should not confuse the localization R_P with the ring of integers $\hat{R}_P$ of the P-adic completion. We use the caret to indicate a complete structure. This is somewhat non-standard in the case of $\mathbf{Z}_p$ that is nearly universally used to denote the complete ring of p-adic integers. We use $\hat{\mathbf{Z}}_p$ for the complete ring.

In the following, we work inside an F-central division algebra $\mathcal{A}$, R being the ring of algebraic integers in F. The next statement illustrates a simple but useful connection between the orders Λ and Λ_P.

Proposition 9.2 (Proposition 2.8 [21]): Let Λ be a R-order in $\mathcal{A}$. The map $f : x \mapsto x + P\Lambda_P$, $x \in \Lambda$ induces an isomorphism of the rings $\Lambda/P\Lambda \cong \Lambda_P/P\Lambda_P$.

Proposition 9.3 (Proposition 3.1 [21]): Let P be a prime ideal of the ring R. The residue class ring $\overline{\Lambda_P} = \Lambda_P/P\Lambda_P$ is an algebra with identity element over the residue class field $\overline{R_P} = R_P/PR_P$ and $dim_F\mathcal{A} = dim_{\overline{R_P}}\overline{\Lambda_P}$. If $\phi : \Lambda_P \to \overline{\Lambda_P}$ is the canonical epimorphism, then $P\Lambda_P \subseteq \mathrm{Rad}(\Lambda_P) = \phi^{-1}\,\mathrm{Rad}(\overline{\Lambda_P})$ and ϕ induces a ring isomorphism $\Lambda_P/\,\mathrm{Rad}(\Lambda_P) \cong \overline{\Lambda_P}/\,\mathrm{Rad}(\overline{\Lambda_P})$. As a consequence, a left (or right) ideal $\mathcal{I}$ of Λ_P is contained in $\mathrm{Rad}(\Lambda_P)$ if and only if there exists a positive integer t such that $\mathcal{I}^t \subseteq P\Lambda_P$.

Combining the last two results we get.

Corollary 9.4: Let P be a prime ideal of the ring R. We then have

$$\phi^{-1}(\mathrm{Rad}(\Lambda/P\Lambda)) = \psi^{-1}(\mathrm{Rad}(\Lambda_P)),$$

where ψ is the embedding $\Lambda \mapsto \Lambda_P$ and ϕ is the canonical epimorphism $\Lambda \to \Lambda/P\Lambda$.

The following facts establish some practical connections between the local and global properties of orders.

Proposition 9.5 (Theorem 2.3 [35]): Let $\mathcal{A}$ be a simple algebra over F. Let P be a prime ideal of R, and Γ be an R-order in $\mathcal{A}$. Then

(i) Γ_P is an R_P-order in $\mathcal{A}$.

(ii) Γ is a maximal R-order in $\mathcal{A}$ if and only if Γ_P is a maximal R_P-order in $\mathcal{A}$ for every prime ideal P of R.

(iii) $d(\Gamma/R)_P = d(\Gamma_P/R_P)$.

Corollary 9.6: If P does not divide $d(\Lambda/R)$, then Λ_P is maximal R_P-order.

Proof: According to previous proposition we always have $d(\Gamma/R)R_P = d(\Gamma_P/R_P)$. On the other hand we supposed that $P \nmid d(\Lambda/R)$ resulting that $d(\Gamma_P/R_P) = d(\Lambda/R)R_P = R_P$. Lemma 3.12 then imply that Λ_P is maximal. ■

Extremal orders and especially Proposition 9.10 below play a key role in the method for constructing maximal orders.

Definition 9.4: We say that Γ_P radically contains Λ_P if and only if $\Lambda_P \subseteq \Gamma_P$ and $\mathrm{Rad}(\Lambda_P) \subseteq \mathrm{Rad}(\Gamma_P)$. The orders maximal with respect to this partial ordering are called *extremal*. Maximal orders are obviously extremal.

Proposition 9.7 (Proposition 4.1 [21]): An R_P-order Λ_P is extremal if and only if $\Lambda_P = \mathcal{O}_l(\mathrm{Rad}(\Lambda_P))$.

Lemma 9.8 (Lemma 2.7 [21]): Let P be a prime ideal of the ring R, Λ an R-order and suppose that $\mathcal{O}_l(\mathrm{Rad}(\Lambda_P)) \supset \Lambda_P$. Let I denote the inverse image of $\mathrm{Rad}(\Lambda_P)$ with respect to the embedding $\Lambda \mapsto \Lambda_P$. Then we have $I \supseteq P\Lambda$ and $\mathcal{O}_l(I) \supset \Lambda$.

The previous corollary together with Corollary 9.4 gives us the following.

Lemma 9.9: If $\mathcal{O}_l(\phi^{-1}(\mathrm{Rad}(\Lambda/P\Lambda)) = \Lambda$, the order Λ_P is extremal.

Proposition 9.10 (Theorem 4.5 [21]): Let $\Lambda_P \subset \Gamma_P$ be R_P-orders in $\mathcal{A}$. Suppose that Λ_P is extremal and that Γ_P is minimal among the R_P-orders properly containing Λ_P. Then there exists an ideal $\mathcal{J}$ of Λ_P minimal among those containing $\mathrm{Rad}(\Lambda_P)$ such that $\mathcal{O}_l(\mathcal{J}) \supseteq \Gamma_P$.

B. The algorithm

Consider again the family of cyclic division algebras $\mathcal{A}_\ell$ of index $n = 2^{\ell-2}$ from Example 5.2. If Λ_ℓ is a maximal order of $\mathcal{A}_\ell$, then according to Corollary 7.6

$$d(\Lambda_\ell/\mathbf{Z}[i]) = (1+i)^{n(n-1)}(2+i)^{n(n-1)}.$$

On the other hand, by Lemma 5.4 we see that the discriminant of the natural order $\Lambda_{\ell,nat}$ of $\mathcal{A}_\ell$ is

$$d(\Lambda_{\ell,nat}/\mathbf{Z}[i]) = (1+i)^{\ell(n/2)n}(2+i)^{n(n-1)}.$$

Hence, we may conclude that the natural order is of index

$$[\Lambda_\ell : \Lambda_{\ell,nat}] = 2^{((2\ell-5)n+1)n/2}.$$

In the cases $\ell = 3, 4, 5$ this index thus equals 2^3, 2^{26}, and 2^{164}, respectively. In other words, using a maximal order as opposed to the natural order one can send 1.5, 6.5, or 20.5 more bits per channel use without compromising neither the transmission power nor the minimum determinant in the respective cases of 2, 4, or 8 antennas! Hence the problem of actually finding these maximal orders rather than simply knowing that they exist becomes quite relevant. In the following we shortly depict how maximal orders can be constructed in general. A more detailed version of the algorithm can be found in [21].

Let again F be an algebraic number field, $\mathcal{A}$ a finite dimensional central simple algebra over F, and Λ be a $\mathcal{O}_F$-order in $\mathcal{A}$. To avoid overcomplicated notation we use shorthand $\mathcal{O}_F = R$. Assume that $\mathcal{A}$ is given by relations (e.g. $u^2 = \gamma$), and that Λ is given by a R-basis. For instance, we can always start with the natural order Λ (cf. Example 3.2). We form a set $S = \{P_1, ..., P_r\}$ consisting of the prime ideals dividing $d(\Lambda)$. According to Corollary 9.6 Λ_P is a maximal R_P-order if $P \notin S$.

The basic idea of the algorithm is to test for $i = 1, ..., r$ whether Λ is maximal at P_i. If the answer is yes, Λ is a maximal R-order. If not, then at the first index i for which Λ_{P_i} is not maximal we can construct a R-order Γ in $\mathcal{A}$ such

that $\Lambda_{P_i} \subset \Gamma_{P_i}$, and hence $\Lambda \subset \Gamma$ (cf. Propositions 9.2–9.10). This can basically be done in two steps. Let $P \in S$ and let ϕ be the canonical reduction map $\Lambda \mapsto \Lambda/P\Lambda$.

STEP 1 REPEAT UNTIL "YES": Compute $\mathcal{I} = \phi^{-1}(\mathrm{Rad}(\Lambda/P\Lambda)) \leq \Lambda$. Does the equality $\mathcal{O}_l(\mathcal{I}) = \Lambda$ hold?

"NO": $\mathcal{O}_l(\mathcal{I}) \supset \Lambda$

$\Lambda \leftarrow \mathcal{O}_l(\mathcal{I})$ (Iteration step)

STEP 2 REPEAT UNTIL "NO": Compute the minimal ideals $\mathcal{J}_1, \mathcal{J}_2, ..., \mathcal{J}_h$ ($h < dim_{\mathbf{Q}}\mathcal{A}$) of $\Lambda/P\Lambda$ which contain $\mathrm{Rad}(\Lambda/P\Lambda)$. FOR $i = 1, ..., h$ compute $\mathcal{I}_i = \phi^{-1}(\mathcal{J}_i)$. Does there exist an index i for which $\mathcal{O}_l(\mathcal{I}_i) > \Lambda$?

"YES": $\Lambda \leftarrow \mathcal{O}_l(\mathcal{I}_i)$ (Iteration step)

"NO": OUTPUT Λ is a maximal $\mathcal{O}_F$-order.

Let $P \in S$. First we test whether Λ_P is an extremal (cf. Definition 9.4) R_P-order by using Lemma 9.9. If not, then we shall construct an R-order $\Gamma > \Lambda$. If Λ_P passes this test, then we can use the test of Proposition 9.10. If there exists an ideal $\mathcal{J}$ minimal among the ideals properly containing $\mathrm{Rad}(\Lambda_P)$ such that $\mathcal{O}_l(\mathcal{J}) > \Lambda_P$, then we construct an R-order $\Gamma > \Lambda$. Otherwise we correctly conclude that Λ is maximal at P and continue with the next P in the list S. In the end, the algorithm yields an R-order Λ which is now maximal. The algorithm can be used similarly for constructing $\mathbf{Z}$-orders, and in the MAGMA software the implementations are for $\mathbf{Z}$-orders only.

For more details concerning the computation of the prime ideals in a ring, see [35]. A thorough explanation and an algorithm for computing the radical can be found in [37].

Remark 9.1: According to Lemma 9.4 we could have as well defined the ideal $\mathcal{I}$ by $\mathcal{I} = \psi^{-1}(\mathrm{Rad}(\Lambda_P)$. This interpretation will be used in Section IX-D.

Let us next exemplify the above algorithm.

C. A 2×2 construction over $\mathbf{Z}[i]$

In the Golden division algebra (cf. Example 3.1 or [3]), i.e. the cyclic algebra $\mathcal{GA} = (E/F, \sigma, \gamma)$ obtained from the data $E = \mathbf{Q}(i, \sqrt{5})$, $F = Q(i)$, $\gamma = i$, $n = 2$, $\sigma(\sqrt{5}) = -\sqrt{5}$, the natural order Λ is already maximal. The norm of the discriminant of Λ (with respect to $\mathbf{Q}$) is 625, whereas the norm of the minimal discriminant is 100 [32]. We will now present a code constructed from a maximal order of the cyclic division algebra $\mathcal{GA}+$ of Example 7.4. The maximal order of $\mathcal{GA}+$ also admits the minimal discriminant and is in that sense optimal. The algorithm now proceeds as follows.

The natural order of the algebra $\mathcal{GA}+$ is $\Lambda = \mathbf{Z}[i] \oplus u'\mathbf{Z}[i] \oplus \lambda\mathbf{Z}[i] \oplus u'\lambda\mathbf{Z}[i]$. Hereafter, we will use a shorter notation $\Lambda = \langle 1, u', \lambda, u'\lambda \rangle_{\mathbf{Z}[i]}$ for this. Let us consider Λ at the place $P = 1 + i$ as it is the only factor of the discriminant for which we can enlarge Λ. The inverse image of the radical (9.3) is $\mathcal{J} = \phi^{-1}(\mathrm{Rad}(\Lambda/P\Lambda)) = \phi^{-1}(\langle 1 + u', 1 + \lambda, 1 + u'\lambda \rangle_{\mathbf{Z}_2}) = \langle 1 + i, 1 + u', 1 + \lambda, 1 + u'\lambda \rangle_{\mathbf{Z}[i]} \subset \Lambda$. A straightforward computation shows us (cf. Proposition 9.1) that the element

$$\rho = \frac{1 + u' + \lambda + u'\lambda}{1 + i} = \frac{(1 + u')(1 + \lambda)}{1 + i} \in \mathcal{O}_l(\mathcal{J}),$$

which means that the answer to the question in STEP 1 is "NO", and hence we set $\Lambda' = \langle 1, u', \lambda, \rho \rangle_{\mathbf{Z}[i]}$ and iterate. This time the inverse image of the radical is $\mathcal{J}' = \phi^{-1}(\mathrm{Rad}(\Lambda'/P\Lambda')) = \phi^{-1}(\langle 1 + u', 1 + \lambda, 1 + \rho \rangle_{\mathbf{Z}_2}) = \langle 1 + i, 1 + u', 1 + \lambda, 1 + \rho \rangle_{\mathbf{Z}[i]} \subset \Lambda'$. By taking the element

$$\tau = \frac{u' + \lambda}{1 + i} \in \mathcal{O}_l(\mathcal{J}')$$

we can again enlarge the order Λ' to $\Lambda'' = \langle 1, u', \tau, \rho \rangle_{\mathbf{Z}[i]}$ and compute $\mathcal{J}'' = \phi^{-1}(\mathrm{Rad}(\Lambda''/P\Lambda'')) = \phi^{-1}(\langle 1 + u', 1 + \rho, \tau \rangle_{\mathbf{Z}_2}) = \langle 1 + i, 1 + u', 1 + \rho, \tau \rangle_{\mathbf{Z}[i]} \subset \Lambda''$. We need one more iteration of STEP 1. Now the element

$$\nu = \frac{(1 + u')(u' + \lambda)}{2} \in \mathcal{O}_l(\mathcal{J}'')$$

and the order Λ'' is enlarged to $\Lambda''' = \langle 1, \tau, \rho, \nu \rangle_{\mathbf{Z}[i]}$. From this iteration we finally get the answer to be "YES".

In STEP 2 there is nothing to do, as the only minimal ideal properly containing the radical is the radical itself. Hence we have constructed a maximal $\mathbf{Z}[i]$-order of $\mathcal{GA}+$ with a $\mathbf{Z}[i]$-basis $\{1, \tau, \rho, \nu\}$.

In order to give a concrete description of this order we describe it in terms of its $\mathbf{Z}[i]$-basis. Let us again denote by λ the first quadrant square root of $2 + i$. The maximal order Λ consists of the matrices $aM_1 + bM_2 + cM_3 + dM_4$, where a, b, c, d are arbitrary Gaussian integers and $M_i, i = 1, 2, 3, 4$ are the following matrices.

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix},$$

$$M_3 = \frac{1}{2}\begin{pmatrix} i + i\lambda & i - \lambda \\ -1 + i\lambda & i - i\lambda \end{pmatrix},$$

$$M_4 = \frac{1}{2}\begin{pmatrix} -1 - i\lambda & i + i\lambda \\ -1 + \lambda & -1 + i\lambda \end{pmatrix}.$$

D. Enhancements to the Ivanyos–Rónyai algorithm in certain special cases

The memory requirements of the above algorithm grow quite rapidly as a function of the dimension of the algebra. For example the MAGMA-implementation runs out of memory on a typical modern PC, when given the index 8 cyclic algebra $\mathcal{A}_5$ of Example 5.2 as an input.

In this subsection, we describe an algorithm that finds maximal orders for the algebras $\mathcal{A}_\ell$. It is an adaptation of the Ivanyos–Rónyai algorithm that utilizes several facts special to this family of algebras, and thus its applicability is rather limited. We list these simple facts in the following lemmas. We will denote $\mathbf{Z}[\zeta_\ell]$ by $\mathcal{O}$ for short.

Lemma 9.11: The only prime ideal of $\mathcal{O}$ that lies above the prime 2 is the principal ideal P_ℓ generated by $1 - \zeta_\ell$.

Lemma 9.12: Let M be a finitely generated free $\mathcal{O}$-module of rank k, and let and $m_1, \ldots, m_k$ be a basis. Let N be a submodule of M such that the index $[M : N]$ is a power of two (in particular this index is finite). Then N is also a free $\mathcal{O}$-module of rank k, and we can find a basis of N of the form

$$n_i = \sum_{j \leq i} a_{ij} m_j \quad , a_{ij} \in \mathcal{O}.$$

Proof: This is a straightforward modification of the standard proof of the corresponding result for modules over a PID. We first define the submodules N_t for all $t = 0, 1, \ldots k$

as consisting of those elements of N whose $(k-t)$ last coordinates vanish,

$$N_t = N \cap \sum_{j=1}^{t} \mathcal{O} m_j.$$

Clearly $N_k = N$ and $N_0 = 0$. The idea is to sequentially produce elements $n_k, n_{k-1}, \ldots, n_1$ in such a way that at each step the following two conditions are satisfied

1) for all $j > 0$, we have $n_j \in N_j$,
2) $N = N_t \oplus \sum_{j>t} \mathcal{O} n_j$.

We proceed by descending induction, so assume that we have already produced $n_k, \ldots, n_{t+1}$, and we next work on finding an element n_t (so t is a fixed index in the range $0 < t \leq k$). Consider the module $N_t^+ = N_t \oplus \sum_{j>t} \mathcal{O} m_j$. Clearly $N \subseteq N_t^+ \subseteq M$, so N_t^+ is also of a finite index in M, and $[M : N_t^+]$ is also a power of two. Consider the homomorphism $f_t : M \to \mathcal{O}$ that maps the element $\sum_j a_j m_j$ to the coordinate a_t. Write $I_t = f_t(N_t) = f_t(N_t^+)$. Because f_t is onto, we get a surjective homomorphism from M/N_t^+ onto $\mathcal{O}/I_t$. Therefore the index of the ideal I_t in $\mathcal{O}$ is also a power of two, and by Lemma 9.11, I_t is a principal ideal generated by a single element $y_t \in \mathcal{O}$. Set $a_{tt} = y_t$. We may thus choose an element $n_t \in N_t$ such that $f_t(n_t) = y_t$, so $n_t = a_{tt} m_t + \sum_{j<t} a_{tj} m_j$ for some elements $a_{tj} \in \mathcal{O}$. If $x = \sum_{j \leq t} b_j m_j$ is any element of N_t, then $b_t = b y_t$ for some $b \in \mathcal{O}$. Therefore $x - b n_t \in N_{t-1}$, and because $\mathcal{O}$ is an integral domain this implies that $N_t = N_{t-1} \oplus \mathcal{O} n_t$. Together with the induction hypothesis $N = N_t \oplus \sum_{j>t} \mathcal{O} n_j$ this implies the induction claim $N = N_{t-1} \oplus \sum_{j>t-1} \mathcal{O} n_j$.

In the end we get (because $N_0 = 0$) $N = \sum_{j=1}^{k} \mathcal{O} n_j$, so the elements $n_j, j = 1, \ldots, k$, generate the module N. Because the matrix (a_{ij}) is lower triangular, and the set $\{m_1, m_2, \ldots, m_k\}$ was assumed to be linearly independent, the set $\{n_1, n_2, \ldots, n_k\}$ is also linearly independent over the integral domain $\mathcal{O}$. Thus N is a free $\mathcal{O}$-module. ∎

Corollary 9.13: The maximal order Λ_ℓ of $\mathcal{A}_\ell$ is a free $\mathcal{O}$-module of rank $n = 2^{\ell-2}$.

Proof: We already know that Λ_ℓ contains $\Lambda_{\ell,nat}$ as a submodule of a finite index. Thus, there exists an integer $M > 0$ with the property that $M\Lambda_\ell$ is a submodule of a finite index in $\Lambda_{\ell,nat}$. The formula for the discriminants tells us that we can further select the multiplier M to be a power of two. Clearly, it suffices to prove that $M\Lambda_\ell$ is a free module of the right rank. As the natural order, obviously, is a free $\mathcal{O}$-module of rank n, this is a consequence of Lemma 9.12. ∎

Let then Γ be any *intermediate order*, i.e. any order with the property $\Lambda_{\ell,nat} \subseteq \Gamma \subseteq \Lambda_\ell$. We will denote by Γ_2 the ring obtained by localizing Γ at the prime $1+i$. This is naturally a subring of the corresponding localized version of the maximal order and consequently also of the completion of the maximal order $\hat{\Lambda}_\ell$. This latter ring is a $\mathbf{Z}_2[i]$-order in the completion of the central simple $\mathbf{Q}_2(i)$-algebra $\hat{\mathcal{A}}_\ell$ obtained from $\mathcal{A}_\ell$ by extending its scalars to the complete field $\mathbf{Q}_2(i)$. Because the algebra $\mathcal{A}_\ell$ has a full local index $2^{\ell-2}$ at the prime $1+i$, $\hat{\mathcal{A}}_\ell$ is actually a division algebra. By [23, Theorem 12.8] and the surrounding discussion therein we know that $\hat{\Lambda}_\ell$ is a non-commutative discrete valuation ring, and that the $(1+i)$-adic valuation of the reduced norm serves as a valuation. E.g. it yields a metric subject to the non-archimedean triangle inequality. So in the matrix representation the valuation of the determinant distinguishes the units from the non-units in the ring $\hat{\Lambda}_\ell$. We immediately see that the same then holds in the ring Γ_2 — the units are precisely the elements whose reduced norm is a $(1+i)$-adic unit. By the non-archimedean triangle inequality the non-units of Γ_2 then form its unique maximal ideal, which is then also the radical $\mathrm{Rad}(\Gamma_2)$.

We distill the following two lemmas from the previous discussion.

Lemma 9.14: Suppose that $\mathcal{A}$ is an F-central division algebra of index n and that Λ is an order in $\mathcal{A}$. If $\mathcal{A} \otimes_F \hat{F}_P$ is a division algebra, then Λ_P has a unique maximal ideal $\mathrm{Rad}\,\Lambda_P$.

Proof: The only open question that was left open in the previous discussion, is whether all the elements in Λ_P whose reduced norm is a P-adic unit are really units in Λ_P. This is true in the maximal order Λ'_P that includes Λ_P, because $\Lambda'_P = \mathcal{A} \cap \hat{\Lambda}'_P$, where $\hat{\Lambda}'_P$ is the maximal order in the division algebra $\mathcal{A} \otimes_F \hat{F}_P$. The claim now follows from [23, Exercise 4, Section 25]. ∎

The following Lemma is the key to our modifications to Step 1 in the main algorithm.

Lemma 9.15: Let Γ be any intermediate order. The ideal $\mathcal{I} = \Gamma \cap \mathrm{Rad}(\Gamma_2)$ consists of exactly those matrices which determinants are divisible by $1+i$.

The following lemma is a simple reformulation of the fact that P_ℓ is of index 2 in $\mathcal{O}$. It will allow us to reduce the range of certain searches from $\mathcal{O}$ to the set $\{0, 1\}$.

Lemma 9.16: Assume that $p(x) = \sum_{i=0}^{k} p_i x^i \in \mathbf{Z}[x]$. Then

$$p(\zeta_\ell) \equiv p_0 + p_1 + \cdots + p_k \pmod{P_\ell}.$$

Let us denote by s_ℓ the complex number

$$s_\ell = \frac{1}{1-\zeta_\ell} = \frac{1+i}{2}\left(1 + \zeta_\ell + \zeta_\ell^2 + \cdots + \zeta_\ell^{n-1}\right).$$

The fractional ideal generated by s_ℓ is then P_ℓ^{-1}.

Proposition 9.17: Let Γ be an intermediate order. Assume that it is a free $\mathcal{O}$-module, and that $g_1, g_2, \ldots, g_n$ is its basis. Let $I = \psi^{-1}(\mathrm{Rad}(\Gamma_2))$ (cf. STEP 1). Then I is also a free $\mathcal{O}$-module of rank n that satisfies $\Gamma \subseteq s_\ell I$. We can find a basis for I that is of the form $r_1, r_2, \ldots, r_n$, where for all i either

$$r_i = g_i + \sum_{j<i} \epsilon_{ij} g_j,$$

such that all the coefficients $\epsilon_{ij} \in \{0, 1\}$, or

$$r_i = (1 - \zeta_\ell) g_i.$$

Proof: Any element of Γ has determinant (= its reduced norm) in $\mathbf{Z}[i]$. The reduced norm of $1 - \zeta_\ell$ is an associate of $1+i$. Therefore $(1-\zeta_\ell)\Gamma \subseteq I \subseteq \Gamma$. Thus the index of I in Γ is a power of two. Hence Lemma 9.12 implies that I is a free $\mathcal{O}$-module of rank n. With the notation of Lemma 9.12 we also see that the coefficient y_n is always either 1 or $1 - \zeta_\ell$. In the former case Lemma 9.16 and the fact that $2 \in P_\ell$ allow us to choose the coefficients ϵ_{ij} as required. In the latter case we

have no reason not to choose $r_i = (1-\zeta_\ell)g_i$ as this element is in I by Lemma 9.15. ∎

Proposition 9.18: Let Γ, I, and the bases $g_1,\dots,g_n$ and $r_1,\dots,r_n$ be as in the previous proposition. Then the left order $\Gamma' = \mathcal{O}_\ell(I)$ is a free $\mathcal{O}$-module contained in $s_\ell\Gamma$. It has a basis $g'_1,\dots,g'_n$, where for all i either

$$g'_i = s_\ell(g_i + \sum_{j<i}\epsilon_{ij}g_j),$$

such that all the coefficients $\epsilon_{ij} \in \{0,1\}$, or

$$g'_i = g_i.$$

Proof: The inclusion $(1-\zeta_\ell)\Gamma \subseteq I$ immediately shows that $\Gamma \subseteq \mathcal{O}_\ell(I) \subseteq s_\ell\Gamma$. Therefore the index of $(1-\zeta_\ell)\Gamma'$ in Γ is a power of two. Again Lemma 9.12 shows that Γ' is a free $\mathcal{O}$-module. We also have the inclusion $(1-\zeta_\ell)\Gamma' \subseteq \Gamma$. An argument similar to the one in the proof of the previous proposition then shows that the algorithm in the proof of Lemma 9.12 yields a basis of the prescribed type. ∎

When we use the natural order Λ_{nat} of the algebra $\mathcal{A}_\ell$ as a starting point, the known discriminants of $\mathcal{A}_\ell$ and the maximal order Λ_{max} tell us that the index $[\Lambda_{max} : \Lambda_{nat}]$ is a power of two. Therefore $p = 1+i$ is the only interesting prime in Step 1 of the main algorithm. This step can now be completed simply by letting Γ to be the natural order, and $g_1,\dots,g_n$ to be its $\mathcal{O}$-module basis. We next find a basis for I by testing, whether any element of the type $r_i = g_i + \sum_{j<i}\epsilon_{ij}g_j$ has a determinant divisible by $1+i$ (and if no such element is found then including $r_i = (1-\zeta_\ell)g_i$ into the basis instead). We then proceed to compute an $\mathcal{O}$-module basis for the left order Γ' of this I. Again we simply check, whether any elements of the form $g'_i = s_\ell(g_i + \sum_{j<i}\epsilon_{ij}g_j)$ belong to Γ'. Observe that it suffices to test a candidate of this form against the basis elements r_i only. If such an element is found, we record that Γ' will be strictly larger than Γ. If no such element is found, we use $g'_i = g_i$ instead. After we have done this for all i, we will know, whether $\Gamma' = \Gamma$. If this is the case, we are done. Otherwise we replace Γ with Γ' and repeat the process.

Now we have taken care of the STEP 1 and we know that $\Gamma_{(1+i)}$ is an extremal order. Luckily for us STEP 2 is not needed as $\Gamma_{(1+i)}$ is actually maximal. We describe the proof shortly. We will use the term hereditary without defining it. First, [23, Theorem 39.25 and the following remark] states that $\Gamma_{(1+i)}$ is hereditary. Lemma 9.14 gives us that $\operatorname{Rad}\Gamma_{(1+i)}$ is the unique maximal two-sided ideal in $\Gamma_{(1+i)}$. Theorem 18.4 in [23] then states that under these conditions $\Gamma_{(1+i)}$ is a maximal order.

We implemented this on the computer algebra system Mathematica, and on a typical modern PC it found a maximal order in the case $\ell = 5$ in less than half an hour. We believe that the memory savings due to the use of $\mathcal{O}$-bases as opposed to $\mathbf{Z}$-bases in the general purpose implementation in MAGMA account for this enhancement in the performance of the algorithm. This algorithm could naturally be ported into any CAS to handle these very specific cases.

Example 9.1: Assume that we have the 4 antenna case $\ell = 4$. Let us denote $s = s_\ell$ in short. In this case, the above algorithm yields an order with (left) $\mathcal{O}$-basis consisting of the elements $u_1,\dots,u_4$:

$$\begin{aligned}
u_1 &= 1,\\
u_2 &= (s^2+s^3) + us^3,\\
u_3 &= (s^4+2s^5+2s^6+s^8+s^{10}) + u(s^5+s^6) + u^2s^{10},\\
u_4 &= (s+s^4+s^5+s^8+s^9+s^{10}+s^{11}+s^{12}+s^{13})\\
&\quad + u(s^9+s^{11}+s^{13}) + u^2(s^{12}+s^{13}) + u^3s^{13}.
\end{aligned}$$

We observe that the highest powers of s appearing in these basis elements are $0, 3, 10$, and 13, respectively. This fits well together with our earlier calculation showing that the index of the natural order in a maximal one is 2^{26}. The number s^{-1} generates the prime ideal lying above 2, and $0+3+10+13 = 26$.

It is a basic fact from the theory of the cyclotomic rings of integers that the conjugate of the element s is of the form $\sigma(s) = u_\sigma s$, where u_σ is a unit of the ring $\mathbf{Z}[\zeta]$. Using this observation and the relation $us = \sigma(s)u$ we see that, instead of the generator u_4 above, we could use the product u_2u_3. After all, the $\mathcal{O}$-module spanned by these elements is an order, so we can utilize the fact that it is closed under multiplication.

Example 9.2: In the 8 antenna case $\ell = 5$ we get a free $\mathcal{O}$-module of rank 8 as a maximal order. The basis elements $u_1,\dots,u_8$ are similar linear combinations of $1, u, u^2, \dots, u^7$ with coefficients of the form $p(s)$, where $p(x) \in \mathbf{Z}[x]$ and $s = s_\ell$. In this case, the polynomial coefficients of the various basis elements have maximal degrees 0, 3, 10, 13, 28, 31, 38 and 41. As expected, these degrees sum up to 164. Taking advantage of the fact that this module is also a ring we can describe the elements of the basis by

$$\begin{aligned}
u_1 &= 1,\\
u_2 &= (s^2+s^3) + us^3,\\
u_3 &= (s+s^2+s^4+2s^5+2s^6+s^8+s^{10})\\
&\quad + u(s^5+s^6) + u^2s^{10},\\
u_4 &= u_2u_3,\\
u_5 &= s+2s^2+s^3+2s^4+5s^5+8s^6+8s^7+3s^8\\
&\quad + 5s^9+6s^{10}+5s^{11}+7s^{12}+6s^{13}+7s^{14}\\
&\quad + 4s^{15}+5s^{16}+2s^{18}+2s^{20}+s^{24}+s^{28}\\
&\quad + u\big(s^5+2s^6+4s^7+s^8+s^9+s^{10}+2s^{11}+2s^{12}\\
&\quad + 3s^{13}+3s^{14}+s^{15}+3s^{16}\big)\\
&\quad + u^2\big(s^{11}+2s^{14}+2s^{15}+s^{16}+s^{18}+s^{20}\big)\\
&\quad + u^3\big(s^{15}+s^{16}\big) + u^4s^{28},\\
u_6 &= u_2u_5,\\
u_7 &= u_3u_5,\\
u_8 &= u_2u_3u_5.
\end{aligned}$$

X. Analysis of the Perfect Algebras

In the following we will analyze the perfect codes of [10]. Specifically, we are going to discuss the structure of the underlying algebras. In order to do so, we have to prove some results that allow us to use our previous machinery also in this situation.

The following simple fact (also known to E. Viterbo, private communication) explains why using a principal one-sided (left or right) ideal instead of the entire order will not change the density or normalized minimum determinant of the code.

Lemma 10.1: Let Λ be an order in a cyclic division algebra of index n over an imaginary quadratic number field. Let $x \in \Lambda$ be any non-zero element. Then

$$\delta(\Lambda x) = \delta(\Lambda).$$

Proof: By the multiplicativity of the norm the minimum determinant of Λx is equal to the absolute value of $nr_{\mathcal{A}/F}(x)$. Let us now determine how the fundamental parallelotope of Λx is related to the fundamental parallelotope of Λ.

We have that $[\Lambda : \Lambda x] = |N_{\mathcal{A}/F}(x)|$ (see [23, Exercise 7, p. 131]). On the other hand [23, Theorem 9.14, p. 119] tells us that

$$\begin{aligned} |N_{\mathcal{A}/\mathbf{Q}}(x)| &= |N_{F/\mathbf{Q}}(N_{\mathcal{A}/\mathbf{F}}(x))| \\ &\overset{\text{Remark 3.3}}{=} |N_{F/\mathbf{Q}}((nr_{\mathcal{A}/F}(x))^n)| \\ &\overset{[F:\mathbf{Q}]=2}{=} |nr_{\mathcal{A}/F}(x)^n|^2 \\ &= |nr_{\mathcal{A}/F}(x)|^{2n}. \end{aligned}$$

Hence, $[\Lambda : \Lambda x] = |nr_{\mathcal{A}/F}(x)|^{2n}$. This implies

$$m(\Lambda)|nr_{\mathcal{A}/F}(x)|^{2n} = m(x\Lambda),$$

and therefore

$$\delta(\Lambda x) = \frac{|nr_{\mathcal{A}/F}(x)|}{(m(\Lambda x))^{1/2n}} = \frac{1}{(m(\Lambda))^{1/2n}} = \delta(\Lambda).$$

■

We remark that the same fact obviously also holds for principal left ideals of a maximal order.

Proposition 10.2: Let $\mathcal{D}_1 = (E_1/F, \sigma_1, \gamma_1)$ and $\mathcal{D}_2 = (E_2/F, \sigma_2, \gamma_2)$ be division algebras that have coprime indices m_1 and m_2. Then $\mathcal{D}_1 \otimes \mathcal{D}_2$ is a division algebra with an index $m_1 m_2$. Furthermore,

$$\mathcal{D}_1 \otimes \mathcal{D}_2 \simeq (E_1E_2/F, \sigma_1\sigma_2, \gamma_1^{m_2}\gamma_2^{m_1}),$$

where $\sigma_1\sigma_2$ is an element of $\mathrm{Gal}(E_1E_2/F) \simeq \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$.

Let P_1 and P_2 be some pair of minimal prime ideals of the field F. If $\mathcal{D}_1$ and $\mathcal{D}_2$ have minimal discriminants that are only divisible by P_1 and P_2, then $\mathcal{D}_1 \otimes \mathcal{D}_2$ has a minimal discriminant that is only divisible by P_1 and P_2.

Proof: For the proof of the first two claims we refer the reader to [26, Theorem 20, p. 99]. The only nontrivial Hasse invariants of the division algebras $\mathcal{D}_1$ and $\mathcal{D}_2$ are those associated with the primes P_1 and P_2. The mappings in the fundamental exact sequence (4) are homomorphisms of groups. Together with the fact that extending scalars to a P-adic completion commutes with the formation of a tensor product shows that the Hasse invariants of $\mathcal{D}_1 \otimes \mathcal{D}_2$ are sums of those of $\mathcal{D}_1$ and $\mathcal{D}_2$. Hence, the discriminant of $\mathcal{D}_1 \otimes \mathcal{D}_2$ is only divisible by the prime ideals P_1 and P_2. By the proof of Theorem 6.12 it is then minimal. ■

Suppose we have a finite cyclic extension E/F of algebraic number fields. Let P be a prime of F and B some prime of E that lies over P. We denote the completion E_B by E_P or $E \cdot \hat{F}_P$. This notation is valid in Galois extensions, because the fields E_B are isomorphic for all primes B that lie over P.

In the following we give an algebraic analysis of perfect codes. The resulting numerical data is collected into Table III.

1) The 2×2 Perfect code: The first perfect algebra is the same as the Golden algebra $\mathcal{GA} = (E/F, \sigma, \gamma)$, where the extension $E/F = \mathbf{Q}(i, \sqrt{5})/\mathbf{Q}(i)$ has discriminant $(2+i)(2-i)$. The discriminant of the natural order is therefore $(2+i)^2(2-i)^2$. Because the discriminant of the algebra $\mathcal{GA}$ divides $(2+i)^2(2-i)^2$ it can have at maximum two prime divisors $(2+i)$ and $(2-i)$. As a consequence the only Hasse invariants that can be nontrivial are $h_{(2+i)}$ and $h_{(2-i)}$.

The algebra $\mathcal{GA}$ must have at least two nontrivial Hasse invariants and therefore $h_{(2+i)}$ and $h_{(2-i)}$ are both nontrivial. Combining the equations

$$LCM[m_{(2+i)}, m_{(2-i)}] = 2$$

and $h_{(2+i)} + h_{(2-i)} = 1$ we get that $h_{(2+i)} = h_{(2-i)} = 1/2$. Theorem 6.11 states that the discriminant of $\mathcal{GA}$ is $(2+i)^2(2-i)^2$. Comparing this to the discriminant of the natural order we see that the natural order Λ_2 is maximal. The actual code is then

$$B_2 = \frac{1}{c}\Lambda_2 a$$

where $a \subseteq \mathcal{O}_E$ and $c \in \mathbf{R}$ is normalizing factor. The element a is chosen so that the vectorized code $\phi(B_2)$ (see Section II) has shape $\mathbf{Z}^{2n^2}$.

2) The 3×3 Perfect code: The underlying algebra of the 3×3 perfect code is $\mathcal{P}_3 = (E/F, \sigma, \omega)$, where again $\omega = (-1+\sqrt{-3})/2$, $F = \mathbf{Q}(\omega)$, $E = \mathbf{Q}(\zeta_7 + \zeta_7^{-1}, \omega)$ and $\sigma : \zeta_7 + \zeta_7^{-1} \longmapsto \zeta_7^2 + \zeta_7^{-2}$. The algebra $\mathcal{P}_3$ has a representation as

$$L \oplus u \cdot L \oplus u^2 \cdot L$$

where $u^3 = \omega$.

The discriminant of the extension E/F is $(2+\sqrt{-3})^2(2-\sqrt{-3})^2 = P_1^2P_2^2$ and the discriminant of the natural order has therefore only two prime factors. By Lemma 7.5 the only nontrivial Hasse invariants of $\mathcal{P}_3$ are h_{P_1} and h_{P_2}. Because LCM $[m_{P_1}, m_{P_2}] = 3$. We get that $m_{P_1} = m_{P_2} = 3$.

To calculate the Hasse invariant h_{P_1} we pass to the completion $\mathcal{P}_{P_1} = \hat{F}_{P_1} \otimes \mathcal{P}_3$. From Theorem 6.10 we get a cyclic generation

$$\mathcal{P}_{P_1} = (\hat{E}_{P_1}/\hat{F}_{P_1}, \sigma_{P_1}, \omega),$$

where $\hat{E}_{P_1}/\hat{F}_{P_1}$ is a totally ramified extension and σ_{P_1} is the natural extension of the automorphism σ. Because the local index $m_{P_1} = 3$, we know that $\mathcal{P}_{P_1}$ is a division algebra.

Next we try to find another cyclic generation for this algebra so that we can use the definition of Hasse invariant to calculate the value of h_{P_1}.

It is readily verified that the field $\hat{F}_{P_1}(u) = \hat{T}_{P_1} \subseteq \mathcal{P}_{P_1}$ is a cyclic and totally inert extension of $\hat{F}_{P_1}$. The Frobenius automorphism of the extension $\hat{T}_{P_1}/\hat{F}_{P_1}$ is defined by the $(\hat{T}_{P_1}/\hat{F}_{P_1}, P_1)(u) = u^7$. The Noether-Skolem Theorem ([23, Theorem 7.21]) states that there is an element $x \in \mathcal{P}_{P_1}$ such that

$$(\hat{T}_{P_1}/\hat{F}_{P_1}, P_1)(a) = x^{-1}ax \quad \forall a \in \hat{T}_{P_1}. \tag{7}$$

For an element x to fulfill (7) it is enough to satisfy the equation

$$(\hat{T}_{P_1}/\hat{F}_{P_1}, P_1)(u) = u^7 = xux^{-1}.$$

By considering the equation $ux = xu^7 = x\omega^2 u$ we see that $x = \zeta_7 + \zeta_7^{-1} + \omega^2(\zeta_7^2 + \zeta_7^{-2}) + \omega(\zeta_7^4 + \zeta_7^{-4}) \in L$ is a suitable element.

We now prove that x^3 is an element of $\hat{F}_{P_1}$, and that $v_{P_1}(x^3) = 1$. The first statement follows from $u\sigma(x^3) = x^3u = x^2u\omega^2x = ux^3$. The second statement is obtained from the equation $v_{P_1}(x^3) = v_{P_1}(nr_{E/F}(x)) = v_{P_1}(7(2 + (\sqrt{-3}))\omega) = 2$.

Proposition 11.1 now states that $\mathcal{B}_1 = (\hat{T}_{P_1}/\hat{F}_{P_1}, (\hat{T}_{P_1}/\hat{F}_{P_1}, P_1), x^3)$ is a division algebra of index 3. By (7) we can consider $\mathcal{B}_1$ as a subset of the algebra $\mathcal{P}_3$. But $\mathcal{B}_1$ is a $\hat{F}_{P_1}$-central division algebra and hence a 9 dimensional over $\hat{F}_{P_1}$. From this we can conclude that $(\hat{T}_{P_1}/\hat{F}_{P_1}, (\hat{T}_{P_1}/\hat{F}_{P_1}, P_1), x^3) = \mathcal{P}_{P_1}$.

Proposition 11.4 now implies that $h_{P_1} = 2/3$. Because the sum of the Hasse invariants has to be an integer, the invariant h_{P_2} equals $1/3$.

By considering the local indices we see that the discriminant of the maximal order is $P_1^6P_2^6$, that is, equal to the discriminant of the natural order Λ_6. Thus, the natural order has to be maximal.

The actual code B_3 is produced similarly to the 2×2 case with exception that the vectorized code lattice has now shape $A_2^{n^2}$, where A_2 is the hexagonal lattice.

3) The 4×4 Perfect code: The underlying division algebra under the 4×4 perfect code is $\mathcal{P}_4 = (E/F, \sigma, i)$, where $\mathbf{Q}(i) = F$, $\mathbf{Q}(i, \zeta_{15} + \zeta_{15}^{-1}) = E$ and $\sigma : \zeta_{15} + \zeta_{15}^{-1} \longmapsto \zeta_{15}^2 + \zeta_{15}^{-2}$.

The extension $E/\mathbf{Q}(i)$ has discriminant $d(E/\mathbf{Q}(i)) = (2+i)^3(2-i)^3(3)^2$, and the only Hasse invariants that can be nontrivial are $h_{(3)}, h_{(2+i)}$ and $h_{(2-i)}$. We use similar methods to those in the case of $\mathcal{P}_3$ to get that $h_{(2+i)} = 3/4$ and $h_{(2-i)} = 1/4$. The sum $h_{(2-i)} + h_{(2+i)} = 1$ and therefore $h_{(3)}$ must be trivial. Further, the local indices reveal that the discriminant of the algebra is $(2+i)^{12}(2-i)^{12}$. The discriminant of the natural order on the other hand is $(2+i)^{12}(2-i)^{12}(3)^8$.

The code B_4 is again constructed by using a principal ideal of the natural order.

4) The 6×6 Perfect code: In the 6×6 perfect code construction the center is $F = \mathbf{Q}(\omega)$ and the maximal subfield $E = K(\theta)$, where $\theta = \zeta_{28} + \zeta_{28}^{-1}$.

In [10] where the perfect codes were introduced, the authors gave the mapping σ_1 by the equation $\sigma_1 : \zeta_{28} + \zeta_{28}^{-1} \longmapsto \zeta_{28}^2 + \zeta_{28}^{-2}$. Unfortunately, this mapping is not an F-automorphism of the field E. We replace σ_1 with the automorphism σ defined by the equation $\sigma : \zeta_{28} + \zeta_{28}^{-1} \longmapsto \zeta_{28}^5 + \zeta_{28}^{-5}$. The relative discriminant of the extension E/F is $(2)^6(2 + \sqrt{-3})^5(2 - \sqrt{3})^5 = (2)^6(7)^5$. We denote the resulting algebra by $\mathcal{P}_6$.

Thus the Hasse invariants of $\mathcal{P}_6$ that can be nontrivial are $h_{(2+\sqrt{-3})}$, $h_{(2-\sqrt{-3})}$, and $h_{(2)}$.

Now we are going to present $\mathcal{P}_6$ as a product of two smaller division algebras. We first calculate the Hasse invariants of these smaller algebras and then from these derive the Hasse invariants of $\mathcal{P}_6$.

Let us first consider the algebra $\mathcal{B}_2 = (\mathbf{Q}(\sqrt{7}, \omega)/\mathbf{Q}(\omega), \sigma_2, -\omega)$. We use similar strategy as in the case of the algebra $\mathcal{D}_4$.

The prime $(2 + \sqrt{-3}) = P_1$ is tamely ramified in the extension E/F. By passing to the P_1-adic completion $\hat{E}_{P_1}/\hat{F}_{P_1}$ we find that the local conductor is P_1. The image of the norm $N_{\hat{E}_{P_1}/\hat{F}_{P_1}}$ includes $\langle(1 + P_1)\rangle \times \langle e(2 + \sqrt{-3})\rangle$, where e is a unit of $\hat{F}_{P_1}$.

The set $\{0, 1, \omega, -\omega, \omega^2, -\omega^2\}$ is a complete residue system of the group $\mathcal{O}_{\hat{F}_{P_1}}/P_1\mathcal{O}_{\hat{F}_{P_1}}$ and whence

$$\hat{F}_{P_1}^* = \langle-\omega\rangle \times (1 + P_1) \times \langle e(2 + \sqrt{-3})\rangle.$$

On the other hand, $\#((\hat{F}_{P_1})^*/N_{\hat{E}_{P_1}/\hat{F}_{P_1}}(\hat{E}_{P_1}^*)) = 2$ and therefore $-\omega$ cannot be a norm. From this it follows that the local algebra $(\mathcal{B}_2)_{P_1}$ is a division algebra of index two.

There is no other choice for the Hasse invariant h_{P_1} than $1/2$.

Replacing the prime P_1 with $P_2 = (2 - \sqrt{-3})$ in the above considerations we see that $h_{P_2} = 1/2$.

The extension E/F has only three ramified primes $(2 - \sqrt{-3}), (2 + \sqrt{-3})$, and (2). Thus, the discriminant of the algebra $\mathcal{B}_2$ can have three prime divisors at maximum. The potential nontrivial Hasse invariants of $\mathcal{B}_2$ are now h_{P_1}, h_{P_2}, and $h_{(2)}$. The sum of h_{P_1} and h_{P_2} is 1, and therefore $h_{(2)}$ must be trivial.

The algebra $\mathcal{B}_2$ is a division algebra with Hasse invariants $h_{(2-\sqrt{-3})} = h_{(2+\sqrt{-3})} = 1/2$.

The algebra $\mathcal{P}_3 = (E/F, \sigma_3, \omega)$ was previously shown to be a division algebra with Hasse invariants $h_{(2-\sqrt{-3})} = 2/3$ and $h_{(2+\sqrt{-3})} = 1/3$. We now consider the algebra $\mathcal{B}_3 = (E/F, \sigma_3, \omega^2)$. By [23, Theorem 30.4] we have $\mathcal{P}_3 \otimes \mathcal{B}_3 \sim (E/F, \sigma_3, 1) \simeq M_3(F)$. This shows that $\mathcal{P}_3 \otimes \mathcal{B}_3$ has trivial Hasse invariants and therefore the Hasse invariants of $\mathcal{B}_3$ are $h_{(2-\sqrt{-3})} = 1/3$ and $h_{(2+\sqrt{-3})} = 2/3$.

If we now consider the algebra $\mathcal{B}_2 \otimes \mathcal{B}_3 \simeq$

$$\simeq (\mathbf{Q}(\sqrt{7}, \omega) \cdot \mathbf{Q}(\zeta_7 + \zeta_7^{-1}, \omega)/\mathbf{Q}(\omega), \sigma_2\sigma_3, (-\omega)^3 \cdot (\omega^2)^2)$$

it is seen that the corresponding Hasse invariants are $h_{(2-\sqrt{-3})} = 1/3 + 1/2 = 5/6$ and $h_{(2+\sqrt{-3})} = 1/2 + 2/3 \equiv 1/6 \pmod 1$.

By considering the equation $\sigma_3(\zeta_7 + \zeta_7^{-1}) = \zeta_7^2 + \zeta_7^{-2} = \zeta_7^5 + \zeta_7^{-5}$ we notice that $\sigma_2\sigma_3 = \sigma_6$. Combining this and the equation $(-\omega)^3 \cdot \omega^4 = -\omega$ we get that $\mathcal{B}_3 \otimes \mathcal{B}_2 \simeq \mathcal{P}_6$.

The algebra $\mathcal{P}_6$ has only two nontrivial Hasse invariants that are $h_{(2+\sqrt{-3})} = 5/6$ and $h_{(2-\sqrt{-3})} = 1/6$. Whence, the discriminant of the maximal order is $(2 - \sqrt{-3})^{30}(2 + \sqrt{-3})^{30} = (7)^{30}$. On the other hand the discriminant of the natural order is $(2)^{36}(7)^{30}$.

The actual code B_6 now has form

$$\frac{1}{c}\Lambda_n I$$

where I is a non-principal ideal of $\mathcal{O}_E$ and $c \in \mathbf{R}$ is a normalizing element. Again I is chosen so that the shape of the lattice is $A_2^{6^2}$. Here our methods fail to determine the exact value of the normalized minimum determinant. In [10] the authors represent an upper and lower bounds for the minimum determinant.

We have collected information about the normalized minimum determinants of the perfect codes and of the underlying natural orders into Table III. We have also added the information, whether the natural orders are maximal.

As an example we show how the values for the first row of the table III has been calculated. The discriminant of the natural order Λ_2 of the golden algebra $\mathcal{GA}$ is $(2+i)^2(2-i)^2$. This implies that the volume of the fundamental parallelotope is 25. Corollary 4.2 then gives that that $\delta(\Lambda_2) = 0.45$.

The actual code B_2 is then $a\Lambda_2$ where a is a suitable element of the natural order. Lemma 10.1 states that $\delta(\Lambda_2 a) = \delta(\Lambda_2) = 0.45$.

TABLE III

n	maximal?	$\delta(\Lambda_n)$	$\delta(B_n)$
2	yes	0.45	0.45
3	yes	0.14	0.14
4	no	0.03	0.03
6	no	0.0001	?

In Table IV we are comparing the normalized minimum determinants of the perfect codes and the maximal order codes ($\Lambda_n^i \mathrm{and} \Lambda_n^\omega$) whose existence is guaranteed by the results in Section VII.

TABLE IV

n	$\delta(\Lambda_n^i)$	$\delta(\Lambda_n^\omega)$	$\delta(B_n)$
2	0.562	0.620	0.447
3	0.316	0.358	0.14
4	0.177	0.207	0.030
5	0.100	0.119	
6	0.056	0.069	?

XI. General construction of division algebras achieving the Discriminant Bound

In their recent paper [14], Elia *et al.* gave an explicit construction for division algebras of an arbitrary degree with centers $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-3})$. In their general constructions they used non-unit, but relatively small, non-norm elements. As they were not interested in maximal orders nor the discriminants of the corresponding division algebras, their algebras (with few exceptions) did not happen to have minimal discriminants.

We are now going to give a general construction for division algebras of arbitrary degree and with minimal discriminants. According to Proposition 10.2, it suffices to study the case, where the index is a prime power. As a drawback our constructions will be dependent on the existence of certain prime numbers. We discuss this existence problem in Section XI-A which is purely number theoretic. We note that the fields we use in our construction are just simple modifications of the fields in [38].

We give one simple lemma for later use, slightly generalizing [11, Theorem 1]. The proof is rather similar to the one given in [11], and therefore we omit it.

Lemma 11.1: Let E be a Galois extension of a number field F and let P be a prime ideal of $\mathcal{O}_F$ that lies under the prime B of the ring $\mathcal{O}_E$. If the inertial degree of P in the extension E/F is f and γ is such an element of F that $(v_P(\gamma), f) = 1$, then $\gamma^i \notin N_{E/F}(E)$ for any $i = 1, 2, \ldots, f-1$.

We first consider two easy prime powers and then move forward to more complicated ones.

To ease the notation, we will denote by $\mathbf{Z}_m$ the residue class ring modulo m, i.e. $\mathbf{Z}_m = \mathbf{Z}/m\mathbf{Z}$. Thus e.g. $\mathbf{Z}_m^*$ is logically the group of units of that ring.

Lemma 11.2: Suppose that E is a cyclic extension of F, and that $a\mathcal{O}_F = P_1$ and P_2 are a pair of smallest primes in F. Assume that P_1 is totally inert and P_2 is the only ramified prime in the extension E/F. Then

$$\mathcal{A} = (E/F, \sigma, a),$$

where $\langle\sigma\rangle = \mathrm{Gal}(E/F)$, is a division algebra that has a minimal discriminant.

Proof: Lemma 11.1 combined with Proposition 3.6 gives that A is a division algebra. The minimality of the discriminant follows from Lemma 7.5. ■

Example 11.1: Let $\ell > 2$ be an integer. The maximal orders of the cyclic division algebra $\mathcal{A}_\ell = (\mathbf{Q}(\zeta_\ell)/\mathbf{Q}(i), \sigma, 2+i)$ from Example 5.2 achieve the discriminant bound.

Example 11.2: The field $\mathbf{Q}(\zeta_{3^{k+1}})$ has a unique subfield Z where $[Z : \mathbf{Q}] = 3^k$. The extension $\mathbf{Q}(\sqrt{-3})Z/\mathbf{Q}(\sqrt{-3})$ has degree 3^k and the prime (2) is totally inert in this extension. The extension also has a very limited ramification, the prime $(\sqrt{-3})$ is the only ramified one.

Primes $(\sqrt{-3})$ and (2) are a pair of minimal primes in the field $\mathbf{Q}(\sqrt{-3})$. Lemma 11.2 states now that the cyclic algebra $\mathcal{A} = (\mathbf{Q}(\sqrt{-3})Z/\mathbf{Q}(\sqrt{-3}), \sigma, 2)$ is a division algebra with a minimal discriminant.

In Example 11.2 we found a suitable extension $E/\mathbf{Q}(\sqrt{-3})$ that only had one ramified prime $(\sqrt{-3})$. However, we can prove that for an arbitrary degree there usually does not exist a cyclic extension that has ramification over $(\sqrt{-3})$ or (2) only. This assures that in general we cannot use such simple methods. Next we will provide a construction method that takes care of most of the prime power degrees. First we need some preliminary results.

Recall the concept of the global Frobenius automorphism. Suppose we have a finite Galois extension E/F and that B is such a prime ideal of $\mathcal{O}_E$ that $B \cap \mathcal{O}_F = P$ is unramified in the extension E/F. There exists a unique element σ of the group $\mathrm{Gal}(E/F)$ that is associated to the prime B and satisfies

$$\sigma(B) = B \tag{8}$$

$$\sigma(a) \equiv (a)^{[\mathcal{O}_F : P]} \pmod{B}. \tag{9}$$

We call this element the Frobenius automorphism of B and denote it with $(B, E/F)$.

If the extension E/F is abelian, all the primes B_i that lie over P share the same Frobenius automorphism and we can denote $(B, E/F)$ by $(P, E/F)$.

For the properties of the Frobenius automorphism we refer the reader to [39, p. 379].

Example 11.3: Let $p_1 \neq p$. Then the Frobenius automorphism $(p_1, \mathbf{Q}(\zeta_p)/\mathbf{Q})$ can be defined by

$$(p_1, \mathbf{Q}(\zeta_p)/\mathbf{Q})(\zeta_p) = \zeta_p^{p_1}.$$

We consider a tower of fields $F_1 \subseteq F_2 \subseteq L$ of finite extensions.

Proposition 11.3: If $F_1 \subseteq F_2 \subseteq E$, E/F_1 and F_2/F_1 are normal and B is such a prime ideal of E that $B \cap F_1 = P$ is unramified in E/F_1, then

$$(B, E/F_1)|_{F_2} = (B \cap F_2, F_2/F_1).$$

The prime P is totally inert in the extension E/F_1 if and only if $(B, E/F_1)$ generates the group $\mathrm{Gal}(E/F_1)$.

Proof: See [39, Theorem 7.10]. ∎

The next lemma is a rather direct consequence of the definition of Hasse invariant.

Lemma 11.4: Let

$$\mathcal{A} = (E/F, \sigma, \gamma)$$

be a division algebra where $\langle\sigma\rangle = \mathrm{Gal}(E/F)$, $\gamma \in F^*$, $[E : F] = n$ and suppose that P is a prime ideal of F that is totally inert in the extension E/F. If k is the smallest possible positive integer so that σ^k is the Frobenius automorphism of P then the Hasse invariant of P

$$h_P = \frac{k v_P(\gamma)}{n}.$$

Proof: [23, p. 281]. ∎

Let us next consider a tower of fields $F_1 \subseteq F_2 \subseteq E$ of finite extensions. The proofs of the next two well known lemmas will be omitted.

Lemma 11.5: Let B be a prime ideal of E, $P_2 = \mathcal{O}_{F_2} \cap B$ and $P_1 = \mathcal{O}_{F_1} \cap B$.

1. Let $f(B/P_1)$, $f(B/P_2)$, and $f(P_2/P_1)$ be the respective inertia degrees of B over P_1, B over P_2, and P_2 over P_1. Then

$$f(B/P_1) = f(B/P_2) f(P_2/P_1).$$

2. Let $e(B/P_1)$, $e(B/P_2)$, and $e(P_2/P_1)$ be the respective ramification indices of B over P_1, B over P_2, and P_2 over P_1. Then

$$e(B/P_1) = e(B/P_2) e(P_2/P_1).$$

Lemma 11.6: Let E/F be a Galois extension, B a prime ideal of E and $P = F \cap B$. Then

$$e(B/P) \mid [E : F]$$

and

$$f(B/P) \mid [E : F].$$

Lemma 11.7: Let p be a prime and n such an integer that $n|(p-1)$. The field $\mathbf{Q}(\zeta_p)$ has a unique subfield Z with $[Z : \mathbf{Q}] = n$.

There exists a group isomorphism ϕ from $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^n$ to $\mathrm{Gal}(Z/\mathbf{Q})$ that takes any prime $p_1 \neq p$ to the corresponding Frobenius automorphism $(p_1, Z/\mathbf{Q})$ in $\mathrm{Gal}(Z/\mathbf{Q})$.

The prime $p_1 \neq p$ is totally inert in the extension $Z/\mathbf{Q}$ if and only if p_1^t is not an nth power $(\bmod p)$ for $t = 1, \ldots, n-1$.

Proof: It is well known that there exists a unique isomorphism ψ from $\mathbf{Z}_p^*$ to $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ which takes prime $p_1 \neq p$ to $(p_1, \mathbf{Q}(\zeta_p)/\mathbf{Q})$. We denote the fixed field of the group $\psi(\mathbf{Z}_p^*)^n$ by Z. It is now clear that Z is unique and $[Z : \mathbf{Q}] = n$. If we first map the elements of $\mathbf{Z}_p^*$ with ψ to $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ and then restrict the resulting automorphisms to the field Z, we obtain an isomorphism ϕ from $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^n$ to $\mathrm{Gal}(Z/\mathbf{Q})$. Proposition 11.3 states that ϕ has the claimed properties.

The last claim follows from the properties of ϕ combined with the last statement of Proposition 11.3. ∎

Proposition 11.8: Suppose that $F = \mathbf{Q}(\sqrt{c})$ is a quadratic field, $q \neq 2$ is a given prime and n a given integer. We suppose that P_1 and P_2 are the smallest primes ideals in F and p_1 and p_2 are the prime numbers that lie under P_1 and P_2.

Let p be such a prime that $q^n|(p-1)$, $(p, c) = 1$, and that p_1 and p_2 are totally inert in the extension $Z/\mathbf{Q}$, where Z is the unique subfield of $\mathbf{Q}(\zeta_p)$ of degree q^n. We also suppose that p is inert in the extension $F/\mathbf{Q}$.

The extension FZ/F is a cyclic Galois extension of degree q^n where the prime ideals P_1 and P_2 are totally inert and $P = p\mathcal{O}_F$ is the only ramified prime ideal in the extension FZ/F.

Proof: Let B be a prime ideal of FZ, $P_Z = \mathcal{O}_Z \cap B$, $P_F = \mathcal{O}_F \cap B$ and $b = \mathbf{Q} \cap B$. We denote the corresponding ramification indices by $e(B/P_Z)$, $e(P_Z/P_F)$ and $e(P_F/b)$. According to Lemma 11.5

$$e(B/b) = e(B/P_Z) e(P_Z/b) = e(B/P_F) e(P_F/b).$$

Lemma 11.6 for its part states that $e(B/P_Z), e(P_F/b) \mid 2$ and $e(P_Z/b), e(B/P_F) \mid q^n$. This together with the previous equation shows that the prime $P_F \subset \mathcal{O}_F$ is ramified in the extension FZ/F if and only if the prime b is ramified in the extension $Z/\mathbf{Q}$.

The prime p is the only ramified prime in $Z/\mathbf{Q}$ and because p is inert in the extension $F/\mathbf{Q}$ we see that P is the only ramified ideal in the extension ZF/F.

If we choose B so that $P_F = P_1$ or $P_F = P_2$, then

$$f(B/b) = f(B/P_Z) f(P_Z/b) = f(B/P_F) f(P_F/b) = q^n \cdot g,$$

where $g = 1$ or $g = 2$. This combined with Lemma 11.6 implies that $f(B/P_F) = q^n$. ∎

In the following propositions we use the notation from Proposition 11.8. We set that $f_1 = f(P_1|p_1)$ and $f_2 = f(P_2|p_2)$.

Lemma 11.9: There exists a group isomorphism ρ between $\mathrm{Gal}(FZ/F)$ and $\mathrm{Gal}(Z/\mathbf{Q})$ such that

$$\rho((P_i, FZ/F)) = (p_i, Z/\mathbf{Q})^{f_i}.$$

Proof: It is a well-known fact that there exists a well defined surjective homomorphism from $\mathrm{Gal}(FZ/\mathbf{Q})$ to $\mathrm{Gal}(Z/\mathbf{Q})$ for which $\sigma \longmapsto \sigma_{|Z}$. The kernel of this map consists of those elements of $\mathrm{Gal}(FZ/\mathbf{Q})$ that act trivially on the field Z. On the other hand, if we restrict the domain of the map to those elements that act trivially on F this map is an injection because the only element of $\mathrm{Gal}(FZ/\mathbf{Q})$ that acts trivially on both fields F and Z is the identity map. As we know that $|\mathrm{Gal}(FZ/F)| = |\mathrm{Gal}(Z/\mathbf{Q})|$ the described map must be an isomorphism. Now the statement about Frobenius maps follows from the basic properties of the Frobenius automorphism. ∎

Proposition 11.10: Let

$$p_1^{f_1} p_2^{f_2} = 1 \tag{10}$$

in the group $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^{q^n}$, $P_1 = a_1\mathcal{O}_F$, and $P_2 = a_2\mathcal{O}_F$. Then

$$\mathcal{A} = (FZ/F, \sigma, a_1 a_2)$$

with $\langle\sigma\rangle = \mathrm{Gal}(FZ/F)$ is a division algebra that has a minimal discriminant.

Proof: The prime P_1 is totally inert in the extension FZ/F. Thus, Lemma 11.1 states that $\mathcal{A}$ is a division algebra.

From the cyclic representation of the algebra $\mathcal{A}$ we instantly see that $\mathcal{A}$ has only three Hasse invariants that can be non-trivial: h_{P_1}, h_{P_2}, and h_P. In what follows we show that the invariant h_P must be trivial.

We first choose σ to be the Frobenius automorphism of P_1. Lemma 11.4 now shows that the Hasse invariant of P_1 is

$$\frac{1}{q^n} = h_{P_1}.$$

Because the group $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^{q^n}$ is cyclic we get from (10) that $p_2^{f_2} = (p_1^{f_1})^{(q^n-1)}$ in $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^{q^n}$. This implies that $(p_2, Z/\mathbf{Q})^{f_2} = ((p_1, Z/\mathbf{Q})^{f_1})^{(q^n-1)}$. According to Lemma 11.9 then $(P_2, FZ/F) = ((P_1, FZ/F)^{q^n-1}$. Lemma 11.4 now states that

$$\frac{q^n-1}{q^n} = h_{P_2}.$$

The sum of the Hasse invariants of $\mathcal{A}$ must be zero (mod 1), whence

$$h_{P_1} + h_{P_2} + h_P \in \mathbf{Z}.$$

But, we already saw that $h_{P_1} + h_{P_2} \in \mathbf{Z}$, which implies that $h_P \in \mathbf{Z}$. The discriminant of the algebra $\mathcal{A}$ has now only two divisors P_1 and P_2.

In the beginning of our proof we make the assumption that σ is the Frobenius of the prime P_1. However, the choice of the generator of the group $\mathrm{Gal}(FZ/F)$ in a cyclic generation does not change the discriminant of the corresponding algebra. ■

Example 11.4: Suppose that the center $F = \mathbf{Q}(i)$. The primes $(1+i)$ and $(2+i)$ are a pair of smallest prime ideals in this field. We want to produce a division algebra of index 10 that has a minimal discriminant. It is not difficult to check that 2^t and 5^t are not 5th powers (mod 11) for $t = 1, \ldots, 4$, and that 11 is inert in the extension $F/\mathbf{Q}$. Lemma 11.8 states that $\mathbf{Q}(\zeta_{11})$ has a subfield Z, $[Z : \mathbf{Q}] = 5$, and that 2 and 5 are totally inert in the extension $Z/\mathbf{Q}$.

Proposition 11.8 states that the primes $(1+i)$ and $(2+i)$ are totally inert in the extension FZ/F and the prime ideal $11\mathcal{O}_F$ is the only ramified ideal in the extension FZ/F.

We easily see that $2 \cdot 5 = 1$ in $\mathbf{Z}_{11}^*/(\mathbf{Z}_{11}^*)^5$. Therefore,

$$(FZ/F, \sigma_1, (1+i)(2+i))$$

is a division algebra with a minimal discriminant.

We previously saw that $\mathcal{A} = (\mathbf{Q}(\zeta_{2^4})/F, \sigma_2, 2+i)$ is a division algebra of index 2 and has a minimal discriminant. Finally, from Proposition 10.2

$$(\mathbf{Q}(\zeta_{2^4})Z/F, \sigma_1\sigma_2, (1+i)^2(2+i)^7)$$

is seen to be a division algebra of degree 10 with a minimal discriminant.

A. The existence of suitable primes

Propositions 11.8 and 11.10 have turned our construction project into a hunt of suitable prime numbers. The problem is that we do not know if there are "enough" suitable prime numbers. The answer is that in most cases there are. This will be proved in Theorem 11.14, but first we need some preliminary results.

For the definition of the Kummer extension we refer the reader to appendix and for a proper introduction to [40, p. 197].

Proposition 11.11: Let E/F be a Kummer extension with $E = F(\alpha)$, $\alpha^n = a \in \mathcal{O}_F$, and let P be a prime ideal of F that is not a divisor of $a \cdot n$. Furthermore, let t be the largest divisor of n such that the congruence

$$x^t \equiv a \pmod{P}$$

has a solution in $\mathcal{O}_F$. Then P decomposes in E into a product of t prime ideals of degree n/t over P.

Lemma 11.12: Suppose that q and p are prime numbers and that $q^t|(p-1)$ for some integer t. If c is an integer and the equation

$$c \equiv x^q \pmod{p} \tag{11}$$

is not solvable, then neither is any of the equations

$$c^k \equiv x^{q^t} \pmod{p}, \tag{12}$$

where $k = 1, \ldots, q^t - 1$.

Proof: Let a be a generator of the cyclic group $\mathbf{Z}_p^*$. Then we can write that $c \equiv a^n \pmod{p}$ for some integer n.

Let us assume that (11) has no solution. This implies that q is not a factor of n. Assume then that for some k there is a solution d for (12). If we write $d \equiv a^s$, then (12) gives that $kn - sq^t = v(p-1)$, where v is some integer. As $q^t|(p-1)$ this would mean that $q^t|kn$. That gives us a contradiction. ■

In the following we use the phrase "the prime P has inertia in the extension E/F". By that we mean that at least one prime ideal B of E that lies over the P has inertial degree $f(P|B) > 1$.

Lemma 11.13: Suppose that F_1 and F_2 are Galois extensions of a field F and $F_1 \cap F_2 = F$. The prime P of $\mathcal{O}_F$ has inertia in the extension F_1F_2 if and only if it has inertia in the extension F_1 or F_2. The prime P is ramified in the extension F_1F_2 if and only if it is ramified in F_1 or in F_2.

Proof: For the proof the reader is referred to [41, p. 263]. ■

The proof of the following theorem is a slightly modified version of the proof of [38, Theorem 1]. We do not suppose here that the center is totally complex nor that the ring $\mathcal{O}_F$ is a PID. However, we suppose that $p_1 \neq p_2$. For the simplicity we also suppose that $f_2 \neq 2$.

Theorem 11.14: Assume that $F = \mathbf{Q}(\sqrt{c})$ is a quadratic field, P_1 and P_2 are the smallest primes in F, $q \nmid 2p_1$ is a given prime, and n a given integer.

If $q \nmid c$, then there exists infinitely many prime numbers p so that p is inert in F, $\mathbf{Q}(\zeta_p)$ has a unique subfield Z, $[Z : \mathbf{Q}] = q^n$, where p_1 and p_2 are totally inert, and $p_1^{f_1} p_2^{f_2} = 1$ in $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^{q^n}$.

Proof: Let us denote $q^n = s$, $K = \mathbf{Q}(\zeta_s)((p_1^{f_1}p_2^{f_2})^{1/s})$, $K_1 = K((p_1)^{1/q})$ and suppose that $q \neq p_1$. By noticing that p_1 is unramified in $\mathbf{Q}(\zeta_s)$ the ideal factorization of p_1p_2 in $\mathbf{Q}(\zeta_s)$ reveals that $(p_1^{f_1}p_2^{f_2})^d$ cannot be an sth power (in $\mathbf{Q}(\zeta_s)$) for any $d = 1, \ldots, s-1$. Therefore $[K : \mathbf{Q}(\zeta_s)] = s$.

As we have supposed that $q \nmid c$ there has to be at least one prime p_3 that has a ramification index 2 in the extension $F/\mathbf{Q}$, but which is not ramified in the extension $\mathbf{Q}(\zeta_s)/\mathbf{Q}$. Earlier, we saw that $[K : \mathbf{Q}(\zeta_s)] = s$. Because p_3 is not ramified in $\mathbf{Q}(\zeta_s)/\mathbf{Q}$ and 2 does not divide $[K : \mathbf{Q}(\zeta_s)]$, none of the prime ideals P_3 in $\mathcal{O}_K$ that lie over p_3 has 2 as a divisor of the ramification index $e(P_3|p_3)$. This implies that $F \not\subseteq K$.

By [38, Lemma 2] we know that $[K_1 : K] = q$. Because $q \neq 2$ and $F \not\subseteq K$, the extension K_1F/K is cyclic and $[K_1F : K] = 2q$.

Chebotarev's density theorem [39, Lemma 7.14] states that K has infinitely many prime ideals that have absolute degree one and are totally inert in the extension K_1F/K. We choose one, P, that not only has an absolute degree one but that is also unramified in the extension $K/\mathbf{Q}$.

We denote the prime of $\mathbf{Q}$ that lies under P by p. The field $\mathbf{Q}(\zeta_{q^n})$ is a subfield of K and therefore p splits completely in the extension $\mathbf{Q}(\zeta_{q^n})/\mathbf{Q}$. The theory of cyclotomic fields [40, p. 195] now gives that

$$p \equiv 1 \pmod{q^n}.$$

Next we are going to show that p_1^t is not an sth power (mod p) for $t = 1, \ldots, s-1$. Lemma 11.12 suggests that we should consider the equation $p_1 \equiv x^q \pmod{p}$. Suppose that $p_1 \equiv a^q \pmod{p}$ for some integer a. Now $p_1 \equiv a^q \pmod{P}$. This last equation however cannot be true because P is totally inert in the Kummer extension K_1/K. Lemma 11.12 now states that equation $p_1^t \equiv x^{q^n} \pmod{p}$ does not have a solution for any $t = 1, \ldots, q^n - 1$.

Lemma 11.7 states that $\mathbf{Q}(\zeta_p)$ has a unique subfield Z with $[Z : \mathbf{Q}] = q^n$, and that p_1 is totally inert in the extension $Z/\mathbf{Q}$.

The prime P has inertial degree one in the extension $K/\mathbf{Q}$ and therefore $(p_1^{f_1}p_2^{f_2})^{1/q^n} \equiv g \pmod{P}$, where g is some integer. This implies that

$$p_1^{f_1}p_2^{f_2} \equiv g^{q^n} \pmod{p}.$$

If we use the notation of Lemma 11.7, the map ϕ takes p_1 to the generator g of the group $\mathrm{Gal}(Z/\mathbf{Q})$ and $p_1^{f_1} \cdot p_2^{f_2}$ to identity. Because $2 \nmid |\mathrm{Gal}(Z/\mathbf{Q})|$ we have that $\phi(p_1)^{f_1}$ is also a generator of $\mathrm{Gal}(Z/\mathbf{Q})$. The map ϕ is a homomorphism and therefore $\phi(p_2)^{f_2}$ and $\phi(p_2)$ are again generators of the group $\mathrm{Gal}(Z/\mathbf{Q})$. Lemma 11.7 now shows that p_2 is totally inert in the extension $Z/\mathbf{Q}$.

To complete the proof we have to show that the prime p is inert in the extension $F/\mathbf{Q}$. The prime P must be inert in the extension FK/K and therefore the prime p has at least some inertia in the extension $FK/\mathbf{Q}$. Because p is totally split in the extension $K/\mathbf{Q}$ it does not have any inertia in this extension and therefore Lemma 11.13 states that p must be inert in the extension $F/\mathbf{Q}$. ∎

Theorem 11.14 states that for the center $\mathbf{Q}(i)$ the only problematic prime power indices are of the form 2^k. Luckily, the construction of example 11.1 covers these cases. As a consequence, we can construct a division algebra with a minimal discriminant for an arbitrary index. In Table V we give explicit representations for division algebras with a prime power index less than 20 and a minimal discriminant.

For each index q^n we have searched the prime p of the Theorem 11.14 along the lines of example 11.4. After the prime p is found the actual minimal polynomial of the extension FZ/F can be easily found by considering the subfields of the extension $\mathbf{Q}(\zeta_p)/\mathbf{Q}$. Both tasks were done by the help of computer algebra system PARI [42].

If the center is $\mathbf{Q}(\sqrt{-3})$, the problematic prime powers are 2^n and 3^n. Algebras of degree 3^n we get from Example 11.2, but degrees 2^n are more difficult. For index 2 we can use the division algebra of Section VIII-B. As a conclusion we can construct a division algebra with a minimal discriminant if the index is not divisible by 4.

In Table VI we give explicit representations for our algebras.

Example 11.5: From Table V we get that

$$\mathcal{A}_3 = (\mathbf{Q}(i)(a_3)/\mathbf{Q}(i), \sigma_3, (1+i)(2+i))$$

and

$$\mathcal{A}_2 = (\mathbf{Q}(i)(a_2)/\mathbf{Q}(i), \sigma_2, (2+i))$$

are division algebras with minimal discriminants. According to Proposition 10.2 algebra $\mathcal{A}_2 \otimes \mathcal{A}_3 = (\mathbf{Q}(i)(a_6)/\mathbf{Q}(i), \sigma_2\sigma_3, (2+i)^5(1+i)^2)$, where a_6 is a zero of the polynomial $x^6 - 2x^5 + (-3i-51)x^4 + (4i-30)x^3 + (-2i+755)x^2 + (-298i+2134)x + -593i + 1628$, is a division algebra of degree 6 and has a minimal discriminant.

One of the unfortunate properties of our construction is that when we produce division algebras of a composite index, the resulting algebras tend to have relatively large non-norm elements γ. In the following example we solve this problem in one specific case and show that we can always use $\gamma = (2+i)(1+i)$. The method has a straightforward generalization to more general situations.

Example 11.6: In what follows we produce the algebra $\mathcal{A}_6$ as a tensor product of two smaller algebras.

Let a_2 be a zero of the polynomial x^2+i. The algebra $\mathcal{B}_2 = (F(a_2)/F, \sigma_2, (1+i)(2+i))$ is a slightly modified version of the algebra $\mathcal{A}_2$ of Table V. Using Proposition 11.1 to the prime $(2+i)$ we see that it is a division algebra. Considering the prime divisors of the natural order we see that it has a minimal discriminant.

The algebra $\mathcal{B}_3 = (F(a_3)/F, \sigma_3, (2+i)^{-1}(1+i)^{-1})$ is a modified version of the algebra $\mathcal{A}_3$. Using Proposition 11.1 to prime $(2+i)$ gives us that $\mathcal{B}_3$ is still a division algebra. By considering the equation $\mathcal{B}_3 \otimes \mathcal{A}_3 \sim M_n(F)$ we see that $\mathcal{B}_3$ has the same discriminant as the algebra $\mathcal{A}_3$.

Because $\mathcal{B}_2$ and $\mathcal{B}_3$ are division algebras with minimal discriminants, it follows from Proposition 10.2 that the tensor product

$$\mathcal{A}_6 = \mathcal{B}_3 \otimes \mathcal{B}_2 = (F(a_2, a_3)/F, \sigma_2\sigma_3, (2+i)(1+i))$$

is a division algebra with a minimal discriminant. The polynomial f_6 is just simply the minimal polynomial of the generator a_6 of the field $F(a_2, a_3)$.

TABLE V

CONDUCTOR p OF THE CYCLOTOMIC FIELD $\mathbf{Q}(\zeta_p)$, THE NON-NORM ELEMENT γ, AND THE MINIMAL POLYNOMIAL f_n OF THE EXTENSION $\mathbf{Q}(i)(a_n)/\mathbf{Q}(i)$

n	p	γ	f_n
2		$2+i$	x^2+i
3	79	$(1+i)(2+i)$	$x^3+x^2-26x+41$
4		$2+i$	x^4+i
5	11	$(1+i)(2+i)$	$x^5+x^4-4x^3-3x^2+3x+1$
7	211	$(1+i)(2+i)$	$x^7+x^6-90x^5+69x^4+1306x^3+124x^2-5249x-4663$
8		$(1+i)(2+i)$	x^8+i
9	271	$(1+i)(2+i)$	$x^9+x^8-120x^7-543x^6+858x^5+6780x^4+7217x^3-2818x^2-4068x-261$
11	859	$(1+i)(2+i)$	$x^{11}+x^{10}-390x^9-653x^8+52046x^7+146438x^6-2723930x^5-11558015x^4+36326009x^3+250960565x^2+385923388x+145865807$
13	6163	$(1+i)(2+i)$	$x^{13}+x^{12}-2844x^{11}-6017x^{10}+2908490x^9+10238862x^8-1340405033x^7-6785664624x^6+281925130086x^5+1909036915713x^4-21097272693753x^3-192054635052100x^2-235667966495418x+213548387827457$
16		$2+i$	$x^{16}+i$
17	239	$(1+i)(2+i)$	$x^{17}+x^{16}-112x^{15}-47x^{14}+3976x^{13}+4314x^{12}-64388x^{11}-136247x^{10}+422013x^9+1631073x^8+411840x^7-5840196x^6-11894369x^5-10635750x^4-4739804x^3-938485x^2-54850x-619$
19	8779	$(1+i)(2+i)$	$x^{19}+x^{18}-4158x^{17}+8463x^{16}+6281539x^{15}-34466097x^{14}-4291513699x^{13}+39454551948x^{12}+1357034568541x^{11}-17014625218525x^{10}-1846142674321 85x^9+3035523756071878x^8+10088401800577582x^7-253111326110358151x^6-1432084484613198 68x^5+10612439791376560471x^4-3774559232798357892x^3-220041647923912963182x^2+860839321205015981 39x+179422120229746149 9641$

TABLE VI

THE CONDUCTOR p OF THE CYCLOTOMIC FIELD $\mathbf{Q}(\zeta_p)$, THE NON-NORM ELEMENT γ, AND THE MINIMAL POLYNOMIAL f_n OF THE EXTENSION $\mathbf{Q}(\sqrt{-3})(a_n)/\mathbf{Q}(\sqrt{-3})$

n	p	γ	f_n
2			
3		2	x^3-3x+1
4			
5	131	$\sqrt{-3}\cdot 2$	$x^5+x^4-52x^3-89x^2+109x+193$
7	449	$\sqrt{-3}\cdot 2$	$x^7+x^6-192x^5+275x^4+3952x^3+4136x^2-81x-863$
8			
9		2	$x^9-9x^7+27x^5-30x^3+9x+1$
11	23	$\sqrt{-3}\cdot 2$	$x^{11}+x^{10}-10x^9-9x^8+36x^7+28x^6-56x^5-35x^4+35x^3+15x^2-6x-1$
13	1613	$\sqrt{-3}\cdot 2$	$x^{13}+x^{12}-744x^{11}-2071x^{10}+172627x^9+432959x^8-17309406x^7-33601543x^6+751073656x^5+1289004819x^4-10171466974x^3-28375196178x^2-23821205823x-6355270027$
16			
17	239	$\sqrt{-3}\cdot 2$	$x^{17}+x^{16}-112x^{15}-47x^{14}+3976x^{13}+4314x^{12}-64388x^{11}-136247x^{10}+422013x^9+1631073x^8+411840x^7-5840196x^6-11894369x^5-10635750x^4-4739804x^3-938485x^2-54850x-619$
19	14897	$\sqrt{-3}\cdot 2$	$x^{19}+x^{18}-7056x^{17}-40523x^{16}+17080680x^{15}+72065222x^{14}-20162799933x^{13}-16167485303x^{12}+12640227359901x^{11}-36746089501267x^{10}-4111622563682675x^9+26076550916951212x^8+59051701290483139 4x^7-556308534776998817 1x^6-185870194645949304 04x^5+24907729711797663886 8x^4+895701349845719274 59x^3-242644330013856319 9068x^2-251407592145492680 9076x+123766441271862044 4787$

XII. An example code and simulation results

One of the ingredients in the construction of the perfect codes was the use of ideals in improving the shape of the code lattices. In [5] we did the same but for the purpose of saving energy and making the lattice easier to encode.

A way of doing that is to choose an element x of the maximal order in such way that the left (or right) ideal $x\Lambda$ is contained in the natural order. By moving the code inside the natural order we then to some extent recover the layered structure of the natural orders, and then, hopefully, also some of the advantages of the inherent orthogonality between layers.

For example in the case of the Golden+ algebra we can use the element $(1-\lambda)^3$ from the ring of integers $\mathcal{O}_E$ of the larger field $E = \mathbf{Q}(\sqrt{2+i})$ as a multiplier. Thus by denoting

$$M = \begin{pmatrix} (1-\lambda)^3 & 0 \\ 0 & (1+\lambda)^3 \end{pmatrix}$$

we get the ideal $\mathcal{I}$ consisting of matrices of the form $aMM_1 + bMM_2 + cMM_3 + dMM_4$, where the coefficients a, b, c, d are Gaussian integers and the matrices $M_j, j = 1, 2, 3, 4$ are from Section IX-C. This ideal is a subset of the natural order $\mathcal{O}_E \oplus u\mathcal{O}_E$.

Our code constructions are based on selecting the prescribed number of lowest energy matrices from a chosen additive coset of the ideal $\mathcal{I}$. In order to reach a target bandwidth utilization of 4, 5 or 6 bpcu we thus selected 256, 1024 or 4096 matrices. In this sense we have done some coset optimization for the Golden+ codes, but make no claims as to having found the best coset. For the rival Golden code from [10] the coset corresponding to assigning all the Gaussian integers the value $(1+i)/2$ stands out. This is because then there are 256 matrices all having the minimal energy, and more importantly because in that case pulse amplitude modulation (PAM) can be used to good effect. We first did some simulations using a PAM-type rule for larger subsets of the Golden code as well by arbitrarily selecting a suitable number of coefficients of the basis matrices from the set $\{-3/2, -1/2, 1/2, 3/2\}$ so that the desired bandwidth efficiency was achieved. This is a natural choice well suited for e.g. the sphere decoding algorithm. While we ended up having a dead even race BLER-wise at 4.0 bpcu, the Golden code lost to the Golden+ code by about 0.9 dB at the higher rates (see Figure 1). In the interest of a fair comparison we then tried coset optimization for the Golden code as well. This narrowed down the gap to about 0.3 dB. However, the resulting subsets of the Golden code no longer have such a structure well suited to PAM. In other words both the rival codes must resort to the use of a codebook. We have not even attempted to solve the problem of optimizing the codebook for the purposes of minimizing BER. This also explains, why our performance plots only show the block error rates (i.e. the probability of decoder deciding in favor of a 2×2 matrix other than the transmitted one) rather than bit error rates. Thus our simulations may also be viewed as measuring the amount of power lost, when one insists on not needing a codebook.

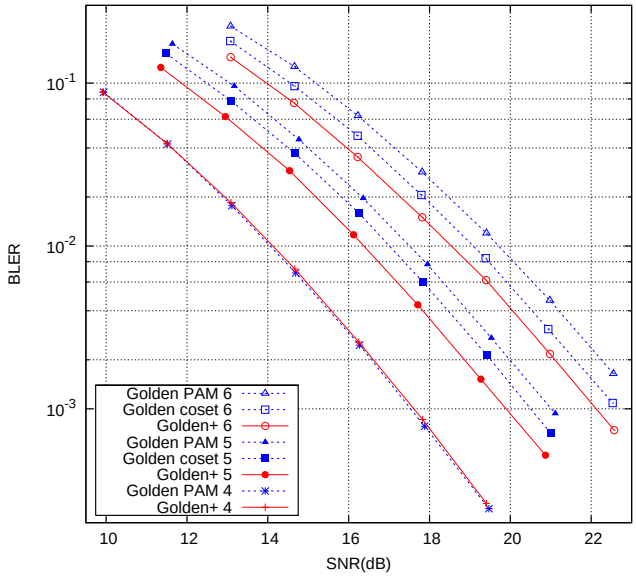


Fig. 1. Block error rates at 4, 5, and 6 bpcu.

XIII. Concluding remarks and suggestions for further work

We have derived a bound for the density of fully multiplexing MIMO matrix lattices resulting in codes with a unit minimum determinant. The bound only applies to codes obtained from the cyclic division algebras and their ideals. While the bound is not constructive per se, we also showed that it can be achieved for any number of transmit antennas, and discussed techniques leading to the construction of CDAs with maximal orders attaining the bound. For more details on the number theoretic techniques we refer the interested reader to the doctoral dissertation of Roope Vehkalahti [29]. We also discussed the Ivanyos–Rónyai algorithm that is needed to actually find these densest possible lattices inside these CDAs, and gave as an example a construction of a fully multiplexing 2×2 code that outperforms the Golden code at least for some data rates.

We concede the point that assigning bit labels to the points on our lattice is more difficult than in the case of linear dispersion codes. A very promising general method of spherical encoding has been studied in [25], where supporting simulation results are also provided. See [43] for the MAGMA commands for explicitly producing maximal orders and for a discussion on *power-controlled* sphere decoding of the maximal order codes.

There are also possibilities for applying these class field theoretical techniques to slightly modified density problems of ST-codes. For example, the bound of Theorem 6.12 has been used in [19] to produce dense asymmetric and multi-block ST codes. Asymmetric situations naturally arise in applications, where the receiver may have a lower number of antennas than the transmitter, e.g. in a broadcast application or in a cellular phone downlink.

An immediate open problem is to utilize maximal orders of the cyclic division algebra of index 2 with center $\mathbf{Q}(\omega)$. When looking for the example code in the previous section a

natural step was to use LLL-algorithm for finding a relatively orthogonal basis for the lattice. That definitely aided the search for a good coset. In the hexagonal case this step is somewhat trickier and using a multiplier to put the maximal order inside the natural order only lead to a code with a disappointing performance. The best way of using this densest known lattice of 2×2-matrices is not known to us. As another open problem we ask, whether the discriminant bound can be broken by a MIMO lattice that does not come from a cyclic division algebra. We believe this to be a very difficult question.

APPENDIX

In this Appendix we first give some results on algebraic number theory. The presentation is not intended to be a nice introduction, but rather a collection of results and concepts needed in this paper. In Section XIII-B, we give a proof of the claimed result in the beginning of the Section IX that natural orders can never reach our discriminant bounds.

A. Some results from algebraic number theory

In this paper, an algebraic number field is a finite algebraic extension of $\mathbf{Q}$. Let K be an algebraic number field and $\mathcal{O}_K$ the ring of algebraic integers in K.

Definition 13.1: Let $K/\mathbf{Q}$ be a finite extension of degree n. Suppose that r_1 and $2r_2$ are the numbers of real and complex embeddings of K to $\mathbf{C}$. We call the 2-tuple (r_1, r_2) *the signature* of the field K.

Proposition 13.1: Let $[K:\mathbf{Q}] = n$. Then

$$r_1 + 2r_2 = n.$$

Remark 13.1: A typical method to determine the number of real and complex embeddings of an algebraic number field is to pick a primitive element a of the extension $K/\mathbf{Q}$ and then count the number of real and complex zeros of the minimal polynomial of a.

If the signature of a field K is $(r_1, 0)$, we say that the field is *totally real*, and if the signature is $(0, r_2)$, we say that the field is *totally complex*.

Lemma 13.2: Let us consider the field $K = \mathbf{Q}(\sqrt{-m})$, where m is a positive square free integer. Each of the elements c in K can be uniquely presented in the form $c = a + b\sqrt{-m}$, where a and b are rational numbers. We then have

$$nr_{K/\mathbf{Q}}(c) = (a + b\sqrt{-m})(a - b\sqrt{-m}) = a^2 + b^2 m = |c|^2.$$

If the element c is in $\mathcal{O}_K$, the algebraic norm takes c to $\mathbf{Z}$. The previous equation then gives us that

$$|c| \geq 1$$

for every c in $\mathcal{O}_K^*$.

Suppose that K is an algebraic number field containing an n^{th} root of unity.

Proposition 13.3: Let us consider the field $L = K[a]$, where $a^n \in K$, and no smaller power of a is in K. Then L/K is a cyclic Galois extension of degree n.

We call such an extension a *Kummer extension*.

Definition 13.2: Suppose that L/K is an n-dimensional extension of algebraic number fields and that $tr_{L/K}$ is the trace function. The *discriminant* $d(L/K)$ of the extension L/K is an ideal in $\mathcal{O}_K$ generated by the set

$$\{\det(tr_{L/K}(x_i x_j))_{i,j=1}^n \mid (x_1, ..., x_n) \in \mathcal{O}_L^n\}.$$

If we want to emphasize that we consider the relation between $\mathcal{O}_K$ and $\mathcal{O}_L$, we can also write $d(\mathcal{O}_L/\mathcal{O}_K)$.
If $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module, then

$$d(\mathcal{O}_L/\mathcal{O}_K) = \det(tr(x_i x_j))_{i,j=1}^n,$$

where $\{x_1, \ldots, x_n\}$ is any $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

The following theorem connects the ramification of finite primes and the discriminant.

Theorem 13.4: Let P be a prime ideal of the ring $\mathcal{O}_K$ and $p = \mathrm{char}(\mathcal{O}_K/P)$. Suppose that

$$P\mathcal{O}_L = B_1^{e_1} \cdots B_g^{e_g}$$

is the prime decomposition of P in the ring $\mathcal{O}_L$. Let f_i stand for the inertial degree $f(B_i|P)$. Then

$$v_P(d(L/K)) = (e_1 - 1)f_1 + \cdots + (e_g - 1)f_g,$$

if $p \nmid e_i$, $i = 1, 2, \ldots, g$, and

$$v_P(d(L/K)) > (e_1 - 1)f_1 + \cdots + (e_g - 1)f_g,$$

if $p \mid e_i$ for some index i.

We say that a prime P is wildly ramified if and only if $p \mid e_i$ for some i, otherwise we say that it is tamely ramified. From the previous proposition we see that the ramification of a tame prime P defines totally the P power index of the discriminant. For wildly ramified ideals we only get a lower bound.

We will need later the following two technical lemmas.

Lemma 13.5: Let $K_2 \supseteq K_1 \supseteq F$ be a tower of finite extensions of $\mathbf{Q}$. Then

$$d(K_2/F) = nr_{K_1/F}(d(K_2/K_1))d(K_1/F)^{[K_2:K_1]},$$

where $nr_{K_1/F}$ is the usual relative norm from algebraic number theory.

Proof: For the proof we refer the reader to [41, p.249]. ■

Lemma 13.6: Suppose that we have an abelian extension L/K of degree n, with a Galois group $\{\sigma_1, \ldots, \sigma_n\}$, and suppose that $\{x_1, x_2, \ldots, x_n\}$ is some $\mathcal{O}_K$-basis of the ring $\mathcal{O}_L$. Then

$$\det(tr_{L/K}(x_i x_j))_{i,j=1}^n = \pm\det(tr_{L/K}(\sigma_k(x_i)x_j))_{i,j=1}^n.$$

Proof: We define $X_i = (\sigma_i(x_1), \ldots, \sigma_i(x_n))$ and consider the matrix X which has vectors X_i as rows. We then have that

$$\det(tr_{L/K}(x_i x_j))_{i,j=1}^n = \det(X^T X).$$

If we replace the rows X_i in the matrix X with the rows

$$\sigma_k(X_i) = (\sigma_k(\sigma_i(x_1)), \ldots, \sigma_k(\sigma_i(x_n))),$$

we get a matrix $\sigma_k(X)$. Then

$$\det(tr_{L/K}(\sigma_k(x_i)x_j))_{i,j=1}^n = \det(\sigma_k(X)^T X).$$

Clearly

$$\det(\sigma_k(X)) = \pm\det(X),$$

and the claim follows.

■

We shall now recall some facts of P-adic fields. Suppose that P is a finite prime of an algebraic number field K, $\hat{K}_P$ the P-adic completion, and $p = \mathrm{char}(\mathcal{O}_K/P)$. We may consider $\hat{K}_P$ as a finite algebraic extension of $\hat{\mathbf{Q}}_p$ and then refer to the algebraic closure of the ring $\hat{\mathbf{Z}}_p$ in $\hat{K}_P$ as $\mathcal{O}_{\hat{K}_P}$, and simply call it the ring of integers in $\hat{K}_P$. In the following, we identify the prime P and the unique prime ideal $P\mathcal{O}_{\hat{K}_P}$ of the ring $\mathcal{O}_{\hat{K}_P}$, and denote both by P.

We extend the concept of wild and tame ramification to local fields. Let $\hat{L}$ be a finite algebraic extension of $\hat{K}_P$, and B the unique prime ideal of $\mathcal{O}_{\hat{L}}$. We say that P is wildly ramified, if p divides the ramification index $e(B|P)$; otherwise we say that P is tamely ramified.

Definition 13.3: Let $\hat{L}$ be a finite and totally inert Galois extension of $\hat{K}_P$, and B the unique prime ideal of the ring of the P-adic algebraic integers $\mathcal{O}_L$ in L. Suppose that $[\mathcal{O}_{\hat{K}_P} : P] = q$. Then $\mathrm{Gal}(\hat{L}/\hat{K}_P)$ has an element $(P, \hat{L}/\hat{K}_P)$ called the (local) *Frobenius automorphism*. It is the unique element of $\mathrm{Gal}(\hat{L}/\hat{K}_P)$ satisfying

$$(P, \hat{L}/\hat{K}_P)(x) \equiv x^q \pmod{B} \quad forall\, x \in \mathcal{O}_L.$$

Suppose that L is an abelian extension of $\hat{K}_P$ and that U is the group of units in $\mathcal{O}_{\hat{K}_P}$.

Definition 13.4: The smallest f such that $nr_{\hat{L}/\hat{K}_P}(L^*)$ contains $1 + P^f$ is called the *conductor* of $L/\hat{K}_P$, except that, when $nr_{\hat{L}/\hat{K}_P}(\hat{L}^*) \subset U$, the conductor is said to be 0.

Remark 13.2: In the previous definition we expected the existence of some f. This is a nontrivial result.

In some special cases the determination of the conductor is easy. For the proof we refer the reader to [30, p.12].

Lemma 13.7: The extension $\hat{L}/\hat{K}_P$ is unramified if and only if its conductor is 0, and tamely ramified if and only if its conductor is ≤ 1.

B. Natural orders do not have minimal discriminants

In the next lemma we use some basic results from the theory of discriminants and differents. For these results and the notion of different we refer the reader to [40, Chapter 3.12]. For the definitions of tame and wild ramification we refer the reader to the previous subsection of this appendix.

Lemma 13.8: Suppose we have a Galois extension E/F of degree n, and that there are g prime ideals B_i of E lying over the prime P of F. If the prime P is wildly ramified in the extension E/F, then

$$v_P(d(E/F)) \geq n.$$

Proof: Suppose that $D_{E/F}$ is the different of the extension E/F. Then it is an easy exercise in Galois theory to show that $v_{B_i}(D_{E/F}) = v_{B_j}(D_{E/F})$ for every i and j. Because P was supposed to be wildly ramified,

$$s = v_{B_i}(D_{E/F}) \geq e, \tag{13}$$

where e is the ramification index of B_i/P.

The theory of normal extensions states that $efg = n$, where f is the inertial degree of B_i/P. Taking into account this and (13), we can conclude that

$$v_P(d(E/F)) = v_P(N_{E/F}(D_{E/F})) = sgf \geq egf = n.$$

■

Remark 13.3: The proof of the following proposition is merely a sketch directed to a reader having sufficient knowledge in algebraic number theory.

Proposition 13.9: Suppose we have a division algebra $\mathcal{D} = (E/\mathbf{Q}(i), \sigma, \gamma)$, where $E/\mathbf{Q}(i) = n$ and γ is an algebraic integer. If Λ is the natural order of the division algebra $\mathcal{D}$, then

$$|d(\Lambda/\mathcal{O}_{\mathbf{Q}(i)})| > |(2+i)^{n(n-1))}(1+i)^{n(n-1)}|.$$

Proof: The natural order Λ is a subset of some maximal order Λ_{max} and therefore

$$|d(\Lambda/\mathcal{O}_{\mathbf{Q}(i)})| \geq |(2+i)^{n(n-1)}(1+i)^{n(n-1)}|.$$

Let us then assume that

$$|d(\Lambda/\mathcal{O}_{\mathbf{Q}(i)})| = |(2+i)^{n(n-1)}(1+i)^{n(n-1)}|.$$

According to Lemma 5.4, the only primes that could be ramified in the extension $E/\mathbf{Q}(i)$ are $(1+i)$, $(2+i)$, and $(2-i)$. Lemma 13.8 assures that none of these primes could be wildly ramified.

One of the main results of the global class field theory [30, p. 124] states that there exists a ray class field $C_{(1+i)(2+i)(2-i)}$ that contains all the cyclic extensions of $\mathbf{Q}(i)$, where $(1+i)$, $(2+i)$, or $(2-i)$ is tamely ramified.

We can now calculate the degree of the extension $C_{(2+i)(1+i)(2-i)}/\mathbf{Q}(i)$. By [30, Theorem 1.5], we have $[C_{(2+i)(1+i)(2-i)} : \mathbf{Q}(i)] = 2$, which implies that $E = C_{(2+i)(1+i)(2-i)}$ and $n = 2$.

The ray class fields $C_{(2+i)(1+i)}$ and $C_{(2-i)(1+i)}$ that admit tame ramification at $(2+i)$ and $(1+i)$ or at $(2+i)$ and $(1-i)$, respectively, are both trivial extensions of $\mathbf{Q}(i)$. Hence, both $(2+i)$ and $(2-i)$ are ramified in E and divide the discriminant of the extension $E/\mathbf{Q}(i)$. The discriminant of the natural order Λ now has to be divisible by at least $(2+i)^2(2-i)^2$. This gives us a contradiction. ■

Proposition 13.10: Suppose we have a division algebra $\mathcal{D} = (E/\mathbf{Q}(\sqrt{-3}), \sigma, \gamma)$, where $E/\mathbf{Q}(\sqrt{-3}) = n$ and γ is an algebraic integer. If Λ is the natural order of the division algebra $\mathcal{D}$, then

$$|d(\Lambda/\mathcal{O}_{\mathbf{Q}(\sqrt{-3})})| > |(\sqrt{-3})^{n(n-1))}(2)^{n(n-1)}|.$$

Proof: The proof is similar to that of the previous proposition. ■

These considerations reveal that in order to reach the optimal density of a code lattice maximal orders are forced upon us.

ACKNOWLEDGMENTS

We are grateful to professor Lajos Rónyai for explaining to us many details of his algorithm for finding maximal orders. We are greatly indebted to Laura Luzzi and the reviewers for their efforts and suggestions that hopefully enhanced the readability of this article.

REFERENCES

[1] J.-C. Guey, M. P. Fitz, M. R. Bell, and W.-Y. Kuo, "Signal design for transmitter diversity wireless communication systems over rayleigh fading channels," in *Proc. IEEE VTC'96*, 1996, pp. 136–140.

[2] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Inf. Theory*, vol. 44, pp. 744–765, Mar. 1998.

[3] J.-C. Belfiore, G. Rekaya, and E.Viterbo, "The Golden code: A 2×2 full-rate space-time code with non-vanishing determinants," in *Proc. 2004 IEEE Int. Symp. Inform. Theory*, Chicago, IL, June 27-July 2 2004, p. 308.

[4] S. M. Alamouti, "A simple transmitter diversity scheme for wireless communications," *IEEE J. Select. Areas Commun.*, pp. 1451–1458, Oct. 1998.

[5] C. Hollanti, J. Lahtonen, and H.-F. Lu, "Maximal orders in the design of dense space-time lattice codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4493–4510, 2008.

[6] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 628–636, Mar. 2002.

[7] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2596– 2616, Oct. 2003.

[8] J.-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," in *Proc. IEEE Information Theory Workshop*, Paris, 31 March - 4 April 2003.

[9] G. Rekaya, J.-C. Belfiore, and E.Viterbo, "Algebraic 3×3, 4×4 and 6×6 space-time codes with non-vanishing determinants," in *Proc. 2004 Int. Symp. Inform. Th and its Applns.*, Parma, Italy, Oct. 10-13 2004.

[10] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect space-time block codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3885– 3902, Sept. 2006.

[11] T. Kiran and B. S. Rajan, "STBC-schemes with non-vanishing determinant for certain number of transmit antennas," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2984–2992, Aug. 2005.

[12] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman, "STBCs using capacity achieving designs from crossed-product division algebras," in *Proc. IEEE ICC 2004*, Paris, France, June 2004, pp. 827–831.

[13] ——, "Information-lossless STBCs from crossed-product algebras," *IEEE Trans. Inf. Theory*, vol. 52, pp. 3913–3935, 2006.

[14] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-F. Lu, "Explicit construction of space-time block codes achieving the diversity-multiplexing gain tradeoff," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3869–3884, Sep. 2006.

[15] G. Wang and X.-G. Xia, "On optimal multi-layer cyclotomic space-time code designs," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 1102–1135, Mar. 2005.

[16] L. Zheng and D. Tse, "Diversity and multiplexing: A fundamental tradeoff in multiple antenna channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.

[17] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, ser. Grundlehren der mathematischen Wissenshaften. Springer, 1988, vol. 290.

[18] H. E. Gamal and J. A. R. Hammons, "A new approach to layered space-time coding and signal processing," *IEEE Trans. Inf. Theory*, vol. 47, p. 2321–2334, 2001.

[19] C. Hollanti and H.-F. Lu, "Construction methods for asymmetric and multi-block space-time codes," *IEEE Trans. Inf. Theory*, in press, 2008.

[20] H.-F. Lu, R. Vehkalahti, C. Hollanti, J. Lahtonen, Y. Hong, and E. Viterbo, "New space-time code construcions for two-user multiple access channels," submitted to *IEEE J. on Special Topics in Signal Processing: Managing Complexity in Multi-user MIMO Systems*, Sep. 2008.

[21] G. Ivanyos and L. Rónyai, "On the complexity of finding maximal orders in semisimple algebras over Q," *Computational Complexity*, vol. 3, pp. 245–261, 1993.

[22] MAGMA Computational Algebra System, University of Sydney, Sydney, Australia, *http://magma.maths.usyd.edu.au/magma/htmlhelp/text835.htm#8121*.

[23] I. Reiner, *Maximal Orders*. New York: Academic Press, 1975.

[24] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, "Algebraic lattice constellations: Bounds on performance," *IEEE Transactions on Information Theory*, vol. 52, pp. 319–327, 2006.

[25] K. R. Kumar and G. Caire, "Space-time codes from structured lattices," *IEEE Trans. Inf. Theory* (in press), 2008. *http://arxiv.org/abs/0804.1811*.

[26] A. A. Albert, *Structure of Algebras*. New York: American Mathematical Society, 1939.

[27] H. Koch, *Algebraic Number Theory*. Berlin: Springer, 1997.

[28] C. Hollanti and J. Lahtonen, "A new tool: Constructing STBCs from maximal orders in central simple algebras," in *Proc. 2006 IEEE Inform. Theory Workshop*, Punta del Este, Uruguay, Mar. 13-17 2006.

[29] R. Vehkalahti, "Class field theoretic methods in the design of lattice signal constellations," Ph.D. dissertation, 2008, *TUCS Dissertations Series*, no. 100, *https://oa.doria.fi/handle/10024/36604*.

[30] J. S. Milne, "Class field theory," lecture notes for a course given at the University of Michigan, Ann Arbor, *http://www.jmilne.org/math/coursenotes/*.

[31] C. Hollanti, J. Lahtonen, K. Ranto, R. Vehkalahti, and E. Viterbo, "On the algebraic structure of the Silver code: A 2x2 Perfect space-time code with non-vanishing determinant," in *Proc. 2008 IEEE Inf. Theory Workshop*, Porto, Portugal, May 2008, pp. 91–94.

[32] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, "Optimal matrix lattices for MIMO codes from division algebras," in *Proc. 2006 IEEE Int. Symp. Inform. Theory*, Seattle, WA, Jul. 2006, pp. 783 – 787.

[33] P. Elia, B. A. Sethuraman, and P. V. Kumar, "Perfect space-time codes for any number of antennas," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 3853–3868, 2007.

[34] J. S. Milne, "Algebraic number theory," lecture notes for a course given at the University of Michigan, Ann Arbor, *http://www.jmilne.org/math/coursenotes/*.

[35] L. Rónyai, "Algorithmic properties of maximal orders in simple algebras over Q," *Computational Complexity*, vol. 2, pp. 225–243, 1992.

[36] N. Jacobson, *Basic Algebra II*. San Francisco: W. H. Freeman and Company, 1980.

[37] L. Rónyai, "Computing the structure of finite algebras," *Journal of Symbolic Computation*, vol. 9, no. 3, pp. 355–373, Mar. 1990.

[38] S. Perlis, "Maximal orders in rational cyclic algebras of composite degree," *Transactions of the American Mathematical Society*, vol. 46, pp. 82–96, 1939.

[39] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*. Berlin: Springer, 1980.

[40] H. Koch, *Number Theory, Algebraic Numbers and Functions*. New York: American Mathematical Society, 2000.

[41] P. Ribenboim, *Classical Theory of Algebraic Numbers*. New York: Springer, 2001.

[42] PARI/GP computer algebra system, version `2.2.12`, Bordeaux, 2005, *http://pari.math.u-bordeaux.fr*.

[43] C. Hollanti and K. Ranto, "Maximal orders in space-time coding: Construction and decoding," in *Proc. 2008 Int. Symp. Inf. Theory and its Appl.*, New Zealand, Dec. 2008, pp. 1459–1463.

Camilla Hollanti received the M.Sc. and Ph.D. degrees from the University of Turku, Finland, in 2003 and 2009, respectively, both in pure mathematics.

Since June 2004, she has been with the Department of Mathematics, University of Turku, Finland. In 2005, she visited the Department of Algebra at Charles' University, Prague, Czech Republic, for six months. In 2009-2011 she will be leading the project "Applications of Class Field Theory in Present and Future Multi-Antenna Communications" at the University of Turku, Finland.

Her research is in the area of applications of algebraic number theory in lattice space-time coding.

Hollanti is a recipient of several grants from various foundations, including the Finnish Cultural Foundation research grant in 2007 and the Finnish Academy of Science research grant in 2008. She has also won the prize for the best presentation in the EWM 2007 conference of European Women in Mathematics that took place in Cambridge, UK in September 2007.

Jyrki Lahtonen (M'96) received the M.Sc. degree from University of Turku, Turku, Finland, in 1986, and the Ph.D. degree from University of Notre Dame, Notre Dame, Indiana, U.S.A. in 1990 respectively, both in pure mathematics.

He was a postdoctoral research fellow at Mathematical Sciences Research Insitute, Berkeley, California in 1990. In January 1991, he joined the faculty of the Department of Mathematics at University of Turku. Since September 2006, he has held a part-time position as a visiting fellow at Nokia Research Center, Helsinki, Finland.

His research interests include sequences, finite fields and their applications into coding theory, and space-time codes.

Kalle Ranto received the M.Sc. and Ph.D. degrees in mathematics from the University of Turku, Finland, in 1997 and 2002, respectively.

Since August 2008, he has been with Nokia Devices, Salo, Finland. His research interests include coding theory, finite fields and signal processing.

Roope Vehkalahti received the M.Sc. and Ph.D. degrees from the University of Turku, Finland, in 2003 and 2008, respectively, both in pure mathematics.

Since September 2003, he has been with the Department of Mathematics, University of Turku, Finland. His research interests include global fields and their applications in coding theory.

Publication III

Hollanti, C. and Ranto, K. (2008). Maximal orders in space-time coding: Construction and decoding. *Proceedings of 2008 International Symposium of Information Theory and Its Applications (ISITA)*, Auckland, New Zealand, pp. 1459–1463.

International Symposium on Information Theory and its Applications, ISITA2008
Auckland, New Zealand, 7-10, December, 2008

Maximal Orders in Space-Time Coding: Construction and Decoding

Camilla Hollanti[†] and Kalle Ranto[‡]

[†] Laboratory of Discrete Mathematics
for Information Technology
Turku Centre for Computer Science
Joukahaisenkatu 3–5 B, 20520 Turku, Finland
E-mail: cajoho@utu.fi

[‡] Department of Mathematics
20014 University of Turku, Finland.
E-mail: kalle.ranto@nokia.com

Abstract

Previously, it was shown why the discriminant of a maximal order within a cyclic division algebra must be minimized in order to get the densest possible matrix lattices with a prescribed non-vanishing minimum determinant. In this paper, the actual procedure of constructing maximal orders is described in more detail, aiming to provide a handy tool also for researchers with only a modest mathematical background. For instance, it is explicitly shown, step by step, how to construct a matrix lattice with QAM coefficients that has 2.5 times as many codewords as the famous Golden code of the same minimum determinant.

In order to decode maximal order based space-time codes, the usual sphere decoder has to be modified. A pseudo algorithm describing the additional steps is given. For the algorithm to function it is essential that we also speed up the search for the shortest lattice vectors ensuring in this way that the usage of a codebook becomes feasible. Both the search and the decoding can be performed by adding an upper bound on the energy of the single vector in use.

1. INTRODUCTION

[1] Recently, maximal orders have been proposed in [1]–[3] as a new design tool for cyclic division algebra (CDA) based space-time block codes (STBCs) (see e.g. [4],[5]). It was shown in [3] that in order to maximize the number of codewords in the available signal space, i.e. to maximize the *code density*, one should look for CDAs having maximal orders with minimal discriminants. Luckily, the minimum determinant of the code does not change when increasing the density in this way. However, the construction of maximal orders is somewhat difficult and involves some serious number theory. Therefore, our aim in this paper is to provide computational tools at everyone's disposal while trying to hide the theory behind.

This work was supported in part by the Finnish Cultural Foundation and the Academy of Finland, grant #108238. K. Ranto is currently with Nokia, Box 86, 24101 Salo, Finland.

2. A BRIEF OVERVIEW ON CYCLIC DIVISION ALGEBRAS AND ORDERS

We refer the interested reader to [6] and [4] for a detailed exposition of the theory of simple algebras, cyclic algebras, their matrix representations and their use in ST-coding. We only recall the basic definitions and notations here. In the following, we consider number field extensions E/F, where F denotes the base field and F^* (resp. E^*) denotes the set of the non-zero elements of F (resp. E). The ring of algebraic integers are denoted by $\mathcal{O}_F$ and $\mathcal{O}_E$, respectively. In the interesting cases the center F is an imaginary quadratic field, either $\mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt{-3})$. We assume that E/F is a cyclic field extension of degree n with the Galois group $\mathrm{Gal}(E/F) = \langle\sigma\rangle$. Let $\mathcal{A} = (E/F, \sigma, \gamma)$ be the corresponding cyclic algebra of degree n, that is

$$\mathcal{A} = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E,$$

as a (right) vector space over E. Here $u \in \mathcal{A}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in F^*$. An element $a = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{A}$ has the following standard representation as a matrix $A =$

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

In the rest of this paper, we identify an element $a \in \mathcal{A}$ with its matrix representation. E.g. when we say determinant of $a \in \mathcal{A}$, we mean $\det(A)$.

The next proposition due to A. A. Albert [6, Theorem 11.12, p. 184] tells us when a cyclic algebra is a division algebra.

Proposition 1 (Norm condition) *The cyclic algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ of degree n is a division algebra if and only if the smallest factor $t \in \mathbf{Z}_+$ of n such that γ^t is the norm of some element of E^* is n.*

Due to the above proposition, the element γ is often referred to as the *non-norm element*.

We do not give a detailed description of orders here. Instead, we try to express the notion of order as simply as possible, yet clearly enough so that one can understand the advantage it can offer us.

One of the simplest examples of an order Λ is the maximal order of an algebraic number field, which is always unique and equal to the ring of algebraic integers. E.g. for the field $F = \mathbf{Q}(i)$, the maximal order is the ring of Gaussian integers $\Lambda = \mathcal{O}_F = \mathbf{Z}[i]$. For non-commutative algebras, an order can be thought of as a generalization to the ring of algebraic integers. However, for non-commutative algebras, a maximal order is not necessarily unique, and the coefficients $x_i \in E$ in the representation $a = x_1 + \cdots + u^{n-1}x_{n-1}$ of an element a taken from an order Λ may be non-integral. If one considers integer coefficients only, the ring produced is what we call a *natural* or *layered order*:

Definition 2 *Let $\gamma \in \mathcal{O}_F$. We see that the $\mathcal{O}_E$-module*

$$\Lambda_{\text{nat}} = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E$$

is an $\mathcal{O}_F$-order in the cyclic algebra $(E/F, \sigma, \gamma)$. We refer to Λ_{nat} as the natural order. It will also serve as a starting point when searching for maximal orders.

For the purposes of constructing MIMO lattices the reason for concentrating on orders is summarized in the following proposition (e.g. [7, Theorem 10.1, p. 125]). We simply rephrase it here in the language of MIMO lattices.

Proposition 3 *Let Λ be an order in a cyclic division algebra $(E/F, \sigma, \gamma)$. Then for any non-zero element $a \in \Lambda$ its reduced norm $nr(a) := \det(a)$ is a non-zero element of the ring of integers $\mathcal{O}_F$ of the center F. In particular, if F is an imaginary quadratic number field (e.g. $F = \mathbf{Q}(i)$), then the minimum determinant of the lattice Λ is equal to one. Hence, when using an order, the non-vanishing determinant (NVD) property is automatically met and the corresponding space-time code is optimal with respect to the diversity-multiplexing tradeoff (DMT) [8].*

Definition 4 *Let $k = \dim_F \mathcal{A}$ and let $\mathcal{O}_F$ be a Euclidean domain (this is the case e.g. when $F = \mathbf{Q}(i)$ or $F = \mathbf{Q}(\sqrt{-3})$, that is, when we use QAM or HEX modulation). The discriminant of the $\mathcal{O}_F$-order Λ is the element*

$$d(\Lambda/\mathcal{O}_F) = \det tr(x_i x_j)_{i,j=1}^k,$$

where $\{x_1, \ldots, x_k\}$ is any $\mathcal{O}_F$-basis of Λ.

Proposition 5 *For the $\mathbf{Z}$-discriminant we have*

$$d(\Lambda/\mathbf{Z}) = N_{F/\mathbf{Q}}(d(\Lambda/\mathcal{O}_F)) d_{F/\mathbf{Q}}^{\dim_F \mathcal{A}},$$

where $N_{F/\mathbf{Q}}$ (resp. $d_{F/\mathbf{Q}}$) denotes the usual field norm (resp. discriminant). When $F = \mathbf{Q}(i)$, we have

$$m(\Lambda) = |d(\Lambda/\mathbf{Z}[i])|$$

(see [3] for details). Here $m(\Lambda)$ denotes the measure *of the fundamental parallelotope of Λ, i.e., the square root of the Gram determinant of the lattice.*

We know (see e.g. [3] or [7]) that all the maximal orders in the same CDA share the same discriminant, and every order is contained in some maximal order. Thus, maximal orders have the minimal discriminant in a given CDA, as from $\Gamma \subset \Lambda$ it follows that $d(\Lambda/\mathcal{O}_F) | d(\Gamma/\mathcal{O}_F)$.

Example 6 *Let us use the* Golden code *(GC) [5] and the* Golden+ code *(GC+) [3] to illustrate the above definitions. The GC is defined as the natural order of the cyclic division algebra*

$$\mathcal{GA} = (\mathbf{Q}(i, \theta)/\mathbf{Q}(i), \sigma : \theta \mapsto 1 - \theta, i),$$

where $\theta = (1 + \sqrt{5})/2$. Moreover, the ideal $(\alpha) = (1 + i - \theta)$ is used in order to get a hypercubical shape. That is,

$$GC = \left\{ \begin{pmatrix} \alpha x_0 & i\sigma(\alpha x_1) \\ \alpha x_1 & \sigma(\alpha x_0) \end{pmatrix}, \; x_0, x_1 \in \mathbf{Z}[i, \theta] \right\}.$$

Actually, the natural order of the Golden algebra $\mathcal{GA}$ is also a maximal order as was shown already in [2], so it is not possible to get a denser lattice by using some other order inside $\mathcal{GA}$. For the order Λ corresponding to the GC we get

$$m(\Lambda) = d(\Lambda/\mathbf{Z}[i]) = 25$$

by Definition 4 and Proposition 5.

In [3], the Golden+ code was constructed as a maximal order of the algebra

$$\mathcal{GA}+ = (\mathbf{Q}(s)/\mathbf{Q}(i), \sigma : s \mapsto -s, i),$$

where $s = \sqrt{2+i}$. Further, the ideal $(\beta) = ((1-s)^3)$ was used to force the maximal order inside the natural order. The resulting code lattice is as much as 2.5 times denser than the Golden code lattice, as we now have

$$m(\Lambda) = d(\Lambda/\mathbf{Z}[i]) = 10$$

by Definition 4 and Proposition 5 (see [3] for more details).

3. CONSTRUCTING MAXIMAL ORDERS

Maximal orders are somewhat tricky to construct by hand. Luckily, the construction algorithm from [9] is implemented in the MAGMA software [10]. In what follows, we explain the required steps for producing a maximal order of the algebra $\mathcal{GA}+$ (denoted by `A` in Table 1). First of all, one needs to define the algebra with *relations*. In $\mathcal{GA}+$ the following relations hold:

$$i^2 = -1,\ s^2 = 2+i,\ u^2 = i,\ su = -us.$$

Now we can start with MAGMA (an explicit sign * is required for the multiplication).

Table 1: Constructing maximal orders with MAGMA

```
% magma
> Q:=Rationals();
> A<i, s, u> := FPAlgebra< Q, i, s, u |
i^2+1, s^2-2-i, u^2-i, s*u+u*s >;
> Dimension(A);
8
> S,s:=Algebra(A); Inv:=Inverse(s);
> for i:=1 to 8 do print Inv(Basis(S)[i]);
end for;
1, u, s, i, u*s, u*i, s*i, u*s*i
/* natural order basis */
> M:=MaximalOrder(S);
> Factorization(Discriminant(M));
[ <2, 10>, <5, 2> ]
/* Z-discriminant equals 2^10 · 5^2 */
> Basis(M);
[ (1/2 1/2 1/2 1/2 1/2 1/2 1/2 7/2),
(0 1/2 1/2 0 0 1/2 1/2 2),
(0 0 1 0 0 0 0 1),
(0 0 0 1/2 1/2 1/2 1/2 2),
(0 0 0 0 1 0 0 1),
(0 0 0 0 0 1 0 1),
(0 0 0 0 0 0 1 1),
(0 0 0 0 0 0 0 1) ]
/* maximal order basis */
```

In Table 1 above, `FPAlgebra` stands for "Finitely Presented Algebra", and `S,s:=Algebra(A)` translates $\mathcal{GA}+$ into an algebra S presented by a multiplication table, and a mapping $s : \mathcal{GA}+ \to S$ is attached to the algebra $\mathcal{GA}+$. This step is needed for the `MaximalOrder` command. For the $\mathcal{GA}$ the natural order is also a maximal order. For the $\mathcal{GA}+$ this is not the case. Instead, we get a maximal order basis (see the last output in Table 1)

$$\begin{aligned}\{f_j\}_{1\le j\le 8} &= \{1/2(\sum_{k=1}^{8} e_i),\\ &\quad 1/2(e_2+e_3+e_6+e_7), e_3,\\ &\quad 1/2(e_4+e_5+e_6+e_7), e_5, e_6, e_7, e_8\},\end{aligned}$$

where

$$\{e_j\}_{1\le j\le 8} = \{1, u, s, i, us, ui, si, usi\}$$

denotes the natural order basis. Note that we have simplified the basis by subtracting multiples of f_8 from the other (original) basis elements $f_1, ..., f_7$.

MAGMA is a commercial software but the commands in Table 1 can be executed in a free online MAGMA calculator [10]. This computation takes a half a second time (there is a limit of 20 seconds) and 7.36MB total memory.

4. POWER CONTROLLED DECODING

We base our sphere decoder on the algorithm in [11] (see also [12]). However, the basic sphere decoder has to be modified, as we need to use a codebook in order to get the full advantage of the density provided by maximal orders.

Example 7 *For the orthogonal GC it is clear that the 2^8 PAM vectors giving the shortest codewords are those with ± 1 in every coordinate. For the non-orthogonal GC+ (see [13] for the basis matrices) the situation is completely different: Even after the standard LLL procedure, e.g., the vector*

$$(1, 1, 1, 1, 3, 1, 1, -1)$$

results in a substantially shorter codeword than the vector

$$(1, 1, 1, 1, -1, -1, -1, 1)$$

(and over 200 other vectors with ± 1s).

The sphere decoding algorithm is quite flexible allowing different kind of modifications. In the so-called code controlled sphere decoding (CCSD) [14] the algorithm was modified by adding certain parity checks to

distinguish the valid codewords. Here we do not assume any simple structure for the codewords but identify the valid codewords by limiting the maximal Euclidean norm.

Our main idea for the codebook construction and sphere decoding was introduced already in [11, Section V.A]: we take the codewords with integer coordinates in some fixed interval $I \subset \mathbf{Z}$ that are in an m-dimensional sphere with a given squared radius P^2. As the Euclidean norm of the vectorized codeword corresponds to the transmitted signal energy, we are actually taking the lattice points which are below some fixed power limit P^2.

In contrast to [11] where the additional power limit was checked only in the end, i.e., when the decoder had found an otherwise valid point, we suggest this check to be done cumulatively in the same manner as the usual sphere decoding check (see STEP 3 in the algorithm). In other words, in our modified algorithm the boundary condition check is conducted in various intermediate steps while in [11] it was done only at leafs of the equivalent tree search. This idea is useful also in the search for the codebook: it is quite evident that for larger lattice dimensions the running time for the search decreases dramatically when using the proposed cumulative approach.

Both the power controlled codebook construction and the power controlled sphere decoding (PCSD) have the same first steps of preprocessing: The complex basis matrices $M_i \in \mathbf{C}^{m\times m}$ of the code lattice are vectorized and written as columns in a real matrix $B' \in \mathbf{R}^{2m^2\times m}$. Then applying QR decomposition on B' we get $B' = Q'R'$ with an upper triangular matrix $R' = (r'_{i,j})_{i,j=1}^m$. Now, the integer vectors $\mathbf{x}$ that admit to the allowed power limit satisfy

$$|B'\mathbf{x}|^2 = |Q'R'\mathbf{x}|^2 = |R'\mathbf{x}|^2 \le P^2.$$

In the search for the shortest vectors, we first assign the last coordinate with some value in I similarly as in the sphere decoding. Here it does not matter whether we use Pohst or Schnorr–Euchner enumeration as we want to check the whole interval. With the given power limit P^2 we check all those coordinates in the search tree which are in I and whose cumulative norms so far do not violate the power limit P^2. The details of this power limit check are integrated in the PCSD algorithm given below.

In PCSD, the basis matrix B' needs to be preprocessed only once, whereas the usual QR decomposition is carried out for every channel matrix H: the channel matrix multiplied by the basis matrices, HM_i, are vectorized and written as columns in a real matrix $B = QR$. Now the upper triangular matrix $R = (r_{i,j})_{i,j=1}^m$ is used to check whether the node in the search tree is still inside the sphere of a given squared radius C_0 in the receiving end. On the other hand, the upper triangular matrix R' is used to check whether the same node is still inside the sphere of a given squared radius P^2 in the transmitting end.

Finally, we present here the new PCSD algorithm as a pseudo-code. All modifications as compared to [11] have been framed. The algorithm can be used directly with the lattice points themselves, i.e., the interval I can equal e.g. $\{-3,-2,\ldots,2,3\}$. We can equally well use PAM coefficients, e.g. $\{-3,-1,1,3\}$, by scaling them to an interval $\{0,1,2,3\}$ but then the energy counting in STEP 3 must be modified. Another possibility with PAM coefficients is to modify the update rules for x_i and Δ_i in STEP 2 and 6.

Algorithm II, Smart Implementation (Input C'_0, $\mathbf{y}'$, R, framed[R', P^2]. Output $\hat{\mathbf{x}}$.)

STEP 1: (Initialization) Set $i := m$, $T_m := 0$, $\xi_m := 0$, framed[$P_m := 0$, $\eta_m =: 0$], and $d_c := C'_0$ (current sphere radius).

STEP 2: (DFE on x_i) Set $x_i := \lfloor (y'_i - \xi_i)/r_{i,i} \rceil$ and $\Delta_i := \mathrm{sign}(y'_i - \xi_i - r_{i,i}x_i)$.

STEP 3: (Main step) If $d_c < T_i + |y'_i - \xi_i - r_{i,i}x_i|^2$, then go to STEP 4 (i.e., we are outside the sphere).

Else if $x_i \notin I$ framed[or $P^2 < P_i + |r'_{i,i}x_i + \eta_i|^2$], go to STEP 6

(i.e., we are inside the sphere but outside the signal set boundaries).

Else (i.e., we are inside the sphere and signal set boundaries) if $i > 1$, then

{let $\xi_{i-1} := \sum_{j=i}^m r_{i-1,j}x_j$,
$T_{i-1} := T_i + |y'_i - \xi_i - r_{i,i}x_i|^2$,
framed[$\eta_{i-1} := \sum_{j=i}^m r'_{i-1,j}x_j$, $P_{i-1} := P_i + |r'_{i,i}x_i + \eta_i|^2$],
$i := i - 1$, and go to STEP 2}.

Else (i=1) go to STEP 5.

STEP 4: (Backtracking) If $i = m$, terminate, else set $i := i + 1$ and go to STEP 6.

STEP 5: (A valid point is found) Let $d_c := T_1 + |y'_1 - \xi_1 - r_{1,1}x_1|^2$, save $\hat{\mathbf{x}} := \mathbf{x}$, let $i := i + 1$, and go to STEP 6.

STEP 6: (Schnorr–Euchner enumeration of level i) Let $x_i := x_i + \Delta_i$, $\Delta_i := -\Delta_i - \mathrm{sign}(\Delta_i)$, and go to STEP 3.

5. Conclusions

In this paper, we wanted to clarify the construction and decoding of maximal order based space-time codes. By introducing the required MAGMA commands and by explicitly pointing out the additional steps needed for (spherical) sphere decoding, we hope that we managed to bring the topic more down-to-earth to non-experts.

Maximal orders are used in space-time coding for the reason that they provide denser lattices and hence larger coding gains as compared to the conventional CDA codes based on natural orders. Recently, Kumar and Caire [15] have showed that the problem of maintaining a codebook can be overcome by using *sphere encoding*. By computer simulations they have shown that the maximal order based codes [3] outperform all the best previously known codes, e.g. the Perfect codes [5], when using two or three antennas. Promising results have been achieved also in the asymmetric scenario [16] and in the MIMO multiple access channels [17]. Hence, our hope is that maximal orders would be more widely adopted to the field of space-time coding.

References

[1] C. Hollanti, J. Lahtonen, and H.-f. (F.) Lu, "Maximal Orders in the Design of Dense Space-Time Lattice Codes", *IEEE Trans. Inf. Theory*, vol. 54, Oct. 2008. http://arxiv.org/abs/0803.2639

[2] C. Hollanti and J. Lahtonen, "A New Tool: Constructing STBCs from Maximal Orders in Central Simple Algebras", in *Proc. IEEE ITW 2006*, pp. 322–326, Punta del Este, March 13–17, 2006.

[3] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, "On the Densest MIMO Lattices from Cyclic Division Algebras", to appear in *IEEE Trans. Inf. Theory*. Preliminary version of has appeared in ISIT 2006. The full manuscript is available at: http://arxiv.org/abs/cs.IT/0703052.

[4] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-Diversity, High-Rate Space-Time Block Codes From Division Algebras", *IEEE Trans. Inf. Theory*, vol. 49, pp. 2596–2616, October 2003.

[5] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect Space-Time Block Codes", *IEEE Trans. Inf. Theory*, vol. 52, pp. 3885–3902, September 2006.

[6] A. A. Albert, *Structure of Algebras*, AMS, 1939.

[7] I. Reiner, *Maximal Orders*, Academic Press, 1975.

[8] L. Zheng and D. Tse, "Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels", *IEEE Trans. Inf. Theory*, vol. 49, pp. 1073–1096, May 2003.

[9] G. Ivanyos and L. Rónyai, "Finding maximal orders in semisimple algebras over Q", *Computational Complexity*, vol. 3, pp. 245–261, 1993.

[10] MAGMA homepage, University of Sydney, Australia: http://magma.maths.usyd.edu.au/

[11] M. O. Damen, H. El Gamal, and G. Caire, "On Maximum-Likelihood Detection and the Search for the Closest Lattice Point", *IEEE Trans. Inf. Theory*, vol. 49, pp. 2389–2402, October 2003.

[12] E. Viterbo and J. Boutros, "A Universal Lattice Code Decoder for Fading Channel", *IEEE Transactions on Information Theory*, vol. 45, pp. 1639–1642, July 1999.

[13] J. Lahtonen and R. Vehkalahti, "Dense MIMO Matrix Lattices — A Meeting Point for Class Field Theory and Invariant Theory", in *Proc. AAECC-17*, Springer LNCS 4851, pp. 247–256, 2007.

[14] C. Hollanti, "Code Controlled Sphere Decoding of Four Efficient MISO Lattices", in *Proc. ISITA 2006*, Seoul, Oct. 29–Nov. 1, 2006.

[15] K. Raj Kumar and Giuseppe Caire, "Space-Time Codes from Structured Lattices", to appear in *IEEE Trans. Inf. Theory*. Available at: http://www.citebase.org/abstract?id=oai:arXiv.org:0804.1811.

[16] C. Hollanti and H.-F. Lu, "Construction Methods for Asymmetric and Multi-Block Space-Time Codes", submitted to *IEEE Trans. Inf. Theory*, Dec. 2007.

[17] H.-F. Lu, C. Hollanti, J. Lahtonen, R. Vehkalahti, Y. Hong, and E. Viterbo, "Optimal Code Construcions for Two-User Multiple Access Channels", under preparation.

Publication IV

Hollanti, C., Lahtonen, J., Ranto, K., Vehkalahti, R., and Viterbo, E. (2008). On the algebraic structure of the Silver code: A 2×2 Perfect space-time code with non-vanishing determinant. *Proceedings of 2008 IEEE Information Theory Workshop (ITW)*, Porto, Portugal, pp. 91–94.

On the Algebraic Structure of the Silver Code: a 2×2 Perfect Space-Time Block Code

C. Hollanti, J. Lahtonen, K. Ranto, R. Vehkalahti, E. Viterbo

I. Introduction

A family of full-rate, full-diversity STBCs for 2×2 MIMO was recently proposed in [1], [2], [3], [4] using a combination of *Clifford-algebra* and Alamouti structures [5], namely *twisted space–time transmit diversity* code. This family was recently rediscovered in [6], where it was also pointed out that such STBCs enable reduced-complexity ML decoding (see also [7] for details). Independently, the same STBCs were found in [8], and named *multi-strata* space–time codes.

In this paper we show how this code can be constructed algebraically from a particular cyclic division algebra. This formulation enables to prove that the code has the non-vanishing determinant property [9] and hence achieves the diversity-multiplexing tradeoff (DMT) optimality [10]. The fact that the normalized minimum determinant [11] is $1/\sqrt{7}$ places this code in the second position with respect to the Golden code [9], which exhibits a minimum determinant of $1/\sqrt{5}$, and motivates the name *silver code*.

The silver code was originally designed to have the cubic shaping property of perfect space–time codes [12], but not the non-vanishing determinant property, which was only conjectured, after it was verified up to 64–QAM.

II. System model and notation

We are interested in the coherent $n \times n$ MIMO-case where the receiver perfectly knows the channel coefficients. The $n \times n$ received signal matrix is

$$Y = HX + N,$$

where H is the Rayleigh fading channel response matrix, the elements of the noise matrix N are i.i.d. complex Gaussian random variables and X is the $n \times n$ transmitted codeword taken from the MIMO-lattice $\Lambda \subset \mathcal{M}_n(\mathbf{C})$, the set of $n \times n$ matrices over the complex field $\mathbf{C}$.

A lattice, i.e., a discrete free abelian group, is determined by its basis $X_1, X_2, \ldots, X_k$ consisting of $n \times n$ matrices that are linearly independent over the field of real numbers. The rank k is thus bounded from above by $2n^2$. A lattice is said to have *full rank*, if $k = 2n^2$. We are interested in the full rank lattices since they yield the full rate space-time codes, with the maximum multiplexing gain.

C. Hollanti, J. Lahtonen, K. Ranto, R. Vehkalahti are with University of Turku and Turku Centre for Computer Science, Finland. E-mails:{cajoho, lahtonen, kara, roiive}@utu.fi. J. Lahtonen is also a Visiting Fellow at NRC, Helsinki, Finland. E. Viterbo is with DEIS - Università della Calabria, Via P. Bucci, 42/C, 87036 Rende (CS), Italy and Visiting Fellow at NRC, Helsinki, Finland. E-mail: {viterbo}@deis.unical.it. This work was supported by the STREP project No. IST-026905 (MASCOT) within the Sixth Framework Programme of the European Commission.

The *Gram matrix* of Λ is defined by

$$G = \left(\Re[\mathrm{Tr}(X_i X_j^\dagger)]\right)_{1 \le i,j \le k}$$

where $\Re$ denotes the real part, Tr denotes the trace of the matrix and $\dagger$ denotes Hermitian transposition. The *determinant* of Λ is defined as $\det(\Lambda) = \det(G)$. The measure, or hypervolume, $m(\Lambda)$ of the *fundamental parallelotope* of the lattice is related to the lattice determinant by $\det(\Lambda) = m(\Lambda)^2$.

Given that any $n \times n$ codeword X from a space-time codebook $\mathcal{C} \subseteq \Lambda$ corresponds to a lattice point of Λ, we define the *minimum determinant* of the code as

$$\min_{X \neq X' \in \mathcal{C}} \det(X - X').$$

For the infinite code $\mathcal{C} = \Lambda$ this can be rewritten as

$$\min_{X \in \mathcal{C} \setminus \{0\}} \det(X),$$

since the difference of any two lattice points is again a lattice point.

As the minimum determinant determines the asymptotic pairwise error probability (PEP), this gives rise to natural numerical measures for the quality of a code.

If all the codebooks of any size contained in Λ have a minimum determinant bounded from below by a non-zero constant, we say that Λ has the *non-vanishing determinant property* and we define

$$\Delta(\Lambda) = \min_{X \in \Lambda \setminus \{0\}} \det(X)$$

If we consider a scaled lattice $r\Lambda$ for some real constant $r > 0$, we have $m(r\Lambda) = r^k m(\Lambda)$ and $\Delta(r\Lambda) = r^n \Delta(\Lambda)$. We can choose r to normalize either $\Delta(\Lambda) = 1$ or $m(\Lambda) = 1$. In order to define a signal-to-noise ratio we can also choose r so that the entries of the codeword matrices have unit average energy, i.e., $\mathbb{E}(x_{ij}) = 1$.

Following [11], we first scale Λ to have a unit size fundamental parallelotope, and denote by $\delta(\Lambda)$ the *normalized minimum determinant* of the lattice Λ. We omit Λ from the paranthesis, whenever the lattice is clear from the context. To make fair comparisons between the minimum determinants of various codes, one should always use the normalized minimum determinant.

For example, the Golden code has $\delta = 1/\sqrt{5}$, when considering unit hypervolume and $\delta = 4/\sqrt{5}$, when assuming $\pm 1, \pm 3, \ldots$ as integer components for the QAM symbols.

III. SILVER CODE AS A CYCLIC DIVISION ALGEBRA

The silver code S is defined in [1], [2], [3], [4] as

$$S = \{X = X_A + TX_B \mid x_1, x_2, x_3, x_4 \in \mathbf{Z}[i]\},$$

where

$$X_A = X_A(x_1, x_2) = \begin{pmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{pmatrix},$$

$$X_B = X_B(z_1, z_2) = \begin{pmatrix} z_1 & -z_2^* \\ z_2 & z_1^* \end{pmatrix},$$

the twisting matrix

$$T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = U \begin{pmatrix} x_3 \\ x_4 \end{pmatrix}$$

with a unitary matrix

$$U = \frac{1}{\sqrt{7}} \begin{pmatrix} 1+i & -1+2i \\ 1+2i & 1-i \end{pmatrix}.$$

We can also think of the code S as a (full) rank 8 lattice $\subseteq \mathcal{M}_2(\mathbf{C})$.

Let us first introduce the basic definitions that are used throughout the paper. In the following, we consider number field extensions E/F, where F denotes the base field and F^* (resp. E^*) denotes the set of the non-zero elements of F (resp. E). Usually, F is an imaginary quadratic field, either $\mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt{-3})$ in order to match the QAM and HEX modulation schemes [12]. We assume that E/F is a cyclic field extension of degree n with Galois group $\mathrm{Gal}(E/F) = \langle\sigma\rangle$. Let $\mathcal{A} = (E/F, \sigma, \gamma)$ be the corresponding cyclic algebra of degree n (n is also called the *index* of $\mathcal{A}$), that is

$$\mathcal{A} = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E,$$

as a (right) vector space over E. Here $u \in \mathcal{A}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in F^*$. An element

$$a = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{A}$$

has the following representation as a matrix

$$A = \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

We refer to this as the *standard matrix representation* of $\mathcal{A}$ and identify an element of a CDA with its standard matrix representation.

Definition 3.1: The determinant of the matrix A above is called the *reduced norm* of the element $a \in \mathcal{A}$ and is denoted by $nr(a)$.

The next proposition due to A. A. Albert [13, Theorem 11.12, p. 184] tells us when a cyclic algebra is a division algebra.

Proposition 3.1 (Norm condition): The cyclic algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ of degree n is a division algebra if and only if the smallest factor $t \in \mathbf{Z}_+$ of n such that γ^t is the norm of some element of E^* is n.

Lemma 3.2: The silver code S is contained as a subset in the cyclic division algebra $\mathcal{A}$ defined as

$$\mathcal{A} = (E/F, \sigma, \gamma),$$

where the center is $F = \mathbf{Q}(\sqrt{-7})$, $E = F(i)$, $\gamma = -1$, and

$$\sigma : \begin{cases} i \mapsto -i \\ \sqrt{7} \mapsto -\sqrt{7}. \end{cases}$$

Proof. As $\sigma(i) = -i = i^*$, the matrix

$$X_A = \begin{pmatrix} x_1 & \gamma\sigma(x_2) \\ x_2 & \sigma(x_1) \end{pmatrix} \in \mathcal{A}.$$

Let us calculate the basis matrices coming from the part TX_B of the code matrix, i.e. we compute $TX_B(z_1, z_2)$, where (x_3, x_4) ranges over the set $\{(1,0), (0,1), (i,0), (0,i)\}$. We end up with the following four basis matrices:

$$\frac{1}{\sqrt{-7}} \begin{pmatrix} -1+i & -2-i \\ 2-i & -1-i \end{pmatrix}, \frac{1}{\sqrt{-7}} \begin{pmatrix} -2-i & 1-i \\ -1-i & -2+i \end{pmatrix},$$

$$\frac{1}{\sqrt{-7}} \begin{pmatrix} -1-i & -1+2i \\ 1+2i & -1+i \end{pmatrix}, \frac{1}{\sqrt{-7}} \begin{pmatrix} 1-2i & -1-i \\ 1-i & 1+2i \end{pmatrix}.$$

Here we have written $\frac{1}{\sqrt{7}} = \frac{1}{-i\sqrt{-7}} = \frac{i}{\sqrt{-7}}$ and multiplied i into the matrices. We see that all these basis matrices are of the form

$$\frac{1}{\sqrt{-7}} \begin{pmatrix} a & \gamma\sigma(b) \\ b & \sigma(a) \end{pmatrix},$$

where $a, b \in \mathbf{Z}[i]$. Thus, both summands in X are elements of $\mathcal{A}$ and $X \in \mathcal{A}$.

Now it remains to prove that $\mathcal{A}$ is a division algebra, i.e. (according to A. A. Albert) there does not exist an element $x \in E$ for which $N_{E/F}(x) = -1$.

We shall work in the extension fields of the 2-adic field $\mathbf{Q}_2$ By Hensel's lifting any integer m congruent to 1 modulo 8 has a square root in $\mathbf{Q}_2$. In particular $\sqrt{-7} \in \mathbf{Q}_2$. Thus we can view the field F as a subfield of $\mathbf{Q}_2$. For the sake of being definite we may choose $\sqrt{-7} \equiv 1 \pmod 4$. Similarly, the field E can be viewed as a subfield of $\mathbf{Q}_2(i)$. Furthermore, the norm map $N_{E/F} : E \to F$ is then a restriction of the norm map $N : \mathbf{Q}_2(i) \to \mathbf{Q}_2$, which, obviously, can be defined via the formula $N(a + bi) = a^2 + b^2$ for all $a, b \in \mathbf{Q}_2$.

Thus, in order to prove our claim, it is sufficient to show that -1 is not in the image of the map N. Assume, on the contrary, that there are 2-adic numbers a and b such that $a^2 + b^2 = -1$. We shall first show that then both a and b must be 2-adic integers. So we assume that at least one of them has a negative exponential 2-adic valuation. The non-archimedean triangle inequality then implies that $v_2(a) = v_2(b)$. In other words, there must exist an integer $t < 0$ such that $a = 2^t a'$, $b = 2^t b'$ with a', b' 2-adic units. But then $a'^2 \equiv b'2 \equiv 1 \pmod 4$, so $v_2(a^2 + b^2) = 2t + 1$ is an odd integer, and hence $a^2 + b^2$ cannot be a 2-adic unit unless both a and b are 2-adic integers. In this case our claim now easily follows from a modulo 8 consideration: the square of an integer is always

congruent to either 0, 1 or 4 modulo 8. Thus the sum of two such squares cannot be congruent to 7 modulo 8. In particular, it cannot be equal to -1. ■

In what follows, we denote the natural order of $\mathcal{A}$ by

$$\Lambda = \mathcal{O}_E \oplus u\mathcal{O}_E,$$

where the ring of integers of E is

$$\mathcal{O}_E = \mathbf{Z}[i] \oplus \frac{1+\sqrt{-7}}{2}\mathbf{Z}[i].$$

For the purposes of constructing MIMO lattices the reason for concentrating on orders is summarized in the following proposition (e.g. [14, Theorem 10.1, p. 125]). We simply rephrase it here in the language of MIMO-lattices.

Proposition 3.3: Let Λ be an order in a cyclic division algebra $(E/F, \sigma, \gamma)$. Then for any non-zero element $a \in \Lambda$ its reduced norm $nr(a)$ is a non-zero element of the ring of integers $\mathcal{O}_F$ of the center F. In particular, if F is an imaginary quadratic number field, then the minimum determinant of the lattice Λ is equal to one.

Theorem 3.4: The silver code S has a nonvanishing determinant and $\min\det(S) \geq 1/7$.

Proof. When looking at the codeword matrices $X = X_A + TX_B \in \Lambda \oplus \frac{1}{\sqrt{-7}}\Lambda$, it is obvious that $\sqrt{-7}S \subseteq \Lambda$ and thus $S \subseteq \frac{1}{\sqrt{-7}}\Lambda$. Now

$$\min\det(S) \geq \left|\min\det(\frac{1}{\sqrt{-7}}\Lambda)\right| = \frac{1}{7}\min\det(\Lambda) = \frac{1}{7}.$$

■

The actual minimum determinant is better than $1/7$, it is equal to $2/\sqrt{7}$ (based on numerical calculations up to 64-QAM) which corresponds to a normalized minimum determinant $1/\sqrt{7}$.

Remark 3.1: In the draft [15] the non-vanishing determinant property is proved numerically in the special cases of PAM and QAM constellations by exploiting just the lattice structure. They derive the normalized minimum determinant $4/\sqrt{7}$ for QAM signal constellations.

Our proof extends the NVD property to any signal constellation $\mathcal{X} \subseteq \mathbf{Z}^8$ of an arbitrary size though we do not, at least not yet, get the exact minimum determinant from our algebraic proof. The code generates an ideal in the lattice, and determining this ideal is the key point to the problem. At this point, we know that the code is not a principal ideal of the natural (nor maximal) order.

Here we have shown (at least up to 64-QAM) that $\min\det(S) = 2/\sqrt{7}$, corresponding to a normalized minimum determinant $\delta(S) = 1/\sqrt{7}$, which is only slightly worse than $\delta(G) = 1/\sqrt{5}$ for the Golden code G and well worth the loss due to much simpler decoding it enables.

Remark 3.2: The silver code is actually a Perfect code [12], as its Gram matrix is orthogonal and the non-norm element is a unit.

IV. Conclusions

We have presented the interesting algebraic structure of the silver code, a 2×2 perfect space-time code with a non-vanishing (normalized) minimum determinant $\geq 1/7$. By computer checks we have verified that the actual normalized minimum determinant is equal to $1/\sqrt{7}$.

This code is very attractive for applications since its error rate performance is only slightly (0.3dB) worse than the one of the Golden code but offers the advantage of reduced complexity decoding.

References

[1] O. Tirkkonen and A. Hottinen, "Square-matrix embeddable space–time block codes for complex signal constellations," in *IEEE Trans. Inform. Theory*, vol. 48, no. 2, , pp. 384–395, February 2002.

[2] O. Tirkkonen and R. Kashaev, "Combined information and performance optimization of linear MIMO modulations," in Proc *IEEE Int. Symp. Inform. Theory (ISIT 2002)*, Lausanne, Switzerland, p. 76, June 2002.

[3] A. Hottinen and O. Tirkkonen, "Precoder designs for high rate space–time block codes," in Proc. *Conference on Information Sciences and Systems*, Princeton, NJ, March 17–19, 2004.

[4] A. Hottinen, O. Tirkkonen and R. Wichman, "Multi-antenna Transceiver Techniques for 3G and Beyound," WILEY publisher, UK.

[5] S. M. Alamouti, "A simple transmit diversity technique for wireless communication", *IEEE J. on Select. Areas in Commun.*, vol. 16, pp. 1451–1458, October 1998.

[6] J. Paredes, A.B. Gershman, and M. G. Alkhanari, "A 2×2 space–time code with non-vanishing determinants and fast maximum likelihood decoding," in Proc *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2007)*, Honolulu, Hawaii, USA, pp. 877–880, April 2007.

[7] E. Biglieri, Y. Hong, and E. Viterbo, "On fast-decodable space-time block codes," submitted to *IEEE Trans. Inform. Theory*, available at http://arxiv.org/abs/0708.2804v1

[8] M. Samuel and M. P. Fitz, "Reducing the detection complexity by using 2×2 Multi-Strata space–time codes," in Proc *IEEE Int. Symp. Inform. Theory (ISIT 2007)*, pp. 1946–1950, Nice, France, June 2007.

[9] J.-C. Belfiore, G. Rekaya, and E. Viterbo: "The Golden code: A 2x2 full-rate space-time code with non-vanishing determinant", *IEEE Transactions on Information Theory*, vol. 51, n. 4, pp. 1432–1436, April 2005.

[10] L. Zheng and D. Tse, "Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels", *IEEE Trans. Inf. Theory*, vol. 49, pp. 1073–1096, May 2003.

[11] J. Lahtonen, "Dense MIMO matrix lattices and class field theoretic themes in their construction", in *Proc. IEEE ITW 2007*, pp. 96–100, Bergen, Norway, July 2007.

[12] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "perfect space-time block codes", *IEEE Trans. Inf. Theory*, vol. 52, pp. 3885–3902, September 2006.

[13] A. A. Albert, *Structure of algebras*, American Mathematical Society, New York City 1939.

[14] I. Reiner, *Maximal orders*, Academic Press, New York 1975.

[15] J. M. Paredes, A. B. Gersham, and M. Gharavi-Alkhansari, "A new full-rate full-diversity space-time block code with non-vanishing determinants and simplified maximum likelihood decoding", submitted.

Publication V

Hollanti, C. and Lu, H.-F. (2008). Construction methods for asymmetric and multi-block space-time codes. *IEEE Transactions on Information Theory* (in press).

Construction Methods for Asymmetric and Multi-Block Space-Time Codes

Camilla Hollanti and Hsiao-feng (Francis) Lu, *Member, IEEE*

***Abstract*— In this paper, the need for the construction of asymmetric and multi-block space-time codes is discussed. Above the trivial puncturing method, i.e. switching off the extra layers in the symmetric multiple input-multiple output (MIMO) setting, two more sophisticated asymmetric construction methods are proposed. The first method, called the Block Diagonal Method (BDM), can be converted to produce multi-block space-time codes that achieve the diversity-multiplexing tradeoff (DMT). It is also shown that maximizing the density of the newly proposed block diagonal asymmetric space-time (AST) codes is equivalent to minimizing the discriminant of a certain order, a result that also holds as such for the multi-block codes. An implicit lower bound for the density is provided and made explicit for an important special case that contains e.g. the systems equipped with 4Tx+2Rx antennas. Further, an explicit scheme achieving the bound is given. Another method proposed here is the Smart Puncturing Method (SPM) that generalizes the subfield construction method proposed in earlier work by C. Hollanti and K. Ranto and applies to any number of transmitting and lesser receiving antennas.**

The use of the general methods is demonstrated by building explicit, sphere decodable codes using different cyclic division algebras (CDAs). Computer simulations verify that the newly proposed methods can compete with the trivial puncturing method, and in some cases clearly outperform it. The conquering construction exploiting maximal orders improves upon the punctured perfect code and the DjABBA code as well as the Icosian code. Also extensive DMT analysis is provided.

***Index Terms*— Asymmetric space-time block codes (AST-BCs), cyclic division algebras (CDAs), dense lattices, discriminants, diversity-multiplexing tradeoff, maximal orders, multi-block codes, multiple-input multiple-output (MIMO) channels, normalized minimum determinant.**

I. Introduction

Multiple-antenna wireless communication promises very high data rates, in particular when we have perfect channel state information (CSI) available at the receiver. In [1] the design criteria for such systems were developed, and further on the evolution of space-time (ST) codes took two directions: trellis codes and block codes. Our work concentrates on the latter branch and especially on the so-called asymmetric and multi-block space-time codes. We are interested in the coherent multiple input-multiple output (MIMO) case where the receiver perfectly knows the channel coefficients. The received signal is

$$Y = HX + N,$$

where X is the transmitted codeword taken from the Space-Time Block Code (STBC) $\mathcal{C}$, H is the Rayleigh fading channel response matrix and the elements of the noise matrix N are i.i.d. complex Gaussian random variables. Throughout the paper, n_t (resp. n_r) denotes the number of transmitting (resp. receiving) antennas #Tx (resp. #Rx).

From the pairwise error probability (PEP) point of view [2], the performance of a space-time code is dependent on two parameters: *diversity gain* and *coding gain*. Diversity gain is the minimum of the rank of the difference matrix $X - X'$ taken over all distinct code matrices $X, X' \in \mathcal{C}$, also called the *rank* of the code $\mathcal{C}$. For non-zero square matrices, being full-rank coincides with being invertible. When $\mathcal{C}$ is full-rank, the coding gain is proportional to the determinant of the matrix $(X - X')(X - X')^\dagger$, where $\dagger$ indicates the complex conjugate transpose of a matrix. The minimum of this determinant taken over all distinct code matrices is called the *minimum determinant* of the code $\mathcal{C}$. If it is bounded away from zero even in the limit as the spectral efficiency approaches infinity, the ST code is said to have the *non-vanishing determinant* (NVD) property [3]. Note that the minimum determinant defined here is actually the square of the minimum determinant of a lattice defined below.

Definition 1.1: The *data rate* R in bits per channel use (bpcu) is given by

$$R = \frac{1}{T}\log_2(|\mathcal{C}|),$$

where $|\mathcal{C}|$ is the size of the code, and T is the block length.

Here, the *code rate* is defined as the ratio of the number of transmitted information symbols (complex, e.g. QAM symbols) to the decoding delay (equivalently, block length) of these symbols at the receiver for any given number of transmit antennas using any complex signal constellations. If this ratio is equal to the delay, the code is said to have *full rate*.

The very first STBC for two transmit antennas was the *Alamouti code* [4] representing multiplication in the ring of quaternions. As the quaternions form a division algebra, such matrices must be invertible, i.e. the resulting STBC meets the rank criterion. Matrix representations of other division algebras have been proposed as STBCs in various papers, e.g. [5]-[18] to name just a few. Major amount of the work

The material in this paper was presented in part at the IEEE Information Theory Workshop, Bergen, Norway, July 2007, and at the IEEE International Symposium on Information Theory, Toronto, Canada, July 2008. The research of C. Hollanti is supported in part by the Finnish Cultural Foundation, the Finnish Academy of Science, and the Foundation of the Rolf Nevanlinna Institute, Finland.

C. Hollanti is currently with Department of Mathematics, FI-20014 University of Turku, Finland (e-mail: cajoho@utu.fi). During this work she was with Laboratory of Discrete Mathematics for Information Technology, Turku Centre for Computer Science, Finland.

H.-f. Lu is with Department of Communications Engineering, National Chiao Tung University, 1001 University Rd., Hsinchu 300, Taiwan ((e-mail: francis@cc.nctu.edu.tw).

in recent years has concentrated on adding multiplexing gain and/or combining it with a good minimum determinant, so that the resulting constructions can achieve the so-called diversity-multiplexing tradeoff (DMT) in [19]. It has been shown in [15] that cyclic division algebra (CDA) based square ST codes with the NVD property achieve the DMT. This result also extends over multi-block space-time codes [20]. The codes proposed in [17] all fall into this category (as do many other codes too) and are in that sense optimal. One of the goals of this paper is to generalize some of the results of [17] to the asymmetric and multi-block case.

After a cyclic division algebra has been chosen, the next step is to choose a corresponding lattice, or what amounts to the same thing, to choose an order within the algebra. Most authors, including [10] and [15], have gone with the so-called natural order (see the next section for a definition). One of the points the authors wanted to emphasize in [17] was to use maximal orders instead. The idea is that one can sometimes use several cosets of the natural order and hence transmit at a higher rate without sacrificing anything in terms of the minimum determinant or the coding gain. So the study of maximal orders is clearly motivated by an analogy from the theory of error correcting codes: why one would use a particular code of a given minimum distance and length, if a larger code with the same parameters is available. The standard matrix representation of the natural order results in codes that have a so-called threaded layered structure [21]. When a maximal order is used, the code will then also extend "between layers". Earlier, maximal orders have been successfully used in the construction of MISO and symmetric MIMO lattices, see [5], [22], [17]. For more information on matrix representations of division algebras and their use as MIMO STBCs the reader can refer to [23], [7].

Recently, different methods for constructing asymmetric [24],[25] and multi-block [20] space-time codes have been proposed. *Asymmetric* codes are targeted at the code design for downlink transmission where the number of Rx antennas is strictly less than the number of Tx antennas. Typical examples of such situations are 3+G mobile phones and DVB-H (Digital Video Broadcasting-Handheld) user equipment, where only a very small number of antennas fits at the end user site. Multi-block codes, for their part, are called for when one wishes to obtain vanishing error probability in addition to the DMT optimality.

Remark 1.1: We want to note that in this paper the emphasis is purely on the construction of sphere decodable asymmetric schemes having a minimum delay, and hence we do not intend to compete with the symmetric schemes that will naturally have a higher rate. The problem of constructing minimum-delay symmetric schemes has been efficiently solved already, see e.g. [10], [17]. However, unless at least n_t receiving antennas is used, such codes cannot be decoded by using simple decoding methods such as a sphere decoder, and this is the very reason why we now consider the construction of sphere decodable codes for n_r receiving antennas, n_r being strictly less than the number of transmitters n_t.

We define a *lattice* to be a discrete finitely generated free abelian subgroup L of a real or complex finite dimensional vector space, called the ambient space. In the space-time (ST) setting a natural ambient space is the space $\mathcal{M}_n(\mathbf{C})$ of complex $n \times n$ matrices. The *Gram matrix* is defined as

$$G(L) = \left(\Re tr(x_i x_j^\dagger)\right)_{1 \leq i,j \leq k}, \tag{1}$$

where tr is the matrix trace (=sum of the diagonal elements), and $x_i \in \mathcal{M}_n(\mathbf{C}),\ i = 1, ..., k$, form a $\mathbf{Z}$-basis of L. The rank k of the lattice is upper bounded by $2n^2$. Note that we really need to take the real part of the trace in the Gram matrix, as the matrices $x_i x_j^\dagger$ are not necessary real as themselves for $i \neq j$. The Gram matrix has a positive determinant equal to the squared measure of the fundamental parallelotope $m(L)^2$. A change of basis does not affect the measure $m(L)$.

Any lattice L with the NVD property [8] can be scaled, i.e. multiplied by a real constant t, either to satisfy $\det_{min}(L) = \min_{M \in L \setminus \{0\}} \det(M) = 1$ or to satisfy $m(L) = 1$. This is because $\det_{min}(tL) = t^n \det_{min}(L)$ and $m(tL) = t^k m(L)$. As the minimum determinant determines the asymptotic pairwise error probability, this gives rise to natural numerical measures for the quality of a lattice.

Definition 1.2: Following [26], we shall denote by $\delta(L)$ the *normalized minimum determinant* of the lattice L, i.e. here we first scale L to have a unit size fundamental parallelotope. Dually we denote by $\rho(L) = 1/m(L)$ the *normalized density* of the lattice L, when we first scale the lattice to have unit minimum determinant, and only then compute the quantity $1/m(L)$. In other words, we define

$$\delta(L) = \frac{\det_{min}(L)}{m(L)^{n/k}},$$

$$\rho(L) = \frac{(\det_{min}(L))^{k/n}}{m(L)}.$$

When comparing the minimum determinants of different codes, one should always use the normalized minimum determinant. To avoid confusion let us mention that from now on, when we talk about minimum determinant we always mean $\det_{min}(L)$ and not its square as in the traditional definition of minimum determinant (see above). The squared normalized minimum determinant $\delta(L)^2$ can be righteously identified with the coding gain. According to the above definition, maximizing the coding gain, i.e. the normalized minimum determinant, is equivalent to maximizing the (normalized) density of the code. Formally, we get

Proposition 1.1: The coding gain of a lattice L equals

$$\delta(L)^2 = \rho(L)^{2n/k}.$$

Hence, increasing the density is equivalent to increasing the coding gain.

Given that maximal orders provide the best codes in terms of minimum determinant vs. average power we are left with the question: Which division algebra should we use? To continue the analogy from the theory of error-correcting codes we want to find the codes with the highest possible density. That is, with the smallest fundamental parallelotope. In [17] we developed the required tools for parameterizing cyclic division algebras with a given center and index. Also an achievable lower bound for the measure of the fundamental parallelotope was derived.

One aim in this paper is to generalize the notions and results from [17] to the *asymmetric scheme* where the number of receiving antennas is strictly less than the number of transmitting antennas. As the main contributions we

- propose new methods for constructing asymmetric space-time codes, one of which is applicable for any number of transmitting and receiving antennas (#Rx<#Tx),
- prove that similarly to the symmetric scheme, maximizing the density (i.e. finding the most efficient packing in the available signal space) of codes arising from the so-called block diagonal method is equivalent to minimizing the discriminant of an order. With the aid of this observation we generalize the density bound from [17] to the asymmetric scheme,
- derive an explicit density upper bound for the 4Tx+2Rx case,
- provide an explicit 4Tx+2Rx construction achieving our density bound,
- give a table comparing the normalized minimum determinants and densities of different block diagonal AST codes,
- show that the block diagonal method can be converted to produce multi-block ST codes [20] that achieve the DMT, and that the density bound is also applicable as such to these multi-block codes,
- provide extensive DMT alalysis of the proposed codes,
- demonstrate by simulations that by using the newly proposed methods we can outperform the punctured Perfect code and the DjABBA code [25] as well as the Icosian code [27] in BLER performance.

The paper is organized as follows. In Section II we will shortly motivate this research and describe our solutions to the stated problems. In Section III, various algebraic notions related to cyclic algebras, orders, and discriminants are introduced. If the reader is familiar with the standard symmetric cyclic division algebra based space-time codes, this introductory section can safely be skipped. Furthermore, it is shown that maximizing the density of the code, i.e. minimizing the fundamental parallelotope is equivalent to minimizing the discriminant. This leads us to Section IV, where we recall the achievable lower bound from [17] for the discriminant in the symmetric case. In Section V we describe the block diagonal construction method for asymmetric ST lattices. We generalize the density bound from [17] to the block diagonal AST codes in Section V-A, and show in Section V-B that it also holds as such to the multi-block codes [20]. Also explicit example codes are given in Section V-C accompanied with a table comparing their densities and normalized minimum determinants. Further, in Section V-D we derive an explicit, achievable density bound for the 4Tx+2Rx case and show that it is achieved by one of the proposed constructions. The smart puncturing method is described in Section VI, and finally some simulation results and DMT analysis are provided in Sections VII and VIII, respectively. Section IX contains the conclusions.

II. Motivation and problem statement

In some applications the number of Rx antennas is required to be strictly less than the number of Tx antennas. Typical examples are 3+G mobile phones and DVB-H (Digital Video Broadcasting-Handheld) user equipment, where only a very small number of antennas fits at the end user site. One may also think of downlink transmissions in wireless networks, where one can usually fit more antennas in the access point than in a laptop. For such application, the symmetric, minimum-delay MIMO constructions arising from the theory of cyclic division algebras (see e.g. [10]) have to be modified. For simplicity, the concrete examples given here concentrate on the 4Tx+2Rx antenna case: if we could afford four Rx antennas, the task would be easy – just to use the 4×4 minimum-delay, rate-optimal CDA-based construction transmitting 16 (complex, usually QAM / HEX) information symbols in four time slots, i.e. four in each time slot. Now, however, the reduced number of Rx antennas limits the transmission down to two symbols per each time slot (cf. Definition 1.1) if we wish to enable efficient decoding such as sphere decoding.

We have come up with two different types of solutions to this problem. Both solutions take advantage of cyclic division algebras and yield rate n_r codes with a non-vanishing determinant. Let us denote by $n_t = n_r m$ the number of transmitters in the usual symmetric CDA-based MIMO system and suppose we want to construct a code for n_tTx+n_rRx antennas. In the *Block Diagonal Method (BDM)* the idea is to first pick an index n_r division algebra with a center that is $2m$-dimensional over $\mathbf{Q}$, form isomorphic copies of it and then use them as $n_r \times n_r$ diagonal blocks in an $n_t \times n_t$ code matrix. Another possibility is to take the symmetric $n_t \times n_t$ MIMO code, but choose the elements in the matrix from an intermediate field of degree $2n_r$ over $\mathbf{Q}$ instead of the maximal subfield. This method can be generalized to *any number of transmitters and receivers (#Rx<#Tx)* by performing so called *Smart Puncturing Method (SPM)* instead of restricting the elements to belong to some fixed subfield. In practice, this means that we puncture at an arbitrary level, i.e. set a required number of QAM/HEX coeffiecients of basis elements to zero. These methods shall be explained in greater detail in Sections V and VI accompanied with illuminating examples.

In this paper we will thoroughly analyze (in class field theoretic terms) the block diagonal method. The smart puncturing method will be treated in more detail in a forthcoming paper.

III. Cyclic algebras, orders, and discriminants

We refer the interested reader to [23] and [7] for a detailed exposition of the theory of simple algebras, cyclic algebras, their matrix representations and their use in ST-coding. We only recall the basic definitions and notations here. In the following, we consider number field extensions E/F, where F denotes the base field and F^* (resp. E^*) denotes the set of the non-zero elements of F (resp. E). In the interesting cases F is an imaginary quadratic field, either $\mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt{-3})$ corresponding to the QAM and HEX alphabets, respectively. We assume that E/F is a cyclic field extension of degree n with the Galois group $\mathrm{Gal}(E/F) = \langle\sigma\rangle$. Let $\mathcal{A} = (E/F, \sigma, \gamma)$

be the corresponding cyclic algebra of degree n (n is also called the *index* of $\mathcal{A}$, and in practice $n_t = n$), that is

$$\mathcal{A} = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E,$$

as a (right) vector space over E. Here $u \in \mathcal{A}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in F^*$. An element $a = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{A}$ has the following representation as a matrix $A =$

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

We refer to this as the standard matrix representation of $\mathcal{A}$. Observe that some variations are possible here. E.g. one may move the coefficients γ from the upper triangle to the lower triangle by conjugating this matrix with a suitable diagonal matrix. Similarly one may arrange to have the first row to contain the "pure" coefficients $x_0, \ldots, x_{n-1}$. Such changes do not affect the minimum determinant nor the density of the resulting lattices.

In practice, some restrictions to the elements $x_i \in E$ and γ have to be made, see Definition 3.4 and the comment below. If we denote the integral basis of E/F by $\{e_0, e_1, ..., e_{n-1}\}$, then the elements $x_i,\ i = 0, ..., n-1$ in the above matrix are restricted to take the form $x_i = \sum_{k=0}^{n-1} f_k e_k$, where $f_k \in \mathcal{O}_F$ for all $k = 0, ..., n-1$. Hence n information symbols are transmitted per channel use, i.e. the design has rate n. In literature this is often referred to as having a *full rate*.

Definition 3.1: The determinant of the matrix A above is called the *reduced norm* of the element $a \in \mathcal{A}$ and is denoted by $nr(a)$.

Remark 3.1: The connection between the usual norm map $N_{\mathcal{A}/F}(a)$ and the reduced norm $nr(a)$ of an element $a \in \mathcal{A}$ is $N_{\mathcal{A}/F}(a) = (nr(a))^n$, where n is the degree of E/F.

Definition 3.2: An algebra $\mathcal{A}$ is called *simple* if it has no nontrivial ideals. An F-algebra $\mathcal{A}$ is *central* if its center $Z(\mathcal{A}) = \{a \in \mathcal{A} \mid aa' = a'a\ \forall a' \in \mathcal{A}\} = F$.

All algebras considered in this paper are central simple.

A division algebra may be represented as a cyclic algebra in many ways as demonstrated by the following example.

Example 3.1: The division algebra $\mathcal{GA}$ used in [3] to construct the Golden code is a cyclic algebra with $F = \mathbf{Q}(i)$, $E = \mathbf{Q}(i, \sqrt{5})$, $\gamma = i$, when the F-automorphism σ is determined by $\sigma(\sqrt{5}) = -\sqrt{5}$. We also note that in addition to this representation $\mathcal{GA}$ can be given another construction as a cyclic algebra. As now $u^2 = i$ we immediately see that $F(u)$ is a subfield of $\mathcal{GA}$ that is isomorphic to the eighth cyclotomic field $E' = \mathbf{Q}(\zeta)$, where $\zeta = (1+i)/\sqrt{2}$. The relation $u\sqrt{5} = -\sqrt{5}u$ read differently means that we can view u as the complex number ζ and $\sqrt{5}$ as the auxiliary generator, call it $u' = \sqrt{5}$. We thus see that the cyclic algebra

$$E' \oplus u'E' = (E'/F, \sigma', \gamma')$$

is isomorphic to the Golden algebra. Here σ' is the F-automorphism of E' determined by $\zeta \mapsto -\zeta$ and $\gamma' = u'^2 = 5$.

The element γ is often called a *non-norm element* due to Theorem 3.2 by A. A. Albert [28, Theorem 11.12, p. 184]. It provides us with a condition of when a cyclic algebra is a division algebra. The original result was stated for $t = 1, 2, ..., n-1$, but can be simplified after the next lemma.

Lemma 3.1: Let $\gamma \in F^*$ and E/F be as above. Consider the set S of exponents $t \in \mathbf{Z}$ such that γ^t is a norm of an element of E. Then

$$S = k\mathbf{Z}$$

for some $k|n$.

Proof: The mapping $f : t \mapsto \gamma^t$ is a homomorphism of groups from $(\mathbf{Z}, +)$ to $(F^*, \cdot)$. Because $H = N_{E/F}(E^*)$ is a subgroup of F^*, and $S = f^{-1}(H)$, we immediately see that S is a subgroup of $(\mathbf{Z}, +)$. From basic algebra it now follows that S is cyclic, i.e. $S = k\mathbf{Z}$ for some $k \in \mathbf{Z}$. On the other hand, as $\gamma \in F^*$ we get that $\gamma^n = N_{E/F}(\gamma)$, and hence $n \in S$. Therefore $k|n$. ∎

Proposition 3.2 (Norm condition): The cyclic algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ of degree n is a division algebra if and only if the smallest factor $t \in \mathbf{Z}_+$ of n such that γ^t is the norm of some element of E^* is n.

Proof: We are to prove the equivalence of two conditions, the original stating that γ^t is not a norm for any t in the range $1, 2, ..., n-1$, and the relaxed version stating the same for those t in the same range that are also divisors of n. One implication is clear, and the other follows from the above lemma. Namely, if there are integers t in the range $1, 2, ..., n-1$ such that γ^t happens to be a norm, then the lemma tells us that the smallest such t must be a divisor of n. ∎

Remark 3.2: We can even relax the above conditions for t. The proof of the previous lemma shows that actually it suffices to check that $\gamma^{n/p}$ is not a norm for any prime divisor p of n. For example, when $n = 8$, it suffices to check that γ^4 is not a norm.

We are now ready to present some of the basic definitions and results from the theory of maximal orders. The general theory of maximal orders can be found in [29].

Let R denote a Noetherian integral domain with a quotient field F (e.g. $R = \mathbf{Z}[i]$ and $F = \mathbf{Q}(i)$), and let $\mathcal{A}$ be a finite dimensional F-algebra.

Definition 3.3: An *R-order* in the F-algebra $\mathcal{A}$ is a subring Λ of $\mathcal{A}$, having the same identity element as $\mathcal{A}$, and such that Λ is a finitely generated module over R and generates $\mathcal{A}$ as a linear space over F. An order Λ is called *maximal*, if it is not properly contained in any other R-order.

In the rest of the paper, Λ will always denote an order and can be treated as an algebraic lattice. Let us illustrate the above definition by concrete examples.

Example 3.2: (a) Orders always exist: If M is a *full* R-lattice in $\mathcal{A}$, i.e. $FM = \mathcal{A}$, then the *left order* of M defined as $\mathcal{O}_l(M) = \{x \in \mathcal{A} \mid xM \subseteq M\}$ is an R-order in $\mathcal{A}$. The right order is defined in an analogous way.

(b) If R is the ring of integers $\mathcal{O}_F$ of the number field F, then the ring of integers $\mathcal{O}_E$ of the extension field E is the unique maximal R-order in E. For example, in the case of the cyclotomic field $E = \mathbf{Q}(\zeta)$, where $\zeta = \exp(2\pi i/k)$ is a primitive root of unity of order k the maximal order is $\mathcal{O}_E = \mathbf{Z}[\zeta]$.

(c) The set of integral elements does not form a ring in the non-commutative case. As an easy counter-example one can use the ring of Lipschitz quaternions

$$\mathcal{L} = \{q = a + bi + cj + dk \in \mathbb{H} \mid a, b, c, d \in \mathbf{Z}, \\ i^2 = j^2 = k^2 = -1, ij = k\},$$

a subring of the Hamiltonian quaternions $\mathbb{H}$ used for the construction of the Alamouti code. For instance, consider the polynomial $f(x) = x^2 + 1$ having integral coefficients. The element $t = \frac{3i+4j}{5}$ is one of the (infinitely many) roots of the polynomial $f(x)$, and hence may be called integral. However, if we try to adjoin t to the ring $\mathcal{L}$, we end up with a set that will also contain the element it. The reduced trace $tr(it) \in \mathbf{Q}$ is not an integer, hence we cannot have an order that would contain both the Lipschitz quaternions and t.

For the purposes of constructing MIMO lattices the reason for concentrating on orders is summarized in the following proposition (e.g. [29, Theorem 10.1, p. 125]). We simply rephrase it here in the language of MIMO-lattices. We identify an order (or its subsets) with its standard matrix representation.

Proposition 3.3: Let Λ be an order in a cyclic division algebra $(E/F, \sigma, \gamma)$. Then for any non-zero element $a \in \Lambda$ its reduced norm $nr(a)$ is a non-zero element of the ring of integers $\mathcal{O}_F$ of the center F. In particular, if F is an imaginary quadratic number field, then the minimum determinant of the lattice Λ is equal to one.

Definition 3.4: In any cyclic algebra we can always choose the element $\gamma \in F^*$ to be an algebraic integer. We immediately see that the $\mathcal{O}_F$-module

$$\Lambda_{NAT} = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E,$$

where $\mathcal{O}_E$ is the ring of integers, is an $\mathcal{O}_F$-order in the cyclic algebra $(E/F, \sigma, \gamma)$. We refer to this $\mathcal{O}_F$-order as the *natural order*. An alternative appellation would be *layered order*, as the corresponding MIMO-lattice of this order has the layered structure described in [21].

Remark 3.3: We want the reader to note that in any central simple algebra a maximal $\mathbf{Z}$-order is a maximal $\mathcal{O}_F$-order as well. Note also that if γ is not an algebraic integer, then Λ fails to be closed under multiplication. This may adversely affect the minimum determinant of the resulting matrix lattice, as elements not belonging to an order may have non-integral (and hence small) norms.

Definition 3.5: Let $m = dim_F\mathcal{A}$. The *discriminant* of the R-order Λ is the ideal $d(\Lambda/R)$ in R generated by the set

$$\{\det(tr(x_i x_j))_{i,j=1}^m \mid (x_1, ..., x_m) \in \Lambda^m\}.$$

In the interesting cases of $F = \mathbf{Q}(i)$ (resp. $F = \mathbf{Q}(\sqrt{-3})$) the ring $R = \mathbf{Z}[i]$ (resp. $R = \mathbf{Z}[\omega]$, $\omega = (-1 + \sqrt{-3})/2$) is a Euclidean domain, so in these cases (as well as in the case $R = \mathbf{Z}$) it makes sense to speak of the discriminant as an element of R rather than as an ideal. We simply pick a generator of the discriminant ideal, and call it the discriminant. Equivalently we can compute the discriminant as

$$d(\Lambda/R) = \det(tr(x_i x_j))_{i,j=1}^m,$$

where $\{x_1, \ldots, x_m\}$ is any R-basis of Λ.

Remark 3.4: It is readily seen that whenever $\Lambda \subseteq \Gamma$ are two R-orders, then $d(\Gamma/R)$ is a factor of $d(\Lambda/R)$. It also turns out (cf. [29, Theorem 25.3]) that all the maximal orders of a division algebra share the same discriminant that we will refer to as the discriminant of the division algebra. In this sense a maximal order has the smallest possible discriminant among all orders within a given division algebra, as all the orders are contained in some maximal order.

The definition of the discriminant closely resembles that of the Gram matrix of a lattice, so the following result proved in [17] is unsurprising and immediately generalizes to the asymmetric scheme as well as was shown in [24].

Lemma 3.4: Assume that F is an imaginary quadratic number field and that 1 and ν form a $\mathbf{Z}$-basis of its ring of integers R. Assume further that the order Λ is a free R-module (an assumption automatically satisfied, when R is a principal ideal domain). Then the measure of the fundamental parallelotope equals

$$m(\Lambda) = |\Im\nu|^{n^2} |d(\Lambda/R)|.$$

In the respective cases $F = \mathbf{Q}(i)$ and $F = \mathbf{Q}(\sqrt{-3})$ we have $\nu = i$ and $\nu = (-1 + \sqrt{-3})/2$ respectively, so we immediately get the following two corollaries.

Corollary 3.5: Let $F = \mathbf{Q}(i), R = \mathbf{Z}[i]$, and assume that $\Lambda \subset (E/F, \sigma, \gamma)$ is an R-order. Then the measure of the fundamental parallelotope equals

$$m(\Lambda) = |d(\Lambda/\mathbf{Z}[i])|.$$

Example 3.3: When we scale the Golden code [3](cf. Example 3.1) to have a unit minimum determinant, all the 8 elements of its $\mathbf{Z}$-basis will have length $5^{1/4}$ and the measure of the fundamental parallelotope is thus 25. In view of all of the above this is also a consequence of the fact that the $\mathbf{Z}[i]$-discriminant of the natural order of the Golden algebra $\mathcal{GA}$ is equal to 25. As was observed in [30] the natural order happens to be maximal in this case, so the Golden code cannot be improved upon by enlarging the order within $\mathcal{GA}$.

Corollary 3.6: Let $\omega = (-1 + \sqrt{-3})/2$, $F = \mathbf{Q}(\omega)$, $R = \mathbf{Z}[\omega]$, and assume that $\Lambda \subset (E/F, \sigma, \gamma)$ is an R-order. Then the measure of the fundamental parallelotope equals

$$m(\Lambda) = (\sqrt{3}/2)^{n^2} |d(\Lambda/\mathbf{Z}[\omega])|.$$

The upshot in [17] was that in both cases maximizing the density of the code, i.e. minimizing the fundamental parallelotope, is equivalent to minimizing the discriminant. Thus, in order to get the densest MIMO-codes one needs to look for division algebras that have a maximal order with as small a discriminant as possible.

For an easy reference we also include the following result [17] that is a relatively easy consequence of the definitions.

Lemma 3.7: Let E/F be as above, assume that γ is an algebraic integer of F, and let Λ be the natural order of Definition 3.4. If $d(E/F)$ is the $\mathcal{O}_F$-discriminant of $\mathcal{O}_E$ (often referred to as the relative discriminant of the extension E/F), then

$$d(\Lambda/\mathcal{O}_F) = d(\mathcal{O}_E/\mathcal{O}_F)^n \gamma^{n(n-1)}.$$

To conclude the section, we include the following simple but interesting result on maximal orders explaining why using a principal one-sided (left or right) ideal instead of the entire order will not change the density of the code. For the proof, see [17, Lemma 7.1].

Lemma 3.8: Let Λ be a maximal order in a cyclic division algebra over an imaginary quadratic number field. Assume that the minimum determinant of the lattice Λ is equal to one. Let $x \in \Lambda$ be any non-zero element. Let $\mu > 0$ be a real parameter chosen so that the minimum determinant of the lattice $\mu(x\Lambda)$ is also equal to one. Then the fundamental parallelotopes of these two lattice have the same measure

$$m(\Lambda) = m(\mu(x\Lambda)).$$

IV. The Discriminant Bound

In this section, we recall some more material from [17] to be used later on in Section V.

Again let F be an algebraic number field that is finite dimensional over $\mathbf{Q}$ and $\mathcal{O}_F$ its ring of integers. In what follows by the size of ideals of $\mathcal{O}_F$ we mean that ideals are ordered by the absolute values of their norms to $\mathbf{Q}$, so e.g. in the case $\mathcal{O}_F = \mathbf{Z}[i]$ we say that the prime ideal generated by $2+i$ is smaller than the prime ideal generated by 3 as they have norms 5 and 9, respectively.

Theorem 4.1: [17, Discriminant bound] Assume that F is a totally complex number field, and that P_1 and P_2 are the two smallest prime ideals in $\mathcal{O}_F$. Then the smallest possible discriminant of all central division algebras over F of index n is

$$(P_1 P_2)^{n(n-1)}.$$

We remark that the division algebra achieving this bound is by no means unique.

Example 4.1: The smallest primes of the ring $\mathbf{Z}[i]$ are $1+i$ and $2 \pm i$. They have norms 2 and 5 respectively. The smallest primes of the ring $\mathbf{Z}[\omega]$ are $\sqrt{-3}$ and 2 with respective norms 3 and 4. Together with Corollaries 3.5 and 3.6 we have arrived at the following bounds.

Let Λ be an order of a central division algebra of index n over the field $\mathbf{Q}(i)$. Then the measure of a fundamental parallelotope of the corresponding lattice

$$m(\Lambda) \geq 10^{n(n-1)/2}.$$

Let Λ be an order of a central division algebra of index n over the field $\mathbf{Q}(\omega)$, $\omega = (-1+\sqrt{-3})/2$. Then the measure of a fundamental parallelotope of the corresponding lattice

$$m(\Lambda) \geq (\sqrt{3}/2)^{n^2} 12^{n(n-1)/2}.$$

Example 4.2: Let $F = \mathbf{Q}(\sqrt{-3})$, so $\mathcal{O}_F = \mathbf{Z}[\omega]$. In this case the two smallest prime ideals are generated by 2 and $1-\omega$ and as noted above they have norms 4 and 3 respectively. By Theorem 4.1 the minimal discriminant is $4(1-\omega)^2$ when $n = 2$. As the absolute value of $1-\omega$ is $\sqrt{3}$ an application of the formula in Corollary 3.6 shows that the lattice L of the code achieving this bound has $m(L) = 27/4$. In [22] we showed that a maximal order of the cyclic algebra $(E/F, \sigma(i) = -i, \gamma = \sqrt{-3})$, where $E = \mathbf{Q}(i, \sqrt{-3})$, achieves this bound.

For more information on finding maximal orders and their discriminants, see [17]. In practice maximal orders can easily be computed with the aid of the (unfortunately commercial) MAGMA software [31], or in small cases by hand following [32] (see also [33],[34]). The computation and decoding of maximal order will be treated in more detail in a forthcoming paper by Hollanti and Ranto [35].

We conclude this section by a couple of remarks[1] related to the use of outer codes and our choice to consider only codes having a minimum delay.

Remark 4.1: While the concatenation of the maximal-order space-time code as the inner code and the conventional error correction code as the outer code is beyond the scope of this work, it is expected that such concatenation will result in a smaller multiplexing gain as the outer code has rate less than 1. However, the error performance will be significantly improved due to the use of additional error correction techniques. On the other hand, we must point out that since (1) the inner maximal-order code makes use of sphere decoding, which is a hard-decision based decoding, and (2) such inner decoder cannot provide soft information for the input of output decoder, it is technically impossible to use either low-density parity check (LDPC) code or turbo code as the outer code as these codes requires a soft-input-soft-output decoder in order to deliver the promised near-capacity performance. Nevertheless, some conclusion can be easily drawn. From simulation we have already seen that, in the symmetric case, the maximal order code outperforms the perfect code, meaning that the former has lower error probability than the latter; the overall error probability of the concatenated maximal-order code after incorporating the outer decoder must be even lower than that of the concatenated perfect code, simply because the BER curve of the outer decoder is monotonically decreasing in SNR, and such conclusion holds for all outer codes.

Remark 4.2: In this paper the focus is on square matrices, i.e., on codes having a minimum delay. If longer delay is allowed, then the optimal DMT can be achieved at least in some special cases. The authors of the present paper have submitted a separate work related to this subject, see [41]. Increasing the delay requires lattices with a higher dimension, so also the decoding process will get more complex.

[1]The remarks are invoked by the comments of the anonymous reviewers of this paper. We thank all the reviewers for the careful reading of our paper. Also complexity issues were brought up by one of the reviewers, hence a short discussion on the decoding complexity has been added in the simulation results section.

V. Constructing asymmetric and multi-block space-time codes by the Block Diagonal Method (BDM)

A straightforward way to obtain AST lattices would be just to "switch off the extra layers" (following [25] and [24]) in a symmetric MIMO setting, i.e. by trivial puncturing. In the case of 4Tx+2Rx antennas this would mean that in the standard matrix representation we set e.g. $x_1 = x_3 = 0$ in order to transmit a limited number of symbols that can be received with only two receivers. In this and the following section we present two more sophisticated methods for constructing AST lattices that still admit efficient sphere decoding.

A. Block diagonal asymmetric ST lattices

In this section, we recall *Method 1* from [24]. Let us rename this method as *Block Diagonal Method* (BDM).

Let us consider an extension tower $F \subseteq L \subseteq E$ with the degrees $[E:L] = n_r, [L:F] = m$ and with the Galois groups $\mathrm{Gal}(E/F) = \langle \tau \rangle$, $\mathrm{Gal}(E/L) = \langle \sigma = \tau^m \rangle$. Let

$$\mathcal{B} = (E/L, \sigma, \gamma) = E \oplus uE \oplus \cdots \oplus u^{n_r-1}E$$

be an index n_r division algebra, where the center L is fixed by $\sigma = \tau^m$. We denote by #Tx $= n_t = n_r m$.

Note that if one has a symmetric, index $n_t = n_r m$ CDA-based STBC, the algebra $\mathcal{B}$ can be constructed by just picking a suitable intermediate field $L \subseteq E$ of a right degree as the new center.

An element $b = x_0 + \cdots + u^{n_r-1}x_{n_r-1},\ x_i \in E,\ i = 0, ..., n_r - 1$ of the algebra $\mathcal{B}$ has the standard representation as an $n_r \times n_r$ matrix $B = (b_{ij})_{1 \le i,j \le n_r}$ as given in Section III.

However, we can afford an $n_t \times n_t$ packing as we are using n_t transmitting antennas. This can be achieved by using the isomorphism τ. Let us denote by $\tau^k(\mathcal{B}) = (E/L, \sigma, \tau^k(\gamma)),\ k = 0, ..., m-1$ the m isomorphic copies of $\mathcal{B}$ and the respective matrix representations by

$$\tau^k(B) = (\tau^k(b_{ij}))_{1 \le i,j \le n_r},\ k = 0, ..., m-1. \qquad (2)$$

The next proposition shows that by using these copies as diagonal blocks we obtain an infinite lattice with non-vanishing determinant.

Proposition 5.1 (BDM): Let $b \in \Lambda \subseteq \mathcal{B}$ and $F = \mathbf{Q}(\delta)$, where $\delta \in \{i, \omega\}$. Assume $\gamma \in \mathcal{O}_L$. The block diagonal lattice

$$\mathcal{C}(\Lambda) = \left\{ M = \begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & \tau(B) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \tau^{m-1}(B) \end{pmatrix} \right\}$$

built from (2) has a non-vanishing determinant $\det(M) = \prod_{i=0}^{m-1} \det(\tau^i(B)) \in \mathbf{Z}[\delta]$. Thus, the minimum determinant is equal to one for all m. The code rate equals $n_r^2 m / n_r m = n_r$.

Proof: According to Definition 3.1 and Proposition 3.3,

$$\begin{aligned} \det(M) &= \prod_{i=0}^{m-1} \det(\tau^i(B)) = \prod_{i=0}^{m-1} nr(\tau^i(b)) \\ &= \prod_{i=0}^{m-1} \tau^i(nr(b))) = N_{L/F}(nr(b)) \in \mathbf{Z}[\delta], \end{aligned}$$

and hence $|\det(M)| \ge 1$. ∎

Remark 5.1: In [36] an approach similar to the BDM was used for the MIMO amplify-and-forward cooperative channel.

Now the natural question is how to choose a suitable division algebra. In [15] and [16] several systematic methods for constructing extensions E/L are provided. All of them make use of cyclotomic fields. Next we will show that also in the asymmetric scheme, maximizing the code density (i.e. minimize the volume of the fundamental parallelotope, see [17]) with a given minimum determinant is equivalent to minimizing a certain discriminant. In the next section we shall show that this also holds for the multi-block codes from [20].

First we need the following result. For the proof, see [29, p. 223].

Lemma 5.2: Suppose $\Lambda \subseteq \mathcal{A} = (E/L, \tau, \gamma)$ is an $\mathcal{O}_F$-order and that $F \subseteq L$. The discriminants then satisfy

$$d(\Lambda/\mathcal{O}_F) = N_{L/F}\left(d(\Lambda/\mathcal{O}_L)\right) d(\mathcal{O}_L/\mathcal{O}_F)^{\dim_L \mathcal{A}}.$$

The same naturally holds in the commutative case when we replace $\mathcal{A}$ with E.

As a generalization to Lemma 3.4, we prove the following proposition.

Proposition 5.3: Assume that F is an imaginary quadratic number field and that $\{1, \nu\}$ forms a $\mathbf{Z}$-basis of its ring of integers $\mathcal{O}_F$. Let $n_r = [E:L]$, $m = [L:F]$, $n_t = n_r m$, and $s = |\Im\nu|^{m n_r^2}$. If the order $\mathcal{C}(\Lambda)$ defined as in Proposition 5.1 is a free $\mathcal{O}_F$-module (which is always the case if $\mathcal{O}_F$ is a principal ideal domain), then the measure of the fundamental parallelotope equals

$$\begin{aligned} m(\mathcal{C}(\Lambda)) &= s|d(\Lambda/\mathcal{O}_F)| && (3) \\ &= s|d(\mathcal{O}_L/\mathcal{O}_F)^{n_r^2} N_{L/F} d(\Lambda/\mathcal{O}_L)| && (4) \\ &= s|d(\mathcal{O}_L/\mathcal{O}_F)^{n_r^2} \prod_{i=0}^{m-1} \tau^i(d(\Lambda/\mathcal{O}_L))|. && (5) \end{aligned}$$

Proof: In order to keep the notation simple let us assume $m = 2$. The proof directly generalizes to an arbitrary m. Let $A = (a_{ij})$ be an $n_t \times n_t$ complex matrix. We flatten it out into a $4 \times 4n_t^2$ matrix $L(A)$ by first forming a vector of length n_t^2 out of the entries (e.g. row by row) and then replacing a complex number z by a diagonal four by four matrix with entries $z, \tau(z), z^*$, and $\tau(z)^*$ (z^* is the usual complex conjugate of z). If A and B are two square matrices with n_t rows we can easily verify the identities $L(A)L(B)^\dagger =$

$$\begin{pmatrix} tr(AB^\dagger) & 0 & 0 & 0 \\ 0 & \tau(tr(AB^\dagger)) & 0 & 0 \\ 0 & 0 & tr(A^\dagger B) & 0 \\ 0 & 0 & 0 & \tau(tr(A^\dagger B)) \end{pmatrix} \qquad (6)$$

and $L(A)L(B^T)^T =$

$$\begin{pmatrix} tr(AB) & 0 & 0 & 0 \\ 0 & \tau(tr(AB)) & 0 & 0 \\ 0 & 0 & tr(AB)^* & 0 \\ 0 & 0 & 0 & \tau(tr(AB))^* \end{pmatrix}. \qquad (7)$$

Next let $\mathcal{X} = \{x_1, x_2, \ldots, x_{n_r^2}\}$ be an $\mathcal{O}_L$-basis for Λ. We form the $4n_r^2 \times 4n_r^2$ matrix $L(\mathcal{X})$ by stacking the matrices

$L(x_i)_{4\times 4r^2}$ on top of each other. Similarly we get $R(\mathcal{X})$ by using the matrices $L(x_i^T)^T$ as column blocks. Then by (7) the matrix

$$M = L(\mathcal{X})R(\mathcal{X})$$

consists of four by four blocks of the form $L(x_i)L(x_j^T)^T =$

$$\text{diag}\left(tr(x_ix_j), \tau(tr(x_ix_j)), tr(x_ix_j)^*, \tau(tr(x_ix_j))^*\right).$$

Clearly

$$\det R(\mathcal{X})R(\mathcal{X})^\dagger = \pm \det L(\mathcal{X})L(\mathcal{X})^\dagger$$

and

$$\det M = |d(\Lambda/\mathcal{O}_L)|^2|\tau(d(\Lambda/\mathcal{O}_L))|^2.$$

Thus,

$$|\det L(\mathcal{X})L(\mathcal{X})^\dagger|^{1/2} = |d(\Lambda/\mathcal{O}_L)||\tau(d(\Lambda/\mathcal{O}_L))|. \quad (8)$$

Next we turn our attention to the Gram matrix. Let $\{1, \theta, ..., \theta^3\}$ be a $\mathbf{Z}$-basis for $\mathcal{O}_L$. Then by our assumptions the set $\mathcal{X} \cup \theta\mathcal{X} \cup \cdots \cup \theta^3\mathcal{X}$ is a $\mathbf{Z}$-basis for Λ. From the theory of algebraic numbers we know that

$$d(\mathcal{O}_F/\mathbf{Z}) = \det D(\nu)^2 \text{ and } d(\mathcal{O}_L/\mathbf{Z}) = \det D(\theta)^2, \quad (9)$$

where $D(\nu) = \begin{pmatrix} 1 & 1 \\ \nu & \nu^* \end{pmatrix}$ and

$$D(\theta) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \theta & \tau(\theta) & \theta^* & \tau(\theta)^* \\ \theta^2 & \tau(\theta^2) & (\theta^2)^* & \tau(\theta^2)^* \\ \theta^3 & \tau(\theta^3) & (\theta^3)^* & \tau(\theta^3)^* \end{pmatrix}.$$

From the identities $\Re(xy^*) = (xy^* + x^*y)/2$ and

$$D(\theta)L(x) = \begin{pmatrix} x & \tau(x) & x^* & \tau(x)^* \\ \vdots & & & \vdots \\ \theta^3 x & \tau(\theta^3 x) & (\theta^3 x)^* & \tau(\theta^3 x)^* \end{pmatrix}$$

together with (6) it follows that for any two $n_t \times n_t$ matrices A and B we have $\frac{1}{2}\left(D(\theta)L(A)\right)\left(D(\theta)L(B)\right)^\dagger =$

$$\begin{pmatrix} \Re(tr(AB^\dagger)) & \cdots & \Re(tr(A(\theta^3 B)^\dagger) \\ \vdots & & \vdots \\ \Re(tr(\theta^3 AB^\dagger)) & \cdots & \Re(tr(\theta^3 A(\theta^3 B)^\dagger)) \end{pmatrix}.$$

Therefore, if we denote by $D^{[n_r]}$ the $4n_r^2 \times 4n_r^2$ matrix having n_r^2 copies of $D(\theta)$ along the diagonal and zeros elsewhere, we get

$$G(\mathcal{C}(\Lambda)) = \frac{1}{2}\left(D^{[n_r]}L(\mathcal{X})\right)\left(D^{[n_r]}L(\mathcal{X})\right)^\dagger.$$

Thus,

$$\begin{aligned} m(\mathcal{C}(\Lambda)) &= \sqrt{\det G(\mathcal{C}(\Lambda))} \\ &= \left|\det L(\mathcal{X})L(\mathcal{X})^\dagger\right|^{1/2} \cdot (\frac{1}{4})^{n_r^2} \left|\det D(\theta)\right|^{n_r^2}. \end{aligned}$$

As

$$(\frac{1}{2})^{2n_r^2} \left|\det D(\theta)\right|^{n_r^2} = |d(\mathcal{O}_L/\mathcal{O}_F)|^{n_r^2} \left|\Im\nu\right|^{2n_r^2}$$

by (9) and Lemma 5.2, Equation (8) now gives us the claim when we still note (again by Lemma 5.2) that

$$d(\mathcal{O}_L/\mathcal{O}_F)^{n_r^2} d(\Lambda/\mathcal{O}_L)\tau(d(\Lambda/\mathcal{O}_L)) = d(\Lambda/\mathcal{O}_F). \quad (10)$$

■

Corollary 5.4: In the case $F = \mathbf{Q}(i)$ the volume equals

$$m(\mathcal{C}(\Lambda)) = \left|d(\Lambda/\mathbf{Z}[i])\right|.$$

Corollary 5.5: In the case $F = \mathbf{Q}(\omega)$ we get

$$m(\mathcal{C}(\Lambda)) = (\frac{\sqrt{3}}{2})^{mn_r^2} \left|d(\Lambda/\mathbf{Z}[\omega])\right|.$$

Now we can conclude (cf. (4)) that the extensions $E/L, L/F$ and the order $\Lambda \subseteq \mathcal{B}$ should be chosen in such a way that the discriminants $d(\mathcal{O}_L/\mathcal{O}_F)$ and $d(\Lambda/\mathcal{O}_L)$ are as small as possible. By choosing a maximal order within a given division algebra we can minimize the norm of $d(\Lambda/\mathcal{O}_L)$ (cf. Remark 3.4). As in practice an imaginary quadratic number field F is contained in L, we know that L is totally complex. In that case the fact that

$$d(\Lambda/\mathcal{O}_L) \geq (P_1P_2)^{n_r(n_r-1)}, \quad (11)$$

where P_1 and P_2 are prime ideals $\in \mathcal{O}_L$ with the smallest norms (to $\mathbf{Q}$) helps us in picking a good algebra (for the proof, see [17, Theorem 3.2]). Note that optimization with respect to $d(\mathcal{O}_L/\mathcal{O}_F)$ may result in a loss in $d(\Lambda/\mathcal{O}_L)$ and vice versa.

Keeping the above notation, we have now arrived at the following theorem.

Theorem 5.6 (Density bound for lattices from BDM): For the density of the lattice $\mathcal{C}(\Lambda), \Lambda \subseteq \mathcal{A}$ it holds that

$$\rho = \frac{1}{m(\mathcal{C}(\Lambda))} \leq s^{-1}|d(\mathcal{O}_L/\mathcal{O}_F)|^{-n_r^2}|N_{L/F}(P_1P_2)|^{n_r(1-n_r)}. \quad (12)$$

Remark 5.2: Note that as opposed to Example 4.1 (cf. [17]), here we do not automatically achieve nice, explicit lower bounds for $m(\mathcal{C}(\Lambda))$. That is a consequence of the fact that the center L can now be any field containing $\mathbf{Q}(i)$ or $\mathbf{Q}(\omega)$, and thus determining the smallest ideals P_1 and P_2 or even the minimal $d(\mathcal{O}_L/\mathcal{O}_F)$ is not at all straightforward. An exact lower bound is hard to derive in the general case as the calculation of minimal number field discriminants is known to be a tricky problem. The reader may ponder over the fact that tables for minimal discriminants do exist in literature (though only for certain degrees, see e.g. [37]) so why not use them. We want to emphasize that these tables cannot be adapted here, as the fields in question do not necessarily contain the desired subfield $\mathbf{Q}(i)$ or $\mathbf{Q}(\omega)$. However, in the smallest (and perhaps the most practical) case of 4Tx+2Rx antennas we are able to give an explicit and even achievable upper bound for the density. We believe that the best one can do in the other cases is to take advantage of known bounds of more general nature such as Odlyzko's bound [38].

B. Minimum-delay multi-block ST codes

The n_tTx+n_rRx antenna AST code from Proposition 5.1 can be transformed into an n_rTx+n_rRx antenna multi-block code [20] by an evident rearrangement of the blocks:

$$\begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & \tau(B) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \tau^{m-1}(B) \end{pmatrix} \leftrightarrow \begin{pmatrix} B & \cdots & \tau^{m-1}(B) \end{pmatrix}. \quad (13)$$

As the Gram matrices of an AST lattice and a multi-block ST lattice coincide, Lemma 5.3 also holds for multi-block ST codes with the same parameters. Let the notation be as in Section V-A.

Proposition 5.7: Let $b \in \Lambda \subseteq \mathcal{B}$ and $F = \mathbf{Q}(\delta)$, where $\delta \in \{i, \omega\}$. Assume $\gamma \in \mathcal{O}_L$. As the lattice

$$\mathcal{C}'(\Lambda) = \left\{M = \left(B, \tau(B), \ldots, \tau^{m-1}(B)\right)\right\}$$

built from (2) satisfies the generalized non-vanishing determinant property (cf. [20],[12]), it is optimal with respect to the DMT for all numbers of fading blocks m. Similarly as in Proposition 5.1, $|\prod_{i=0}^{m-1} \det(\tau^i(B))| \geq 1$. The code rate equals $n_r^2 m / n_r m = n_r$.

Proof: For the proof, see [20]. ∎

Proposition 5.8: The Gram determinants (cf. (1)) of the lattices $\mathcal{C}(\Lambda)$ and $\mathcal{C}'(\Lambda)$ coincide:

$$\det G(\mathcal{C}(\Lambda)) = \det G(\mathcal{C}'(\Lambda)).$$

Proof: This is obvious, as

$$\begin{aligned} & tr(diag(BB^\dagger, .., \tau^{m-1}(B)\tau^{m-1}(B)^\dagger)) \\ &= \sum_{i=0}^{m-1} tr(\tau^i(B)\tau^i(B)^\dagger) \\ &= tr(\sum_{i=0}^{m-1} (\tau^i(B)\tau^i(B)^\dagger)). \end{aligned}$$

∎

An immediate consequence of Proposition 5.8 is

Corollary 5.9: The lattices $\mathcal{C}(\Lambda)$ and $\mathcal{C}'(\Lambda)$ share the same density, i.e. Proposition 5.3 can be adapted as such to the multi-block scheme.

C. Explicit codes using BDM

In this section we provide explicit asymmetric constructions for the important case of 4Tx + 2Rx antennas. These codes can be modified for 2×2 multi-block use (cf. (13). The primitive nth root of unity will be denoted by ζ_n. The first three examples are given in terms of an asymmetric construction, whereas the last one is described as a multi-block code. However, with the aid of (13), an asymmetric code can always be transformed into a multi-block code and vice versa.

1) Perfect algebra $\mathcal{PA}$: Let us consider an algebra with the same maximal subfield that was used for the 4×4 Perfect code in [10]. We have the nested sequence of fields $F \subseteq L \subseteq E$, where $F = \mathbf{Q}(i)$, $L = \mathbf{Q}(\sqrt{5}, i)$, and $E = \mathbf{Q}(\theta, i)$ with $\theta = \zeta_{15} + \zeta_{15}^{-1} = 2\cos(2\pi/15)$. We denote this algebra by $\mathcal{PA} = (E/L, \sigma = \tau^2, \gamma) = E \oplus uE$, where $u^2 = \gamma = i$ and $\tau(\theta) = \theta^2 - 2$. As $\tau(\sqrt{5}) = -\sqrt{5}$, the field L is indeed fixed by $\sigma = \tau^2$. By embedding the algebra $\mathcal{PA}$ as in Proposition 5.1 we obtain the AST code

$$\mathcal{PA}_1 \subseteq \left\{ \begin{pmatrix} x_0 & i\sigma(x_1) & 0 & 0 \\ x_1 & \sigma(x_0) & 0 & 0 \\ 0 & 0 & \tau(x_0) & i\tau(\sigma(x_1)) \\ 0 & 0 & \tau(x_1) & \tau(\sigma(x_0)) \end{pmatrix} \right\},$$

where $x_i \in \mathcal{O}_E$. As the center is L with $[L : \mathbf{Q}(i)] = 2$ and $\mathcal{O}_L = \mathbf{Z}[i, \pi = (1 + \sqrt{5})/2]$, the elements x_k in the matrix are of the form $x_k = a_{k,0} + a_{k,1}\pi + a_{k,2}\theta + a_{k,3}\pi\theta$, where $a_{k,j} \in \mathbf{Z}[i]$. Thus, the code transmits, on the average, 2 independent QAM symbols per channel use.

We can further improve the performance by taking the elements x_i from the ideal $a\mathcal{O}_E$, where $a = 1 - 3i + i\theta^2 \in \mathcal{O}_E$. Moreover, a change of basis given by

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -3 & 0 & 1 \\ -1 & -3 & 1 & 1 \end{pmatrix}$$

guarantees an orthogonal lattice.

2) Cyclotomic algebra $\mathcal{CA}$: The algebra $\mathcal{CA} = (E/L, \sigma = \tau^2 : \xi \mapsto -\xi, \gamma = 1 + s - i) = E \oplus uE$ (cf. [12], [22], [24]), for its part, has the nested sequence of fields $F \subseteq L \subseteq E$ with $F = \mathbf{Q}(i)$, $L = \mathbf{Q}(s = \zeta_8)$, and $E = \mathbf{Q}(\xi = \zeta_{16})$. As we have $\tau : \xi \mapsto i\xi, s \mapsto -s$, the field L is fixed by $\sigma = \tau^2$. Again by embedding the algebra $\mathcal{CA}$ as in Proposition 5.1, the AST code

$$\mathcal{CA}_1 \subseteq \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_1) & 0 & 0 \\ x_1 & \sigma(x_0) & 0 & 0 \\ 0 & 0 & \tau(x_0) & \tau(\gamma)\tau(\sigma(x_1)) \\ 0 & 0 & \tau(x_1) & \tau(\sigma(x_0)) \end{pmatrix} \right\}$$

with $x_i \in \mathcal{O}_E$ is obtained. The center is L with $[L : \mathbf{Q}(i)] = 2$ and $\mathcal{O}_L = \mathbf{Z}[s]$. The elements x_k in the matrix are of the form $x_k = \sum_{j=0}^{3} a_{k,j}\xi^j$, where $a_{k,j} \in \mathbf{Z}[i]$, hence the above code transmits on the average, 2 independent QAM symbols per channel use.

Note that we have chosen here a suitable non-norm element γ from $\mathcal{O}_L$ instead of $\mathcal{O}_F$ (cf. Section V-A). We get some energy savings as $|1 + s - i| < |2 + i|$.

The code $\mathcal{CA}_1$ can be made perfect (see [11]) by forcing γ to be unit, i.e. we can choose $\gamma = \frac{2+i}{2-i}$. The loss in the minimum determinant is compensated by an improvement in performance. We denote the perfect version of the code by $\mathcal{CA}_1\ PERF$.

By doing this, we need not sacrifice the NVD property: Let $X = (X_1\ X_2\ X_3\ X_4)^T \in \mathcal{CA}_1\ PERF$. If we denote by M the matrix where we have multiplied the matrix rows containing γ by $2 - i$, that is

$$M = ((2-i)X_1\ X_2\ (2-i)X_3\ X_4)^T \in \mathcal{CA}_1,$$

then we have

$$|\det(M)| = |(2-i)^2 \det(X)| \geq 1$$

and hence

$$|\det(X)| \geq \frac{1}{5} > 0.$$

Note also that this is only possible because of the *additive* structure of the code. Taking powers of the elements $X \in \mathcal{CA}_1\ PERF$ into the code would result in a vanishing determinant (cf. Remark 3.3).

3) Algebra $\mathcal{IA}$ – an improved maximal order: Similarly as in the two previous subsections, we obtain a rate-2 AST code $\mathcal{IA}_1$ by introducing yet another algebra $\mathcal{IA} = (E/L, \sigma = \tau^2, \gamma = \sqrt{-3})$, where $F = \mathbf{Q}(i)$, $L = \mathbf{Q}(i, \sqrt{3})$, $E = L(a = \sqrt{1+i})$, and $\tau : \sqrt{3} \mapsto -\sqrt{3}, \sqrt{1+i} \mapsto -\sqrt{1+i}$. Among our example algebras, $\mathcal{IA}$ has the densest maximal order. In Section V-D we will show that its maximal order is also the densest in general, when $F = \mathbf{Q}(i)$ and $m = n_r = 2$.

Let us now describe the code explicitly. If we order the $\mathbf{Z}$-basis of the natural order of $\mathcal{IA}$ as $\{e_i\}_{1 \le i \le 16} =$

$$\{1, u, i, \gamma, a, ui, u\gamma, ua, i\gamma, ia, a\gamma, ui\gamma, uia, ua\gamma, ia\gamma, uia\gamma\},$$

then (according to the MAGMA software [31]) the maximal order $\Lambda_{MAX} \subseteq \mathcal{IA}$ has a $\mathbf{Z}$-basis

$$\begin{aligned}\{ &\frac{1}{2} \quad (\quad e_1 + e_2 + e_3 + e_6 \ ), \\ &\frac{1}{2} \quad (\quad e_2 + e_6 + e_9 + e_{12} + e_{14} + e_{16} \ ), \\ &\frac{1}{2} \quad (\quad e_3 + e_6 + e_7 + e_9 + e_{14} + e_{15} \ ), \\ &\frac{1}{2} \quad (\quad e_4 + e_6 + e_7 + e_9 + e_{12} \ ), \\ &\frac{1}{2} \quad (\quad e_5 + e_8 + e_{10} + e_{13} \ ), \ e_6, \ e_7, \\ &\frac{1}{2} \quad (\quad e_8 + e_{13} + e_{15} + e_{16} \ ), \ e_9, \\ &\frac{1}{2} \quad (\quad e_{10} + e_{13} + e_{14} + e_{15} \ ), \\ &\frac{1}{2} \quad (\quad e_{11} + e_{14} + e_{15} + e_{16} \ ), \\ &\qquad e_{12}, \ e_{13}, \ e_{14}, \ e_{15}, \ e_{16} \ \}.\end{aligned}$$

Now the codebook $\mathcal{C} \subseteq \Lambda_{MAX}$ of an arbitrary size can be produced as

$$\mathcal{C} \subseteq \{M \in \Lambda_{MAX} \mid ||M|| \le E\},$$

where $||\cdot||$ denotes the Frobenius norm (corresponds to the squared Euclidean norm of the vectorized matrix, i.e. the sum of the squares of all the matrix elements), and E is some desired energy limit.

4) Algebra $\mathcal{QA}$ – an improved natural order: Let us use the multi-block notation for a change. Here we consider another tower of number fields $F \subset L \subset E$, where $E = \mathbf{Q}(\zeta_5, i)$, $F = \mathbf{Q}(i)$, and where $L = \mathbf{Q}(\theta, i)$ with $\theta = \zeta_5 + \zeta_5^{-1}$. Clearly we have $\mathrm{Gal}(E/F) = \langle\tau\rangle$, $\tau(\zeta_5) = \zeta_5^2$, and $\tau(\theta) = \theta^2 - 2$. Thus we obtain the CDA $\mathcal{QA} = (E/L, \sigma = \tau^2, \gamma) = E \oplus uE$, and $\gamma = u^2 = i$ is a non-norm element. Embedding the algebra $\mathcal{QA}$ as in Proposition 5.1 yields the following multi-block ST code with coding over 2 consecutive fading blocks:

$$\mathcal{QA}_1 \quad \subseteq \quad \{(B \ \tau(B)) \mid x_i \in \mathcal{O}_E\},$$

where

$$B = \begin{pmatrix} x_0 & i\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix}$$

and

$$\tau(B) = \begin{pmatrix} \tau(x_0) & i\tau(\sigma(x_1)) \\ \tau(x_1) & \tau(\sigma(x_0)) \end{pmatrix}.$$

The elements x_k in the above are of the form $x_k = \sum_{j=0}^{3} a_{k,j}\zeta_5^j$, where $a_{k,j} \in \mathbf{Z}[i]$, hence the above code transmits on the average, 2 independent QAM symbols per channel use.

Among our example algebras, $\mathcal{QA}$ has the densest natural order.

TABLE I

NORMALIZED MINIMUM DETERMINANT δ AND NORMALIZED DENSITY $\rho = 1/m(\Lambda)$ OF NATURAL AND MAXIMAL ORDERS OF DIFFERENT ALGEBRAS.

	$\mathcal{QA}$	$\mathcal{CA}$	$\mathcal{IA}$	$\mathcal{PA}$
	$\mathbf{\Lambda_{NAT}}$	Λ_{NAT}	Λ_{NAT}	Λ_{NAT}
δ	$\mathbf{0.0894}$	0.0361	0.0340	0.0298
ρ	$5^{-6} = 6.4 \cdot 10^{-5}$	$2^{-16} \cdot 3^{-2} = 1.7 \cdot 10^{-6}$	$2^{-10} \cdot 3^{-6} = 1.4 \cdot 10^{-6}$	$3^{-4} \cdot 5^{-6} = 7.9 \cdot 10^{-7}$
	$\mathcal{IA}$	$\mathcal{CA}$	$\mathcal{QA}$	$\mathcal{PA}$
	$\mathbf{\Lambda_{MAX}}$	Λ_{MAX}	Λ_{MAX}	Λ_{MAX}
δ	$\mathbf{0.1361}$	0.1214	0.0894	0.0894
ρ	$2^{-2} \cdot 3^{-6} = \mathbf{3.4 \cdot 10^{-4}}$	$2^{-9} \cdot 3^{-2} = 2.2 \cdot 10^{-4}$	$5^{-6} = 6.4 \cdot 10^{-5}$	$5^{-6} = 6.4 \cdot 10^{-5}$

Example 5.1: Let us calculate the normalized minimum determinant of the algebra $\mathcal{IA}$ as an example (cf. Section I, Definitions 3.4, 3.5, and Propositions 5.1,5.3). The other algebras can be treated likewise. In Table I we have listed the normalized minimum determinants δ and densities ρ of the natural and maximal orders of the algebras $\mathcal{PA}, \mathcal{CA}, \mathcal{IA}$, and $\mathcal{QA}$. Note that for $\mathcal{QA}$ these two actually coincide. We can conclude that among the natural orders, that of the algebra $\mathcal{QA}$ has the largest normalized minimum determinant, i.e. the highest density. The algebra $\mathcal{IA}$, for its part, has the densest maximal order. The corresponding numbers are shown **bold** in Table I.

For the natural order of $\mathcal{IA}$ we have $\det_{min}(\mathcal{C}(\Lambda_{NAT})) = 1$ and $\rho^{-1} = m(\mathcal{C}(\Lambda_{NAT})) = 2^{10} \cdot 3^6$, hence $t = 2^{-5/8} \cdot 3^{-3/8}$. Now $m(t\mathcal{C}(\Lambda_{NAT})) = 1$ and the normalized minimum determinant is $\delta = \det_{min}(t\mathcal{C}(\Lambda_{NAT})) = 2^{-5/2} \cdot 3^{-3/2} \cdot 1 \approx 0.0340$.

The maximal order of $\mathcal{IA}$ has $\det_{min}(\mathcal{C}(\Lambda_{MAX})) = 1$ and $m(\mathcal{C}(\Lambda_{MAX})) = 2^2 \cdot 3^6$, thus $t = 2^{-1/8} \cdot 3^{-3/8}$ and $\delta = \det_{min}(t\mathcal{C}(\Lambda_{MAX})) = \frac{1}{3\sqrt{2}\sqrt{3}} \approx 0.1361$.

D. An explicit density upper bound for the lattices $\mathcal{C}(\Lambda)$ with $F = \mathbf{Q}(i)$ and $n_t = 4$

As shown in Example 5.1, for the maximal order Λ of $\mathcal{IA}$ we have

$$\begin{aligned} m(\mathcal{C}(\Lambda)) &= d(\mathcal{O}_L/\mathcal{O}_F)^{dim_L \mathcal{IA}} N_{L/F}(d(\Lambda/\mathcal{O}_L)) \\ &= d(\mathcal{O}_L/\mathcal{O}_F)^4 N_{L/F}(P_1^2 P_2^2) \\ &= 3^4 \cdot 2^2 \cdot 3^2 = 2916, \end{aligned}$$

where P_1 and P_2 are the norm wise smallest ideals of $\mathcal{O}_L$. In what follows, we will show that when $F = \mathbf{Q}(i)$ and $m =$

$n_r = 2$ we cannot go below this, i.e. the maximal order of $\mathcal{IA}$ has optimal density.

Let us now assume that we would have such an extension $L/\mathbf{Q}(i)$ that the corresponding lattice would have $m(\Lambda) < 2916$. If the prime $1+i$ splits, this would mean that $d(\mathcal{O}_L/\mathbf{Z}[i]) < \sqrt{27} \approx 5.196$. If $1+i$ does not split, then the discriminant should be even smaller so this is a sufficient upper bound for $d(\mathcal{O}_L/\mathbf{Z}[i])$.

Let $\alpha \in \mathcal{O}_L$ such that $\{1, \alpha\}$ is an integral basis for $L/\mathbf{Q}(i)$. Now this degree two extension has a minimal polynomial of the form $f_\alpha(x) = x^2 + bx + c$, where $b, c \in \mathbf{Z}[i]$, and the discriminant

$$d(\mathcal{O}_L/\mathcal{O}_F) = b^2 - 4c \in \mathbf{Z}[i].$$

Note that a minimal polynomial of the form $x^2 + c$ is out of the question, as then $|d(\mathcal{O}_L/\mathcal{O}_F)| = 4|c| \geq 4\sqrt{2} > 5.196$. Furthermore, $d(\mathcal{O}_L/\mathcal{O}_F)$ cannot be a square, as then it would trivially follow that $\alpha \in \mathbf{Q}(i)$ and $L = \mathbf{Q}(i)$. Now we are left with the choices $d(\mathcal{O}_L/\mathcal{O}_F) \in \{1+i, (1+i)^3, 2+i, (1+i)(2+i), (1+i)^2(2+i), 3(1+i), 3, 2+3i, (1+i)(2+3i), 4+i\}$ or the obvious translates with the same absolute value.

Let us treat in detail the cases $d(\mathcal{O}_L/\mathcal{O}_F) = (1+i)^j,\ j = 1, 3$ to set an example. As the prime $1+i$ ramifies in this extension, we know that the smallest ideal is $P_1 \in \mathcal{O}_L$ above $1+i$ and $N(P_1) = 1+i$. The second ideal P_2 would depend on the behavior of the primes $2+i$ and 3. However, as $d(\mathcal{O}_L/\mathcal{O}_F) = b^2 - 4c = (r+si)^2 - 4(t+ui) = (r^2 - s^2 - 4t) + (2rs - 4u)i = (1+i)^j,\ r, s, t, u \in \mathbf{Z}$, it immediately follows that neither of $j = 1, 3$ fit into the equation.

The other cases are equally straightforward. In the case $d(\mathcal{O}_L/\mathcal{O}_F) = \pm 3$ we note that we end up into an isomorphic extension $L/\mathbf{Q}(i) \simeq \mathbf{Q}(\zeta_{12}) \simeq \mathbf{Q}(i, \sqrt{3})/\mathbf{Q}(i)$ that we already have. For $d(\mathcal{O}_L/\mathcal{O}_F) = 1 + 4i$ it would require that $1+i$ splits which is not the case.

We have now proved the following proposition. For the notation, cf. Proposition 5.1.

Proposition 5.10 (Density Bound for $n_t = 4$, $F = \mathbf{Q}(i)$): Let $m = n_r = 2$, i.e. $n_t = 4$. For the density of the lattice $\mathcal{C}(\Lambda)$ it holds that

$$\rho = 1/m(\mathcal{C}(\Lambda)) \leq \frac{1}{2^2 \cdot 3^6} \approx 0.00034. \tag{14}$$

The lower bound is achieved e.g. by the maximal order of the algebra $\mathcal{IA}$, see Table I. ∎

VI. Constructing AST lattices by the Smart Puncturing Method (SPM)

Another way to construct AST lattices would be as follows (cf. [24]). Let $\mathcal{A} = (E/F, \tau, \gamma)$ be an index n_t division algebra and $[E : L] = m,\ [L : F] = n_r$. If in the standard matrix representation the elements x_i are restricted to belong to L (rather than to E), we obtain another division algebra $\mathcal{A}'$. Obviously also the algebra $\mathcal{A}'$ is a division algebra as it is contained in $\mathcal{A}$. This construction also yields rate n_r codes for n_tTx+n_rRx antennas with a non-vanishing determinant. As L is fixed by $\sigma = \tau^{n_r}$ we have

$$lu^{n_r} = u\tau(l)u^{n_r-1} = \cdots = u^{n_r}\tau^{n_r}(l) = u^{n_r}\sigma(l) = u^{n_r}l$$

for all $l \in L$. Thus, the center F of $\mathcal{A}$ is extended by the element u^{n_r}.

Proposition 6.1: Let $\mathcal{O}_L$ be the ring of algebraic integers of L and $F = \mathbf{Q}(i)$. The lattice

$$\mathcal{C}_2 = \left\{ \begin{pmatrix} x_0 & \gamma\tau(x_3) & \cdots & \gamma\tau^{n_t-1}(x_1) \\ x_1 & \tau(x_0) & \cdots & \gamma\tau^{n_t-1}(x_2) \\ \vdots & & & \vdots \\ x_{n_t-1} & \tau(x_{n_t-2}) & \cdots & \tau^{n_t-1}(x_0) \end{pmatrix} \right\},$$

$x_i \in \mathcal{O}_L$ has a non-vanishing determinant $\det(\mathcal{C}_2) \in \mathbf{Z}[i]$. Thus, the minimum determinant is equal to one.

Proof: This immediately follows from the way of construction. ∎

As we consider the construction of Proposition 6.1 only for natural orders, we denote it by $\mathcal{C}_2$ as opposed to the notation $\mathcal{C}_1(\Lambda)$ where we needed to specify the order in use. The above *subfield construction method* [24] can be generalized so that it applies to any number of receiving antennas #Rx<#Tx. The idea is that instead of restricting the elements x_i to belong to a subfield, we can puncture at *any* level. By this we mean that we can set an arbitrary number of the QAM/HEX coefficients equal to zero. More formally, let us denote

$$x_j = \sum_{k=0}^{n_t-1} a_{k,j} e_j \in \mathcal{O}_E \quad (j = 0, ..., n_t - 1),$$

where $a_{k,j} \in \mathbf{Z}[\delta]$ and $e_0, ..., e_{n_t-1}$ is an integral basis of E/F. If we wish to use n_r receiving antennas, we set any $n_t - n_r$ of the coefficients $a_{k,j}$ to zero for each x_j. Nevertheless, to enable efficient decoding one should choose the same set of indices k at where to puncture for each x_j. We call this the *Smart Puncturing Method (SPM)*.

For instance, one option is to define $a_{k,j} = 0$ for $n_r \leq k \leq n_t - 1$, that is

$$x_j = \sum_{k=0}^{n_r-1} a_{k,j} e_j$$

for $j = 0, ..., n_t - 1$.

A. Explicit codes using SPM

Let us now use the SPM for constructing AST codes. To simplify the notation, we use the subfield construction as a special case of SPM. To set an example, we write down the constructions for the algebras $\mathcal{PA}$ and $\mathcal{CA}$, the other algebras can be treated similarly.

1) Algebra $\mathcal{PA}$: By using the algebra $\mathcal{PA}$ (cf. Section V-C.1) and the subfield construction 6.1, we get

$$\mathcal{PA}_2 \subseteq \left\{ \begin{pmatrix} x_0 & i\tau(x_3) & ix_2 & i\tau(x_1) \\ x_1 & \tau(x_0) & ix_3 & i\tau(x_2) \\ x_2 & \tau(x_1) & x_0 & i\tau(x_3) \\ x_3 & \tau(x_2) & x_1 & \tau(x_0) \end{pmatrix} \;\middle|\; x_i \in \mathcal{O}_L \right\}.$$

Each of the elements x_k is of the form $x_k = a_{k,0} + a_{k,1}\pi$, where $a_{k,j} \in \mathbf{Z}[i]$. Thus, the code rate is again equal to two.

2) Algebra $\mathcal{CA}$: Let us then construct a code using $\mathcal{CA}$ (cf. Section V-C.2) and 6.1. This time we have

$$\mathcal{CA}_2 \subseteq \left\{ \left(\begin{array}{cccc} x_0 & \gamma\tau(x_3) & \gamma x_2 & \gamma\tau(x_1) \\ x_1 & \tau(x_0) & \gamma x_3 & \gamma\tau(x_2) \\ x_2 & \tau(x_1) & x_0 & \gamma\tau(x_3) \\ x_3 & \tau(x_2) & x_1 & \tau(x_0) \end{array} \right) \;\middle|\; x_i \in \mathcal{O}_L \right\}$$

with $\gamma = 2 + i$.

Each of the elements x_k is of the form $a_{k,0} + a_{k,1}s$, where $a_{k,j} \in \mathbf{Z}[i]$. Thus, the code rate equals two.

Again we could also use a unit non-norm element $\gamma = \frac{2+i}{2-i}$.

VII. Simulation results

In Figure 1, the different construction methods are denoted by subscripts: 0 = Trivial Puncturing Method, 1 = Block Diagonal Method (cf. V-C), and 2 = Subfield Construction Method (cf. VI-A).

The use of a maximal order instead of the natural order will be indicated by 'MAX', e.g. we write $\mathcal{IA}_{1,MAX}$ for the code designed using the BDM and a maximal order of the algebra $\mathcal{IA}$.

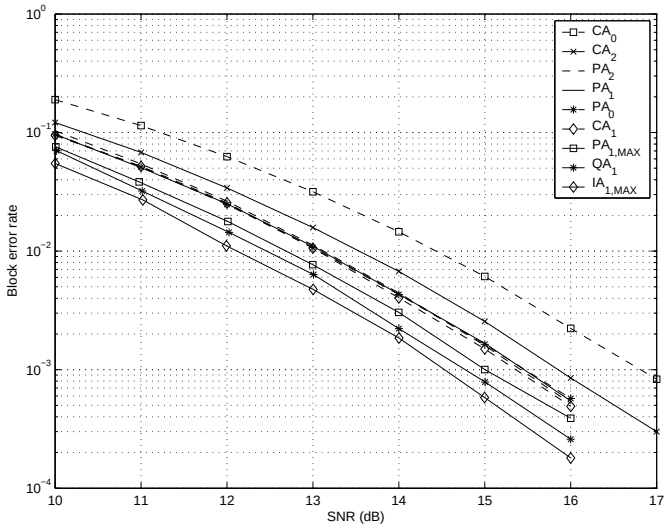


Fig. 1. Block error rates at 4 bpcu.

First of all, we have to admit that we have not carried out optimization as much as would have been possible. For example, the use of ideals has not been taken advantage of, except in the case of the punctured Perfect code $\mathcal{PA}_0$ and the code $\mathcal{PA}_1$, for which we used the ideal given in V-C.1. Still, the simulation results are indeed very satisfactory.

The codes $\mathcal{CA}_1$, $\mathcal{PA}_2$, $\mathcal{PA}_1$, and $\mathcal{PA}_0$ perform more or less equally. The code $\mathcal{CA}_2$ is beaten by these by 0.2-0.7 dB, depending on the SNR. Next comes $\mathcal{CA}_0$ ($x_1 = x_3 = 0$), losing still by $0.7 - 1$ dB to $\mathcal{CA}_2$. Despite of its lower density, the code $\mathcal{PA}_1$ performs equally well as the code $\mathcal{CA}_1$, possibly because of the careful optimization of $\mathcal{PA}_1$ carried out in [10] such that it falls into the category of *information lossless (IL)* codes (see [40] for the definition) and has a good (orthogonal) lattice *shaping*. Probably for the same reason, it appears to be irrelevant to which construction method is used for $\mathcal{PA}$, whereas the same is not true at all for the other algebras. Thus, the simulation results of the $\mathcal{PA}$ codes suggest that having a good shaping is also important at low SNR regime and it is better that the code has this property.

Do note that information losslessness is a property defined for linear dispersion (LD) codes and as such does not concern the maximal order codes (they are not linear dispersion codes when optimally used). Orthogonal shaping, for its part, has many other justifications than that of yielding information lossless codes. As mentioned earlier, orthogonal (or hexagonal) shaping enables simple bit labeling and usually makes the decoding less complex. Hence, in addition to density (maximization of the normalized minimum determinant), it is preferable to have orthogonal or nearly orthogonal shaping. In our simulations we did not do lattice reduction or use any other methods to simplify the decoding, as we feel that these concepts should be treated in a paper of their own.

To summarize the above, by orthogonal shaping one can compensate somewhat the lower density. That is, if we have two equally dense codes, then one might prefer the one that is closer to being orthogonal. But do note that by using orthogonal codes only, one cannot achieve the excellent performance provided by the maximal order codes as is clearly shown by the simulations. Also the data rate used in Figure 1 is very much in favor of $\mathcal{PA}$ as its shape fits perfectly with the constellation. At a different data rate (e.g. at 5 bpcu), however, the performance of $\mathcal{PA}$ can be expected to get worse as compared to the maximal order codes as then the orthogonal shape does not help that much and the density has more impact. Similar phenomenon was experienced when comparing the Golden code with the Golden+ code [17]: At the rate 4 bpcu that is ideal for the Golden code it could not be beaten, but immediately when taking a bigger data rate the difference became clear and the denser Golden+ code was shown to outperform the Golden code.

The code $\mathcal{IA}_{1,MAX}$ obtained by combining BDM with the use of a maximal order (cf. V-C.3 and [22]) triumphs over all the other codes. It outperforms the next best code $\mathcal{QA}_1$ by approximately 0.3 dB and $\mathcal{PA}_{1,MAX}$ by 0.5 dB. In [25] the authors show that the DjABBA code wins the punctured Perfect code by 0.5 dB or less in the BER performance at the rate 4 bpcu. The same holds for the BLER performance and thus our code improves even upon the DjABBA code. Also the Icosian code for 4Tx+2Rx antennas exploiting the Icosian ring (which also happens to be a maximal order) loses to $\mathcal{IA}_{1,MAX}$ by 0.7-1 dB. The curves depicting the DjABBA code, the Icosian code and the perfect version of $\mathcal{CA}_1$ are not shown in the picture in order to keep it readable. The perfect version of the code $\mathcal{CA}_{1,PERF}$ performs almost equally to $\mathcal{PA}_{1,MAX}$ being just slightly better.

Remark 7.1: There are some practical problems related to maximal order codes in general. Using maximal orders or more generally highly skewed lattices can make the bit labeling less obvious and the decoding process more complex even when the same decoding procedure is used. E.g. comparing the number of points in the search tree visited by a sphere decoder shows that usually a skewed lattice causes more visits than an orthogonal one. So these are purely properties the system designer can choose to use or not to use, depending

on the situation. Nevertheless, the decoding complexity can be significantly reduced by using sphere encoding together with some suboptimal decoding techniques getting very close to the maximal-likelihood (ML) performance, see [42] for the promising results.

Here, a suitably modified (more details will follow in a forthcoming paper, see [35]) sphere decoder was used for decoding the lattices. Briefly, the sphere decoder performs an additional energy check, checking that the decoded codeword is valid and within the desired energy sphere. This step is required because of the spherical shape used for the constellation. The codebook can be formed beforehand, so it has to be carried out only once. Alternatively, maintaining a codebook can be overcome by using sphere encoding as mentioned above. The maximal order codes can be also used as linear dispersion codes, but then the full advantage of the density of maximal orders is not achieved. If used as LD codes, no additional steps are needed for decoding.

The DMT analysis (Section VIII) tells us that asymptotically BDM should outperform the other constructions methods, but we want to emphasize that, as suggested by Figure 1, at the low SNR this is not necessarily the case. Indeed it seems that at the low SNRs, the best construction method depends on the very algebra (and especially on its density) that is in use. Figure 1 also shows that the trivial puncturing method used by other authors [25] is not always the first choice (as again implied by the DMT analysis too, see Section VIII), hence proving the point of new construction methods. Actually, for the algebra $\mathcal{CA}$ puncturing actually yields the worst performance.

VIII. Diversity-multiplexing tradeoff analyses

Diversity-Multiplexing Tradeoff (DMT) analyses of several constructions of asymmetric space-time codes will be given in this section. We try to make this section self contained. In a MIMO communication system with n_t transmit and n_r receive antennas, under the quasi-static MIMO Rayleigh block fading channel model, it is known that the ergodic MIMO channel capacity C equals [39]

$$C \;=\; \min\{n_t, n_r\}\log_2 \mathsf{SNR} + O(1) \quad \text{bits/channel use} \tag{15}$$

at high SNR regime.

Let R denote that data rate of a space-time code $\mathcal{X}$ defined in Definition 1.1, and let r denote the *normalized rate* of $\mathcal{X}$, also known as the *multiplexing gain* [19], given by

$$r \;:=\; \frac{R}{\log_2 \mathsf{SNR}}. \tag{16}$$

From (15) it can be seen that the maximum achievable multiplexing gain equals $\min\{n_t, n_r\}$. Given the code $\mathcal{X}$ with multiplexing gain r, we say $\mathcal{X}$ achieves *diversity gain* $d(r)$ if at high SNR regime, the codeword error probability of $\mathcal{X}$ is on the order of

$$P_e(r) \;\doteq\; \mathsf{SNR}^{-d(r)}. \tag{17}$$

By $\doteq$ we mean the exponential equality [19], i.e. we say the function $f(\mathsf{SNR}) \doteq \mathsf{SNR}^b$ if and only if

$$\lim_{\mathsf{SNR}\to\infty} \frac{\log f(\mathsf{SNR})}{\log \mathsf{SNR}} = b. \tag{18}$$

The notations of $\dot{\geq}$ and $\dot{\leq}$ are defined similarly.

Zheng and Tse [19] showed that there exists a fundamental tradeoff between the multiplexing and the diversity gains, referred to as the *diversity-multiplexing tradeoff* (DMT). For the cases when $T \geq n_t + n_r - 1$ and when the code $\mathcal{X}$ spans over m independent block fading channels, the DMT asserts that the maximum possible diversity gain $d^*(r)$ for any space-time coding scheme with multiplexing gain r is a piecewise linear function connecting the points $(k, d^*(k))$, $k = 0, 1, \cdots, \min\{n_t, n_r\}$, and

$$d^*(k) \;=\; m\,(n_t - k)\,(n_r - k)\,. \tag{19}$$

Furthermore, it has been shown in [20] using explicit constructions that the tradeoff (19) holds whenever $T \geq n_t$. On the other hand, if $T < n_t$, only upper and lower bounds on $d^*(r)$ are available in [19].

A. DMT for the trivial puncturing construction

Let $\mathfrak{D}_0$ denote the cyclic division algebra $(E/F, \sigma, \gamma)$ where $[E : F] = n_t$ and E/F is cyclic Galois. Let $F = \mathbf{Q}(i)$ and let $\mathcal{D}_0$ be the corresponding $(n_t \times n_t)$ cyclic algebra:

$$\mathcal{D}_0 \;=\; \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_{n_t-1}) & \cdots & \gamma\sigma^{n_t-1}(x_1) \\ x_1 & \sigma(x_0) & \cdots & \gamma\sigma^{n_t-1}(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ x_{n_t-1} & \sigma(x_{n_t-2}) & \cdots & \sigma^{n_t-1}(x_0) \end{pmatrix} \right\},$$

where $x_i \in E$. The puncturing construction $\mathcal{X}_0$ is thus obtained by setting $x_{n_r} = \cdots = x_{n_t-1} = 0$ in $\mathcal{D}_0$ and by restricting the elements $x_0, \cdots, x_{n_r-1}$ to be of form

$$x_i \;=\; \sum_{j=0}^{n_t-1} a_{i,j} e_i, \quad a_{i,j} \in \mathcal{A}_0, \quad i = 0, \cdots, n_r - 1,$$

where $\mathcal{A}_0 \subset \mathbf{Z}[i]$ is the underlying base-alphabet and where $\{e_0, \cdots, e_{n_t-1}\}$ is an integral basis for E/F.

Remark 8.1: If $|\gamma| = 1$, it does not matter which ones of the coefficients x_i we set equal to zero. However, if $|\gamma| > 1$, then we should choose the indices for which $x_i = 0$ in such a way that the overall energy is minimized. It can be easily verified that the above puncturing method, i.e. $x_{n_r} = \cdots = x_{n_t-1} = 0$, is the most efficient in energy.

To achieve multiplexing gain at value r, we require

$$|\mathcal{X}_0| \;=\; |\mathcal{A}_0|^{n_t n_r} \;\doteq\; \mathsf{SNR}^{n_t r}, \tag{20}$$

hence

$$|\mathcal{A}_0| \;=\; \mathsf{SNR}^{\frac{r}{n_r}}. \tag{21}$$

Given the transmitted code matrix $X_0 \in \mathcal{X}_0$, the received signal matrix Y_0 at the receiver end is

$$Y_0 \;=\; \theta_0 H X_0 + W \tag{22}$$

where we set

$$\theta_0^2 \;=\; \mathsf{SNR}^{1-\frac{r}{n_r}} \tag{23}$$

to ensure the power constraint $\frac{1}{n_t}\mathbb{E}\,\|X_0\|^2 \leq \mathsf{SNR}$. Let $\lambda_1 \leq \cdots \lambda_{n_r}$ be the ordered eigenvalues of $HH^\dagger$, and for any $X_0 \neq X_0' \in \mathcal{X}_0$, let $\delta_1 \geq \cdots \geq \delta_{n_t}$ be the ordered eigenvalues

of $\Delta X_0 \Delta X_0^\dagger$, where $\Delta X_0 = X_0 - X_0'$. Then given H, the squared Euclidean distance between $\theta_0 H X_0$ and $\theta_0 H X_0'$ is

$$\begin{aligned} d_E^2(X_0, X_0') &:= \theta_0^2 \|H \Delta X_0\|^2 \geq \theta_0^2 \sum_{i=1}^{n_r} \lambda_i \delta_{n_t - n_r + i} \\ &\geq \theta_0^2 \sum_{i=n_r-k+1}^{n_r} \lambda_i \delta_{n_t-n_r+i} \\ &\dot{\geq} \theta_0^2 \left(\prod_{i=n_r-k+1}^{n_r} \lambda_i \delta_{n_t-n_r+i} \right)^{\frac{1}{k}} \end{aligned}$$

for $k = 1, 2, \cdots, n_r$. In particular,

$$\begin{aligned} \prod_{i=n_r-k+1}^{n_r} \delta_{n_t-n_r+i} &\geq \frac{1}{\prod_{i=1}^{n_t-k} \delta_i} \dot{\geq} \|\Delta X_0\|^{-2(n_t-k)} \\ &\doteq \mathsf{SNR}^{-\frac{r(n_t-k)}{n_r}}. \end{aligned}$$

Combining the two results above and setting $\alpha_i = -\log_{SNR} \lambda_i$ we have $d_E^2(X_0, X_0') \dot{\geq} \mathsf{SNR}^{E_k}$ and

$$\begin{aligned} E_k &= 1 - \frac{r}{n_r} - \frac{1}{k} \sum_{i=n_r-k+1}^{n_r} \alpha_i - \frac{r(n_t-k)}{k n_r} \\ &= \frac{1}{k} \left[\sum_{i=n_r-k+1}^{n_r} (1-\alpha_i) - mr \right]. \end{aligned}$$

Now we see the DMT for the puncturing construction is lower bounded by

$$d_0(r) \geq \inf_{\alpha_i : E_k < 0} \sum_{i=1}^{n_r} (2i - 1 + n_r(m-1)) \alpha_i \qquad (24)$$

and the right-hand-side is given by the lines connecting the points $(n_t - mr)(n_r - mr)$ for integral values of mr.

B. DMT for the block diagonal construction

Let E/F be cyclic Galois with $[E:F] = n_t$, $\mathrm{Gal}(E/F) = \langle \tau \rangle$ and $F = \mathbf{Q}(i)$. Let $L \subset E$ be such that $[E:L] = n_r$ and $[L:F] = m$ with $\mathrm{Gal}(E/L) = \langle \sigma \rangle$ where $\sigma = \tau^m$. It should be noted that we have assumed $n_t = m n_r$. Let $\mathfrak{D}_1$ be the cyclic division algebra $(E/L, \sigma, \gamma)$ and let $\mathcal{D}_1$ be the corresponding $(n_r \times n_r)$ algebra:

$$\mathcal{D}_1 = \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_{n_r-1}) & \cdots & \gamma\sigma^{n_r-1}(x_1) \\ x_1 & \sigma(x_0) & \cdots & \gamma\sigma^{n_r-1}(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ x_{n_r-1} & \sigma(x_{n_r-2}) & \cdots & \sigma^{n_r-1}(x_0) \end{pmatrix} \right\},$$

$x_i \in E$. The block diagonal construction $\mathcal{X}_1$ is

$$\mathcal{X}_1 = \left\{ \mathrm{diag}(X_1, \tau(X_1), \cdots, \tau^{m-1}(X_1)) \right\}, \qquad (25)$$

where $X_1 \in \mathcal{D}_1$ with $x_i = \sum_{j=0}^{n_t-1} a_{i,j} e_i$, $a_{i,j} \in \mathcal{A}_1$. $\mathcal{A}_1 \subset \mathbf{Z}[i]$ denotes the underlying base-alphabet and $\{e_0, \cdots, e_{n_t-1}\}$ is an integral basis for E/F.

To achieve multiplexing gain at value r, we require

$$|\mathcal{X}_1| = |\mathcal{A}_1|^{n_t n_r} \doteq \mathsf{SNR}^{n_t r}, \qquad (26)$$

hence

$$|\mathcal{A}_1| = \mathsf{SNR}^{\frac{r}{n_r}}. \qquad (27)$$

Given the transmitted code matrix

$$\mathrm{diag}(X, \tau(X), \cdots, \tau^{m-1}(X)) \in \mathcal{X}_1,$$

the received signal matrix Y_1 at the receiver end is

$$Y = \theta_1 H \mathrm{diag}(X, \tau(X), \cdots, \tau^{m-1}(X)) + W \qquad (28)$$

where we set

$$\theta_1^2 = \mathsf{SNR}^{1-\frac{r}{n_r}} \qquad (29)$$

to ensure the power constraint. On the other hand, we may partition the matrices Y, H, and W into

$$\begin{aligned} Y &= [Y_0\ Y_1\ \cdots\ Y_{m-1}], \quad H = [H_0\ H_1\ \cdots\ H_{m-1}], \\ W &= [W_0\ W_1\ \cdots\ W_{m-1}] \end{aligned}$$

and rewrite (28) as

$$Y_i = \theta_1 H_i \tau^i(X) + W_i$$

for $i = 0, 1, \cdots, m-1$. Let

$$\lambda_{i,1} \leq \cdots \leq \lambda_{i,n_r}$$

be the ordered eigenvalues of $H_i H_i^\dagger$, and for any

$$\begin{aligned} &\mathrm{diag}(X, \tau(X), \cdots, \tau^{m-1}(X)) \\ &\neq \mathrm{diag}(X', \tau(X'), \cdots, \tau^{m-1}(X')) \in \mathcal{X}_1, \end{aligned}$$

let

$$\delta_{i,1} \geq \cdots \geq \delta_{i,n_r}$$

be the ordered eigenvalues of $\Delta X_i \Delta X_i^\dagger$, where $\Delta X_i = \tau^i(X - X')$. We will re-order and re-index the set of eigenvalues $\{\lambda_{i,j}\}$ and $\{\delta_{i,j}\}$ such that $\lambda_1 \leq \lambda_2 \cdots \leq \lambda_{n_t}$ and $\delta_1 \geq \delta_2 \geq \cdots \geq \delta_{n_t}$. Thus the squared Euclidean distance between the two noise-free received signal matrices can be lower bounded by

$$\begin{aligned} d_E^2(X, X') &= \theta_1^2 \sum_{i=0}^{m-1} \|H_i \Delta X_i\|^2 \geq \theta_1^2 \sum_{i=1}^{n_t} \lambda_i \delta_i \\ &\geq \theta_1^2 \sum_{i=n_t-k+1}^{n_t} \lambda_i \delta_i \\ &\dot{\geq} \theta_1^2 \left(\prod_{i=n_t-k+1}^{n_t} \lambda_i \delta_i \right)^{\frac{1}{k}}. \end{aligned}$$

Moreover,

$$\begin{aligned} \prod_{i=n_t-k+1}^{n_t} \delta_i &\geq \frac{1}{\prod_{i=1}^{n_t-k} \delta_i} \dot{\geq} \left(\sum_{i=0}^{m-1} \|\Delta X_i\|^2 \right)^{-(n_t-k)} \\ &\doteq \mathsf{SNR}^{-\frac{r(n_t-k)}{n_r}}. \end{aligned}$$

Combining the two results above and setting $\alpha_i = -\log_{SNR} \lambda_i$ we have $d_E^2(X, X') \dot{\geq} \mathsf{SNR}^{E_k}$ and

$$\begin{aligned} E_k &= 1 - \frac{r}{n_r} - \frac{1}{k} \sum_{i=n_t-k+1}^{n_t} \alpha_i - \frac{r(n_t-k)}{k n_r} \\ &= \frac{1}{k} \left(\sum_{i=n_t-k+1}^{n_t} (1-\alpha_i) - rm \right). \end{aligned}$$

Now we see the DMT for the block-diagonal construction is given by

$$d_1(r) \;=\; \inf_{\alpha_i: E_k<0} \sum_{i=1}^{n_t} (2i-1)\,\alpha_i \tag{30}$$

and is obtained by the lines connecting the points $(n_t - mr)(n_r - r)$ for integral values of r.

C. DMT for the subfield construction

The DMT derived here for the subfield construction also holds for the more general codes designed using the smart puncturing method.

Let E/F be a cyclic Galois extension with $\mathrm{Gal}(E/F) = \langle\sigma\rangle$ and $[E:F] = n_t$, and $F = \mathbf{Q}(i)$. Let $\mathfrak{D}_2$ be the cyclic division algebra $(E/F, \sigma, \gamma)$ and let

$$\mathcal{D}_2 \;=\; \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_{n_t-1}) & \cdots & \gamma\sigma^{n_t-1}(x_1) \\ x_1 & \sigma(x_0) & \cdots & \gamma\sigma^{n_t-1}(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ x_{n_t-1} & \sigma(x_{n_t-2}) & \cdots & \sigma^{n_t-1}(x_0) \end{pmatrix} \right\},$$

where $x_i \in L$, $L \subset E$ and $[L:F] = n_r$. The subfield construction $\mathcal{X}_2$ is thus obtained by restricting the elements $x_0, \cdots, x_{n_t-1}$ to be of form

$$x_i \;=\; \sum_{j=0}^{n_r-1} a_{i,j} e_i, \quad a_{i,j} \in \mathcal{A}_2, \quad i = 0, \cdots, n_t - 1,$$

where $\mathcal{A}_2 \subset \mathbf{Z}[i]$ is the underlying base-alphabet and where $\{e_0, \cdots, e_{n_r-1}\}$ is an integral basis for L/F.

To achieve multiplexing gain at value r, we require

$$|\mathcal{X}_2| \;=\; |\mathcal{A}_2|^{n_t n_r} \;\doteq\; \mathsf{SNR}^{n_t r}, \tag{31}$$

hence

$$|\mathcal{A}_2| \;=\; \mathsf{SNR}^{\frac{r}{n_r}}. \tag{32}$$

Given the transmitted code matrix $X_2 \in \mathcal{X}_2$, the received signal matrix Y_2 at the receiver end is

$$Y_2 \;=\; \theta_2 H X_2 + W \tag{33}$$

where we set

$$\theta_2^2 \;=\; \mathsf{SNR}^{1-\frac{r}{n_r}} \tag{34}$$

to ensure the power constraint. Now we see the DMT for this construction has the same lower bound as that for the puncturing construction, hence

$$d_2(r) \;\geq\; \inf_{\alpha_i: E_k<0} \sum_{i=1}^{n_r} (2i - 1 + n_r(m-1))\,\alpha_i \tag{35}$$

and the right-hand-side is obtained by the lines connecting the points $(n_t - mr)(n_r - mr)$ for integral values of mr.

D. DMT for the original CDA construction

Let E/F be a cyclic Galois extension with $\mathrm{Gal}(E/F) = \langle\sigma\rangle$ and $[E:F] = n_t$, and $F = \mathbf{Q}(i)$. Let $\mathfrak{D}_3$ be the cyclic division algebra $(E/F, \sigma, \gamma)$ and let

$$\mathcal{D}_3 \;=\; \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_{n_t-1}) & \cdots & \gamma\sigma^{n_t-1}(x_1) \\ x_1 & \sigma(x_0) & \cdots & \gamma\sigma^{n_t-1}(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ x_{n_t-1} & \sigma(x_{n_t-2}) & \cdots & \sigma^{n_t-1}(x_0) \end{pmatrix} \right\},$$

$x_i \in E$. The original construction $\mathcal{X}_3$ (cf. e.g. [15]) is obtained by restricting the elements $x_0, \cdots, x_{n_t-1}$ to be of form

$$x_i \;=\; \sum_{j=0}^{n_t-1} a_{i,j} e_i, \quad a_{i,j} \in \mathcal{A}_3, \quad i = 0, \cdots, n_t - 1,$$

where $\mathcal{A}_3 \subset \mathbf{Z}[i]$ is the underlying base-alphabet and where $\{e_0, \cdots, e_{n_t-1}\}$ is an integral basis for E/F.

To achieve multiplexing gain at value r, we require

$$|\mathcal{X}_3| \;=\; |\mathcal{A}_3|^{n_t n_t} \;\doteq\; \mathsf{SNR}^{n_t r}, \tag{36}$$

hence

$$|\mathcal{A}_3| \;=\; \mathsf{SNR}^{\frac{r}{n_t}}. \tag{37}$$

Given the transmitted code matrix $X_3 \in \mathcal{X}_3$, the received signal matrix Y_3 at the receiver end is

$$Y_3 \;=\; \theta_3 H X_3 + W \tag{38}$$

where we set

$$\theta_3^2 \;=\; \mathsf{SNR}^{1-\frac{r}{n_t}} \tag{39}$$

to ensure the power constraint. Let $\lambda_1 \leq \cdots \lambda_{n_r}$ be the ordered eigenvalues of $HH^\dagger$, and for any $X_3 \neq X_3' \in \mathcal{X}_3$, let $\delta_1 \geq \cdots \geq \delta_{n_t}$ be the ordered eigenvalues of $\Delta X_3 \Delta X_3^\dagger$, where $\Delta X_3 = X_3 - X_3'$. Then given H, the squared Euclidean distance between $\theta_3 H X_3$ and $\theta_3 H X_3'$ is

$$\begin{aligned} d_E^2(X_0, X_0') \;&:=\; \theta_3^2 \left\|H \Delta X_3\right\|^2 \;\geq\; \theta_3^2 \sum_{i=1}^{n_r} \lambda_i \delta_{n_t-n_r+i} \\ &\geq\; \theta_3^2 \sum_{i=n_r-k+1}^{n_r} \lambda_i \delta_{n_t-n_r+i} \\ &\dot{\geq}\; \theta_3^2 \left(\prod_{i=n_r-k+1}^{n_r} \lambda_i \delta_{n_t-n_r+i} \right)^{\frac{1}{k}}. \end{aligned}$$

for $k = 1, 2, \cdots, n_r$. In particular,

$$\begin{aligned} \prod_{i=n_r-k+1}^{n_r} \delta_{n_t-n_r+i} \;&\geq\; \frac{1}{\prod_{i=1}^{n_t-k} \delta_i} \;\dot{\geq}\; \left\|\Delta X_0\right\|^{-2(n_t-k)} \\ &\doteq\; \mathsf{SNR}^{-\frac{r(n_t-k)}{n_t}}. \end{aligned}$$

Combining the two results above and setting $\alpha_i = -\log_{SNR} \lambda_i$ we have $d_E^2(X_3, X_3') \dot{\geq} \mathsf{SNR}^{E_k}$ and

$$\begin{aligned} E_k \;&=\; 1 - \frac{r}{n_t} - \frac{1}{k} \sum_{i=n_r-k+1}^{n_r} \alpha_i - \frac{r(n_t-k)}{k n_t} \\ &=\; \frac{1}{k} \left[\sum_{i=n_r-k+1}^{n_r} (1-\alpha_i) - r \right]. \end{aligned}$$

Now we see the DMT for the CDA construction is given by

$$d_3(r) \;=\; \inf_{\alpha_i : E_k < 0} \sum_{i=1}^{n_r} \left(2i - 1 + n_r(m-1)\right) \alpha_i \qquad (40)$$

and the right-hand-side is obtained by the lines connecting the points $(n_t - r)(n_r - r)$ for integral values of r.

Remark 8.2: One might ponder why not use the original symmetric construction with a smaller constellation as it is DMT optimal. In principle, AST codes can indeed be designed just by using the standard CDA-based MIMO code with a smaller constellation. Nevertheless, this destroys the lattice structure and causes exponential complexity at the receiver.

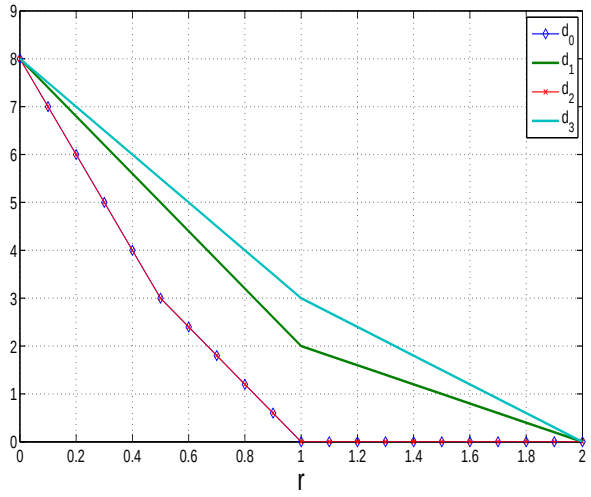


Fig. 2. DMT for $n_t = 4$, $n_r = 2$, and $m = 2$.

IX. Concluding remarks and suggestions for further work

We have introduced new construction methods for asymmetric space-time codes based on cyclic division algebras and their orders. Part of the results were reviewed from [24] and [17]. One of the methods, the so-called smart puncturing method, is suitable for an arbitrary number of transmitting antennas and lesser receiving antennas.

The density bound from [17] was generalized to the block diagonal asymmetric case and made explicit for the 4Tx+2Rx antenna case when building upon $\mathbf{Q}(i)$. Also a construction achieving this bound was provided. It was noted that in the more general case, the most reasonable way to derive density bounds is with the aid of Odlyzko bound as the computation of minimal discriminants is in general a hard problem.

We proved the connection between the block diagonal asymmetric and multi-block codes, hence showing that the density results hold as such in the multi-block case.

We have not yet exhausted the box of optimization tools on our code. E.g. the codes can be pre- and post-multiplied by any complex matrix of determinant one without affecting neither its density nor its good minimum product distance. In particular, if we use non-unitary matrix multipliers, the geometry of the lattice will change. While we cannot always turn the lattice into a rectangular one in this manner, some energy savings and perhaps also shaping gains are available. The simulations were carried out by using a suitably modified sphere decoder (on which more details in a forthcoming paper [35]). It was shown that the newly proposed codes outperform in block error performance the punctured Perfect code, the DjABBA code as well as the Icosian code, all aimed at transmission with four transmitting and two receiving antennas.

Also extensive DMT analysis was provided, showing that amongst the previously and newly proposed methods, the BDM is the best way to construct asymmetric codes in this respect.

X. Acknowledgments

We thank Professor P. Vijay Kumar (Indian Institute of Science, Bangalore, India) for bringing the perfect version of the code $\mathcal{CA}_1$ to our notice. We are also indebted to Dr. J. Lahtonen (University of Turku, Finland) for the helpful discussions during the revision process of this paper. Dr. R. Vehkalahti (University of Turku, Finland) is gratefully acknowledged for his help in Section V-C.3.

References

[1] J.-C. Guey, M. P. Fitz, M. R. Bell, and W. Y. Kuo, "Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels," *Proc. IEEE Vehicular Technology Conf.*, 1996, pp. 136–140. Also in *IEEE Trans. Commun.*, vol. 47, pp. 527–537, April 1999.

[2] V. Tarokh, N. Seshadri, and A.R. Calderbank, "Space-time codes for high data rate wireless communications: performance criterion and code construction," *IEEE Trans. Inf. Theory*, vol. 44, pp. 744–765, March 1998.

[3] J.-C. Belfiore, G. Rekaya, and E. Viterbo: "The Golden code: a 2x2 full-rate space-time code with non-vanishing determinant," *IEEE Trans. Inf. Theory*, vol. 51, n. 4, pp. 1432–1436, April 2005.

[4] S. M. Alamouti, "A simple transmit diversity technique for wireless communication," *IEEE J. on Select. Areas in Commun.*, vol. 16, pp. 1451–1458, October 1998.

[5] C. Hollanti and J. Lahtonen, "Maximal orders in the design of dense space-time lattice codes," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4493–4510, Oct. 2008.

[6] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Trans. Inf. Theory*, vol. 48, pp. 628–636, March 2002.

[7] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inf. Theory*, vol. 49, pp. 2596–2616, October 2003.

[8] J.-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," *Proc. ITW 2003*, Paris, France, March 31 - April 4, 2003.

[9] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "Algebraic 3x3, 4x4 and 6x6 space-time codes with non-vanishing determinants," in *Proc. IEEE ISITA 2004*, Parma, Italy, October 10 - 13, 2004.

[10] J.-C. Belfiore, F. Oggier, G. Rekaya, and E. Viterbo, "Perfect space-time block codes," *IEEE Trans. Inf. Theory*, vol. 52, pp. 3885–3902, September 2006.

[11] P. Elia, B. A. Sethuraman, and P. Vijay Kumar, "Perfect space-time codes for any number of antennas," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 3853–3868, Nov. 2007.

[12] Kiran. T and B. S. Rajan, "STBC-schemes with non-vanishing determinant for certain number of transmit antennas," *IEEE Trans. Inf. Theory*, vol. 51, pp. 2984–2992, August 2005.

[13] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman "STBCs using capacity achieving designs from crossed-product division algebras," in *Proc. IEEE ICC 2004*, pp. 827–831, Paris, France, 20-24 June 2004.

[14] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman, "Information-lossless STBCs from crossed-product algebras," *IEEE Trans. Inf. Theory*, vol. 52, pp. 3913–3935, September 2006.

[15] P. Elia, K. R. Kumar, P. V. Kumar, H.-F. Lu, and S. A. Pawar, "Explicit space-time codes achieving the diversity-multiplexing gain tradeoff," *IEEE Trans. Inf. Theory*, vol. 52, pp. 3869–3884, September 2006.
[16] H.-F. Lu, P. Elia, S. A. Pawar, K. R. Kumar, and P. V. Kumar, "Space-time codes meeting the diversity-multiplexing gain tradeoff with low signaling complexity," *Proc. CISS 2005*, Baltimore MD, March 2005.
[17] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, "On the densest MIMO lattices from cyclic division algebras," *IEEE Trans. Inf. Theory*, to appear. Available at: http://arxiv.org/abs/cs.IT/0703052.
[18] G. Wang and X.-G. Xia, "On Optimal Multi-Layer Cyclotomic Space-Time Code Designs," *IEEE Trans. Inf. Theory*, vol. 51, pp. 1102–1135, March 2005.
[19] L. Zheng and D. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1073–1096, May 2003.
[20] H.-f. (F.) Lu, "Explicit constructions of multi-block space-time codes that achieve the diversity-multiplexing tradeoff," in *Proc. IEEE ISIT 2006*, pp. 1149–1153, Seattle, 2006.
[21] H. El Gamal and A. R. Hammons, Jr., "A new approach to layered space-time coding and signal processing," *IEEE Trans. Inf. Theory*,vol. 47, pp. 2321–2334, Sep. 2001.
[22] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, "Optimal matrix lattices for MIMO codes from division algebras," in *Proc. IEEE ISIT 2006*, pp. 783–787, Seattle, July 9 - 14, 2006.
[23] N. Jacobson, *Basic Algebra II*, W. H. Freeman and Company, San Francisco 1980.
[24] C. Hollanti and K. Ranto, "Asymmetric space-time block codes for MIMO systems," *Proc. IEEE ITW 2007*, pp. 101–105, Bergen, Norway, July 2007.
[25] A. Hottinen, Y. Hong, E. Viterbo, C. Mehlführer, and C. F. Mecklenbräuker, "A comparison of high rate algebraic and non-orthogonal STBCs," *Proc. ITG/IEEE Workshop on Smart Antennas WSA 2007*, Vienna, Austria, February 2007.
[26] J. Lahtonen, "Dense MIMO matrix lattices and class field theoretic themes in their construction," *Proc. IEEE ITW 2007*, pp. 96–100, Bergen, Norway, July 2007.
[27] J. Liu and A. R. Calderbank, "The Icosian code and the E_8 lattice: a new 4×4 space-time code with nonvanishing determinant," *Proc. IEEE ISIT 2006*, Seattle, July 9 - 14, 2006.
[28] A. A. Albert, *Structure of Algebras*, American Mathematical Society, New York City 1939.
[29] I. Reiner, *Maximal Orders*, Academic Press, New York 1975.
[30] C. Hollanti and J. Lahtonen, "A new tool: constructing STBCs from maximal orders in central simple algebras," in *Proc. IEEE ITW 2006*, pp. 322–326, Punta del Este, March 13-17, 2006.
[31] Web page: http://magma.maths.usyd.edu.au/magma/htmlhelp/text835.htm#8121.
[32] G. Ivanyos and L. Rónyai, "On the complexity of finding maximal orders in semisimple algebras over Q," Computational Complexity 3, pp. 245–261, 1993.
[33] L. Rónyai, "Algorithmic properties of maximal orders in simple algebras over Q," *Computational Complexity 2*, pp. 225–243, 1992.
[34] L. Rónyai, "Computing the structure of finite algebras," *Journal of Symbolic Computation 9*, pp. 355–373, 1990.
[35] C. Hollanti and K. Ranto, "Maximal orders in space-time coding: construction and decoding," *Proc. 2008 Int. Symp. Inf. Theory and its Appl. (ISITA)*, New Zealand, Dec. 2008, to appear.
[36] S. Yang and J.-C. Belfiore, "Optimal space-time codes for the MIMO amplify-and-forward cooperative channel," *IEEE Trans. Inf. Theory*, vol. 53, pp. 647–663, Feb. 2007.
[37] H. Cohen, F. Diaz y Diaz, and M. Olivier, "A table of totally complex number fields of small discriminants," *Lecture Notes In Computer Science, Proceedings of the Third International Symposium on Algorithmic Number Theory*, pp. 381 – 391, 1998.
[38] A. M. Odlyzko, "Lower bounds for discriminants in number fields II," *Tohoku Math. J.*, no. 29, pp. 209–216, 1977.
[39] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Europ. Trans. Telecomm.*, vol. 10, no. 6, pp. 585–595, Nov.-Dec. 1999.
[40] M. O. Damen, A. Tewfik, J.-C. Belfiore, "A construction of a space-time code based on number theory," *IEEE Trans. Inform. Theory*, vol. 48, no. 3, pp. 753-760, Mar. 2002.
[41] H.-F. Lu and C. Hollanti, "Optimal diversity multiplexing tradeoff and code constructions of constrained asymmetric MIMO systems," submitted to *IEEE Trans. on Inform. Theory*, May 2008.
[42] K. Raj Kumar and Giuseppe Caire, "Space-time codes from structured lattices," submitted to *IEEE Trans. Inf. Theory*, April 2008. Preprint available at http://www.citebase.org/abstract?id=oai:arXiv.org:0804.1811.

Camilla Hollanti received the M.S. and Ph.D. degrees from the University of Turku, Finland, in 2003 and 2009, respectively, both in pure mathematics.

Since June 2004, she has been with the Department of Mathematics, University of Turku, Finland. In 2005, she visited the Department of Algebra at Charles' University, Prague, Czech Republic, for six months. In 2009-2011 she will be leading the project "Applications of Class Field Theory in Present and Future Multi-Antenna Communications" at the University of Turku, Finland.

Her research is in the area of applications of algebraic number theory and class field theory in lattice space-time coding.

Hollanti is a recipient of several grants from various foundations, including the Finnish Cultural Foundation research grant in 2007 and the Finnish Academy of Science research grant in 2008. She has also won the prize for the best presentation in the EWM 2007 conference of European Women in Mathematics that took place in Cambridge, UK in September 2007.

Hsiao-feng (Francis) Lu (S'98-M'04) received the B.S. degree from Tatung University, Taipei, Taiwan, in 1993, and the M.S.E.E. and Ph.D. degrees from the University of Southern California (USC), Los Angeles, in 1999 and 2003, respectively, all in electrical engineering.

He was a postdoctoral research fellow at University of Waterloo, ON, Canada, during 2003-2004. In February 2004, he joined the faculty of the Department of Communications Engineering, National Chung-Cheng University, Chiayi, Taiwan, and was promoted to Associate Professor in August 2007. Since August 2008, he has been with the Department of Communications Engineering, National Chiao Tung University, Hsinchu, Taiwan. His research is in the area of space-time codes, MIMO systems, error correcting codes, wireless communication, optical fiber communication, and multi-user detection.

Dr. Lu is a recipient of several research awards, including the 2006 IEEE Information Society Taipei Chapter and IEEE Communications Society Taipei/Tainan Chapter Best Paper Award for Young Scholars, the 2007 Wu Da You Memorial award from Taiwan National Science Council, the 2007 IEEE Communication Society Asia Pacific Outstanding Young Researchers Award, and the 2008 Academia Sinica Research Award for Junior Research Investigators.

Publication VI

Lu, H.-F. and Hollanti, C. (2008). Optimal diversity-multiplexing tradeoff and code constructions of constrained asymmetric MIMO systems. Submitted to *IEEE Transactions on Information Theory*.

Optimal Diversity Multiplexing Tradeoff and Code Constructions of Constrained Asymmetric MIMO Systems

Hsiao-feng (Francis) Lu and Camilla Hollanti

Abstract*— In multiple-input multiple-output (MIMO) communications, the type of asymmetric channel refers to the situation when the number of transmit antennas is strictly larger than the number of receive antennas, and such channel can often be found in MIMO downlink transmissions. While existing cyclic-division-algebra-(CDA-)based codes can still be applied to this channel and achieve optimal performance in terms of the well-known diversity-multiplexing tradeoff (DMT) at high SNR regime, such codes cannot be decoded using either zero-forcing or sphere decoding. Other methods such as minimal mean-square-error estimators would not perform well in this situation either, due to the shortage of observations. Thus, these codes cannot achieve the promised optimal performance unless maximal likelihood decoding is employed. To make simple decoding possible, it is better to constrain the number of active transmit antennas to be no larger than the number of receive, and the resulting system is coined *constrained asymmetric MIMO system.

Two general types of asymmetrical channels are considered in this paper. Specifically, when 1) there are two receive antennas and arbitrary number of transmit antennas, and 2) the number of transmit antennas is one larger than the number of receive antennas, the optimal transmission schemes of the constrained asymmetric MIMO channels are presented. The newly proposed constrained coding schemes are shown to achieve the same DMT performance as their unconstrained counterparts, meaning there is no performance loss in using lesser number of active transmit antennas. Explicit constructions of DMT optimal constrained codes for these constrained channels are also given. Furthermore, these codes are shown to be approximately universal and can be applied to more general asymmetric MIMO channels.

I. Introduction

The use of multiple antennas for wireless communication has been proved to be able to linearly increase the channel capacity [1] and at the same time, improve the diversity gain and provide better reliability [2]. In an $(n_t \times n_r)$ MIMO communication channel consisting of n_t transmit and n_r receive antennas, most of the existing literature [2]–[15] has focused on the case of $n_t \leq n_r$ and has extensively investigated the corresponding code designs. On the other hand, in MIMO downlink transmissions, it is often found that there can be more transmit antennas available at the base stations than the receive antennas at the mobile user end. That is, it corresponds to the case of $n_t > n_r$. Such MIMO channel is commonly referred to as the *asymmetric MIMO channel* [16].

Assuming that all the n_t transmit antennas are active during transmission, let $\underline{x}$ be the length-n_t code vector[1] sent from the transmitter to the receiver and let H be the corresponding $(n_r \times n_t)$ channel matrix. The length-n_r received signal vector $\underline{y}$ at the receiver end is given by

$$\underline{y} \;=\; H\underline{x} + \underline{w}, \tag{1}$$

where $\underline{w}$ is a length-n_r vector used to capture the effects of additive white Gaussian noise. For Rayleigh fading channels, entries of the channel matrix H and the noise vector $\underline{w}$ are modeled as i.i.d. complex Gaussian random variables with zero mean and unit variance. Further, the code vector $\underline{x}$ is required to satisfy the following power constraint

$$\mathrm{Tr}\left(\mathbb{E}\underline{x}\underline{x}^{\dagger}\right) \;\leq\; \mathrm{SNR}, \tag{2}$$

where by $\dagger$ we mean the Hermitian transpose of a vector.

When the channel matrix H is known completely to the receiver but not to the transmitter, Telatar [1] first showed that the ergodic channel capacity of such $(n_t \times n_r)$ MIMO channel approximates $\min\{n_t, n_r\}\log_2 \mathrm{SNR}$ at high SNR regime, regardless of the relation between n_t and n_r. Furthermore, it was shown that such capacity can be achieved by using i.i.d. complex Gaussian random vectors $\underline{x}$ having covariance matrix $K_X = \frac{\mathrm{SNR}}{n_t} I_{n_t}$. On the other hand, assuming that the transmitter communicates at rate

$$R \;=\; r\log_2 \mathrm{SNR} \qquad \text{(bits/channel use)}, \tag{3}$$

where r, $0 \leq r \leq \min\{n_t, n_r\}$, is termed *multiplexing gain*, Zheng and Tse [17] proved that given r, the smallest bit error probability that can be achieved by any coding schemes is given by

$$P_{\mathrm{e,min}}\left(\mathrm{SNR}\right) \;\doteq\; \mathrm{SNR}^{-d^*(r)}, \tag{4}$$

where by $\doteq$ we mean the exponential equality defined by

$$\lim_{\mathrm{SNR}\to\infty} \frac{\log P_{\mathrm{e,min}}\left(\mathrm{SNR}\right)}{\log \mathrm{SNR}} \;=\; -d^*(r). \tag{5}$$

The negative exponent $d^*(r)$ is termed *diversity gain*, and is given by a piecewise-linear function connecting the points

$$\left\{(k, (n_t-k)(n_r-k)) \;:\; k = 0, 1, \cdots, \min\{n_t, n_r\}\right\}. \tag{6}$$

$d^*(r)$ indicates an optimal tradeoff between the multiplexing gain r and the diversity gain, and is thus termed the *diversity-multiplexing tradeoff* (DMT). It is also proved in [17] that $d^*(r)$ can be achieved by using i.i.d. length-n_t complex Gaussian random vectors, provided that the asymmetric MIMO Rayleigh fading channel is quasi-static and the channel matrix H remains fixed for $T \geq n_t + n_r - 1$ channel uses.

[1]Throughout paper, all the vectors are column vectors.

Invigorated by this remarkable results, a considerable amount of research activities has been devoted to constructing coding schemes [10]–[12], [15], [18] to achieve the optimal tradeoff $d^*(r)$ in (6). In particular, Elia *et al.* [11] have provided a sufficient condition for having deterministic DMT optimal codes. Furthermore, for any n_t, using a cyclic division algebra (CDA) with degree n_t^2 over its center $\mathbb{Q}(\imath)$, where $\imath = \sqrt{-1}$, an algebraic construction of $(n_t \times n_t)$ matrix codes meeting this sufficient condition is proposed in [11] for all $T \geq n_t$.

While all the aforementioned coding schemes, including the Gaussian random codes and the CDA-based codes, are DMT optimal, it should be noted that all the n_t transmit antennas must be active during each channel use. Specifically, we mean that the signals sent by each transmit antenna during each channel use are non-zero with probability one. Such requirement would lead to some unavoidable difficulty in decoding. To see this, note that the channel matrix H is of size $(n_r \times n_t)$ with $n_t > n_r$. Therefore H has no left multiplicative matrix inverse, and it is impossible to use zero-forcing (ZF) decoder to decode the code. Similarly, the same requirement again forbids the possibility of using sphere decoder which relies on the QR decomposition of the matrix H, and H has linearly dependent column vectors. In particular, in Appendix IV we will give a brief discussion of the obstacle of using sphere decoding to decode the conventional CDA-based codes.

For the minimum-mean square error (MMSE) detector, due to the number of observations, n_r, in each channel use, is strictly less than the number of unknowns, which is n_t in this case, the performance of MMSE decoding technique cannot be good in general.

In order to use ZF decoder, sphere decoder, or MMSE decoder to reduce the decoding complexity, the number of active transmit antennas in each channel use must not exceed n_r. With this additional constraint, the resulting system is termed *constrained asymmetric MIMO system* in this paper, and coding schemes satisfying this additional requirement are coined *constrained asymmetric space-time codes*. Similarly, codes without this constraint will be termed *unconstrained codes*.

In [16], Hollanti and Ranto considered the special case of 4 transmit and 2 receive antennas, i.e., $n_t = 4$ and $n_r = 2$, and proposed a block-diagonal coding method for constructing the constrained asymmetric space-time codes. The construction first partitions the 4 transmit antennas into two groups, say $\{T_1, T_2\}$ and $\{T_3, T_4\}$, and then performs a joint-encoding between these two groups by making use of the multi-block space-time codes [19]. Specifically, let $\mathcal{X}$ be a (2×4) multi-block space-time code where the coding is applied over 2 consecutive (2×2) independent fading blocks, and let H_1 (resp. H_2) denote the (2×2) channel matrix corresponding to the transmit $\{T_1, T_2\}$ (resp. $\{T_3, T_4\}$) and the receive antennas. Given the transmitted code matrix $X = [X_1\, X_2] \in \mathcal{X}$, where each submatrix X_i is of size (2×2), the resulting receive signal matrix is

$$Y_i \;=\; H_i X_i + W_i, \qquad i = 1, 2, \tag{7}$$

where W_i is the (2×2) noise matrix. Clearly the original (2×4) channel matrix equals $H = [H_1\, H_2]$. Given the desired multiplexing gain r, it can be easily shown by using results in [19] that the resulting diversity gain $d(r)$ achieved by $\mathcal{X}$ is given by a piecewise-linear function connecting the points $(k, 2\,(2-k)\,(2-k))$, for $k = 0, 1, 2$. From Fig. 1 it can be seen that the DMT performance achieved by $\mathcal{X}$ is far from being optimal compared to $d^*(r)$ in (6) .

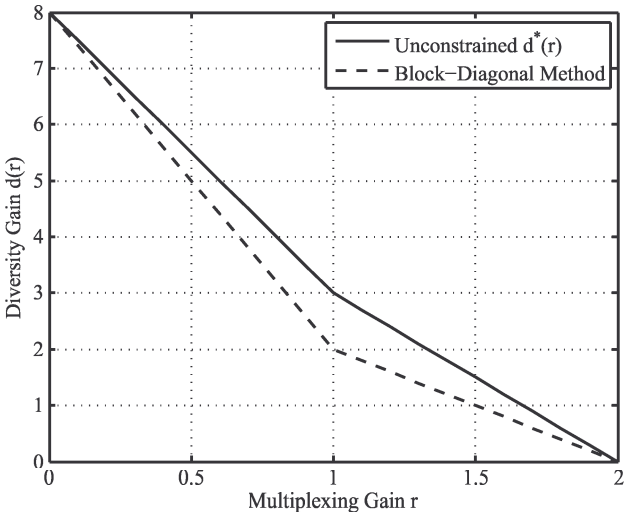


Fig. 1. The DMT performances of unconstrained coding schemes and codes derived from block-diagonal constructions [16].

In this paper, we will investigate the optimal DMT of the constrained asymmetric MIMO systems, and in particular, we will focus on the following two cases:

1) $n_t > n_r = 2$: it corresponds to the case when there are two receive antennas and when the number of transmit antennas is strictly larger than two, and
2) $n_t = n_r + 1$: it is the case when the number of transmit antennas is one larger than the number of receive antennas.

The two cases above have covered almost all the practical MIMO downlink scenarios. Specifically, it includes the (3×2), (4×2), and (4×3) asymmetric MIMO channels as special cases which can be widely found in the existing MIMO-based wireless communication standards [20]–[23].

As for the case of $n_t > n_r = 1$, here we remark that by regarding the $(n_t \times 1)$ asymmetric MIMO channel as an SISO channel with n_t independent fading blocks, it can be easily shown that the optimal DMT of this $(n_t \times 1)$ constrained asymmetric channel equals $d^*(r) = n_t(1-r)$, for $0 \leq r \leq 1$, which is exactly the same as that of the unconstrained channel. In other words, the transmission scheme we are proposing here is to allow only one transmit antenna to be active in each channel use, hence the $(n_t \times 1)$ asymmetric channel is equivalent to the n_t consecutive (1×1) SISO channels, each having a different fading coefficient. Furthermore, the optimal diversity gain $d^*(r)$ can be achieved by using the multi-block space-time codes [24] for SISO channel when coding is applied over n_t consecutive channel uses.

This paper is organized as follows. In Section II, we will present DMT optimal transmission schemes for any constrained asymmetric MIMO systems with $n_t > n_r = 2$ and with $n_t = n_r + 1$, and show that the resulting DMT equals $d^*(r)$ in (6), respectively. It means that if the codes are properly designed, there will be no performance loss with the additional constraint on the number of active transmit antennas used in each channel use. In a nutshell, our proposed DMT optimal transmission schemes are selection patterns of active transmit antennas in each channel use, and given the number of transmit and receive antennas, our schemes only use n_r antennas for transmission at every channel use. Hence, all the aforementioned decoding schemes, such as ZF, sphere-decoding, or MMSE, can be safely and easily applied at the receiver end. For the ease of presentation, detailed proofs to the DMT optimality of the proposed transmission schemes will be relegated to appendices. Having obtained the optimal transmission schemes, the corresponding DMT optimal coding schemes, termed *transmit antenna selection* (TAS) codes, that follow the proposed optimal selection pattern will be given in Section III. Furthermore, it will be shown that the TAS codes are much stronger than what is required in the constrained asymmetric MIMO coding, in the sense that they will be shown to satisfy the *approximately universal* property. What this means is that for any given selection pattern of the transmit antennas, the TAS codes are guaranteed to achieve the optimal DMT performance associated with that selection pattern, regardless of the underlying fading statistics and of whether such pattern is optimal or not.

II. Proposed DMT Optimal Transmission Scheme for Constrained Asymmetric MIMO Systems

In the previous section, we have shown that in order to employ ZF, sphere, or MMSE decoding techniques for decoding the transmitted signal matrix in an asymmetric MIMO channel, the number of active transmit antennas in each channel use cannot exceed the number of receive antennas n_r. In this section, we will focus on two cases: 1) when $n_t > n_r = 2$, and 2) when $n_t = n_r + 1$. For both cases, we will present DMT optimal transmission schemes that can achieve the same optimal DMT $d^*(r)$ of the unconstrained asymmetric channels. To describe the proposed transmission scheme, we first define the following.

Definition 1: In an $(n_t \times n_r)$ constrained asymmetric MIMO channel, let $\mathcal{T} = \{T_1, \cdots, T_{n_t}\}$ be the set of indices of n_t transmit antennas. We say

$$\mathcal{S} := \{(\mathcal{T}_1, n_1), \cdots, (\mathcal{T}_s, n_s)\} \tag{8}$$

is an *antenna-selection transmission scheme* if the antenna selection patterns $\mathcal{T}_i$ are distinct proper subsets of $\mathcal{T}$ and have size $1 \leq |\mathcal{T}_i| \leq n_r < n_t$ for each i. Moreover, each antenna selection pattern $\mathcal{T}_i$ will be used for n_i transmissions and it is assumed that the MIMO channel remains fixed for T channel uses with

$$T \geq \sum_{i=1}^{s} n_i. \tag{9}$$

Example 1: For example, the block-diagonal coding method proposed in [16] for the (4×2) constrained asymmetric MIMO channel can be regarded as an antenna-selection transmission scheme with

$$\mathcal{S}_{BD} = \{(\{T_1, T_2\}, 2), (\{T_3, T_4\}, 2)\}. \tag{10}$$

However, we have already seen in Section I that the above scheme $\mathcal{S}_{BD}$ is not DMT optimal in the (4×2) constrained asymmetric MIMO channel. On the other hand, for any antenna-selection transmission scheme $\mathcal{S} = \{(\mathcal{T}_1, n_1), \cdots, (\mathcal{T}_s, n_s)\}$ with $|\mathcal{T}_i| = n_r$, it is clear that the ergodic channel capacity achieved by $\mathcal{S}$ is the same as that achieved by the unconstrained schemes. To see this, let H_i denote the channel matrix associated with the selection pattern $\mathcal{T}_i$ and the set of all receive antennas, and let $\underline{x}_{ij}$, $1 \leq i \leq s$ and $1 \leq j \leq n_i$ be i.i.d. zero-mean complex Gaussian random vectors having the same covariance matrix $K = \frac{\text{SNR}}{n_r} I_{n_r}$. Then following the same approach as in [1] the ergodic channel capacity achieved by $\mathcal{S}$ using random code $\underline{x}_{ij}$ as transmitted signal vectors is

$$\begin{aligned} & \mathcal{C}(\text{SNR}) \\ = & \frac{1}{\sum_{i=1}^{s} n_i} \sum_{i=1}^{s} \mathbb{E}\left[n_i \log_2 \det\left(I_{n_r} + H_i K H_i^\dagger\right)\right] \\ = & \mathbb{E} \log_2 \det\left(I_{n_r} + \frac{\text{SNR}}{n_r} H_1 H_1^\dagger\right) \\ \approx & n_r \log_2 \text{SNR} \end{aligned} \tag{11}$$

at high SNR regime, and is the same as that achieved by the unconstrained schemes.

A. Proposed Optimal Transmission Scheme for $n_t > n_r = 2$

Earlier we have seen that the block-diagonal method has no loss in channel capacity, but it is not optimal in terms of DMT. To improve the DMT performance, for any $n_t > n_r = 2$ below we provide another transmission scheme and we will prove that it can achieve the optimal DMT $d^*(r)$ given in (6).

Clearly, in this case, the maximal value of multiplexing gain r is upper bounded by $\min\{n_t, n_r\} = 2$, hence $0 \leq r \leq 2$. The proposed scheme is the following.

Theorem 1: In an $(n_t \times 2)$ constrained asymmetric MIMO system with $n_t > 2$, let $\mathcal{T} = \{T_1, \cdots, T_{n_t}\}$ be the set of indices of n_t transmit antennas. Given the desired multiplexing gain r,

1) if the multiplexing gain r falls within the range of $[1, 2]$, the following antenna-selection scheme

$$\begin{aligned} \mathcal{S}_1 = & \{(\{T_1, T_2\}, 2), (\{T_2, T_3\}, 2), \cdots, \\ & (\{T_{n_t-1}, T_{n_t}\}, 2)\} \end{aligned} \tag{12}$$

achieves the optimal DMT $d^*(r)$ of (6), and

2) if $r \in [0, 1)$,

$$\begin{aligned} \mathcal{S}_2 = & \{(\{T_1, T_2\}, 4), (\{T_2, T_3\}, 2), \cdots, \\ & (\{T_{n_t-2}, T_{n_t-1}\}, 2), (\{T_{n_t-1}, T_{n_t}\}, 4)\} \end{aligned} \tag{13}$$

is DMT optimal in terms of $d^*(r)$.

First of all, the only difference between the selection patterns $\mathcal{S}_1$ and $\mathcal{S}_2$ is that when $0 \leq r < 1$, the sets $\{T_1, T_2\}$ and $\{T_{n_t-1}, T_{n_t}\}$ are used twice more than the other sets. Secondly, for the case of (4×2) constrained asymmetric MIMO channel, the scheme in Theorem 1 is given by

$$\mathcal{S}_1 = \{(\{T_1, T_2\}, 2), (\{T_2, T_3\}, 2), (\{T_3, T_4\}, 2)\}$$

for multiplexing gain $r \in [1, 2]$ and

$$\mathcal{S}_2 = \{(\{T_1, T_2\}, 4), (\{T_2, T_3\}, 2), (\{T_3, T_4\}, 4)\}$$

for $r \in [0, 1)$. Comparing to the block-diagonal method $\mathcal{S}_{BD}$, the proposed scheme requires two more transmissions for $r \geq 1$ and six more for $r < 1$. However, the price of using more transmissions is well paid off by having a much better error performance and achieving the same DMT performance as the unconstrained systems.

The proof of Theorem 1 involves the outage performance analysis of the proposed transmission scheme and is relegated to Appendix I for the ease of reading. In particular, we will prove in Appendix I that the diversity gains achieved by the proposed scheme are given by

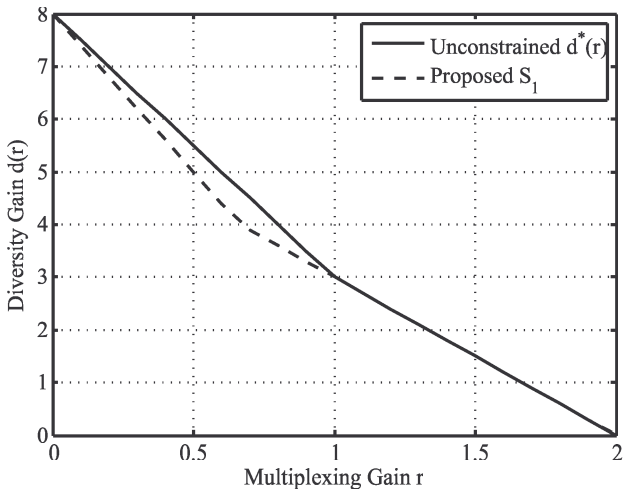
1) for the scheme $\mathcal{S}_1$, we have

$$\begin{aligned} d(r) &\geq (n_t - 1)(2 - r) \quad \text{and} \\ d(r) &\geq 2n_t - 2(n_t - 1)r. \end{aligned} \tag{14}$$

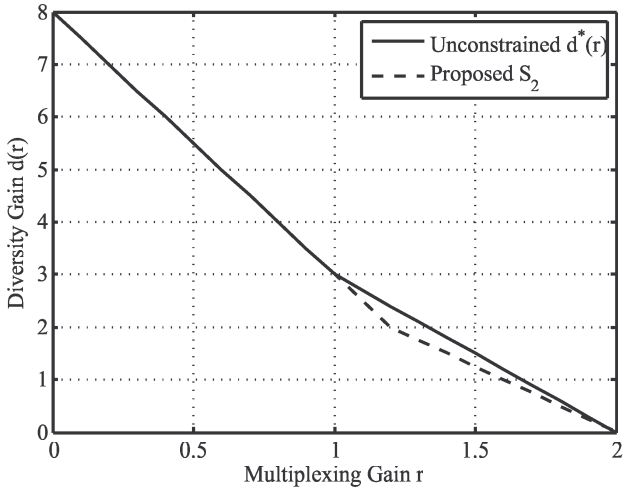
2) for the scheme $\mathcal{S}_2$, we have

$$\begin{aligned} d(r) &\geq 2n_t - (n_t + 1)r \quad \text{and} \\ 2d(r) &\geq (n_t + 1)(2 - r). \end{aligned} \tag{15}$$

Based on (14) and (15), in Fig. 2 we have provided the exact DMT performances of the transmission schemes $\mathcal{S}_1$ and $\mathcal{S}_2$ proposed in Theorem 1 for the (4×2) constrained asymmetric MIMO system. It can be easily seen that the schemes are DMT optimal and achieve the optimal DMT $d^*(r)$ of (6) within the designated regions.



(a)



(b)

Fig. 2. DMT performances of (a) the proposed scheme $\mathcal{S}_1$ and (b) the proposed scheme $\mathcal{S}_2$ for the (4×2) constrained asymmetric MIMO system.

B. Proposed Optimal Transmissions Schemes for $n_t = n_r + 1$.

Given n_t and n_r, the numbers of transmit and receive antennas with $n_t = n_r + 1$, the transmitter is constrained to use at most n_r antennas to transmit signals in each channel use. Let $\{T_1, T_2, \cdots, T_{n_r}, T_{n_r+1}\}$ be the set of transmit antennas. The proposed transmission scheme is a two-phase transmission. In the first phase, the transmitter uses the set $\mathcal{T}_1 = \{T_1, \cdots, T_{n_r-1}, T_{n_r}\}$ of transmit antennas for the first transmission. For the second transmission, the transmitter changes the selection to the set $\mathcal{T}_2 = \{T_1, \cdots, T_{n_r-1}, T_{n_r+1}\}$. This transmission scheme can be applied to signal transmission in, for example the (3×2), (4×3), or (5×4) constrained asymmetric MIMO communication systems. It should be noted that here we have assumed that the transmitter has no access to the channel state information. However, even having no channel state information at the transmitter side, the above scheme turns out to be DMT optimal, and achieves the same DMT performance as the unconstrained ones. We have the following theorem.

Theorem 2: In an $(n_t \times n_r)$ constrained asymmetric MIMO system with $n_t = n_r + 1$, let $\{T_1, \cdots, T_{n_r}, T_{n_r+1}\}$ be the set of indices of n_t transmit antennas. Given the desired multiplexing gain r, the following transmission scheme

$$\begin{aligned} \mathcal{P} := \Big\{ &(\mathcal{T}_1 = \{T_1, \cdots, T_{n_r-1}, T_{n_r}\}, n_r), \\ &(\mathcal{T}_2 = \{T_1, \cdots, T_{n_r-1}, T_{n_r+1}\}, n_r) \Big\} \end{aligned} \tag{16}$$

achieves the optimal DMT $d^*(r)$ of (6).

Proof: The proof is relegated to Appendix II for the ease of reading. ■

Comparing to the conventional CDA-based unconstrained space-time codes [11] where only n_t channel uses are required to complete the transmission of codeword matrices, the transmission scheme proposed in Theorem 2 has asked for $2n_r$ channel uses, i.e., it is $(n_t - 2)$ more than the CDA-based codes. Below we provide an example to further illustrate the

scheme proposed in Theorem 2

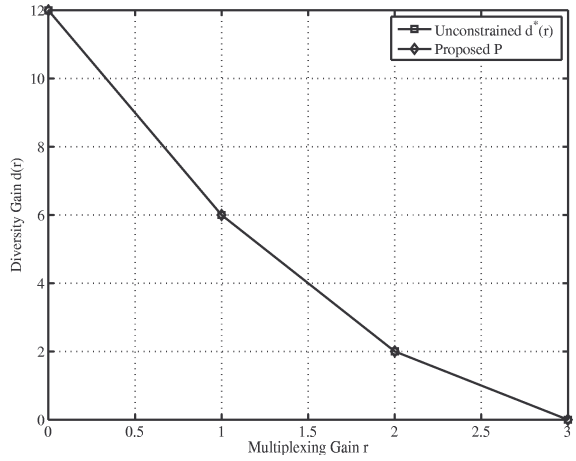


Fig. 3. DMT performances of unconstrained and the constrained transmission scheme $\mathcal{P}$ for (4×3) asymmetric MIMO system.

Example 2: Consider a (4×3) asymmetrical MIMO communication system consisting of 4 transmit and 3 receive antennas. In [11], the authors have proposed to use a cyclic division algebra of degree 16 over its center $\mathbb{Q}(\imath)$ to construct a space-time code consisting of (4×4) code matrices. However, as the received signal matrices are of size (3×4), it is not possible to decode the code using low complexity techniques such as ZF, sphere, or MMSE, and one might have to resort to exhaustive search for maximal likelihood decoding.

On the other hand, in constrained asymmetric MIMO transmission, at most $n_r = 3$ receive antennas can be active for transmission in each channel use. In particular, let $\{T_1, T_2, T_3, T_4\}$ be the set of indices of the transmit antennas. Then Theorem 2 has shown that it is possible to have a space-time code consisting of (3×6) matrices that can achieve the same DMT performance as the unconstrained ones, provided that, say, the left-half of the (3×6) matrix is sent by using transmit antennas $\mathcal{T}_1 = \{T_1, T_2, T_3\}$ and the right-half by $\mathcal{T}_2 = \{T_1, T_2, T_4\}$. In Fig. 3 we have provided the DMTs of the unconstrained and the constrained system, and it is clear that both have the same DMT.

Finally, here we remark that the ordering of the antennas in set $\mathcal{T}_i$, and at which 3 out of 6 channel uses are used by set $\mathcal{T}_1$, do not affect the DMT performance. Similarly, any rearrangement of the indices $\{T_1, T_2, T_3, T_4\}$ would still result in the same DMT.

III. DMT Optimal Codes for Constrained Asymmetric MIMO Systems

In Section II, we have identified two DMT optimal transmission schemes for the constrained asymmetric MIMO systems, one aimed at the case of $n_t > n_r = 2$ and the other at the case of $n_t = n_r + 1$. In particular, these schemes use only n_r out of n_t transmit antennas during each transmission, and therefore enable the use of simple decoding methods, such as ZF, sphere decoding, and MMSE decoders. To achieve the promised optimal DMT performance, in this section we will provide a systematic construction of codes that is able to achieve this optimal DMT performance at high SNR regime. Furthermore, the proposed construction can be applied to any constrained MIMO channel with arbitrary selection patterns, and it will be shown that the constrained codes obtained from the proposed construction are in fact *approximately universal* [18], meaning that these codes are able to achieve the optimal DMT performance associated with the designated selection pattern.

A. Extended Set of Transmit Antenna Selection

Since the construction can be applied to all kinds of constrained MIMO channels, below we begin with the consideration of a general selection pattern. In an $(n_t \times n_r)$ constrained asymmetric MIMO channel, let $\mathcal{T} = \{T_1, \cdots, T_{n_t}\}$ be the set of indices of n_t transmit antennas, and let

$$\mathcal{S} \ := \ \{(\mathcal{T}_1, n_1), \cdots, (\mathcal{T}_s, n_s)\} \tag{17}$$

be an antenna-selection transmission scheme with

$$\mathcal{T}_1, \ \cdots, \mathcal{T}_s \ \subset \ \mathcal{T}, \tag{18}$$

$$n := |\mathcal{T}_1| \ = \ \cdots \ = \ |\mathcal{T}_s| \leq n_r. \tag{19}$$

The $\mathcal{T}_i$'s represent the subsets of transmit antennas $\mathcal{T}$ that are active during transmission, and the number n_i means the number of times that the subset $\mathcal{T}_i$ is used.

Given the selection pattern $\mathcal{S}$ in (17), we first define another extended pattern, denoted by $\mathcal{S}_{\text{ext}}$, as follows:

$$\mathcal{S}_{\text{ext}} \ := \ \{(\mathcal{T}_1, \ell n_1), \cdots, (\mathcal{T}_s, \ell n_s)\} \tag{20}$$

where ℓ is the smallest positive integer such that the numbers ℓn_i are divisible by $n = |\mathcal{T}_1|$. It should be noted that in (19) we have required that all the subsets $\mathcal{T}_i$ are of the same size.

Furthermore, we remark that in a quasi-static MIMO fading channel with a quasi-static interval T satisfying

$$T \ \geq \ \ell \sum_{i=1}^{s} n_i, \tag{21}$$

it is straightforward to see that the scheme $\mathcal{S}_{\text{ext}}$ has the same outage performance[2] as $\mathcal{S}$. Thus, assuming (21) holds, below we will work with the selection pattern $\mathcal{S}_{\text{ext}}$ instead of $\mathcal{S}$.

B. Proposed Construction for Selection $\mathcal{S}_{ext}$

Given $\mathcal{S}_{\text{ext}}$ we first define the parameter m

$$m \ := \ \frac{\ell}{n} \sum_{i=1}^{s} n_i, \tag{22}$$

which must be an integer due to the condition of ℓ given in (20), where n is given in (19). Next, the proposed construction calls for the use of multi-block space-time codes [24] that are originally designed to encode information across multiple

[2]In fact, with a stronger condition on n_i of $n_i \geq n$ for all i, using results in [11] it can be shown that both schemes $\mathcal{S}_{\text{ext}}$ and $\mathcal{S}$ have not only the same outage performance, but also the same DMT performance.

independent fading blocks, and it turns out such construction can be modified to cater to the present scenario.

Specifically, let $\mathbb{E}$ be a number field that is a cyclic Galois extension of the number field $\mathbb{F} = \mathbb{Q}(\imath)$ of degree mn with Galois group $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = \langle\sigma\rangle$ generated by σ, where $\imath := \sqrt{-1}$. By $\langle\ \varphi\rangle$ we mean the cyclic group generated by φ, i.e., $\langle\varphi\rangle = \{id, \varphi, \varphi^2, \cdots\}$, where id is the identity element. Also, for any possible mn, the construction of such number field $\mathbb{E}$ can be found in [11], [25].

Next, let $\mathbb{L}$ be the intermediate number field that is fixed by the Galois group $\langle\tau = \sigma^m\rangle$, i.e., we have $\mathrm{Gal}(\mathbb{E}/\mathbb{L}) = \langle\tau\rangle$. Let z be an indeterminate satisfying

1) $xz \ = \ z\tau(x)$ for every $x \in \mathbb{E}$, and
2) $z^n = \gamma \in \mathbb{L}^*$, for some non-norm element γ, by which we mean the smallest positive integer e such that γ^e is the relative norm $N_{\mathbb{E}/\mathbb{L}}(x)$ for some element $x \in \mathbb{E}^*$ is n.

Thus, with proper choice of $\gamma \in \mathbb{L}^*$, the set

$$\mathfrak{D} \ := \ \left\{ \sum_{i=0}^{n-1} z^i x_i \ : \ x_i \in \mathbb{E} \right\} \tag{23}$$

is a cyclic division algebra (CDA) with center $\mathbb{L}$. The algebra $\mathfrak{D}$ defined as above is often shortly referred to as $\mathfrak{D} = (\mathbb{E}/\mathbb{L}, \tau, \gamma)$.

Let $\psi : \mathfrak{D} \to \mathbb{E}^{n\times n}$ be the map of left-regular representation of elements in $\mathfrak{D}$ [11]

$$\psi(x) \ = \ \begin{bmatrix} x_0 & \gamma\tau(x_{n-1}) & \cdots & \gamma\tau^{n-1}(x_1) \\ x_1 & \tau(x_0) & \cdots & \gamma\tau^{n-1}(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & \tau(x_{n-2}) & \cdots & \tau^{n-1}(x_0) \end{bmatrix}, \tag{24}$$

where

$$x \ = \ \sum_{i=0}^{n-1} z^i x_i \in \mathfrak{D}, \quad x_i \in \mathbb{E}^*. \tag{25}$$

Thus, similar to the multi-block construction of [24] we have the following code

$$\begin{aligned} \mathcal{X}_g \ := \Bigg\{ & \big(X, \sigma(X), \cdots, \sigma^{m-1}(X)\big) : X = \psi(x), \\ & x \ = \ \sum_{i=0}^{n-1} z^i x_i \in \mathfrak{D}, \quad x_i = \sum_{j=0}^{nm-1} a_{i,j} e_j, \\ & a_{i,j} \in \mathcal{A}_g \subset \mathbb{Z}[\imath] \Bigg\}, \end{aligned} \tag{26}$$

where $\{e_0, \cdots, e_{nm-1}\}$ is an integral basis for $\mathbb{E}/\mathbb{F}$, $\mathcal{A}_g$ is a QAM base-alphabet of size

$$|\mathcal{A}_g| \ \doteq \ \mathrm{SNR}^{\frac{r}{n}}, \tag{27}$$

and where r is the desired multiplexing gain given in (3).

It should be noted that for each $\big(X, \sigma(X), \cdots, \sigma^{m-1}(X)\big) \in \mathcal{X}_g$ the code matrix X is of size $(n \times n)$ with $n \le n_r$ and furthermore that the code $\mathcal{X}_g$ satisfies the property of *generalized non-vanishing determinant* [24], meaning that for every $(X, \sigma(X), \cdots, \sigma^{m-1}(X)) \ne (X', \sigma(X'), \cdots, \sigma^{m-1}(X')) \in \mathcal{X}_g$ we have

$$\prod_{i=0}^{m-1} \left|\det\left(\sigma^i(X) - \sigma^i(X')\right)\right| \ \ge 1. \tag{28}$$

To apply the code $\mathcal{X}_g$ to the designated selection pattern $\mathcal{S}_{\text{ext}}$, we first recall that

$$\mathcal{S}_{\text{ext}} \ := \ \{(\mathcal{T}_1, \ell n_1), \cdots, (\mathcal{T}_s, \ell n_s)\}$$

in which each ℓn_i is a multiple of $n = |\mathcal{T}_i|$ by construction. Define

$$m_i \ := \ \frac{\ell n_i}{n}, \quad i = 1, \cdots, s, \tag{29}$$

and it is clear that

$$\sum_{i=1}^{s} m_i \ = \ m \tag{30}$$

where m is defined in (22). Next, let $\mathcal{M}_1, \cdots, \mathcal{M}_s$ be a partition of the set $\{0, 1, \cdots, m-1\}$ with

$$|\mathcal{M}_i| \ = \ m_i. \tag{31}$$

Finally, the proposed code is the following. Given code matrices $\big(X, \sigma(X), \cdots, \sigma^{m-1}(X)\big) \in \mathcal{X}_g$, the set of code matrices

$$\left\{\theta\sigma^j\left(X\right) \ : \ j \in \mathcal{M}_i\right\} \tag{32}$$

will be transmitted by the set of antennas $\mathcal{T}_i$ for each $i = 1, \cdots, s$, where the parameter θ is given by

$$\theta \ := \ \mathrm{SNR}^{\frac{1}{2}\left(1-\frac{r}{n}\right)}. \tag{33}$$

The reason for having θ is because for every $a_{i,j} \in \mathcal{A}_g \subset \mathbb{Z}[\imath]$ we have

$$|a_{i,j}|^2 \ \dot{\le} \mathrm{SNR}^{\frac{r}{n}}. \tag{34}$$

Hence it in turn implies that

$$|x_i|^2 \ = \ \left|\sum_{j=0}^{nm-1} a_{i,j} e_j\right|^2 \ \dot{\le} \ \mathrm{SNR}^{\frac{r}{n}}$$

since the basis elements do not change as SNR increases. Thus for every $(X, \cdots, \sigma^{m-1}(X)) \in \mathcal{X}_g$ we have

$$\left|\sigma^j(X)\right|_F^2 \ \dot{\le} \ \mathrm{SNR}^{\frac{r}{n}}, \tag{35}$$

where by $|A|_F$ we mean the Frobenius norm of the matrix A. To ensure the power constraint (2) we need to add and set parameter θ as in (33) so that

$$\left|\theta\sigma^j(X)\right|_F^2 \ \dot{\le} \ \mathrm{SNR}. \tag{36}$$

Clearly, the transmission of each code matrix $\sigma^j(X)$ takes n channel uses, hence the set of transmit antennas $\mathcal{T}_i$ will be used exactly

$$n \cdot |\mathcal{M}_i| = nm_i = \ell n_i \tag{37}$$

times. In other words, in the proposed scheme, to complete the transmission of the codeword $\big(X, \sigma(X), \cdots, \sigma^{m-1}(X)\big) \in \mathcal{X}_g$, each selection pattern $\mathcal{T}_i$ will be used exactly ℓn_i times and therefore the proposed scheme satisfies the requirement specified by the antenna selection pattern $\mathcal{S}_{\text{ext}}$.

We now use the following example to illustrate the proposed coding and transmission scheme.

Example 3: Consider the following antenna selection pattern for the (4×2) constrained asymmetric MIMO channel

$$\mathcal{S}_2 \;=\; \{(\{T_1,T_2\},4),(\{T_2,T_3\},2),(\{T_3,T_4\},4)\}.$$

Such pattern was shown to be DMT optimal when the multiplexing gain r falls in the range of $[0,1)$ in Theorem 1. To apply the proposed coding scheme to this selection pattern we have

$$\begin{aligned} n &= |\{T_1,T_2\}| = \cdots = |\{T_3,T_4\}| = 2 = n_r, \\ n_1 &= 4,\ n_2 = 2, \quad \text{and } n_3 = 4. \end{aligned}$$

Since all n_1, n_2, n_3 are divisible by $n = 2$, we have $\ell = 1$, hence $\mathcal{S}_{2,\text{ext}} = \mathcal{S}_2$. Next, the parameter m should be set as

$$m \;=\; \frac{\ell}{n}\sum_{i=1}^{3} n_i \;=\; 5. \tag{38}$$

Now let $\mathbb{E}$ be a cyclic Galois extension of $\mathbb{F} = \mathbb{Q}(\imath)$ with degree of extension equal to $nm = 10$. This can be easily done by choosing

$$\mathbb{E} \;=\; \mathbb{Q}(\imath, \zeta_{11}),$$

where ζ_{11} is the complex, primitive, 11th root of unity. Let σ be the generator of the cyclic Galois group $\text{Gal}(\mathbb{E}/\mathbb{F})$, $\sigma(\zeta_{11}) = \zeta_{11}^2$, and let $\mathbb{L}$ be the intermediate field fixed by $\tau = \sigma^m = \sigma^5$. Now let $\mathcal{X}_g$ be the code resulting from the CDA $\mathfrak{D} = (\mathbb{E}/\mathbb{L}, \tau, \gamma = \imath)$ and be given by

$$\begin{aligned} \mathcal{X}_g \;:=\Bigg\{ & \big(X, \sigma(X), \cdots, \sigma^4(X)\big) : X = \psi(x), \\ & x \;=\; \sum_{i=0}^{1} z^i x_i \in \mathfrak{D}, \quad x_i = \sum_{j=0}^{9} a_{i,j}\zeta_{11}^j, \\ & a_{i,j} \in \mathcal{A}_g \subset \mathbb{Z}[\imath] \Bigg\}, \end{aligned} \tag{39}$$

where $\{1, \zeta_{11}, \cdots, \zeta_{11}^9\}$ is an integral basis for $\mathbb{E}/\mathbb{F}$, $\mathcal{A}_g$ is a QAM base-alphabet of size

$$|\mathcal{A}_g| \;\doteq\; \text{SNR}^{\frac{r}{2}}. \tag{40}$$

It should be noted that the matrices $\sigma^i(X)$, $i = 0,1,2,3,4$, are all of size (2×2).

The parameters m_i are set according to (29) and are therefore given by

$$m_1 = 2,\ m_2 = 1,\ m_3 = 2.$$

Similarly, the sets $\mathcal{M}_i$ can be set for example as

$$\mathcal{M}_1 = \{0,4\},\ \mathcal{M}_2 = \{2\}, \quad \text{and } \mathcal{M}_3 = \{1,3\}, \tag{41}$$

which are a partition of the set $\{0,1,2,3,4\}$. This means that the code matrices $\{\theta X, \theta\sigma^4(X)\}$ will be transmitted by antennas $\mathcal{T}_1 = \{T_1, T_2\}$, $\{\theta\sigma^2(X)\}$ by antennas $\mathcal{T}_2 = \{T_2, T_3\}$, and $\{\theta\sigma^1(X), \theta\sigma^3(X)\}$ by antennas $\mathcal{T}_3 = \{T_3, T_4\}$. According to (33) of the proposed construction, given the multiplexing gain r, the parameter θ should be set at

$$\theta \;=\; \text{SNR}^{\frac{1}{2}\left(1-\frac{r}{2}\right)}. \tag{42}$$

In other words, if we let

$$X \;=\; \psi(x) \;=\; \begin{bmatrix} \underline{x}_1^t \\ \underline{x}_2^t \end{bmatrix},$$

where $\underline{x}_i$, $i = 1,2$, are column vectors of length 2, the overall transmitted code matrix is actually the following

$$\theta \begin{bmatrix} \underline{x}_1^t & & & & \sigma^4(\underline{x}_1^t) \\ \underline{x}_2^t & & \sigma^2(\underline{x}_1^t) & & \sigma^4(\underline{x}_2^t) \\ & \sigma(\underline{x}_1^t) & \sigma^2(\underline{x}_2^t) & \sigma^3(\underline{x}_1^t) & \\ & \sigma(\underline{x}_2^t) & & \sigma^3(\underline{x}_2^t) & \end{bmatrix}, \tag{43}$$

where the ith row is transmitted by the transmit antenna T_i, and where the columns correspond to each channel use. Clearly there are 10 channel uses, and transmit antennas $\mathcal{T}_1 = \{T_1, T_2\}$ are used 4 times, $\mathcal{T}_2 = \{T_2, T_3\}$ are used 2 times, and $\mathcal{T}_3 = \{T_3, T_4\}$ are used 4 times. Thus, we have fulfilled exactly the designated antenna selection pattern $\mathcal{S}_2$. To conclude this example, we remark that in the actual code matrix given in (43) there are exactly $n_r = 2$ active transmit antennas in each channel use. Hence, this code can be easily decoded by making use of ZF, sphere, or MMSE decoding techniques.

Example 4: Consider now the following antenna selection pattern for the (4×2) constrained asymmetric MIMO channel

$$\mathcal{S}_1 \;=\; \{(\{T_1,T_2\},2),(\{T_2,T_3\},2),(\{T_3,T_4\},2)\}.$$

Such pattern was shown to be DMT optimal when the multiplexing gain r falls in the range of $[1,2]$ in Theorem 1. To apply the proposed coding scheme to this selection pattern we have

$$\begin{aligned} n &= |\{T_1,T_2\}| = \cdots = |\{T_3,T_4\}| = 2 = n_r, \\ n_1 &= 2,\ n_2 = 2, \quad \text{and } n_3 = 2. \end{aligned}$$

Since all n_1, n_2, n_3 are divisible by $n = 2$, we have $\ell = 1$, hence $\mathcal{S}_{1,\text{ext}} = \mathcal{S}_1$. Next, the parameter m should be set as

$$m \;=\; \frac{\ell}{n}\sum_{i=1}^{3} n_i \;=\; 3. \tag{44}$$

Now let $\mathbb{E}$ be a cyclic Galois extension of $\mathbb{F} = \mathbb{Q}(\imath)$ with degree of extension equal to $nm = 6$. This can be easily done by choosing

$$\mathbb{E} \;=\; \mathbb{Q}(\imath, \zeta_7),$$

where ζ_7 is the complex, primitive, 7th root of unity. Let σ be the generator of the cyclic Galois group $\text{Gal}(\mathbb{E}/\mathbb{F})$, $\sigma(\zeta_7) = \zeta_7^3$, and let $\mathbb{L}$ be the intermediate field fixed by $\tau = \sigma^m = \sigma^3$. Now let $\mathcal{X}_g$ be the code resulting from the CDA $\mathfrak{D} = (\mathbb{E}/\mathbb{L}, \tau, \gamma = \imath)$ and be given by

$$\begin{aligned} \mathcal{X}_g \;:=\Bigg\{ & \big(X, \sigma(X), \sigma^2(X)\big) : X = \psi(x), \\ & x \;=\; \sum_{i=0}^{1} z^i x_i \in \mathfrak{D}, \quad x_i = \sum_{j=0}^{5} a_{i,j}\zeta_7^j, \end{aligned}$$

$$a_{i,j} \in \mathcal{A}_g \subset \mathbb{Z}[\imath] \Big\}, \tag{45}$$

where $\{1, \zeta_7, \cdots, \zeta_7^5\}$ is an integral basis for $\mathbb{E}/\mathbb{F}$, $\mathcal{A}_g$ is a QAM base-alphabet of size

$$|\mathcal{A}_g| \doteq \text{SNR}^{\frac{r}{2}}. \tag{46}$$

It should be noted that the matrices $\sigma^i(X)$, $i = 0, 1, 2$, are all of size (2×2).

The parameters m_i are set according to (29) and are therefore given by

$$m_1 = 1,\ m_2 = 1,\ m_3 = 1.$$

Similarly, the sets $\mathcal{M}_i$ can be set for example as

$$\mathcal{M}_1 = \{0\},\ \mathcal{M}_2 = \{1\},\ \text{ and } \mathcal{M}_3 = \{2\}, \tag{47}$$

which are a partition of the set $\{0, 1, 2\}$. This means that the code matrix θX will be transmitted by antennas $\mathcal{T}_1 = \{T_1, T_2\}$, $\theta\sigma(X)$ by antennas $\mathcal{T}_2 = \{T_2, T_3\}$, and $\theta\sigma^2(X)$ by antennas $\mathcal{T}_3 = \{T_3, T_4\}$. According to (33) of the proposed construction, given the multiplexing gain r, the parameter θ should be set at

$$\theta \ = \ \text{SNR}^{\frac{1}{2}\left(1-\frac{r}{2}\right)}. \tag{48}$$

In other words, if we let

$$X \ = \ \psi(x) \ = \ \begin{bmatrix} \underline{x}_1^t \\ \underline{x}_2^t \end{bmatrix},$$

where $\underline{x}_i$, $i = 1, 2$, are column vectors of length 2, the overall transmitted code matrix is actually the following

$$\theta \begin{bmatrix} \underline{x}_1^t & & \\ \underline{x}_2^t & \sigma\left(\underline{x}_1^t\right) & \\ & \sigma\left(\underline{x}_2^t\right) & \sigma^2\left(\underline{x}_1^t\right) \\ & & \sigma^2\left(\underline{x}_2^t\right) \end{bmatrix}, \tag{49}$$

where the ith row is transmitted by the transmit antenna T_i, and where the columns correspond to each channel use. Clearly there are 6 channel uses, and all the transmit antenna patterns $\mathcal{T}_1$, $\mathcal{T}_2$, and $\mathcal{T}_3$, are used twice. Thus, we have fulfilled exactly the designated antenna selection pattern $\mathcal{S}_1$. To conclude this example, we remark that in the actual code matrix given in (49) there are exactly $n_r = 2$ active transmit antennas in each channel use. Hence, this code can be easily decoded by making use of ZF, sphere, or MMSE decoding techniques.

In Appendix IV, we have provided a short discussion of how to decode the proposed code using sphere decoders. It will be seen that as the code uses at most n_r active transmit antennas for transmission in each channel use, it can be easily decoded by using low complexity sphere decoding techniques.

C. DMT Performance of the Proposed Code

To analyze the DMT performance achieved by the proposed code, we first focus on the transmission rate. To this end, recall that $\mathcal{A}_g$ is of size $\text{SNR}^{\frac{r}{n}}$ given in (27), and that all $\left(X, \sigma(X), \cdots, \sigma^{m-1}(X)\right) \in \mathcal{X}_g$ are distinct due to the generalized non-vanishing determinant property satisfied by $\mathcal{X}_g$. Thus, we have

$$|\mathcal{X}_g| \ = \ \left(|\mathcal{A}_g|^{nm}\right)^n \ = \ \text{SNR}^{rmn}. \tag{50}$$

On the other hand, the transmission of $(X, \sigma(X), \cdots, \sigma^{m-1}(X))$ takes

$$\sum_{i=1}^{s} \ell n_i \ = \ nm \tag{51}$$

channel uses. Thus, the code $\mathcal{X}_g$ transmits on the average

$$\frac{1}{nm} \log_2 |\mathcal{X}_g| = r \log_2 \text{SNR} \tag{52}$$

bits per channel uses, meaning that it achieves exactly the desired multiplexing gain at value r. Moreover, in the theorem below we will show that the proposed code $\mathcal{X}_g$ indeed achieves the optimal DMT performance associated with the antenna selection pattern $\mathcal{S}_{\text{ext}}$.

Theorem 3: In an $(n_t \times n_r)$ MIMO communication system with antenna selection pattern $\mathcal{S}_{\text{ext}} := \{(\mathcal{T}_1, \ell n_1), \cdots, (\mathcal{T}_s, \ell n_s)\}$, where ℓ is defined as before. Given the desired multiplexing gain r, let $\mathcal{X}_g$ be the corresponding space-time code defined in (26); then by transmitting code matrices in $\mathcal{X}_g$ according to the proposed transmission scheme, the usage of transmit antennas follows exactly the selection pattern $\mathcal{S}_{ext}$. Furthermore, at high SNR regime the codeword error probability of $\mathcal{X}_g$ is upper bounded by

$$P_{\text{cwe},\mathcal{X}_g}(\text{SNR}) \ \dot{\leq} \ P_{\text{out}}(\text{SNR}) \ \doteq \text{SNR}^{-d(r)}, \tag{53}$$

where $P_{\text{out}}(\text{SNR})$ is the outage probability associated with the selection pattern $\mathcal{S}_{\text{ext}}$, and where $d(r)$ is the corresponding diversity gain advantage. In other words, the code $\mathcal{X}_g$ and the proposed transmission scheme are optimal in terms of the DMT of $\mathcal{S}_{\text{ext}}$.

Proof: The proof to the claim of the use of transmit antennas follows from the above discussion, and we only need to prove the claim of codeword error probability (53). For the ease of reading, the proof of this part is relegated to Appendix III. ■

In particular, we can apply the previous theorem to the antenna selection patterns $\mathcal{S}_1$, $\mathcal{S}_2$, and $\mathcal{P}$ given respectively in Theorems 1 and 2. Namely, we have the following corollaries.

Corollary 4: In an $(n_t \times 2)$ constrained asymmetric quasi-static MIMO Rayleigh channel with $n_t > 2$ and with quasi-static interval T, given the desired multiplexing gain r, let $\mathcal{S}$ be the corresponding antenna selection pattern specified by Theorem 1. Let $\mathcal{X}_g$ be the constrained code obtained from the construction in Theorem 3 using the designated pattern $\mathcal{S}$. Then by using the proposed transmission scheme, the resulting codeword error probability $P_{\text{cwe}}(\text{SNR})$ is upper bounded by

$$P_{\text{cwe}}(\text{SNR}) \ \dot{\leq} \text{SNR}^{-d^*(r)},$$

where $d^*(r)$ is the DMT of the unconstrained $(n_t \times 2)$ MIMO channel given by (6), provided that the quasi-static interval

$$T \ \geq \ 2\left(n_t - 1\right)$$

if $r \in [1,2]$, and

$$T \;\geq\; 2\,(n_t+1)$$

if $r \in [0,1)$.

Corollary 5: In an $(n_t \times n_r)$ constrained asymmetric quasi-static MIMO Rayleigh channel with $n_t = n_r + 1$ and with quasi-static interval

$$T \;\geq\; 2(n_t - 1),$$

given the desired multiplexing gain r, let $\mathcal{S}$ be the corresponding antenna selection pattern specified by Theorem 2. Let $\mathcal{X}_g$ be the constrained code obtained from the construction in Theorem 3 using the designated pattern $\mathcal{S}$. Then by using the proposed transmission scheme, the resulting codeword error probability $P_{\text{cwe}}(\text{SNR})$ is upper bounded by

$$P_{\text{cwe}}(\text{SNR}) \;\dot{\leq} \text{SNR}^{-d^*(r)},$$

where $d^*(r)$ is the DMT of the unconstrained $(n_t \times 2)$ MIMO channel given by (6).

IV. Conclusion

When the number of transmit antennas n_t is strictly larger than the number of receive n_r, almost all existing DMT optimal codes require that all the transmit antennas are active during transmission, hence forbid the possibility of having a ZF, sphere, or MMSE decoder. To remedy this, the number of active transmit antennas must be constrained to be less than or equal to n_r. For the cases when $n_t > n_r = 2$ and when $n_t = n_r + 1$, two optimal transmission schemes satisfying the above constraint were presented in this paper and were shown to achieve the same DMT performance as the unconstrained schemes. A systematic construction of DMT optimal constrained codes was also provided.

Appendix I
Proof of Theorem 1

As the scheme $\mathcal{S}_1$ differs from $\mathcal{S}_2$ only in the number of times used for each antenna selection pattern $\mathcal{T}_i$, here we consider the following general scheme:

$$\mathcal{S} \;:=\; \left\{\left(\{T_1,T_2\},n_1\right),\cdots\left(\{T_{n_t-1},T_{n_t}\},n_{n_t-1}\right)\right\}. \quad (54)$$

In the above scheme $\mathcal{S}$, the ith selection $\{T_i, T_{i+1}\}$ will be used for n_i times during transmission. Moreover, for the ith selection, let $\underline{x}_{i_j}$ be the length-n_r, zero-mean, complex Gaussian random code vector with covariance $K_i = \frac{\text{SNR}}{2} I_{n_r}$. The subindex j, $j = 0, 1, \cdots, n_i - 1$, represents the jth use of the selection pattern $\{T_i, T_{i+1}\}$. Thus given $\underline{x}_{i_j}$, the resulting received signal vector is given by

$$\underline{y}_{i_j} \;=\; H_i\,\underline{x}_{i_j} + \underline{w}_{i_j} \quad (55)$$

where $H_i \;:=\; \left[\underline{h}_i \;\underline{h}_{i+1}\right]$ and $\underline{h}_i$ is length-2 vector consisting of the fading coefficients between the ith transmit antenna T_i and the receive antennas. $\underline{w}_{i_j}$ is the zero-mean complex Gaussian random vector of length 2 used to model the effect of additive white Gaussian noise. Thus, given the channel matrix H_i, the mutual information between the transmit and receive signal vectors is

$$\begin{aligned} I\left(\underline{x}_{i_j};\underline{y}_{i_j}|H_i\right) &= \log_2\det\left(I_2 + \frac{\text{SNR}}{2}H_iH_i^\dagger\right) \\ &\approx \log_2\det\left(I_2 + \text{SNR}H_iH_i^\dagger\right), \end{aligned}$$

where we have neglected the 2 appearing in the denominator of $\frac{\text{SNR}}{2}$ as here we are only interested in the high SNR regime for the sake of DMT performance analysis. Define

$$N \;:=\; \sum_{j=1}^{n_t-1} n_j. \quad (56)$$

Given the desired multiplexing gain r, the channel outage probability of $\mathcal{S}$ is

$$\begin{aligned} P_{\text{out}}(r) \;:=\; &\left\{\sum_{i=1}^{n_t-1} n_i \log\det\left(I_2 + \text{SNR}H_iH_i^\dagger\right) \;\leq\right. \\ &\left. Nr\log\text{SNR}\right\} \;\doteq\; \text{SNR}^{-d(r)}. \end{aligned} \quad (57)$$

In particular, the mutual information associated with the selection $\{T_1, T_2\}$ can be rewritten as

$$\begin{aligned} &\log\det\left(I_2 + \text{SNR}H_1H_1^\dagger\right) \\ =\;& \log\det\left(I_2 + \text{SNR}\underline{h}_1\underline{h}_1^\dagger + \text{SNR}\underline{h}_2\underline{h}_2^\dagger\right) \\ =\;& \log\det\left(I_2 + \text{SNR}D_1\right) + \\ & \log\left(1 + \text{SNR}\underline{h}_2^\dagger U_1\left(I_2 + \text{SNR}D_1\right)^{-1}U_1^\dagger\underline{h}_2\right) \\ =\;& \log\left(1 + \text{SNR}\left|\underline{h}_1\right|_F^2\right) + \\ & \log\left(1 + \text{SNR}\underline{g}_2^\dagger\left(I_2 + \text{SNR}D_1\right)^{-1}\underline{g}_2\right), \end{aligned}$$

where $U_1 D_1 U_1^\dagger$ is the eigen-decomposition of the rank-1 matrix $\underline{h}_1\underline{h}_1^\dagger$ and where $\underline{g}_2 \;:=\; U_1^\dagger\underline{h}_2$ has the same joint probability density function as that of $\underline{h}_2$. By $|\underline{h}_1|_F$ we mean the Frobenius norm of vector $\underline{h}_1$. Hence, without affecting the calculation of (57), we can set the channel matrix associated with the second selection pattern $\{T_2, T_3\}$ as

$$H_2' \;=\; \left[\underline{g}_2 \;\; \underline{h}_3\right] \quad (58)$$

and the corresponding mutual information changes to

$$\begin{aligned} I\left(\underline{x}_{2_j};\underline{y}_{2_j}|H_2'\right) \;=\; &\log\left(1 + \text{SNR}\left|\underline{g}_2\right|_F^2\right) + \\ &\log\left(1 + \text{SNR}\underline{g}_3^\dagger\left(I_2 + \text{SNR}D_2\right)^{-1}\underline{g}_3\right) \end{aligned}$$

where $U_2 D_2 U_2^\dagger$ is the eigen-decomposition of the rank-1 matrix $\underline{g}_2\underline{g}_2^\dagger$ and $\underline{g}_3 = U_2^\dagger\underline{h}_3$. Continuing in this fashion, we can rewrite the overall mutual information associated with scheme $\mathcal{S}$ as

$$\begin{aligned} &\sum_{i=1}^{n_t-1} n_i \log\det\left(I_2 + \text{SNR}H_i'H_i'^\dagger\right) \\ =\;& \sum_{i=1}^{n_t-1} n_i\left[\log\left(1 + \text{SNR}\left|\underline{g}_i\right|_F^2\right) + \right. \end{aligned}$$

$$\log\left(1+\frac{\mathrm{SNR}\,|g_{i+1,1}|^2}{1+\mathrm{SNR}\left|\underline{g}_i\right|_F^2}+\mathrm{SNR}\,|g_{i+1,2}|^2\right)\Bigg], \tag{59}$$

where we have set $\underline{g}_1 = \underline{h}_1$, and for $i = 2, \cdots, n_t$, $\underline{g}_i = U_{i-1}^\dagger \underline{h}_i = [g_{i,1} \;\; g_{i,2}]^t$. $U_i D_i U_i^\dagger$ is the eigen-decomposition of $\underline{g}_i \underline{g}_i^\dagger$.

Now define

$$|g_{i,j}|^2 \doteq \mathrm{SNR}^{-\alpha_{i,j}} \tag{60}$$

and at high SNR we can rewrite (59) as

$$\begin{aligned}
&\frac{1}{\log \mathrm{SNR}} \sum_{i=1}^{n_t-1} n_i \log\det\left(I_2+\mathrm{SNR} H_i' H_i'^\dagger\right) \\
&\approx \sum_{i=1}^{n_t-1} n_i \Bigg[\Bigg(\underbrace{\max_j\left\{(1-\alpha_{i,j})^+\right\}}_{:=(1-\beta_i)^+}\Bigg) + \\
&\Bigg(\max\left\{\left(1-\alpha_{i+1,1}-(1-\beta_i)^+\right)^+, \right. \\
&\qquad\qquad \left.(1-\alpha_{i+1,2})^+\right\}\Bigg)\Bigg],
\end{aligned}$$

where

$$(x)^+ := \max\{0, x\}. \tag{61}$$

Thus, the diversity gain achieved by the general scheme $\mathcal{S}$ is

$$d(r) \;=\; \inf_{\mathcal{A}(r)} \sum_{i=1}^{n_t}\sum_{j=1}^{2} \alpha_{i,j}, \tag{62}$$

where

$$\begin{aligned}
\mathcal{A}(r) \;=\; \Bigg\{&(\alpha_{1,1}, \cdots, \alpha_{n_t,2}) \;:\; \sum_{i=1}^{n_t-1} n_i \Bigg[(1-\beta_i)^+ \\
&+\max\Bigg\{\left(1-\alpha_{i+1,1}-(1-\beta_i)^+\right)^+, \\
&(1-\alpha_{i+1,2})^+\Bigg\}\Bigg] \le Nr, \alpha_{i,j} \ge 0\Bigg\}
\end{aligned} \tag{63}$$

While the optimization of $d(r)$ subject to the constraint (63) appears to be a non-linear optimization problem, below we will convert it to a problem of linear programming. First note that for each $\alpha_{i,j}$, the probability of $\alpha_{i,j} < 0$ is zero. Secondly, to minimize the diversity gain $d(r)$, we do not need $\alpha_{i,j}$ to be larger than 1 as $(1-\alpha_{i,j})^+ = 0$ for $\alpha_{i,j} \ge 1$ and setting $\alpha_{i,j} = 1$ minimizes the cost of $d(r)$. Thus, we have the following sets of linear constraints:

$$0 \le \alpha_{i,j} \le 1 \quad \text{for all } i = 1, \cdots, n_t - 1,\ j = 1, 2 \tag{64}$$

Next, for $i = 1, 2, \cdots, n_t - 1$, setting

$$\begin{aligned}
r_{i,1} &:= (1-\beta_i)^+ \\
&= \max\{(1-\alpha_{i,1})^+, (1-\alpha_{i,2})^+\}
\end{aligned} \tag{65}$$

yields the following linear constraints:

$$\begin{aligned}
\alpha_{i,1} &\ge 1 - r_{i,1}, && (66)\\
\alpha_{i,2} &\ge 1 - r_{i,1}, && (67)\\
1 &\ge r_{i,1} \ge 0. && (68)
\end{aligned}$$

Again, for $i = 1, 2, \cdots, n_t - 1$, setting

$$\begin{aligned}
&r_{i,2} := \\
&\max\left\{\left(1-\alpha_{i+1,1}-(1-\beta_i)^+\right)^+, (1-\alpha_{i+1,2})^+\right\}
\end{aligned} \tag{69}$$

gives the following linear constraints:

$$\begin{aligned}
\alpha_{i+1,1} &\ge 1 - r_{i,1} - r_{i,2}, && (70)\\
\alpha_{i+1,2} &\ge 1 - r_{i,2}, && (71)\\
1 &\ge r_{i+1,2} \ge 0. && (72)
\end{aligned}$$

To achieve the desired multiplexing gain r, the linear constraint on the $r_{i,j}$ is given by

$$\sum_{i=1}^{n_t-1} n_i \left(r_{i,1} + r_{i,2}\right) \;\le\; Nr. \tag{73}$$

Using standard linear programming techniques to minimize $d(r)$ of (62) subject to the constraints of (64), (66), (67), (68), (70), (71), (72), and (73), it can be shown that

1) for the scheme $\mathcal{S}_1$, i.e., $n_i = 2$ for all i, we have $N = 2(n_t - 1)$ and

$$\begin{aligned}
d(r) &\ge (n_t-1)(2-r) \quad \text{and} && (74)\\
d(r) &\ge 2n_t - 2(n_t-1)r. && (75)
\end{aligned}$$

Hence for the region of $1 \le r \le 2$, the DMT achieved by $\mathcal{S}_1$ is given by

$$\begin{aligned}
d(r) &\ge \max\{(n_t-1)(2-r), \\
&\qquad\qquad 2n_t - 2(n_t-1)r\} \\
&= (n_t-1)(2-r), \quad \text{for } 1 \le r \le 2.
\end{aligned} \tag{76}$$

2) for the scheme $\mathcal{S}_2$, i.e., the case when $n_1 = n_{n_t-1} = 4$ and the remaining $n_i = 2$, we have $N = 2n_t + 2$, and

$$\begin{aligned}
d(r) &\ge 2n_t - (n_t+1)r \quad \text{and} && (77)\\
2d(r) &\ge (n_t+1)(2-r) && (78)
\end{aligned}$$

Thus for the region of $0 \le r \le 1$, the DMT achieved by scheme $\mathcal{S}_2$ is given by

$$\begin{aligned}
d(r) &\ge \max\Bigg\{2n_t - (n_t+1)r, \\
&\qquad\qquad \frac{n_t+1}{2}(2-r)\Bigg\} \\
&= 2n_t - (n_t+1)r, \quad \text{for } 0 \le r \le 1.
\end{aligned} \tag{79}$$

The proof is now complete after noting that the DMTs (76) and (79) achieved respectively by schemes $\mathcal{S}_1$ and $\mathcal{S}_2$ in the region of $r \in [1, 2]$ and $r \in [0, 1)$ match exactly the optimal DMT $d^*(r)$ given in (6).

APPENDIX II
PROOF OF THEOREM 2

First note that in the proposed transmission scheme

$$\mathcal{P} \;:=\; \Big\{ (\mathcal{T}_1 = \{T_1, \cdots, T_{n_r-1}, T_{n_r}\}, n_r), \; (\mathcal{T}_2 = \{T_1, \cdots, T_{n_r-1}, T_{n_r+1}\}, n_r) \Big\}$$

the set of transmit antennas

$$\mathcal{T}_0 \;:=\; \{T_1, \cdots, T_{n_r-1}\} \tag{80}$$

is used for both transmissions, and in each channel use, we add a new transmit antenna to the set $\mathcal{T}_0$, i.e.,

$$\mathcal{T}_i \;:=\; \mathcal{T}_0 \cup \{T_{n_r-i+1}\} \tag{81}$$

for $i = 1, 2$. For the ith selection pattern of the proposed scheme $\mathcal{P}$, let $\underline{x}_{i_j}$ be the jth signal vector transmitted by using the set $\mathcal{T}_i$ of transmit antennas, $j = 0, 1, \cdots, n_r - 1$. Similar to the proof of Theorem 1, to analyze the DMT performance we use a random Gaussian codebook and the vector $\underline{x}_{i_j}$ is a length n_r complex Gaussian random code vector having zero mean and covariance matrix $K_i = \frac{\text{SNR}}{n_r} I_{n_r}$. Hence, the signal vector $\underline{y}_{i_j}$ received at the receiver end is given by

$$\underline{y}_{i_j} \;=\; H_i \, \underline{x}_{i_j} + \underline{w}_{i_j} \tag{82}$$

where the channel matrix is

$$H_i \;=\; [H_0 \;\; \underline{h}_i]. \tag{83}$$

The random matrix H_0 is of size $(n_r \times (n_r - 1))$ and is used to model the transmission channels between the set $\mathcal{T}_0 = \{T_1, \cdots, T_{n_r-1}\}$ of transmit antennas and the receive antennas. The length-n_r vector $\underline{h}_i$ represents the fading coefficients between the transmit antenna T_{n_r+i-1} and the receive antennas. Entries of H_i are modeled as i.i.d. circularly symmetric, complex Gaussian random variables having zero mean and unit variance. The length-n_r vector $\underline{w}_{i_j}$ represents the additive white Gaussian noise and is composed of i.i.d. circularly symmetric, zero-mean, complex Gaussian random variables with unit variance. The transmit code vectors $\underline{x}_{i_j}$ are also assumed to be i.i.d.

Assuming the receiver has complete knowledge of channel state information, the mutual information between the received signal vectors $\underline{y}_{i_j}$'s and the transmitted signal vectors $\underline{x}_{i_j}$'s equals

$$\begin{aligned} & I\left(\underline{x}_{i_j}; \underline{y}_{i_j} | H_1, H_2\right) \\ =\;& \log\det\left(I_{n_r} + \frac{\text{SNR}}{n_r} H_i H_i^\dagger\right). \end{aligned}$$

Given the desired multiplexing gain r, the channel outage probability associated with scheme $\mathcal{P}$ is therefore given by

$$P_{\text{out}}(r) \;:=\; \Pr\left\{ \sum_{i=1}^{2} \log\det\left(I_{n_r} + \frac{\text{SNR}}{n_r} H_i H_i^\dagger\right) \le 2r \log \text{SNR} \right\}. \tag{84}$$

First note that for each channel matrix $H_i = [H_0 \; \underline{h}_i]$, the matrix product $H_i H_i^\dagger$ can be written as

$$H_i H_i^\dagger \;=\; H_0 H_0^\dagger + \underline{h}_i \underline{h}_i^\dagger. \tag{85}$$

Hence, for each j, $j = 0, 1, \cdots, n_r - 1$, we can rewrite the sum of mutual information as

$$\begin{aligned} & \sum_{i=1}^{2} I\left(\underline{x}_{i,j}; \underline{y}_{i,j} | H_1, H_2\right) \\ \doteq\;& \sum_{i=1}^{2} \log\det\left(I_{n_r} + \text{SNR} H_i H_i^\dagger\right) \\ =\;& \sum_{i=1}^{2} \log\det\left(I_{n_r} + \text{SNR} H_0 H_0^\dagger + \text{SNR}\, \underline{h}_i \underline{h}_i^\dagger\right). \end{aligned} \tag{86}$$

Let $H_0 H_0^\dagger = U D_0 U^\dagger$ be the eigen-decomposition of the $(n_r \times n_r)$ non-negative Hermitian symmetric matrix $H_0 H_0^\dagger$ with non-decreasing eigenvalues

$$0 = \lambda_0 < \lambda_1 \le \lambda_2 \;\cdots\; \le \;\lambda_{n_r-1} \tag{87}$$

and $\lambda_1 > 0$ with probability 1. Then following a similar approach as in the proof of Theorem 1 we can rewrite each summand in (86) as

$$\begin{aligned} & \log\det\left(I_{n_r} + \text{SNR} H_0 H_0^\dagger + \text{SNR}\, \underline{h}_i \underline{h}_i^\dagger\right) \\ =\;& \log\det\left(I_{n_r} + \text{SNR} D_0 + \text{SNR}\, U^\dagger \underline{h}_i \underline{h}_i^\dagger U\right) \\ =\;& \log\det\left(I_{n_r} + \text{SNR} D_0 + \text{SNR}\, \underline{g}_i \underline{g}_i^\dagger\right) \\ =\;& \log\det\left(I_{n_r} + \text{SNR} D_0\right) + \\ & \log\left[1 + \text{SNR} \underline{g}_i^\dagger (I_{n_r} + \text{SNR}\, D_0)^{-1} \underline{g}_i\right] \\ =\;& \left[\sum_{j=1}^{n_r-1} \log\left(1 + \text{SNR}\lambda_j\right)\right] + \\ & \log\left(1 + \sum_{j=1}^{n_r-1} \frac{\text{SNR}|g_{i,j}|^2}{1 + \text{SNR}\lambda_j} + \text{SNR}\,|g_{i,n_r}|^2\right), \end{aligned} \tag{88}$$

where $\underline{g}_i := U^\dagger \underline{h}_i = [g_{i,1} \cdots g_{i,n_r}]^t$. It should be noted that both $\underline{h}_i$ and $\underline{g}_i$ have the same statistical property, i.e., have the same joint probability density function.

Define

$$\lambda_i \;:=\; \text{SNR}^{-\alpha_i} \quad \text{and} \quad |g_{i,j}|^2 \;:=\; \text{SNR}^{-\beta_{i,j}} \tag{89}$$

and we can rewrite (88) as

$$\begin{aligned} & \log_{\text{SNR}} \det\left(I_{n_r} + \text{SNR} H_0 H_0^\dagger + \text{SNR}\, \underline{h}_i \underline{h}_i^\dagger\right) \\ =\;& \sum_{j=1}^{n_r-1} (1 - \alpha_j)^+ + \\ & \max_{1 \le j \le n_r-1} \Big\{ (1 - \beta_{i,j} - (1 - \alpha_j)^+)^+, \\ & \qquad (1 - \beta_{i,n_r})^+ \Big\}, \end{aligned} \tag{90}$$

where again, $(x)^+ := \max\{x, 0\}$.

With the above, we can now rewrite the mutual information (86) at high SNR as

$$\begin{aligned}&\frac{1}{\log \mathrm{SNR}} \sum_{i=1}^{2} I\left(\underline{x}_{i_j}; \underline{y}_{i_j} | H_1, H_2\right) \\ = \;& \left[2 \sum_{j=1}^{n_r-1} (1-\alpha_j)^+\right] + \\ & \sum_{i=1}^{2} \max_{1 \le j \le n_r-1} \Big\{(1-\beta_{i,j}-(1-\alpha_j)^+)^+, \\ & \qquad (1-\beta_{i,n_r})^+\Big\}. \end{aligned} \tag{91}$$

Next, it can be shown [17], [26] that the joint probability density function for $\alpha_1 \ge \cdots \ge \alpha_{n_r-1}$ and $\beta_{i,j}$'s is given by

$$\begin{aligned} & f(\alpha_1, \cdots, \alpha_{n_r-1}, \beta_{1,1}, \cdots, \beta_{2,n_r}) \\ & \qquad \doteq \begin{cases} 0, & \text{if any } \alpha_i, \beta_{i,j} < 0 \\ \mathrm{SNR}^{-d}, & \text{otherwise,} \end{cases} \end{aligned} \tag{92}$$

where

$$d = \left[2 \sum_{i=1}^{n_r-1} i \cdot \alpha_i\right] + \sum_{i=1}^{2} \sum_{j=1}^{n_r} \beta_{i,j} \tag{93}$$

Thus, define

$$\begin{aligned} \mathcal{A}(r) := \Big\{ & (\alpha_1, \cdots, \alpha_{n_r-1}, \beta_{1,1}, \cdots, \beta_{2,n_r}) : \\ & \left[2 \sum_{j=1}^{n_r-1} (1-\alpha_j)^+\right] + \\ & \sum_{i=1}^{2} \max_{1 \le j \le n_r-1} \Big\{(1-\beta_{i,j}-(1-\alpha_j)^+)^+, \\ & (1-\beta_{i,n_r})^+\Big\} \le 2r, \; \beta_{i,j} \ge 0, \\ & \alpha_1 \ge \alpha_2 \ge \cdots \ge \alpha_{n_r-1} \ge 0 \Big\}, \end{aligned} \tag{94}$$

and the diversity gain $d(r)$ equals

$$d(r) = \inf_{\mathcal{A}(r)} \left\{ \left[2 \sum_{i=1}^{n_r-1} i \cdot \alpha_i\right] + \sum_{i=1}^{2} \sum_{j=1}^{n_r} \beta_{i,j} \right\}. \tag{95}$$

To find the infimum, note the symmetries between the $\beta_{i,j}$, hence we are free to set $\beta_{2,j} = \beta_{1,j}$. Therefore, we can rewrite (95) as

$$d(r) = 2 \inf_{\mathcal{A}'(r)} \left\{ \left[\sum_{i=1}^{n_r-1} i \cdot \alpha_i\right] + \sum_{j=1}^{n_r} \beta_{1,j} \right\} \tag{96}$$

and

$$\begin{aligned} \mathcal{A}'(r) := \Big\{ & (\alpha_1, \cdots, \alpha_{n_r-1}, \beta_{1,1}, \cdots, \beta_{1,n_r}) : \\ & \left[\sum_{j=1}^{n_r-1} (1-\alpha_j)^+\right] + \\ & \max_{1 \le j \le n_r-1} \Big\{(1-\beta_{1,j}-(1-\alpha_j)^+)^+, \\ & (1-\beta_{1,n_r})^+\Big\} \le r, \; \beta_{1,j} \ge 0, \\ & \alpha_1 \ge \alpha_2 \ge \cdots \ge \alpha_{n_r-1} \ge 0 \Big\}. \end{aligned} \tag{97}$$

For $n_t = n_r + 1$, it can be shown that when $K - 1 \le r \le K$ for some integer K, the infimum is achieved at

$$\alpha_i = \begin{cases} 1, & \text{if } i = 1, \cdots, n_r - K - 1 \\ K - r, & \text{if } i = n_r - K \\ 0, & \text{if } i \ge n_r - K + 1 \end{cases} \tag{98}$$

and

$$\begin{aligned} \beta_{1,j} &= \beta_{2,j} \\ &= \begin{cases} \alpha_j, & \text{if } 1 \le j \le n_r - 1 \\ 1, & \text{if } j = n_r \text{ and } K = 1, \cdots, n_r - 1 \\ n_r - r, & \text{if } j = n_r \text{ and } K = n_r \end{cases} \end{aligned} \tag{99}$$

and the corresponding diversity gain $d(r) = d^*(r)$ which is a piecewise-linear function connecting the points

$$\begin{aligned} & (k, (n_r - k)(n_r - 1 - k) + (n_t - n_r + 1)(n_r - k)) \\ & = (k, (n_t - k)(n_r - k)) \end{aligned} \tag{100}$$

for $k = 0, 1, \cdots, n_r$. This completes the proof.

Appendix III
Proof of Theorem 3

In an $(n_t \times n_r)$ constrained asymmetric MIMO channel, let $\mathcal{T} = \{T_1, \cdots, T_{n_t}\}$ be the set of indices of the transmit antennas. For each transmit antenna T_i, let $\underline{h}_i$ be the length-n_r vector consisting of the fading coefficients from the transmit antenna T_i to the all n_r receive antennas.

Given the antenna selection pattern

$$\mathcal{S}_{\text{ext}} = \{(\mathcal{T}_1, \ell n_1), \cdots, (\mathcal{T}_s, \ell n_s)\},$$

for each selection pattern $\mathcal{T}_i \subset \mathcal{T}$, let H_i

$$H_i = \left[\underline{h}_j\right]_{T_j \in \mathcal{T}_i} \tag{101}$$

be the $(n_r \times n)$ channel matrix associated with $\mathcal{T}_i$, where $n = |\mathcal{T}_i|$ for all i by assumption. Prior to proving the main claim, we first note that given the selection pattern $\mathcal{S}_{\text{ext}}$ and the desired multiplexing gain r, the resulting channel outage probability is

$$\begin{aligned} P_{\text{out}}(r) = \mathrm{Pr}\Bigg\{ & \sum_{i=1}^{s} \ell n_i \log\det\left(I_n + \frac{\mathrm{SNR}}{n} H_i^\dagger H_i\right) \\ & \le Nr \log \mathrm{SNR} \Bigg\}, \end{aligned} \tag{102}$$

where

$$N \;:=\; \sum_{i=1}^{s} \ell n_i, \tag{103}$$

and where we have assumed the use of i.i.d. white Gaussian complex random code vectors as channel input.

It then follows from Fano's inequality [27] as well as the results of [17] that any constrained coding scheme $\mathcal{X}$ with multiplexing gain r that satisfies transmission selection pattern $\mathcal{S}_{\text{ext}}$ cannot have error performance smaller than the outage probability. That is, the codeword error probability $P_{\text{cwe},\mathcal{X}}(\text{SNR})$ of $\mathcal{X}$ must be lower bounded by the outage probability $P_{\text{out}}(r)$, i.e.,

$$P_{\text{cwe},\mathcal{X}}(\text{SNR}) \;\dot{\geq}\; P_{\text{out}}(r) \tag{104}$$

at high SNR regime. Thus, to prove Theorem 3 we need to establish the converse of (104) for the proposed code $\mathcal{X}_g$, i.e., we have to show that

$$P_{\text{cwe},\mathcal{X}_g}(\text{SNR}) \;\dot{\leq}\; P_{\text{out}}(r) \tag{105}$$

Given the code matrices $(X,\, \sigma(X),\, \cdots,\, \sigma^{m-1}(X)) \in \mathcal{X}_g$ and the partition $\{\mathcal{M}_1, \cdots, \mathcal{M}_s\}$ of $\{0, 1, \cdots, m-1\}$ we can assume without loss of generality that the code matrices are transmitted in the order of $X, \sigma(X), \cdots, \sigma^{m-1}(X)$, meaning that the code matrix X is transmitted first, and then follows by $\sigma(X)$, etc., each using the designated transmission antennas as specified by the sets of $\mathcal{M}_i$'s and $\mathcal{T}_i$'s. The set of $(n_r \times n)$ received signal matrices is thus given by

$$Y_j \;=\; \theta\, G_j\, \sigma^j(X) + W_j \tag{106}$$

for $j = 0, 1, \cdots, m-1$. The channel matrices G_j are given by

$$G_j \;=\; H_i \quad \text{if } j \in \mathcal{M}_i, \tag{107}$$

and the matrix W_j is a noise matrix consisting of i.i.d. circularly symmetric, complex Gaussian random variables with zero mean and unit variance. The θ is set at

$$\theta^2 \;:=\; \text{SNR}^{1-\frac{r}{n}} \tag{108}$$

to ensure the proper SNR value used for transmission.

Thus for any $X_p = \big(X, \sigma(X), \cdots, \sigma^{m-1}(X)\big) \neq X'_p = \big(X', \sigma(X'), \cdots, \sigma^{m-1}(X')\big) \in \mathcal{X}_g$, the square Euclidean distance between the noise-free received signal matrices is given by

$$\begin{aligned} d_E^2\left(X_p, X'_p\right) &= \theta^2 \sum_{i=0}^{m-1} \text{Tr}\left(G_i \Delta X_{p,i} \Delta X_{p,i}^\dagger G_i^\dagger\right) \\ &= \theta^2 \sum_{i=0}^{m-1} \text{Tr}\left(\Delta X_{p,i} \Delta X_{p,i}^\dagger G_i^\dagger G_i\right) \end{aligned} \tag{109}$$

where $\Delta X_{p,i} := \sigma^i(X - X')$.

Let $\delta_{i,j}$ and $\ell_{i,j}$ be the set of ordered eigenvalues of matrices $G_i^\dagger G_i$ and $\Delta X_{p,i} \Delta X_{p,i}^\dagger$, respectively, with the following ordering:

$$\delta_{i,1} \leq \delta_{i,2} \leq \cdots \leq \delta_{i,n}, \tag{110}$$

$$\ell_{i,1} \geq \ell_{i,2} \geq \cdots \geq \ell_{i,n}. \tag{111}$$

Note that by assumption we have $n \leq n_r$. It then follows from the mismatch eigenvalue bound [11], [28] that (109) can be lower bounded by

$$d_E^2\left(X_p, X'_p\right) \;\geq\; \theta^2 \sum_{i=0}^{m-1} \sum_{j=1}^{n} \delta_{i,j} \ell_{i,j}. \tag{112}$$

Furthermore, by rearranging and re-indexing the $\delta_{i,j}$'s and $\ell_{i,j}$'s according to the following ordering:

$$\delta_1 \leq \delta_2 \leq \cdots \leq \delta_{mn}, \tag{113}$$

$$\ell_1 \geq \ell_2 \geq \cdots \geq \ell_{nm}, \tag{114}$$

we can further lower-bound the quantity $d_E^2\left(X_p, X'_p\right)$ by

$$\begin{aligned} d_E^2\left(X_p, X'_p\right) &\geq \theta^2 \sum_{i=1}^{mn} \delta_i \ell_i \;\geq\; \theta^2 \sum_{i=mn-k+1}^{mn} \delta_i \ell_i \\ &\dot{\geq} \theta^2 \left[\prod_{i=mn-k+1}^{mn} \delta_i \ell_i\right]^{\frac{1}{k}} \\ &\geq \theta^2 \left[\prod_{i=mn-k+1}^{mn} \delta_i\right]^{\frac{1}{k}} \left[\frac{1}{\prod_{i=1}^{mn-k} \ell_i}\right]^{\frac{1}{k}} \\ &\dot{\geq} \theta^2 \left[\prod_{i=mn-k+1}^{mn} \delta_i\right]^{\frac{1}{k}} \left[\frac{1}{\left[\sum_{i=1}^{mn-k} \ell_i\right]^{mn-k}}\right]^{\frac{1}{k}} \\ &\geq \theta^2 \left[\prod_{i=mn-k+1}^{mn} \delta_i\right]^{\frac{1}{k}} \cdot \\ &\qquad \left[\frac{1}{\left[\sum_{i=0}^{m-1} \|\triangle X_{p,i}\|_F^2\right]^{mn-k}}\right]^{\frac{1}{k}} \\ &\doteq \text{SNR}^{1-\frac{r}{n}} \text{SNR}^{-\frac{1}{k}\sum_{i=mn-k+1}^{mn} \beta_i} \text{SNR}^{-\frac{mn-k}{k}\frac{r}{n}} \end{aligned} \tag{115}$$

$$:= \quad \text{SNR}^{d_k(\underline{\beta})}, \tag{116}$$

where

$$\beta_i \;:=\; -\frac{\log \delta_i}{\log \text{SNR}} \tag{117}$$

$$\underline{\beta} \;:=\; [\beta_1, \cdots, \beta_{mn}]^t, \tag{118}$$

and where $k = 1, 2, \cdots, mn$.

The inequality (115) is due to property of generalized non-vanishing determinant satisfied by $\mathcal{X}_g$, namely, we have

$$\begin{aligned} \prod_{i=1}^{mn} \ell_i &= \prod_{i=0}^{m-1} \det\left(\Delta X_{p,i} \Delta X_{p,i}^\dagger\right) \\ &= \prod_{i=1}^{m-1} \sigma^i \left[\det\left(\Delta X_{p,0} \Delta X_{p,0}^\dagger\right)\right] \in \mathbb{Z}^+, \end{aligned} \tag{119}$$

where by $\mathbb{Z}^+$ we mean the set of positive integers. Hence,

$$\prod_{i=1}^{mn} \ell_i \geq 1. \tag{120}$$

Finally, for each $k = 1, 2, \cdots, mn$ we have

$$d_k\left(\underline{\beta}\right) = \frac{1}{k}\left[k - rm - \sum_{i=mn-k+1}^{mn} \beta_i\right]. \tag{121}$$

It should be noted that we have used lose lower bounds on $d_E^2\left(X_p, X_p'\right)$ and the resulting $d_k\left(\underline{\beta}\right)$ depends only on the channel matrices G_j and is independent of the pair $\left(X_p, X_p'\right)$.

Next, recall that the received signal matrix Y_j is given by

$$Y_j \;=\; \theta\, G_j\, \sigma^j(X) + W_j$$

and that entries of W_j are i.i.d. complex Gaussian random variables $\mathbb{C}\mathcal{N}(0,1)$. Given $\underline{\beta} = [\beta_1, \cdots, \beta_{mn}]^t$, the codeword error probability of $\mathcal{X}_g$ can be upper bounded by

$$\begin{aligned} & P_{\text{cwe},\mathcal{X}_g}\left(\text{SNR} \mid \underline{\beta}\right) \\ &\leq \;\; \Pr\left\{\sum_{i=0}^{m-1} \|W_i\|_F^2 \geq \frac{d_E^2\left(X_p, X_p'\right)}{4}\right\} \\ &\dot{\leq} \;\; \Pr\left\{\sum_{i=0}^{m-1} \|W_i\|_F^2 \;\geq\; \text{SNR}^{d_k\left(\underline{\beta}\right)}\right\} \\ &= \;\; \exp\left(-\text{SNR}^{d_k\left(\underline{\beta}\right)}\right) \sum_{i=0}^{n_r mn-1} \frac{\left(\text{SNR}^{d_k\left(\underline{\beta}\right)}\right)^i}{i!}. \end{aligned} \tag{122}$$

It is clear that if $d_k\left(\underline{\alpha}\right) > 0$,

$$\lim_{\text{SNR}\to\infty} \exp\left(-\text{SNR}^{d_k\left(\underline{\beta}\right)}\right) \sum_{i=0}^{n_r mn-1} \frac{\left(\text{SNR}^{d_k\left(\underline{\beta}\right)}\right)^i}{i!} = 0.$$

Thus, let $f(\underline{\beta})$ be the joint probability distribution function of the ordered vector $\underline{\beta}$; then the codeword error probability can be upper bounded by

$$\begin{aligned} & P_{\text{cwe},\mathcal{X}_g}\left(\text{SNR}\right) \\ &= \int_{\underline{\beta}\in\mathbb{R}^{mn}} P_{\text{cwe},\mathcal{X}_g}\left(\text{SNR} \mid \underline{\beta}\right) f(\underline{\beta})\, d\underline{\beta} \\ &\doteq \int_{\mathcal{D}(r)} P_{\text{cwe},\mathcal{X}_g}\left(\text{SNR} \mid \underline{\beta}\right) f(\underline{\beta})\, d\underline{\beta} \\ &\leq \int_{\mathcal{D}(r)} f(\underline{\beta})\, d\underline{\beta}, \end{aligned} \tag{123}$$

where

$$\begin{aligned} \mathcal{D}(r) \;:=\; \Bigg\{ & \underline{\beta} \in \mathbb{R}^{mn} \;: \\ & k d_k\left(\underline{\beta}\right) = k - rm - \sum_{i=mn-k+1}^{mn} \alpha_i \leq 0, \\ & \text{for all } k\,, \beta_1 \geq \cdots \geq \beta_{mn} \Bigg\}. \end{aligned} \tag{124}$$

Furthermore, it can be shown [29], [30] that the set $\mathcal{D}(r)$ can be alternatively represented by

$$\begin{aligned} \mathcal{D}(r) \;:=\; \Bigg\{ & \underline{\beta} \in \mathbb{R}^{mn} \;:\; \sum_{i=1}^{mn} (1-\beta_i)^+ \leq mr, \\ & \beta_1 \geq \cdots \geq \beta_{mn} \Bigg\}. \end{aligned} \tag{125}$$

Having obtained (125), the codeword error probability $P_{\text{cwe},\mathcal{X}_g}(\text{SNR})$ can be further upper bounded by

$$\begin{aligned} & P_{\text{cwe},\mathcal{X}_g}(\text{SNR}) \\ &\leq \int_{\mathcal{D}(r)} f(\underline{\beta})\, d\underline{\beta} \;=\; \Pr\left\{\underline{\beta} \in \mathcal{D}(r)\right\} \\ &= \Pr\Bigg\{ \underline{\beta} \in \mathbb{R}^{mn} \;:\; \sum_{i=1}^{mn} (1-\beta_i)^+ \leq mr, \\ &\qquad\qquad \beta_1 \geq \cdots \geq \beta_{mn} \Bigg\} \\ &= \Pr\Bigg\{ \sum_{i=0}^{m-1} \log\det\left(I_n + \frac{\text{SNR}}{n} G_i^\dagger G_i\right) \leq \\ &\qquad\qquad mr \log \text{SNR} \Bigg\} \\ &= \Pr\Bigg\{ \sum_{i=1}^{s} m_i \log\det\left(I_n + \frac{\text{SNR}}{n} H_i^\dagger H_i\right) \leq \\ &\qquad\qquad mr \log \text{SNR} \Bigg\}, \end{aligned} \tag{126}$$

where we recall that $m_i = |\mathcal{M}_i|$ and that the $\mathcal{M}_i$'s are a partition of the set $\{0, 1, \cdots, m-1\}$.

Note that by construction we have

$$m_i = \frac{\ell n_i}{n} \;\text{ and }\; m = \frac{\ell}{n}\sum_{i=1}^{s} n_i \;=\; \frac{N}{n}. \tag{127}$$

Hence we can rewrite (126) as

$$\begin{aligned} & P_{\text{cwe},\mathcal{X}_g}(\text{SNR}) \,\dot{\leq} \\ & \Pr\Bigg\{ \sum_{i=1}^{s} \ell n_i \log\det\left(I_n + \frac{\text{SNR}}{n} H_i^\dagger H_i\right) \leq \\ & \qquad\qquad Nr \log \text{SNR} \Bigg\}, \end{aligned} \tag{128}$$

which coincides exactly with the outage probability of the transmit antenna selection $\mathcal{S}_{\text{ext}}$ given in (102). Hence it proves that the code $\mathcal{X}_g$ is optimal in terms of achieving the DMT.

Appendix IV
Sphere Decodability of Codes over Asymmetric Channels

In this section, we will provide brief discussions of why the conventional unconstrained CDA-based codes fail to be sphere decodable, and how the codes from the proposed construction in Theorem 3 can be decoded using sphere decoding techniques.

First of all, for an $(n_t \times n_r)$ asymmetric MIMO system with $n_t > n_r$, the CDA-based code proposed by the authors of [11] calls for a cyclic division algebra $\mathfrak{D}$ of degree n_t^2 over number

field $\mathbb{Q}(\imath)$, and each code matrix X has the following linear dispersion form:

$$X = \sum_{i=1}^{n_t^2} a_i E_i \tag{129}$$

for some independent QAM constellation points a_i and where the $(n_t \times n_t)$ matrices E_i are the basis elements for $\mathfrak{D}/\mathbb{Q}(\imath)$ which can be regarded as vector space of degree n_t^2. Set

$$E_i = \left[\underline{e}_{i,1} \cdots \mathbf{e}_{i,n_t}\right] \tag{130}$$

and let

$$Y = \left[\underline{y}_1 \cdots y_{n_r}\right] = \theta H X + W \tag{131}$$

be the $(n_r \times n_t)$ received signal matrix, where H is the channel matrix of size $(n_r \times n_t)$ and W is the noise matrix. θ is again some constant set to ensure the satisfaction of power constraint. To perform sphere decoding of X over Y, we can reformulate Y of (131) as

$$\begin{bmatrix} \underline{y}_1 \\ \vdots \\ \underline{y}_{n_t} \end{bmatrix} = \theta \underbrace{\begin{bmatrix} H & & \\ & \ddots & \\ & & H \end{bmatrix}}_{:=\hat{H}} \cdot \underbrace{\begin{bmatrix} \underline{e}_{1,1} & \cdots & \underline{e}_{n_t^2,1} \\ \vdots & \ddots & \vdots \\ \underline{e}_{1,n_t} & \cdots & \underline{e}_{n_t^2,n_t} \end{bmatrix}}_{:=\hat{E}} \underbrace{\begin{bmatrix} a_1 \\ \vdots \\ a_{n_t^2} \end{bmatrix}}_{:=\underline{a}} + \underline{w}, \tag{132}$$

where $\underline{w}$ is the $(n_t n_r \times 1)$ noise vector obtained by vertically concatenating the column vectors of noise matrix W. Clearly, we have

1) the $(n_r n_t \times n_t^2)$ block-diagonal matrix $\hat{H}$ is of full rank $n_t \cdot n_r$ with probability one, and
2) the $(n_t^2 \times n_t^2)$ square matrix $\hat{E}$ has full rank since the matrices $\{E_i\}$ form a basis for $\mathfrak{D}/\mathbb{Q}(\imath)$.

It is now straightforward to see that the $(n_t n_r \times n_t^2)$ product matrix $\hat{H}\hat{E}$ has rank equal to $n_t n_r$ and has linearly dependent columns since $n_t > n_r$ for asymmetric channel assumption. Thus, we conclude that X is not sphere decodable.

Next, for the proposed construction of constrained codes presented in Theorem 3, below we will show that unlike the unconstrained ones, the proposed code can be easily decoded using sphere decoders. Using notations defined in Appendix III, let $X_p = (X, \sigma(X), \cdots, \sigma^{m-1}(X)) \in \mathcal{X}_g$ be the $(n \times mn)$ code matrix chosen for transmission, and for each $(n \times n)$ submatrix $\sigma^j(X)$, let Y_j be the corresponding received signal matrix

$$Y_j = \left[\underline{y}_{j,1} \cdots \underline{y}_{j,n}\right] = \theta G_j \sigma^j(X) + W_j, \tag{133}$$

$j = 0, 1, \cdots, m-1$, where we recall that n is the size of each selection pattern of the transmit antennas and we have assumed $n \leq n_r$.

First note that, similar to the CDA-based code, the proposed $\mathcal{X}_g$ can also be written in a linear dispersion form, i.e., for any $X_p \in \mathcal{X}_g$, we have

$$X_p = \sum_{i=1}^{n^2 m} a_i C_i \tag{134}$$

for some independent QAM constellation points a_i and for some constant matrices C_i, each of size $(n \times nm)$, since the CDA $\mathfrak{D}$ defined in (23) is of degree nm^2 over its center $\mathbb{Q}(\imath)$ with a basis $\{C_i\}$. Similar to the discussion of the previous case, we can set

$$C_i = \left[\underline{c}_{i,1} \cdots \underline{c}_{i,nm}\right]$$

Now we are ready to rewrite (133) as

$$\begin{bmatrix} \underline{y}_{0,1} \\ \vdots \\ \underline{y}_{0,n} \\ \underline{y}_{1,1} \\ \vdots \\ \underline{y}_{m-1,n} \end{bmatrix} = \theta \underbrace{\begin{bmatrix} G_0 & & & \\ & \ddots & & \\ & & G_0 & \\ & & & \ddots \\ & & & & G_{m-1} \end{bmatrix}}_{:=\hat{G}} \cdot \underbrace{\begin{bmatrix} \underline{c}_{1,1} & \cdots & \underline{c}_{n^2 m,1} \\ \vdots & \ddots & \vdots \\ \underline{c}_{1,nm} & \cdots & \underline{c}_{n^2 m,nm} \end{bmatrix}}_{:=\hat{C}} \underbrace{\begin{bmatrix} a_1 \\ \vdots \\ a_{n^2 m} \end{bmatrix}}_{:=\underline{a}} + \underline{w}, \tag{135}$$

where $\hat{G}$ is a block-diagonal matrix of size $(n_r nm \times n^2 m)$ and $\hat{C}$ is of size $(n^2 m \times n^2 m)$. Thus, it is clear that the product matrix $\hat{G}\hat{C}$ is of size $(n_r nm \times n^2 m)$ and has linearly independent columns since $n_r > n$ by assumption. Hence we have shown that the proposed code $\mathcal{X}_g$ can be decoded by using sphere decoder.

REFERENCES

[1] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Europ. Trans. Telecomm.*, vol. 10, no. 6, pp. 585–595, Nov.-Dec. 1999.

[2] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Trans. Inf. Theory*, vol. 44, pp. 744–765, Mar. 1998.

[3] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 628–636, Mar. 2002.

[4] B. Hassibi and M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1804–1824, Jul. 2002.

[5] H. F. Lu and P. V. Kumar, "Rate-diversity tradeoff of space-time codes with fixed alphabet and optimal constructions for PSK modulation," *IEEE Trans. Inf. Theory*, pp. 2747–2751, Oct. 2003.

[6] ——, "A unified construction of space-time codes with optimal rate-diversity tradeoff," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1709–1730, May 2005.

[7] H. El Gamal and A. R. Hammons Jr., "On the design of algebraic space-time codes for MIMO block fading channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 151–163, Jan. 2003.

[8] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2596– 2616, Oct. 2003.

[9] M. O. Damen, H. El Gamal, and N. C. Beaulieu, "Linear threaded algebraic space-time constellations," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2372– 2388, Oct. 2003.

[10] H. El Gamal, G. Caire, and M. Damen, "Lattice coding and decoding achieve the optimal diversity-multilpexing tradeoff of MIMO channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 968–985, Jun. 2004.
[11] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-F. Lu, "Explicit construction of space-time block codes achieving the diversity-multiplexing gain tradeoff," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3869–3884, Sep. 2006.
[12] T. Kiran and B. S. Rajan, "STBC-schemes with non-vanishing determinant for certain number of transmit antennas," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2984–2992, Aug. 2005.
[13] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate, space-time block codes from division algebras," *IEEE Trans. Inf. Theory*, vol. 49, pp. 2596–2616, Oct. 2003.
[14] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect space time codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3885– 3902, Sept. 2006.
[15] J.-C. Belfiore, G. Rekaya, and E.Viterbo, "The Golden code: a 2×2 full-rate space-time code with non-vanishing determinants," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1432–1436, Apr. 2005.
[16] C. Hollanti and K. Ranto, "Asymmetric space-time block codes for mimo systems," in *Proc. 2007 IEEE Inform. Theory Workshop*, Solstrand, Norway, Jul. 2007, pp. 101–105.
[17] L. Zheng and D. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple antenna channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.
[18] S. Tavildar and P. Viswanath, "Approximately universal codes over slow fading channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3233–3258, Jul. 2006.
[19] H. F. Lu and P. V. Kumar, "Optimal constructions of space-time codes over multiple fading blocks," in *Proc. 2004 IEEE Int. Symp. on Information Theory*, Chicago, IL., 2004, p. 135.
[20] "IEEE P802.11 Wireless LANs: TGn Sync Proposal Technical Specification," *IEEE 802.11-04/0889r7*.
[21] "Draft Amendment to *IEEE* Standard for Local and Metropolitan Area Networks–Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems–Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands," IEEE *802.16e D11*, Sep. 13 2005.
[22] "Digital Video Broadcasting (DVB); Transmission System for Handheld Terminals," *ETSI Standard: EN 302 304 V1.1.1*, Nov. 2004.
[23] "Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television," *ETSI Standard: EN 300 744 V1.5.1*, Nov. 2004.
[24] H. F. Lu, "Explicit constructions of multi-block space-time codes that achieve the diversity-multiplexing tradeoff," in *Proc. 2006 IEEE Int. Symp. Inform. Theory*, Seattle, WA, Jul. 2006, pp. 1149–1153.
[25] H. F. Lu, P. Elia, S. A. Pawar, K. R. Kumar, and P. V. Kumar, "Space-time codes meeting the diversity-multiplexing gain tradeoff with low signalling complexity," in *Proc. CISS 2005*, Baltimore MD, Mar. 2005.
[26] A. Edelman, "Eigenvalues and conditional numbers of random matrices," Ph.D. dissertation, MIT, 1989.
[27] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New Jersey: John Wiley & Sons, 1991.
[28] C. Köse and R. D. Wesel, "Universal space-time trellis codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2717–2727, Oct. 2003.
[29] S. Yang and J.-C. Belfiore, "Optimal space-time codes for the amplify-and-forward cooperative channel," in *Proc. 43nd Allerton Conference on Communication, Control and Computing*, Monticello, Illinois, Sep. 2005.
[30] P. Elia and P. V. Kumar, "Approximately-universal space-time codes for the parallel, multi-block and cooperative-dynamic-decode-and-forward channels," Jul. 2007, http://arxiv.org/pdf/0706.3502.

Turku Centre for Computer Science
TUCS Dissertations

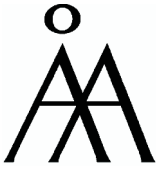
79. **Viorel Preoteasa**, Program Variables – The Core of Mechanical Reasoning about Imperative Programs
80. **Jonne Poikonen**, Absolute Value Extraction and Order Statistic Filtering for a Mixed-Mode Array Image Processor
81. **Luka Milovanov**, Agile Software Development in an Academic Environment
82. **Francisco Augusto Alcaraz Garcia**, Real Options, Default Risk and Soft Applications
83. **Kai K. Kimppa**, Problems with the Justification of Intellectual Property Rights in Relation to Software and Other Digitally Distributable Media
84. **Drago$ Tru$can**, Model Driven Development of Programmable Architectures
85. **Eugen Czeizler**, The Inverse Neighborhood Problem and Applications of Welch Sets in Automata Theory
86. **Sanna Ranto**, Identifying and Locating-Dominating Codes in Binary Hamming Spaces
87. **Tuomas Hakkarainen**, On the Computation of the Class Numbers of Real Abelian Fields
88. **Elena Czeizler**, Intricacies of Word Equations
89. **Marcus Alanen**, A Metamodeling Framework for Software Engineering
90. **Filip Ginter**, Towards Information Extraction in the Biomedical Domain: Methods and Resources
91. **Jarkko Paavola**, Signature Ensembles and Receiver Structures for Oversaturated Synchronous DS-CDMA Systems
92. **Arho Virkki**, The Human Respiratory System: Modelling, Analysis and Control
93. **Olli Luoma**, Efficient Methods for Storing and Querying XML Data with Relational Databases
94. **Dubravka Ili¿**, Formal Reasoning about Dependability in Model-Driven Development
95. **Kim Solin**, Abstract Algebra of Program Refinement
96. **Tomi Westerlund**, Time Aware Modelling and Analysis of Systems-on-Chip
97. **Kalle Saari**, On the Frequency and Periodicity of Infinite Words
98. **Tomi Kärki**, Similarity Relations on Words: Relational Codes and Periods
99. **Markus M. Mäkelä**, Essays on Software Product Development: A Strategic Management Viewpoint
100. **Roope Vehkalahti**, Class Field Theoretic Methods in the Design of Lattice Signal Constellations
101. **Anne-Maria Ernvall-Hytönen**, On Short Exponential Sums Involving Fourier Coefficients of Holomorphic Cusp Forms
102. **Chang Li**, Parallelism and Complexity in Gene Assembly
103. **Tapio Pahikkala**, New Kernel Functions and Learning Methods for Text and Data Mining
104. **Denis Shestakov**, Search Interfaces on the Web: Querying and Characterizing
105. **Sampo Pyysalo**, A Dependency Parsing Approach to Biomedical Text Mining
106. **Anna Sell**, Mobile Digital Calendars in Knowledge Work
107. **Dorina Marghescu**, Evaluating Multidimensional Visualization Techniques in Data Mining Tasks
108. **Tero Säntti**, A Co-Processor Approach for Efficient Java Execution in Embedded Systems
109. **Kari Salonen**, Setup Optimization in High-Mix Surface Mount PCB Assembly
110. **Pontus Boström**, Formal Design and Verification of Systems Using Domain-Specific Languages
111. **Camilla J. Hollanti**, Order-Theoretic Methods for Space-Time Coding: Symmetric and Asymmetric Designs

Turku
Centre *for*
Computer
Science

Joukahaisenkatu 3-5 B, 20520 Turku, Finland | www.tucs.fi

University of Turku

- Department of Information Technology
- Department of Mathematics



Åbo Akademi University

- Department of Information Technologies

Turku School of Economics

- Institute of Information Systems Sciences

ISBN 978-952-12-2217-7
ISSN 1239-1883

Camilla J. Hollanti

Order-Theoretic Methods for Space-Time Coding: Symmetric and Asymmetric Designs

Camilla J. Hollanti

Order-Theoretic Methods for Space-Time Coding: Syymetric and Asymmetric Designs