Applications of the Footprint and the Feng-Rao Bounds

Martin, Stefano

Publication date:
2014

Document Version
Peer reviewed version

PhD Report Series - No. 29 - 2014

Applications of the Footprint and the Feng-Rao Bounds

Stefano Martin

AALBORG UNIVERSITY
Department of Mathematical Sciences

Applications of the Footprint and the Feng-Rao Bounds

Stefano Martin

Thesis submitted: October 3, 2014

Thesis defended: December 8, 2014

PhD degree conferred: December 15, 2014

PhD supervisors: Prof. Olav Geil and Associate Prof. Diego Ruano
Department of Mathematical Sciences
Aalborg University, Denmark

PhD committee: Associate Prof. Carlos Munuera
Department of Applied Mathematics
University of Valladolid, Spain

Associate Prof. Maria Bras-Amorós
School of Engineering
Universitat Rovira i Virgil, Spain

Adjunct Prof. Tom Høholdt
Department of Mathematical Sciences
Aalborg University, Denmark

DEPARTMENT OF MATHEMATICAL SCIENCES
Fredrik Bajers Vej 7G
9220 Aalborg, Denmark
http://www.math.aau.dk

ISSN 1601-8346

AALBORG UNIVERSITY

Faculty of Engineering and Science
Department of Mathematical Sciences

Dissertation for the degree of Philosophiae Doctor

APPLICATIONS OF THE FOOTPRINT AND THE FENG-RAO BOUNDS

by

Stefano Martin

October 2014

Mandatory page

Thesis title: Applications of the footprint and the Feng-Rao bounds

Name of the PhD student: Stefano Martin

Name and title of supervisor and any other supervisors: Professor Olav Geil, Associate Professor Diego Ruano

List of published papers:

I Geil Olav, Martin Stefano and Matsumoto Ryutaroh, "A new method for constructing small-bias spaces from Hermitian codes", *Journal reference WAIFI 2012*, LNCS vol. 7369, pp. 29-44, 2012
preprint at arXiv: 1203.0491v1 [cs.IT], doi: 10.1007/978-3-642-31662-3_3

II Geil Olav and Martin Stefano, "An improvement of the Feng-Rao bound for primary codes", *published in Designs, Codes and Cryptography (DESI)*, 2013
preprint at arXiv: 1307.3107v2 [cs.IT], doi: 10.1007/s10623-014-9983-z

III Geil Olav and Martin Stefano, "Further improvements on the Feng-Rao bound for dual codes", *published in Finite Fields and their Applications*, vol.30, pages 33-48, 2013
preprint at arXiv: 1305.1091v1 [cs.IT], doi: 10.1016/j.ffa.2014.05.006

IV Geil Olav, Martin Stefano, Matsumoto Ryutaroh, Ruano Diego and Luo Yuan, "Relative generalized Hamming weights of one-point algebraic geometric codes", *published in IEEE Transaction of Information Theory*, vol.60, no. 10, pages 5938-5949, 2014
preprint at arXiv: 1403.7985v3 [cs.IT], doi: 10.1109/TIT.2014.2345375

V Martin Stefano and Geil Olav, "Relative generalized Hamming weights of q-ary Reed-Muller codes", *submitted*, 2014
preprint at arXiv: 1407.6185v2 [cs.IT]

This thesis has been submitted for assessment in partial fulfillment of the PhD degree. The thesis is based on the submitted or published scientific papers which are listed above. Parts of the papers are used directly or indirectly in the extended summary of the thesis. As part of the assessment, co-author statements have been made available to the assessment committee and are also available at the Faculty. The thesis is not in its present form acceptable for open publication but only in limited and closed circulation as copyright may not be ensured

Acknowledgements

I am glad to be able to have the possibility to thank in this section the people that were near to me during these three years of my PhD-studies and that contributed to make me and my research better and better.

First of all I want to express my deepest gratitude to my main supervisors Professor Olav Geil and Associate Professor Diego Ruano. They were always very helpful, giving me several advices and ideas to develop my research. They proposed me several interesting problems sharing with me their knowledge and experience. I thank them because they were for me teachers, supervisors and friends.

I am very thankful to guest Professor Ryutaroh Matsumoto of Tokyo Institute of Technology for his continuous help and encouragement. I am very grateful to Professor Chen Hao of East China Normal University for hosting me during my visit to Shanghai and to share his ideas with me.

I would also like to convey thanks to all my colleagues at the Department of Mathematical Sciences of Aalborg University for creating such a pleasant environment to work in. In addition, cordial thanks are due to the administrative staff for their enthusiastic help with practical issues.

Last but not least, I wish to acknowledge my indebtedness to my entire family and friends for their endless support and patience during the whole period of my education. My wife Peng Yuan deserves a special "Thank you" for entering my life during my PhD-studies giving me the strength and the happiness that I needed.

The author gratefully acknowledge the support from the Danish National Research Foundation and the National Natural Science Foundation of China (Grant No. 11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography.

Abstract

Minimum distance, general Hamming weights and relative generalized Hamming weights are parameters of great importance in coding theory and cryptography. Their computation is often very hard and for this reason there exist some bounds to estimate them. We analyse the footprint bound and the Feng-Rao bounds with the one-way well-behaving property. Furthermore we give two improvements of these bounds for primary and dual codes. We propose three different applications of the bounds:

- Using the footprint bound we propose a new method to build small-bias spaces from Hermitian codes that perform well.
- We illustrate how to bound or compute the relative generalized Hamming weights of one-point algebraic geometric codes, Hermitian codes and q-ary Reed-Muller codes.
- Finally with our improvement we prove that affine variety codes are better than their reputation.

Summary

Before the exposition of the five papers we give an introduction.

Introduction

The introduction is divided into two parts.

In the first part we illustrate how the footprint bound, the Feng-Rao bounds with one-way well-behaving property and our improvements of these bounds are useful tools in the case of affine variety codes. Further we generalize these two last bounds showing how to apply them for any primary and dual linear codes.

The second part is structured in three sections where we focus on three applications of these bounds. The first one is dedicated to a new method for building small-bias spaces from Hermitian codes. Using the footprint bound we show that this construction performs well. In the second section we illustrate how to apply the relative generalized Hamming weights to evaluate the security of linear secret sharing schemes. We use the Feng-Rao bound to bound the relative generalized Hamming weights for one-point algebraic geometric codes (in particular Hermitian codes). Furthermore with the help of the footprint bound we show how to compute the exact values of the relative generalized Hamming weights of q-ary Reed-Muller codes. In the last section we prove, using our improvements, that the affine variety codes are better than their reputation.

Papers

Paper I is dedicated to a new method for constructing small-bias spaces from Hermitian codes. We show that our construction is competitive in speed of construction and that it performs better than the ones related to norm-trace codes. Paper II and III examine our improvement of the Feng-Rao bound with one-way well-behaving property for primary and dual linear codes respectively. In Paper IV we explain how to use the relative generalized Hamming weights to evaluate the security of linear secret sharing schemes. Furthermore in this paper we show how to bound these parameters with one-point algebraic geometric codes and Hermitian codes especially. Paper V is focused on the computation of the relative generalized Hamming weights of q-ary Reed-Muller codes.

Abstrakt på dansk

Minimumsafstand, genereliserede Hammingvægte og relative genereliserede Hammingvægte er parametre af stor betydning i kodningsteori og kryptografi. Beregningen af dem er ofte meget vanskellig – og af den grund findes der grænser ved hjælp af hvilke, man kan estimere dem. Vi analyserer fodaftryksgrænsen og Feng-Rao-grænserne i one-way well-behaving versionerne. Videre præsenterer vi to forbedringer af disse grænser – nemlig for primære koder og for duale koder. Vi præsenterer tre forskellige anvendelser af grænserne:

- Ved hjælp af fodaftryksgrænsen indfører en ny metode til at bygge gode small-bias spaces fra Hermitiske koder.
- Vi viser, hvordan man kan estimere og beregne de relative genereliserede Hammingvægte for et-punkts algebraisk geometrikoder, Hermitiske koder og q-æriske Reed-Muller koder.
- Endelig viser vi ved hjælp af vores forbedrede grænser, at affine varietetskoder er bedre end deres rygte.

Resume på danks

Afhandlingen indledes med en introduktion, hvorefter de fem artikler følger.

Introduktion

Introduktionen er inddelt i to dele.

I den første del illustrerer vi, hvorledes fodaftryksgrænsen, Feng-Rao grænserne i one-way well-behaving versionerne og vores forbedringer af disse kan tjene som nyttige værktøjer i forbindelse med affine varietetskoder. Endvidere generaliserer vi de to sidstnævnte grænser, således at de kan anvendes på vilkårlige primære eller duale lineære koder.

Del to er inddelt i tre underafsnit, hvor vi fokuserer på de tre anvendelser af grænserne. Det første underafsnit beskæftiger sig med en ny metode til at konstruere small-bias spaces fra Hermitiske koder. Ved hjælp af fodaftryksgrænsen viser vi, at denne konstruktion har gode egenskaber. I det næste underafsnit forklarer vi, hvorledes man kan anvende relative genereliserede Hammingvægte til at evaluere sikkerheden af lineære secret sharing schemes. Ved hjælp af Feng-Rao grænsen viser vi, hvorledes man kan estimere de relative genereliserede Hammingvægte for et-punkts algebraiske geometrikoder (herunder specielt Hermitiske koder). Endvidere viser vi, hvorledes man i tilfældet af q-æriske Reed-Muller koder, ved hjælp af fodaftryksgrænsen kan beregne de eksakte værdier af de relative genereliserede Hammingvægte. I det sidste underafsnit beviser vi ved hjælp af vores forbedrede grænser, at affine varietets koder er bedre ende deres rygte.

Artikler

Artikel I beskæftiger sig med en ny metode til at konstruere small-bias spaces ved hjælp af Hermitiske koder. Vi demonstrerer, at vores konstruktion er konkurrencedygtig med hensyn til konstruktionshastighed samt at vores small-bias spaces har bedre parametre end small-bias spacene defineret ved hjælp af norm-trace-koder. Artikel II og III undersøger vores forbedringer af Feng-Rao grænserne i versionen med one-way well-behaving – såvel for primære som duale koder. I artikel IV forklarer vi, hvorledes man kan anvende relative genereliserede Hammingvægte til at evaluere sikkerheden af lineære secret sharing schemes. Endvidere viser vi i denne artikel, hvorledes man kan estimere disse parametre for et-punkts algebraiske geometrikoder og for Hermitiske koder specielt. Artikel V fokuserer på beregningen af relative genereliserede Hammingvægte for q-æriske Reed-Muller koder.

List of Papers

I Geil Olav, Martin Stefano and Matsumoto Ryutaroh, "A new method for constructing small-bias spaces from Hermitian codes", *Journal reference WAIFI 2012*, LNCS vol. 7369, pp. 29-44, 2012
preprint at arXiv: 1203.0491v1 [cs.IT], doi: 10.1007/978-3-642-31662-3_3

II Geil Olav and Martin Stefano, "An improvement of the Feng-Rao bound for primary codes", *published in Designs, Codes and Cryptography (DESI)*, 2013
preprint at arXiv: 1307.3107v2 [cs.IT], doi: 10.1007/s10623-014-9983-z

III Geil Olav and Martin Stefano, "Further improvements on the Feng-Rao bound for dual codes", *published in Finite Fields and their Applications*, vol.30, pages 33-48, 2013
preprint at arXiv: 1305.1091v1 [cs.IT], doi: 10.1016/j.ffa.2014.05.006

IV Geil Olav, Martin Stefano, Matsumoto Ryutaroh, Ruano Diego and Luo Yuan, "Relative generalized Hamming weights of one-point algebraic geometric codes", *published in IEEE Transaction of Information Theory*, vol.60, no. 10, pages 5938-5949, 2014
preprint at arXiv: 1403.7985v3 [cs.IT], doi: 10.1109/TIT.2014.2345375

V Martin Stefano and Geil Olav, "Relative generalized Hamming weights of q-ary Reed-Muller codes", *submitted*, 2014
preprint at arXiv: 1407.6185v2 [cs.IT]

Contents

INTRODUCTION

Chapter 1

Bounds

Throught the introduction we use the following notation: q is a power of a prime and we denote with $\mathbb{F}_q$ a field with q elements. Given a monomial ordering $\prec$, we denote by $\mathrm{lm}(F)$ the leading monomial of the polynomial F.

In this part we give the definition of generalized Hamming weights and relative generalized Hamming weights. We continue introducing the footprint bound, the Feng-Rao bound and our improvements of the Feng-Rao bound.

1.1 Generalized Hamming weights and relative generalized Hamming weights

A well-know concept in coding theory is the generalized Hamming weights [12, 10, 24] which we start by introducing. Recall that for $D \subseteq \mathbb{F}_q^n$ the support of D is defined as

$$\mathrm{supp}(D) = \{i \mid c_i \neq 0 \text{ for some } \vec{c} = (c_1, \ldots, c_n) \in D\}.$$

Definition 1. Let C be a linear code and k its dimension. For $r = 1, \ldots, k$, the r-th generalized Hamming weight (GHW) of C is defined by

$$d_r(C) = \min\{\#\mathrm{supp}(D) \mid D \text{ is a linear subcode of } C \text{ and } \dim(D) = r\}.$$

The sequence $(d_1(C), \ldots, d_k(C))$ is called the hierarchy of the GHWs of C.

In particular $d_1(C)$ is the minimum distance of C. A further generalization of GHWs was introduced by Luo et al. in [15].

Definition 2. Let $C_2 \subsetneq C_1$ be linear codes, $\ell = \dim(C_1) - \dim(C_2)$ the codimension of C_1 and C_2, and n the length of the codes. For $m = 1, \ldots, \ell$, the m-th relative generalized Hamming weight (RGHW) of C_1 with respect to C_2 is defined by

$$M_m(C_1, C_2) = \min_{J \subseteq \{1,\ldots,n\}} \{\#J \mid \dim((C_1)_J) - \dim((C_2)_J) = m\}$$

where $(C_i)_J = \{\vec{c} \in C_i \mid c_t = 0 \text{ for } t \notin J\}$ for $i = 1, 2$. The sequence $(M_1(C_1, C_2), \ldots, M_\ell(C_1, C_2))$ is called the hierarchy of the RGHWs of C_1 with respect to C_2.

If C_2 is the zero code $\{\vec{0}\}$ then the m-th RGHW of C_1 with respect to C_2 is equivalent to the m-th GHW of C_1. This fact should be more clear from the following result [14, Lem. 1].

Theorem 3. *Let $C_2 \subsetneq C_1$ be linear codes and $\ell = \dim(C_1) - \dim(C_2)$ be the codimension of C_1 and C_2. For $m = 1, \ldots, \ell$ we have that*

$$M_m(C_1, C_2) = \min\{\#\mathrm{supp}(D) \mid D \text{ is a linear subcode of } C_1, \\ D \cap C_2 = \{\vec{0}\} \text{ and } \dim(D) = m\}.$$

1.2 The footprint bound

The computation of the above mentioned parameters is usually hard, however there exists some bounds to estimate them. If our code is an affine variety code the footprint bound, the Feng-Rao bounds and our improvement of the Feng-Rao bound are powerful tools. Because in this case the Feng-Rao bounds and our improvements can be viewed as consequences of the footprint bound from Gröbner basis then we start introducing the affine variety codes and the footprint bound.

Affine variety codes were introduced by Fitzgerald and Lax in [7] as follows. Consider an ideal $I \subseteq \mathbb{F}_q[X_1, \ldots, X_s]$ and define

$$I_q = I + \langle X_1^q - X_1, \ldots, X_s^q - X_s \rangle$$

$$R_q = \mathbb{F}_q[X_1, \ldots, X_s]/I_q.$$

Let $\{P_1, \ldots, P_n\} = \mathbb{V}_{\mathbb{F}_q}(I_q)$ be the corresponding variety over $\mathbb{F}_q$. Here, $P_i \neq P_j$ for $i \neq j$. Define the $\mathbb{F}_q$-linear map $\mathrm{ev} : R_q \to \mathbb{F}_q^n$ by $\mathrm{ev}(F + I_q) = (F(P_1), \ldots, F(P_n))$. It is well-known that this map is a vector space isomorphism.

Definition 4. Let L be an $\mathbb{F}_q$ vector subspace of R_q. Define $C(I, L) = \mathrm{ev}(L)$ and $C^{\perp}(I, L) = \big(C(I, L)\big)^{\perp}$.

We shall call $C(I, L)$ a primary affine variety code and $C^{\perp}(I, L)$ a dual affine variety code. We now give the definition of footprint and the theorem for the computation of the footprint bound [9, 11].

Definition 5. Given a monomial ordering $\prec$ and an ideal $I \subseteq k[X_1, \ldots, X_s]$ (here k is any field) the footprint is

$$\Delta_{\prec}(I) := \{X_1^{\alpha_1} \cdots X_s^{\alpha_s} \mid X_1^{\alpha_1} \cdots X_s^{\alpha_s} \text{ is not a leading monomial of any polynomial in } I\}.$$

Theorem 6. *Assume I is zero-dimensional (meaning that $\Delta_{\prec}(I)$ is finite). The variety $\mathbb{V}_{\mathbb{F}}(I)$ satisfies $\#\mathbb{V}_{\mathbb{F}}(I) \leq \#\Delta_{\prec}(I)$.*

As a consequence of the footprint bound we obtain the following result that we can use to bound the RGHWs of an affine variety code.

Corollary 7. *Let* $D = \mathrm{span}_{\mathbb{F}_q}\{ev(F_1), \ldots, ev(F_m)\}$ *be a subspace of* $C(I, L)$ *and* $\prec$ *any monomial ordering. We have:*

$$\#\mathrm{supp}(D) \geq n - \#\Delta_\prec(\langle F_1, \ldots, F_m\rangle + I_q)$$

Thus if we consider two $\mathbb{F}_q$-vector subspaces of R_q, $L_2 \subsetneq L_1$, then we obtain:

$$\begin{aligned}
& M_m(C(I, L_1), C(I, L_2)) \\
= \; & \min\{\#\mathrm{supp}(D) \mid D \text{ is linear subcode of } C(I, L_1), \\
& \dim(D) = m \text{and } D \cap C(I, L_2) = \{\vec{0}\}\} \\
\geq \; & \min\{\#\mathrm{supp}(D) \mid D = \mathrm{span}_{\mathbb{F}_q}\{\mathrm{ev}(F_1), \ldots, \mathrm{ev}(F_m)\}, \\
& \mathrm{lm}(F_i) \in \mathrm{lm}(L_1), \mathrm{lm}(F_i) \notin \mathrm{lm}(L_2) \text{ for } i = 1, \ldots, m, \\
& \mathrm{lm}(F_i) \neq \mathrm{lm}(F_j) \text{ for } i \neq j\} \\
\geq \; & n - \max\{\#\Delta_\prec(\langle F_1, \ldots, F_m\rangle + I_q) \mid \\
& \mathrm{lm}(F_i) \in \mathrm{lm}(L_1), \mathrm{lm}(F_i) \notin \mathrm{lm}(L_2) \text{ for } i = 1, \ldots, m, \\
& \mathrm{lm}(F_i) \neq \mathrm{lm}(F_j) \text{ for } i \neq j\}
\end{aligned}$$

for $m = 1, \ldots, \ell$, where $\ell = \dim(C(I, L_1)) - \dim(C(I, L_2))$ is their codimension.

In Paper I we use the footprint bound to evaluate a new method for constructing small-bias spaces from Hermitian codes and in Paper V we use it to compute the RGHWs of q-ary Reed-Muller codes.

1.3 The Feng-Rao bounds

1.3.1 The Feng-Rao bound for primary affine variety codes

In this section we recall the interpretation from [8] of the Feng-Rao bound for primary affine variety codes.

Definition 8. Let $\mathcal{G}$ be a Gröbner basis for I_q with respect to a monomial ordering $\prec$. An ordered pair of monomials (M_i, M_j), $M_i, M_j \in \Delta_\prec(I_q)$ is said to be one-way well-behaving (OWB) if for all $H \in \mathbb{F}_q[X_1, \ldots, X_s]$ with $\mathrm{Supp}(H) \subseteq \Delta_\prec(I_q)$ and $\mathrm{lm}(H) = M_i$ it holds that

$$\mathrm{lm}(M_i M_j \text{ rem } \mathcal{G}) = \mathrm{lm}(H M_j \text{ rem } \mathcal{G}).$$

Here, F rem $\mathcal{G}$ means the remainder of F after division with $\mathcal{G}$ (see [6, Sec. 2.3] for the division algorithm for multivariate polynomials).

Definition 9. A basis $\{B_1 + I_q, \ldots, B_{\dim(L)} + I_q\}$ for a subspace $L \subseteq R_q$ where $\mathrm{Supp}(B_i) \subseteq \Delta_\prec(I_q)$ for $i = 1, \ldots, \dim(L)$ and where $\mathrm{lm}(B_1) \prec \cdots \prec \mathrm{lm}(B_{\dim(L)})$, is said to be well-behaving with respect to $\prec$. Also we define

$$\square_\prec(L) = \{\mathrm{lm}(B_1), \ldots, \mathrm{lm}(B_{\dim(L)})\}$$

where $\{B_1 + I_q, \ldots, B_{\dim(L)} + I_q\}$ is any well-behaving basis for L.

Using this definition and the footprint bound as described in Theorem 6 we obtain the Feng-Rao bound with OWB property.

Theorem 10. *Let $\mathcal{G}$ be a Gröbner basis for I_q with respect to a monomial ordering $\prec$. Consider a non-zero word $\vec{c}$ and let F be the unique polynomial such that $Supp(F) \subseteq \Delta_\prec(I_q)$ and $\vec{c} = ev(F)$. Let $lm(F) = P$. We have*

$$w_H(\vec{c}) \geq \#\{K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q) \text{ such that } (P,N) \text{ is OWB and } lm(PN \text{ rem } \mathcal{G}) = K\}. \quad (1.1)$$

A bound on the minimum distance of $C(I,L)$ is found by taking the minimum of (1.1) when P runs through $\Box_\prec(L)$.

The Feng-Rao bound is particularly suited for affine varieties which satisfy the order domain conditions [8, Def. 4.22]. In its most general form the order domain conditions involve a weighted degree monomial ordering with weights $w(X_1), \ldots, w(X_s)$ in $\mathbb{N}_0^r \backslash \{\vec{0}\}$, with r a positive integer (see [8, Def. 4.21]).

Definition 11. Let $w(X_1), \ldots, w(X_s) \in \mathbb{N}_0^r \backslash \{\vec{0}\}$ and define the weight of $X_1^{i_1} \cdots X_s^{i_s}$ to be the number $w(X_1^{i_1} \cdots X_s^{i_s}) = i_1 w(X_1) + \cdots + i_s w(X_s)$. The weighted degree ordering $\prec_w$ on $\mathcal{M}(X_1, \ldots, X_s)$ is the ordering with $X_1^{i_1} \cdots X_s^{i_s} \prec_w X_1^{j_1} \cdots X_s^{j_s}$ if either $w(X_1^{i_1} \cdots X_s^{i_s}) < w(X_1^{j_1} \cdots X_s^{j_s})$ holds or $w(X_1^{i_1} \cdots X_s^{i_s}) = w(X_1^{j_1} \cdots X_s^{j_s})$ holds but $X_1^{i_1} \cdots X_s^{i_s} \prec X_1^{j_1} \cdots X_s^{j_s}$. Here, $\prec$ is some fixed monomial ordering.

We now state the order domain conditions.

Definition 12. Consider an ideal $I \subseteq k[X_1, \ldots, X_s]$ where k is a field. Let a weighted degree ordering $\prec_w$ be given. Assume that I possesses a Gröbner basis $\mathcal{G}$ with respect to $\prec_w$ such that:

(C1) Any $F \in \mathcal{G}$ has exactly two monomials of highest weight.

(C2) No two monomials in $\Delta_{\prec_w}(I)$ are of the same weight.

Then we say that I and $\prec_w$ satisfy the order domain conditions.

These conditions give us the following interesting property.

Proposition 13. *Assume $I \subseteq \mathbb{F}_q[X_1, \ldots, X_s]$ and $\prec_w$ satisfy the order domain conditions. A pair (P,N) where $P, N \in \Delta_{\prec_w}(I_q)$ is OWB if $w(P) + w(N) \in w(\Delta_{\prec_w}(I_q))$.*

We can generalize Theorem 10 to also work for RGHWs.

Corollary 14. *Let $\mathcal{G}$ be a Gröbner basis for I_q with respect to a monomial ordering $\prec$. Let $D = \{ev(F_1), \ldots, ev(F_m)\}$ be an m-dimensional subspace of $\mathbb{F}_q^n$ where without loss of generality $\mathrm{lm}(F_i) \neq \mathrm{lm}(F_j)$ for $i \neq j$. Let $\mathrm{lm}(F_i) = P_i$ for $i = 1, \ldots, m$. We have:*

$$\#\mathrm{supp}(D) \geq \# \bigcup_{i=1}^{m} \widetilde{\Lambda}_{P_i}$$

where $\widetilde{\Lambda}_P = \{K \in \Delta_{\prec_w}(I_q) \mid \exists N \in \Delta_\prec(I_q) \text{ such that } (P,N) \text{ is OWB and } lm(PN \text{ rem } \mathcal{G}) = K\}$.

If I and $\prec_w$ satisfy the order domain conditions then by Proposition 13 we can redefine the set $\widetilde{\Lambda}_P$ in the following way:

$$\widetilde{\Lambda}_P = \{N \in \Delta_{\prec_w}(I_q) \mid w(P) + w(N) \in w(\Delta_{\prec_w}(I_q))\}.$$

Also if we consider two $\mathbb{F}_q$-vector subspaces of R_q, $L_2 \subsetneq L_1$, then we obtain:

$$\begin{aligned} M_m(C(I,L_1),C(I,L_2)) \quad \geq \quad & \min\{\#\cup_{s=1}^{m} \widetilde{\Lambda}_{P_i} \mid \\ & P_i \in \Delta_{\prec_w}(I_q) \cap \mathrm{lm}(L_1), \\ & P_i \notin \mathrm{lm}(L_2) \text{ for any } i = 1,\ldots,m, \\ & P_i \neq P_j \text{ for } i \neq j\} \end{aligned}$$

for $m = 1,\ldots,\ell$, where $\ell = \dim(C(I,L_1)) - \dim(C(I,L_2))$ is their codimension.

1.3.2 Our improved Feng-Rao bound for primary affine variety codes

The order domain conditions historically [11, 21, 2, 8] were designed to support the Feng-Rao bounds and therefore it is not surprising that the bounds do not work very well without the order domain conditions. The improvement to the Feng-Rao bound that we introduced in Paper II allows us to consider relaxed conditions by producing good estimates in the case that the order domain condition (C1) is satisfied but (C2) is not.

Definition 15. Let $\mathcal{G}$ be a Gröbner basis for I_q with respect to a fixed arbitrary monomial ordering $\prec$. Write $\Delta_{\prec}(I_q) = \{M_1,\ldots,M_n\}$ with $M_1 \prec \cdots \prec M_n$. Let $\mathcal{I} = \{1,\ldots,n\}$ and consider $\mathcal{I}' \subseteq \mathcal{I}$. An ordered pair of monomials (M_i, M_j), $1 \leq i,j \leq n$ is said to be strongly one-way well-behaving (SOWB) with respect to $\mathcal{I}'$ if for all H with $\mathrm{Supp}(H) \subseteq \{M_s \mid s \in \mathcal{I}'\}$, $M_i \in \mathrm{Supp}(H)$ it holds that $\mathrm{lm}(M_iM_j \text{ rem } \mathcal{G}) = \mathrm{lm}(HM_j \text{ rem } \mathcal{G})$.

Remark 16. SOWB is a generalization of OWB. Concretely $(M_i,\ M_j)$ is OWB if and only if (M_i, M_j) is SOWB with respect to $\{1,\ldots,i\}$.

Theorem 17. *Let $\prec$ be a fixed arbitrary monomial ordering. Consider $\vec{c} = ev(\sum_{s=1}^{i} a_sM_s + I_q)$, $a_s \in \mathbb{F}_q$, $s = 1,\ldots,i$, and $a_i \neq 0$. Let v be an integer $0 \leq v < i$. We have $w_H(\vec{c}) \geq \sigma(i,v)$ where $\sigma(i,v) = \min\{\#\mathcal{L}(1),\ldots,\#\mathcal{L}(v+1)\}$. Here, for $t = 1,\ldots,v$*

$$\begin{aligned} \mathcal{L}(t) \quad = \quad & \big\{K \in \Delta_{\prec}(I_q) \mid \exists M_j \in \Delta_{\prec}(I_q) \textit{ such that either} \\ & (M_i, M_j) \textit{ is SOWB with respect to } \{1,\ldots,i-t,i\} \\ & \textit{and } lm(M_iM_j \textit{ rem } \mathcal{G}) = K \textit{ or} \\ & (M_{i-t}, M_j) \textit{ is SOWB with respect to } \{1,\ldots,i-t,i\} \\ & \textit{and } lm(M_{i-t}M_j \textit{ rem } \mathcal{G}) = K\big\}, \end{aligned}$$

and

$$\begin{aligned} \mathcal{L}(v+1) \quad = \quad & \big\{K \in \Delta_{\prec}(I_q) \mid \exists M_j \in \Delta_{\prec}(I_q) \textit{ such that } (M_i, M_j) \\ & \textit{is SOWB with respect to } \{1,\ldots,i-v-1,i\} \\ & \textit{and } lm(M_iM_j \textit{ rem } \mathcal{G}) = K\big\}. \end{aligned}$$

Given a code $C(I,L)$ write $\square_{\prec}(L) = \{M_{i_1}, \ldots, M_{i_{\dim(L)}}\}$ and choose numbers $v_{i_1}, \ldots, v_{i_{\dim(L)}}$ with $0 \leq v_{i_s} < i_s$, $s = 1, \ldots, \dim(L)$. The minimum distance of $C(I,L)$ is at least $\min\{\sigma(i_1, v_1), \ldots, \sigma(i_{\dim(L)}, v_{i_{\dim(L)}})\}$.

A generalization of this Theorem for subspaces of dimension 2 is described in Section 6 of Paper II. This is useful to bound the second RGHWs of affine variety codes. In Paper II we used the improved Feng-Rao bound to show that affine variety codes are better than their reputation.

1.3.3 Formulation at linear code level

The Feng-Rao bound and our improvement can be generalized for any linear code described by means of a generator matrix.

Consider a fixed ordered triple $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ where $\mathcal{U} = \{\vec{u}_1, \ldots, \vec{u}_n\}$, $\mathcal{V} = \{\vec{v}_1, \ldots, \vec{v}_n\}$, and $\mathcal{W} = \{\vec{w}_1, \ldots, \vec{w}_n\}$ are three (possibly different) bases for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. We shall always denote by $\mathcal{I}$ the set $\{1, \ldots, n\}$.

Definition 18. Consider a basis $\mathcal{A} = \{\vec{a}_1, \ldots, \vec{a}_n\}$ for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. We define the function $\bar{\rho}_{\mathcal{A}} : \mathbb{F}_q^n \to \{0, 1, \ldots, n\}$ as follows. For $\vec{c} \in \mathbb{F}_q \backslash \{\vec{0}\}$ we let $\bar{\rho}_{\mathcal{A}}(\vec{c}) = i$ if $\vec{c} \in \mathrm{Span}_{\mathbb{F}_q}\{\vec{a}_1, \ldots, \vec{a}_i\} \backslash \mathrm{Span}_{\mathbb{F}_q}\{\vec{a}_1, \ldots, \vec{a}_{i-1}\}$. Here, we used the notion $\mathrm{Span}_{\mathbb{F}_q} \emptyset = \{\vec{0}\}$. Finally, we let $\bar{\rho}_{\mathcal{A}}(\vec{0}) = 0$.

The component wise product plays a crucial role in the linear code enhancement of Theorem 10 and Theorem 17.

Definition 19. The component wise product of two vectors $\vec{u}$ and $\vec{v}$ in $\mathbb{F}_q^n$ is defined by $(u_1, \ldots, u_n) * (v_1, \ldots, v_n) = (u_1 v_1, \ldots, u_n v_n)$.

Definition 20. An ordered pair $(i,j) \subseteq \mathcal{I} \times \mathcal{I}$ is said to be one-way well-behaving (OWB) if $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ holds for all $i' \in \mathcal{I}$ with $i' < i$.

The following theorem is the generalization of the Feng-Rao bound for primary codes.

Theorem 21. *Consider $\vec{c} = \sum_{s=1}^{i} a_s \vec{u}_s$ with $a_s \in \mathbb{F}_q$, $s = 1, \ldots, i$, $a_i \neq 0$. We have*

$$w_H(\vec{c}) \geq \#\big\{ l \in \mathcal{I} \mid \exists j \in \mathcal{I} \ \text{ such that } \ \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l, (i,j) \ \text{ is OWB } \ \big\}.$$

For the computation of the RGHWs we rewrite the previous theorem in the following way.

Corollary 22. *Let $D \subseteq \mathbb{F}_q^n$ be a space of dimension at least 1. We have*

$$\#\mathrm{supp}(D) \geq \# \bigcup_{i \in \bar{\rho}_{\mathcal{W}}(D)} \Lambda_i$$

where $\Lambda_i = \{l \in \mathcal{I} \mid \exists j \in \mathcal{I}$ such that (i,j) is OWB and $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l\}$.

And thus we have that, given two linear codes in $\mathbb{F}_q^n$ $C_2 \subsetneq C_1$, the Feng-Rao bound for their RGHWs is:

$$M_m(C_1, C_2) \geq \min\{\# \bigcup_{i \in \bar{\rho}_{\mathcal{W}}(D)} \Lambda_i : D \text{ subspace of } C_1, \\ D \cap C_2 = \{\vec{0}\}, \dim(D) = m\}$$

for $m = 1, \ldots, \ell$ where $\ell = \dim(C_1) - \dim(C_2)$.

In Paper IV we use the Feng-Rao bound to bound the RGHWs of one-point algebraic geometric codes (in particular Hermitian codes).

A slight modification of Definition 20 and the above proof allows us to obtain further improvements.

Definition 23. Let $\mathcal{I}' \subseteq \mathcal{I}$. A pair $(i, j) \in \mathcal{I}' \times \mathcal{I}$ is called strongly one-way well-behaving (SOWB) with respect to $\mathcal{I}'$ if $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ holds for all $i' \in \mathcal{I}' \backslash \{i\}$.

The following theorem is the linear code interpretation of Theorem 17. Besides working for a larger class of codes, it is slightly stronger than the previous formulation. Concretely, what makes it stronger than Theorem 17 is the presence of the set $\hat{\mathcal{I}}$.

Theorem 24. *Consider a non-zero codeword $\vec{c} = \sum_{t=1}^{i} a_t \vec{u}_t$, $a_t \in \mathbb{F}_q$ for $t = 1, \ldots, i$, $a_i \neq 0$. Let v be an integer $0 \leq v < i$. Assume that for some set $\hat{\mathcal{I}} \subseteq \{1, \ldots, i-1\}$ we know a priori that $a_x = 0$ when $x \in \hat{\mathcal{I}}$. Let $z_1 < \cdots < z_s$ be the numbers in $\{z \in \{i-v, \ldots, i-1\} \mid z \notin \hat{\mathcal{I}}\}$. Write $\mathcal{I}^* = \{z \in \{1, \ldots, i-v-1\} \mid z \notin \hat{\mathcal{I}}\}$. We have $w_H(\vec{c}) \geq \bar{\sigma}(i, v)$ where $\bar{\sigma}(i, v) = \min\{\#\mathcal{L}'(1), \ldots, \#\mathcal{L}'(s+1)\}$. Here for $t = 1, \ldots, s$ we have*

$$\begin{aligned} \mathcal{L}'(t) &= \big\{l \in \mathcal{I} \mid \exists z \in \{z_{s-t+1}, i\} \text{ and } j \in \mathcal{I} \text{ such that} \\ &\quad \bar{\rho}_{\mathcal{W}}(\vec{u}_z * \vec{v}_j) = l, (z, j) \text{ is SOWB with respect to} \\ &\quad \mathcal{I}^* \cup \{z_1, \ldots, z_{s-t+1}, i\}\big\}, \\ &\quad \text{and} \\ \mathcal{L}'(s+1) &= \big\{l \in \mathcal{I} \mid \exists j \in \mathcal{I} \text{ such that } \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l \\ &\quad (i, j) \text{ is OWB with respect to } \mathcal{I}^* \cup \{i\}\big\}. \end{aligned}$$

To establish a lower bound on the minimum distance of a code C we choose for each $i \in \bar{\rho}_{\mathcal{U}}(C)$ the corresponding integer v_i, $0 \leq v_i < i$. The minimum distance is at least $\min\{\bar{\sigma}(i, v_i) \mid i \in \bar{\rho}_{\mathcal{U}}(C)\}$.

1.3.4 The Feng-Rao bound for dual linear codes

We now reformulate the Feng-Rao bound for dual linear codes. To work with them we need an additional definition.

Definition 25. Let an ordered triple of bases $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ be given. We define $m : \mathbb{F}_q^n \backslash \{\vec{0}\} \to \mathcal{I}$ by $m(\vec{c}) = l$ if l is the smallest number in $\mathcal{I}$ for which $\vec{c} \cdot \vec{w}_l \neq 0$. Let $D \subseteq \mathbb{F}_q^n$ be a subspace, we define $m(D) = \{m(\vec{c}) \mid \vec{c} \in D \backslash \{\vec{0}\}\}$.

Theorem 26. *For $\vec{c} \in \mathbb{F}_q^n \backslash \{\vec{0}\}$ write $l = m(\vec{c})$. The Hamming weight of $\vec{c}$ satisfies*

$$w_H(\vec{c}) \quad \geq \quad \#\{(i,j) \in \mathcal{I} \times \mathcal{I} \mid \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l \text{ and } (i,j) \text{ is OWB}\}$$

For the computation of the RGHWs we rewrite this theorem in the following way.

Corollary 27. *Let $D \subseteq \mathbb{F}_q^n$ be a space of dimension at least 1. We have*

$$\#\mathrm{supp}(D) \geq \# \bigcup_{l \in m(D)} V_l$$

where $V_l = \{i \in \mathcal{I} \mid \exists j \in \mathcal{I}$ such that (i,j) is OWB and $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l\}$.

Thus letting u be the largest element in $\bar{\rho}_{\mathcal{W}}(C_1 \backslash \{\vec{0}\})$, for $m = 1, \ldots, \dim C_1 - \dim C_2 = \dim C_2^\perp - \dim C_1^\perp$ we have

$$\begin{aligned} M_m(C_2^\perp, C_1^\perp) \quad \geq \quad & \min\{\# \cup_{s=1}^m V_{i_s} \mid 1 \leq i_1 < \cdots < i_m \leq u, \\ & \qquad i_1, \ldots, i_m \notin \bar{\rho}_{\mathcal{W}}(C_2)\}. \end{aligned}$$

1.3.5 Our improved Feng-Rao bound for dual linear code

As done in the primary case, it is possible to improve the Feng-Rao bound for dual codes.

Definition 28. Consider the numbers $1 \leq l, l+1, \ldots, l+g \leq n$. A set $\mathcal{I}' \subseteq \mathcal{I}$ is said to have the μ-property with respect to l with exception $\{l+1, \ldots, l+g\}$ if for all $i \in \mathcal{I}'$ there exists $j \in \mathcal{I}$ such that

(1a) $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l$,

(1b) for all $i' \in \mathcal{I}'$ with $i' < i$ one of the following conditions holds:

- $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < l$,
- $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) \in \{l+1, \ldots, l+g\}$.

Assume next that $l + g + 1 \leq n$. The set $\mathcal{I}'$ is said to have the relaxed μ-property with respect to $(l, l+g+1)$ with exception $\{l+1, \ldots, l+g\}$ if for all $i \in \mathcal{I}'$ there exists $j \in \mathcal{I}$ such that either conditions $(1a)$ and $(1b)$ above hold or

(2a) $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l + g + 1$,

(2b) (i,j) is one-way well-behaving with respect to $\mathcal{I}'$, i.e. for all $i' \in \mathcal{I}'$ with $i' < i$, $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$,

(2c) no $i' \in \mathcal{I}'$ with $i' < i$ satisfies $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) = l$.

Theorem 29. *Consider a non-zero codeword $\vec{c}$ and let $l = m(\vec{c})$. Choose a non-negative integer v such that $l + v \leq n$. Assume that for some indexes $x \in \{l + 1, \ldots, l + v\}$ we know a priori that $\vec{c} \cdot \vec{w}_x = 0$. Let $l'_1 < \cdots l'_s$ be the remaining indexes from $\{l + 1, \ldots, l + v\}$. Consider the sets $\mathcal{I}'_0, \mathcal{I}'_1, \ldots, \mathcal{I}'_s$ such that:*

- *$\mathcal{I}'_0$ has the μ-property with respect to l with exception $\{l + 1, \ldots, l + v\}$.*
- *For $i = 1, \ldots, s$, $\mathcal{I}'_i$ has the relaxed μ-property with respect to (l, l'_i) with exception $\{l + 1, \ldots, l'_i - 1\}$.*

We have

$$w_H(\vec{c}) \geq \min\{\#\mathcal{I}'_0, \#\mathcal{I}'_1, \ldots, \#\mathcal{I}'_s\}. \tag{1.2}$$

To establish a lower bound on the minimum distance of a code C we repeat the above process for each $l \in m(C)$. For each such l we choose a corresponding v, we determine sets $\mathcal{I}'_i$ as above and we calculate the right side of (1.2). The smallest value found constitutes a lower bound on the minimum distance.

The generalization for the computation of RGHWs is very technical. However in Proposition 22 of Paper III we give an estimation of the support size of a subspace of dimension 2.

Chapter 2

Applications

In the following part we show three applications of the bounds that we illustrated previously. The first section is dedicated to a new method for constructing small-bias spaces from Hermitian codes. In the second one we introduce the concept of secret sharing schemes and explain the importance of the RGHWs to evaluate the security of these schemes. Then using the footprint bound or the Feng-Rao bound we give some formulas to estimate or to compute the hierarchy of RGHWs of some linear codes. In the third section we show, using our improvements of the Feng-Rao bounds, that affine variety codes are better than their reputation.

2.1 New method for constructing small-bias spaces from Hermitian codes

To obtain our new method for constructing small-bias spaces from Hermitian codes we use the following ideal:

$$I_{q^2}^{(2)} := \langle X_1^{q+1} - Y_1^q - Y_1, X_2^{q+1} - Y_2^q - Y_2, X_1^{q^2} - X_1, Y_1^{q^2} - Y_1, X_2^{q^2} - X_2, Y_2^{q^2} - Y_2 \rangle$$

and the corresponding variety $\mathbb{V}_{\mathbb{F}_{q^2}}(I_{q^2}^{(2)}) = \{Q_1, \ldots, Q_{q^6}\}$.
As described in Definition 11 we define the monomial function $w^{(2)}$ given by $w^{(2)}(X_1) = (q, 0)$, $w^{(2)}(Y_1) = (q+1, 0)$, $w^{(2)}(X_2) = (0, q)$, and finally $w^{(2)}(Y_2) = (0, q+1)$. Let $\prec_{\mathbb{N}_0^2}$ be any monomial ordering on $\mathbb{N}_0^2$ and define $\prec_{w^{(2)}}$ as a weighted degree ordering.
For the code construction we need the following bijective evaluation map

$$\mathrm{ev} : \mathbb{F}_{q^2}[X_1, Y_1, X_2, Y_2]/I^{(2)} \to \mathbb{F}_{q^2}^{q^6}$$

given by $\mathrm{ev}(F + I_{q^2}^{(2)}) = (F(Q_1,), \ldots, F(Q_{q^6}))$. We consider a codeword $\vec{c} = \mathrm{ev}(F + I_{q^2}^{(2)})$ where without loss of generality we assume that $F \in \Delta_{\prec_{w^{(2)}}}(I_{q^2}^{(2)})$. We write $\lambda^{(2)} = (\lambda_1, \lambda_2) = w^{(2)}(\mathrm{lm}(F))$. Thus we obtain the estimate

$$\#\Delta_{\prec_{w^{(2)}}}(\langle F(X_1, Y_1, X_2, Y_2)\rangle + I_{q^2}^{(2)}) \quad \leq \quad q^6 - (q^3 - \lambda_1)(q^3 - \lambda_2).$$

Hence by the footprint bound we obtain $w_H(\vec{c}) \geq (q^3 - \lambda_1)(q^3 - \lambda_2)$.

Consider the code $\widetilde{E}(\delta)$ which is to Hermitian codes what Massey-Costello-Justesen codes [16] are to Reed-Solomon codes

$$\begin{aligned}\widetilde{E}(\delta) \quad := \quad & \mathrm{Span}_{\mathbb{F}_{q^2}} \Big\{ \mathrm{ev}(X_1^{i_1} Y_1^{j_1} X_2^{i_2} Y_2^{j_2} + I_{q^2}^{(2)}) \mid 0 \leq i_1, i_2 < q^2, \\ & 0 \leq j_1, j_2 < q, (q^3 - w(X_1^{i_1} Y_1^{j_1}))(q^3 - w(X_2^{i_2} Y_2^{j_2})) \geq \delta \Big\}.\end{aligned}$$

Proposition 30. *Assume $\delta \geq T$ where $T = q^3 - g$ where g is the genus of the Hermitian curve. The parameters of $\widetilde{E}(\delta)$ are $[n = q^6, k \geq T^2 - \delta + \delta \ln(\delta/T^2), d \geq \delta]$.*

2.1.1 Epsilon balanced code

In this section we show that by using the previous construction as outer code we obtain a good ϵ-bias space. We start by giving the definition of ϵ-bias space and ϵ-balanced code, then in Theorem 33 we show that these definitions are strongly correlated.

Definition 31. A multiset[1] $\mathcal{X} \subseteq \mathbb{F}_2^k$ is called an ϵ-bias space if

$$\frac{1}{\#\mathcal{X}} \left| \sum_{\vec{x} \in \mathcal{X}} (-1)^{\sum_{i \in T} x_i} \right| \leq \epsilon$$

holds for every non-empty indexed set $T \subseteq \{1, \ldots, k\}$.

Definition 32. A binary $[n, k]$ code is said to be ϵ-balanced if every non-zero code word $\vec{c}$ satisfies

$$\frac{1 - \epsilon}{2} \leq \frac{w_H(\vec{c})}{n} \leq \frac{1 + \epsilon}{2}.$$

We can create ϵ-bias spaces using the generator matrix of an ϵ-balanced code. In fact we have that:

Theorem 33. *Let G be a generator matrix for an ϵ-balanced binary $[n, k]$ code. The columns of G constitute an ϵ-bias space $\mathcal{X} \subseteq \mathbb{F}_2^k$ of size n. Similarly, using the elements of an ϵ-bias space $\mathcal{X}$ as columns of a generator matrix an ϵ-balanced code is derived.*

A standard construction from [1] tells us how to make small-balanced codes (meaning ϵ-biased codes with ϵ small):

Theorem 34. *Let $q = 2^s$ for some positive integer s and consider a q-ary $[N, K, D]$ code C. Let C_s be the (binary) $[2^s, s]_2$ Walsh-Hadamard code. The concatenated code derived by using C as outer code and C_s as inner code is an $\epsilon = (N - D)/N$-balanced binary code of length $n = N2^s$ and dimension $k = Ks$.*

[1] A multiset is a generalization of the notion of a set in which the elements can be repeated.

The literature contains various examples of small-bias spaces that cannot all be compared to each other. We refer to [4, Sec. 1] for more details. In the following table we concentrate on important families of multisets for which comparison can be made. Note that a family of ϵ-bias spaces is considered to behave well if when given ϵ and k the size of $\mathcal{X}$ is small. Our construction used as outer code gives us in some range one of the best solution.

Outer code	$\#\mathcal{X}$
Reed-Solomon codes (RS)	$\mathcal{O}\left(\frac{k^2}{\epsilon^2 \ln^2(k/\epsilon)}\right)$
Algebraic geometric codes (AG)	$\mathcal{O}\left(\frac{k}{\epsilon^3 \ln(1/\epsilon)}\right)$
Hermitian codes (BT)	$\mathcal{O}\left(\left(\frac{k}{\epsilon^2 \ln(1/\epsilon)}\right)^{\frac{5}{4}}\right)$
Norm-Trace codes	$\mathcal{O}\left(\left(\frac{k}{\epsilon^{l-\sqrt{l}} \ln(1/\epsilon)}\right)^{\frac{l+1}{l}}\right)$
Our construction (OC)	$\mathcal{O}\left(\left(\frac{k}{\epsilon+(1-\epsilon)\ln(1-\epsilon)}\right)^{\frac{4}{3}}\right)$
Bound	$\#\mathcal{X}$
Gilbert-Varshamov (GV)	$\mathcal{O}\left(\frac{k}{\epsilon^2}\right)$
Linear programming (LP)	$\mathcal{O}\left(\frac{k}{\epsilon^2 \log(1/\epsilon)}\right)$

One way of comparing the above results is to choose $\epsilon = k^{-\alpha}$, $\alpha \in \mathbb{R}^+$ and then to take the logarithm with base k. The big O notation suggests that we then let k go to infinity. The origin of this point of view is [4, Sec. 1].

Outer code	$\log_k(\#\mathcal{X})$
Reed-Solomon codes (RS)	$2 + 2\alpha + o(1)$ for all $\alpha \in \mathbb{R}^+$
AG codes (AG)	$1 + 3\alpha + o(1)$ for all $\alpha \in \mathbb{R}^+$
Hermitian codes (BT)	$\frac{5}{4} + \frac{5}{2}\alpha + o(1)$ for all $\alpha > \frac{1}{2}$
Norm-Trace codes	$\frac{l+1}{l}(1 + \alpha(l - \sqrt{l})) + o(1)$ for $l = 4, 5, \ldots$, and for all $\alpha \geq \frac{\sqrt{l}}{l}$
Our construction (OC)	$\frac{4}{3} + \frac{8}{3}\alpha + o(1)$ for all $\alpha \in \mathbb{R}^+$
Bound	$\log_k(\#\mathcal{X})$
Gilbert-Varshamov (GV)	$1 + 2\alpha + o(1)$ for all $\alpha \in \mathbb{R}^+$
Linear programming (LP)	$1 + 2\alpha + o(1)$ for all $\alpha \in \mathbb{R}^+$

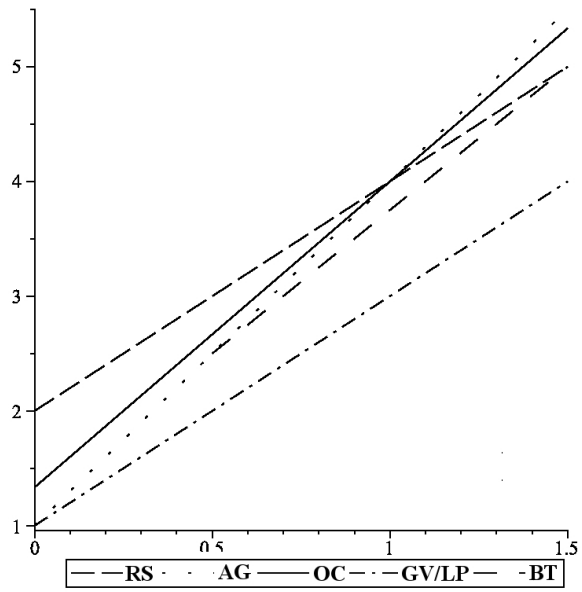

Figure 2.1: Comparison of various constructions: First axis is α, second axis corresponds to $\log_k(\#\mathcal{X})$ when $k \to \infty$.

2.2 Relative generalized Hamming weights

2.2.1 Linear secret sharing schemes

In this section we show how to compute or estimate the RGHWs of different linear codes. We start by introducing the ramp secret sharing schemes so that the reader will understand the importance of the hierarchy of the RGHWs of linear codes.

Definition 35. Let n, ℓ, t and r be positive integers, $t < r$ and $\ell \leq n$. A ramp secret sharing scheme with t-privacy and r-reconstruction is an algorithm that given an input $\vec{s} \in \mathbb{F}_q^\ell$, called a secret, outputs a vector $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, the vector of shares that we want to share among n players, such that given a collection of shares $\{x_i \mid i \in \mathcal{I}\}$, $\mathcal{I} \subseteq \{1, \ldots, n\}$; one has no information about $\vec{s}$ if $\#\mathcal{I} \leq t$ and one can recover $\vec{s}$ if $\#\mathcal{I} \geq r$.

We shall always assume that t is largest possible and that r is smallest possible such that the above holds.

A linear ramp secret sharing scheme with n participants and shares belonging to $\mathbb{F}_q$ can be described as a coset construction C_1/C_2 where $C_2 \subsetneq C_1 \subseteq \mathbb{F}_q^n$ are linear codes over $\mathbb{F}_q$ [5]. Given C_1, C_2 as above let $L \subseteq \mathbb{F}_q^n$ be such that $C_1 = L \oplus C_2$ (here, $\oplus$ denotes the direct sum). We shall call $\ell = \dim(L) = \dim(C_1) - \dim(C_2)$ the codimension of C_1 and C_2. We consider a secret $\vec{s} \in \mathbb{F}_q^\ell$, a vector space isomorphism $\psi : \mathbb{F}_q^\ell \to L$ and $\vec{c}_2 \in C_2$, chosen randomly (uniformly distributed). Finally

we consider $\vec{x} = \psi(\vec{s}) + \vec{c}_2 \in C_1$. The n shares consist of the n coordinates of $\vec{x}$.

We now generalize the notation of t-privacy and r-reconstruction.

Definition 36. We say that a ramp secret sharing scheme has $(t_1, \ldots, t_\ell)$-privacy and $(r_1, \ldots, r_\ell)$-reconstruction if $t_1, \ldots, t_\ell$ are chosen largest possible and $r_1, \ldots, r_\ell$ are chosen smallest possible such that for $m = 1, \ldots, \ell$:

- an adversary cannot obtain m q-bits of information about $\vec{s}$ with any t_m shares,
- it is possible to recover m q-bits of information about $\vec{s}$ with any collection of r_m shares.

In particular, one has $t = t_1$ and $r = r_\ell$.

From [3, Th. 6.7],[13, Th. 4] and Theorem 6 of Paper IV we have the following characterization of these parameters:

Theorem 37. *Let C_1/C_2, where $\dim C_1 - \dim C_2 = \ell$, be a linear ramp secret sharing scheme with $(t_1, \ldots, t_\ell)$-privacy and $(r_1, \ldots, r_\ell)$-construction. Then for $m = 1, \ldots, \ell$ we have $t_m = M_m(C_2^\perp, C_1^\perp) - 1$ and $r_m = n - M_{\ell-m+1}(C_1, C_2) + 1$.*

Unfortunately, it is not easy to find the hierarchy of RGHWs of two general linear codes and only for a few classes of codes these parameters have been found or estimated. Actually – until recently – only for a single class of codes the parameters were known, namely MDS codes for which the situation is particular simple [15].

In the next sections we show how to compute or estimates the RGHWs of one-point algebraic geometric codes (in particular Hermitian codes) and q-ary Reed-Muller codes.

2.2.2 One-point algebraic geometric codes

Given an algebraic function field F of transcendence degree one, let $P_1, \ldots, P_n$, Q be distinct rational places. For $f \in F$ write $\rho(f) = -\nu_Q(f)$, where ν_Q is the valuation at Q, and denote by $H(Q)$ the Weierstrass semigroup of Q. That is, $H(Q) = \rho\big(\cup_{\mu=0}^{\infty} \mathcal{L}(\mu Q)\big)$. In the following let $\{f_\lambda \mid \lambda \in H(Q)\}$ be any fixed basis for $R = \cup_{\mu=0}^{\infty} \mathcal{L}(\mu Q)$ with $\rho(f_\lambda) = \lambda$ for all $\lambda \in H(Q)$. Let $D = P_1 + \cdots + P_n$ and define

$$\begin{aligned} H^*(Q) &= \{\mu \mid C_{\mathcal{L}}(D, \mu Q) \neq C_{\mathcal{L}}(D, (\mu - 1)Q)\} \\ &= \{\gamma_1, \ldots, \gamma_n\} \subsetneq H(Q). \end{aligned}$$

Here, the enumeration is chosen such that $\gamma_1 < \cdots < \gamma_n$. Consider the map $\mathrm{ev} : F \to \mathbb{F}_q^n$ given by $\mathrm{ev}(f) = (f(P_1), \ldots, f(P_n))$.

As proved in Section 5 of Paper IV using the Feng-Rao bound we can define the function Z that it is useful to bound the RGHWs of one-point algebraic geometric codes.

Definition 38. Consider a numerical semigroup Γ and a positive integer μ. Define $Z(\Gamma,\mu,1)=0$ and for $1<m\leq\mu$.

$$\begin{aligned} Z(\Gamma,\mu,m) &= \min\big\{\#\{\alpha\in\cup_{s=1}^{m-1}(i_s+\Gamma)\mid\alpha\notin\Gamma\}\mid \\ &\qquad -\mu+1\leq i_1<\cdots<i_{m-1}\leq -1\big\}. \end{aligned}$$

Theorem 39. *Let μ_1,μ_2 be positive integers with $\mu_2<\mu_1$. For $m=1,\ldots,\dim C_{\mathcal{L}}(D,\mu_1Q)-\dim C_{\mathcal{L}}(D,\mu_2Q)$ we have*

$$M_m(C_{\mathcal{L}}(D,\mu_1Q),C_{\mathcal{L}}(D,\mu_2Q))\geq n-\mu_1+Z(H(Q),\mu,m)$$

where $\mu=\mu_1-\mu_2$.

Using the Feng-Rao bound for dual codes we can also obtain an estimate of the RGHWs of the duals of one-point algebraic geometric codes

Theorem 40. *Let μ_1,μ_2 and m be as in Theorem 39. We have*

$$\begin{aligned} & M_m(C_{\mathcal{L}}^{\perp}(D,\mu_2Q),C_{\mathcal{L}}^{\perp}(D,\mu_1Q)) \\ \geq\ & \min\Big\{\#\big(H(Q)\cap\big(\cup_{s=1}^{m}(\gamma_{i_s}-H(Q))\big)\big) \\ & \qquad\mid\gamma_{i_1},\ldots,\gamma_{i_m}\in H^*(Q),\mu_2<\gamma_{i_1}<\cdots<\gamma_{i_m}\leq\mu_1\Big\}. \end{aligned}$$

2.2.3 Hermitian codes

In this section we focus when our one-point algebraic geometric code is a Hermitian code. The Hermitian function field over $\mathbb{F}_{q^2}$ is given by the equation $x^{q+1}-y^q-y$ and it possesses exactly q^3+1 rational places which we denote $P_1,\ldots,P_{q^3},Q$ – the last being the pole of x. The Weierstrass semigroup of Q, $H(Q)=\langle\rho(x)=q,\rho(y)=q+1\rangle$, has $g=q(q-1)/2$ gaps and conductor $c=q(q-1)$. Let $D=P_1+\cdots+P_{q^3}$. In the following by a Hermitian code [23, 22] we mean a code of the form $C_{\mathcal{L}}(D,\mu Q)$. Clearly, this code is of length $n=q^3$. As is well-known the dual of a Hermitian code is a Hermitian code.

Theorem 41. *Consider the Hermitian curve $x^{q+1}-y^q-y$ over $\mathbb{F}_{q^2}$. Let $P_1,\ldots,P_{n=q^3}$, and Q be the rational places and $D=P_1+\cdots+P_n$. Let μ_1,μ_2 be non-negative integers with $1\leq\mu_1-\mu_2\leq q+1$. For $1\leq m\leq\dim(C_{\mathcal{L}}(D,\mu_1Q))-\dim(C_{\mathcal{L}}(D,\mu_2Q))$ we have:*

$$M_m(C_{\mathcal{L}}(D,\mu_1Q),C_{\mathcal{L}}(D,\mu_2Q))\geq n-\mu_1+q(m-1)-\frac{(m-2)(m-1)}{2}.$$

The equality holds if $c-1\leq\mu_2$ and $\mu_1<n-c$ (recall that the conductor $c=q(q-1)$). Further in this case we have that $\dim(C_{\mathcal{L}}(D,\mu_1Q))-\dim(C_{\mathcal{L}}(D,\mu_2Q))=\mu_1-\mu_2$.

2.2.4 q-ary Reed-Muller codes

Let u and s be positive integers, and write $n = q^s$. To define a q-ary Reed-Muller codes we enumerate the elements of $(\mathbb{F}_q)^s$ as $\{P_1, \ldots, P_n\}$ and consider $\mathrm{ev} : \mathbb{F}_q[X_1, \ldots, X_s] \to \mathbb{F}_q^n$, $\mathrm{ev}(f) = (f(P_1), \ldots, f(P_n))$. The q-ary Reed-Muller code of order u in s variables is defined by

$$\begin{aligned} RM_q(u, s) &= \{\mathrm{ev}(f) : f \in \mathbb{F}_q[X_1, \ldots, X_s], \deg(f) \leq u\} \\ &= \mathrm{span}_{\mathbb{F}_q}\{\mathrm{ev}(X_1^{a_1} \cdots X_s^{a_s}) \mid 0 \leq a_1, \ldots, a_s < q, a_1 + \cdots + a_s \leq u\}. \end{aligned}$$

We shall use the convention $\deg(0) = -1$ and $\mathrm{span}_{\mathbb{F}_q}\emptyset = \{\vec{0}\}$. Hence $RM_q(-1, s) = \{\vec{0}\}$.

Using the footprint bound we are able to find the hierarchy of the RGHWs of q-ary Reed-Muller codes.

Definition 42. We write

$$Q_q^s = \{(a_1, \ldots, a_s) \in \mathbb{N}_0^s \mid 0 \leq a_i < q, i = 1, \ldots, s\}$$

and given $\vec{a} = (a_1, \ldots, a_s) \in Q_q^s$, we call $\deg(\vec{a}) = \deg(\vec{X}^{\vec{a}}) = \sum_{t=1}^s a_t$ the degree of $\vec{a}$. Let a, b be two integers with $0 \leq a \leq b \leq s(q-1)$, then we define

$$F_q((a, b), s) = \{\vec{a} \in Q_q^s \mid a \leq \deg(\vec{a}) \leq b\}.$$

Theorem 43. *Given $C_2 = RM_q(u_2, s) \subsetneq C_1 = RM_q(u_1, s)$, let $\vec{a}$ be the m-th element in $F(u_2 + 1, u_1)$ with respect to the anti lexicographic ordering. Because $F(u_2 + 1, u_1) \subseteq F(0, u_1) \subseteq Q_q^s$ there exist r and t such that $\vec{a}$ is the r-th element in $F(0, u_1)$ and the t-th element in Q_q^s with respect to the anti lexicographic ordering. We have*

$$M_m(C_1, C_2) = t - r + m.$$

To compute the GHWs of C_1 is enough to suppose that $C_2 = \{\vec{0}\}$. In this case $u_2 = -1$ and $r = m$, thus for $r = 1, \ldots, \ell$ we obtain $d_r(C_1) = t$ where t is the index in Q_q^s of the r-th element of $F(0, u_1)$.

2.3 Affine variety codes are better than their reputation

As mentioned our improvement of the Feng-Rao bound is effective for affine variety codes where the order domain condition (C1) is satisfied, but the order domain condition (C2) is not. A particular simple class of curves that satisfy the order domain conditions are the well-known C_{ab} curves. They were introduced by Miura in [18, 19, 20] to facilitate the use of the Feng-Rao bound for dual codes.

We begin by giving the definition of generalized C_{ab} polynomials and $(\mathbb{F}_{p^m}, \mathbb{F}_p)$ polynomials. Then we give a proposition that shows how to obtain $(\mathbb{F}_{p^m}, \mathbb{F}_p)$ polynomials.

Definition 44. Let $w(X) = \frac{b}{\gcd(a,b)}$ and $w(Y) = \frac{a}{\gcd(a,b)}$ where a and b are two different positive integers. Given a field k, let $F(X,Y) = X^a + \alpha Y^b + R(X,Y) \in k[X,Y]$, $\alpha \in k\backslash\{0\}$, be such that all monomials in the support of R have smaller weight than $w(X^a) = w(Y^b) = \frac{ab}{\gcd(a,b)}$. Then $F(X,Y)$ is called a generalized C_{ab} polynomial.
If $k = \mathbb{F}_q$ and $F(X,Y)$ is a generalized C_{ab} polynomial with aq zeros, then we say that F is an optimal generalized C_{ab} polynomial.

The generalized C_{ab} polynomials with aq zeros are called optimal because a bivariate polynomial with leading monomial X^a can have no more zeros over $\mathbb{F}_q$, as is seen from the footprint bound in Theorem 6.

Definition 45. Let m be an integer, $m \geq 2$. A polynomial $F(X) \in \mathbb{F}_{p^m}[X]$ is called an $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomial if $F(\gamma) \in \mathbb{F}_p$ holds for all $\gamma \in \mathbb{F}_{p^m}$.

Proposition 46. *Let $C_{i_1}, \ldots, C_{i_t}$ be the different cyclotomic cosets modulo $p^m - 1$ (multiplication by p). Here, for $s = 1, \ldots, t$ it is assumed that i_s is chosen as the smallest element in the given coset. For $s = 1, \ldots, t$, $F_{i_s}(X) = \sum_{l \in C_{i_s}} X^l$, is an $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomial. Furthermore, the polynomial X^{p^m-1} is an $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomial.*

Generalized C_{ab} polynomials $F(X,Y) = G(X) - H(Y)$ can be obtained using the trace polynomial $G(X)$ of degree a and an $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomial $H(Y)$ of degree b different from the trace polynomial as described in Proposition 46. Furthermore these polynomials have aq zeros and thus they are optimal. Using these polynomials we obtain codes for which we can easily apply our improved Feng-Rao bound.

Theorem 47. *Let I_q be defined from an optimal generalized C_{ab} polynomial with aq zeros and let the weights $w(X)$ and $w(Y)$ be as in Definition 44. Let $\prec_w$ be a weighted degree ordering as defined in Definition 11. Consider $\vec{c} = \mathrm{ev}(f + I_q)$, we can assume without losing of generality $\mathrm{lm}(f) \in \Delta_w(I_q)$. Write $lm(f) = X^{\alpha_1} Y^{\alpha_2}$ and $T = \alpha_1$ rem $w(Y)$. We have that*

$$w_H(\vec{c}) \geq (a - \alpha_1)(q - \alpha_2) + \epsilon \text{ where}$$

$$\epsilon = \begin{cases} 0 & \text{if } q - b \leq \alpha_2 < q \\ T(q - \alpha_2 - b) & \text{if } 0 \leq \alpha_1 \leq a - w(Y) \\ & \text{and } 0 \leq \alpha_2 < q - b \\ \alpha_1(q - \alpha_2 - b) & \text{if } a - w(Y) < \alpha_1 < a \text{ and} \\ & q - w(X) - \alpha_1 \frac{b - w(X)}{a - w(Y)} < \alpha_2 < q - b \\ T(q - \alpha_2 - w(X)) & \text{if } a - w(Y) < \alpha_1 < a \text{ and} \\ & 0 \leq \alpha_2 \leq q - w(X) - \alpha_1 \frac{b - w(X)}{a - w(Y)}. \end{cases}$$

Remark 48. If for codes from optimal generalized C_{ab} polynomials rather than applying the bound in Theorem 17 we apply the footprint bound then the ϵ in

Theorem 47 should be equal 0. If we apply the Feng-Rao bound (Theorem 10) with OWB then the ϵ in Theorem 47 should be replaced with:

$$\begin{cases} 0 & \text{if } q-b \leq \alpha_2 < q \\ T(q-\alpha_2-b) & \text{and } 0 \leq \alpha_2 < q-b. \end{cases}$$

We see that our new bound improves the Feng-Rao bound by

$$\begin{cases} 0 & \text{if } q-b \leq \alpha_2 < q \\ & \text{or } 0 \leq \alpha_1 \leq a-w(Y) \\ (\alpha_1 - T)(q-\alpha_2-b) & \text{if } a-w(Y) < \alpha_1 < a \text{ and} \\ & q-w(X)-\alpha_1\frac{b-w(X)}{a-w(Y)} < \alpha_2 < q-b \\ T(b-w(X)) & \text{if } a-w(Y) < \alpha_1 < a \text{ and} \\ & 0 \leq \alpha_2 \leq q-w(X)-\alpha_1\frac{b-w(X)}{a-w(Y)}. \end{cases}$$

Chapter 3

Summary of the papers

3.1 Paper I

In this paper we propose a new method for constructing small-bias spaces through a combination of Hermitian codes as explained in Section 2.1.1 of the introduction. Using the footprint bound we prove that our construction has competitive performance with more known codes, as one-point algebraic geometric codes. In particular we illustrate that although for $\alpha < 1$ our construction performs worse than the spaces coming from the algebraic geometric codes, we have that to build spaces with $\alpha < \frac{1}{2}$ from the one-point algebraic geometric construction requires quite a number of operations. In contrast, our construction is considerable fast. We prove that the small bias-spaces obtained in this paper performs better than the ones related to norm-traces codes reported in [17].

3.2 Paper II and III

These two papers focus on the improvements on the Feng-Rao bounds for primary and dual codes, respectively. Paper II starts by showing that the Feng-Rao bound with one-way well-behaving property is a powerful tool to bound the Hamming weight of a word in primary affine variety codes that satisfy the order domain conditions. We show that we can avoid the second order domain condition without losing significant performance for the minimum distance. To prove this fact we use our improved Feng-Rao bound based on the strongly one-way well-behaving property, a generalization of the one-way well behaving property. As mentioned in Section 2.3 of the introduction we prove that for a family of primary affine variety codes based on C_{ab} polynomials it is possible to obtain a formula for our improved bound. In section 5 of paper II we give an example which illustrates that the construction of a good affine variety code is not always trivial. We conclude the discussion on affine variety codes with a proposition that explains how to bound the second generalized Hamming weight of affine variety codes. The paper continues

showing that it is possible to use our improvement at linear code level and that there exist a related bound for dual codes.
Paper III is focused on the improved Feng-Rao bound for dual codes. After introducing the Feng-Rao bound with one-way well-behaving property, we show that we can improve it in similar way as we did for primary codes. The last section is dedicated to several examples that illustrate that our improved bound gives interesting results.

3.3 Paper IV and V

These two papers are focused on the computation of the RGHWs of some linear codes. Paper IV introduces the linear secret sharing schemes and explains why the computation of RGHWs is crucial to evaluate the security of these cryptographic systems. The paper continues by applying the Feng-Rao bound with one-way well-behaving property to bound the RGHWs of one-point algebraic geometric codes, in particular Hermitian codes. Using the footprint bound Paper V continues the analysis of the previous paper computing precisely the RGHWs of q-ary Reed-Muller codes. The main result is given in Theorem 20 and we propose an algorithm to use it in an efficient way. The last section gives several formulas for the RGHWs of q-ary Reed-Muller codes in two variables.

Bibliography

[1] N. Alon, O. Goldreich, J. Håstad, and R. Peralta. Simple constructions of almost k-wise independent random variables. *Random Structures & Algorithms*, 3(3):289–304, 1992.

[2] H. E. Andersen and O. Geil. Evaluation codes from order domain theory. *Finite Fields Appl.*, 14(1):92–123, 2008.

[3] T. Bains. Generalized Hamming weights and their applications to secret sharing schemes. *Master's thesis*, 2008.

[4] A. Ben-Aroya and A. Ta-Shma. Constructing small-bias sets from algebraic-geometric codes. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 191–197. IEEE, 2009.

[5] H. Chen, R. Cramer, S. Goldwasser, R. De Haan, and V. Vaikuntanathan. Secure computation from random error correcting codes. In *Advances in Cryptology-EUROCRYPT 2007*, pages 291–310. Springer, 2007.

[6] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*, volume 10. Springer, 1997.

[7] J. Fitzgerald and R. F. Lax. Decoding affine variety codes using Gröbner bases. *Designs, Codes and Cryptography*, 13(2):147–158, 1998.

[8] O. Geil. Evaluation codes from an affine variety code perspective. In E. Martínez-Moro, C. Munuera, and D. Ruano, editors, *Advances in algebraic geometry codes*, volume 5 of *Coding Theory and Cryptology*, pages 153–180. World Scientific, Singapore, 2008.

[9] O. Geil and T. Hoholdt. Footprints or generalized Bezout's theorem. *Information Theory, IEEE Transactions on*, 46(2):635–641, 2000.

[10] T. Helleseth, T. Kløve, and J. Mykkeltveit. The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/N)$. *Discrete Mathematics*, 18(2):179–211, 1977.

[11] T. Høholdt, J. H. van Lint, and R. Pellikaan. Algebraic geometry codes. *Handbook of coding theory*, 1(Part 1):871–961, 1998.

[12] T. Kløve. The weight distribution of linear codes over $GF(q^l)$ having generator matrix over $GF(q)^*$. *Discrete Mathematics*, 23(2):159–168, 1978.

[13] J. Kurihara, T. Uyematsu, and R. Matsumoto. Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 95(11):2067–2075, 2012.

[14] Z. Liu, W. C. Zihui, and Y. Luo. The relative generalized Hamming weight of linear q-ary codes and their subcodes. *Designs, Codes and Cryptography*, 48(2):111–123, 2008.

[15] Y. Luo, C. Mitrpant, A. H. Vinck, and K. Chen. Some new characters on the wire-tap channel of type II. *Information Theory, IEEE Transactions on*, 51(3):1222–1229, 2005.

[16] J. L. Massey, D. J. Costello, and J. Justesen. Polynomial weights and code constructions. *Information Theory, IEEE Transactions on*, 19(1):101–110, 1973.

[17] G. L. Matthews and J. D. Peachey. Small-bias sets from extended norm-trace codes. In *Theory and Applications of Finite Fields: The 10th International Conference on Finite Fields and Their Applications, July 11-15, 2011, Ghent, Belgium*, volume 579, page 143. American Mathematical Soc., 2012.

[18] S. Miura. Algebraic geometric codes on certain plane curves. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 76(12):1–13, 1993. (in Japanese).

[19] S. Miura. *Study of Error-Correcting Codes based on Algebraic Geometry*. PhD thesis, Univ. Tokyo, 1997. (in Japanese).

[20] S. Miura. Linear codes on affine algebraic curves. *Trans. IEICE*, J81-A(10):1398–1421, 1998. (in Japanese).

[21] R. Pellikaan. On the existence of order functions. *Journal of Statistical Planning and Inference*, 94(2):287–301, 2001.

[22] H. Stichtenoth. A note on Hermitian codes over $GF(q^2)$. *Information Theory, IEEE Transactions on*, 34(5):1345–1348, 1988.

[23] H. J. Tiersma. Remarks on codes from Hermitian curves. *IEEE Trans. Inform. Theory*, 33(4):605–609, 1987.

[24] V. K. Wei. Generalized Hamming weights for linear codes. *Information Theory, IEEE Transactions on*, 37(5):1412–1418, 1991.

SCIENTIFIC RESULTS

PAPER I

A new method for constructing small-bias spaces from Hermitian codes

Geil Olav Martin Stefano Matsumoto Ryutaroh

Geil Olav, Martin Stefano and Matsumoto Ryutaroh, "A new method for constructing small-bias spaces from Hermitian codes", *Journal reference WAIFI 2012*, LNCS vol. 7369, pp. 29-44, 2012, preprint at arXiv: 1203.0491v1 [cs.IT], DOI: 10.1007/978-3-642-31662-3_3

A new method for constructing small-bias spaces from Hermitian codes

Olav Geil[11], Stefano Martin[21], and Ryutaroh Matsumoto[31,2]

[1]Department of Mathematical Sciences, Aalborg University
[2] Department of Communications and Integrated Systems, Tokyo Institute of Technology, Japan

[1]olav@math.aau.dk
[2]stefano@math.aau.dk
[3]ryutaroh@rmatsumoto.org

Abstract

We propose a new method for constructing small-bias spaces through a combination of Hermitian codes. For a class of parameters our multisets are much faster to construct than what can be achieved by use of the traditional algebraic geometric code construction. So, if speed is important, our construction is competitive with all other known constructions in that region. And if speed is not a matter of interest the small-bias spaces of the present paper still perform better than the ones related to norm-trace codes reported in [12].

Keywords: Small-bias space, balanced code, Gröbner basis, Hermitian code.

Chapter 1

Introduction

Let $\vec{X} = (X_1, \ldots, X_k)$ be a random vector that takes on values in $\mathbb{F}_2^k$. As shown by Vazirani [17] the variables $X_1, \ldots, X_k$ are independent and uniformly distributed if and only if

$$\text{Prob}\left(\sum_{i\in T} X_i = 0\right) = \text{Prob}\left(\sum_{i\in T} X_i = 1\right) = \frac{1}{2} \tag{1.1}$$

holds for every non-empty set of indexes $T \subseteq \{1, \ldots, k\}$. In particular, if (1.1) is to hold for a space $\mathcal{X} \subseteq \mathbb{F}_2^k$ then necessarily $\mathcal{X}$ must be equal to $\mathbb{F}_2^k$. There is a need for much smaller spaces $\mathcal{X} \subseteq \mathbb{F}_2^k$ with statistical properties close to that of (1.1). In the following by a space we will mean a multiset $\mathcal{X}$ with elements from $\mathbb{F}_2^k$ (this we write $\mathcal{X} \subseteq \mathbb{F}_2^k$). The multiset $\mathcal{X}$ is made into a probability space by adjoining to each element $\vec{x} \in \mathcal{X}$ the probability $p(\vec{x}) = i(\vec{x})/|\mathcal{X}|$ where $i(\vec{x})$ denotes the number of times $\vec{x}$ appears in $\mathcal{X}$. As a measure for describing how close a given space $\mathcal{X}$ is to the above situation with respect to randomization, Naor and Naor [15], and Alon et. al. [1] introduced the concept of ϵ-biasness [15, Def. 3]. (See also [14]).

Definition 1. *A multiset $\mathcal{X} \subseteq \mathbb{F}_2^k$ is called an ϵ-bias space if*

$$\frac{1}{|\mathcal{X}|}\left|\sum_{\vec{x}\in\mathcal{X}} (-1)^{\sum_{i\in T} x_i}\right| \leq \epsilon \tag{1.2}$$

holds for every non-empty index set $T \subseteq \{1, \ldots, k\}$.

Clearly, the ϵ in Definition 1 can be taken to be a number between 0 and 1. Good randomization properties are achieved when ϵ is close to 0 as (1.2) becomes (1.1) when $\epsilon = 0$. Multisets with ϵ small are called small-bias spaces. Citing [15, Abstract] they are used to construct almost k-wise independent random variables. From [15, Abstract] we have the following list of applications:

- Derandomization of algorithms.
- Reducing the number of random bits required by certain randomized algorithms, e.g., verification of matrix multiplication.

- Exhaustive testing of combinatorial circuits.
- Communication complexity: Two parties can verify equality of strings with high probability exchanging only a logarithmic number of bits.
- Hash functions.

Further examples can be found in [15, Sec. 10].
Rather than saying that a multiset is an ϵ-bias space we will often just say that it is ϵ-biased. Another name for ϵ-bias space is ϵ-bias set [2, Def. 1] and [12, Def. 1.1]. This notion may be a little misleading as the item under consideration is actually a multiset.
One way of constructing small-bias spaces is through the use of error-correcting codes.

Definition 2. *A binary $[n, k]$ code is said to be ϵ-balanced if every non-zero code word $\vec{c}$ satisfies*

$$\frac{1-\epsilon}{2} \leq \frac{w_H(\vec{c})}{n} \leq \frac{1+\epsilon}{2}.$$

Here $[n, k]$ means that the code is linear, of dimension k and length n. Further, w_H denotes the Hamming weight.

There is a simple direct translation [1] between the concepts described in Definition 1 and Definition 2:

Theorem 3. *Let G be a generator matrix for an ϵ-balanced binary $[n, k]$ code. The columns of G constitute an ϵ-bias space $\mathcal{X} \subseteq \mathbb{F}_2^k$ of size n. Similarly, using the elements of an ϵ-bias space $\mathcal{X}$ as columns of a generator matrix an ϵ-balanced code is derived.*

The following example illustrates the above theorem. It also shows why it is important in Definition 1 to work with multisets rather than sets.

Example 1. *Consider the matrix*

$$G = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The code having G as a generator matrix is ϵ-balanced with $\epsilon = 1/3$ and indeed the multiset made from the columns of G is $\epsilon = 1/3$ biased. Treating the columns as a set (rather than a multiset) we derive

$$\mathcal{X}' = \{(0,0,1), (1,0,1), (0,1,1), (1,1,1), (0,0,0)\}.$$

The smallest value of ϵ for which $\mathcal{X}'$ is ϵ-biased is $\epsilon = 3/5$.

A standard construction from [1] tells us how to make small-balanced codes (meaning ϵ-biased codes with ϵ small):

Theorem 4. *Let $q = 2^s$ for some integer s and consider a q-ary $[N, K, D]$ code C. Let C_s be the (binary) $[2^s, s]_2$ Walsh-Hadamard code, $s \geq 1$. The concatenated code derived by using C as outer code and C_s as inner code is an $\epsilon = (N-D)/N$-balanced binary code of length $n = N2^s$ and dimension $k = Ks$.*

Proof. The result relies on the fact that every non-zero codeword of C_s contains exactly as many 0s as 1s. □

The literature contains various examples of small-bias spaces that cannot all be compared to each other. We refer to [2, Sec. 1] for more details. In the following we will concentrate on important families of multisets for which comparison can be made. We remind the reader of how bigO notation works when given functions of multiple variables. In our situation we have real valued positive functions $f_i(x, y), i = 1, 2$ where x can take on any value in $\mathbb{Z}^+$ but for every fixed choice of x the variable y can only take on values in an interval $I(x) \subseteq \mathbb{R}^+$. By $f_1(x, y) = \mathcal{O}(f_2(x, y))$ we mean that a witness (C, κ) exists such that for all x with $\kappa < x$ and all $y \in I(x)$ it holds that $f_1(x, y) \leq C f_2(x, y)$. We are interested in upper bounding the size of $\mathcal{X}$ which will be done in terms of bigO estimates as above. At the same time we are interested in lower bounding the length of the words in the multiset $\mathcal{X}$. Such estimates are described using bigOmega notation. We remind the reader that by definition $f(x) = \Omega(g(x))$ if and only if $g(x) = \mathcal{O}(f(x))$. As we are only interested in bigOmega estimates the meaning of k changes accordingly. In the following list of results note that a family of ϵ-bias spaces is considered to behave well if when given ϵ and k the size of $\mathcal{X}$ is small.

- Using Reed-Solomon codes as outer codes in Theorem 4 one achieves [1, 2] for all possible choices of ϵ and k

$$\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}, \quad |\mathcal{X}| = \mathcal{O}\left(\frac{k^2}{\epsilon^2 \log^2(k/\epsilon)}\right).$$

  This is called the RS-bound.

- Let $P_1, \ldots, P_{\mathcal{N}-1}, Q$ be rational places of an algebraic function field over $\mathbb{F}_q$ and denote by g the genus. Assume $\mathcal{N} = (\sqrt{q} - 1)g$. That is, we assume that the function field attains the Drinfeld-Vladut bound. Using codes $C_{\mathcal{L}}(U = P_1 + \cdots + P_{\mathcal{N}-1}, mQ)$ with $g < m$ as outer codes one gets for all ϵ and k (see Section 2 for a discussion)

$$\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}, \quad |\mathcal{X}| = \mathcal{O}\left(\frac{k}{\epsilon^3 \log(1/\epsilon)}\right).$$

  This result which is in the folklore is known as the AG-bound.

- Using Hermitian codes with $m < g$ as outer codes one achieves [2] for $\epsilon \geq k^{-\frac{1}{2}}$

$$\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}, \quad |\mathcal{X}| = \mathcal{O}\left(\left(\frac{k}{\epsilon^2 \log(1/\epsilon)}\right)^{\frac{5}{4}}\right). \tag{1.3}$$

  This we call the BT-bound after the authors of [2], Ben-Aroya and Ta-Shma.

- Using in larger generality Norm-Trace codes of low dimension as outer codes one achieves [12] for $l = 4, 5, \ldots$ and $\epsilon \geq k^{-\frac{1}{\sqrt{l}}}$ (see Section 5)

$$\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}, \quad |\mathcal{X}| = \mathcal{O}\left(\left(\frac{k}{\epsilon^{l-\sqrt{l}}\log(1/\epsilon)}\right)^{\frac{l+1}{l}}\right).$$

  Here, $l = 4$ corresponds to the Hermitian case described in [2].

- The Gilbert-Varshamov bound also applies to the small-bias spaces (as usual in a non-constructive way). It is derived by plugging into the Gilbert-Varshamov bound for binary codes $d = n/2$ and to make a Taylor approximation on the resulting formula. The construction uses Theorem 3 directly. It guarantees for all ϵ and k the existence of multisets with

$$\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}, \quad |\mathcal{X}| = \mathcal{O}\left(\frac{k}{\epsilon^2}\right).$$

- The linear programming bound tells us that we cannot hope to produce ϵ-bias spaces with

$$\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}, \quad |\mathcal{X}| = \mathcal{O}\left(\frac{k}{\epsilon^2\log(1/\epsilon)}\right).$$

One way of comparing the above results is to choose $\epsilon = k^{-\alpha}$, $\alpha \in \mathbb{R}^+$ and then to take the logarithm with base k. The bigO notation suggests that we then let k go to infinity. The origin of this point of view is [2, Sec. 1]. When making the above operation we must be careful to specify which choices of α are allowed. We remind the reader of the little-o notation. Given functions $f_i(x) : \mathbb{Z}^+ \to \mathbb{R}^+, i = 1, 2$ by $f_1(x) = o(f_2(x))$ we mean that for every choice of $c \in \mathbb{R}^+$ there exists a $\kappa(c) \in \mathbb{Z}^+$ such that when $\kappa(c) < x$ then necessarily $f_1(x) \leq cf_2(x)$. The above list of results translates to (note that when given α we want $\log_k(|\mathcal{X}|)$ to approach a low value):

- RS-bound: The family of concatenated codes from Theorem 4 with Reed-Solomon codes as outer codes gives

$$\log_k(|\mathcal{X}|) = 2 + 2\alpha + o(1)$$

  for all choices of $\alpha \in \mathbb{R}^+$.

- AG-bound: The family of concatenated codes from Theorem 4 with algebraic geometric codes as outer codes and $g < m$ gives

$$\log_k(|\mathcal{X}|) = 1 + 3\alpha + o(1)$$

  for all choices of $\alpha \in \mathbb{R}^+$.

- BT-bound: The family of concatenated codes from Theorem 4 with Hermitian codes as outer codes and $m < g$ gives

$$\log_k(|\mathcal{X}|) = \frac{5}{4} + \frac{5}{2}\alpha + o(1)$$

  for all choices of $\alpha \in]1/2, \infty[$.

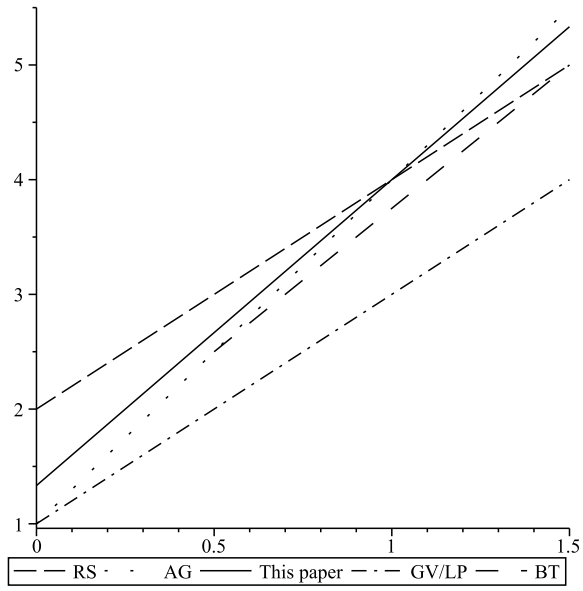

Figure 1.1: Comparison of various constructions: First axis is α, second axis corresponds to $\log_k(|\mathcal{X}|)$ when $k \to \infty$.

- The family of concatenated codes from norm-trace codes of low dimension gives
$$\log_k(|\mathcal{X}|) = \frac{l+1}{l}(1 + \alpha(l - \sqrt{l})) + o(1)$$
for $l = 4, 5, \ldots$, and for all $\alpha \in [1/\sqrt{l}, \infty[$ (see Section 5).

- The Gilbert-Varshamov bound and the Linear Programming bound in combination tell us that we can achieve
$$\log_k(|\mathcal{X}|) = 1 + 2\alpha + o(1)$$
for all choices of $\alpha \in \mathbb{R}^+$ but no better than this.

In the present paper we shall introduce a new family of small-bias spaces using a combination of Hermitian codes as outer code. This family gives

$$\log_k(|\mathcal{X}|) = \frac{4}{3} + \frac{8}{3}\alpha + o(1)$$

for all choices of $\alpha \in \mathbb{R}^+$. We allow $2g < m$ and it is therefore surprising that for $\alpha \in]1, \infty[$ the achievements are better than those of the Hermitian codes with $g < m$. Our small-bias spaces perform better than the ones derived from norm-trace codes for all $l \geq 5$ (see Section 5 for the proof). For $\alpha < 1$ they behave

better than what can be achieved using Reed-Solomon codes as outer code. For $\alpha < 1$ admittedly the new ϵ-bias spaces perform worse than the spaces coming from the AG construction. This, however, is only part of the picture. It turns out that to construct the spaces with $\alpha < 1/2$ from the AG construction requires quite a number of operations. In contrast, our construction is considerable faster. We shall revert to this issue in Section 4. Before dealing with the new construction we will investigate how to ensure $\epsilon = k^{-\alpha}$ in the case of the AG bound. It turns out that for $\alpha < 1/2$ the situation is rather complicated. We include the description here, as to our best knowledge, the details cannot be found in the literature.

Chapter 2

The AG-bound

Let q be a power of 2 and consider an algebraic function field over $\mathbb{F}_{q^2}$ of genus g with at least $\mathcal{N} = (q-1)g$ rational places. That is, the function field attains the Drinfeld-Vladut bound. As noted in the introduction Theorem 4 equipped with a one-point algebraic geometric code from the above function field produces ϵ-bias spaces $\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}$ with

$$|\mathcal{X}| = \mathcal{O}\left(\frac{k}{\epsilon^3 \log_2(\frac{1}{\epsilon})}\right). \tag{2.1}$$

In the following we investigate how to achieve corresponding values ϵ and k under the requirement $\epsilon = k^{-\alpha}$, $\alpha > 0$, and $k \to \infty$. Observe, that in this situation for any fixed α we have $\epsilon \to 0$. For completeness we start by proving (2.1) in this setting.
Consider rational places $P_1, \ldots, P_{\mathcal{N}-1}, Q$ and let $U = P_1 + \cdots + P_{\mathcal{N}-1}$ and $G = (ag)Q$ with $a \geq 1$. The code $C_{\mathcal{L}}(U, G)$ has parameters $N = (q-1)g - 1$, $K \geq \deg G - g = (a-1)g$, and $D \geq N - \deg G = ((q-1)-a)g - 1$. As we are interested in asymptotics we shall assume $N = (q-1)g$ and $D \geq ((q-1)-a)g$. From Theorem 4 we get ϵ-bias spaces with $\epsilon = a/(q-1)$, $\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}$. Here, $k = 2\log_2(q)(a-1)g$ and we have $|\mathcal{X}| = q^2 N = (q^3 - q^2)g$. As a is bounded below by 1 and $\epsilon \to 0$ we need $q \to \infty$ when $k \to \infty$. So the task basically boils down to establishing a sequence of function fields over increasingly large fields and a corresponding function $a(q)$ such that

$$|\mathcal{X}| = \mathcal{O}\left(\frac{2\log_2(q)(a-1)g}{\left(\frac{a}{q-1}\right)^3 \log_2\left(\frac{q-1}{a}\right)}\right). \tag{2.2}$$

Note that the argument on the right side is a function in the single variable q as by construction now g is a function of q. We have

$$\frac{2\log_2(q)(a-1)g}{\left(\frac{a}{q-1}\right)^3 \log_2\left(\frac{q-1}{a}\right)} \geq \frac{1}{2}\frac{\log_2(q)(a-1)}{a^3(\log_2(q-1) - \log_2(a))}|\mathcal{X}|$$

as $(q-1)^3 \geq \frac{1}{4}(q^3-q^2)$ holds for $q \geq 2$. In conclusion (2.2) holds if $a(q) = \mathcal{O}(1)$. We first assume that the sequence of function fields are the Hermitians which are function fields with $g = q(q-1)/2$. Here, actually the number of rational places is $2qg + q^2 + 1$ but we shall only use $(q-1)g$ of them. Let $a = 1 + q^{-c}$ where $0 \leq c < 2$. Clearly, $a(q) = \mathcal{O}(1)$ as requested. We have $k = 2\log_2(q)q^{-c}g = q^{2-c}q^{\beta}$ where $\beta(q) \to 0$ for $q \to \infty$. Hence, asymptotically $\epsilon = k^{-\alpha}$ with $\alpha = 1/(2-c)$. In other words the situation is clear for $\alpha \in [\frac{1}{2}, \infty[$.
To achieve $\alpha \in]0, \frac{1}{2}[$ is more difficult. The problem is to keep $a(q) = \mathcal{O}(1)$ at the same time as having $\epsilon = k^{-\alpha}$. For this purpose we consider families of towers of function fields over $\mathbb{F}_{q^2}$ attaining the Drinfeld-Vladut bound [5]. We will need one tower for each value of q. Note that in such a tower for arbitrary $v \geq 2$ we can find a function field with $g \geq q^v$. Say $g = q^{v+d(q)}$, where $d(q) \geq 0$ holds. Let $a(q) = 1 + q^{-d(q)}$ then clearly $a(q) = \mathcal{O}(1)$ holds. We have $k = 2\log_2(q)(a-1)g = q^{v+\beta}$ where $\beta(q) \to 0$ for $q \to \infty$. Also $\epsilon = q^{-1+\gamma}$ where $\gamma(q) \to 0$ for $q \to \infty$. Hence, $k^{-\alpha} = \epsilon$ asymptotically means $v\alpha = 1 \Rightarrow \alpha = 1/v$. As we only assumed $v \geq 2$ we have established that all $\alpha \in]0, \frac{1}{2}[$ can be attained.
For our purpose the best candidate for a family of good towers of function fields is the second construction by Garcia and Stichtenoth [5]. In [16] it was shown how to construct $C_{\mathcal{L}}(U, G)$ codes from this tower using

$$\mathcal{O}\left((N\log_q(N))^3\right) \tag{2.3}$$

operations over $\mathbb{F}_{q^2}$. Although we might only need codes of small dimension the method as stated requests us to find bases for all one-point codes. As shall be demonstrated in Section 4 the small-bias spaces of the present paper can be constructed much faster than what (2.3) guarantees for the AG construction.

Chapter 3

The new small-bias spaces

In the present paper we propose a new choice of outer codes in the construction of Theorem 4. As already mentioned this results in small-bias spaces with good properties. The new choice of outer codes is derived by combining two Hermitian codes as described below. The easiest way to explain the combination is by using the language of affine variety codes [4] and we therefore start our investigations with a presentation of Hermitian codes as such.

Definition 5. *Given a monomial ordering $\prec$ and an ideal $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$ (here $\mathbb{F}$ is any field) the footprint is*

$$\Delta_\prec(I) \quad := \quad \{X_1^{\alpha_1} \cdots X_m^{\alpha_m} \mid X_1^{\alpha_1} \cdots X_m^{\alpha_m} \quad \textit{is not a leading monomial of any polynomial in} \quad I\}.$$

We have the following two useful results [3, Pro. 4 and Pro. 8, Sec. 5.3].

Theorem 6. *The set $\{M + I \mid M \in \Delta_\prec(I)\}$ is a basis for $\mathbb{F}[X_1, \ldots, X_m]/I$ as a vector space over $\mathbb{F}$.*

As a corollary one gets the following result often referred to as the footprint bound [7, 9].

Theorem 7. *Assume I is zero-dimensional (meaning that $\Delta_\prec(I)$ is finite). The variety $\mathbb{V}_{\bar{\mathbb{F}}}(I)$ satisfies $|\mathbb{V}_{\bar{\mathbb{F}}}(I)| \leq |\Delta_\prec(I)|$.*

Consider the Hermitian polynomial $X^{q+1} - Y^q - Y$ and the corresponding ideal

$$I = \langle X^{q+1} - Y^q - Y \rangle \subseteq \mathbb{F}_{q^2}[X, Y].$$

Define a monomial function w by $w(X) = q$ and $w(Y) = (q + 1)$ and consider the weighted degree monomial ordering $\prec_w$ given by $X^{\alpha_1} Y^{\beta_1} \prec_w X^{\alpha_2} Y^{\beta_2}$ if one of the following two conditions holds:

1. $w(X^{\alpha_1} Y^{\beta_1}) < w(X^{\alpha_2} Y^{\beta_2})$.
2. $w(X^{\alpha_1} Y^{\beta_1}) = w(X^{\alpha_2} Y^{\beta_2})$ but $\beta_1 < \beta_2$.

Observe for later use that no two different monomials in

$$\Delta_{\prec_w}(I) = \{X^iY^j \mid 0 \leq i \text{ and } 0 \leq j < q\}$$

are of the same weight implying that $w : \Delta_{\prec_w}(I) \to \langle q, q+1\rangle$ is a bijection. Observe also that the Hermitian polynomial $X^{q+1} - Y^q - Y$ contains exactly two monomials of highest weight. The implication of this is that

$$w(\mathrm{lm}(F(X,Y)) = w(\mathrm{lm}(F(X,Y) \text{ rem } \{X^{q+1} - Y^q - Y\})$$

holds for any polynomial $F(X,Y)$ that possesses exactly one monomial of highest weight in its support.
Consider next the ideal

$$I_{q^2} := \langle X^{q^2} - X, Y^{q^2} - Y\rangle + I.$$

The variety $\mathbb{V}_{\mathbb{F}_{q^2}}(I) = \mathbb{V}_{\mathbb{F}_{q^2}}(I_{q^2})$ consists of $n = q^3$ different points $\{P_1, \ldots P_n\}$. The set $\{X^{q^2} - X, X^{q+1} - Y^q - Y\}$ constitutes a Gröbner basis for I_{q^2} with respect to $\prec_w$ and therefore

$$\Delta_{\prec_w}(I_{q^2}) = \{X^iY^j \mid 0 \leq i < q^2, 0 \leq j < q\}$$

holds. It now follows from Theorem 6 that

$$\{X^iY^j + I_{q^2} \mid 0 \leq i < q^2, 0 \leq j < q\}$$

is a basis for $\mathbb{F}_{q^2}[X,Y]/I_{q^2}$ as a vector space over $\mathbb{F}_{q^2}$. The code construction relies on the bijective evaluation map $\mathrm{ev} : \mathbb{F}_{q^2}[X,Y]/I_{q^2} \to \mathbb{F}_{q^2}^n$ given by $\mathrm{ev}(F(X,Y) + I_{q^2}) = (F(P_1), \ldots, F(P_n))$. Theorem 7 tells us that we can estimate the Hamming weight of a word $\vec{c} = \mathrm{ev}(F(X,Y) + I_{q^2})$ by

$$w_H(\vec{c}) \geq n - |\Delta_{\prec_w}(\langle F(X,Y)\rangle + I_{q^2})|.$$

Without loss of generality we can assume $\mathrm{Supp}(F) \subseteq \Delta_{\prec_w}(I_{q^2})$. From the discussion prior to the definition of I_{q^2} we conclude that no two different monomials in $F(X,Y)$ are of the same weight. As a consequence

$$w(\mathrm{lm}(X^\alpha Y^\beta F(X,Y)) = w(\mathrm{lm}(X^\alpha Y^\beta F(X,Y) \text{ rem } \{X^{q+1} - Y^q - Y\})$$

holds for all $X^\alpha Y^\beta$. Write $\Lambda = w(\Delta_{\prec_w}(I)) = \langle q, q+1\rangle$, $\Lambda^* = w(\Delta_{\prec_w}(I_{q^2})) \subseteq \Lambda$ and $\lambda = w(\mathrm{lm}(F)) \in \Lambda^*$. We have

$$|\Delta_{\prec_w}(\langle F(X,Y)\rangle + I_{q^2})| \leq |(\Lambda^* - (\lambda + \Lambda))| \leq |(\Lambda \backslash (\lambda + \Lambda)| = \lambda,$$

where the last equality comes from [10, Lem. 5.15]. Hence, $w_H(\vec{c}) \geq n - \lambda$ holds. Observe that

$$\Lambda^* = \{\lambda_1, \ldots, \lambda_g\} \cup \{2g, \ldots, n-1\} \cup \{\lambda_{n-g+1}, \ldots, \lambda_n\}, \tag{3.1}$$

where $\lambda_i \leq g - 1 + i$ for $i = 1, \ldots, g$. This is a general result for Weierstrass semigroups and not particular for the Hermitian function field. Having described

the Hermitian codes as affine variety codes we are now ready to introduce the combination of codes on which our construction of small-bias spaces rely. Consider the ideal

$$\begin{aligned} I^{(2)}_{q^2} &:= \langle X_1^{q+1} - Y_1^q - Y_1, X_2^{q+1} - Y_2^q - Y_2, \\ &\quad X_1^{q^2} - X_1, Y_1^{q^2} - Y_1, X_2^{q^2} - X_2, Y_2^{q^2} - Y_2 \rangle \end{aligned}$$

and the corresponding variety

$$\mathbb{V}_{\mathbb{F}_{q^2}}(I^{(2)}_{q^2}) = \mathbb{V}_{\mathbb{F}_{q^2}}(I_{q^2}) \times \mathbb{V}_{\mathbb{F}_{q^2}}(I_{q^2}) = \{Q_1, \ldots, Q_{q^6}\}.$$

Define a monomial function $w^{(2)}$ given by $w^{(2)}(X_1) = (q, 0)$, $w^{(2)}(Y_1) = (q + 1, 0)$,$w^{(2)}(X_2) = (0, q)$, and finally $w^{(2)}(Y_2) = (0, q+1)$. Let $\prec_{\mathbb{N}_0^2}$ be any monomial ordering on $\mathbb{N}_0^2$ and define $\prec_{w^{(2)}}$ by

$$X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}} \prec_w^{(2)} X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}}$$

if one of the following two conditions holds:

1. $w^{(2)}(X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}}) \prec_{\mathbb{N}_0^2} w^{(2)}(X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}})$
2. $w^{(2)}(X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}}) = w^{(2)}(X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}})$
   but
   $X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}} \prec_{\text{lex}} X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}}$.

Here, $X_1 \succ_{\text{lex}} Y_1 \succ_{\text{lex}} X_2 \succ_{\text{lex}} Y_2$ is assumed. The set $\{X_1^{q+1} - Y_1^q - Y_1, X_2^{q+1} - Y_2^q - Y_2, X_1^{q^2} - X_1, X_2^{q^2} - X_2\}$ is a Gröbner basis for $I^{(2)}_{q^2}$ with respect to $\prec_{w^{(2)}}$ giving us the basis

$$\{X_1^{i_1} Y_1^{j_1} X_2^{i_2} Y_2^{j_2} + I_{q^2} \mid 0 \leq i_1, i_2 < q^2, 0 \leq j_1, j_2 < q\}$$

for $\mathbb{F}_{q^2}[X_1, Y_1, X_2, Y_2]/I^{(2)}_{q^2}$ as a vectorspace over $\mathbb{F}_{q^2}$. For the code construction we need the following bijective evaluation map

$$\text{EV} : \mathbb{F}_{q^2}[X_1, Y_1, X_2, Y_2]/I^{(2)} \to \mathbb{F}_{q^2}^{q^6}$$

given by $\text{EV}(F(X_1, Y_1, X_2, Y_2) + I^{(2)}_{q^2}) = (F(Q_1,), \ldots, F(Q_{q^6}))$. Define $\Lambda^{(2)} = \Lambda \times \Lambda$ and $\left(\Lambda^{(2)}\right)^* = \Lambda^* \times \Lambda^*$. We have

$$\left(\Lambda^{(2)}\right)^* = w^{(2)}(\Delta_{\prec_{w^{(2)}}}(I^{(2)}_{q^2}))$$

where no two monomials in $\Delta_{\prec_{w^{(2)}}}(I^{(2)}_{q^2})$ have the same weight. Similar to the situation of a Hermitian code we consider a codeword $\vec{c} = \text{EV}(F(X_1, Y_1, X_2, Y_2) +$

$I^{(2)}_{q^2}$) where without loss of generality we will assume that $F(X_1, Y_1, X_2, Y_2) \in \Delta_{\prec_{w^{(2)}}}(I^{(2)}_{q^2})$. We write $\lambda^{(2)} = (\lambda_1, \lambda_2) = w^{(2)}(\mathrm{lm}(F))$. We can estimate

$$\begin{aligned} |\Delta_{\prec_{w^{(2)}}}(\langle F(X_1, Y_1, X_2, Y_2)\rangle + I^{(2)}_{q^2})| &\leq |\Lambda^{(2)} - (\lambda^{(2)} + \Lambda^{(2)})| \\ &\leq q^6 - (q^3 - \lambda_1)(q^3 - \lambda_2). \end{aligned}$$

Hence, $w_H(\vec{c}) \geq (q^3 - \lambda_1)(q^3 - \lambda_2)$.
Consider the code $\widetilde{E}(\delta)$ which is to Hermitian codes what Massey-Costello-Justesen codes [13] are to Reed-Solomon codes

$$\begin{aligned} \widetilde{E}(\delta) := \mathrm{Span}_{\mathbb{F}_{q^2}} \Big\{ & \mathrm{ev}(X_1^{i_1} Y_1^{j_1} X_2^{i_2} Y_2^{j_2} + I^{(2)}_{q^2}) \mid 0 \leq i_1, i_2 < q^2, \\ & 0 \leq j_1, j_2 < q, (q^3 - w(X_1^{i_1} Y_1^{j_1}))(q^3 - w(X_2^{i_2} Y_2^{j_2})) \geq \delta \Big\}. \end{aligned}$$

From our discussion we conclude that the minimum distance satisfies $d(\widetilde{E}(\delta)) \geq \delta$. To estimate the dimension we make use of the characterization (3.1). The task is to estimate the number of (λ_1, λ_2)s that satisfies $(q^3 - \lambda_1)(q^3 - \lambda_2) \geq \delta$. For this purpose we can replace Λ^* with

$$\{g, g+1, \ldots, q^3 - 1\} \cup \{\lambda_{n-g+1}, \ldots, \lambda_n\}.$$

When estimating the dimension $k(\widetilde{E}(\delta))$ we shall furthermore ignore the elements in $\{\lambda_{n-g+1}, \ldots, \lambda_n\}$. Writing $T = q^3 - g$ we thereby get

$$\begin{aligned} k(\widetilde{E}(\delta)) &\geq |\{(i,j) \mid 0 \leq i, j \leq T-1, (T-i)(T-j) \geq \delta\}| \\ &\geq \int_0^{T - \frac{\delta}{T}} \int_0^{T - \frac{\delta}{T-i}} djdi = T^2 - \delta + \ln\left(\frac{\delta}{T^2}\right), \end{aligned}$$

where the last inequality holds under the assumption $\delta \geq T$.

Proposition 8. *Assume $\delta \geq T$ where $T = q^3 - g$. The parameters of $\widetilde{E}(\delta)$ are $[n = q^6, k \geq T^2 - \delta + \delta \ln(\delta/T^2), d \geq \delta]$.*

In [8] Feng-Rao improved codes $\widetilde{C}(\delta)$ over $\mathbb{F}_{q^2}[X_1, Y_1, X_2, Y_2]/I^{(2)}_{q^2}$ were considered and a formula similar to the above proposition was derived under a stronger assumption on δ. Feng-Rao improved codes are described by means of their parity check matrix which is not very useful when the aim is to construct a small-bias space. This is why we included the description of $\widetilde{E}(\delta)$ in the present paper. We have a proof that $\widetilde{E}(\delta) = \widetilde{C}(\delta)$, however, we do not include it here as it has no implication for the construction of small-bias spaces. Observe that to derive Proposition 8 we did not use detailed information about the Weierstrass semigroup Λ but relied only on the genus and the number of roots of the Hermitian polynomial. Proposition 8 can be generalized to hold for not only two copies of Hermitian function fields but to arbitrary many such copies. Such constructions, however, are not useful when dealing with small-bias spaces so we do not treat them here.
From Proposition 8 and Theorem 4 we get a new class of ϵ-bias spaces:

Theorem 9. *For any ϵ, $0 < \epsilon < 1$ using codes $\widetilde{E}(\delta)$ as outer code in the construction of Theorem 4 one can construct ϵ-bias spaces with*

$$\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}, \qquad |\mathcal{X}| = \mathcal{O}\left(\left(\frac{k}{\epsilon + (1-\epsilon)\ln(1-\epsilon)}\right)^{\frac{4}{3}}\right). \tag{3.2}$$

Proof. In the following we will use the substitution $1-\epsilon = \delta/N$ which follows from $\epsilon = (N-\delta)/N$. Assume $\delta > \sqrt{N}$. We then have $\delta > T$ which is the condition in Proposition 8. Note that $\delta > \sqrt{N}$ is equivalent to $\epsilon < 1 - (1/\sqrt{N})$. For $N \to \infty$ this becomes $\epsilon < 1$ which is actually no restriction at all. From the proposition we get

$$\begin{aligned} \frac{K}{N} &\geq \left(\frac{q^3-g}{q^6}\right)^2 - \frac{\delta}{q^6} + \frac{\delta}{q^6}\ln\left(\frac{\delta}{(q^3-g)^2}\right) \\ &\geq o(1) + 1 - (1-\epsilon) + (1-\epsilon)\ln(1-\epsilon) \\ &= o(1) + \epsilon + (1-\epsilon)\ln(1-\epsilon). \end{aligned}$$

With $q^2 = 2^s$ we have

$$|\mathcal{X}| \leq \frac{2^s}{s}\left(\frac{k}{o(1) + \epsilon + (1-\epsilon)\ln(1-\epsilon)}\right).$$

But $|\mathcal{X}| = (2^s)^4$ implies $2^s = |\mathcal{X}|^{1/4}$ and (3.2) has been demonstrated. □

Theorem 10. *Consider the family of ϵ-bias spaces in Theorem 9. Given $\alpha \in \mathbb{R}^+$ choose $\epsilon = k^{-\alpha}$ and let $k \to \infty$. We have*

$$\log_k(|\mathcal{X}|) = \frac{4}{3} + \frac{8}{3}\alpha + o(1). \tag{3.3}$$

Proof. We have

$$\log_k(|\mathcal{X}|) \leq \frac{4}{3} - \frac{4}{3}\log_k(\epsilon + (1-\epsilon)\ln(1-\epsilon)).$$

We now apply Taylors formula to derive $\ln(1-\epsilon) = -\epsilon - \epsilon^2/2(1-c)^2$ for some $c \in [0, \epsilon]$. This produces

$$\begin{aligned} \log_k(|\mathcal{X}|) &\leq \frac{4}{3} - \frac{4}{3}\log_k\left(\epsilon + (1-\epsilon)(-\epsilon - \frac{\epsilon^2}{2(1-\epsilon)^2})\right) \\ &\leq \frac{4}{3} - \frac{4}{3}\log_k\left(\epsilon^2\left(\frac{2(1-\epsilon)^2 - \epsilon^2}{(1-\epsilon)^2}\right)\right). \end{aligned}$$

With $\epsilon = k^{-\alpha}$ we arrive at (3.3). □

Chapter 4

Time complexity considerations

To build the multiset $\mathcal{X}$ in our construction we need to construct a generator matrix for the concatenated code. This involves the following tasks:

1. Build the generator matrix G_1 for $\widetilde{E}(\delta)$.
2. Express every entry of G_1 as a binary vector giving us G_2 (a matrix with binary vectors as entries).
3. For every row in G_2 we produce $s = \log_2(q^2)$ rows. This is done by taking cyclic shifts of all the vectors appearing in the row. We arrive at a matrix G_3.
4. Every entry in G_3 is a vector of length s and it must be multiplied with the $s \times 2^s$ generator matrix of the Walsh-Hadamard code producing G_4.

The total cost in binary operations is estimated as follows:

1. Determining functions and points for the code construction is inexpensive. To produce one entry costs $\mathcal{O}(\log(N)\log(\log(N)))$ operations. G_1 is a $K \times N$ matrix. Using $K \leq N-D+1$, $\epsilon = (N-D)/N$, $\epsilon = k^{-\alpha}$, and $k = K\log_2(N)/6$ we arrive at $K \leq N^{\frac{1}{1+\alpha}}(\log_2(N))^{\frac{-\alpha}{1+\alpha}}6^{\frac{\alpha}{1+\alpha}}$. So the price for building G_1 is $\mathcal{O}\left(N^{\frac{2+\alpha}{1+\alpha}}(\log(N))^{\frac{1}{1+\alpha}}\log(\log(N))\right)$.
2. To produce one entry in G_2 costs $\mathcal{O}\left(N^{\frac{1}{3}}\log(N^{\frac{1}{3}})\log(\log(N^{\frac{1}{3}}))\right)$ operations. That is, to produce G_2 from G_1 amounts to $\mathcal{O}\left(N^{\frac{7+4\alpha}{3+3\alpha}}\log(N)^{\frac{1}{1+\alpha}}\log(\log(N))\right)$ operations.
3. There will be $\mathcal{O}\left(N^{\frac{2+\alpha}{1+\alpha}}(\log(N))^{\frac{1}{1+\alpha}}\right)$ entries in G_3 each coming with a cost of s operations. Altogether we have $\mathcal{O}\left(N^{\frac{2+\alpha}{1+\alpha}}(\log(N))^{\frac{2+\alpha}{1+\alpha}}\right)$ operations.

4. The price for multiplying with a generator matrix for the Walsh-Hadamard code is $N^{\frac{1}{3}} \log(N)$ giving a total cost of

$$\mathcal{O}\left(N^{\frac{7+4\alpha}{3+3\alpha}} (\log(N))^{\frac{2+\alpha}{1+\alpha}}\right) \tag{4.1}$$

operations for producing G_4 from G_3.

Clearly, the overall cost is that of (4.1). Note that (4.1) counts binary operations in contrast to (2.3) which counts operations in $\mathbb{F}_{q^2}$.

Chapter 5

Small-bias spaces from norm-trace codes

The method developed by Ben-Aroya and Ta-Shma for Hermitian codes in [2] were generalized to norm-trace codes by Matthews and Peachey in [12]. Given $r \geq 2$ consider the C_{ab} curve [11]

$$X^{\frac{q^r-1}{q-1}} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y^q - Y$$

known as the norm-trace curve over $\mathbb{F}_{q^r}$ [6]. Clearly, $r = 2$ corresponds to the Hermitian function field. The following theorem from [12] coincides with (1.3) when $l = 4$.

Theorem 11. *Given an integer l, $l \geq 4$, define $r = \lfloor (l+2)/3 \rfloor$. Let k be a positive integer and ϵ a real number, $0 < \epsilon < 1$ such that*

$$\frac{\epsilon}{\left(\log_v(1/\epsilon)\right)^{\frac{1}{\sqrt{l}}}} \leq k^{\frac{-1}{\sqrt{l}}} \tag{5.1}$$

holds. Here, v is any fixed real number larger than 1. Using the norm-trace function field over $\mathbb{F}_{q^r}$ one can construct an ϵ-bias space $\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}$ with

$$|\mathcal{X}| = \mathcal{O}\left(\left(\frac{k}{\epsilon^{l-\sqrt{l}}\log_v(1/\epsilon)}\right)^{\frac{l+1}{l}}\right).$$

In the above theorem it is not completely clear how well the cases $l \geq 5$ compete with the case $l = 4$. Below we address this question and also compare the small-bias spaces from Theorem 11 with those achieved by using the codes $\widetilde{E}(\delta)$ as is done in the present paper.
We first translate Theorem 11 into the setting from Section 1 where for increasing k and fixed α we consider a sequence of ϵ-bias multisets with $\epsilon = k^{-\alpha}$. Condition (5.1) from Theorem 11 then translates into

$$k^{1-\alpha\sqrt{l}} \leq \alpha \log_v(k).$$

For fixed v, $\log_v(k) = \mathcal{O}\left(k^{\beta}\right)$ holds for any $\beta > 0$. Therefore we have

$$1 - \alpha\sqrt{l} \leq \log_k(\alpha).$$

Letting $k \to \infty$ we get the condition

$$\frac{1}{\sqrt{l}} \leq \alpha.$$

Theorem 11 therefore guarantees that for any $\alpha \geq 1/\sqrt{l}$ we can construct an infinite sequence of ϵ-bias spaces with $\epsilon = k^{-\alpha}$, $\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}$ such that

$$\log_k(|\mathcal{X}|) = \frac{l+1}{l}(1 + \alpha(l - \sqrt{l})) + o(1). \tag{5.2}$$

Given an α and two integers $l_1, l_2 \geq 4$ with $\alpha \geq 1/\sqrt{l_i}$, $i = 1, 2$ it is clear from (5.2) that the best result is obtained by choosing the smallest l_i. So the advantage of Theorem 11 over (1.3) boils down to the fact that Theorem 11 allows for any α provided that the l is chosen accordingly while (1.3) requires $\alpha \geq 1/2$. Recall from Section 3 that using the code $\widetilde{E}(\delta)$ in the construction of Theorem 4 one achieves

$$\log_k(|\mathcal{X}|) = \frac{4}{3} + \frac{8}{3}\alpha + o(1) \tag{5.3}$$

for any choice of α. We now compare this result with (5.2) ignoring of course the $o(1)$ parts. For fixed l (5.2) is a linear expression in α which is smaller than the linear expression from (5.3) when $\alpha = 0$. We now show that for $\alpha = 1/\sqrt{l}$ (which is the smallest α allowed) (5.2) is larger than (5.3) when $l \geq 5$. It follows that none of the cases $l \geq 5$ can compete with the construction of the present paper. To show that (5.2) is larger than (5.3) for $\alpha = 1/\sqrt{l}$ we substitute $k = \sqrt{l}$ into (5.2)-(5.3) to get

$$\frac{1}{k^2}(k^3 - \frac{4}{3}k^2 - \frac{5}{3}k).$$

The function $k^3 - \frac{4}{3}k^2 - \frac{5}{3}k$ is positive for k belonging to the interval from 0 to approximately 2.119 and negative for higher values of k. Therefore for all $l \geq 5$ indeed (5.3) is better than (5.2). The situation is illustrated in Figure 5.1.

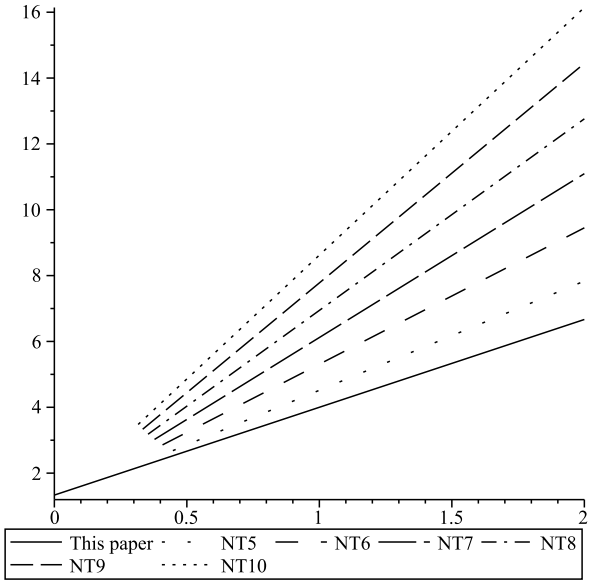

Figure 5.1: Comparison of new construction with NT-construction where $l \in \{5, \ldots, 10\}$. First axis is α, second axis corresponds to $\log_k(|\mathcal{X}|)$ when $k \to \infty$.

Acknowledgments

The present work was done while Ryutaroh Matsumoto was visiting Aalborg University as a Velux Visiting Professor supported by the Villum Foundation. The authors gratefully acknowledge this support. The authors also gratefully acknowledge the support from the Danish National Research Foundation and the National Science Foundation of China (Grant No. 11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography.

Bibliography

[1] N. Alon, O. Goldreich, J. Hastad, and R. Peralta: Simple constructions of almost k-wise independent random variables. *Random Structures Algorithms* **3** (1992), no. 3, 289-303.

[2] A. Ben-Aroya and A. Ta-Shma: Constructing small-bias sets from algebraic-geometric codes. *FOCS'2009*, 191-197.

[3] D. Cox, J. Little and D. O'Shea: *Ideals, Varieties, and Algorithms, Sec. Ed.*, Springer, 1997.

[4] J. Fitzgerald and R. F. Lax: Decoding Affine Variety Codes Using Gröbner Bases. *Des. Codes Cryptography,* **13**, 1998, 147-158.

[5] A. Garcia and H. Stichtenoth: On the asymptotic behaviour of some towers of function fields over finite fields. *J. Number Theory,* **61**, 1996, 248-273.

[6] O. Geil: On codes from norm-trace curves. *Finite Fields and their Applications* **9** (2003), 351-371.

[7] O. Geil and T. Høholdt: Footprints or Generalized Bezout's Theorem. *IEEE Trans. Inform. Theory,* **46**, 2000, 635-641.

[8] O. Geil and T. Høholdt: On Hyperbolic Type Codes. *Proceedings of 2003 IEEE International Symposium on Inf. Theory,* Yokohama, 2003, 331.

[9] T. Høholdt: On (or in) Dick Blahut's 'footprint', in "Codes, Curves and Signals," (A. Vardy, Ed.), Kluwer Academic, Norwell, MA, 1998, 3-9.

[10] T. Høholdt, J. van Lint and R. Pellikaan: Algebraic Geometry Codes, Chapter 10 in "Handbook of Coding Theory," (V.S. Pless and W.C. Huffman, Eds.), vol. 1, Elsevier, Amsterdam, 1998, 871-961.

[11] S. Miura and N. Kamiya: Geometric-Goppa codes on some maximal curves and their minimumdistance. *Proc. of 1993 IEEE Inf. Th. Workshop* Susononshi, Shizuoka, Japan, June 4-8, 1993, 85-86.

[12] G. L. Matthews and J. Peachey: Small-bias sets from extended norm-trace codes. To appear in Proceedings of Fq10, *Contemporary Mathematics*, AMS.

[13] J. Massey, D. J. Costello, and J. Justesen: Polynomial Weights and Code Constructions. *IEEE Trans. Inf. Theory*, **19**, 1973, 101-110.

[14] R. Meka and D. Zuckerman: Small-Bias Spaces for Group Products. *APPROX-RANDOM* 2009, 658-672.

[15] J. Naor and M. Naor: Small-bias probability spaces: eficient construction and applications. *SIAM J. Comput.* **22** (1993), 838-856.

[16] K. W. Shum, I. Aleshnikov, P. Vijay Kumar, H. Stichtenoth, and V. Deolalikar: A Low-Complexity Algorithm for the Construction of Algebraic-Geometric Codes Better Than the Gilbert-Varshamov Bound. *IEEE Trans. Inform. Theory,* **47**, 2001, 2225-2241.

[17] U. V. Vazirani: Randomness, adversaries, and computation, Ph.D. thesis, EECS, UC Berkeley, 1986.

PAPER II

An improvement of the Feng-Rao bound for primary codes

Geil Olav Martin Stefano

Geil Olav and Martin Stefano, "An improvement of the Feng-Rao bound for primary codes", *accepted to Designs, Codes and Cryptography (DESI)*, 2013, preprint at arXiv: 1307.3107v2 [cs.IT], DOI: 10.1007/s10623-014-9983-z

An improvement of the Feng-Rao bound for primary codes

Olav Geil[11] and Stefano Martin[21,2]

[1]Department of Mathematical Sciences, Aalborg University
[2]Engineering Software Institute, East China Normal University

[1]olav@math.aau.dk
[2]stefano@math.aau.dk

Abstract

We present a new bound for the minimum distance of a general primary linear code. For affine variety codes defined from generalised C_{ab} polynomials the new bound often improves dramatically on the Feng-Rao bound for primary codes [1, 12]. The method does not only work for the minimum distance but can be applied to any generalised Hamming weight.

Keywords: Affine variety code, C_{ab} curve, Feng-Rao bound, footprint bound, generalised C_{ab} polynomial, generalised Hamming weight, minimum distance, one-way well-behaving pair, order domain conditions.

MSC: 94B65, 94B27, 94B05.

Chapter 1

Introduction

In this paper we present an improvement to the Feng-Rao bound for *primary* codes [1, 12, 10]. Our method does not only apply to the minimum distance but estimates any generalised Hamming weight. In the same way as the Feng-Rao bound for primary codes suggests an improved code construction our new bound does also. The new bound is particularly suited for affine variety codes for which it often improves dramatically on the Feng-Rao bound. Interestingly, for such codes it can be viewed as a simple application of the footprint bound from Gröbner basis theory. We pay particular attention to the case of the affine variety being defined by a bivariate polynomial that, in the support, has two univariate monomials of the same weight and all other monomials of lower weights. Such polynomials can be viewed as a generalisation of the polynomials defining C_{ab} curves and therefore we name them *generalised C_{ab} polynomials*. We develop a method for constructing generalised C_{ab} polynomials with many zeros by the use of $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomials, that are polynomials returning values in $\mathbb{F}_p$ when evaluated in $\mathbb{F}_{p^m}$ (see, [23, Chap. 1]). Here, p is any prime power and m is an integer larger than 1. With this method in hand we can design long affine variety codes for which our bound produces good results. The new bound of the present paper is closely related to an improvement of the Feng-Rao bound for *dual* codes that we presented recently in [9]. Recall from [10] that the usual Feng-Rao bound for primary and dual codes can be viewed as consequences of each other. This result holds when one uses the concept of well-behaving pairs or one-way well-behaving pairs. For weakly well-behaving pairs a possible connection is unknown. In a similar way as the proof from [10] breaks down for weakly well-behaving, it also breaks down when one tries to establish a connection between the new bound from the present paper and the new bound from [9]. We shall leave it as an open problem to decide if the two bounds are consequences of each other or not.

In the first part of the paper we concentrate solely on affine variety codes. For such codes the new method is intuitive. We start by formulating in Section 2 our new bound at the level of affine variety codes and explain how it gives rise to an improved code construction $\widetilde{E}_{imp}(\delta)$. Then we continue in Section 3 by showing

how to construct generalised C_{ab} polynomials with many zeros. In Section 4 we give a thorough treatment of codes defined from so-called optimal generalised C_{ab} polynomials demonstrating the strength of our new method. In Section 5 we show how to improve the improved code construction $\widetilde{E}_{imp}(\delta)$ even further. This is done for the case of the affine variety being the Klein quartic. Having up till now only considered the minimum distance, in Section 6 we explain how to deal with generalised Hamming weights. Section 7 generalises the new bound to arbitrary primary linear codes. In Section 8 we recall the recent bound from [9] on dual codes, and in Section 9 we discuss the relation between this bound and the new bound of the present paper. Section 10 is the conclusion.

Chapter 2

Improving the Feng-Rao bound for primary affine variety codes

Affine variety codes were introduced by Fitzgerald and Lax in [5] as follows. For q a prime power consider an ideal $I \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$ and define

$$I_q = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle, \tag{2.1}$$

$$R_q = \mathbb{F}_q[X_1, \ldots, X_m]/I_q.$$

Let $\{P_1, \ldots, P_n\} = \mathbb{V}_{\mathbb{F}_q}(I_q)$ be the corresponding variety over $\mathbb{F}_q$. Here, $P_i \neq P_j$ for $i \neq j$. Define the $\mathbb{F}_q$-linear map $\mathrm{ev} : R_q \to \mathbb{F}_q^n$ by $\mathrm{ev}(A + I_q) = (A(P_1), \ldots, A(P_n))$. It is well-known that this map is a vector space isomorphism.

Definition 1. *Let L be an $\mathbb{F}_q$ vector subspace of R_q. Define $C(I, L) = ev(L)$ and $C^{\perp}(I, L) = \big(C(I, L)\big)^{\perp}$.*

We shall call $C(I, L)$ a primary affine variety code and $C^{\perp}(I, L)$ a dual affine variety code. For the case of primary affine variety codes both the Feng-Rao bound and the bound of the present paper can be viewed as consequences of the footprint bound from Gröbner basis theory as we now explain.

Definition 2. *Let $J \subseteq k[X_1, \ldots, X_m]$ be an ideal and let $\prec$ be a fixed monomial ordering. Here, k is an arbitrary field. Denote by $\mathcal{M}(X_1, \ldots, X_m)$ the monomials in the variables $X_1, \ldots, X_m$. The footprint of J with respect to $\prec$ is the set*

$$\begin{aligned} \Delta_{\prec}(J) \quad = \quad & \{M \in \mathcal{M}(X_1, \ldots, X_m) \mid M \text{ is not} \\ & \qquad \text{the leading monomial of any polynomial in } J\}. \end{aligned}$$

Proposition 3. *Let the notation be as in Definition 2. The set $\{M + J \mid M \in \Delta_{\prec}(J)\}$ constitutes a basis for $k[X_1, \ldots, X_m]/J$ as a vector space over k.*

Proof. See [3, Pro. 4, Sec. 5.3]. □

We shall make extensive use of the following incidence of the footprint bound (for a more general version, see [8]).

Corollary 4. *Let $F_1, \ldots, F_s \in \mathbb{F}_q[X_1, \ldots, X_m]$. For any monomial ordering $\prec$ the variety $\mathbb{V}_{\mathbb{F}_q}(\langle F_1, \ldots, F_s \rangle)$ is of size equal to $\#\Delta_\prec(\langle F_1, \ldots, F_s, X_1^q - X_1, \ldots, X_m^q - X_m \rangle)$.*

Proof. Follows from Proposition 3 and the fact that the map ev is a bijection. □

We next recall the interpretation from [7] of the Feng-Rao bound for primary affine variety codes.

Definition 5. *A basis $\{B_1 + I_q, \ldots, B_{\dim(L)} + I_q\}$ for a subspace $L \subseteq R_q$ where $Supp(B_i) \subseteq \Delta_\prec(I_q)$ for $i = 1, \ldots, \dim(L)$ and where $lm(B_1) \prec \cdots \prec lm(B_{\dim(L)})$, is said to be well-behaving with respect to $\prec$. Here, $lm(F)$ means the leading monomial of the polynomial F.*

For fixed $\prec$ the sequence $(\mathrm{lm}(B_1), \ldots, \mathrm{lm}(B_{\dim(L)}))$ is the same for all choices of well-behaving bases of L. Therefore the following definition makes sense.

Definition 6. *Let L be a subspace of R_q and define*

$$\square_\prec(L) = \{lm(B_1), \ldots, lm(B_{\dim(L)})\},$$

where $\{B_1 + I_q, \ldots, B_{\dim(L)} + I_q\}$ is any well-behaving basis for L.

The concept of one-way well-behaving plays a crucial role in the Feng-Rao bound as well as in our new bound. It is a relaxation of the well-behaving property and the weakly well-behaving property [7, 12] and therefore it gives the strongest bounds.

Definition 7. *Let $\mathcal{G}$ be a Gröbner basis for I_q with respect to $\prec$. An ordered pair of monomials (M_i, M_j), $M_i, M_j \in \Delta_\prec(I_q)$ is said to be one-way well-behaving (OWB) if for all $H \in \mathbb{F}_q[X_1, \ldots, X_m]$ with $Supp(H) \subseteq \Delta_\prec(I_q)$ and $lm(H) = M_i$ it holds that*

$$lm(M_i M_j \ rem \ \mathcal{G}) = lm(H M_j \ rem \ \mathcal{G}).$$

Here, F rem $\mathcal{G}$ means the remainder of F after division with $\mathcal{G}$ (see [3, Sec. 2.3] for the division algorithm for multivariate polynomials).

Remark 8. *An alternative, but equivalent, definition is that (M_i, M_j) is OWB if*

$$lm(M_{i'} M_{j'} \ rem \ \mathcal{G}) \prec lm(M_i M_j \ rem \ \mathcal{G}) \tag{2.2}$$

holds for all $i' < i$ and $j = j'$. From this form it is easy to see the relation to well-behaving pairs (WB) and weakly well-behaving pairs (WWB). A pair is WB if (2.2) holds for all $i' \leq i$, $j' \leq j$ such that $(i', j') \neq (i, j)$. Finally, for WWB the requirement is that the result should hold for all pairs (i', j') such that either $i' < i$ and $j' = j$ or $i' = i$ and $j' < j$. Hence, OWB implies WWB which implies WB.

As noted in [7] the concept of OWB is independent of which Gröbner basis $\mathcal{G}$ is used as long as I_q and $\prec$ are fixed. We are now ready to describe the Feng-Rao bound for primary affine variety codes. We include the proof from [7, Th. 4.9].

Theorem 9. *Let $\mathcal{G}$ be a Gröbner basis for I_q with respect to $\prec$. Consider a non-zero word $\vec{c}$ and let A be the unique polynomial such that $Supp(A) \subseteq \Delta_\prec(I_q)$ and $\vec{c} = ev(A)$. Let $lm(A) = P$. We have*

$$\begin{aligned} w_H(\vec{c}) \quad \geq \quad & \#\{K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q) \text{ such that} \\ & (P, N) \text{ is OWB and } lm(PN \text{ rem } \mathcal{G}) = K\}. \end{aligned} \tag{2.3}$$

A bound on the minimum distance of $C(I, L)$ is found by taking the minimum of (2.3) when P runs through $\Box_\prec(L)$.

Proof. From Corollary 4 we know that

$$\begin{aligned} w_H(\vec{c}) &= n - \#\Delta_\prec(I_q + \langle A \rangle) \\ &= \#\Delta_\prec(I_q) - \#\Delta_\prec(I_q + \langle A \rangle) \\ &= \#\Big(\Delta_\prec(I_q) \backslash \Delta_\prec(I_q + \langle A \rangle)\Big). \end{aligned} \tag{2.4}$$

If $N, K \in \Delta_\prec(I_q)$ satisfy that (P, N) is OWB and $\mathrm{lm}(PN \text{ rem } \mathcal{G}) = K$ then $K \in \Delta_\prec(I_q) \backslash \Delta_\prec(I_q + \langle A \rangle)$. Hence,

$$\begin{aligned} w_H(\vec{c}) \quad \geq \quad & \#\{K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q) \text{ such that} \\ & (P, N) \text{ is OWB and } \mathrm{lm}(PN \text{ rem } \mathcal{G}) = K\}. \end{aligned}$$

□

The Feng-Rao bound is particular suited for affine varieties which satisfy the order domain conditions [7, Def. 4.22] (the order domain conditions are listed in Definition 11 below). For other varieties it does not seem to produce very good results. The new bound of the present paper solves this problem for affine varieties which satisfy the first half of the order domain conditions. This gives a lot of freedom as the latter set of varieties is much larger than the former. In its most general form the order domain conditions involve a weighted degree monomial ordering with weights $w(X_1), \ldots, w(X_m)$ in $\mathbb{N}_0^r \backslash \{\vec{0}\}$, r a positive integer (see [7, Def. 4.21]). Here, for simplicity we shall only consider weights in $\mathbb{N}$.

Definition 10. *Let $w(X_1), \ldots, w(X_m) \in \mathbb{N}$ and define the weight of $X_1^{i_1} \cdots X_m^{i_m}$ to be the number $w(X_1^{i_1} \cdots X_m^{i_m}) = i_1 w(X_1) + \cdots + i_m w(X_m)$. The weighted degree ordering $\prec_w$ on $\mathcal{M}(X_1, \ldots, X_m)$ is the ordering with $X_1^{i_1} \cdots X_m^{i_m} \prec_w X_1^{j_1} \cdots X_m^{j_m}$ if either $w(X_1^{i_1} \cdots X_m^{i_m}) < w(X_1^{j_1} \cdots X_m^{j_m})$ holds or $w(X_1^{i_1} \cdots X_m^{i_m}) = w(X_1^{j_1} \cdots X_m^{j_m})$ holds but $X_1^{i_1} \cdots X_m^{i_m} \prec' X_1^{j_1} \cdots X_m^{j_m}$. Here, $\prec'$ is some fixed monomial ordering. When $\prec'$ is the lexicographic ordering $\prec_{lex}$ with $X_m \prec_{lex} \cdots \prec_{lex} X_1$ we shall call $\prec_w$ a weighted degree lexicographic ordering.*

We now state the order domain conditions which play a central role in the present paper.

Definition 11. *Consider an ideal $J \subseteq k[X_1, \ldots, X_m]$ where k is a field. Let a weighted degree ordering $\prec_w$ be given. Assume that J possesses a Gröbner basis $\mathcal{F}$ with respect to $\prec_w$ such that:*

(C1) Any $F \in \mathcal{F}$ has exactly two monomials of highest weight.

(C2) No two monomials in $\Delta_{\prec_w}(J)$ are of the same weight.

Then we say that J and $\prec_w$ satisfy the order domain conditions.

If J satisfies the conditions in Definition 11 then $k[X_1, \ldots, X_m]/J$ is an order domain (see [7, Th. 4.31]). This explains why they are called the order domain conditions.

In the following we restrict to weighted degree orderings where $\prec' = \prec_{lex}$. That is, $\prec_w$ shall always be a weighted degree lexicographic ordering.

Example 1. *Consider $I = \langle X^2 + X - Y^3 \rangle \subseteq \mathbb{F}_4[X, Y]$ and I_4 accordingly (see (2.1)). Choosing $X = X_1$, $Y = X_2$, $w(X) = 3$ and $w(Y) = 2$ we see that the order domain conditions are satisfied. By inspection we have*

$$\Delta_{\prec_w}(I_4) = \{1, Y, X, Y^2, XY, Y^3, XY^2, XY^3\}$$

with corresponding weights $\{0, 2, 3, 4, 5, 6, 7, 9\}$. Consider a word $\vec{c} = ev(A + I_4)$ where $A = a_1 1 + a_2 Y + a_3 X$, $a_1, a_2 \in \mathbb{F}_4$ and $a_3 \in \mathbb{F}_4 \backslash \{0\}$. By Corollary 4 the length is $n = 8$. We now estimate the Hamming weight $w_H(\vec{c}) = \#\big(\Delta_{\prec_w}(I_4) \backslash \Delta_{\prec_w}(I_4 + \langle A \rangle)\big)$ (see (2.4)). The following elements in $\Delta_{\prec_w}(I_4)$ do not belong to $\Delta_{\prec_w}(I_4 + \langle A \rangle)$. Namely, $lm(A \cdot 1) = X$, $lm(A \cdot Y) = XY$, $lm(A \cdot Y^2) = XY^2$, $lm(A \cdot Y^3) = XY^3$, and $lm(A \cdot X \text{ rem } X^2 + X - Y^3) = Y^3$. Observe that the last calculation holds due to the fact that $X^2 + X - Y^3$ contains exactly two monomials of the highest weight. We have shown that the Hamming weight of $\vec{c}$ is at least 5. With the proof of Theorem 9 in mind an equivalent formulation of the above is to observe that $(X, 1)$, (X, Y), (X, Y^2), (X, Y^3), and (X, X) are OWB. Another equivalent method is guaranteed by the condition that $\Delta_{\prec_w}(I)$ does not contain two monomials of the same weight. This implies that rather than counting the above OWB pairs we only need to observe that $w(\Delta_{\prec_w}(I_4)) \cap \big(w(X) + w(\Delta_{\prec_w}(I_4))\big) = \{3, 5, 6, 7, 9\}$. Again, a set of size 5.

The following Proposition (corresponding to [7, Pro. 4.25]) summarises how the Feng-Rao bound is supported by the order domain condition.

Proposition 12. *Assume $I \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$ and $\prec_w$ satisfy the order domain conditions. Consider $I_q = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$. A pair (P, N) where $P, N \in \Delta_{\prec_w}(I_q)$ is OWB if $w(P) + w(N) \in w(\Delta_{\prec_w}(I_q))$.*

The order domain conditions historically [15, 22, 1, 7] were designed to support the Feng-Rao bounds and therefore it is not surprising that the bound does not work very well without them. The improvement to the Feng-Rao bound that we introduce below allows us to consider relaxed conditions in that we can produce good estimates in the case that the order domain condition (C1) is satisfied but (C2) is not. Note that the order domain condition (C1) alone does not ensure that the quotient ring is a domain – consider for instance $\langle (X^2 - Y^3)(X^2 + Y^3) \rangle$. The following example illustrates the idea in our improvement to Theorem 9.

Example 2. *Consider* $I = \langle X^4 + X^2 + X - Y^6 - Y^5 - Y^3 \rangle \subseteq \mathbb{F}_8[X, Y]$. *Let* $\prec_w$ *be the weighted degree lexicographic ordering (Definition 10) given by* $X = X_1$, $Y = X_2$, $w(X) = 3$ *and* $w(Y) = 2$. *From [24, Sec. 3] and [9, Sec. 4.2] we know that the variety* $\mathbb{V}_{\mathbb{F}_8}(I_8)$ *is of size* 32. *Combining this observation with Corollary 4 we see that*

$$\Delta_{\prec_w}(I_8) = \{X^\alpha Y^\beta \mid 0 \leq \alpha < 4, 0 \leq \beta < 8\}.$$

By inspection we see that some weights appear twice in $\Delta_{\prec_w}(I_8)$, *some only once. Consider* $\vec{c} = ev(A + I_8)$ *where* $lm(A) = X^3$. *That is,*

$$\begin{aligned} A &= a_1 1 + a_2 Y + a_3 X + a_4 Y^2 + a_5 XY + a_6 Y^3 + a_7 X^2 + \\ &\quad a_8 XY^2 + a_9 Y^4 + a_{10} X^2 Y + a_{11} XY^3 + a_{12} X^3. \end{aligned}$$

Here, $a_i \in \mathbb{F}_8$, $i = 1, \ldots, 12$ *and* $a_{12} \neq 0$. *Note that* A *has two monomials of the highest weight if* $a_{11} \neq 0$, *namely* X^3 *and* XY^3. *Following the proof of Theorem 9 we consider* $P = X^3$ *and look for* $N, K \in \Delta_{\prec_w}(I_8)$ *such that* (P, N) *is OWB and* $lm(PN \text{ rem } \mathcal{G}) = K$. *We have the following possible choices of* (N, K), *namely* $(1, X^3)$, (Y, X^3Y), $(Y^2, X^3Y^2), \ldots, (Y^7, X^3Y^7)$, (X^3, X^2Y^6), (X^3Y, X^2Y^7). *From this we conclude that* $w_H(\vec{c}) \geq 10$.
Note that $X^3 \cdot X \text{ rem } \mathcal{G} = Y^6$. *However,* (X^3, X) *is not OWB as*

$$XY^3 \prec_w X^3 \text{ but } XY^3 \cdot X \text{ rem } \mathcal{G} = X^2Y^3 \succ_w Y^6. \tag{2.5}$$

Our improved method consists in considering separately two different cases: $XY^3 \in Supp(A)$ *and* $XY^3 \notin Supp(A)$.

Case 1: Assume $a_{11} \neq 0$. *Following (2.5) we see that* $lm(A \cdot X \text{ rem } \mathcal{G}) = X^2Y^3$. *In a similar way we derive* $lm(A \cdot XY \text{ rem } \mathcal{G}) = X^2Y^4$ *and* $lm(A \cdot XY^2 \text{ rem } \mathcal{G}) = X^2Y^5$. *From this we conclude*

$$\begin{aligned} \Delta_{\prec_w}(I_q + \langle A \rangle) \subseteq \{X^\alpha Y^\beta \quad \mid \quad & 0 \leq \alpha < 3, 0 \leq \beta < 8, \\ & \text{and if } \alpha = 2 \text{ then } \beta < 3\} \end{aligned}$$

and therefore that $w_H(\vec{c}) = n - \#\Delta_{\prec_w}(I_8 + \langle A \rangle) \geq 32 - 19 = 13$.

Case 2: Assume $a_{11} = 0$. *This means that we do not have to worry about (2.5) and consequently* $lm(A \cdot X \text{ rem } \mathcal{G}) = Y^6$ *holds. In a similar way we derive* $lm(A \cdot X^2 \text{ rem } \mathcal{G}) = XY^6$, $lm(A \cdot XY \text{ rem } \mathcal{G}) = Y^7$, *and* $lm(A \cdot X^2Y \text{ rem } \mathcal{G}) = XY^7$. *We conclude that*

$$\Delta_{\prec_w}(I_q + \langle A \rangle) \subseteq \{X^\alpha Y^\beta \mid 0 \leq \alpha < 3, 0 \leq \beta < 6\}$$

and therefore from the proof of Theorem 9 we have that $w_H(\vec{c}) = n - \#\Delta_{\prec_w}(I_8 + \langle A \rangle) \geq 32 - 18 = 14$.

In conclusion $w_H(\vec{c}) \geq \min\{13, 14\} = 13$.

With Example 2 in mind we now improve upon Theorem 9.

Definition 13. *Let $\mathcal{G}$ be a Gröbner basis for I_q with respect to a fixed arbitrary monomial ordering $\prec$. Write $\Delta_\prec(I_q) = \{M_1, \ldots, M_n\}$ with $M_1 \prec \cdots \prec M_n$. Let $\mathcal{I} = \{1, \ldots, n\}$ and consider $\mathcal{I}' \subseteq \mathcal{I}$. An ordered pair of monomials (M_i, M_j), $1 \leq i, j \leq n$ is said to be strongly one-way well-behaving (SOWB) with respect to $\mathcal{I}'$ if for all H with $Supp(H) \subseteq \{M_s \mid s \in \mathcal{I}'\}$, $M_i \in Supp(H)$ it holds that $lm(M_i M_j \ rem \ \mathcal{G}) = lm(H M_j \ rem \ \mathcal{G})$.*

Remark 14. *SOWB is a generalisation of OWB. Concretely (M_i, M_j) is OWB if and only if (M_i, M_j) is SOWB with respect to $\{1, \ldots, i\}$.*

In the following, when writing $\Delta_\prec(I_q) = \{M_1, \ldots, M_n\}$, we shall always assume that $M_1 \prec \cdots \prec M_n$ holds.
Consider a non-zero codeword $\vec{c} = \mathrm{ev}(A + I_q)$, where $A = \sum_{s=1}^{i} a_s M_s$, $i \geq 2$, $a_s \in \mathbb{F}_q$ for $s = 1, \ldots, i$ and $a_i \neq 0$. Let v be an integer $1 \leq v < i$. We consider $v + 1$ different cases that cover all possibilities:

Case 1: $a_{i-1} \neq 0$.

Case 2: $a_{i-1} = 0$, $a_{i-2} \neq 0$.

$\vdots$

Case v: $a_{i-1} = a_{i-2} = \cdots = a_{i-v+1} = 0$, $a_{i-v} \neq 0$.

Case v+1: $a_{i-1} = \cdots = a_{i-v} = 0$.

For each of the above $v + 1$ cases we shall estimate $n - \#\Delta_\prec(I_q + \langle A \rangle)$. Then the minimal obtained value constitutes a lower bound on $w_H(\vec{c})$. Note that in Example 2 we used $v = 1$.

Theorem 15. *Let $\prec$ be a fixed arbitrary monomial ordering. Consider $\vec{c} = ev(\sum_{s=1}^{i} a_s M_s + I_q)$, $a_s \in \mathbb{F}_q$, $s = 1, \ldots, i$, and $a_i \neq 0$. Let v be an integer $0 \leq v < i$. We have $w_H(\vec{c}) \geq \sigma(i, v)$ where $\sigma(i, v) = \min\{\#\mathcal{L}(1), \ldots, \#\mathcal{L}(v + 1)\}$. Here, for $t = 1, \ldots, v$*

$$\begin{aligned} \mathcal{L}(t) \ = \ & \big\{K \in \Delta_\prec(I_q) \mid \exists M_j \in \Delta_\prec(I_q) \text{ such that either} \\ & (M_i, M_j) \text{ is SOWB with respect to } \{1, \ldots, i - t, i\} \\ & \text{and } lm(M_i M_j \ rem \ \mathcal{G}) = K \text{ or} \\ & (M_{i-t}, M_j) \text{ is SOWB with respect to } \{1, \ldots, i - t, i\} \\ & \text{and } lm(M_{i-t} M_j \ rem \ \mathcal{G}) = K\big\}, \end{aligned}$$

and

$$\begin{aligned} \mathcal{L}(v + 1) \ = \ & \big\{K \in \Delta_\prec(I_q) \mid \exists M_j \in \Delta_\prec(I_q) \text{ such that } (M_i, M_j) \\ & \text{is SOWB with respect to } \{1, \ldots, i - v - 1, i\} \\ & \text{and } lm(M_i M_j \ rem \ \mathcal{G}) = K\big\}. \end{aligned}$$

Given a code $C(I,L)$ write $\Box_{\prec}(L) = \{M_{i_1}, \ldots, M_{i_{\dim(L)}}\}$ and choose numbers $v_{i_1}, \ldots, v_{i_{\dim(L)}}$ with $0 \leq v_{i_s} < i_s$, $s = 1, \ldots, \dim(L)$. The minimum distance of $C(I,L)$ is at least $\min\{\sigma(i_1, v_1), \ldots, \sigma(i_{\dim(L)}, v_{i_{\dim(L)}})\}$.

Proof. To establish the bound on $w_H(\vec{c})$ note that if $v = 0$ then only the last set $\mathcal{L}(v+1)$ is present and this set equals the set in (2.3). For $v > 0$ the $v+1$ expressions correspond to the $v+1$ cases described prior to the theorem (in the same order). The proof technique resembles the arguments used in Example 2. □

Remark 16. *Consider an ideal $I \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$ and a corresponding weighted degree lexicographic ordering $\prec_w$ such that the order domain condition (C1) is satisfied but (C2) is not. Let $\mathcal{F}$ be a Gröbner basis for I with respect to $\prec_w$. Assume Theorem 15 is used to estimate the Hamming weight of $\vec{c} = ev(A + I_q)$ where $lm(A) = M_i$. A natural choice of v is the unique non-negative integer which satisfies $w(M_i) = w(M_{i-1}) = \cdots = w(M_{i-v}) > w(M_{i-v-1})$. To see why this choice of v is natural, note that when reducing AM_j modulo $\mathcal{F}$ the weight of the leading monomial remains the same. Hence, the leading monomial of AM_j rem $\mathcal{F}$ can not be equal to $M_t M_j$ rem $\mathcal{F}$ for $t \leq i - v - 1$. On the other hand as illustrated in Example 2 this may happen when $t \geq i - v$. If both order domain conditions are satisfied the above choice of v is $v = 0$. In this case Theorem 15 simplifies to the usual Feng-Rao bound Theorem 9.*

Theorem 15 can be applied to any code $C(I,L)$. However, it is not clear if there is any advantage in considering other choices of L than $L = \mathrm{Span}_{\mathbb{F}_q}\{\mathrm{ev}(M_{i_1} + I_q), \ldots, \mathrm{ev}(M_{i_k} + I_q)\}$. When $i_1 = 1, \ldots, i_k = k$ we shall denote the corresponding code by $E(k)$. Observe that Theorem 15 suggests an improved code construction as follows.

Definition 17. *Consider a set of integers $v_1, \ldots, v_n$ with $0 \leq v_i < i$ for $i = 1, \ldots n$. Let $L = Span_{\mathbb{F}_q}\{ev(M_i + I_q) \mid \sigma(i, v_i) \geq \delta\}$, The corresponding code $C(I,L)$ is denoted by $\widetilde{E}_{imp}(\delta)$.*

Proposition 18. *The minimum distance of $\widetilde{E}_{imp}(\delta)$ satisfies $d(\widetilde{E}_{imp}(\delta)) \geq \delta$.*

The above improved code construction is in the spirit of Feng and Rao's work. When improved codes are constructed on the basis of the Feng-Rao bound, Theorem 9, rather than on the basis of the improved bound of the present paper, Theorem 15, the notation used is $\widetilde{E}(\delta)$ (see [7, Def. 4.38]). In Section 5 we shall see that one can sometimes derive even further improved codes from Theorem 15 than $\widetilde{E}_{imp}(\delta)$. In a straight forward manner one can enhance the above bound to deal also with generalised Hamming weights. We postpone the discussion of the details to Section 6.

A huge class of ideals and weighted degree lexicographic orderings satisfies the conditions in Remark 16. For every such pair I, $\prec_w$ it is easy to apply the method of Theorem 15 using a computer. In the remaining part of the paper we shall mainly concentrate on studying certain families of affine variety codes for which we can derive closed formula expressions. The potential of Theorem 15 goes beyond this. We leave it as an open research problem to establish closed formula expressions for other families.

Chapter 3

Generalised C_{ab} polynomials

As mentioned in the previous section good candidates for our new bound are affine variety codes where the order domain condition (C1) is satisfied, but the order domain condition (C2) is not. A particular simple class of curves that satisfy the order domain conditions are the well-known C_{ab} curves. They were introduced by Miura in [19, 20, 21] to facilitate the use of the Feng-Rao bound for dual codes. In this section we introduce generalised C_{ab} polynomials which correspond to allowing the same weight to occur more than once in the footprint (condition (C2)). It should be stressed that we make no assumption that generalised C_{ab} polynomials are irreducible as it has no implication for our analysis.
From [21, App. B and the lemma at p. 1416] we have a complete characterisation of C_{ab} curves. We shall adapt the description in [18] which is an English translation of Miura's results. From [18, Th. 1] we have:

Theorem 19. *Let $\bar{k}$ be the algebraic closure of a perfect field k, $\mathcal{X} \subseteq \bar{k}^2$ be a possibly reducible affine algebraic set defined over k, x, y the coordinates of the affine plane $\bar{k}^2$, and a, b relatively prime positive integers. The following two conditions are equivalent:*

- *$\mathcal{X}$ is an absolutely irreducible algebraic curve with exactly one k rational place Q at infinity, and the pole divisors of x and y are bQ and aQ, respectively.*
- *$\mathcal{X}$ is defined by a bivariate polynomial of the form*

$$\alpha_{a,0}x^a + \alpha_{0,b}y^b + \sum_{ib+ja<ab} \alpha_{i,j}x^i y^j, \tag{3.1}$$

where $\alpha_{i,j} \in k$ for all i, j and $\alpha_{a,0}$, $\alpha_{0,b}$ are non-zero.

The definition of C_{ab} curves given in the literature is that of (3.1). We recall the following result from [21]. We adapt the description from [18, Cor. 3].

Proposition 20. *Let $F(X,Y) \in k[X,Y]$ be a polynomial of the form (3.1), Q a unique place at infinity of the C_{ab} curve defined by $F(X,Y)$. Then*

$$\{X^iY^j + \langle F(X,Y)\rangle \mid 0 \le i \le a-1, 0 \le j\}$$

is a k-basis for $k[X,Y]/\langle F(X,Y)\rangle$ and the elements in the basis have pairwise distinct discrete valuations at Q. If the C_{ab} curve is non-singular, then

$$k[X,Y]/\langle F(X,Y)\rangle = \mathcal{L}(\infty Q)$$

holds, and as a basis for $\mathcal{L}(mQ)$, $m \geq 0$, we can choose

$$\{X^iY^j + \langle F(X,Y)\rangle \mid 0 \leq i \leq a-1, 0 \leq j, ai+bj \leq m\}.$$

Let $w(X)$ and $w(Y)$, respectively, be minus the discrete valuation of x at Q and minus the discrete valuation of y at Q, respectively. Consider the corresponding weighted degree lexicographic ordering with $X = X_1$ and $Y = X_2$. If we combine (3.1) with the first part of Proposition 20 we see that C_{ab} curves satisfy the order domain conditions. Observe, that we can consider the related affine variety codes $C(I,L)$ and $C^{\perp}(I,L)$ regardless of the curve being non-singular or not. This point of view is taken in [15, Sec. 4.2]. Even if the curve is non-singular no simple generic method is known to describe the corresponding affine variety code as an algebraic geometric code. We now introduce generalised C_{ab} polynomials.

Definition 21. *Let $w(X) = \frac{b}{\gcd(a,b)}$ and $w(Y) = \frac{a}{\gcd(a,b)}$ where a and b are two different positive integers. Given a field k, let $F(X,Y) = X^a + \alpha Y^b + R(X,Y) \in k[X,Y]$, $\alpha \in k\backslash\{0\}$, be such that all monomials in the support of R have smaller weight than $w(X^a) = w(Y^b) = \frac{ab}{\gcd(a,b)}$. Then $F(X,Y)$ is called a generalised C_{ab} polynomial.*

Miura in [19, Sec. 4.1.4] treated the curves related to irreducible generalised C_{ab} polynomials. Besides that we do not require the generalised C_{ab} polynomials to be irreducible, our point of view is different from Miura's as we will use for the code construction the algebra $\mathbb{F}_q[X,Y]/\langle F(X,Y)\rangle$. For generalised C_{ab} polynomials this algebra does not in general equal a space $\mathcal{L}(m_1P_1 + \cdots + m_sP_s)$, $P_1, \ldots, P_s$ being rational places. We mention that the variations of C_{ab} curves considered by Feng and Rao in [4] are different from Definition 21.

For the code construction we would like to have generalised C_{ab} polynomials with many zeros and at the same time to have a variety of possible a, b to choose from, as these parameters turn out to play a crucial role in our bound for the minimum distance. As we shall now demonstrate there is a simple technique for deriving this when the field under consideration is not prime. The situation is in contrast to C_{ab} curves for which it is only known how to get many points for restricted classes of a and b. Our method builds on ideas from [24] and [19, Sec. 5]. Let p be a prime power and $q = p^m$ where $m \geq 2$ is an integer. The technique that we shall employ involves letting $F(X,Y) = G(X) - H(Y)$ where both G and H are $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomials.

Definition 22. *Let m be an integer, $m \geq 2$. A polynomial $F(X) \in \mathbb{F}_{p^m}[X]$ is called an $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomial if $F(\gamma) \in \mathbb{F}_p$ holds for all $\gamma \in \mathbb{F}_{p^m}$.*

An obvious characterisation of $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomials is that $F(X) = (X^{p^m} - X)Q(X) + F'(X)$, where $F'(X)$ is an $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomial of degree less than p^m.

Here, we used the convention that $\deg(0) = -\infty$. By Fermat's little theorem the set of $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomials of degree less than p^m constitutes a vector space over $\mathbb{F}_p$. Clearly, one could derive a basis by Lagrange interpolation. For our purpose, however, it is interesting to know what are the possible degrees of the polynomials in the vector space.

Proposition 23. *Let $C_{i_1}, \ldots, C_{i_t}$ be the different cyclotomic cosets modulo $p^m - 1$ (multiplication by p). Here, for $s = 1, \ldots, t$ it is assumed that i_s is chosen as the smallest element in the given coset. For $s = 1, \ldots, t$, $F_{i_s}(X) = \sum_{l \in C_{i_s}} X^l$, is an $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomial. Furthermore, the polynomial X^{p^m-1} is an $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomial.*

Proof. For all the polynomials F in the proposition we have $F^p \bmod X^{p^m} - X = F$. □

The set $\{F_{i_1}, \ldots, F_{i_t}, X^{p^m-1}\}$ contains two of the most prominent $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomials, namely the trace polynomial $F_1(X) = X^{p^{m-1}} + X^{p^{m-2}} + \cdots + X^p + X$ and the norm polynomial $X^{(p^m-1)/(p-1)}$. Note that the norm polynomial equals $F_{(p^m-1)/(p-1)}$ if $p > 2$. For $p = 2$ it equals X^{p^m-1}. Observe also that except for the constant polynomial $F_0 = 1$, the trace polynomial is of lowest possible degree. From [14, Prop. 3.2] we have (see also [2]):

Proposition 24. *A polynomial $F(X) \in \mathbb{F}_{p^m}[X]$ is an $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomial of degree less than $p^m - 1$ if and only if*

$$F(X) = F_1(H(X)) \text{ rem } (X^{p^m-1} - 1)$$

for some $H(X) \in \mathbb{F}_{p^m}[X]$.

From Proposition 23 and Proposition 24 we conclude:

Corollary 25. *Let $F(X)$ be an $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomial of degree less than p^m. Then $\deg(F) \in \{\deg(F_{i_1}), \ldots, \deg(F_{i_t}), p^m - 1\}$.*

We now return to the question of designing generalised C_{ab} polynomials $F(X, Y) = G(X) - H(Y)$ with many zeros. One way of doing this is to choose $G(X)$ to be the trace polynomial [24, Sec. 3]. As is well-known this polynomial maps exactly p^{m-1} elements from $\mathbb{F}_{p^m}$ to each value in $\mathbb{F}_p$. Hence, such a polynomial $F(X, Y)$ must have p^{2m-1} zeros. However, there are other polynomials in the above set with properties similar to the trace polynomial.

Proposition 26. *Consider the polynomials F_{i_s}, $s = 1, \ldots, t$ related to a field extension $\mathbb{F}_{p^m}/\mathbb{F}_p$, $m \geq 2$ (Proposition 23). We have $\gcd(i_s, p^m - 1) = 1$ if and only if for each $\eta \in \mathbb{F}_p$ there exist exactly p^{m-1} $\gamma \in \mathbb{F}_{p^m}$ such that $F_{i_s}(\gamma) = \eta$.*

Proof. We have $F_{i_s}(X) = F_1(X^{i_s}) \bmod (X^{p^m-1} - 1)$, where $F_1(X)$ is the trace polynomial. Under the condition that $\gcd(i_s, p^m - 1) = 1$ the monomial X^{i_s} defines a bijective map from $\mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$. This proves the "only if" part. We leave the "if" part for the reader. □

Example 3. *Consider first the field extension* $\mathbb{F}_8/\mathbb{F}_2$*. The non-trivial cyclotomic cosets modulo* 7 *are* $C_1 = \{1, 2, 4\}$*, and* $C_3 = \{3, 6, 5\}$*. From this we find the following* $(\mathbb{F}_8, \mathbb{F}_2)$*-polynomials:* $F_1(X) = X^4 + X^2 + X$*,* $F_3(X) = X^6 + X^5 + X^3$*, and* X^7*. The first two polynomials have the property described in Proposition 26. This is a consequence of* 7 *being a prime.*
Consider next the field extension $\mathbb{F}_{16}/\mathbb{F}_2$*. The non-trivial cyclotomic cosets modulo* 15 *are* $C_1 = \{1, 2, 4, 8\}$*,* $C_3 = \{3, 6, 12, 9\}$*,* $C_5 = \{5, 10\}$*,* $C_7 = \{7, 14, 13, 11\}$*. Hence, we get the following* $(\mathbb{F}_{16}, \mathbb{F}_2)$*-polynomials* $F_1(X) = X^8 + X^4 + X^2 + X$*,* $F_3(X) = X^{12}+X^9+X^6+X^3$*,* $F_5(X) = X^{10}+X^5$*,* $F_7(X) = X^{14}+X^{13}+X^{11}+X^7$*, and* X^{15}*. The polynomials with the property described in Proposition 26 are* $F_1(X)$*,* $F_7(X)$*.*
Consider finally the field extension $\mathbb{F}_{32}/\mathbb{F}_2$*. Observe that* 31 *is a prime. Hence, all the polynomials* F_{i_s}*,* $i_s > 0$*, have the property of Proposition 26. These are* $F_1(X) = X^{16} + X^8 + X^4 + X^2 + X$*,* $F_3(X) = X^{24} + X^{17} + X^{12} + X^6 + X^3$*,* $F_5(X) = X^{20} + X^{18} + X^{10} + X^9 + X^5$*,* $F_7(X) = X^{28} + X^{25} + X^{19} + X^{14} + X^7$*,* $F_{11}(X) = X^{26}+X^{22}+X^{21}+X^{13}+X^{11}$*, and* $F_{15}(X) = X^{30}+X^{29}+X^{27}+X^{23}+X^{15}$*.*

Chapter 4

Codes from optimal generalised C_{ab} polynomials

In this section we consider codes from generalised C_{ab} polynomials over $\mathbb{F}_q$ with $n = aq$ zeros. These polynomials are optimal in the sense that a bivariate polynomial with leading monomial X^a can have no more zeros over $\mathbb{F}_q$, as is seen from the footprint bound Corollary 4. Hence, we shall call them *optimal generalised C_{ab} polynomials*.

We list a couple of properties of optimal generalised C_{ab} polynomials $F(X,Y) = X^a + \alpha Y^b + R(X,Y)$. It holds that $a < b$, that $a \leq q$ and that $\{F(X,Y), Y^q - Y\}$ constitutes a Gröbner basis $\mathcal{G}$ for $I_q = \langle F(X,Y), X^q - X, Y^q - Y\rangle$ with respect to $\prec_w$. Here, and in the remaining part of the section, $\prec_w$ is the weighted degree lexicographic ordering in Definition 10 with weights as in Definition 21, $w(X) = \frac{b}{\gcd(a,b)}$, $w(Y) = \frac{a}{\gcd(a,b)}$, and with $X = X_1$, $Y = X_2$. Moreover, it holds that $\{M_1, \ldots, M_n\} = \Delta_{\prec_w}(I_q) = \{X^{i_1}Y^{i_2} \mid 0 \leq i_1 < a, 0 \leq i_2 < q\}$ (recall, that we assume $M_1 \prec_w \cdots \prec_w M_n$). A given weight in $w(\Delta_{\prec_w}(I_q)$ appears at most $\gcd(a,b)$ times. To see this note that for general monomials $X^{\alpha_1}Y^{\alpha_2}$, $X^{\beta_1}Y^{\beta_2}$ with $\alpha_1 \leq \beta_1$ we have $w(X^{\alpha_1}Y^{\alpha_2}) = w(X^{\beta_1}Y^{\beta_2})$ if and only if $\beta_1 = \alpha_1 + uw(Y)$ and $\beta_2 = \alpha_2 - uw(X)$ for some non-negative integer u. For $X^{\alpha_1}Y^{\alpha_2}, X^{\beta_1}Y^{\beta_2} \in \Delta_{\prec_w}(I_q)$ to hold we must have $\beta_1 < a$ and consequently also $u < \gcd(a,b)$.

From the previous section we have a simple method for constructing optimal generalised C_{ab} polynomials over $\mathbb{F}_q = \mathbb{F}_{p^m}$, where p is a prime power and m is an integer greater or equal to 2. The method consists in letting $F(X,Y) = G(X) - H(Y)$ where $G(X)$ is the trace polynomial and $H(Y)$ is an arbitrary non-trivial $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomial. We stress that the results of the present section hold for any optimal generalised C_{ab} polynomial over arbitrary finite field $\mathbb{F}_q$. The main result of the section is:

Theorem 27. *Let I_q be defined from an optimal generalised C_{ab} polynomial and let the weights $w(X)$ and $w(Y)$ be as in Definition 21. Consider $\vec{c} = \mathrm{ev}(\sum_{s=1}^{i} a_s M_s +$*

$I_q)$, $a_s \in \mathbb{F}_q$, $s = 1, \ldots, i$ *and* $a_i \neq 0$. *Write* $M_i = X^{\alpha_1} Y^{\alpha_2}$ *and* $T = \alpha_1$ *rem* $w(Y)$. *We have that*

$$w_H(\vec{c}) \geq (a - \alpha_1)(q - \alpha_2) + \epsilon \text{ where}$$

$$\epsilon = \begin{cases} 0 & \text{if } q - b \leq \alpha_2 < q \\ T(q - \alpha_2 - b) & \text{if } 0 \leq \alpha_1 \leq a - w(Y) \\ & \text{and } 0 \leq \alpha_2 < q - b \\ \alpha_1(q - \alpha_2 - b) & \text{if } a - w(Y) < \alpha_1 < a \text{ and} \\ & q - w(X) - \alpha_1 \frac{b - w(X)}{a - w(Y)} < \alpha_2 < q - b \\ T(q - \alpha_2 - w(X)) & \text{if } a - w(Y) < \alpha_1 < a \text{ and} \\ & 0 \leq \alpha_2 \leq q - w(X) - \alpha_1 \frac{b - w(X)}{a - w(Y)}. \end{cases}$$

The proof of Theorem 27 is done by applying Theorem 15 carefully. It consists in demonstrating how $\mathcal{L}(1), \ldots, \mathcal{L}(v + 1)$ can be build from the sets $B_1(X^{\alpha_1} Y^{\alpha_2})$, $B_2(X^{\alpha_1} Y^{\alpha_2})$ and $B_3(X^{\alpha_1} Y^{\alpha_2}, u)$ which we define below. Immediately after the definition we illustrate with an example the main idea of the proof of Theorem 27 including the role of the below sets.

Definition 28. *Let the notation be as in Definition 21 and Theorem 27. For arbitrary integers* α_1, α_2, $0 \leq \alpha_1 < a$, $0 \leq \alpha_2 < q$ *we define*

$$B_1(X^{\alpha_1} Y^{\alpha_2}) = \{X^{\gamma_1} Y^{\gamma_2} \mid \alpha_1 \leq \gamma_1 < a, \alpha_2 \leq \gamma_2 < q\},$$

$$B_2(X^{\alpha_1} Y^{\alpha_2}) =$$

$$\begin{cases} \left\{X^{\gamma_1} Y^{\gamma_2} \mid \alpha_1 - T \leq \gamma_1 < \alpha_1, \right. \\ \qquad\qquad \left. \alpha_2 + b \leq \gamma_2 < q \right\} & \text{if } T \neq 0 \text{ and} \\ & 0 \leq \alpha_2 < q - b \\ \emptyset & \text{otherwise,} \end{cases}$$

and for $u = 1, \ldots, \gcd(a, b)$

$$B_3(X^{\alpha_1} Y^{\alpha_2}, u) =$$

$$\begin{cases} \left\{X^{\gamma_1} Y^{\gamma_2} \mid a - w(Y)u \leq \gamma_1 < \alpha_1, \right. \\ \qquad \left. \alpha_2 + w(X)u \leq \gamma_2 < q \right\} & \text{if } a - w(Y) < \alpha_1 < a \\ & \text{and } 0 \leq \alpha_2 < q - b \\ \emptyset & \text{otherwise.} \end{cases}$$

Observe that the set $B_3(X^{\alpha_1} Y^{\alpha_2}, u)$, $u = 1, \ldots, \gcd(a, b)$ is never empty when $a - w(Y) < \alpha_1 < a$ and $0 \leq \alpha_2 < q - b$ hold. Similarly, $B_2(X^{\alpha_1} Y^{\alpha_2})$ is never empty when $T \neq 0$ and $0 \leq \alpha_2 < q - b$ hold.

Example 4. *Consider an optimal generalised C_{ab} polynomial $F(X,Y) = X^9 - Y^{12} + R(X,Y) \in \mathbb{F}_{27}[X,Y]$. We have $a = 9$, $b = 12$, $w(X) = 4$, $w(Y) = 3$, and $\Delta_{\prec_w}(I_{27}) = \{X^{i_1}Y^{i_2} \mid 0 \leq i_1 < 9, 0 \leq i_2 < 27\}$. From the discussion at the beginning of the section we know that $\gcd(a,b) = 3$ equals the maximal number of times a given weight can appear in $w(\Delta_{\prec_w}(I_{27}))$. In Figure 4.1 and Figure 4.2 this is illustrated by the division of $w(\Delta_{\prec_w}(I_{27}))$ into 3 disjoint sets of columns, within each set no weight appears twice.*

Y26	78	82	86	90	94	98	102	106	110
Y25	75	79	83	87	91	95	99	103	107
Y24	72	76	80	84	88	92	96	100	104
Y23	69	73	77	81	85	89	93	97	101
Y22	66	70	74	78	82	86	90	94	98
Y21	63	67	71	75	79	83	87	91	95
Y20	60	64	68	72	76	80	84	88	92
Y19	57	61	65	69	73	77	81	85	89
Y18	54	58	62	66	70	74	78	82	86
Y17	51	55	59	63	67	71	75	79	83
Y16	48	52	56	60	64	68	72	76	80
Y15	45	49	53	57	61	65	69	73	77
Y14	42	46	50	54	58	62	66	70	74
Y13	39	43	47	51	55	59	63	67	71
Y12	36	40	44	48	52	56	60	64	68
Y11	33	37	41	45	49	53	57	61	65
Y10	30	34	38	42	46	50	54	58	62
Y9	27	31	35	39	43	47	51	55	59
Y8	24	28	32	36	40	44	48	52	56
Y7	21	25	29	33	37	41	45	49	53
Y6	18	22	26	30	34	38	42	46	50
Y5	15	19	23	27	31	35	39	43	47
Y4	12	16	20	24	28	32	36	40	44
Y3	9	13	17	21	25	29	33	37	41
Y2	6	10	14	18	22	26	30	34	38
Y	3	7	11	15	19	23	27	31	35
1	0	4	8	12	16	20	24	28	32
	1	X	X2	X3	X4	X5	X6	X7	X8

Y26	78	82	86	90	94	98	102	106	110
Y25	75	79	83	87	91	95	99	103	107
Y24	72	76	80	84	88	92	96	100	104
Y23	69	73	77	81	85	89	93	97	101
Y22	66	70	74	78	82	86	90	94	98
Y21	63	67	71	75	79	83	87	91	95
Y20	60	64	68	72	76	80	84	88	92
Y19	57	61	65	69	73	77	81	85	89
Y18	54	58	62	66	70	74	78	82	86
Y17	51	55	59	63	67	71	75	79	83
Y16	48	52	56	60	64	68	72	76	80
Y15	45	49	53	57	61	65	69	73	77
Y14	42	46	50	54	58	62	66	70	74
Y13	39	43	47	51	55	59	63	67	71
Y12	36	40	44	48	52	56	60	64	68
Y11	33	37	41	45	49	53	57	61	65
Y10	30	34	38	42	46	50	54	58	62
Y9	27	31	35	39	43	47	51	55	59
Y8	24	28	32	36	40	44	48	52	56
Y7	21	25	29	33	37	41	45	49	53
Y6	18	22	26	30	34	38	42	46	50
Y5	15	19	23	27	31	35	39	43	47
Y4	12	16	20	24	28	32	36	40	44
Y3	9	13	17	21	25	29	33	37	41
Y2	6	10	14	18	22	26	30	34	38
Y	3	7	11	15	19	23	27	31	35
1	0	4	8	12	16	20	24	28	32
	1	X	X2	X3	X4	X5	X6	X7	X8

Figure 4.1: In both parts $X^{\alpha_1}Y^{\alpha_2} = X^8Y^3$. Left part: Light grey area is B_1, medium grey area is B_2, and dark grey area plus medium grey area correspond to $B_3(X^{\alpha_1}Y^{\alpha_2}, 1)$. Right part: Light grey area is B_1, medium grey area is B_2, and dark grey area plus medium grey area correspond to $B_3(X^{\alpha_1}Y^{\alpha_2}, 3)$.

Assume first that $\vec{c} = ev(A + I_{27})$ where $lm(A) = X^8Y^3$. We can write $A = a_1 1 + \cdots + a_{79}X^2Y^{11} + a_{80}X^5Y^7 + a_{81}X^8Y^3$, $a_{81} \neq 0$. Note that $w(X^2Y^{11}) = w(X^5Y^7) = w(X^8Y^3)$ and that any monomial in the support of A different from these three monomials must be of lower weight. We first make some observations that hold regardless of a_{79} and a_{80}, respectively, being zero or not. Let $j = 0, \ldots, 23$. Then

$$lm(AY^j \ rem \ \mathcal{G}) = lm(X^8Y^3Y^j \ rem \ \mathcal{G}) = X^8Y^{3+j}.$$

Hence, (X^8Y^3, Y^j) is OWB (or equivalently SOWB with respect to $\{1, \ldots, 81\}$) and

$$B_1(X^8Y^3) = \{X^8Y^{3+j} \mid j = 0, \ldots, 23\}$$

is a subset of $\mathcal{L}(u)$, $u = 1, 2, 3$.
Similarly, let $i = 0, 1, 2$ and $j = 0, \ldots, 11$. Then

$$lm(AX^{7+i}Y^j \ rem \ \mathcal{G}) = lm(X^8Y^3X^{7+i}Y^j \ rem \ \mathcal{G}) = X^{6+i}Y^{15+j}.$$

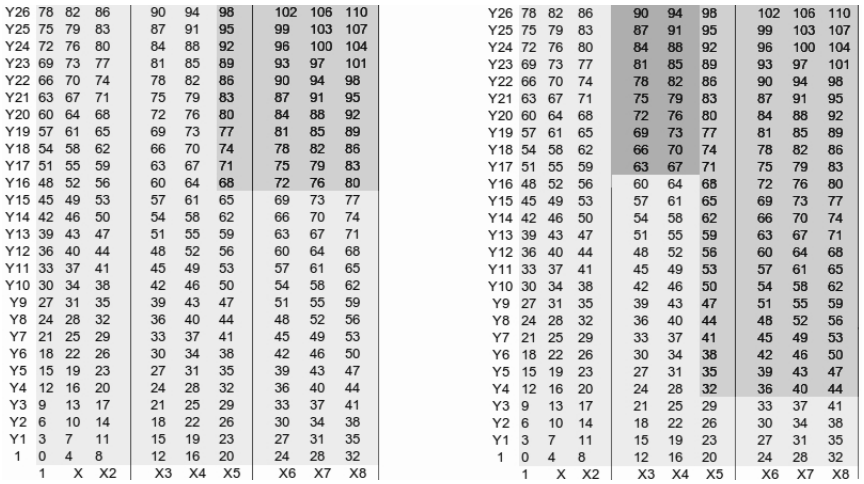

Figure 4.2: Left part: $X^{\alpha_1}Y^{\alpha_2} = X^5Y^{16}$. Only B_1 present. Right part: $X^{\alpha_1}Y^{\alpha_2} = X^5Y^4$. Light grey area is B_1, medium grey area is B_2. B_3 is not present.

Hence, $(X^8Y^3, X^{7+i}Y^j)$ *is OWB (or equivalently SOWB with respect to* $\{1, \ldots, 81\}$*) and*

$$B_2'(X^8, Y^3) = \{X^{6+i}Y^{15+j} \mid i = 0, 1, 2,\ j = 0, \ldots, 11\}$$

is a subset of $\mathcal{L}(u)$*,* $u = 1, 2, 3$*. But then also* $B_2(X^8Y^3) = B_2'(X^8Y^3) \backslash B_1(X^8Y^3)$ *is a subset of* $\mathcal{L}(u)$*. Note that the idea behind* $B_2'(X^8Y^3)$ *is to multiply* A *with monomials* M *such that* $X^2Y^{11}M$*,* X^5Y^7M*, and* X^8Y^3M *belong to* $X^9 \cdot \Delta_{\prec_w}(I_{27})$*. This ensures that* $lm(A \cdot M \ rem\ X^9 - Y^{12} + R(X, Y)) = lm(X^8Y^3 \cdot M \ rem\ X^9 - Y^{12} + R(X, Y))$*.*
We next consider separately the three different cases where we take into account if a_{79} *and* a_{80}*, respectively, are zero or not.*
Case 1: Assume $a_{80} \neq 0$*. Let* $i = 1, 2, 3$ *and* $j = 0, \ldots, 19$*. then*

$$lm(A \cdot X^iY^j \ rem\ \mathcal{G}) = lm(X^5Y^7 \cdot X^iY^j \ rem\ \mathcal{G}) = X^{5+i}Y^{7+j}.$$

This corresponds to saying that (X^5Y^7, X^iY^j) *is SOWB with respect to* $\{1, \ldots, 81\}$ *and*

$$B_3'(X^8Y^3, 1) = \{X^{5+i}Y^{7+j} \mid i = 1, 2, 3,\ j = 0, \ldots, 19\}$$

therefore is a subset of $\mathcal{L}(1)$*. But then also* $B_3(X^8Y^3, 1) = B_3'(X^8Y^3, 1) \backslash B_1(X^8Y^3, 1)$ *is a subset of* $\mathcal{L}(1)$*. The left part of Figure 4.1 shows the sets derived so far. Note that* $B_2(X^8Y^3) \subseteq B_3(X^8Y^3, 1)$ *and the information we have therefore boils down to* $B_3(X^8Y^3, 1) \cup B_1(X^8Y^3) \subseteq \mathcal{L}(1)$ *(actually, one can show that equality holds). We conclude*

$$w_H(\vec{c}) \geq \#B_3(X^8Y^3, 1) + \#B_1(X^8Y^3) = 40 + 24 = 64.$$

Case 2: Assume $a_{79} \neq 0$*,* $a_{80} = 0$*. In this case we use the fact that* $lm(A \cdot X \ rem\ \mathcal{G}) = X^3Y^{11}$*. We leave it for the reader to show that this results in a*

set $B_3(X^8Y^3, 2)$ *of size* 80 *which has as a subset* $B_2(X^8Y^3)$. *Hence,* $w_H(\vec{c}) \geq 80 + 24 = 104$.
Case 3: Assume $a_{79} = a_{80} = 0$. *Let* $i = 1, \ldots, 9$ *and* $j = 0, \ldots, 11$. *Then*

$$lm(A \cdot X^iY^j \text{ rem } \mathcal{G}) = lm(X^8Y^3 \cdot X^iY^j \text{ rem } \mathcal{G}) = X^{i-1}Y^{15+j}.$$

This corresponds to saying that (X^8Y^3, X^iY^j) *is SOWB with respect to* $\{1, \ldots, 78, 81\}$ *and*

$$B_3'(X^8Y^3, 3) = \{X^{i-1}Y^{15+j} \mid i = 1, \ldots, 9,\ j = 0, \ldots, 11\}$$

therefore is a subset of $\mathcal{L}(3)$. *But then also* $B_3(X^8Y^3, 3) = B_3'(X^8Y^3, 3) \backslash B_1(X^8Y^3)$ *is a subset of* $\mathcal{L}(3)$. *The right part of Figure 4.1 illustrates the sets derived above. Note that* $B_2(X^8Y^3) \subseteq B_3(X^8Y^3, 3)$ *and the information gathered boils down to* $B_3(X^8Y^3, 3) \cup B_1(X^8Y^3) \subseteq \mathcal{L}(3)$ *(actually one can show equality). We conclude that* $w_H(\vec{c}) \geq 96 + 24 = 120$.
Taking finally the worst of the three cases we conclude that $w_H(\vec{c}) \geq \min\{64, 104, 120\} = 64$. *Note that with the Feng-Rao bound with OWB we only get* $w_H(\vec{c}) \geq \#B_2(X^8Y^3) + \#B_1(X^8Y^3) = 24 + 24 = 48$.

We next consider a word $\vec{c} = ev(A + I_{27})$ *with*

$$A = a_1 1 + \cdots + a_{167}X^2Y^{20} + a_{168}X^5Y^{16}.$$

Note that $w(X^2Y^{20}) = w(X^5Y^{16})$ *and that all monomials in the support of* A *different from these two monomials must be of lower weights. A set* $B_1(X^5Y^{16})$ *is established similarly as above (see the left part of Figure 4.2). Trying to establish a set* $B_2'(X^5Y^{16})$ *we multiply* A *by* $X^{7+i}Y^j$ *where* i *and* j *are to be determined such that* $X^2Y^{20} \cdot X^{7+i}Y^j$ *as well as* $X^5Y^{16} \cdot X^{7+i}Y^j$ *belong to* $X^9 \cdot \Delta_{\prec_w}(I_{27})$. *However,* $lm(X^{9+i}Y^{20+j} \text{ rem } X^9 - Y^{12} + R(X, Y)) = X^iY^{32+j}$ *which is not in* $\Delta_{\prec_w}(I_{27})$. *Hence, reducing* $X^{9+i}Y^{20+j}$ *modulo* $\mathcal{G}$ *involves reducing modulo* $Y^{27} - Y$ *which does not possess in its support two monomials of highest weight. Similar remarks hold for the second mentioned monomial and in conclusion we therefore have no information about what is the leading monomial of* $A \cdot X^{7+i}Y^j$ *rem* $\mathcal{G}$. *Note that the reason why we cannot define a set* $B_2'(X^5Y^{16})$ *is that the power of* Y *in* X^5Y^{16} *is too high. In a similar way, to establish a set* $B_3'(X^5Y^{16}, u)$ *we need the power of* X *in* X^5Y^{16} *to be in* $\{a - (\gcd(a, b) - 1), \ldots, a - 1\} = \{7, 8\}$ *(we leave it for the reader to verify this). Hence, the only information we have is* $B_1(X^5Y^{16}) \subseteq \mathcal{L}(u)$, $u = 1, 2$, *(actually one can show that equality holds), and consequently* $w_H(\vec{c}) \geq \#B_1(X^5Y^{16}) = 44$.

We finally assume $\vec{c} = ev(A + I_{27})$ *where* $A = a_1 1 + \cdots + a_{52}X^2Y^8 + a_{53}X^5Y^4$, $a_{53} \neq 0$. *The set* $B_1(X^5Y^4)$ *is illustrated in the right part of Figure 4.2. As the power of* Y *in* X^5Y^4 *is small enough we also have a set* $B_2'(X^5Y^4)$ *inside* $\Delta_{\prec_w}(I_{27})$. *The corresponding set* $B_2(X^5Y^4)$ *is illustrated in the same figure. The power of* X *in* X^5Y^4 *does not belong to* $\{7, 8\}$. *Hence, we have no set* $B_3'(X^5Y^4, u)$. *We conclude* $B_2(X^5Y^4) \cup B_1(X^5Y^4) \subseteq \mathcal{L}(u)$, $u = 1, 2$, *(actually one can show equality). From the right part of Figure 4.2 we conclude* $w_H(\vec{c}) \geq \#B_2(X^5Y^4) + \#B_1(X^5Y^4) = 20 + 92 = 112$.

Lemma 29. *For any choice of $u \in \{1, \ldots, \gcd(a,b)\}$ and $M \in \Delta_{\prec}(I_q)$ it holds that $B_1(M) \cap B_2(M) = B_1(M) \cap B_3(M,u) = \emptyset$. If $B_3(M,u) \neq \emptyset$ then $B_2(M) \subseteq B_3(M,u)$.*

Proof. By inspection of Definition 28. □

Lemma 30. *Consider $\vec{c} = ev(\sum_{s=1}^{i} a_s M_s + I_q)$, $a_s \in \mathbb{F}_q$, $s = 1, \ldots, i$, and $a_i \neq 0$. Let $M_i = X^{\alpha_1} Y^{\alpha_2}$ and $v = \alpha_1$ div $w(Y)$ (that is, v satisfies $\alpha_1 = w(Y)v + T$, where $T = \alpha_1$ rem $w(Y)$). It holds that:*

1. *$B_1(X^{\alpha_1} Y^{\alpha_2}) \subseteq \mathcal{L}(u)$ for $u = 1, \ldots, v+1$.*
2. *$B_2(X^{\alpha_1} Y^{\alpha_2}) \subseteq \mathcal{L}(u)$ for $u = 1, \ldots, v+1$.*
3. *$B_3(X^{\alpha_1} Y^{\alpha_2}, \gcd(a,b)) \subseteq \mathcal{L}(v+1)$.*
4. *$B_3(X^{\alpha_1} Y^{\alpha_2}, u) \subseteq \mathcal{L}(u)$ for $u = 1, \ldots, v$.*

Proof.
Part 1: Assume $M_l = X^{\gamma_1} Y^{\gamma_2} \in B_1(X^{\alpha_1} Y^{\alpha_2})$. We have $\alpha_1 \leq \gamma_1 < a$ and $\alpha_2 \leq \gamma_2 < q$. Choosing $M_j = X^{\gamma_1 - \alpha_1} Y^{\gamma_2 - \alpha_2}$ we get $\mathrm{lm}(M_i M_j \text{ rem } \mathcal{G}) = M_l$. Let $i' \in \{1, \ldots, i-1\}$, then by the properties of a monomial ordering $M_{i'} M_j \prec_w M_i M_j$ holds. This means that (M_i, M_j) is SOWB with respect the set $\{1, \ldots, i\}$. Thus $M_l \in \mathcal{L}(u)$ for $u = 1, \ldots, v+1$.

Part 2: If $T = 0$ or $q - b \leq \alpha_2 < q$ then the result follows trivially. Assume $T \neq 0$ and $0 \leq \alpha_2 < q - b$. Let $M_l = X^{\gamma_1} Y^{\gamma_2} \in B_2(X^{\alpha_1} Y^{\alpha_2})$. We have $\alpha_1 - T \leq \gamma_1 < \alpha_1$ and $\alpha_2 + b \leq \gamma_2 < q$. Choosing $M_j = X^{\gamma_1 - \alpha_1 + a} Y^{\gamma_2 - \alpha_2 - b}$ (which belongs to $\Delta_{\prec_w}(I_q)$ by the definition of B_2) we get

$$\mathrm{lm}(M_i M_j \text{ rem } \mathcal{G}) = \mathrm{lm}(M_i M_j - X^{\gamma_1} Y^{\gamma_2 - b} F(X,Y)) = X^{\gamma_1} Y^{\gamma_2}.$$

We want to prove that (M_i, M_j) is SOWB with respect the set $\{1, \ldots, i\}$. We consider $M_{i'}$ with $i' \in \{1, \ldots, i-1\}$. If $w(M_{i'}) < w(M_i)$ then the proof follows from $w(M_{i'} M_j) < w(M_i M_j)$ using the fact that reducing modulo F does not change the weight of the leading monomial. If $w(M_{i'}) = w(M_i)$ then there exists an integer z with $\alpha_1 - z w(Y) \geq 0$ such that $M_{i'} = X^{\alpha_1 - z w(Y)} Y^{\alpha_2 + z w(Y)}$. Therefore $\gamma_1 - z w(Y) \geq 0$.
Now $M_{i'} M_j = X^{a + \gamma_1 - z w(Y)} Y^{\gamma_2 - b + z w(X)}$ and therefore

$$\begin{aligned} \mathrm{lm}(M_{i'} M_j \text{ rem } \mathcal{G}) &= \mathrm{lm}(M_{i'} M_j - X^{\gamma_1 - z w(Y)} Y^{\gamma_2 - b + z w(X)} F(X,Y)) \\ &= X^{\gamma_1 - z w(Y)} Y^{\gamma_2 + z w(X)} \prec_w X^{\gamma_1} Y^{\gamma_2}. \end{aligned}$$

Again we employed the fact that reducing modulo F does not change the weight of the leading monomial. We conclude that $\mathrm{lm}(M_{i'} M_j \text{ rem } \mathcal{G}) \prec_w X^{\gamma_1} Y^{\gamma_2}$ and that (M_i, M_j) is SOWB with respect the set $\{1, \ldots, i\}$. Thus $M_l \in \mathcal{L}(u)$ for $u = 1, \ldots, v+1$.

Part 3: If $0 \leq \alpha_1 \leq a - w(Y)$ or $q - b \leq \alpha_2 < q$ then the result follows trivially. Assume $a - w(Y) < \alpha_1 < a$ and $0 \leq \alpha_2 < q - b$, then $v = \gcd(a,b) - 1$. Let $M_l =$

$X^{\gamma_1}Y^{\gamma_2} \in B_3(X^{\alpha_1}Y^{\alpha_2}, \gcd(a,b))$. As $w(X)\gcd(a,b) = b$ and $w(Y)\gcd(a,b) = a$ we have $0 \leq \gamma_1 < \alpha_1$ and $\alpha_2 + b \leq \gamma_2 < q$. Choosing $M_j = X^{\gamma_1-\alpha_1+a}Y^{\gamma_2-\alpha_2-b}$ we get $\mathrm{lm}(M_iM_j \text{ rem } \mathcal{G}) = M_l$. We want to prove that (M_i, M_j) is SOWB with respect the set $\{1, \ldots, i-v-1\}$. We consider $M_{i'}$ with $i' \in \{1, \ldots, i-1\}$. If $w(M_{i'}) < w(M_i)$ the proof follows because $w(M_{i'}M_j) < w(M_iM_j)$ using the fact that reducing modulo F does not change the weight of the leading monomial. As $v = \gcd(a,b) - 1$ there does not exists any $i' \in \{1, \ldots, i-v-1, i\}$ such that $w(M_{i'}) = w(M_i)$. From this it follows that (M_i, M_j) is SOWB with respect the set $\{1, \ldots, i-v-1\}$ and thus $M_l \in \mathcal{L}(v+1)$.

Part 4: If $q - b \leq \alpha_2 < q$ or $0 \leq \alpha_1 \leq a - w(Y)$ then the result follows trivially. Assume $a - w(Y) < \alpha_1 < a$ and $0 \leq \alpha_2 < q - b$, then $v = \gcd(a,b) - 1$. Let $M_l = X^{\gamma_1}Y^{\gamma_2} \in B_3(X^{\alpha_1}Y^{\alpha_2}, u)$. We have $a - w(Y)u \leq \gamma_1 < \alpha_1$ and $\alpha_2 + w(X)u \leq \gamma_2 < q$. By the definition of $\prec_w$ and the form of $\Delta_{\prec_w}(I_q)$ we have that $M_{i-u} = X^{\alpha_1-w(Y)u}Y^{\alpha_2+w(X)u}$. Choosing $M_j = X^{\gamma_1-\alpha_1+w(Y)u}Y^{\gamma_2-\alpha_2-w(Y)u}$ we get $\mathrm{lm}(M_{i-u}M_j \text{ rem } \mathcal{G}) = M_l$. Note that M_{i-u} and M_j are in $\Delta_{\prec_w}(I_q)$ because $v = \gcd(a,b) - 1$, $a - w(Y) < \alpha_1 < a$ and $0 \leq \alpha_2 < q - b$. We want to prove that (M_i, M_j) is SOWB with respect the set $\{1, \ldots, i-u, i\}$. We consider $M_{i'}$ with $i' \in \{1, \ldots, i-1\}$. If $w(M_{i'}) < w(M_i)$ then the proof follows from $w(M_{i'}M_j) < w(M_iM_j)$ using the fact that reducing modulo F does not change the weight of the leading monomial. The monomials $M_{i'}$ which satisfy $w(M_{i'}) = w(M_{i-u})$ are M_i and M_{i-z} for $z = u, \ldots, v$. However, M_iM_j rem $\mathcal{G} \prec_w M_{i-u}M_j$ rem $\mathcal{G}$ because $\gamma_1 + w(Y)u > a$ and $M_{i-t}M_j \prec_w M_{i-u}M_j$ for any $t = u+1, \ldots, v$ due to the properties of a monomial ordering. From this it follows that (M_i, M_j) is SOWB with respect the set $\{1, \ldots, i-u, i\}$ and thus $M_l \in \mathcal{L}(u)$, for $u = 1, \ldots, v$. □

Lemma 31. *Consider* $\vec{c} = ev(\sum_{s=1}^{i} a_sM_s + I_q)$, $a_s \in \mathbb{F}_q$, $s = 1, \ldots, i$, *and* $a_i \neq 0$. *Write* $M_i = X^{\alpha_1}Y^{\alpha_2}$. *For* $u = 1, \ldots, v+1$, *with* $v = \alpha_1$ *div* $w(Y)$, *we have*

$$B_1(X^{\alpha_1}Y^{\alpha_2}) \cup B_2(X^{\alpha_1}Y^{\alpha_2}) \subseteq \mathcal{L}(u), \tag{4.1}$$

$$B_1(X^{\alpha_1}Y^{\alpha_2}) \cup B_3(X^{\alpha_1}Y^{\alpha_2}, u) \subseteq \mathcal{L}(u). \tag{4.2}$$

Proof. The lemma follows directly from Lemma 29 and Lemma 30. □

It is not hard to compute the cardinality of the sets B_1, B_2 and B_3. For $u = 1, \ldots, \gcd(a,b)$, we have that:

$$\#B_1(X^{\alpha_1}Y^{\alpha_2}) = (a-\alpha_1)(q-\alpha_2),$$

$$\#B_2(X^{\alpha_1}Y^{\alpha_2}) = \begin{cases} \alpha_1(q-\alpha_2-b) & \text{if } 0 \leq \alpha_2 < q-b \\ 0 & \text{otherwise,} \end{cases}$$

$$\#B_3(X^{\alpha_1}Y^{\alpha_2}, u) = \begin{cases} (w(Y)u - a + \alpha_1)\cdot & \text{if } 0 \leq \alpha_2 < q-b \text{ and} \\ \quad (q - \alpha_2 - w(X)u) & a - w(Y) < \alpha_1 < a \\ 0 & \text{otherwise.} \end{cases}$$

We are ready to prove Theorem 27.

Proof of Theorem 27. Let $v = \alpha_1 \operatorname{div} w(Y)$. If $0 \leq \alpha_1 \leq a - w(Y)$ then by Lemma 31 we obtain

$$\begin{aligned} w_H(\vec{c}) &\geq \min\{\#\mathcal{L}(1), \ldots, \#\mathcal{L}(v+1)\} \\ &\geq \#B_2(X^{\alpha_1}Y^{\alpha_2}) + \#B_1(X^{\alpha_1}Y^{\alpha_2}) \\ &= (a-\alpha_1)(q-\alpha_2) + \\ &\quad \begin{cases} \alpha_1(q-\alpha_2-b) & \text{if } 0 \leq \alpha_2 < q-b \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

If $a - w(Y) < \alpha_1 < a$, then $v = \gcd(a,b) - 1$ and by Lemma 31 we obtain

$$\begin{aligned} w_H(\vec{c}) &\geq \min\{\#\mathcal{L}(1), \ldots, \#\mathcal{L}(v+1)\} \\ &\geq \min\{\#B_3(X^{\alpha_1}Y^{\alpha_2}, u) + \#B_1(X^{\alpha_1}Y^{\alpha_2}) \mid \\ &\qquad u = 1, \ldots, \gcd(a,b)\} \\ &= (a-\alpha_1)(q-\alpha_2) + \\ &\quad \begin{cases} \min\{(w(Y)u - a + \alpha_1)(q-\alpha_2 - & \text{if } 0 \leq \alpha_2 < q-b \\ \quad - w(X)u) \mid u = 1, \ldots, v+1\} & \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

The function $f(u) = (w(Y)u - a + \alpha_1)(q - \alpha_2 - w(X)u)$ is a concave parabola, thus we have minimum in $u = 1$ or $u = v+1 = \gcd(a,b)$. By inspection $f(1) = (w(Y) - a + \alpha_1)(q - \alpha_2 - w(X)) = T(q - \alpha_2 - w(X))$ and $f(\gcd(a,b)) = (w(Y)\gcd(a,b) - a + \alpha_1)(q - \alpha_2 - w(X)\gcd(a,b)) = \alpha_1(q - \alpha_2 - b)$. We therefore get the equivalence:

$$f(1) \leq f(\gcd(a,b)) \Leftrightarrow \alpha_2 \leq q - w(X) - \alpha_1 \frac{b - w(X)}{a - w(Y)},$$

and the theorem follows. □

Remark 32. *If for codes from optimal generalised C_{ab} polynomials rather than applying Theorem 15 we apply the Feng-Rao bound (Theorem 9) with OWB then the ϵ in Theorem 27 should be replaced with:*

$$\begin{cases} 0 & \text{if } q - b \leq \alpha_2 < q \\ T(q - \alpha_2 - b) & \text{and } 0 \leq \alpha_2 < q - b. \end{cases}$$

This is because our improvement comes from the sets $B_3(X^{\alpha_1}Y^{\alpha_2})$ as can be seen from the proof of Lemma 30. We see that our new bound improves the Feng-Rao bound by

$$\begin{cases} 0 & \text{if } q - b \leq \alpha_2 < q \\ & \text{or } 0 \leq \alpha_1 \leq a - w(Y) \\ (\alpha_1 - T)(q - \alpha_2 - b) & \text{if } a - w(Y) < \alpha_1 < a \text{ and} \\ & q - w(X) - \alpha_1 \frac{b-w(X)}{a-w(Y)} < \alpha_2 < q - b \\ T(b - w(X)) & \text{if } a - w(Y) < \alpha_1 < a \text{ and} \\ & 0 \leq \alpha_2 \leq q - w(X) - \alpha_1 \frac{b-w(X)}{a-w(Y)}. \end{cases}$$

Remark 33. *One can prove that equality holds in (4.1) whenever* $B_3(X^{\alpha_1}Y^{\alpha_2}, 1) = \emptyset$. *When this set is not empty equality holds in (4.2). Theorem 27 therefore is the strongest possible result one can derive from Theorem 15 regarding the minimum distance of codes from optimal generalised* C_{ab} *polynomials.*

In the following we apply Theorem 27 in a number of cases where $F(X,Y) = G(X) - H(Y) \in \mathbb{F}_{p^m}[X,Y]$ with $G(X)$ being the trace polynomial and $H(Y)$ being an $(\mathbb{F}_{p^m}, \mathbb{F}_p)$-polynomial of another degree. Recall from the discussion at the beginning of the section that these are optimal generalised C_{ab} polynomials. The strength of our new bound Theorem 15 and Theorem 27 lies in the cases where a and b are not relatively prime, as for a and b relatively prime it reduces to the usual Feng-Rao bound for primary codes (see the last part of Remark 16). The well-known norm-trace polynomial corresponds to choosing $H(Y)$ to be the norm polynomial. This gives $a = p^{m-1}$ and $b = (p^m - 1)/(p - 1)$ which are clearly relatively prime. The related codes, which are called norm-trace codes, are one-point algebraic geometric codes. It seems fair to compare the outcome of Theorem 27, when $\gcd(a,b) > 1$ keeping a fixed but varying b, with the parameters of the norm-trace codes over the same alphabet. The two corresponding sets of ideals have the same footprint $\Delta_{\prec_w}(I_q)$ and consequently the corresponding codes are of the same length. We remind the reader that it was shown in [6] that the Feng-Rao bound gives the true parameters of the norm-trace codes.

Example 5. *In this example we consider optimal generalised* C_{ab} *polynomials derived from* $(\mathbb{F}_8, \mathbb{F}_2)$*-polynomials. The trace polynomial* $G(X)$ *is of degree* $a = 4$ *and from Example 3 we see that besides the norm polynomial which is of degree* $b = 7$ *we can choose* $H(Y)$ *as* $F_3(Y) = Y^6 + Y^5 + Y^3$ *which is of degree* $b = 6$. *The corresponding codes are of length* $n = 32$ *over the alphabet* $\mathbb{F}_8$. *In Figure 4.3 we compare the parameters of the related two sequences of improved codes* $\widetilde{E}_{imp}(\delta)$ *(Definition 17). For few choices of* δ *the norm-trace code is the best, but for many choices of* δ, *from* $(a,b) = (4,6)$ *we get better codes. We note that the latter sequence of codes contains two non-trivial codes that have the best known parameters according to the linear code bound at [13], namely* $[n,k,d]$ *equal to* $[32,2,28]$ *and* $[32,15,12]$.
Concentrating solely on the case $(a,b) = (4,6)$ *we finally investigate in a couple of cases how well our new bound, Proposition 18, performs in comparison with the usual Feng-Rao bound for primary codes. By Proposition 18 the minimum distance of* $\widetilde{E}_{imp}(13)$ *is at least* 13 *but the Feng-Rao bound with OWB and WB, respectively, only produces the numbers* 10 *and* 8, *respectively. For* $\widetilde{E}_{imp}(12)$ *the lower bounds on* d *are* 12, 10, *and* 8, *respectively. For* $\widetilde{E}_{imp}(10)$ *they are* 10, 8, *and* 7, *respectively, and finally for* $\widetilde{E}_{imp}(9)$, 9, 8, *and* 7, *respectively.*

Example 6. *In this example we consider optimal generalised* C_{ab} *polynomials derived from* $(\mathbb{F}_{16}, \mathbb{F}_2)$*-polynomials. The trace polynomial* $G(X)$ *is of degree* $a = 8$ *and from Example 3 we see that besides the norm polynomial which is of degree* $b = 15$ *we can choose* $H(Y)$ *to be of degree* 10, 12 *and* 14. *The corresponding codes are of length* $n = 128$ *over the alphabet* $\mathbb{F}_{16}$. *In Figure 4.4 we compare the parameters of the related two sequences of improved codes* $\widetilde{E}_{imp}(\delta)$ *when* $b = 10$ *and when* $b = 15$

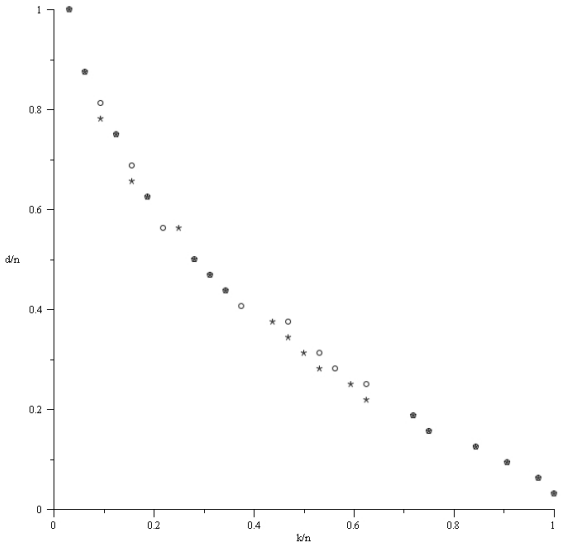

Figure 4.3: Improved codes from Example 5. A $\circ$ corresponds to $(a, b) = (4, 6)$, and an $*$ corresponds to $(a, b) = (4, 7)$ (the norm-trace codes).

(the norm-trace codes). For most choices of δ from $(a, b) = (8, 10)$ we get the best codes. The norm-trace codes are never strictly best.
Concentrating on the codes $\widetilde{E}_{imp}(\delta)$ related to $(a, b) = (8, 10)$ we compare in Figure 4.5 our new bound Proposition 18 with the Feng-Rao bound – the latter equipped with OWB and WB, respectively. For many rates Proposition 18 is superior.

Example 7. *In this example we consider optimal generalised C_{ab} polynomials derived from $(\mathbb{F}_{32}, \mathbb{F}_2)$-polynomials. The trace polynomial $G(X)$ is of degree $a = 16$ and from Example 3 we see that besides the norm-polynomial which is of degree $b = 31$ we can choose $H(Y)$ to be of degree 20, 24, 26, 28 and 30. The corresponding codes are of length $n = 512$ over the alphabet $\mathbb{F}_{32}$. In Figure 4.6 we compare the parameters of the related three sequences of improved codes $\widetilde{E}_{imp}(\delta)$ when $b = 20$, $b = 26$ and when $b = 31$ (the norm-trace codes). For no choices of δ the norm-trace codes are strictly best (this holds for all values of k/n). For some choices $b = 20$ gives the best codes for other choices the best parameters are found by choosing $b = 26$.*

Example 8. *In this example we consider optimal generalised C_{ab} polynomials derived from $(\mathbb{F}_{64}, \mathbb{F}_2)$-polynomials. The trace polynomial $G(X)$ is of degree $a = 32$ and by studying cyclotomic cosets we see that as an alternative to the norm polynomial which is of degree $b = 63$ we can for instance choose an $H(Y)$ of degree 42. The corresponding codes are of length $n = 2048$ over the alphabet $\mathbb{F}_{64}$. In Figure 4.7 we compare the parameters of the related two sequences of improved codes $\widetilde{E}_{imp}(\delta)$ when $b = 42$ and when $b = 63$ (the norm-trace codes). As is seen the first codes outperform the last codes for all parameters.*

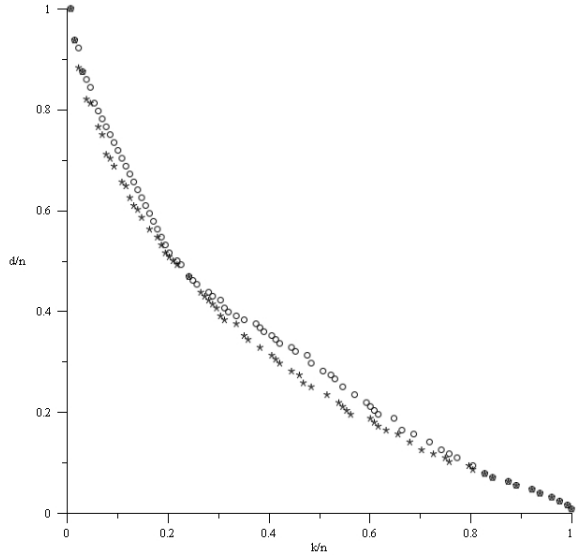

Figure 4.4: Improved codes from Example 6. A $\circ$ corresponds to $(a, b) = (8, 10)$, and an $*$ corresponds to $(a, b) = (8, 15)$ (the norm-trace codes).

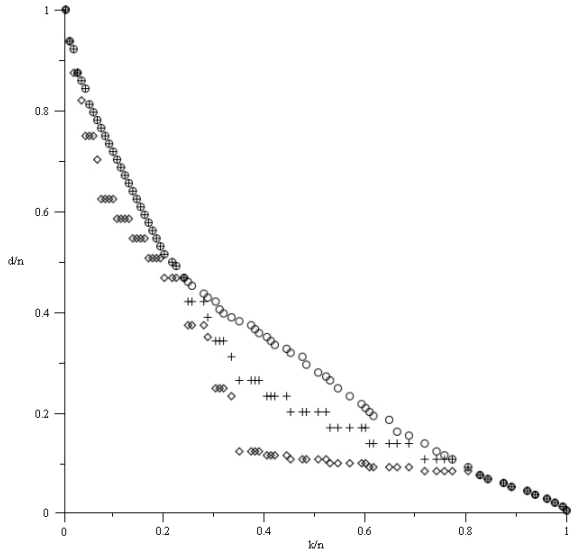

Figure 4.5: Estimated parameters of the codes $\widetilde{E}_{imp}(\delta)$ from Example 6 with $(a, b) = (8, 10)$. A $\circ$ corresponds to Proposition 18. The estimates coming from the Feng-Rao bound when equipped with OWB and WB, respectively, are marked with $+$ and $\diamond$, respectively.

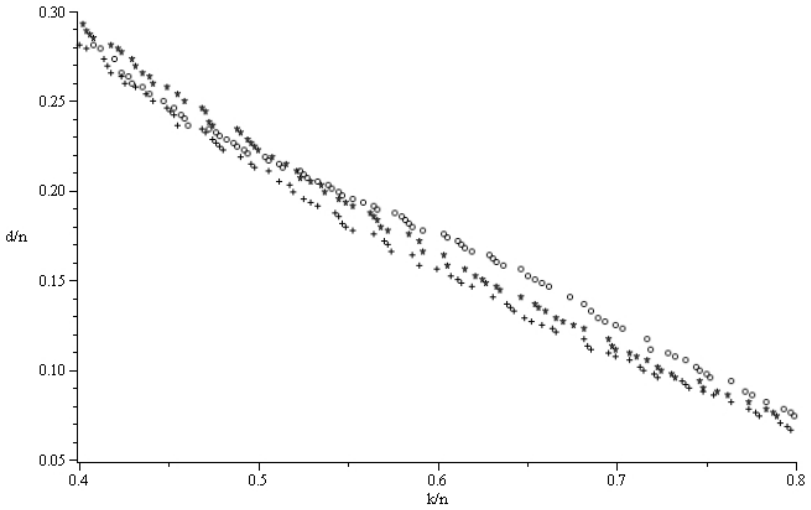

Figure 4.6: Improved codes from Example 7. A $\circ$ corresponds to $(a, b) = (16, 20)$, an $*$ to $(a, b) = (16, 26)$, and finally a $+$ corresponds to $(a, b) = (16, 31)$ (the norm-trace codes).

Concentrating finally on the codes $\widetilde{E}_{imp}(\delta)$ related to $(a, b) = (32, 42)$ we compare in Figure 4.8 our new bound Proposition 18 with the Feng-Rao bound – the latter equipped with OWB and WB, respectively. As demonstrated Proposition 18 is superior.

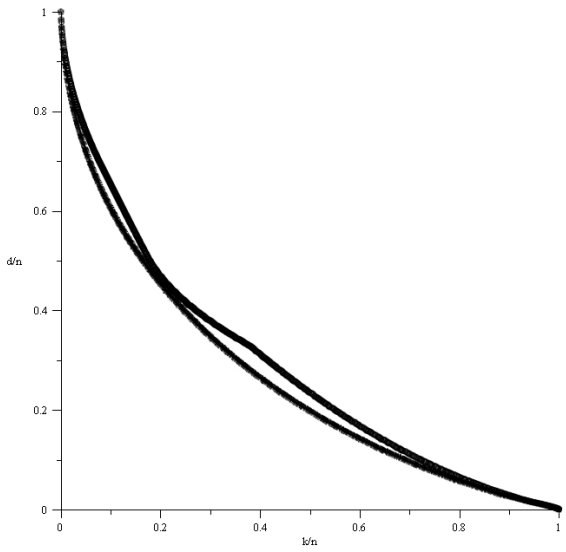

Figure 4.7: Improved codes from Example 8. The upper curve corresponds to $(a, b) = (32, 42)$, the lower curve to $(a, b) = (32, 63)$ (the norm-trace codes)

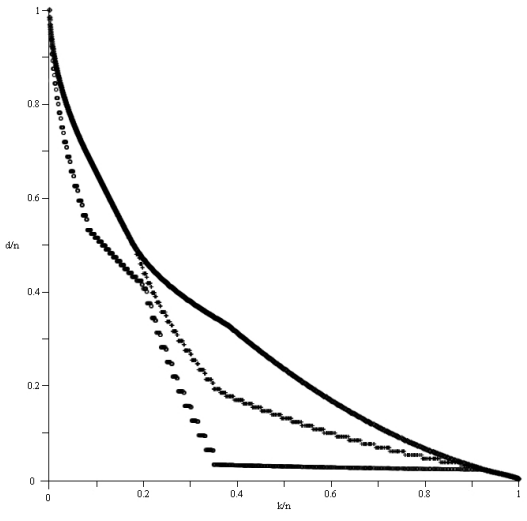

Figure 4.8: Estimated parameters of the codes $\widetilde{E}_{imp}(\delta)$ from Example 8 with $(a, b) = (32, 42)$. Upper point plot corresponds to Proposition 18. The estimates coming from the Feng-Rao bound when equipped with OWB and WB are the lower point plots.

Chapter 5

A new construction of improved codes

In Definition 17 we presented a Feng-Rao style improved code construction $\widetilde{E}_{imp}(\delta)$. As shall be demonstrated in this section it is sometimes possible to do even better. Recall that the idea behind Theorem 15 is to consider case 1 up till case $v+1$ as described prior to the theorem. Consider a general codeword

$$\vec{c} = \mathrm{ev}\big(\sum_{s=1}^{i} a_s M_s + I_q\big) \in C(I, L)$$

$a_i \neq 0$, where L is some fixed known subspace of $\mathbb{F}_q^n$. From L we might *a priori* be able to conclude that certain a_ss equal zero for all codewords as above. Hence, some of the cases, case 1 up to case v, do not occur. Clearly we could then leave out the corresponding sets in Theorem 15. This might result in a higher estimate on $w_H(\vec{c})$. We illustrate the phenomenon with an example in which we also show how to derive improved codes based on this observation.

Example 9. *In this example we consider the Klein quartic $X^3Y + Y^3 + X \in \mathbb{F}_8[X,Y]$. Let $w(X) = 2$ and $w(Y) = 3$. The ideal $I = \langle X^3Y + Y^3 + X\rangle \subseteq \mathbb{F}_8[X,Y]$ and the corresponding weighted degree lexicographic ordering $\prec_w$ satisfy order domain condition (C1) but not (C2) (as usual, in the definition of $\prec_w$ we choose $X = X_1$ and $Y = X_2$). Hence, it makes sense to apply Theorem 15. The footprint of $I_8 = \langle X^3Y + Y^3 + X, X^8 + X, Y^8 + Y\rangle$ is (for a reference see [7, Ex. 4.19] and [4, Ex. 3.3]):*

$$\begin{aligned}\Delta_{\prec_w}(I_8) \;=\; &\{1, X, Y, X^2, XY, Y^2, X^3, X^2Y, XY^2, X^4, Y^3, X^2Y^2,\\ &X^5, XY^3, Y^4, X^6, X^2Y^3, XY^4, X^7, Y^5, X^2Y^4, Y^6\}\end{aligned}$$

written in increasing order with respect to $\prec_w$. Consider

$$\vec{c} = ev\big(a_1 1 + a_2 X + a_3 Y + a_4 X^2 + a_5 XY + a_6 Y^2 + a_7 X^3 + I_8\big),$$

$a_7 \neq 0$. *We have* $w(X^3) = w(Y^2) > w(XY)$. *Hence, by Remark 16 we choose* $v = 1$.
By inspection the set corresponding to case 1 is

$$\mathcal{L}(1) = \{X^3, X^4, X^5, X^6, X^7, X^2Y^4\}.$$

(Note that X^2Y^4 *belongs to* $\mathcal{L}(1)$ *of the following reason: We have* $lm(X^3X^5$ *rem* $X^8 + X) = X$ *and* $lm(Y^2X^5$ *rem* $X^3Y + Y^3 + X) = X^2Y^4$, *and from* $w(Y^2X^5) = w(X^2Y^4) > w(X)$ *we conclude that* (Y^2, X^5) *is SOWB with respect to* $\{1, 2, 3, 4, 5, 6, 7\}$.*)*
The set corresponding to case 2 is

$$\begin{aligned}\mathcal{L}(2) \quad = \quad & \{X^3, X^4, Y^3, X^5, XY^3, Y^4, X^6, \\ & X^2Y^3, XY^4, X^7, Y^5, X^2Y^4, Y^6\}.\end{aligned}$$

If we know a priori that $a_6 = 0$ *then we can conclude from the above that* $w_H(\vec{c}) \geq \#\mathcal{L}(2) = 13$. *Without such an information we can only conclude*

$$w_H(\vec{c}) \geq \min\{\#\mathcal{L}(1), \#\mathcal{L}(2)\} = 6.$$

It can be shown using Theorem 15 that $\widetilde{E}_{imp}(11) = C(I, L)$ *where*

$$L = ev\big(Span_{\mathbb{F}_8}\{1 + I_8, X + I_8, Y + I_8, X^2 + I_8, XY + I_8, Y^2 + I_8\}\big).$$

That is, a code with parameters $[n, k, d]$ *equal to* $[22, 6, \geq 11]$.
If instead we choose

$$\widetilde{L} = ev\big(Span_{\mathbb{F}_8}\{1 + I_8, X + I_8, Y + I_8, X^2 + I_8, XY + I_8, X^3 + I_8\}\big)$$

then we do not need to consider the case 1 described above. By inspection the code parameters $[n, k, d]$ *of* $C(I, \widetilde{L})$ *are* $[22, 6, \geq 12]$.

Chapter 6

Generalised Hamming weights

As mentioned at the end of Section 2 it is possible to lift Theorem 15 to also deal with generalised Hamming weights. Recall that these parameters are important in the analysis of the wiretap channel of type II as well as in the analysis of secret sharing schemes based on coding theory, see [25], [17] and [16]. In the following definition note that d_1 corresponds to the minimum distance.

Definition 34. *Let $C \subseteq \mathbb{F}_q^n$ be a code of dimension k. For $t = 1, \ldots, k$ the tth generalised Hamming weight is*

$$d_t(C) = \min\{\#Supp\, D \mid D \text{ is a subspace of } C \text{ of dimension } t\}.$$

Here, $Supp\, D$ means the entries for which some word in D is different from zero.

We start with an example that illustrates the idea in our generalisation of Theorem 15.

Example 10. *This is a continuation of Example 2 where we considered $I = \langle X^4 + X^2 + X - Y^6 - Y^5 - Y^3 \rangle \subseteq \mathbb{F}_8[X, Y]$ and the weighted degree lexicographic ordering $\prec_w$ (Definition 10) given by $X = X_1$, $Y = X_2$, $w(X) = 3$ and $w(Y) = 2$. The reduced Gröbner basis for I_8 with respect to $\prec_w$ equals $\mathcal{G} = \{X^4 + X^2 + X - Y^6 - Y^5 - Y^3, Y^8 - Y\}$. We shall estimate $\#Supp\, D$ for $D = Span_{\mathbb{F}_8}\{ev(A + I_8), ev(B + I_8)\}$ where*

$$\begin{aligned} A &= a_1 1 + a_2 Y + a_3 X + a_4 Y^2 + a_5 XY + a_6 Y^3 + a_7 X^2 + \\ &\quad a_8 XY^2 + a_9 Y^4 + a_{10} X^2 Y + a_{11} XY^3 + a_{12} X^3 + a_{13} Y^5 + \\ &\quad a_{14} X^2 Y^2 + a_{15} XY^4 + a_{16} X^3 Y, \\ B &= b_1 1 + b_2 Y + b_3 X + b_4 Y^2 + b_5 XY + b_6 Y^3 + b_7 X^2 + \\ &\quad b_8 XY^2 + b_9 Y^4 + b_{10} X^2 Y + b_{11} XY^3 + b_{12} X^3. \end{aligned}$$

Here, $a_i \in \mathbb{F}_8$, $i = 1, \ldots, 16$, $b_i \in \mathbb{F}_8$, $i = 1, \ldots, 12$ and $a_{16} \neq 0$ and $b_{12} \neq 0$. Depending on a_{15} being equal to zero or not, A has in its support either one or two monomials of highest weight which is 11. Similarly, depending on b_{11} being zero or

not, B has in its support either one or two monomials of highest weight which is 9.

Case (1,1): Assume $a_{15} \neq 0$, $b_{11} \neq 0$. We have $lm(A) = X^3Y$, $lm(A \cdot X \text{ rem } \mathcal{G}) = X^2Y^4$, $lm(B) = X^3$ and $lm(B \cdot X \text{ rem } \mathcal{G}) = X^2Y^3$. Hence,

$$\begin{aligned}\Delta_{\prec_w}(I_8 + \langle A, B\rangle) \quad \subseteq \quad & \{X^\alpha Y^\beta \mid 0 \leq \alpha < 3, 0 \leq \beta < 8 \text{ and if} \\ & \alpha = 2 \text{ then } \beta < 3\}\end{aligned}$$

and therefore by Corollary 4 (see also the proof of Theorem 9)

$$\#Supp\, D = n - \#\Delta_{\prec_w}(I_8 + \langle A, B\rangle) \geq 32 - 19 = 13.$$

Case (2,1): Assume $a_{15} = 0$, $b_{11} \neq 0$. We have $lm(A) = X^3Y$, $lm(A \cdot X \text{ rem } \mathcal{G}) = Y^7$, $lm(B) = X^3$ and $lm(B \cdot X \text{ rem } \mathcal{G}) = X^2Y^3$. Hence,

$$\begin{aligned}\Delta_{\prec_w}(I_8 + \langle A, B\rangle) \quad \subseteq \quad & \{X^\alpha Y^\beta \mid 0 \leq \alpha < 3, 0 \leq \beta < 7 \text{ and if} \\ & \alpha = 2 \text{ then } \beta < 3\}\end{aligned}$$

and therefore

$$\#Supp\, D = n - \#\Delta_{\prec_w}(I_8 + \langle A, B\rangle) \geq 32 - 17 = 15.$$

Case (1,2): Assume $a_{15} \neq 0$, $b_{11} = 0$. We have $lm(A) = X^3Y$, $lm(A \cdot X \text{ rem } \mathcal{G}) = X^2Y^4$, $lm(B) = X^3$ and $lm(B \cdot X \text{ rem } \mathcal{G}) = Y^6$. Hence,

$$\begin{aligned}\Delta_{\prec_w}(I_8 + \langle A, B\rangle) \quad \subseteq \quad & \{X^\alpha Y^\beta \mid 0 \leq \alpha < 3, 0 \leq \beta < 6 \text{ and if} \\ & \alpha = 2 \text{ then } \beta < 4\}\end{aligned}$$

and therefore

$$\#Supp\, D = n - \#\Delta_{\prec_w}(I_8 + \langle A, B\rangle) \geq 32 - 16 = 16.$$

Case (2,2): Assume $a_{15} = b_{11} = 0$. We have $lm(A) = X^3Y$, $lm(A \cdot X \text{ rem } \mathcal{G}) = Y^7$, $lm(B) = X^3$ and $lm(B \cdot X \text{ rem } \mathcal{G}) = Y^6$. Hence,

$$\Delta_{\prec_w}(I_8 + \langle A, B\rangle) \subseteq \{X^\alpha Y^\beta \mid 0 \leq \alpha < 3, 0 \leq \beta < 6\}$$

and therefore by Corollary 4 (see also the proof of Theorem 9)

$$\#Supp\, D = n - \#\Delta_{\prec_w}(I_8 + \langle A, B\rangle) \geq 32 - 18 = 14.$$

In conclusion $\#Supp\, D \geq \min\{13, 15, 16, 14\} = 13$. Note that without the four different sets of assumptions on a_{15} and b_{11} we would only be able to establish

$$\begin{aligned}\Delta_{\prec_w}(I_8 + \langle A, B\rangle) \quad \subseteq \quad & \{X^\alpha Y^\beta \mid 0 \leq \alpha < 3, 0 \leq \beta < 8 \\ & \text{and if } \alpha = 2 \text{ then } \beta < 6\}\end{aligned}$$

from which we would only be able to conclude $\#Supp\, D \geq 32 - 22 = 10$.

Following the idea in Example 10 we reformulate Theorem 15 to deal with the second generalised Hamming weight. From this the reader can understand how to treat any generalised Hamming weight.

Proposition 35. *Let $D \subseteq \mathbb{F}_q^n$ be a subspace of dimension 2. Write $D = Span_{\mathbb{F}_q}\{ ev(\sum_{s=0}^{i_1} a_s M_s), ev(\sum_{s=0}^{i_2} b_s M_s)\}$. Here, $\Delta_\prec(I_q) = \{M_1, \ldots, M_n\}$, $a_s \in \mathbb{F}_q$, $b_s \in \mathbb{F}_q$ with $a_{i_1} \neq 0$ and $b_{i_2} \neq 0$. Without loss of generality we may assume $i_1 \neq i_2$. Let v_1 and v_2 be integers satisfying $0 \leq v_1 < i_1$ and $0 \leq v_2 < i_2$. We have*

$$\#Supp(D) \geq \min\{\#\mathcal{L}(z_1, z_2) \mid 1 \leq z_1 \leq v_1 + 1, 1 \leq z_2 \leq v_2 + 1\}.$$

The above sets are defined as follows: For $z_1 = 1, \ldots, v_1$ and $z_2 = 1, \ldots, v_2$ we have

$$\begin{aligned}
&\mathcal{L}(z_1, z_2) = \\
&\big\{K \in \Delta_\prec(I_q) \mid \exists M_j \in \Delta_\prec(I_q) \text{ such that for some } u \in \{1, 2\} \\
&(M_{i_u}, M_j) \text{ is SOWB with respect to } \{1, \ldots, i_u - z_u, i_u\} \\
&\text{and } lm(M_{i_u} M_j \text{ rem } \mathcal{G}) = K \\
&\text{or} \\
&(M_{i_u - z_u}, M_j) \text{ is SOWB with respect to } \{1, \ldots, i_u - z_u, i_u\} \\
&\text{and } lm(M_{i_u - z_u} M_j \text{ rem } \mathcal{G}) = K\big\},
\end{aligned}$$

For $z = 1, \ldots, v_1$

$$\begin{aligned}
&\mathcal{L}(z, v_2 + 1) = \\
&\big\{K \in \Delta_\prec(I_q) \mid \exists M_j \in \Delta_\prec(I_q) \text{ such that either} \\
&(M_{i_1}, M_j) \text{ is SOWB with respect to } \{1, \ldots, i_1 - z, i_1\} \\
&\text{and } lm(M_{i_1} M_j \text{ rem } \mathcal{G}) = K \\
&\text{or} \\
&(M_{i_1 - z}, M_j) \text{ is SOWB with respect to } \{1, \ldots, i_1 - z, i_1\} \\
&\text{and } lm(M_{i_1 - z} M_j \text{ rem } \mathcal{G}) = K \\
&\text{or} \\
&(M_{i_2}, M_j) \text{ is SOWB with respect to } \{1, \ldots, i_2 - v_2 - 1\} \\
&\text{and } lm(M_{i_2} M_j \text{ rem } \mathcal{G}) = K\big\}.
\end{aligned}$$

For $z = 1, \ldots, v_2$, $\mathcal{L}(v_1 + 1, z)$ is defined in a similar way. Finally

$$\begin{aligned}
&\mathcal{L}(v_1 + 1, v_2 + 1) = \\
&\big\{K \in \Delta_\prec(I_q) \mid \exists M_j \in \Delta_\prec(I_q) \text{ such that } (M_{i_u}, M_j) \text{ is SOWB} \\
&\text{with respect to } \{1, \ldots, i_u - v_u - 1\} \text{ and } lm(M_{i_u} M_j \text{ rem } \mathcal{G}) = K \\
&\text{for some } u \in \{1, 2\}\big\}.
\end{aligned}$$

The second generalised Hamming weight of $C(I, L)$ is found by repeating the above process for all possible choices of $i_1 < i_2$ corresponding to the cases that $D \subseteq C(I, L)$.

Proof. The proof is a straight forward enhancement of the proof for Theorem 15. □

For the choice of v_1 and v_2 in Proposition 35 we refer to Remark 16. Admittedly, the proposition is rather technical. Nevertheless even its generalisation to higher generalised Hamming weights can often be quite manageable. We shall comment further on this in Section 9.

Chapter 7

Formulation at linear code level

As mentioned in the introduction the Feng-Rao bound for primary codes in its most general form is a bound on any linear code described by means of a generator matrix. All other versions of the bound, such as the order bound for primary codes and the Feng-Rao bound for primary affine variety codes, can be viewed as corollaries to it. Below we reformulate the new bound in Theorem 15 at the linear code level.
Let n be a positive integer and q a prime power. Consider a fixed ordered triple $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ where $\mathcal{U} = \{\vec{u}_1, \ldots, \vec{u}_n\}$, $\mathcal{V} = \{\vec{v}_1, \ldots, \vec{v}_n\}$, and $\mathcal{W} = \{\vec{w}_1, \ldots, \vec{w}_n\}$ are three (possibly different) bases for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. We shall always denote by $\mathcal{I}$ the set $\{1, \ldots, n\}$.

Definition 36. *Consider a basis $\mathcal{A} = \{\vec{a}_1, \ldots, \vec{a}_n\}$ for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. We define a function $\bar{\rho}_{\mathcal{A}} : \mathbb{F}_q^n \to \{0, 1, \ldots, n\}$ as follows. For $\vec{c} \in \mathbb{F}_q \backslash \{\vec{0}\}$ we let $\bar{\rho}_{\mathcal{A}}(\vec{c}) = i$ if $\vec{c} \in Span_{\mathbb{F}_q}\{\vec{a}_1, \ldots, \vec{a}_i\} \backslash Span_{\mathbb{F}_q}\{\vec{a}_1, \ldots, \vec{a}_{i-1}\}$. Here, we used the notion $Span_{\mathbb{F}_q} \emptyset = \{\vec{0}\}$. Finally, we let $\bar{\rho}_{\mathcal{A}}(\vec{0}) = 0$.*

The component wise product plays a crucial role in the linear code enhancement of Theorem 15.

Definition 37. *The component wise product of two vectors $\vec{u}$ and $\vec{v}$ in $\mathbb{F}_q^n$ is defined by $(u_1, \ldots, u_n) * (v_1, \ldots, v_n) = (u_1 v_1, \ldots, u_n v_n)$.*

Definition 38. *Let $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ and $\mathcal{I}$ be as above. Consider $\mathcal{I}' \subseteq \mathcal{I}$. An ordered pair $(i, j) \subseteq \mathcal{I}' \times \mathcal{I}$ is said to be one-way well-behaving (OWB) with respect to $\mathcal{I}'$ if $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ holds for all $i' \in \mathcal{I}'$ with $i' < i$.*

The following theorem is a first generalisation of the Feng-Rao bound for primary codes. The generalisation compared to the usual Feng-Rao bound [1, 12] is that we allow $\mathcal{I}'$ to be different from $\{1, \ldots, \#\mathcal{I}'\}$. This is in the spirit of Section 5.

Theorem 39. *Consider* $\vec{c} = \sum_{s=1}^{t} a_s \vec{u}_{i_s}$ *with* $a_s \in \mathbb{F}_q$, $s = 1, \ldots, t$, $a_t \neq 0$ *and* $i_1 < \cdots < i_t$. *We have*

$$w_H(\vec{c}) \geq \#\big\{l \in \mathcal{I} \mid \exists j \in \mathcal{I} \;\; \text{such that} \;\; \bar{\rho}_{\mathcal{W}}(\vec{u}_{i_t} * \vec{v}_j) = l, \\ (i_t, j) \;\; \text{is OWB with respect to} \;\; \{i_1, \ldots, i_t\}\big\}. \tag{7.1}$$

Proof. Let $l_1 < \cdots < l_\sigma$ be the indexes l counted in (7.1). Denote by $j_1, \ldots, j_\sigma$ the corresponding j-values from (7.1). By assumption $\vec{c} * \vec{v}_{j_1}, \ldots, \vec{c} * \vec{v}_{j_\sigma}$ are linearly independent and therefore

$$\mathrm{Span}_{\mathbb{F}_q}\{\vec{c} * \vec{v}_{j_1}, \ldots, \vec{c} * \vec{v}_{j_\sigma}\} = \vec{c} * \mathrm{Span}_{\mathbb{F}_q}\{\vec{v}_{j_1}, \ldots, \vec{v}_{j_\sigma}\}$$

is a vector space of dimension σ. The theorem follows from the fact that $\vec{c} * \mathbb{F}_q^n$ is a vector space of dimension $w_H(\vec{c})$ containing the above space. □

A slight modification of Definition 38 and the above proof allows for further improvements.

Definition 40. *Let* $\mathcal{I}' \subseteq \mathcal{I}$. *A pair* $(i, j) \in \mathcal{I}' \times \mathcal{I}$ *is called strongly one-way well-behaving (SOWB) with respect to* $\mathcal{I}'$ *if* $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ *holds for all* $i' \in \mathcal{I}' \backslash \{i\}$.

The following theorem is the linear code interpretation of Theorem 15. Besides working for a larger class of codes, it is slightly stronger in that we formulate it in such a way that it supports the technique explained in Section 5. Concretely, what makes it stronger than Theorem 15 is the presence of the set $\hat{\mathcal{I}}$.

Theorem 41. *Consider a non-zero codeword* $\vec{c} = \sum_{t=1}^{i} a_t \vec{u}_t$, $a_t \in \mathbb{F}_q$ *for* $t = 1, \ldots, i$, $a_i \neq 0$. *Let* v *be an integer* $0 \leq v < i$. *Assume that for some set* $\hat{\mathcal{I}} \subseteq \{1, \ldots, i-1\}$ *we know a priori that* $a_x = 0$ *when* $x \in \hat{\mathcal{I}}$. *Let* $z_1 < \cdots < z_s$ *be the numbers in* $\{z \in \{i-v, \ldots, i-1\} \mid z \notin \hat{\mathcal{I}}\}$. *Write* $\mathcal{I}^* = \{z \in \{1, \ldots, i-v-1\} \mid z \notin \hat{\mathcal{I}}\}$. *We have* $w_H(\vec{c}) \geq \bar{\sigma}(i, v)$ *where* $\bar{\sigma}(i, v) = \min\{\#\mathcal{L}'(1), \ldots, \#\mathcal{L}'(s+1)\}$. *Here for* $t = 1, \ldots, s$ *we have*

$$\begin{aligned} \mathcal{L}'(t) \;\; = \;\; & \big\{l \in \mathcal{I} \mid \exists z \in \{z_{s-t+1}, i\} \;\; \text{and} \;\; j \in \mathcal{I} \;\; \text{such that} \\ & \bar{\rho}_{\mathcal{W}}(\vec{u}_z * \vec{v}_j) = l, (z, j) \;\; \text{is SOWB with respect to} \\ & \mathcal{I}^* \cup \{z_1, \ldots, z_{s-t+1}, i\}\big\}, \end{aligned}$$

and

$$\begin{aligned} \mathcal{L}'(s+1) \;\; = \;\; & \big\{l \in \mathcal{I} \mid \exists j \in \mathcal{I} \;\; \text{such that} \;\; \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l \\ & (i, j) \;\; \text{is OWB with respect to} \;\; \mathcal{I}^* \cup \{i\}\big\}. \end{aligned}$$

To establish a lower bound on the minimum distance of a code C *we choose for each* $i \in \bar{\rho}_{\mathcal{U}}(C)$ *a corresponding integer* v_i, $0 \leq v_i < i$. *The minimum distance is at least* $\min\{\bar{\sigma}(i, v_i) \mid i \in \bar{\rho}_{\mathcal{U}}(C)\}$.

Proof. The proof is a direct translation of the proof of Theorem 15. □

Remark 42. *For $v = 0$ Theorem 41 reduces to Theorem 39. For higher values of v Theorem 41 is at least as strong as Theorem 39 and sometimes stronger. In the same way as Theorem 15 was lifted in Section 6 to deal with generalised Hamming weights one can lift Theorem 39 and Theorem 41.*

Remark 43. *The order bound applies when the code construction is supported by an algebra with an order function (see [15, 11, 1]). Such an algebra is known as an order domain. The idea behind the bound is to detect OWB pairs by studying the behaviour of the order function. The method, however, does not always find all of them.*

Chapter 8

A related bound for dual codes

In the recent paper [9] we presented a new bound for dual codes. This bound is an improvement to the Feng-Rao bound for such codes as well as an improvement to the advisory bound from [24]. The new bound of the present paper can be viewed as a natural counter part to the bound from [9], the one bound dealing with primary codes and the other with dual codes.

Definition 44. *Consider an ordered triple of bases $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ for $\mathbb{F}_q^n$ and $\mathcal{I}$ as in Section 7. We define $m : \mathbb{F}_q^n \backslash \{\vec{0}\} \to \mathcal{I}$ by $m(\vec{c}) = l$ if l is the smallest number in $\mathcal{I}$ for which $\vec{c} \cdot \vec{w}_l \neq 0$. (Here, and in the following the symbol $\cdot$ means the usual inner product).*

Definition 45. *Consider numbers $1 \leq l, l+1, \ldots, l+g \leq n$. A set $\mathcal{I}' \subseteq \mathcal{I}$ is said to have the μ-property with respect to l with exception $\{l+1, \ldots, l+g\}$ if for all $i \in \mathcal{I}'$ a $j \in \mathcal{I}$ exists such that*

(1a) $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l$, and

(1b) for all $i' \in \mathcal{I}'$ with $i' < i$ either $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < l$ or $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) \in \{l+1, \ldots, l+g\}$ holds.

Assume next that $l+g+1 \leq n$. The set $\mathcal{I}'$ is said to have the relaxed μ-property with respect to $(l, l+g+1)$ with exception $\{l+1, \ldots, l+g\}$ if for all $i \in \mathcal{I}'$ a $j \in \mathcal{I}$ exists such that either conditions (1a) and (1b) above hold or

(2a) $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l+g+1$, and

(2b) (i, j) is OWB with respect to $\mathcal{I}'$, and

(2c) no $i' \in \mathcal{I}'$ with $i' < i$ satisfies $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) = l$.

The new bound from [9, Th. 19] reads:

Theorem 46. *Consider a non-zero codeword $\vec{c}$ and let $l = m(\vec{c})$. Choose a non-negative integer v such that $l + v \leq n$. Assume that for some indexes $x \in \{l+1, \ldots, l+v\}$ we know a priori that $\vec{c} \cdot \vec{w}_x = 0$. Let $l'_1 < \cdots < l'_s$ be the remaining indexes from $\{l+1, \ldots, l+v\}$. Consider the sets $\mathcal{I}'_0, \mathcal{I}'_1, \ldots, \mathcal{I}'_s$ such that:*

- *$\mathcal{I}'_0$ has the μ-property with respect to l with exception $\{l+1,\ldots,l+v\}$.*
- *For $i=1,\ldots,s$, $\mathcal{I}'_i$ has the relaxed μ-property with respect to (l,l'_i) with exception $\{l+1,\ldots,l'_i-1\}$.*

We have

$$w_H(\vec{c}) \geq \min\{\#\mathcal{I}'_0, \#\mathcal{I}'_1, \ldots, \#\mathcal{I}'_s\}. \tag{8.1}$$

To establish a lower bound on the minimum distance of a code C we repeat the above process for each $l \in m(C)$. For each such l we choose a corresponding v, we determine sets $\mathcal{I}'_i$ as above and we calculate the right side of (8.1). The smallest value found when l runs through $m(C)$ constitutes a lower bound on the minimum distance.

The sets $\mathcal{I}'_i$ and the use of Theorem 46 are illustrated in the next section where we discuss affine variety codes defined from ideals I_q satisfying that $\Delta_{\prec_w}(I_q)$ is a box.

If we compare Theorem 46 with Theorem 41 we see that to some extent they have the same flavor. Besides that one deals with dual codes and the other with primary codes another difference is that Theorem 46 has the freedom to choose appropriate sets $\mathcal{I}'_0,\ldots,\mathcal{I}'_s$ whereas the sets $\mathcal{L}'(1),\ldots,\mathcal{L}'(s+1)$ in Theorem 41 are unique. In [9] it was also shown how to lift Theorem 46 to deal with generalised Hamming weights. Similar remarks as above hold for the two bounds when applied to such parameters.

Chapter 9

A comparison of the new bounds for primary and dual codes

Recall that it was shown in [10] how the Feng-Rao bound for primary codes and the Feng-Rao bound for dual codes can be viewed as consequences of each other. This result holds when the bound is equipped with one of the well-behaving properties WB or OWB. Regarding the case where WWB is used a possible connection is unknown. In a similar fashion as the proof in [10] breaks down if one uses WWB it also breaks down when one tries to prove a correspondence between Theorem 41 and Theorem 46. We leave it as an open research problem to decide if a general connection exists or not.

In Section 4 we analysed the parameters of primary affine variety codes coming from optimal generalised C_{ab} polynomials. Using the method from Section 8 one can make a similar analysis for the corresponding dual codes producing similar code parameters. As an alternative, below we explain how to derive this result directly from what we have already shown regarding primary codes from optimal generalised C_{ab} polynomials.

Recall that for optimal generalised C_{ab} polynomials $\Delta_{\prec_w}(I_q)$ is a box:

$$\Delta_{\prec_w}(I_q) = \{M_1, \ldots, M_n\} = \{X^{\alpha_1}Y^{\alpha_2} \mid 0 \leq \alpha_1 < a, 0 \leq \alpha_2 < q\}.$$

This fact gives us the following crucial implication (as usual we assume $M_1 \prec_w \cdots \prec_w M_n$):

$$M_i = X^{\alpha_1}Y^{\alpha_2} \Rightarrow M_{n-i+1} = X^{a-1-\alpha_1}Y^{q-1-\alpha_2}, \text{ for } i = 1, \ldots, n. \tag{9.1}$$

Consider codewords $\vec{c} = \mathrm{ev}\big(\sum_{s=1}^{i} a_s M_s + I_q\big)$, $a_s \in \mathbb{F}_q$, $a_i \neq 0$, and $\vec{c}' \in \mathbb{F}_q^n$ such that $m(\vec{c}') = n - i + 1$. Let v be an integer, $0 \leq v < i$. Recall that in Section 4 we determined $\mathcal{L}(u)$, $u = 1, \ldots, v+1$. If we use Theorem 46 with $\{l+1, \ldots, l+v\} = \{l'_1, \ldots, l'_s\}$ (no *a priori* knowledge) then we can choose

$$\mathcal{I}'_0 = \{n - l + 1 \mid M_l \in \mathcal{L}(v+1)\}$$

and for $u = 1, \ldots, v$

$$\mathcal{I}'_u = \{n - l + 1 \mid M_l \in \mathcal{L}(u)\}.$$

For $S \subseteq \{1, \ldots, n\}$ define $\bar{S} = \{1, \ldots, n\} \backslash \{n - s + 1 \mid s \in S\}$. Consider

$$L = \mathrm{Span}_{\mathbb{F}_q}\{\mathrm{ev}(M_s + I_q) \mid s \in S\},$$

$$\bar{L} = \mathrm{Span}_{\mathbb{F}_q}\{\mathrm{ev}(M_s + I_q) \mid s \in \bar{S}\}.$$

As $\#\mathcal{I}'_0 = \#\mathcal{L}(v+1)$ and for $u = 1, \ldots, v$, $\#\mathcal{I}'_u = \#\mathcal{L}(u)$ we conclude that Theorem 46 produces the same estimate for the minimum distance of $C^{\perp}(I, \bar{L})$ as Theorem 15 produces for the minimum distance of $C(I, L)$. However, we do not in general have $C(I, L) = C^{\perp}(I, \bar{L})$ and therefore the above analysis does not imply that Theorem 15 is a consequence of Theorem 46 even in the case of optimal generalised C_{ab} polynomials.
The above correspondence regarding the minimum distance immediately carries over to the generalised Hamming weights. In [9, Sec. 4] we implemented the enhancement of Theorem 46 to generalised Hamming weights for a couple of concrete dual affine variety codes coming from optimal generalised C_{ab} polynomials. As a consequence of (9.1) the estimates found in [9, Sec. 4] for $C^{\perp}(I, \bar{L})$ also hold for $C(I, L)$. This demonstrates the usefulness of the method described in Section 6.

We conclude the section by demonstrating that $d\big(C(I, L)\big) = d\big(C^{\perp}(I, \bar{L})\big)$ does not hold for all generalised C_{ab} polynomials.

Example 11. *In this example we consider the generalised C_{ab} polynomial $F(X, Y) = G(X) - H(Y) \in \mathbb{F}_{32}[X, Y]$ where $G(X) = X^{20} + X^{18} + X^{10} + X^9 + X^5$ and $H(Y) = Y^{26} + Y^{22} + Y^{21} + Y^{13} + Y^{11}$. Observe that both G and H are $(\mathbb{F}_{32}, \mathbb{F}_2)$-polynomials and that G satisfies the condition in Proposition 26 ensuring that for each $\eta \in \mathbb{F}_2$ there exists exactly $2^4 = 16$ $\gamma \in \mathbb{F}_{32}$ such that $G(\gamma) = \eta$. In particular $F(X, Y)$ has exactly 512 zeros in $\mathbb{F}_{32}$. As $a = \deg G > 16$ $\{F(X, Y), X^{32} - X, Y^{32} - Y\}$ cannot be a Gröbner basis with respect to $\prec_w$ (it would violate the footprint bound, Corollary 4). Applying Buchberger's algorithm we find a Gröbner basis and from that the corresponding footprint*

$$\begin{aligned} \Delta_{\prec_w}(I_{32}) &= \{X^{\alpha_1} X^{\alpha_2} \mid 0 \leq \alpha_1 < 12, 0 \leq \alpha_2 < 32\} \\ &\quad \cup \{X^{\alpha_1} X^{\alpha_2} \mid 12 \leq \alpha_1 < 20, 0 \leq \alpha_2 < 16\}. \end{aligned}$$

Recall the improved construction $\widetilde{E}_{imp}(\delta)$ of primary affine variety codes as introduced in Definition 17. In a similar way, as Theorem 15 gives rise to the above Feng-Rao style improved primary codes, Theorem 46 gives rise to improved dual codes. These codes were named $\widetilde{C}_{fim}(\delta)$ in [9, Rem. 20]. In a computer experiment we calculated the parameters of these codes. In Figure 9.1 we plot the derived relative parameters. As is seen for some designed distances δ, $\widetilde{E}_{imp}(\delta)$ has the highest dimension. For other designed distances δ, $\widetilde{C}_{fim}(\delta)$ is of highest dimension.

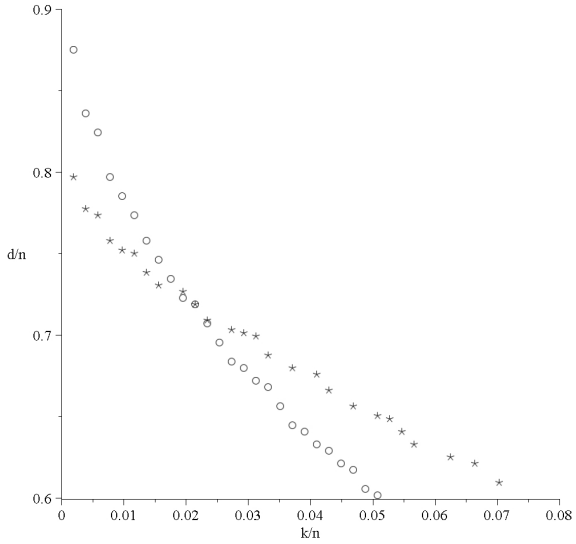

Figure 9.1: Improved codes from Example 11. A $\circ$ corresponds to $\widetilde{E}_{imp}(\delta)$, and an $*$ corresponds to $\widetilde{C}_{fim}(\delta)$.

Chapter 10

Conclusion

In this paper we proposed a new bound for the minimum distance and the generalised Hamming weights of general linear code for which a generator matrix is known. We demonstrated the usefulness of our bound in the case of affine variety codes where only the first of the two order domain conditions is satisfied. For this purpose we introduced the concept of optimal generalised C_{ab} polynomials and we derived closed formula expressions for the corresponding code words. We leave it for further research to establish closed formula expressions for other families of ideals where only the first order domain condition is satisfied. We touched upon the connection to a bound for dual codes introduced in the recent paper [9], but leave an investigation of a possible general relation between the two bounds for further research. It is an interesting question if there exist examples where our new method improves on the Feng-Rao bound for one-point algebraic geometric codes (the case where both order domain conditions are satisfied). This would require that we do not choose v as in Remark 16 and that we make extensive use of the polynomials $X_i^q - X_i$. Also this question is left for further research. The usual Feng-Rao bound for primary codes comes with a decoding algorithm that corrects up to half the estimated minimum distance [10]. This result holds when the bound is equipped with the well-behaving property WB. For the case of WWB or OWB no decoding algorithm is known. Finding a decoding algorithm that corrects up to half the value guaranteed by Theorem 15 would impose the missing decoding algorithms mentioned above.

Acknowledgements

Part of this research was done while the second listed author was visiting East China Normal University. We are grateful to Professor Hao Chen for his hospitality. The authors also gratefully acknowledge the support from the Danish National Research Foundation and the National Science Foundation of China (Grant No. 11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography. The authors would like to thank Diego Ruano, Peter Beelen and Ryutaroh Matsumoto for pleasant discussions. Finally

we are grateful to the anonymous reviewers for their careful reading and useful suggestions.

Bibliography

[1] H. E. Andersen and O. Geil. Evaluation codes from order domain theory. *Finite Fields Appl.*, 14(1):92–123, 2008.

[2] Herivelto Borges and Ricardo Conceição. On the characterization of minimal value set polynomials. *J. Number Theory*, 133(6):2021–2035, 2013.

[3] D.A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*, volume 10. Springer, 1997.

[4] G. L. Feng and T. R. N. Rao. A simple approach for construction of algebraic-geometric codes from affine plane curves. *IEEE Trans. Inform. Theory*, 40(4):1003–1012, 1994.

[5] J. Fitzgerald and R. F. Lax. Decoding affine variety codes using Gröbner bases. *Des. Codes Cryptogr.*, 13(2):147–158, 1998.

[6] O. Geil. On codes from norm-trace curves. *Finite Fields Appl.*, 9(3):351–371, 2003.

[7] O. Geil. Evaluation codes from an affine variety code perspective. In Edgar Martínez-Moro, Carlos Munuera, and Diego Ruano, editors, *Advances in algebraic geometry codes*, volume 5 of *Coding Theory and Cryptology*, pages 153–180. World Scientific, Singapore, 2008.

[8] O. Geil and T. Høholdt. Footprints or generalized Bezout's theorem. *IEEE Trans. Inform. Theory*, 46(2):635–641, 2000.

[9] O. Geil and S. Martin. Further improvements on the Feng-Rao bound for dual codes. *arXiv preprint arXiv:1305.1091*, 2013.

[10] O. Geil, R. Matsumoto, and D. Ruano. Feng-Rao decoding of primary codes. *Finite Fields Appl.*, 23:35–52, 2013.

[11] O. Geil and R. Pellikaan. On the structure of order domains. *Finite Fields Appl.*, 8(3):369–396, 2002.

[12] O. Geil and C. Thommesen. On the Feng-Rao bound for generalized Hamming weights. In M. P.C. Fossorier, H. Imai, S. Lin, and A. Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 3857 of *Lecture Notes in Computer Science*, pages 295–306. Springer, 2006.

[13] M. Grassl. Code Tables: Bounds on the parameters of various types of codes. `http://www.codetables.de`, Jun. 2013.

[14] F. Hernando, K. Marshall, and M. E. O'Sullivan. The dimension of subcode-subfields of shortened generalized Reed–Solomon codes. *Des. Codes Cryptogr.*, pages 1–12, 2011.

[15] T. Høholdt, J. H. van Lint, and R. Pellikaan. Algebraic geometry codes. In Vera S. Pless and William Cary Huffman, editors, *Handbook of Coding Theory*, volume 1, pages 871–961. Elsevier, Amsterdam, 1998.

[16] J. Kurihara, T. Uyematsu, and R. Matsumoto. Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight. *IEICE Trans. Fundamentals*, E95-A(11):2067–2075, Nov. 2012.

[17] Y. Luo, C. Mitrpant, A.J.H. Vinck, and K. Chen. Some new characters on the wire-tap channel of type II. *IEEE Trans. Inform. Theory*, 51(3):1222–1229, 2005.

[18] R. Matsumoto. The C_{ab} curve. `http://www.rmatsumoto.org/cab.pdf`, 1998.

[19] S. Miura. Algebraic geometric codes on certain plane curves. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 76(12):1–13, 1993. (in Japanese).

[20] S. Miura. *Study of Error-Correcting Codes based on Algebraic Geometry*. PhD thesis, Univ. Tokyo, 1997. (in Japanese).

[21] S. Miura. Linear codes on affine algebraic curves. *Trans. IEICE*, J81-A(10):1398–1421, 1998. (in Japanese).

[22] R. Pellikaan. On the existence of order functions. *Journal of Statistical Planning and Inference*, 94(2):287–301, 2001.

[23] L. Rédei. *Lacunary Polynomials over Finite Fields*. North-Holland Publ. Comp., Amsterdam, 1973.

[24] G. Salazar, D. Dunn, and S. B. Graham. An improvement of the Feng-Rao bound on minimum distance. *Finite Fields Appl.*, 12:313–335, 2006.

[25] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.

PAPER III

Further improvements on the Feng-Rao bound for dual codes

Geil Olav Martin Stefano

Geil Olav and Martin Stefano, "Further improvements on the Feng-Rao bound for dual codes", *accepted to Finite Fields and their Applications*, 2013, preprint at arXiv: 1305.1091v1 [cs.IT], DOI: 10.1016/j.ffa.2014.05.006

Further improvements on the Feng-Rao bound for dual codes

Olav Geil[1] and Stefano Martin[2,1]

[1]Department of Mathematical Sciences, Aalborg University
[2]Engineering Software Institute, East China Normal University

[1]olav@math.aau.dk
[2]stefano@math.aau.dk

Abstract

Salazar, Dunn and Graham in [16] presented an improved Feng-Rao bound for the minimum distance of dual codes. In this work we take the improvement a step further. Both the original bound by Salazar et. al., as well as our improvement are lifted so that they deal with generalized Hamming weights. We also demonstrate the advantage of working with one-way well-behaving pairs rather than weakly well-behaving or well-behaving pairs.

Keywords: advisory bound, affine variety code, Feng-Rao bound, generalized Hamming weight, minimum distance, well-behaving pair

MSC: 94B65, 94B27, 94B05

Chapter 1

Introduction

The celebrated Feng-Rao bound for the minimum distance of dual codes [2, 3] was originally presented in a language close to that of affine variety codes [4]. A more general result was derived by formulating the bound at the level of general linear codes [15, 14, 13, 7]. Among the general linear code formulations the weakest version uses one basis for $\mathbb{F}_q^n$ and the concept of *well-behaving pairs* (WB). The stronger versions use two or even three bases and the concept of *weakly well-behaving* (WWB) or even *one-way well-behaving* (OWB). The strong linear code formulation is the most general of all versions of the Feng-Rao bound in the sense that all other formulations, including the order bound [9], can be viewed as corollaries to it.

In [16] Salazar, Dunn and Graham presented a clever improvement to the Feng-Rao bound for the minimum distance of dual codes which they name *the advisory bound* [16, Def. 40]. Their exposition uses a language close to that of Feng and Rao's original papers. In the present paper we start by giving a general linear code enhancement of their bound and we lift it to deal with generalized Hamming weights improving upon the usual Feng-Rao bound for generalized Hamming weights of dual codes [8, 7]. We remind the reader that generalized Hamming weights among other things are relevant for the analysis of wiretap channels of type II [17, 12] and secret sharing schemes based on error correcting codes [10]. Our proof demonstrates that the advisory bound is a consequence of a lemma from which further improvements can be derived. These improvements are investigated in detail and are formulated in a separate bound. The new bound is then lifted to deal with generalized Hamming weights. Our exposition involves as a main ingredient a relaxation of the concept of OWB.

The paper [16] describes two families of affine variety codes for which the advisory bound is sometimes strictly better than the Feng-Rao bound. The first family [16, Sec. 3.1] is related to a curve over $\mathbb{F}_8$. The second family [16, Sec. 3.2] relates to a surface over $\mathbb{F}_4$. In Section 4 we shall give a thorough treatment of the curve from [16, Sec. 3.1] and a related curve over $\mathbb{F}_{27}$. As it shall be demonstrated for these curves sometimes the new bound produces much better results than the advisory bound. Also it is demonstrated for the first time in the literature that

the Feng-Rao bound equipped with OWB can sometimes be much better than the same bound equipped with WWB. We do not treat the surface from [16, Sec. 3.2] in the present paper. This is due to the fact that it is more natural to treat the corresponding quotient ring as an order domain with weights in $\mathbb{N}_0^2$ [6, 1]. Doing so, one finds much better code parameters by applying the usual Feng-Rao bound than what was produced in [16, Sec. 3.2] by the advisory bound. It is beyond the scope of the present paper to give the details.

Chapter 2

Enhancements of the advisory bound

To explain better what is the essence of Salazar, Dunn, and Graham's method, below we explain it at the level of general linear codes. We also extend their method to deal with generalized Hamming weights.

Let n be a positive integer and q a prime power. Throughout the following two sections we consider a fixed ordered triple $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ where $\mathcal{U} = \{\vec{u}_1, \ldots, \vec{u}_n\}$, $\mathcal{V} = \{\vec{v}_1, \ldots, \vec{v}_n\}$, and $\mathcal{W} = \{\vec{w}_1, \ldots, \vec{w}_n\}$ are three (possibly different) bases for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. By $\mathcal{I}$ we shall always mean the set $\{1, \ldots, n\}$.

Definition 1. Let the function $\bar{\rho}_{\mathcal{W}} : \mathbb{F}_q^n \to \{0, 1, \ldots, n\}$ be given as follows. For $\vec{c} \neq \vec{0}$ we let $\bar{\rho}_{\mathcal{W}}(\vec{c}) = i$ if $\vec{c} \in \mathrm{Span}\{\vec{w}_1, \ldots, \vec{w}_i\} \setminus \mathrm{Span}\{\vec{w}_1, \ldots, \vec{w}_{i-1}\}$. Here, we used the notion $\mathrm{Span}\,\emptyset = \{\vec{0}\}$. Finally, we let $\bar{\rho}_{\mathcal{W}}(\vec{0}) = 0$.

The following two concepts play a crucial role in our exposition.

Definition 2. The component wise product of two vectors $\vec{u}$ and $\vec{v}$ in $\mathbb{F}_q^n$ is defined by $(u_1, \ldots, u_n) * (v_1, \ldots, v_n) = (u_1 v_1, \ldots, u_n v_n)$.

Definition 3. Let an ordered triple of bases $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ be given. We define $m : \mathbb{F}_q^n \setminus \{\vec{0}\} \to \mathcal{I}$ by $m(\vec{c}) = l$ if l is the smallest number in $\mathcal{I}$ for which $\vec{c} \cdot \vec{w}_l \neq 0$.

We start by stating the Feng-Rao bound for the minimum distance of dual codes.

Definition 4. Let $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ and $\mathcal{I}$ be as above.

- An ordered pair $(i, j) \in \mathcal{I} \times \mathcal{I}$ is said to be well-behaving (WB) if $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_{j'}) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ holds for all $i' \leq i$, $j' \leq j$ with $(i', j') \neq (i, j)$.
- Less restrictive $(i, j) \in \mathcal{I} \times \mathcal{I}$ is said to be weakly well-behaving (WWB) if $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ and $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_{j'}) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ hold for all $i' < i$ and $j' < j$.

- Even less restrictive $(i,j) \in \mathcal{I} \times \mathcal{I}$ is said to be one-way well-behaving (OWB) if $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ holds for all $i' < i$.

The usual Feng-Rao bound for the minimum distance of dual codes reads.

Theorem 5. *For $\vec{c} \in \mathbb{F}_q^n \backslash \{\vec{0}\}$ write $l = m(\vec{c})$. The Hamming weight of $\vec{c}$ satisfies*

$$\begin{aligned} w_H(\vec{c}) &\geq \#\{(i,j) \in \mathcal{I} \times \mathcal{I} \mid \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l \\ &\qquad\qquad \textit{and } (i,j) \textit{ is OWB}\} \qquad (2.1) \\ &\geq \#\{(i,j) \in \mathcal{I} \times \mathcal{I} \mid \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l \\ &\qquad\qquad \textit{and } (i,j) \textit{ is WWB}\} \qquad (2.2) \\ &\geq \#\{(i,j) \in \mathcal{I} \times \mathcal{I} \mid \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l \\ &\qquad\qquad \textit{and } (i,j) \textit{ is WB}\}. \qquad (2.3) \end{aligned}$$

From [13, Ex. 2.6] and [16, Sec. 3.1] we have examples where (2.2) are stronger than (2.3). Section 4 demonstrates that also (2.1) can be stronger than (2.2). This fact was not known before.

Although [16] considered only WB and WWB we shall state our enhancement of the advisory bound using OWB. Doing so we get the strongest possible version which in addition requires the minimal number of calculations.

Definition 6. Let $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ and $\mathcal{I}$ be as above, and consider a subset $\mathcal{I}' = \{i_1, \ldots, i_s\}$ of $\mathcal{I}$ with $i_a \neq i_b$ for $a \neq b$. An ordered pair (i,j) in $\mathcal{I}' \times \mathcal{I}$ is said to be one-way well-behaving (OWB) with respect to $\mathcal{I}'$ if $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ holds for all $i' \in \mathcal{I}'$ with $i' < i$.
We say that $\mathcal{I}'$ has the μ-property with respect to l if for all $i \in \mathcal{I}'$ there exists a $j \in \mathcal{I}$ such that

1. (i,j) is OWB with respect to $\mathcal{I}'$,
2. $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l$.

The following theorem is an enhancement of the advisory bound from [16, Th. 48].

Theorem 7. *Let $\vec{c} \in \mathbb{F}_q^n \backslash \{\vec{0}\}$. We have*

$$\begin{aligned} w_H(\vec{c}) \quad \geq \quad & \max\{\#\mathcal{I}' \mid \mathcal{I}' \subseteq \mathcal{I}, \mathcal{I}' \textit{ has the } \mu\textit{-property} \\ & \qquad\qquad \textit{with respect to } m(\vec{c})\}. \end{aligned}$$

Proof. The theorem is a special case of Theorem 14 below. □

Remark 8. Consider the code $C(s) = \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c} \cdot \vec{w}_1 = \cdots = \vec{c} \cdot \vec{w}_s = 0\}$. To estimate the minimum distance of $C(s)$ we calculate the minimal value from Theorem 7 when $m(\vec{c})$ runs through all possible numbers in $\{s+1, \ldots, n\}$. As an alternative to $C(s)$ we get an improved code construction by using as parity checks only those $\vec{w}_l$, $l \in \mathcal{I}$ for which Theorem 7 with $m(\vec{c}) = l$ produces values less than δ. The minimum distance of this code, which we denote by $\widetilde{C}_{adv}(\delta)$, is at least δ.

We next consider the generalized Hamming weights.

Definition 9. Let $C \subseteq \mathbb{F}_q^n$ be a code of dimension k. For $t = 1, \ldots, k$ the tth generalized Hamming weight is

$$d_t(C) = \min\{\#\mathrm{Supp}\, D \mid D \text{ is a subspace of } C \text{ of dimension } t\}.$$

Clearly, d_1 is nothing but the usual minimum distance. To estimate generalized Hamming weights we first need to extend Definition 6 and Definition 3.

Definition 10. Consider $1 \leq l_1 < \cdots < l_t \leq n$ and let $\mathcal{I}' \subseteq \mathcal{I}$. We will say that $\mathcal{I}'$ has the μ-property with respect to $\{l_1, \ldots, l_t\}$ if for all $i \in \mathcal{I}'$ there exists a $j \in \mathcal{I}$ such that

- (i, j) is OWB with respect to $\mathcal{I}'$,
- $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) \in \{l_1, \ldots, l_t\}$.

Definition 11. Let $D \subseteq \mathbb{F}_q^n$ be a subspace. We define

$$m(D) = \big\{m(\vec{c}) \mid \vec{c} \in D \backslash \{\vec{0}\}\big\}.$$

The following proposition is easily proved.

Proposition 12. *If $D \subseteq \mathbb{F}_q^n$ is a subspace of dimension t then $\#m(D) = t$.*

Our enhancement of the advisory bound is based on the following lemma from which we shall also in the next section derive an even better bound.

Lemma 13. *Consider a subspace $D \subseteq \mathbb{F}_q^n$. Let $U \subseteq \mathbb{F}_q^n$ be a subspace of dimension δ such that for all non-zero words $\vec{u} \in U$ for some $\vec{v}_j \in \mathcal{V}$ and some $\vec{c} \in D$ we have $(\vec{u} * \vec{v}_j) \cdot \vec{c} \neq 0$ then $|Supp\, D| \geq \delta$.*

Proof. Aiming for a contradiction we assume that the above criteria holds true, but that $|\mathrm{Supp}\, D| < \delta$. Without loss of generality we write $\mathrm{Supp}\, D = \{1, \ldots, g\}$. Clearly $g \leq \delta - 1$. Consider a matrix whose rows constitute a basis for U. After having performed Gaussian elimination we arrive at a matrix whose last row, say $\vec{u}'$, starts with $\delta - 1$ zeros. Therefore $\vec{u}' * \vec{c} = \vec{0}$ holds for all $\vec{c} \in D$. On the other hand by assumption for some particular word $\vec{c} \in D$ we have $(\vec{u}' * \vec{v}_j) \cdot \vec{c} \neq 0 \Rightarrow \vec{u}' * \vec{c} \neq \vec{0}$. This is a contradiction. □

Theorem 14. *Consider a subspace $D \subset \mathbb{F}_q^n$. We have*

$$\#Supp\, D \quad \geq \quad \max\{\#\mathcal{I}' \mid \mathcal{I}' \subseteq \mathcal{I}, \mathcal{I}' \text{ has the } \mu\text{-property with respect to } m(D)\}.$$

Proof. Let $\mathcal{I}' = \{i_1, \ldots, i_\delta\}$, $i_a \neq i_b$ for $a \neq b$, be a set which has the μ-property with respect to $m(D)$. Consider $\sum_{r=1}^{s} \alpha_r \vec{u}_{i_r}$, $1 \leq s \leq \delta$ with $\alpha_r \in \mathbb{F}_q$, $\alpha_s \neq 0$. By assumption there exists a $j \in \mathcal{I}$ such that (i_s, j) is OWB with respect to $\mathcal{I}'$ and such that $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i_s} * \vec{v}_j) \in m(D)$. Therefore, $\bar{\rho}_{\mathcal{W}}\big(\big(\sum_{r=1}^{s} \alpha_r \vec{u}_{i_r}\big) * \vec{v}_j\big) \in m(D)$ and consequently for some $\vec{c} \in D$ we have $\big(\big(\sum_{r=1}^{s} \alpha_r \vec{u}_{i_r}\big) * \vec{v}_j\big) \cdot \vec{c} \neq 0$. The theorem now follows from Lemma 13. □

Remark 15. Let $\{\vec{d_1},\ldots,\vec{d_{n-k}}\} \subseteq \mathbb{F}_q^n$ be a linearly independent set and consider the code $C = \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c}\cdot\vec{d_1} = \cdots = \vec{c}\cdot\vec{d_{n-k}} = 0\}$. Without loss of generality we may assume that $\bar{\rho}_{\mathcal{W}}(\vec{d_1}) < \cdots < \bar{\rho}_{\mathcal{W}}(\vec{d_{n-k}})$ holds, say these numbers are $l_1 < \cdots < l_{n-k}$. It can be proven that $m(C) = \mathcal{I}\backslash\{l_1,\ldots,l_{n-k}\}$.

Combining Theorem 14 and Remark 15 we get:

Theorem 16. *Let $C = \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c}\cdot\vec{d_1} = \cdots = \vec{c}\cdot\vec{d_{n-k}} = 0\}$, where $\{\vec{d_1},\ldots,\vec{d_{n-k}}\}$ and $\{l_1,\ldots,l_{n-k}\}$ are as in Remark 15. For $t = 1,\ldots,k$ the tth generalized Hamming weight of C satisfies*

$$d_t(C) \geq \min\Big\{ \max\big\{\#\mathcal{I}' \mid \mathcal{I}' \subseteq \mathcal{I}, \mathcal{I}' \text{ has the } \mu\text{-property with respect to } \{m_1,\ldots,m_t\}\big\} \mid m_1 < \cdots < m_t, \; m_s \in \mathcal{I}\backslash\{l_1,\ldots,l_{n-k}\} \text{ for } s = 1,\ldots,t \Big\}.$$

In Section 4 we illustrate with a couple of examples that Theorem 16 is operational even though it does appear technical at a first glance.

In a straight forward manner one can enhance Theorem 16 to also deal with relative generalized Hamming weights (See [12, 11]). This bound should be compared with the naive bound, that the relative generalized Hamming weight is always at least as large as the estimate on the generalized Hamming weight from Theorem 16. It should also be compared to the Feng-Rao bound for relative generalized Hamming weights. As we have no examples where the mentioned enhancement of Theorem 16 produces results which are simultaneously better than the above mentioned two alternatives and as at the same time the enhancement of Theorem 16 is rather technical we do not give the details here.

Chapter 3

Further improvements

In the following we will strengthen the results from the previous section. We start by explaining how to improve upon Theorem 7. Given $\vec{c} \in \mathbb{F}_q^n \backslash \{\vec{0}\}$, consider the corresponding number $m(\vec{c}) = \min\{l \mid \vec{c} \cdot \vec{w}_l \neq 0\}$ and a set $\mathcal{I}' \subseteq \mathcal{I}$ which has the μ-property with respect to $m(\vec{c})$. Theorem 7 relies on the observation that if for $i \in \mathcal{I}'$, $j \in \mathcal{I}$ is the corresponding number such that $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = m(\vec{c})$ and (i, j) is OWB with respect to $\mathcal{I}'$ then

$$\vec{c} \cdot \left(\Big(\sum_{\substack{i' \in \mathcal{I}' \\ i' \leq i}} \alpha_{i'} \vec{u}_{i'} \Big) * \vec{v}_j \right) \neq 0$$

holds whenever $\alpha_{i'} \in \mathbb{F}_q$, $\alpha_i \neq 0$. Note that the above argument uses no information regarding the status of $\vec{c} \cdot \vec{w}_{m(\vec{c})+1}, \ldots, \vec{c} \cdot \vec{w}_n$. Indeed, if the only information we have on $\vec{c}$ is $m(\vec{c})$ then these numbers can take on all possible combinations of values from $\mathbb{F}_q$.

Remark 17. Let C be as in Remark 15 with

$$\bar{\rho}_{\mathcal{W}}(\vec{d}_1) = l_1 < \cdots < \bar{\rho}_{\mathcal{W}}(\vec{d}_{n-k}) = l_{n-k}. \tag{3.1}$$

Consider a general codeword $\vec{c} \in C \backslash \{\vec{0}\}$. If the only thing we know about $\vec{d}_1, \ldots, \vec{d}_{n-k}$ is (3.1) then we have no information regarding $\vec{c} \cdot \vec{w}_{l_1}, \ldots, \vec{c} \cdot \vec{w}_{l_{n-k}}$. If however, as the other extreme, we know that $\vec{d}_1 = \vec{w}_{l_1}, \ldots, \vec{d}_{n-k} = \vec{w}_{l_{n-k}}$ then we have $\vec{c} \cdot \vec{w}_{l_1} = \cdots = \vec{c} \cdot \vec{w}_{l_{n-k}} = 0$.

Write $l = m(\vec{c})$ and consider the indexes $l+1, \ldots, l+v \leq n$. Here, v is some positive integer. For some of the above indexes x we may *a priori* know that $\vec{c} \cdot \vec{w}_x = 0$ (Remark 17). Let $l'_1, \ldots, l'_s$ be the remaining indexes from $\{l+1, \ldots, l+v\}$. The idea in our improvement to Theorem 7 is to consider separately the following

$s+1$ cases:

$$\begin{array}{ll}
\text{Case 0:} & \vec{c}\cdot\vec{w}_{l'_1} = \cdots = \vec{c}\cdot\vec{w}_{l'_s} = 0. \\
\text{Case 1:} & \vec{c}\cdot\vec{w}_{l'_1} \neq 0. \\
\text{Case 2:} & \vec{c}\cdot\vec{w}_{l'_1} = 0, \vec{c}\cdot\vec{w}_{l'_2} \neq 0. \\
 & \vdots \\
\text{Case s:} & \vec{c}\cdot\vec{w}_{l'_1} = \cdots = \vec{c}\cdot\vec{w}_{l'_{s-1}} = 0, \vec{c}\cdot\vec{w}_{l'_s} \neq 0.
\end{array}$$

In each case z we establish a set $\mathcal{I}'_z \subseteq \mathcal{I}$ such that for every non-zero linear combination $\sum_{i\in\mathcal{I}'_z} \alpha_i\vec{u}_i$, $\alpha_i \in \mathbb{F}_q$, a $\vec{v}_j \in \mathcal{V}$ exists with

$$\vec{c}\cdot\left(\left(\sum_{i\in\mathcal{I}'_z}\alpha_i\vec{u}_i\right) * \vec{v}_j\right) \neq 0.$$

From Lemma 13 it then follows that $w_H(\vec{c}) \geq \min\{\#\mathcal{I}'_0, \ldots, \#\mathcal{I}'_s\}$. The following definition is what we need to deal with the above set-up. We should stress that although Definition 18 may appear long and technical, it is often quite manageable. This will be demonstrated in Section 4.

Definition 18. Consider the numbers $1 \leq l, l+1, \ldots, l+g \leq n$. A set $\mathcal{I}' \subseteq \mathcal{I}$ is said to have the μ-property with respect to l with exception $\{l+1, \ldots, l+g\}$ if for all $i \in \mathcal{I}'$ there exists $j \in \mathcal{I}$ such that

(1a) $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l$,

(1b) for all $i' \in \mathcal{I}'$ with $i' < i$ one of the following conditions holds:

- $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < l$,
- $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) \in \{l+1, \ldots, l+g\}$.

Assume next that $l+g+1 \leq n$. The set $\mathcal{I}'$ is said to have the relaxed μ-property with respect to $(l, l+g+1)$ with exception $\{l+1, \ldots, l+g\}$ if for all $i \in \mathcal{I}'$ there exists $j \in \mathcal{I}$ such that either conditions $(1a)$ and $(1b)$ above hold or

(2a) $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l+g+1$,

(2b) (i, j) is OWB with respect to $\mathcal{I}'$,

(2c) no $i' \in \mathcal{I}'$ with $i' < i$ satisfies $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) = l$.

From the discussion above we arrive at the following improvement to Theorem 7.

Theorem 19. *Consider a non-zero codeword $\vec{c}$ and let $l = m(\vec{c})$. Choose a non-negative integer v such that $l + v \leq n$. Assume that for some indexes $x \in \{l+1, \ldots, l+v\}$ we know a priori that $\vec{c}\cdot\vec{w}_x = 0$. Let $l'_1 < \cdots l'_s$ be the remaining indexes from $\{l+1, \ldots, l+v\}$. Consider the sets $\mathcal{I}'_0, \mathcal{I}'_1, \ldots, \mathcal{I}'_s$ such that:*

- *$\mathcal{I}'_0$ has the μ-property with respect to l with exception $\{l+1, \ldots, l+v\}$.*

- *For $i = 1, \ldots, s$, $\mathcal{I}'_i$ has the relaxed μ-property with respect to (l, l'_i) with exception $\{l+1, \ldots, l'_i - 1\}$.*

We have

$$w_H(\vec{c}) \geq \min\{\#\mathcal{I}'_0, \#\mathcal{I}'_1, \ldots, \#\mathcal{I}'_s\}. \tag{3.2}$$

To establish a lower bound on the minimum distance of a code C we repeat the above process for each $l \in m(C)$. For each such l we choose a corresponding v, we determine sets $\mathcal{I}'_i$ as above and we calculate the right side of (3.2). The smallest value found constitutes a lower bound on the minimum distance.

Remark 20. The results in Remark 8 also hold if we replace Theorem 7 with Theorem 19. We shall denote the resulting improved codes by $\widetilde{C}_{fim}(\delta)$ (here, *fim* stands for further improved).

Remark 21. Assume $\mathcal{I}'$ has the μ-property with respect to l. One possible choice of sets $\mathcal{I}'_0, \mathcal{I}'_1, \ldots, \mathcal{I}'_s \subseteq \mathcal{I}$ in Theorem 19 would be to choose all of them to be equal to $\mathcal{I}'$. It follows that Theorem 19 is indeed at least as strong as Theorem 7. The above observation relates to the fact that Theorem 19 reduces to Theorem 7 when v is chosen to be always equal to 0.

As shall be demonstrated later in the paper, Theorem 19 can sometimes be much better than Theorem 7. For Theorem 19 to be operational we need a clever method to choose for each $l \in m(C)$ the corresponding number v. As shall be clear form the examples in Section 4 for affine variety codes there is a very natural way to do this. Another remark is that when the task is to estimate the minimum distance of a fixed code, then we can set v equal to 0 for most values of l, reserving non-zero values to those l for which Theorem 7 produces the smallest numbers. These are the numbers that need to be improved.

In a similar way as Theorem 7 was enhanced to deal with generalized Hamming weighs and relative generalized Hamming weights we can enhance Theorem 19. The notation in Definition 18 being already involved we only illustrate how to deal with the second generalized Hamming weight. From that description it should be clear how to deal with higher weights.

Proposition 22. *Let the notation be as in Theorem 19. Consider a subspace $D \subseteq C$ of dimension 2, say $m(D) = \{a, b\}$. Let v_a be the v corresponding to $l = a$. Let $a'_1 < \cdots < a'_{s_a}$ be the numbers $l'_1 < \cdots < l'_s$ corresponding to $l = a$. Analogously for the case b. Referring to Definition 18, for $\alpha = 1, \ldots, s_a$ and $\beta = 1, \ldots, s_b$ we define subsets of $\mathcal{I}$ as follows:*

- *$\mathcal{I}''_{0,0}$ is a set such that for all $i \in \mathcal{I}''_{0,0}$ for an $l \in \{a, b\}$ a j exists such that (1a) and (1b) hold with $g = v_a$ if $l = a$, and $g = v_b$ if $l = b$.*
- *$\mathcal{I}''_{\alpha,0}$ is a set such that for all $i \in \mathcal{I}''_{\alpha,0}$ a j exists such that one of the following two conditions holds:*
  - *Either (1a), (1b) or (2a), (2b), (2c) hold with $l = a$, $g + 1 = a'_\alpha$.*
  - *(1a) and (1b) hold with $l = b$, $g = v_b$.*

- $\mathcal{I}''_{0,\beta}$ *is defined similarly to* $\mathcal{I}''_{\alpha,0}$.
- $\mathcal{I}''_{\alpha,\beta}$ *is a set such that for all* $i \in \mathcal{I}''_{\alpha,\beta}$ *an* $l \in \{a, b\}$ *and a* $j \in \mathcal{I}$ *exist such that either (1a), (1b) or (2a), (2b), (2c) hold. Here,* $g + 1 = a'_\alpha$ *if* $l = a$, *and* $g + 1 = b'_\beta$ *if* $l = b$.

The support of D *is of size at least equal to the smallest cardinality of the above sets. To establish a lower bound on the second generalized Hamming weight of a code* C *we repeat the above process for each* $(a, b) \in m(C) \times m(C)$ *with* $a < b$. *The smallest value found constitutes a lower bound on the second generalized Hamming weight.*

Applying in larger generality the method described in the above proposition we derive lower bounds on any generalized Hamming weights of C. It is clear that this method can be of much higher complexity than the method described in Theorem 16. To lower the complexity we choose (referring to the case of the second weight) most v_a and v_b equal to zero, reserving non-zero values to those (a, b) for which Theorem 16 produces low values. As shall be demonstrated in the following section, Proposition 22 and its generalization to higher weights can sometimes produce much better results than Theorem 16.

Similar results on the relative generalized Hamming weights as those mentioned at the end of Section 2 holds for the method described above.

Chapter 4

Examples

In this section we apply the advisory bound and the improved bound from Section 3 to affine variety codes coming from two particular curves. The first curve corresponds to [16, Sec. 3.1]. It is a plane curve over $\mathbb{F}_8$. The second curve is the natural counterpart for the field $\mathbb{F}_{27}$. We shall need a couple of results from Gröbner basis theory.

4.1 Some results from Gröbner basis theory

Let $\prec$ be a monomial ordering on the set of monomials in $X_1, \ldots, X_m$. Given an ideal $J \subseteq k[X_1, \ldots, X_m]$, where k is a field, the footprint $\Delta_\prec(J)$ is the set of monomials that can not be found as leading monomial of any polynomial in J. A Gröbner basis, by definition, is a generating set for J from which the footprint can be easily read. More formally, $\{L_1(X_1, \ldots, X_m), \ldots, L_s(X_1, \ldots, X_m)\} \subseteq J$ is a Gröbner basis for J with respect to $\prec$ if for any $F(X_1, \ldots, X_m) \in J$ for some $i \in \{1, \ldots, s\}$ we have $\mathrm{lm}(L_i) \mid \mathrm{lm}(F)$. Recall that $\{M + J \mid M \in \Delta_\prec(J)\}$ is a basis for the quotient ring $k[X_1, \ldots, X_m]/J$ as a vector space over k. In the following we shall assume that $k = \mathbb{F}_q$ and that J contains all the equations $X_1^q - X_1, \ldots, X_m^q - X_m$, in which case we write $J = I_q$. Thus the variety of I_q is finite. Let the variety be $\{P_1, \ldots, P_n\}$ and consider the evaluation map $\mathrm{ev} : \mathbb{F}_q[X_1, \ldots, X_m]/I_q \to \mathbb{F}_q^n$ given by $\mathrm{ev}(F + I_q) = (F(P_1), \ldots, F(P_n))$. It is well-known that this map is a vector space isomorphism implying that $n = \#\Delta_\prec(I_q)$ holds. If we embark the vector space $\mathbb{F}_q^n$ with a second binary operation, namely the component wise product from Definition 2 then it becomes an $\mathbb{F}_q$-algebra. It is not difficult to see that the map ev in this way becomes an isomorphism between $\mathbb{F}_q$-algebras. Hence, if we enumerate the elements of $\Delta_\prec(I_q) = \{M_1, \ldots, M_n\}$ according to $\prec$ and define $\mathcal{U} = \mathcal{V} = \mathcal{W} = \{\vec{b}_1 = \mathrm{ev}(M_1 + I_q), \ldots, \vec{b}_n = \mathrm{ev}(M_n + I_q)\}$ then we can translate information on the algebraic structure of $\mathbb{F}_q[X_1, \ldots, X_m]/I_q$ into information regarding the well-behaving properties as introduced in Definition 4, 6, 10, 18 and Proposition 22. We shall illustrate how to do this in the following.

Y^7	XY^7	X^2Y^7	X^3Y^7	14	17	20	23	21	26	30	32
Y^6	XY^6	X^2Y^6	X^3Y^6	12	15	18	21	17	23	28	31
Y^5	XY^5	X^2Y^5	X^3Y^5	10	13	16	19	13	19	25	29
Y^4	XY^4	X^2Y^4	X^3Y^4	8	11	14	17	9	15	22	27
Y^3	XY^3	X^2Y^3	X^3Y^3	6	9	12	15	6	11	18	24
Y^2	XY^2	X^2Y^2	X^3Y^2	4	7	10	13	4	8	14	20
Y	XY	X^2Y	X^3Y	2	5	8	11	2	5	10	16
1	X	X^2	X^3	0	3	6	9	1	3	7	12
Monomials in $\Delta_{\prec_w}$				Corresponding weights				Indexing of $\mathcal{W}$			

Figure 4.1: The construction of $\mathcal{W}$ from $\Delta_{\prec_w}(I)$.

4.2 Codes from a curve over $\mathbb{F}_8$

In [16, Sec. 3.1] Salazar et. al. considered curves of the form

$$F_8(X,Y) = G_8(X) - H_8(Y) \in \mathbb{F}_8[X,Y]$$

where $G_8(X)$ is a polynomial of degree 4 and $H_8(Y)$ is a polynomial of degree 6 both having the property that when evaluated in $\mathbb{F}_8$ they return values in $\mathbb{F}_2$. It is of no implication to the estimation of code parameters if we restrict to $G_8(X)$ being the trace polynomial X^4+X^2+X and if we choose $H_8(Y) = Y^6+Y^5+Y^3$. Consider the trace-polynomial corresponding to a general field extension. It is well-known that the preimages of all the elements in the ground field are of the same size. From this we conclude that the particular polynomial $F_8(X,Y) = G_8(X) - H_8(Y)$ under consideration has exactly $2^5 = 32$ zeros.

Let $I_8 = \langle F_8(X,Y), X^8 - X, Y^8 - Y\rangle \subseteq \mathbb{F}_8[X,Y]$. From the above discussion we know that the corresponding variety is of size 32. If we consider a monomial ordering such that $\mathrm{lm}(F_8) = X^4$ then there exist exactly 32 monomials which are not divisible by any of the monomials $\mathrm{lm}(F_8) = X^4, \mathrm{lm}(Y^8 - Y) = Y^8$. Hence, $\{F_8(X,Y), Y^8 - Y\}$ is a Gröbner basis for I_8 and $\Delta_{\prec}(I_8) = \{X^\alpha Y^\beta \mid 0 \leq \alpha < 4, 0 \leq \beta < 8\}$ holds. In the following we consider a particular weighted degree lexicographic ordering for which $\mathrm{lm}(F_8) = X^4$ holds. Let $w(X) = 3$, $w(Y) = 2$, and in general $w(X^\alpha Y^\beta) = 3\alpha + 2\beta$. We define $\prec_w$ to be the monomial ordering given by $X^{\alpha_1}Y^{\beta_1} \prec_w X^{\alpha_2}Y^{\beta_2}$ if either $w(X^{\alpha_1}Y^{\beta_1}) < w(X^{\alpha_2}Y^{\beta_2})$ or if alternatively $w(X^{\alpha_1}Y^{\beta_1}) = w(X^{\alpha_2}Y^{\beta_2})$ and $\alpha_1 < \alpha_2$ hold.

Let $\Delta_{\prec_w}(I_8) = \{M_1, \ldots, M_{32}\}$, the monomials being enumerated with respect to $\prec_w$. For the code construction we consider the basis

$$\mathcal{W} = \{\vec{w}_1 = \mathrm{ev}(M_1 + I_8), \ldots, \vec{w}_{32} = \mathrm{ev}(M_{32} + I_8)\}.$$

The situation is described in Figure 4.1. We then set $\vec{u}_i = \vec{v}_i = \vec{w}_i$ for $i = 1, \ldots, 32$ defining the bases $\mathcal{U}$ and $\mathcal{V}$.

By definition, $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l$ if and only if

$$\mathrm{lm}(M_i M_j \text{ rem } \{F_8(X,Y), X^8 - X, Y^8 - Y\}) = M_l.$$

Further, (i,j) is WB if and only if

$$\mathrm{lm}(M_{i'}M_{j'} \text{ rem } \{F_8(X,Y), X^8 - X, Y^8 - Y\}) \prec_w M_l \tag{4.1}$$

holds for all $i' \leq i$ and $j' \leq j$ with $(i',j') \neq (i,j)$. There are two particular easy cases to analyze:

- **Rule (I):** If $M_iM_j = M_l$ then by the property of a monomial ordering (4.1) holds.
- **Rule (II):** If $w(M_i) + w(M_j) = w(M_l)$ and $w(M_{i'}) < w(M_i)$ for all $i' < i$ and if $w(M_{j'}) < w(M_j)$ for all $j' < j$, then (4.1) holds.

In a straightforward manner one derives similar rules regarding WWB and OWB.

Consider $l = 17$. Using Rule (I) we see that every

$$(i,j) \in \{(1,17),(2,13),(4,9),(6,6),(9,4),(13,2),(17,1)\}$$

is WB with $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = 17$.
We have $\bar{\rho}_{\mathcal{W}}(\vec{u}_3 * \vec{v}_{12}) = 17$ as

$$\begin{aligned} & \mathrm{lm}(M_3M_{12} \text{ rem } \{F_8(X,Y), X^8 - X, Y^8 - Y\}) \\ = \; & \mathrm{lm}(X^4 \text{ rem } \{F_8(X,Y), X^8 - X, Y^8 - Y\}) \\ = \; & \mathrm{lm}(Y^6 + Y^5 + X^2 + Y^3 + X) = Y^6 = M_{17}. \end{aligned}$$

But $M_3M_{11} = M_{18}$ implying that $\bar{\rho}_{\mathcal{W}}(\vec{u}_3 * \vec{v}_{11}) = 18$. Therefore $(3,12)$ is not WWB. However $w(M_{i'}) < w(M_3)$ for all $i' < 3$ and by a result similar to Rule (II), $(3,12)$ therefore is OWB.
We next claim that $\mathcal{I}' = \{1,2,4,6,9,13,17,3,12\}$ has the μ-property with respect to 17. To this end, the only thing missing to be checked is the case $i = 12$. Clearly, $\bar{\rho}_{\mathcal{W}}(\vec{u}_{12} * \vec{v}_3) = 17$. Note that $w(M_{12}) = 9$ does not belong to $\{w(M_i) \mid i \in \mathcal{I}' \backslash \{12\}\}$ and by an argument similar to Rule (II) we conclude that $(12,3)$ is OWB with respect to $\mathcal{I}'$.

We next apply Theorem 19 with $l = 17$ and $v = 1$. Observe that $w(M_{17}) = w(M_{18}) < w(M_{19})$ which is what makes the choice $v = 1$ natural. Using similar arguments as above we see that

$$\mathcal{I}'_0 = \{1,2,4,6,9,13,17,3,12\} \cup \{7\}$$

has the μ-property with respect to 17 with exception $\{18\}$ and that

$$\mathcal{I}'_1 = \{1,2,4,6,9,13,17\} \cup \{3,5,8,11\}$$

has the relaxed μ-property with respect to $(17,18)$ with exception $\{\}$. Clearly, $\mathcal{I}'_0$ is the smallest of these two sets.

In conclusion, if $m(\vec{c}) = 17$ we get the following estimates:

- The Feng-Rao bound in the version with WB or WWB produces $w_H(\vec{c}) \geq 7$.
- The same bound in the version with OWB gives $w_H(\vec{c}) \geq 8$.

	Feng-Rao WB	Feng-Rao WWB	Feng-Rao OWB	Advisory bound	Section 3
d_1	7	7	8	9	10
d_2	8	8	10	12	13

Table 4.1: Estimates on first and second generalized Hamming weight of the code $C(16)$ over $\mathbb{F}_8$.

- From the advisory bound we get $w_H(\vec{c}) \geq 9$.
- Finally, our new bound produces $w_H(\vec{c}) \geq 10$.

Applying exactly the same techniques as above we get the following estimates of $w_H(\vec{c})$ when $m(\vec{c}) = 21$:

- The Feng-Rao bound with WB or WWB gives $w_H(\vec{c}) \geq 8$.
- The same bound in the version with OWB produces $w_H(\vec{c}) \geq 10$.
- From the advisory bound we get $w_H(\vec{c}) \geq 12$ (This is done by choosing $\mathcal{I}' = \{1, 2, 4, 6, 9, 13, 17, 21\} \cup \{3, 5, 12, 16\}$).
- Finally, our new bound produces $w_H(\vec{c}) \geq 13$ (This is done by choosing $v = 1$, $\mathcal{I}'_0 = \{1, 2, 4, 6, 9, 13, 17, 21\} \cup \{3, 7, 12, 5, 10, 16\}$ and finally $\mathcal{I}'_1 = \{1, 2, 4, 6, 9, 13, 17, 21\} \cup \{3, 5, 8, 11, 15\}$).

For the remaining choices of $l \in \mathcal{I}$ neither the advisory bound nor the improved bound from the present paper produces better results than the Feng-Rao bound with WWB. By [16], for $m(\vec{c}) = 28$ and $m(\vec{c}) = 30$, respectively, the Feng-Rao bound with WWB improves upon the same bound with WB by lifting the estimates from 21 to 22 and from 24 to 26, respectively.

We first consider the codes $C(s)$ (See Remark 8 for the definition). In Figure 4.2 we illustrate the parameters k, $d_1(C(s)), \ldots, d_5(C(s))$. As is seen, for all of the five choices of bounds: the Feng-Rao bound with WB, WWB, OWB, the advisory bound, and the bound from Section 3, there exist numbers i and s such that the best estimate on $d_i(C(s))$ is obtained by this particular bound (and consequently also by the sharper bounds as well). Regarding the 6th generalized Hamming weight, only for one s we can improve upon what is derived from the Feng-Rao bound with WB. Namely, for $C(4)$ where the Feng-Rao bound with WB or WWB produces the estimate 8 whereas all other bounds give 9. In Table 4.1 we illustrate that the various bounds sometimes improve very much on each other by showing estimates for the first two weights of the code $C(16)$. For this particular code for higher weights all estimates are the same.

We next consider the improved codes $\widetilde{C}_{adv}(\delta)$ and $\widetilde{C}_{fim}(\delta)$ (See Remark 8 and Remark 20 for the definitions). For two designed distances $\delta = 10, 13$, the code $\widetilde{C}_{fim}(\delta)$ is of higher dimension than $\widetilde{C}_{adv}(\delta)$. In Table 4.2 we list estimates from the

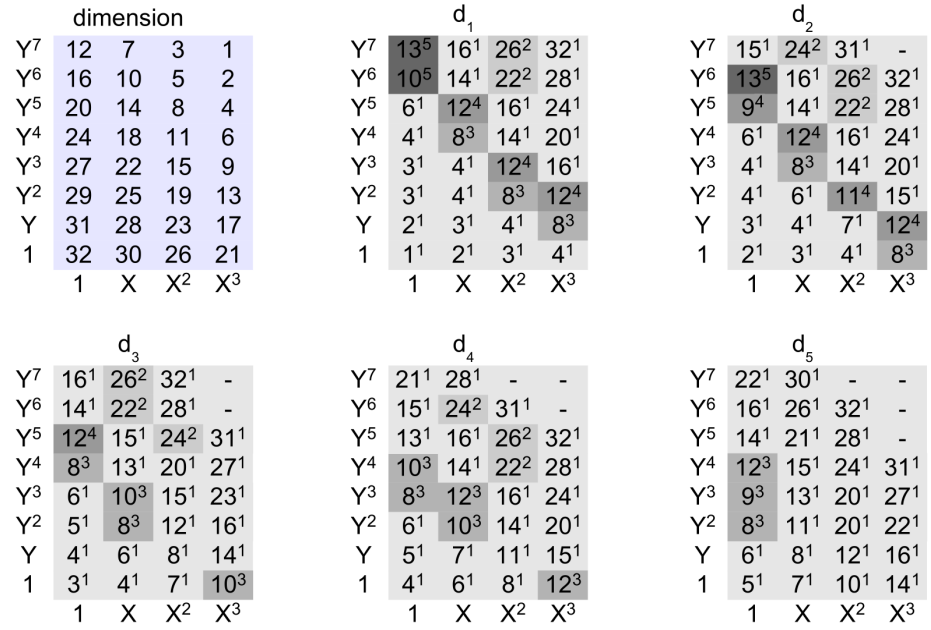

Figure 4.2: The figure lists the dimensions of codes $C(s)$ over $\mathbb{F}_8$ and corresponding estimates on $d_1, \ldots, d_5$. Information about $C(s)$ is placed at the position of $\vec{w}_{s+1}$. An entry z^1 means that the value z was obtained from the Feng-Rao bound with WB, z^2 indicate that the same bound with WWB was used, and finally z^3 the same bound with OWB. With z^4 we indicate that the value z was obtained from the advisory bound and by z^5 that the method from Section 3 was used. The symbol - inside the table indicates that the corresponding parameter does not exist.

	k	d_2	d_3	d_4	d_5	d_6
$\widetilde{C}_{adv}(10)$	16	12	14	15	16	20
$\widetilde{C}_{fim}(10)$	17	12	13	14	15	16
$\widetilde{C}_{adv}(13)$	11	16	20	22	24	26
$\widetilde{C}_{fim}(13)$	12	15	16	21	22	24

Table 4.2: Parameters of improved codes over $\mathbb{F}_8$. By definition, the codes $\widetilde{C}_{adv}(10)$ and $\widetilde{C}_{fim}(10)$ are of designed minimum distance 10. Similarly, $\widetilde{C}_{adv}(13)$ and $\widetilde{C}_{fim}(13)$, are of designed minimum distance 13. By k we denote the dimension. The values of $d_2, \ldots, d_6$ for $\widetilde{C}_{adv}(10)$ and $\widetilde{C}_{adv}(13)$ are estimated using the advisory bound. For $\widetilde{C}_{fim}(10)$ and $\widetilde{C}_{fim}(13)$ the method from Section 3 is used.

advisory bound on the generalized Hamming weights of the first code and estimates from the bound of Section 3 on the generalized Hamming weights of the latter code, respectively. We see that for higher generalized Hamming weights there is a price to be paid for the increase in dimension.

4.3 Codes from a curve over $\mathbb{F}_{27}$

Similarly to the curve $F_8(X,Y) \in \mathbb{F}_8[X,Y]$ from the previous section we now consider the curve $F_{27}(X,Y) = G_{27}(X) - H_{27}(Y) \in \mathbb{F}_{27}[X,Y]$. Here, $G_{27}(X)$ is the trace-polynomial $X^9 + X^3 + X$ and $H_{27}(Y) = Y^{12} + Y^{10} + Y^4$ satisfies that when evaluated in elements from $\mathbb{F}_{27}$ it returns values from $\mathbb{F}_3$. The arguments of the previous subsection translate immediately. Only difference is that now instead of having many pairs of monomials in the footprint being of the same weight we now have many triples of monomials in the footprint being of the same weight. The implication is that when applying Theorem 19 we will often need $v = 2$ rather than $v = 1$. The codes being of length $n = 3^5 = 243$ we cannot give many details, but restrict to consider the minimum distance and the second generalized Hamming weight of the codes $C(s)$. See Figure 4.3. Again, all five bounds come into action.

To illustrate how much the advisory bound and the bound of Section 3 improve upon the various versions of the Feng-Rao bound we treat in detail the codes $C(75)$, $C(76)$, $C(83)$ in Table 4.3. These codes are of dimension 168, 167 and 160.

dimension

Y^{26}	54	43	33	24	17	11	6	3	1
Y^{25}	63	51	40	30	22	15	9	5	2
Y^{24}	72	60	48	37	28	20	13	8	4
Y^{23}	81	69	57	45	35	26	18	12	7
Y^{22}	90	78	66	53	42	32	23	16	10
Y^{21}	99	87	75	62	50	39	29	21	14
Y^{20}	108	96	84	71	59	47	36	27	19
Y^{19}	117	105	93	80	68	56	44	34	25
Y^{18}	126	114	102	89	77	65	52	41	31
Y^{17}	135	123	111	98	86	74	61	49	38
Y^{16}	144	132	120	107	95	83	70	58	46
Y^{15}	153	141	129	116	104	92	79	67	55
Y^{14}	162	150	138	125	113	101	88	76	64
Y^{13}	171	159	147	135	122	110	97	85	73
Y^{12}	180	168	156	143	131	119	106	94	82
Y^{11}	189	177	165	152	140	128	115	103	91
Y^{10}	198	186	174	161	149	137	124	112	100
Y^{9}	206	195	183	170	158	146	133	121	109
Y^{8}	213	203	192	179	167	155	142	130	118
Y^{7}	219	210	200	188	176	164	151	139	127
Y^{6}	225	217	208	197	185	173	160	148	136
Y^{5}	230	223	215	205	194	182	169	157	145
Y^{4}	234	228	221	212	202	191	178	166	154
Y^{3}	237	232	226	218	209	199	187	175	163
Y^{2}	240	236	231	224	216	207	196	184	172
Y	242	239	235	229	222	214	204	193	181
1	243	241	238	233	227	220	211	201	190
	1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8

d_1

Y^{26}	73^4	77^4	81^1	138^3	150^3	162^1	219^2	231^2	243^1
Y^{25}	70^4	74^4	78^1	132^3	144^3	156^1	210^2	222^2	234^1
Y^{24}	67^4	71^4	75^4	81^1	138^3	150^3	162^1	213^2	225^2
Y^{23}	64^4	68^4	72^4	77^4	87^1	138^3	150^3	162^1	216^2
Y^{22}	61^4	65^4	69^4	74^4	78^1	132^3	144^3	156^3	207^2
Y^{21}	58^4	62^4	66^4	71^4	75^4	81^1	138^3	150^3	162^1
Y^{20}	55^4	59^4	63^4	68^4	72^4	77^4	81^1	138^3	150^3
Y^{19}	52^4	56^4	60^4	65^4	69^4	73^4	77^4	81^1	138^3
Y^{18}	49^4	53^4	57^4	62^4	66^4	70^4	74^4	78^1	132^3
Y^{17}	46^4	50^4	54^4	59^4	63^4	67^4	71^4	75^4	81^1
Y^{16}	43^4	47^4	51^4	56^4	60^4	64^4	68^4	72^4	77^4
Y^{15}	40^5	44^4	48^4	53^4	57^4	61^4	65^4	69^4	73^4
Y^{14}	37^5	41^5	45^4	50^4	54^4	58^4	62^4	66^4	70^4
Y^{13}	30^5	38^5	42^4	47^4	51^4	55^4	59^4	63^4	67^4
Y^{12}	21^5	33^5	39^4	44^4	48^4	52^4	56^4	60^4	64^4
Y^{11}	12^1	24^4	36^5	41^5	45^4	49^4	53^4	57^4	61^4
Y^{10}	9^1	18^4	27^5	38^5	42^4	46^4	50^4	54^4	58^4
Y^{9}	8^1	9^1	18^4	33^5	39^4	43^4	47^4	51^4	55^4
Y^{8}	7^1	8^1	9^1	24^4	36^5	40^5	44^4	48^4	52^4
Y^{7}	7^1	8^1	9^1	18^4	27^5	36^5	41^5	45^4	49^4
Y^{6}	6^1	7^1	8^1	9^1	18^4	27^5	38^5	42^4	46^4
Y^{5}	5^1	6^1	7^1	8^1	9^1	18^4	33^5	39^5	43^4
Y^{4}	4^1	5^1	6^1	7^1	8^1	9^1	24^4	36^5	40^5
Y^{3}	4^1	5^1	6^1	7^1	8^1	9^1	18^4	27^5	36^5
Y^{2}	3^1	4^1	5^1	6^1	7^1	8^1	9^1	18^4	27^5
Y	2^1	3^1	4^1	5^1	6^1	7^1	8^1	9^1	18^4
1	1^1	2^1	3^1	4^1	5^1	6^1	7^1	8^1	9^1
	1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8

d_2

Y^{26}	76^4	80^1	135^3	149^3	161^1	216^2	230^2	242^1	-
Y^{25}	73^4	77^4	81^1	138^3	150^3	162^1	219^2	231^2	243^1
Y^{24}	70^4	74^4	78^1	132^3	144^3	156^1	210^2	222^2	234^1
Y^{23}	67^4	71^4	75^4	80^1	135^3	149^3	161^1	213^2	225^2
Y^{22}	64^4	68^4	72^4	77^4	81^1	138^3	150^3	162^1	216^2
Y^{21}	61^4	65^4	69^4	74^4	78^1	132^3	144^3	156^1	207^2
Y^{20}	58^4	62^4	66^4	71^4	75^4	80^1	135^3	149^3	161^1
Y^{19}	55^4	59^4	63^4	68^4	72^4	76^4	80^1	135^3	149^3
Y^{18}	52^4	56^4	60^4	65^4	69^4	73^4	77^4	81^1	138^3
Y^{17}	49^4	53^4	57^4	62^4	66^4	70^4	74^4	78^1	132^3
Y^{16}	46^4	50^4	54^4	59^4	63^4	67^4	71^4	75^4	80^1
Y^{15}	43^4	47^4	51^4	56^4	60^4	64^4	68^4	72^4	76^4
Y^{14}	40^5	44^4	48^4	53^4	57^4	61^4	65^4	69^4	73^4
Y^{13}	37^5	41^5	45^4	50^4	54^4	58^4	62^4	66^4	70^4
Y^{12}	30^5	38^5	42^4	47^4	51^4	55^4	59^4	63^4	67^4
Y^{11}	21^5	33^5	39^5	44^4	48^4	52^4	56^4	60^4	64^4
Y^{10}	12^1	24^4	36^5	41^5	45^4	49^4	53^4	57^4	61^4
Y^{9}	9^1	17^4	27^5	38^5	42^4	46^4	50^4	54^4	58^4
Y^{8}	8^1	9^1	18^4	33^5	39^5	43^4	47^4	51^4	55^4
Y^{7}	8^1	9^1	12^1	24^4	35^5	40^5	44^4	48^4	52^4
Y^{6}	7^1	8^1	9^1	17^4	26^4	36^5	41^5	45^4	49^4
Y^{5}	6^1	7^1	8^1	9^1	17^4	27^5	38^5	42^4	46^4
Y^{4}	5^1	6^1	7^1	8^1	9^1	18^4	33^5	39^5	43^4
Y^{3}	5^1	6^1	7^1	8^1	9^1	12^1	24^4	35^5	40^5
Y^{2}	4^1	5^1	6^1	7^1	8^1	9^1	17^4	26^4	36^5
Y	3^1	4^1	5^1	6^1	7^1	8^1	9^1	17^4	27^5
1	2^1	3^1	4^1	5^1	6^1	7^1	8^1	9^1	18^4
	1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8

Figure 4.3: Dimensions, minimum distance and second generalized Hamming weight of codes $C(s)$ over $\mathbb{F}_{27}$. Notation as in Figure 4.2

	Feng-Rao WB	Feng-Rao WWB	Feng-Rao OWB	Advisory bound	Section 3
$d_1(C(75))$	15	15	21	29	33
$d_2(C(75))$	16	16	24	34	38
$d_1(C(76))$	15	15	21	33	36
$d_2(C(76))$	16	16	24	38	39
$d_1(C(83))$	16	16	24	34	38
$d_2(C(83))$	17	17	27	39	41

Table 4.3: Estimates of minimum distance and second generalized Hamming weight for a selection of codes over $\mathbb{F}_{27}$.

Chapter 5

Concluding remarks

In this paper we treated two improvements to the Feng-Rao bound for dual codes: the advisory bound and a new bound which is an improvement to it. The latter bound is closely related to a new bound for primary codes which we treat in a separate paper [5]. Part of this research was done while the second listed author was visiting East China Normal University. We are grateful to Professor Hao Chen for his hospitality. The authors also gratefully acknowledge the support from the Danish National Research Foundation and the National Science Foundation of China (Grant No. 11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography.

Bibliography

[1] H.E. Andersen, O. Geil, Evaluation codes from order domain theory, Finite Fields Appl. 14 (2008) 92–123.

[2] G.L. Feng, T.R.N. Rao, A simple approach for construction of algebraic-geometric codes from affine plane curves, IEEE Trans. Inform. Theory 40 (1994) 1003–1012.

[3] G.L. Feng, T.R.N. Rao, Improved geometric Goppa codes part I: Basic theory, IEEE Trans. Inform. Theory 41 (1995) 1678–1693.

[4] J. Fitzgerald, R.F. Lax, Decoding affine variety codes using Gröbner bases, Des. Codes Cryptogr. 13 (1998) 147–158.

[5] O. Geil, S. Martin, An improvement of the Feng-Rao bound for primary codes, arXiv:1307.3107 (2013)

[6] O. Geil, R. Pellikaan, On the structure of order domains, Finite Fields Appl. 8 (2002) 369–396.

[7] O. Geil, C. Thommesen, On the Feng-Rao bound for generalized Hamming weights, in: M.P. Fossorier, H. Imai, S. Lin, A. Poli (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, volume 3857 of *Lecture Notes in Computer Science*, Springer, 2006, pp. 295–306.

[8] P. Heijnen, R. Pellikaan, Generalized Hamming weights of q-ary Reed-Muller codes, IEEE Trans. Inform. Theory 44 (1998) 181–196.

[9] T. Høholdt, J.H. van Lint, R. Pellikaan, Algebraic geometry codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, volume 1, Elsevier, Amsterdam, 1998, pp. 871–961.

[10] J. Kurihara, T. Uyematsu, R. Matsumoto, Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized hamming weight, IEICE Trans. Fundamentals E95-A (2012) 2067–2075.

[11] Z. Liu, W. Chen, Y. Luo, The relative generalized Hamming weight of linear q-ary codes and their subcodes, Des. Codes Cryptogr. 48 (2008) 111–123.

[12] Y. Luo, C. Mitrpant, A. Vinck, K. Chen, Some new characters on the wire-tap channel of type ii, IEEE Trans. Inform. Theory 51 (2005) 1222–1229.

[13] R. Matsumoto, S. Miura, On the Feng-Rao bound for the $\mathcal{L}$-construction of algebraic geometry codes, IEICE Trans. Fundamentals E83-A (2000) 926–930.

[14] S. Miura, Study of Error-Correcting Codes based on Algebraic Geometry, Ph.D. thesis, Univ. Tokyo, 1997. (in Japanese).

[15] R. Pellikaan, On the efficient decoding of algebraic-geometric codes, in: P. Camion, P. Charpin, S. Harari (Eds.), Eurocode '92 International Symposium on Coding Theory and Applications, number 339 in CISM Courses and Lectures, CISM International Centre for Mechanical Sciences, Springer, 1993, pp. 231–253.

[16] G. Salazar, D. Dunn, S.B. Graham, An improvement of the Feng-Rao bound on minimum distance, Finite Fields Appl. 12 (2006) 313–335.

[17] V. Wei, Generalized hamming weights for linear codes, IEEE Trans. Inform. Theory 37 (1991) 1412–1418.

PAPER IV

Relative generalized Hamming weights of one-point algebraic geometric codes

Geil Olav Martin Stefano Matsumoto Ryutaroh
Ruano Diego Luo Yuan

Geil Olav, Martin Stefano, Matsumoto Ryutaroh, Ruano Diego and Luo Yuan, "Relative generalized Hamming weights of one-point algebraic geometric codes", *submitted*, 2014, preprint at arXiv: 1403.7985v3 [cs.IT], DOI: 10.1109/TIT.2014.2345375

Relative generalized Hamming weights of one-point algebraic geometric codes[1]

Olav Geil[21], Stefano Martin[31], Ryutaroh Matsumoto, *Member, IEEE*[42], Diego Ruano[51] and Yuan Luo, *Member, IEEE*[63]

[1]Department of Mathematical Sciences, Aalborg University
[2]Department of Communications and Computer Engineering, Tokyo Institute of Technology, Japan
[3]Computer Science and Engineering Department, Shanghai Jiao Tong University, China

[1]The results in this paper will in part be presented at IEEE Information Theory Workshop (ITW 2014) [16]. This research is supported by the Danish National Research Foundation, the National Natural Science Foundation of China (Grant No. 11061130539 – the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography), Japan Society for the Promotion of Science (Grant Nos. 23246071 and 26289116), the Danish Council for Independent Research (Grant No. DFF–4002-00367), the Spanish MINECO (Grant No. MTM2012-36917-C03-03), National Basic Research Program of China (Grant No. 2013CB338004), and National Natural Science Foundation of China (Grant No. 61271222).

[2]olav@math.aau.dk
[3]stefano@math.aau.dk
[4]ryutaroh@rmatsumoto.org
[5]diego@math.aau.dk
[6]yuanluo@sjtu.edu.cn

Abstract

Security of linear ramp secret sharing schemes can be characterized by the relative generalized Hamming weights of the involved codes [30, 28]. In this paper we elaborate on the implication of these parameters and we devise a method to estimate their value for general one-point algebraic geometric codes. As it is demonstrated, for Hermitian codes our bound is often tight. Furthermore, for these codes the relative generalized Hamming weights are often much larger than the corresponding generalized Hamming weights.

Keywords: linear code, Feng-Rao bound, Hermitian code, one-point algebraic geometric code, relative dimension/length profile, relative generalized Hamming weight, secret sharing, wiretap channel of type II.

Chapter 1

Introduction

A secret sharing scheme is a cryptographic method to encode a secret into multiple shares later distributed to participants, so that only specified sets of participants can reconstruct the secret. The first secret sharing scheme was proposed by Shamir [39]. It was a perfect scheme, in which a set of participants unable to reconstruct the secret has absolutely no information on the secret. Later, non-perfect secret sharing schemes were proposed [4, 46] in which there are sets of participants that have non-zero amount of information about the secret but cannot reconstruct it. The term ramp secret sharing scheme is sometimes used for the latter mentioned type of schemes, sometimes for the union of the two types. In this paper we will apply the most general definition, but concentrate our investigation on non-perfect secret sharing schemes. Secret sharing has been used, for example, to store confidential information to multiple locations geographically apart. By using secret sharing schemes in such a scenario, the likelihoods of both data loss and data theft are decreased. As far as we know, in many applications both perfect and non-perfect ramp secret sharing schemes can be used. In the perfect scheme, the size of a share must be at least that of the secret [5]. On the other hand, ramp secret sharing schemes allow shares to be smaller than the secret, which is what we concentrate on in this paper. Such schemes are particularly useful for storing bulk data [7].

A linear ramp secret sharing scheme can be described as a coset construction C_1/C_2 where $C_2 \subsetneq C_1$ are linear codes [6]. It was shown in [2, 28, 41] that the corresponding relative dimension/length profile (RDLP) expresses the worst case information leakage to unauthorized sets in such a system. The RDLP was proposed by Luo et al. [30]. They [30] also proposed the relative generalized Hamming weight (RGHW) and its equivalence to the RDLP, similar to the one demonstrated by Forney [13] between the dimension/length profile and the generalized Hamming weight. The m-th RGHW expresses the smallest size of unauthorized sets that can obtain m q-bits [2, 28], where q is the size of the alphabet of $C_2 \subsetneq C_1$. In order to investigate the potential of linear codes to construct useful ramp secret sharing schemes, it is indispensable to study the RGHW and the RDLP. However,

not much research has been done so far, partly because the connection between the secret sharing and RGHW/RDLP was only recently reported. In particular, few classes of linear codes have been examined for their RGHW/RDLP. In this paper we study the RGHW of general linear codes by the Feng-Rao approach [17], and explore its consequences for one-point algebraic geometry (AG) codes [43, 22] and, in particular the Hermitian codes [42, 40, 47].

The present paper starts with a discussion of known results regarding linear ramp secret sharing schemes and it continues with demonstrating that the RGHWs can also be used to express the best case information leakage. The main result of the paper is a method to estimate RGHW of one-point algebraic geometric codes. This is done by carefully applying the Feng-Rao bounds [17] for primary [1] as well as dual [11, 12, 37, 22, 32, 21] codes. From this we derive a relatively simple bound which uses information on the corresponding Weierstrass semigroup [24, 8]. As shall be demonstrated for Hermitian codes the new bound is often sharp. Moreover, for the same codes the RGHW are often much larger than the corresponding generalized Hamming weights (GHW) [44] which means that studies of RGHW cannot be substituted by those of GHW.

The paper is organized as follows. Section 2 describes the use of RGHW in connection with linear ramp secret sharing schemes, and in connection with communication over the wiretap channel of type II. In Section 3 we apply the theory to the special case of MDS codes. In Section 4 we show – at the level of general linear codes – how to employ the Feng-Rao bounds to estimate RGHW. This method is then applied to one-point algebraic geometric codes in Section 5. We investigate Hermitian codes in Section 6, and treat the corresponding ramp secret sharing schemes in Section 7.

Chapter 2

Ramp secret sharing schemes and wiretap channels of type II

Ramp secret sharing schemes were introduced in [4, 46]. Let $\mathbb{F}_q$ be the finite field with q elements. A ramp secret sharing scheme with t-privacy and r-reconstruction is an algorithm that, given an input $\vec{s} \in \mathbb{F}_q^\ell$, outputs a vector $\vec{x} \in \mathbb{F}_q^n$, the vector of shares that we want to share among n players, such that, given a collection of shares $\{x_i \mid i \in \mathcal{I}\}$ where $\mathcal{I} \subseteq \{1, \ldots, n\}$, one has no information about $\vec{s}$ if $\#\mathcal{I} \leq t$ and one can recover $\vec{s}$ if $\#\mathcal{I} \geq r$ [6]. We shall always assume that t is largest possible and that r is smallest possible such that the above hold. We say that one has a t-threshold secret sharing scheme if $t = r + 1$.

We consider the secret sharing schemes introduced in [6, Section 4.2], which was the first general construction of ramp secret sharing schemes using arbitrary linear codes: Let $C_2 \subsetneq C_1 \subseteq \mathbb{F}_q^n$ be two linear codes. Set $k_2 = \dim(C_2)$ and $k_1 = \dim(C_1)$ and let $L \subsetneq \mathbb{F}_q^n$ be such that $C_1 = L \oplus C_2$ (direct sum). That is, $L \cap C_2 = \{\vec{0}\}$ and the union of a basis for L and a basis for C_2 constitutes a basis for C_1. We denote by $\ell = \dim(L) = \dim(C_1/C_2) = k_1 - k_2$.

We consider a secret $\vec{s} \in \mathbb{F}_q^\ell$; note that $\ell > 0$ since $C_1 \neq C_2$. We fix a vector space isomorphism $\psi : \mathbb{F}_q^\ell \to L$ which maps the secret $\vec{s} \in \mathbb{F}_q^\ell$ to L, and choose $\vec{c}_2 \in C_2$ randomly (uniformly distributed). Finally, consider $\vec{x} = \psi(\vec{s}) + \vec{c}_2 \in C_1$. The n shares consist of the n coordinates of $\vec{x}$; this scheme is clearly $\mathbb{F}_q$-linear [6]. One may also consider that the secret $\vec{s}$ is represented by the coset $\psi(\vec{s}) + C_2$ in C_1/C_2. Note that there are q^ℓ different cosets in C_1/C_2 and there are q^{k_2} possible representatives for every coset, i.e. for generating the shares of a secret $\vec{s}$. The schemes in [9, 31] form a particular case of the above scheme with $\ell = 1$.

Remark 1. *All linear ramp secret sharing schemes with shares in $\mathbb{F}_q$ are of the above type. For constructions that use puncturing [31], [6, Sec. 4.1] we can take C_1, C_2 to be the punctured codes.*

Let $\mathcal{I} \subseteq \mathcal{J} = \{1, \ldots, n\}$. We consider that an unauthorized set of participants obtains the shares $\{x_i \mid i \in \mathcal{I}\}$. We represent the shares by a random variable $\vec{X}$, and the shares obtained by an unauthorized set of participants by $f_{\mathcal{I}}(\vec{x}) = (x_i \mid i \in \mathcal{I})$ where $f_{\mathcal{I}} : \mathbb{F}_q^n \to \mathbb{F}_q^{\#\mathcal{I}}$. The amount of information in q-bits that the unauthorized set obtains is measured by $I(\vec{S}; f_{\mathcal{I}}(\vec{X}))$, the mutual information, where $\vec{S}$ is the random variable that represents the secrets, and $f_{\mathcal{I}}(\vec{X})$ is the random variable that represents the shares that an unauthorized set may obtain. We assume that both $\vec{S}$ and $\vec{X}$ are uniformly distributed. In particular we have t-privacy and r-reconstruction if t is largest possible and r is smallest possible such that $I(\vec{S}; f_{\mathcal{I}}(\vec{X})) = 0$ for all $\#\mathcal{I} \leq t$ and $I(\vec{S}; f_{\mathcal{I}}(\vec{X})) = \ell$ for all $\#\mathcal{I} \geq r$. A (non sharp) bound for r and t was given in [6]: $r < n - d(C_1)$ and $t > d(C_2^\perp)$ where $d(C_i)$ denotes the minimum distance of C_i, for $i = 1, 2$. The exact values can be derived from [28, Proof of Theorem 4] as

$$\begin{aligned} I(\vec{S}; f_{\mathcal{I}}(\vec{X})) &= \ell - \dim((V_{\overline{\mathcal{I}}} \cap C_1)/(V_{\overline{\mathcal{I}}} \cap C_2)), & (2.1) \\ &= \dim((C_2^\perp \cap V_{\mathcal{I}})/(C_1^\perp \cap V_{\mathcal{I}})), & (2.2) \end{aligned}$$

where $\overline{\mathcal{I}} = \mathcal{J} \setminus I$ and $V_{\mathcal{I}} = \{\vec{x} \in \mathbb{F}_q^n \mid x_i = 0 \text{ for all } i \notin \mathcal{I}\}$.

For the convenience of the reader we include the computation of the previous mutual information: since the variables $\vec{S}$ and $\vec{X}$ are uniformly distributed one has that $H_q(f_{\mathcal{I}}(\vec{X})) = \log_q \#f_{\mathcal{I}}(C_1) = \dim(f_{\mathcal{I}}(C_1)) = k_1 - \dim(\ker(f_{\mathcal{I}}) \cap C_1)$, and $H_q(f_{\mathcal{I}}(\vec{X})|S) = \log_q \#f_{\mathcal{I}}(C_2) = \dim(f_{\mathcal{I}}(C_2)) = k_2 - \dim(\ker(f_{\mathcal{I}}) \cap C_2)$. Here, H_q is the entropy function to base q. Therefore $I(\vec{S}; f_{\mathcal{I}}(\vec{X})) = k_1 - k_2 - \big(\dim(\ker(f_{\mathcal{I}}) \cap C_1) - \dim(\ker(f_{\mathcal{I}}) \cap C_2)\big)$ and we obtain equation (2.1). Equation (2.2) follows from (2.1) and an extension of Forney's second duality lemma [27, Lemma 25]: Let $V \subseteq \mathbb{F}_q^n$, then

$$\begin{aligned} & \dim((C_2^\perp \cap V^\perp)/(C_1^\perp \cap V^\perp)) \\ = \; & \dim(C_1/C_2) - \dim((C_1 \cap V)/(C_2 \cap V)). \end{aligned}$$

In order to characterize the security of secret sharing schemes, one considers the jth relative dimension/length profile (RDLP) of two codes $C_2 \subsetneq C_1$ with $j \in \{1, \ldots, n\}$ [30]:

$$K_j(C_1, C_2) = \max_{\mathcal{I} \subseteq \mathcal{J}, \#\mathcal{I} = j} \dim((C_1 \cap V_{\mathcal{I}})/(C_2 \cap V_{\mathcal{I}})),$$

and the mth relative generalized Hamming weight (RGHW) with $m \in \{1, \ldots, \ell\}$ [30]:

$$M_m(C_1, C_2) = \min_{\mathcal{I} \subseteq \mathcal{J}} \{\#\mathcal{I} \mid \dim((C_1 \cap V_{\mathcal{I}})/(C_2 \cap V_{\mathcal{I}})) = m\}. \quad (2.3)$$

In this way the worst amount of information leakage of $\vec{s}$ from j shares is precisely characterized by the jth relative dimension/length profile of $C_2^\perp$ and $C_1^\perp$

[28, Theorem 4]:

$$\begin{aligned} & \max_{\mathcal{I}\subseteq\mathcal{J},\#\mathcal{I}=j} I(\vec{S}; f_{\mathcal{I}}(\vec{X})) \\ = & \max_{\mathcal{I}\subseteq\mathcal{J},\#\mathcal{I}=j} \dim((C_2^{\perp} \cap V_{\mathcal{I}})/(C_1^{\perp} \cap V_{\mathcal{I}})) \\ = & K_j(C_2^{\perp}, C_1^{\perp}). \end{aligned}$$

The smallest possible number of shares for which an unauthorized set of participants can determine m q-bits of information is

$$\begin{aligned} & \min_{\mathcal{I}\subseteq\mathcal{J}}\{\#\mathcal{I} \mid I(\vec{S}; f_{\mathcal{I}}(\vec{X})) = m\} \\ = & \min_{\mathcal{I}\subseteq\mathcal{J}}\{\#\mathcal{I} \mid \dim((C_2^{\perp} \cap V_{\mathcal{I}})/(C_1^{\perp} \cap V_{\mathcal{I}})) = m\} \\ = & M_m(C_2^{\perp}, C_1^{\perp}). \end{aligned}$$

In particular $t = M_1(C_2^{\perp}, C_1^{\perp}) - 1$ [28, Theorem 9]. (See also [2, Th. 6.7] and for the special case of $\ell = 1$ [9, Cor. 1.7]). We now generalize the notion of t-privacy and r-reconstruction.

Definition 2. *We say that a ramp secret sharing scheme has $(t_1, \ldots, t_\ell)$-privacy and $(r_1, \ldots, r_\ell)$-reconstruction if $t_1, \ldots, t_\ell$ are chosen largest possible and $r_1, \ldots, r_\ell$ are chosen smallest possible such that:*

- *an adversary cannot obtain m q-bits of information about $\vec{s}$ with any t_m shares,*
- *it is possible to recover m q-bits of information about $\vec{s}$ with any collection of r_m shares.*

In particular, one has $t = t_1$ and $r = r_\ell$.

By our previous discussion one has that $t_m = M_m(C_2^{\perp}, C_1^{\perp}) - 1$ since $M_m(C_2^{\perp}, C_1^{\perp})$ is the smallest size of a set of shares that can determine m q-bits of information about $\vec{s}$ [28, Theorem 4]. We will show that $(r_1, \ldots, r_\ell)$ can be characterized in terms of the RGHWs as well. Let r'_m be the largest size of a set of shares that cannot determine m q-bits of information about $\vec{s}$, i.e.

$$r'_m = \max_{\mathcal{I}\subseteq\mathcal{J}}\{\#\mathcal{I} \mid I(\vec{S}; f(\vec{X})) < m\}. \tag{2.4}$$

This value is closely related to r_m since any strictly larger set of shares will

determine m q-bits of information about $\vec{s}$ and thus

$$\begin{aligned}
& r_m \\
= \; & r'_m + 1 \\
= \; & \max_{\mathcal{I}\subseteq\mathcal{J}}\{\#\mathcal{I} \mid I(\vec{S}; f_{\mathcal{I}}(\vec{X})) < m\} + 1 \\
= \; & \max_{\mathcal{I}\subseteq\mathcal{J}}\{\#\mathcal{I} \mid I(\vec{S}; f_{\mathcal{I}}(\vec{X})) = m-1\} + 1 \\
= \; & \max_{\mathcal{I}\subseteq\mathcal{J}}\{\#\mathcal{I} \mid \dim((C_1 \cap V_{\overline{\mathcal{I}}})/(C_2 \cap V_{\overline{\mathcal{I}}})) = \\
& \quad \ell - m + 1\} + 1, \text{ by (2.1)} \\
= \; & n - \min_{\overline{\mathcal{I}}\subseteq\mathcal{J}}\{\#\overline{\mathcal{I}} \mid \dim((C_1 \cap V_{\overline{\mathcal{I}}})/(C_2 \cap V_{\overline{\mathcal{I}}})) = \\
& \quad \ell - m + 1\} + 1 \\
= \; & n - M_{\ell-m+1}(C_1, C_2) + 1. \qquad (2.5)
\end{aligned}$$

In particular one has that $r = r_\ell = n - M_1(C_1, C_2) + 1$ [28, Theorem 9] (see also [9, Cor. 1.7] for the special case $\ell = 1$). We note that r'_m corresponds to the $(m-1)$th conjugate relative length/dimension profile in [48].

Theorem 3. *Let C_1/C_2, where $\dim(C_1) - \dim(C_2) = \ell$, be a linear ramp secret sharing scheme with $(t_1, \ldots, t_\ell)$-privacy and $(r_1, \ldots, r_\ell)$-reconstruction. Then for $m = 1, \ldots, \ell$ we have $t_m = M_m(C_2^\perp, C_1^\perp) - 1$ and $r_m = n - M_{\ell-m+1}(C_1, C_2) + 1$.*

We shall relate the above concept of $(t_1, \ldots, t_\ell)$-privacy and $(r_1, \ldots, r_\ell)$-reconstruction to the literature: let $D_1 \subsetneq D_2 \subseteq \mathbb{F}_q^n$ be vector spaces of codimension ℓ and define for $1 \leq m \leq \ell$,

$$A_m(D_1, D_2) = \{\mathcal{I} \subseteq \mathcal{J} \mid m = \dim(D_1 \cap V_{\mathcal{I}})/(D_2 \cap V_{\mathcal{I}})\}.$$

Since $I(\vec{S}; f_{\mathcal{I}}(\vec{X})) = \dim((C_2^\perp \cap V_{\mathcal{I}})/(C_1^\perp \cap V_{\mathcal{I}}))$ we have that, for $D_1 = C_2^\perp$ and $D_2 = C_1^\perp$, $A_m(D_1, D_2)$ is the collection of shares that give m q-bits of information about $\vec{S}$. In addition, $A_\ell(D_1, D_2)$ is the access structure in the sense of [25], and $A_m(D_1, D_2)$ is equivalent to A_m in [26, Definition 1].

In particular we are interested in the largest and smallest element of such a collection of shares

$$\begin{aligned}
& A_m^{\min}(D_1, D_2) \\
= \; & \{\mathcal{I} \in A_m(D_1, D_2) \mid \nexists \mathcal{K} \in A_m(D_1, D_2) \text{ s.t. } \mathcal{K} \subsetneq \mathcal{I}\} \\
& A_m^{\max}(D_1, D_2) \\
= \; & \{\mathcal{I} \in A_m(D_1, D_2) \mid \nexists \mathcal{K} \in A_m(D_1, D_2) \text{ s.t. } \mathcal{K} \supsetneq \mathcal{I}\}
\end{aligned}$$

and, as we are interested in its size, we define

$$\begin{aligned}
A_m^d(D_1, D_2) &= \{\mathcal{I} \in A_m(D_1, D_2) \mid d = \#\mathcal{I}\} \\
A_m^{\min,d}(D_1, D_2) &= \{\mathcal{I} \in A_m^{\min}(D_1, D_2) \mid d = \#\mathcal{I}\} \\
A_m^{\max,d}(D_1, D_2) &= \{\mathcal{I} \in A_m^{\max}(D_1, D_2) \mid d = \#\mathcal{I}\}.
\end{aligned}$$

Moreover, we are interested in the smallest and the largest size of a collection of shares that reveal m q-bits of information: the first one being the smallest $d \in \{1, \ldots, n\}$ such that $A_m^{\min,d}(D_1, D_2)$ is non-empty and it is equal to $M_m(D_1, D_2) = t_m + 1$. Analogously, the largest size of a collection of shares that reveals m q-bits of information is the largest $d \in \{1, \ldots, n\}$ such that $A_m^{\max,d}(D_1, D_2)$ is non-empty and it is equal to $n - M_{\ell-m+1}(C_1, C_2) + 1 = r_m$.

Ramp secret sharing schemes with $\ell > 1$ are relevant in the situation where the set of possible secrets is large but one wants to keep the size of each share small. A further motivation for considering $\ell > 1$ is the analogy to the wiretap channels of type II [45, 36]. Recall that this model involves a main channel from Alice to Bob which is assumed to be error and erasure free, and a secondary channel from Alice to the eavesdropper Eve which is a q-ary erasure channel. Consider the slightly more general situation where also the main channel is a q-ary erasure channel [41]. Assuming that the probability of erasure is much smaller on the main channel than on the secondary channel we see that to achieve reliable and secure communication we should use long codes $C_2 \subsetneq C_1$. To retain a positive information rate on the main channel we therefore need $\ell > 1$. The exact values of the mutual information on the main and the secondary channel could be calculated from $A_m(D_1, D_2)$, $m = 1, \ldots, \ell$ and the erasure probabilities of the two channels; but it seems a difficult task to determine $A_m(D_1, D_2)$ even for simple codes. Finding $M_m(D_1, D_2) = t_m + 1$ and $n - M_{\ell-m+1}(C_1, C_2) + 1 = r_m$, however, would be a first step in this direction. As we shall see in the following, for many codes we can easily estimate these last mentioned parameters.

In the remaining part of this paper we shall concentrate on methods to estimate RGHW. We shall need the following definition which by [29] is equivalent to (2.3) (see also [2, Def. 6.2]).

Definition 4. *Let $C_2 \subsetneq C_1$ be linear codes over $\mathbb{F}_q$. For $m = 1, \ldots, \dim(C_1) - \dim(C_2)$ the mth relative generalized Hamming weight is defined as*

$$\begin{aligned} M_m(C_1, C_2) \quad = \quad & \min\{\#\mathit{Supp}\, D \mid D \ \textit{is a subspace of} \ C_1, \\ & \dim(D) = m, D \cap C_2 = \{\vec{0}\}\}. \end{aligned}$$

From this definition the connection between the RGHW and the generalized Hamming weight (GHW) becomes clear – the latter being $d_m(C_1) = M_m(C_1, C_2)$ with $C_2 = \{\vec{0}\}$. Before embarking with more general classes of codes in the next section we discuss the parameters t_m, r_m in the case of MDS codes.

Chapter 3

Ramp schemes based on MDS codes

Let C be an MDS code of dimension k. Then $C^\perp$ is also MDS and consequently

$$d_m(C) = n - k + m, \qquad m = 1, \ldots, k \tag{3.1}$$

$$d_m(C^\perp) = k + m, \qquad m = 1, \ldots, n - k \tag{3.2}$$

which means that all generalized Hamming weights attain the Singleton bound. Consider two MDS codes $C_2 \subsetneq C_1$ with $\dim(C_1) = k_1$ and $\dim(C_2) = k_2$. By definition, $M_m(C_1, C_2) \geq d_m(C_1)$, $m = 1, \ldots, \ell = k_1 - k_2$. However, the Singleton bound for RGHW is identical to the Singleton bound for GHW [30, Sec. IV] and therefore $M_m(C_1, C_2) = d_m(C_1)$ and $M_m(C_2^\perp, C_1^\perp) = d_m(C_2^\perp)$ [41]. Based on (3.1) and (3.2) one can show that

$$M_m(C_2^\perp, C_1^\perp) = n - M_{\ell-m+1}(C_1, C_2) + 1, \tag{3.3}$$

and from Theorem 3 it now follows that if we base a ramp scheme on two MDS codes then the size of a group uniquely determines how much information it can reveal:

$$t_m = r_m - 1, \;\; t_{m+1} = t_m + 1, \;\; t_1 = k_2, \;\; r_\ell = k_1.$$

When the number of participants is larger than two times the field size minus 1 then by [23, Cor. 7.4.4] C_1 and C_2 cannot be MDS – unless $k_1 = n - 1$ and $k_2 = 1$ – and consequently we can no longer assume (3.3). What is obviously needed is a method to estimate the left and the right side of (3.3) for codes of any length. As shall be demonstrated in the following the Feng-Rao method makes this possible.

Chapter 4

The Feng-Rao bounds for RGHW

The Feng-Rao bounds come in two versions: One for primary codes [1, 18, 17] and the other for dual codes [10, 11, 12, 37, 22, 32]. The most general formulations deal with arbitrary linear codes, whereas more specialized formulations – such as the order bounds – require that the code construction is supported by certain types of algebraic structures. The bounds have been applied to the minimum distance, the generalized Hamming weights – and for the case of dual codes of co-dimension 1 – also the relative minimum distance [9]. It is not difficult to extend the method for estimating GHW to a method for estimating RGHW. In the following we give the details for primary codes in the language of general linear codes. The details for dual codes are similar, hence for these codes we shall give a more brief description.

We start by introducing some terminology that shall be used throughout the section. Let $\mathcal{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$ be a fixed basis for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$ and write $\mathcal{J} = \{1, \ldots, n\}$.

Definition 5. *The function $\bar{\rho} : \mathbb{F}_q^n \to \mathcal{J} \cup \{0\}$ is given as follows. For non-zero $\vec{c}$ we have $\bar{\rho}(\vec{c}) = i$ where i is the unique integer such that*

$$\vec{c} \in Span\{\vec{b}_1, \ldots, \vec{b}_i\} \backslash Span\{\vec{b}_1, \ldots, \vec{b}_{i-1}\}.$$

Here we used the convention that $Span\,\emptyset = \{\vec{0}\}$. Finally, $\bar{\rho}(\vec{0}) = 0$.

The component wise product of two vectors in $\mathbb{F}_q^n$ plays a fundamental role in our exposition. This product is given by

$$(\alpha_1, \ldots, \alpha_n) * (\beta_1, \ldots, \beta_n) = (\alpha_1\beta_1, \ldots, \alpha_n\beta_n).$$

Definition 6. *An ordered pair $(i, j) \in \mathcal{J} \times \mathcal{J}$ is said to be one-way well-behaving (OWB) if $\bar{\rho}(\vec{b}_{i'} * \vec{b}_j) < \bar{\rho}(\vec{b}_i * \vec{b}_j)$ holds true for all $i' \in \mathcal{J}$ with $i' < i$.*

Definition 7. *For $i \in \mathcal{J}$ define*

$$\begin{aligned}\Lambda_i &= \{l \in \mathcal{J} \mid \exists\, j \in \mathcal{J} \text{ such that } (i,j) \text{ is OWB and} \\ &\qquad \bar{\rho}(\vec{b}_i * \vec{b}_j) = l\}.\end{aligned}$$

As is easily seen – if $D \subseteq \mathbb{F}_q^n$ is a vector space of dimension m then it holds that $\#\bar{\rho}\big(D\backslash\{\vec{0}\}\big) = m$. (Actually, any set $\{\vec{d}_1, \ldots, \vec{d}_m\} \subseteq D\backslash\{\vec{0}\}$ with $\bar{\rho}(\vec{d}_1) < \cdots < \bar{\rho}(\vec{d}_m)$ constitutes a basis for D). The following result is a slight modification of the material in [1].

Proposition 8. *Let $D \subseteq \mathbb{F}_q^n$ be a vector space of dimension at least 1. The support size of D satisfies*

$$\#Supp(D) \geq \#\cup_{i \in \bar{\rho}(D\backslash\{\vec{0}\})} \Lambda_i. \tag{4.1}$$

Proof. Let $l_1 < \cdots < l_\sigma$ be the elements in $\cup_{i \in \bar{\rho}(D\backslash\{\vec{0}\})}\Lambda_i$ and let $i_1, \ldots, i_\sigma$ and $j_1, \ldots, j_\sigma$ be such that for $s = 1, \ldots, \sigma$ it holds that:

- $i_s \in \bar{\rho}(D\backslash\{\vec{0}\})$,
- (i_s, j_s) is OWB and $\bar{\rho}(\vec{b}_{i_s} * \vec{b}_{j_s}) = l_s$.

Choose $\vec{d}_1, \ldots \vec{d}_\sigma \in D$ with $\bar{\rho}(\vec{d}_s) = i_s$, $s = 1, \ldots, \sigma$. Clearly $\bar{\rho}(\vec{d}_s * \vec{b}_{j_s}) = l_s$ and therefore $\vec{d}_1 * \vec{b}_{j_1}, \ldots, \vec{d}_\sigma * \vec{b}_{j_\sigma}$ are linearly independent. In conclusion $D * \mathbb{F}_q^n = \{\vec{d} * \vec{c} \mid \vec{d} \in D, \vec{c} \in \mathbb{F}_q^n\}$ is of dimension at least σ. The dimension of $D * \mathbb{F}_q^n$ equals the size of the support of D and the proposition follows. □

We now turn to RGHW. Observe that although $C_2 \subsetneq C_1$ implies $\bar{\rho}(C_2) \subsetneq \bar{\rho}(C_1)$, it does not always hold that $\vec{c} \in C_1\backslash C_2$ implies $\bar{\rho}(\vec{c}) \in \bar{\rho}(C_1)\backslash\bar{\rho}(C_2)$. However, some observations can still be made.

Theorem 9. *Consider linear codes $C_2 \subsetneq C_1$, $\dim(C_1) = k_1$, $\dim(C_2) = k_2$. Let u be the smallest element in $\bar{\rho}(C_1)$ that is not in $\bar{\rho}(C_2)$. For $m = 1, \ldots, k_1 - k_2$ we have*

$$\begin{aligned}M_m(C_1, C_2) &\geq \min\big\{\#\cup_{s=1}^m \Lambda_{i_s} \mid u \leq i_1 < \cdots < i_m, \\ &\qquad i_1, \ldots, i_m \in \bar{\rho}(C_1\backslash\{\vec{0}\})\big\}.\end{aligned}$$

Proof. If D is an m-dimensional subspace of C_1 with $D \cap C_2 = \{\vec{0}\}$ then we can write $\bar{\rho}(D\backslash\{\vec{0}\}) = \{i_1, \ldots, i_m\} \subseteq \bar{\rho}(C_1\backslash\{\vec{0}\})$ with $u \leq i_1 < \cdots < i_m$. The theorem now follows from Proposition 8. □

Corollary 10. *Consider a k_1-dimensional code C_1, say $C_1 = Span\{\vec{f}_1, \ldots, \vec{f}_{k_1}\}$, where without loss of generality we assume $\bar{\rho}(\vec{f}_1) < \cdots < \bar{\rho}(\vec{f}_{k_1})$. For $k_2 < k_1$ let $C_2 = Span\{\vec{f}_1, \ldots, \vec{f}_{k_2}\}$. We have*

$$\begin{aligned}M_m(C_1, C_2) &\geq \min\big\{\#\cup_{s=1}^m \Lambda_{i_s} \mid i_1 < \cdots < i_m, \\ &\qquad i_1, \ldots, i_m \in \{\bar{\rho}(\vec{f}_{k_2+1}), \ldots, \bar{\rho}(\vec{f}_{k_1})\}\big\}.\end{aligned}$$

Next we treat dual codes.

Definition 11. *For $\vec{c} \in \mathbb{F}_q^n \backslash \{\vec{0}\}$ define $M(\vec{c})$ to be the smallest number $i \in \mathcal{J}$ such that $\vec{c} \cdot \vec{b}_i \neq 0$. Here $\vec{a} \cdot \vec{b}$ means the usual inner product between $\vec{a}$ and $\vec{b}$.*

It is clear that for an m-dimensional space D we have $\#M(D\backslash\{\vec{0}\}) = m$. Also it is clear that if $D \subseteq C^{\perp}$, where C is a linear code, then $M(D\backslash\{\vec{0}\}) \cap \bar{\rho}(C) = \emptyset$.

Definition 12. *For $l \in \mathcal{J}$ define*

$$V_l = \{i \in \mathcal{J} \mid \bar{\rho}(\vec{b}_i * \vec{b}_j) = l \text{ for some } \vec{b}_j \in \mathcal{B} \text{ with } (i,j) \text{ OWB}\}.$$

The following result is proved by slightly modifying the proof of [21, Prop. 3.12] and [20, Th. 5].

Proposition 13. *Let $D \subseteq \mathbb{F}_q^n$ be a space of dimension at least 1. We have*

$$\#Supp(D) \geq \# \cup_{l \in M(D\backslash\{\vec{0}\})} V_l.$$

From the above discussion we derive

Theorem 14. *Consider linear codes $C_2 \subsetneq C_1$. Let u be the largest element in $\bar{\rho}(C_1\backslash\{\vec{0}\})$. For $m = 1, \ldots, \dim(C_1) - \dim(C_2) = \dim(C_2^{\perp}) - \dim(C_1^{\perp})$ we have*

$$M_m(C_2^{\perp}, C_1^{\perp}) \geq \min\{\# \cup_{s=1}^{m} V_{i_s} \mid 1 \leq i_1 < \cdots < i_m \leq u, i_1, \ldots, i_m \notin \bar{\rho}(C_2)\}. \tag{4.2}$$

To apply Theorem 9, Corollary 10 and Theorem 14 we need information on which pairs are OWB. This suggests the use of a supporting algebra. One class of algebras that works well is the order domains [22, 35, 19]. In the present paper we will concentrate on the most prominent example of order domain codes – namely one-point algebraic geometric codes.

Remark 15. *In our exposition we used a single (but arbitrary) basis $\mathcal{B}$ for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. Following [37] one could reformulate all the above results in a more general setting that uses three bases $\mathcal{U}$, $\mathcal{V}$, and $\mathcal{W}$. This point of view is important when one considers affine variety codes [38], but it does not improve the results for order domain codes. In [14] and [15], the concept of OWB was relaxed giving new improved Feng-Rao bounds. All the above results could be reformulated in this setting – but again – for order domain codes the results stay unchanged.*

Chapter 5

One-point algebraic geometric codes

Given an algebraic function field F of transcendence degree one, let $P_1, \ldots, P_n$, Q be distinct rational places. For $f \in F$ write $\rho(f) = -\nu_Q(f)$, where ν_Q is the valuation at Q, and denote by $H(Q)$ the Weierstrass semigroup of Q. That is, $H(Q) = \rho\big(\cup_{\mu=0}^{\infty} \mathcal{L}(\mu Q)\big)$. In the following let $\{f_\lambda \mid \lambda \in H(Q)\}$ be any fixed basis for $R = \cup_{\mu=0}^{\infty} \mathcal{L}(\mu Q)$ with $\rho(f_\lambda) = \lambda$ for all $\lambda \in H(Q)$. Let $D = P_1 + \cdots + P_n$ and define

$$\begin{aligned} H^*(Q) &= \{\mu \mid C_{\mathcal{L}}(D, \mu Q) \neq C_{\mathcal{L}}(D, (\mu - 1)Q)\} \\ &= \{\gamma_1, \ldots, \gamma_n\} \subsetneq H(Q). \end{aligned} \tag{5.1}$$

Here, the enumeration is chosen such that $\gamma_1 < \cdots < \gamma_n$. Consider the map $\mathrm{ev} : F \to \mathbb{F}_q^n$ given by $\mathrm{ev}(f) = (f(P_1), \ldots, f(P_n))$. The set

$$\{\vec{b}_1 = \mathrm{ev}(f_{\gamma_1}), \ldots, \vec{b}_n = \mathrm{ev}(f_{\gamma_n})\} \tag{5.2}$$

clearly is a basis for $\mathbb{F}_q^n$ and by [1, Pro. 27] a pair (i, j) is OWB if $\rho(f_{\gamma_i}) + \rho(f_{\gamma_j}) = \rho(f_{\gamma_l})$, i. e. $\gamma_i + \gamma_j = \gamma_l$, in which case of course $\bar{\rho}(\vec{b}_i * \vec{b}_j) = l$. From [1, Pro. 28] we know that if $\delta \in H^*(Q)$ and $\alpha, \beta \in H(Q)$ satisfy $\alpha + \beta = \delta$ then we have $\alpha, \beta \in H^*(Q)$. We therefore get the following lemma.

Lemma 16. *Let $\{\vec{b}_1, \ldots, \vec{b}_n\}$ be as above. For $i \in \mathcal{J}$ it holds that*

$$\{l \in \mathcal{J} \mid \gamma_l - \gamma_i \in H(Q)\} \subseteq \Lambda_i$$

where Λ_i is as in Definition 7.

Proposition 17. *Let $D \subseteq \mathbb{F}_q^n$ be a vector space of dimension m. There exist unique numbers $\gamma_{i_1} < \cdots < \gamma_{i_m}$ in $H^*(Q)$ such that $\bar{\rho}(D \backslash \{\vec{0}\}) = \{i_1, \ldots, i_m\}$. The*

support of D satisfies

$$\begin{aligned} \#Supp(D) &\geq \#\Big(H^*(Q) \cap \big(\cup_{s=1}^{m} (\gamma_{i_s} + H(Q)) \big) \Big) && (5.3) \\ &\geq n - \gamma_{i_m} + \#\{\lambda \in \cup_{s=1}^{m-1} (\gamma_{i_s} + H(Q)) \mid \\ &\qquad \lambda \notin \gamma_{i_m} + H(Q)\}. && (5.4) \end{aligned}$$

Proof. By Lemma 16 the right side of (5.3) is lower than or equal to $\# \cup_{s=1}^{m} \Lambda_{i_s}$, and (5.3) therefore follows from Proposition 8. Another way of writing the right side of (5.3) is $n - \#\big(H^*(Q) \backslash \cup_{s=1}^{m} (\gamma_{i_s} + H(Q))\big)$. This number is greater than or equal to

$$\begin{aligned} & n - \#\big(H(Q) \backslash \cup_{s=1}^{m} (\gamma_{i_s} + H(Q))\big) \\ = \; & n - \#\big(H(Q) \backslash (\gamma_{i_m} + H(Q))\big) \\ & \quad + \# \{\lambda \in \cup_{s=1}^{m-1} (\gamma_{i_s} + H(Q)) \mid \lambda \notin \gamma_{i_m} + H(Q)\}. \end{aligned}$$

From [22, Lem. 5.15] we know that for any numerical semigroup Γ and $\lambda \in \Gamma$, one has $\lambda = \#\big(\Gamma \backslash (\lambda + \Gamma)\big)$. In particular $\#\big(H(Q) \backslash (\gamma_{i_m} + H(Q))\big) = \gamma_{i_m}$ and (5.4) follows. □

From (5.4) we can obtain a manageable bound on the RGHWs of one-point algebraic geometric codes as we now explain. This bound can even be used when one does not know $H^*(Q)$. Given non-negative integers $\lambda_1 < \cdots < \lambda_m$ (note that we make no assumptions that $\lambda_1, \ldots, \lambda_m \in H(Q)$) let $i_j = \lambda_j - \lambda_m$, $j = 1, \ldots, m-1$ and observe that

$$\begin{aligned} & \#\{\lambda \in \cup_{s=1}^{m-1} (\lambda_i + H(Q) \mid \lambda \notin \lambda_m + H(Q)\} \\ & \qquad = \#\{\alpha \in \cup_{s=1}^{m-1} (i_s + H(Q)) \mid \alpha \notin H(Q)\} && (5.5) \end{aligned}$$

since λ is in the first set if and only if $\lambda - \lambda_m$ is in the second set. The function Z in the definition below shall help us estimate the last expression in (5.4).

Definition 18. *Consider a numerical semigroup Γ and a positive integer μ. Define $Z(\Gamma, \mu, 1) = 0$ and for $1 < m \leq \mu$*

$$\begin{aligned} Z(\Gamma, \mu, m) &= \min \big\{ \#\{\alpha \in \cup_{s=1}^{m-1} (i_s + \Gamma) \mid \alpha \notin \Gamma\} \mid \\ &\qquad -\mu + 1 \leq i_1 < \cdots < i_{m-1} \leq -1 \big\}. && (5.6) \end{aligned}$$

We are now ready for the main result of the section.

Theorem 19. *Let μ_1, μ_2 be positive integers with $\mu_2 < \mu_1$.*

For $m = 1, \ldots, \dim(C_{\mathcal{L}}(D, \mu_1 Q)) - \dim(C_{\mathcal{L}}(D, \mu_2 Q))$ *we have*

$$\begin{aligned} & M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) \\ \geq \; & \min\Big\{ \#\big(H^*(Q) \cap \big(\cup_{s=1}^{m} (\gamma_{i_s} + H(Q))\big)\big) \mid \\ & \gamma_{i_1}, \ldots, \gamma_{i_m} \in H^*(Q), \mu_2 < \gamma_{i_1} < \cdots < \gamma_{i_t} \leq \mu_1 \Big\} \end{aligned} \tag{5.7}$$

$$\begin{aligned} \geq \; & \min\Big\{ n - \gamma_{i_m} + \\ & \#\{\lambda \in \cup_{s=1}^{m-1} (\gamma_{i_s} + H(Q)) \mid \lambda \notin \gamma_{i_m} + H(Q)\} \mid \\ & \gamma_{i_1}, \ldots, \gamma_{i_m} \in H^*(Q), \mu_2 < \gamma_{i_1} < \cdots < \gamma_{i_t} \leq \mu_1 \Big\} \end{aligned} \tag{5.8}$$

$$\geq \; n - \mu_1 + Z(H(Q), \mu, m), \tag{5.9}$$

where $\mu = \mu_1 - \mu_2$.

Proof. Consider an m-dimensional vector space $D \subseteq C_{\mathcal{L}}(D, \mu_1 Q)$ with $D \cap C_{\mathcal{L}}(D, \mu_2 Q) = \{\vec{0}\}$. Let $\gamma_{i_1} < \cdots < \gamma_{i_m}$ be as described in Theorem 17. By the definition of the codes we have $\gamma_{i_1}, \ldots, \gamma_{i_m} \in \{\mu_2 + 1, \ldots, \mu_1\}$ (this is the situation of Corollary 10). Consequently (5.7) and (5.8), respectively, follow from (5.3) and (5.4), respectively. We have $-\mu_1 \leq -\gamma_{i_m}$. Similarly, by (5.5) $Z(H(Q), \mu, m)$ is smaller than or equal to the last term in (5.4). These observations prove (5.9). □

Note that (5.9) may be strictly smaller than (5.8). Firstly, μ_1 may not belong to $H^*(Q)$. Secondly, when applying the function $Z(H(Q), \mu, m)$ we do not discard the numbers in $\{\mu_2 + 1, \ldots, \mu_1 - 1\}$ that are gaps of $H(Q)$, and least of all the numbers in the interval that are not present in $H^*(Q)$. The connection to the usual Goppa bound for primary codes is seen from the expression in (5.9): letting $m = 1$ we get by Definition 18 $Z(H(Q), \mu, m) = 0$ and the formula simplifies to the well-known bound on the minimum distance $d\big(C_{\mathcal{L}}(D, \mu_1 Q)\big) \geq n - \mu_1$.

For duals of one-point algebraic geometric codes we have a bound similar to (5.7), but no bounds similar to (5.8) or (5.9).

Theorem 20. *Let* μ_1, μ_2 *and* m *be as in Theorem 19. We have*

$$\begin{aligned} & M_m(C_{\mathcal{L}}^{\perp}(D, \mu_2 Q), C_{\mathcal{L}}^{\perp}(D, \mu_1 Q)) \\ \geq \; & \min\Big\{ \#\big(H(Q) \cap \big(\cup_{s=1}^{m} (\gamma_{i_s} - H(Q))\big)\big) \mid \\ & \gamma_{i_1}, \ldots, \gamma_{i_m} \in H^*(Q), \mu_2 < \gamma_{i_1} < \cdots < \gamma_{i_m} \leq \mu_1 \Big\}. \end{aligned} \tag{5.10}$$

Chapter 6

RGHWs of Hermitian codes

In this section we apply the results of Section 5 to the case of Hermitian codes [42, 40]. Our main result is that (5.9) is often tight. The Hermitian function field over $\mathbb{F}_{q^2}$ (q a prime power) is given by the equation $x^{q+1} - y^q - y$ and it possesses exactly $q^3 + 1$ rational places which we denote $P_1, \ldots, P_{q^3}, Q$ – the last being the pole of x. The Weierstrass semigroup of Q, $H(Q) = \langle \rho(x) = q, \rho(y) = q + 1 \rangle$, has $g = q(q-1)/2$ gaps and conductor $c = q(q-1)$. Let $D = P_1 + \cdots + P_{q^3}$. In the following by a Hermitian code we mean a code of the form $C_{\mathcal{L}}(D, \mu Q)$. Clearly, this code is of length $n = q^3$. As is well-known the dual of a Hermitian code is a Hermitian code. This fact will be useful when in a later section we consider ramp schemes based on Hermitian codes. We start our investigation with a lemma that treats a slightly more general class of semigroups than the semigroup $\langle q, q+1 \rangle$ relevant to us.

Lemma 21. *Let a be an integer, $a \geq 2$. Define $\Gamma = \langle a, a+1 \rangle$. For integers m, μ with $1 \leq m \leq \mu \leq a+1$ it holds that*

$$Z(\Gamma, \mu, m) = \sum_{s=0}^{m-2} (a - s) = a(m-1) - (m-2)(m-1)/2. \tag{6.1}$$

Proof. Recall that a positive integer λ is called a gap of Γ if $\lambda \notin \Gamma$. All other non-negative integers are called non-gaps. For the given semigroup Γ the set of non-negative integers consists of one non-gap followed by $a-1$ gaps, then two non-gaps followed by $a-2$ gaps and so on up to $a-1$ non-gaps followed by $a - (a-1) = 1$ gap. All the following numbers are non-gaps. We denote the above maximal sequences of consecutive gaps $G_1, \ldots, G_{a-1}$ with $\#G_v = a - v$, $v = 1, \ldots, a-1$ (such sequences are called deserts in [34, Ex. 3]).
First assume $1 \leq m \leq \mu \leq a+1$. Let $-\mu \leq i_1 < \ldots < i_{m-1} \leq -1$. We have

$$\#G_v \cap \left(\cup_{s=1}^{m-1} (i_s + \Gamma) \right) \geq \min\{\#G_v, m-1\}$$

with equality when $i_{m-1} = -1, i_{m-2} = -2, \ldots, i_1 = -(m-1)$. Summing up the contribution from all G_v accounts for $\sum_{s=1}^{m-2}(a-s)$. The term in (6.1) corresponding

to $s = 0$, namely a, comes from considering the number of negative integers in $\sum_{s=1}^{m-1}(i_s + \Gamma)$. Thus we have established (6.1). □

Recall from Theorem 19 that we have three bounds on the RGHW of which (5.9) is the weakest. Using Lemma 21, for Hermitian codes of codimension at most $q+1$, (5.9) translates into a closed-formula expression in (6.2). Surprisingly, this expression is often equal to the true value of the RGHW.

Theorem 22. *Consider the Hermitian curve $x^{q+1} - y^q - y$ over $\mathbb{F}_{q^2}$. Let $P_1, \ldots, P_{n=q^3}$, and Q be the rational places and $D = P_1 + \cdots + P_n$. Let μ_1, μ_2 be non-negative integers with $1 \leq \mu_1 - \mu_2 \leq q+1$. For $1 \leq m \leq \dim(C_{\mathcal{L}}(D, \mu_1 Q)) - \dim(C_{\mathcal{L}}(D, \mu_2 Q))$ we have*

$$\begin{aligned} & M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) \\ \geq \;& n - \mu_1 + \sum_{s=0}^{m-2}(q - s) \\ = \;& n - \mu_1 + q(m-1) - (m-2)(m-1)/2. \end{aligned} \tag{6.2}$$

If

$$c - 1 \leq \mu_2 \text{ and } \mu_1 < n - c. \tag{6.3}$$

(recall that $c = q(q-1)$) then we have $\dim(C_{\mathcal{L}}(D, \mu_1 Q)) - \dim(C_{\mathcal{L}}(D, \mu_2 Q)) = \mu_1 - \mu_2$ and equality in (6.2).

Proof. Equation (6.2) is a consequence of the last part of Theorem 19 and the first part of Lemma 21. The result concerning the dimensions is well-known. That equality holds in (6.2) under condition (6.3) follows from Lemma 23 below. □

Lemma 23. *Let μ_1 and m be positive integers with $m \leq q+1$, $\mu_1 < n - c$ and $c - 1 < \mu_1 - (m-1)$. Then there exist m functions $f_0, \ldots, f_{m-1}$ such that*

- *$f_i \in \mathcal{L}((\mu_1 - i)Q) \backslash \mathcal{L}((\mu_1 - (i+1))Q)$, $i = 0, \ldots, m-1$.*
- *The number of common zeros of $f_0, \ldots, f_{m-1}$ is exactly $\mu_1 - \sum_{i=0}^{m-2}(q - i)$.*

Proof. As is well-known $\cup_{\mu=0}^{\infty}\mathcal{L}(\mu Q)$ is isomorphic to $\mathbb{F}_{q^2}[X, Y]/I$, where $I = \langle X^{q+1} - Y^q - Y \rangle$. The isomorphism is given by $\varphi(x) = X + I$ and $\varphi(y) = Y + I$. We call $X^{q+1} - Y^q - Y = \mathrm{N}(X) - \mathrm{Tr}(Y)$ the Hermitian polynomial – N being the norm and Tr the trace corresponding to the field extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. In this description the rational places $P_1, \ldots, P_{q^3}$ correspond to the affine points of the Hermitian polynomial. We remind the reader of the following few facts which play a crucial role in the below induction proofs:

- For any $\delta \in \mathbb{F}_{q^2}$ we have $\mathrm{N}(\delta), \mathrm{Tr}(\delta) \in \mathbb{F}_q$.
- For every $\epsilon \in \mathbb{F}_q$ there exists exactly q different δ such that $\mathrm{Tr}(\delta) = \epsilon$.
- There exist exactly $q+1$ different δ such that $\mathrm{N}(\delta) = 1$.

We start by fixing some notation. Let $\{\alpha_1, \ldots, \alpha_q\}$ be the elements in $\mathbb{F}_{q^2}$ that map to 1 under Tr. Let $\{\beta_1, \ldots, \beta_{q^2-(q+1)}\}$ be the elements that do not map to 1 under N and $\{\gamma_1, \ldots, \gamma_{q+1}\}$ the elements that do.
Write $\mu_1 = iq + j(q+1)$ with $0 \leq j < q$. First assume $1 \leq m \leq j+1$ and that $i < q^2 - q$. By induction on m (in this interval) one can show that the set $\{F_0, F_1, \ldots, F_{m-1}\}$ where

$$F_0 = \big(\prod_{s=1}^{i}(X-\beta_s)\big)\big(\prod_{s=1}^{j}(Y-\alpha_s)\big), \tag{6.4}$$

$$F_1 = \big(\prod_{s=1}^{i}(X-\beta_s)\big)(X-\gamma_1)\big(\prod_{s=1}^{j-1}(Y-\alpha_s)\big), \tag{6.5}$$

$$\vdots$$

$$F_{m-1} = \big(\prod_{s=1}^{i}(X-\beta_s)\big)\big(\prod_{s=1}^{m-1}(X-\gamma_s)\big) \big(\prod_{s=1}^{j-m+1}(Y-\alpha_s)\big), \tag{6.6}$$

has exactly $iq + j(q+1) - \sum_{s=0}^{m-2}(q-s)$ zeros in common with the Hermitian polynomial $X^{q+1} - Y^q - Y$ (we leave the technical details for the reader).
Finally, assume $j+1 \leq m \leq j+q$. By induction on m (in this interval) one can

show that the set $\{F_0, F_1, \ldots, F_{m-1}\}$ where

$$\begin{aligned}
F_0 &= \Big(\prod_{s=1}^{i-q+j}(X-\beta_s)\Big)\Big(\prod_{s=1}^{q-j}(X-\gamma_s)\Big) \\
&\quad \Big(\prod_{s=1}^{j}(Y-\alpha_s)\Big), \qquad (6.7)\\
F_1 &= \Big(\prod_{s=1}^{i-q+j}(X-\beta_s)\Big)\Big(\prod_{s=1}^{q-j+1}(X-\gamma_s)\Big) \\
&\quad \Big(\prod_{s=1}^{j-1}(Y-\alpha_s)\Big), \qquad (6.8)\\
&\vdots \\
F_j &= \Big(\prod_{s=1}^{i-q+j}(X-\beta_s)\Big)\Big(\prod_{s=1}^{q}(X-\gamma_s)\Big), \qquad (6.9)\\
F_{j+1} &= \Big(\prod_{s=1}^{i-q+j}(X-\beta_s)\Big)\Big(\prod_{s=1}^{q-1}(Y-\alpha_s)\Big), \\
F_{j+2} &= \Big(\prod_{s=1}^{i-q+j}(X-\beta_s)\Big)\Big(\prod_{s=1}^{q-2}(Y-\alpha_s)\Big)(X-\gamma_1), \\
&\vdots \\
F_{m-1} &= \Big(\prod_{s=1}^{i-q+j}(X-\beta_s)\Big)\Big(\prod_{s=1}^{q-m+j+1}(Y-\alpha_s)\Big) \\
&\quad \Big(\prod_{s=1}^{m-j-2}(X-\gamma_s)\Big),
\end{aligned}$$

has exactly $iq + j(q+1) - \sum_{s=0}^{m}(q-s)$ zeros in common with the Hermitian polynomial $X^{q+1} - Y^q - Y$ (again we leave the technical details for the reader). For simplicity we covered the case $m = j+1$ and $i < q^2-q$ in both induction proofs. Observe that the basis step $m = j+1$ of the last induction proof corresponds to the terms in (6.7), (6.8), (6.9) which are different from (6.4), (6.5), (6.6) with $m = j+1$. □

For $1 \le m \le \mu_1 - \mu_2 \le q+1$ but with μ_1 and μ_2 not satisfying the condition in (6.3) we can often derive much better estimates than (6.2).
For $\mu_2 < c-1$ it may happen that not all of the numbers $\mu_1, \mu_1-1, \ldots, \mu_1-(m-1)$ belong to $H(Q)$, and so the worst case in the proof of Theorem 19 may not be realized. Hence, we should rather apply (5.8) or (5.7) (which in this situation are equivalent).
For $n - c \le \mu_1$ it may happen that $H^*(Q)\backslash(\mu_1 + H(Q))$ is strictly smaller than $H(Q)\backslash(\mu_1 + H(Q))$ (this will happen if $\mu_1 = iq + j(q+1)$, with $q^2 - q \le i < q^2$ and

$0 < j < q$). In such a case $\#\big(H^*(Q) \cap (\mu_1 + H(Q))\big)$ will be strictly larger than $n - \mu_1$. Moreover, all the numbers $\mu_1, \mu_1 - 1, \ldots, \mu_1 - (m-1)$ need not belong to $H^*(Q)$ (this may happen if $\mu_1 \geq n$) and again the worst case considered in the proof of Theorem 19 may not be realizable. In this situation we should rather apply (5.7).

We illustrate our observations with three examples. The first two are concerned with $\mu_2 < c - 1$ and the last with $n - c \leq \mu_1$.

Example 1. *In this example we consider codes over* $\mathbb{F}_{q^2} = \mathbb{F}_{16}$. *Hence,* $q = 4$, $H(Q) = \langle 4, 5\rangle$ *and* $n = 64$. *The first numbers of* $H^*(Q)$ *(and* $H(Q)$*) are* $0, 4, 5, 8, 9, 10, 12$. *Hence,* $dim C_{\mathcal{L}}(D, 8Q) = 4$, $dim C_{\mathcal{L}}(D, 12Q) = 7$. *Theorem 22 tells us that* $M_m(C_{\mathcal{L}}(D, 12Q), C_{\mathcal{L}}(D, 8Q))$ *is at least* 52, 56 *and* 59, *for* m *equal to* 1, 2 *and* 3, *respectively. Using (5.8) we now show that for* $m = 2$ *and* $m = 3$ *the true values are at least* 58 *and* 60, *respectively. We first concentrate on* $m = 2$. *Using the notation from Proposition 17 we must investigate all* $\gamma_{i_1}, \gamma_{i_2} \in \{9, 10, 12\}$ *with* $\gamma_{i_1} < \gamma_{i_2}$, *We have three different choices of* $(\gamma_{i_1}, \gamma_{i_2})$ *to consider, namely* $(10, 12)$, $(9, 12)$ *and* $(9, 10)$. *We first observe that*

$$\begin{aligned} 12 + H(Q) &= \{12, 16, 17, 20, 21, 22, 24, \ldots\} \\ 10 + H(Q) &= \{10, 14, 15, 18, 19, 20, 22, 23, 24, \ldots\} \\ 9 + H(Q) &= \{9, 13, 14, 17, 18, 19, 21, 22, 23, 24, \ldots\}. \end{aligned}$$

Note that if $\alpha \in H(Q) \backslash (\lambda + H(Q))$ *for* $\lambda \in \{9, 10, 12\}$ *then also* $\alpha \in H^*(Q)$.

$\underline{(\gamma_{i_1}, \gamma_{i_2}) = (10, 12)}$*: We have*

$$\begin{aligned} \#(H^*(Q) \cap (12 + H(Q)) &= n - 12 = 52, \\ \#((10 + H(Q)) \backslash (12 + H(Q)) &= 6. \end{aligned} \tag{6.10}$$

Hence, we get the value $52 + 6 = 58$.

$\underline{(\gamma_{i_1}, \gamma_{i_2}) = (9, 12)}$*: Combining (6.10) with*

$$\#((9 + H(Q)) \backslash (12 + H(Q)) = 6$$

again give us the value $52 + 6 = 58$.

$\underline{(\gamma_{i_1}, \gamma_{i_2}) = (9, 10)}$*: We have*

$$\begin{aligned} \#(H^*(Q) \cap (10 + H(Q)) &= n - 10 = 54, \\ \#((9 + H(Q)) \backslash (10 + H(Q)) &= 4 \end{aligned}$$

producing the value $54 + 4 = 58$.

The minimum of the above three values is 58 *which is then our estimate on* $M_2(C_{\mathcal{L}}(D, 12Q), C_{\mathcal{L}}(D, 8Q))$.

Finally consider $m = 3$. *There is only one choice of* $(\gamma_{i_1}, \gamma_{i_2}, \gamma_{i_3})$ *namely* $(9, 10, 12)$. *By inspection there are exactly* 8 *numbers that are in either* $9+H(Q)$ *or* $10+H(Q)$ *but not in* $12+H(Q)$. *Hence, our estimate on* $M_3(C_{\mathcal{L}}(D, 12Q), C_{\mathcal{L}}(D, 8Q))$ *becomes* $n - 12 + 8 = 60$.

Example 2. *This is a continuation of Example 1. The dimension of* $C_{\mathcal{L}}(D, 10Q)$ *and* $C_{\mathcal{L}}(D, 5Q)$ *are* 6 *and* 3, *respectively. Theorem 22 tells us that* $M_m(C_{\mathcal{L}}(D, 10Q), C_{\mathcal{L}}(D, 5Q))$ *is at least* $n - 10 = 54$, $n - 10 + 4 = 58$ *and* $n - 10 + 4 + 3 = 61$, *for* m *equal to* 1, 2 *and* 3, *respectively. The possible values of* γ_{i_s} *to consider are* $8, 9, 10$, *which constitute a sequence without gaps. Hence, according to our discussion prior to Example 1 in this case we cannot improve upon Theorem 19.*

Example 3. *This is a continuation of Examples 1 and 2. The last numbers of* $H^*(Q)$ *are* $\{65, 66, 67, 69, 70, 71, 74, 75, 79\}$. *Hence,* $\dim(C_{\mathcal{L}}(D, 69Q)) = 64 - 5 = 59$ *and* $\dim(C_{\mathcal{L}}(D, 65Q)) = 64 - 8 = 56$. *Theorem 22 gives no information on the first two RGHWs and only tells us that the third relative weight is larger than or equal to* 2. *This, however, is useless information as any space* D *of dimension* 3 *has a support of size at least* 3. *As we will now demonstrate (5.7) guarantees that the three RGHWs are at least* 3, 6, *and* 8, *respectively. We first observe that*

$$\begin{aligned} H^*(Q) \cap (69 + H(Q)) &= \{69, 74, 79\} \\ H^*(Q) \cap (67 + H(Q)) &= \{67, 71, 75, 79\} \\ H^*(Q) \cap (66 + H(Q)) &= \{66, 70, 71, 74, 75, 79\}. \end{aligned}$$

The smallest set is of size 3 *and we get* $M_1(C_{\mathcal{L}}(D, 69Q), C_{\mathcal{L}}(D,\ 65Q)) = 3$.
The smallest union of two sets is the union of the first two. This union is of size 6 *giving us* $M_2(C_{\mathcal{L}}(D, 69Q), C_{\mathcal{L}}(D, 65Q)) \geq 6$.
The union of all three sets is of size 8. *Hence,* $M_3(C_{\mathcal{L}}(D, 69Q),\ C_{\mathcal{L}}(D, 65Q)) \geq 8$.

6.1 A comparison between RGHW and GHW

In [33] and [3], respectively, Munuera & Ramirez and Barbero & Munuera determined the GHWs of any Hermitian code. To state all their results is too extensive. However, already from their master theorem [33, Prop. 12], [3, Prop. 2.3], one can deduce that the RGHWs are often much larger than the corresponding GHWs.

Definition 24. *Let* $ev : \cup_{\mu=0}^{\infty} C_{\mathcal{L}}(D, \mu Q) \to \mathbb{F}_q^n$ *be the map* $ev(f) = (f(P_1), \ldots, f(P_n))$. *The abundance* $\alpha(\mu)$ *is the dimension of* $\ker ev$ *when* ev *is restricted to* $C_{\mathcal{L}}(D, \mu Q)$.

The following is the master theorem from [33, 3]. Here, and throughout the rest of this section, we use the notation $H(Q) = \{\rho_1, \rho_2, \ldots\}$ with $\rho_i < \rho_j$ for $i < j$.

Theorem 25. *For* $m = 1, \ldots, \dim(C_{\mathcal{L}}(D, \mu Q))$

$$d_m(C_{\mathcal{L}}(D, \mu Q)) \geq n - \mu + \rho_m + \alpha(\mu). \tag{6.11}$$

Equality holds under the following conditions:

1. $\mu \in H^*(Q)$

2. $n-\mu+\rho_{m+\alpha(\mu)} \in H(Q)$, *in which case we write* $n-\mu+\rho_{m+\alpha(\mu)} = iq+j(q+1)$, *where* i, j *are non-negative integers with* $j < q$.

3. $i \leq q^2-q-1$ *or* $j = 0$.

Observe that Theorem 25 and Theorem 22, respectively, produce similar estimates for the minimum distance and the relative minimum distance. Similarly for the second GHW and the second RGHW. From the last part of Theorem 22 we conclude that for $m = 1, 2$, whenever $m \leq \mu_1 - \mu_2 \leq q+1$, $c-1 \leq \mu_2$ and $\mu_1 < n-c$ holds, then $M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) = d_m(C_{\mathcal{L}}(D, \mu_1 Q))$ (recall that c is the conductor). As shall be demonstrated in the following, for higher values of m, $M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q))$ is often much larger than $d_m(C_{\mathcal{L}}(D, \mu_1 Q))$.

Proposition 26. *For* $q > 2$, $1 \leq m \leq q+1$ *and* $2q^2 - q \leq \mu \leq n-c$ *we have* $d_m(C_{\mathcal{L}}(D, \mu Q)) = n - \mu + \rho_m$.

Proof. It is well-known [42] that for $\mu \leq q^3 - 1$ we have $\alpha(\mu) = 0$. Therefore (6.11) simplifies to $d_m(C_{\mathcal{L}}(D, \mu Q)) \geq n - \mu + \rho_m$ under the conditions of the proposition. To prove the proposition it suffices to demonstrate the conditions 1, 2, and 3 of Theorem 25. As is well-known $\mu \in H^*(Q)$ when $c \leq \mu < n$. However, $c < 2q^2 - q$ and therefore condition 1 follows. To see that condition 2 is satisfied note that by assumption $c \leq n - \mu$ and so $n - \mu + \rho_{m+\alpha(\mu)} \geq c$. To demonstrate condition 3 it suffices to show

$$n - \mu + \rho_m \leq q^3 - q^2. \tag{6.12}$$

Observe that $\rho_m \leq q(q-1)$ which holds because of the assumption that $m \leq q+1$ and $q > 2$ and because the number of gaps in $H(Q)$ equals $q(q-1)/2$. As a consequence the assumption $2q^2 - q \leq \mu$ implies $q^2 + \rho_m \leq \mu$ from which we derive (6.12). □

Proposition 27. *Consider the field* $\mathbb{F}_{q^2}$, *with* $q > 2$. *Let* $3 \leq \widetilde{\mu} \leq q+1$ *be fixed. For* $m = 3, \ldots, \widetilde{\mu}$ *there are at least* $q^3 - 3q^2 + 1$ *different codes* $C_{\mathcal{L}}(D, \mu Q)$ *for which* $d_m(C_{\mathcal{L}}(D, \mu Q)) = n - \mu + \rho_m$ *and simultaneously* $M_m(C_{\mathcal{L}}(D, \mu Q), C_{\mathcal{L}}(D, (\mu - \widetilde{\mu})Q)) = n - \mu + \sum_{i=0}^{m-2}(q-i)$ *hold. For these codes we have*

$$\begin{aligned} M_m(C_{\mathcal{L}}(D, \mu Q), C_{\mathcal{L}}(D, (\mu - \widetilde{\mu})Q)) - d_m(C_{\mathcal{L}}(D, \mu Q)) \\ = \big(\sum_{s=0}^{m-2} (q-s) \big) - \rho_m > 0. \end{aligned} \tag{6.13}$$

Proof. Follows from Theorem 25, Theorem 22 and a study of $H(Q)$. □

Note that if for fixed $\widetilde{\mu}$ we divide the number of different codes $C_{\mathcal{L}}(D, \mu Q)$ for which (6.13) holds by the number of different codes, which is q^3, then we get the ratio $R(q) \geq (q^3 - 3q^2 + 1)/q^3 \geq 1 - 3/q$. This ratio approaches 1 as q approaches infinity. For $q = 4, 5, 7, 8, 9, 16$, and 32, respectively, $R(q)$ is at least 0.25, 0.4, 0.57, 0.62, 0.66, 0.81, and 0.9, respectively. In Table 6.1 for different values of m and q we list the difference between the parameters as expressed in (6.13).

Table 6.1: Diff(m, q) is the value of (6.13).

m	3	4	5	6	7	8	9	10
Diff(m,4)	2	1	1					
Diff(m,5)	3	2	3	3				
Diff(m,7)	5	4	7	9	6	6		
Diff(m,8)	6	5	9	12	9	10	10	
Diff(m,16)	14	13	25	36	33	42	50	57

m	11	12	13	14	15	16	17
Diff(m,16)	51	56	60	63	65	55	55

Chapter 7

Ramp schemes based on Hermitian codes

In this section we consider ramp secret sharing schemes D_1/D_2 where $D_1 = C_2^{\perp}$, $D_2 = C_1^{\perp}$, and $C_2 \subsetneq C_1$ are Hermitian codes over $\mathbb{F}_{q^2}$, with $\dim(C_1) - \dim(C_2) = \widetilde{\mu}$. Recall from Theorem 3 in Section 2 that $t_m + 1 = M_m(C_1, C_2)$, $m = 1, \ldots, \widetilde{\mu}$ is the size of the smallest group that can reveal m q^2-bits of information. Also recall that $r_m = n - M_{\widetilde{\mu}-m+1}(D_1, D_2) + 1$ is the smallest number such that any group of this size can reveal m q^2-bits of information. From Section 6 we know how to determine/estimate $M_m(C_1, C_2)$. Now [42, Th. 1] tells us that for $\mu \in H^*(Q)$ we have $C_{\mathcal{L}}(D, \mu Q)^{\perp} = C_{\mathcal{L}}(D, (n + c - 2 - \mu)Q)$. To establish information on r_m we therefore need not apply Theorem 20 (the theorem for duals of one-point algebraic geometric codes), but can instead use the already established information on the RGHW of $C_2 \subseteq C_1$. From Theorem 22 we get the following result:

Theorem 28. *Let $\mu, \widetilde{\mu}$ be positive integers satisfying*

$$\widetilde{\mu} \leq q + 1, \; c - 1 + \widetilde{\mu} \leq \mu \leq n - 1. \tag{7.1}$$

Consider the ramp secret sharing scheme $D_1/D_2 = C_2^{\perp}/C_1^{\perp}$ where $C_1 = C_{\mathcal{L}}(D, \mu Q)$ and $C_2 = C_{\mathcal{L}}(D, (\mu - \widetilde{\mu})Q)$. The codimension (and thereby the length of the secret) equals $\widetilde{\mu}$. Furthermore for $m = 1, \ldots, \widetilde{\mu}$ it holds that

$$t_m \geq n - \mu + \sum_{s=0}^{m-2} (q - s) - 1, \tag{7.2}$$

$$r_m \leq n - \mu + c + \widetilde{\mu} - 1 - \sum_{s=0}^{\widetilde{\mu}-m-1} (q - s). \tag{7.3}$$

Equality holds simultaneously in (7.2) and (7.3) when the second condition in (7.1) is replaced with

$$2c - 2 + \widetilde{\mu} < \mu < n - c. \tag{7.4}$$

Table 7.1: Parameters of the ramp schemes in Example 4.

m	1	2	3	4	5	6	7	8	9
$G_1(m,8)$	0	8	15	21	26	30	33	35	36
$G_2(m,9,8)$	28	29	31	34	38	43	49	56	64

Table 7.2: Parameters of the ramp schemes in Example 5.

m	1	2	3	4	5	6	7	8
$G_1(m,16)$	0	16	31	45	58	70	81	91
$G_2(m,16,16)$	120	122	125	129	134	140	147	155

m	9	10	11	12	13	14	15	16
$G_1(m,16)$	100	108	115	121	126	130	133	135
$G_2(m,16,16)$	164	174	185	197	210	224	239	255

Example 4. *In this example we consider schemes over* $\mathbb{F}_{64}$. *That is,* $q = 8$ *and the number of participants is* $n = 512$. *The assumption (7.1) for (7.2) and (7.3) to hold is* $\widetilde{\mu} \leq 9$, $55+\widetilde{\mu} \leq \mu \leq 511$, *the latter corresponding to* $1 \leq n-\mu \leq 457-\widetilde{\mu}$. *By (7.4) equality holds simultaneously in (7.2) and (7.3) when* $56 < n-\mu < 402-\widetilde{\mu}$ *holds. In Table 7.1 we list for* $\widetilde{\mu} = q+1$ *the values of* $G_1(m,q) = \sum_{s=0}^{m-2}(q-s)$ *(which is our lower bound on* $(t_m+1)-(n-\mu)$*) and* $G_2(m,\widetilde{\mu},q) = c+\widetilde{\mu}-1-\sum_{s=0}^{\widetilde{\mu}-m-1}(q-s)$ *(which is our upper bound on* $r_m-(n-\mu)$*). Note that* $G_1(m,q) = Z(H(Q),\mu,m)$ *(Lemma 21). For the considered choice of* $\widetilde{\mu}$ *the secret is of size equal to* 9 q^2*-bits. One can get much information from Table 7.1. Assume for instance* $n-\mu = 130$. *Then the smallest group that can derive some information is of size* $130+0 = 130$, *hence* $t_1 = 129$. *The smallest group size for which any group can derive some information is* $r_1 = 130+28 = 158$. *Groups of size* 158 *on the other hand can never obtain more than* 5 q^2*-bits of information as* $G_1(5,8) \leq 158-130 < G_1(6,8)$. *Some group of size* $t_3+1 = 130+15 = 145$ *can derive at least* 3 q^2*-bits of information, however,* $r_3 = 130+31 = 161$ *is the smallest group size guaranteed to reveal* 3 q^2*-bits of information. Any group of size* $r_9 = 130+64 = 194$ *can reveal the entire secret. Some group of size* $t_9+1 = 130+36 = 166$ *can reveal the entire secret whereas other groups of size* 166 *can reveal no more than* 4 q^2*-bits of information.*

Example 5. *In this example we consider schemes over* $\mathbb{F}_{256}$. *That is,* $q = 16$ *and the number of participants is* $n = 4096$. *Assumption (7.1) is* $1 \leq n-\mu < 3857-\widetilde{\mu}$ *and by (7.4) equality holds in (7.2) and (7.3) simultaneously if*

$$240 < n-\mu < 3618-\widetilde{\mu} \tag{7.5}$$

In Table 7.2 we list values of $G_1(m,16)$ *and* $G_2(m,16,16)$ *where the functions* G_1 *and* G_2 *are as in Example 4. Assuming (7.5), then from the table we get the following information: Some groups of size* $t_1+1 = n-\mu$ *may reveal* 1 q^2*-bit of*

information whereas other groups of size $n-\mu+119$ *cannot as* $r_1 = n-\mu+120$. *Some group of size* $t_{11}+1 = n-\mu+115$ *can reveal* 11 q^2*-bits of information whereas some group of the same size can not reveal anything. Any group of size* $n-\mu+135$ *can for sure reveal* 5 q^2*-bits of information and some group of the same size can reveal everything. Any group of size* $r_{16} = n-\mu+255$ *can reveal the entire secret.*

Remark 29. *Assume that (7.1) holds and let* $m \leq \widetilde{\mu}$. *The difference between the smallest size for which any group can reveal* m q^2*-bits of information and the smallest size for which some group can reveal* m q^2*-bits of information equals* $(n - M_{\widetilde{\mu}+1-m}(C_2^{\perp}, C_1^{\perp}) + 1) - M_m(C_1, C_2)$ *which is at most*

$$c + \widetilde{\mu} - 1 - \sum_{s=0}^{\widetilde{\mu}-m-1} (q-s) - \sum_{s=0}^{m-2} (q-s) \tag{7.6}$$

(with equality if $2c - 2 + \widetilde{\mu} < \mu < n - c$*). The maximum of (7.6) is attained at* $m = 1$ *and* $m = \widetilde{\mu}$. *The corresponding "worst-case" difference equals* $c + \widetilde{\mu} - 1 - \frac{\widetilde{\mu}-1}{2}(2q - \widetilde{\mu} + 2)$. *This number is highest possible when* $\widetilde{\mu} = q$ *and* $\widetilde{\mu} = q+1$, *in which case it equals the genus* $g = (q^2 - q)/2$.

We conclude the section with an example in which we show how to improve upon (7.2) and (7.3) when the condition (7.4) is not satisfied.

Example 6. *In this example we consider schemes over* $\mathbb{F}_{16}$. *That is,* $q = 4$ *and the number of participants is* $n = 64$. *We consider secrets of length* 3. *Hence, we require that*

$$\dim(C_1 = C_{\mathcal{L}}(D, \mu_1 Q)) - \dim(C_2 = C_{\mathcal{L}}(D, \mu_2 Q)) = 3.$$

We have

$$\begin{aligned} H^*(Q) \;\; = \;\; & \{0, 4, 5, 8, 9, 10, 12, 13, \cdots, \\ & 62, 63, 65, 66, 67, 70, 71, 75\} \end{aligned}$$

and therefore without loss of generality the possible choices of (μ_1, μ_2) *are* $\{(\mu_1^{(1)}, \mu_2^{(1)}),$ $\ldots,$ $(\mu_1^{(62)}, \mu_2^{(62)})\} = \{(5,-1),$ $(8,0),$ $(9,4),$ $(10,5),$ $(12,8),$ $(13,9),$ $(14,10),$ $(15,12),$ $\ldots,$ $(63,60),$ $(65,61),$ $(66,62),$ $(67,63),$ $(70,65),$ $(71,66),$ $(75,67)\}$, *where for* $(5,-1)$ *we mean that* C_2 *equals* $\{\vec{0}\}$. *In the following we calculate*

$$\begin{aligned} t_m \;\; &= \;\; M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) - 1, \\ r_m \;\; &= \;\; n - M_{\mu_2-\mu_1-m+1}(C_{\mathcal{L}}(D, (n+c-2-\mu_2)Q), \\ &\qquad C_{\mathcal{L}}(D, (n-c+2-\mu_1)Q)) + 1 \\ &= \;\; n - M_{\mu_2-\mu_1-m+1}(C_{\mathcal{L}}(D, (74-\mu_2)Q), \\ &\qquad C_{\mathcal{L}}(D, (74-\mu_1)Q)) + 1, \end{aligned}$$

$m = 1, 2, 3$, *for all the above choices of* (μ_1, μ_2).

Recall from the discussion prior to Example 1 in Section 6 that for some choices of (μ_1, μ_2) we may achieve better estimates on the RGHW than (6.2). This is done by applying the method of Example 1 and Example 3 which corresponds to (5.8) and (5.7), respectively. Specifically for $\mu_1 = 5, 8, 9, 10, 12, 13$ we do not have

$$\{\mu_1, \mu_1 - 1, \mu_1 - 2\} \subseteq H^*(Q) \tag{7.7}$$

and to calculate t_m we therefore apply the method of Example 1. By inspection, for $\mu_1 = 53$, 57, 58, 61, 62, 63, 65, 66, 67, 70, 71, 75 we have that $H^*(Q)\backslash(\mu_1 + H(Q))$ is strictly smaller than $H(Q)\backslash(\mu_1 + H(Q))$ and also for some of these values, (7.7) does not hold either. Hence, we apply the method of Example 3. In conclusion the values of μ_1 for which we can potentially obtain improved information on t_m are

$$\begin{aligned} S_1 &= \{\mu_1^{(1)}, \mu_1^{(2)}, \ldots, \mu_1^{(6)}, \\ &\quad \mu_1^{(46)}, \mu_1^{(50)}, \mu_1^{(51)}, \mu_1^{(54)}, \mu_1^{(55)}, \ldots, \mu_1^{(62)}\} \\ &= \{5, 8, 9, 10, 12, 13, \\ &\quad 53, 57, 58, 61, 62, 63, 65, 66, 67, 70, 71, 75\}. \end{aligned} \tag{7.8}$$

We next discuss r_m. Here, a little care is needed in the analysis: as an example for $(\mu_1, \mu_2) = (\mu_1^{(4)}, \mu_2^{(4)}) = (10, 5)$ we have $C_2^{\perp} = C_{\mathcal{L}}(D, (74 - \mu_2)Q) = C_{\mathcal{L}}(D, 69Q)$, but this code is the same as $C_{\mathcal{L}}(D, 67Q)$ because 68 and 69 do not belong to $H^*(Q)$. This phenomenon corresponds to the fact that actually $C_{\mathcal{L}}(D, \mu_2^{(s)}Q)^{\perp} = C_{\mathcal{L}}(D, \mu_1^{(63-s)}Q)$, $s = 1, \ldots, 62$. Hence, from (7.8) we see that the values of μ_1 for which we can potentially derive improved information regarding r_m are

$$\begin{aligned} S_2 &= \{\mu_1^{(63-1)}, \ldots, \mu_1^{(63-6)}, \mu_1^{(63-46)}, \mu_1^{(63-50)}, \mu_1^{(63-51)}, \\ &\quad \mu_1^{(63-54)}, \ldots, \mu_1^{(63-62)}\} \\ &= \{5, 8, 9, 10, 12, 13, 14, 15, 16, \\ &\quad 19, 20, 24, 65, 66, 67, 70, 71, 75\}. \end{aligned}$$

Applying a mixture of the method from Example 1 and Example 3 plus (6.2) we derive for $\mu_1 \in S_1 \cup S_2$ the information given in Table 7.3.

For the remaining values of μ_1, that is for

$$\begin{aligned} \mu_1 &\in \{5, 8, 9, 10, 12, \ldots, 63, 65, 66, 67, 70, 71, 75\} \\ &\quad \backslash(S_1 \cup S_2) \\ &= \{17, 18, 21, 22, 23, 25, 26, 27, \ldots, \\ &\quad 51, 52, 54, 55, 56, 59, 60\} \end{aligned}$$

we have $\mu_2 = \mu_1 - 3$, and the best bounds (sometimes tight) are obtained from (6.2). They are: $[t_1 \geq n - \mu_1 - 1, r_1 \leq n - \mu_1 + 7]$, $[t_2 \geq n - \mu_1 + 3, r_2 \leq n - \mu_1 + 10]$ and $[t_3 \geq n - \mu_1 + 6, r_3 \leq n - \mu_1 + 14]$.

Table 7.3: Lower bounds on t_m and upper bounds on r_m for the schemes in Example 6.

μ_1	5	8	9	10	12	13
$[t_1, r_1]$	[58,62]	[55,61]	[54,60]	[53,59]	[51,58]	[50,57]
$[t_2, r_2]$	[62,63]	[59,62]	[58,61]	[57,60]	[57,60]	[54,59]
$[t_3, r_3]$	[63,64]	[62,63]	[61,63]	[60,62]	[59,62]	[58,62]

μ_1	14	15	16	19	20	24
$[t_1, r_1]$	[49,56]	[48,56]	[47,55]	[44,52]	[43,51]	[39,47]
$[t_2, r_2]$	[53,58]	[52,58]	[51,58]	[48,54]	[47,54]	[43,50]
$[t_3, r_3]$	[56,61]	[55,61]	[54,61]	[51,57]	[50,57]	[46,53]

μ_1	53	57	58	61	62	63
$[t_1, r_1]$	[11,18]	[7,14]	[7,13]	[3,10]	[3,9]	[3,8]
$[t_2, r_2]$	[14,21]	[10,17]	[10,16]	[6,13]	[6,12]	[6,11]
$[t_3, r_3]$	[17,25]	[13,21]	[12,20]	[9,17]	[8,16]	[8,15]

μ_1	65	66	67	70	71	75
$[t_1, r_1]$	[2,6]	[2,5]	[2,4]	[1,3]	[1,2]	[0,1]
$[t_2, r_2]$	[5,10]	[4,7]	[4,7]	[3,6]	[2,5]	[1,2]
$[t_3, r_3]$	[7,14]	[6,13]	[5,11]	[4,10]	[3,9]	[2,6]

Acknowledgments

The authors would like to thank Ignacio Cascudo, Hao Chen, Ronald Cramer and Carlos Munuera for pleasant discussions. Also the authors would like to thank the anonymous reviewers for valuable comments that helped us improve the paper.

Bibliography

[1] H. E. Andersen and O. Geil, "Evaluation codes from order domain theory," *Finite Fields Appl.*, vol. 14, no. 1, pp. 92–123, 2008.

[2] T. Bains, "Generalized Hamming weights and their applications to secret sharing schemes," Master's thesis, Univ. Amsterdam, 2008.

[3] A. I. Barbero and C. Munuera, "The weight hierarchy of Hermitian codes," *SIAM J. Discrete Math.*, vol. 13, no. 1, pp. 79–104, 2000. [Online]. Available: `http://dx.doi.org/10.1137/S089548019834342X`

[4] G. R. Blakley and C. Meadows, "Security of ramp schemes," in *Advances in cryptology (Santa Barbara, Calif., 1984)*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 1985, vol. 196, pp. 242–268.

[5] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, "On the size of shares for secret sharing schemes," *Journal of Cryptology*, vol. 6, no. 3, pp. 157–167, 1993.

[6] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, "Secure computation from random error correcting codes," in *Advances in cryptology—EUROCRYPT 2007*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 2007, vol. 4515, pp. 291–310.

[7] L. Csirmaz, "Ramp secret sharing and secure information storage," 2009, presented at IntelliSec'09. Available from `http://eprints.renyi.hu/19/`.

[8] A. Del Centina, "Weierstrass points and their impact in the study of algebraic curves: a historical account from the lückensatz to the 1970s," *Annali dell'Università di Ferrara*, vol. 54, no. 1, pp. 37–59, 2008.

[9] I. M. Duursma and S. Park, "Coset bounds for algebraic geometric codes," *Finite Fields Appl.*, vol. 16, no. 1, pp. 36–55, 2010. [Online]. Available: `http://dx.doi.org/10.1016/j.ffa.2009.11.006`

[10] G. L. Feng and T. R. N. Rao, "Decoding algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 39, no. 1, pp. 37–45, 1993.

[11] ——, "A simple approach for construction of algebraic-geometric codes from affine plane curves," *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1003–1012, 1994.

[12] ——, "Improved geometric Goppa codes part I: Basic theory," *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1678–1693, 1995.

[13] G. D. J. Forney, "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 6, pp. 1741–1752, Nov 1994.

[14] O. Geil and S. Martin, "Further improvements on the Feng-Rao bound for dual codes," *Finite Fields Appl.*, vol. 30, pp. 33–48, 2014.

[15] ——, "An improvement of the Feng–Rao bound for primary codes," *Des. Codes Cryptogr.*, 2014, dOI: 10.1007/s10623-014-9983-z. To appear. [Online]. Available: `arXiv:1307.3107`

[16] O. Geil, S. Martin, R. Matsumoto, D. Ruano, and L. Yuan, "Relative generalized Hamming weights of one-point algebraic geometric codes," Apr. 2014, to appear in Proc. IEEE Information Theory Workshop (ITW 2014).

[17] O. Geil, R. Matsumoto, and D. Ruano, "Feng-Rao decoding of primary codes," *Finite Fields Appl.*, vol. 23, pp. 35–52, 2013.

[18] O. Geil, C. Munuera, D. Ruano, and F. Torres, "On the order bounds for one-point AG codes," *Adv. Math. Commun.*, vol. 5, no. 3, pp. 489–504, 2011. [Online]. Available: `http://dx.doi.org/10.3934/amc.2011.5.489`

[19] O. Geil and R. Pellikaan, "On the structure of order domains," *Finite Fields Appl.*, vol. 8, no. 3, pp. 369–396, 2002.

[20] O. Geil and C. Thommesen, "On the Feng-Rao bound for generalized Hamming weights," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, ser. Lecture Notes in Computer Science, M. P. C. Fossorier, H. Imai, S. Lin, and A. Poli, Eds. Springer, 2006, vol. 3857, pp. 295–306.

[21] P. Heijnen and R. Pellikaan, "Generalized Hamming weights of q-ary Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 44, no. 1, pp. 181–196, 1998.

[22] T. Høholdt, J. H. van Lint, and R. Pellikaan, "Algebraic geometry codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam: Elsevier, 1998, vol. 1, pp. 871–961.

[23] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*. Cambridge university press Cambridge, 2003, vol. 22.

[24] A. Hürwitz, "Über algebraische Gebilde mit eindeutigen Transformationen in sich," *Math. Ann*, vol. 41, no. 3, pp. 403–442, 1892.

[25] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Electron. Comm. Jpn. Pt. III*, vol. 72, no. 9, pp. 56–63, 1989. [Online]. Available: doi:10.1002/ecjc.4430720906

[26] M. Iwamoto and H. Yamamoto, "Strongly secure ramp secret sharing schemes for general access structures," *Inform. Process. Lett.*, vol. 97, no. 2, pp. 52–57, Jan. 2006. [Online]. Available: doi:10.1016/j.ipl.2005.09.012

[27] J. Kurihara, R. Matsumoto, and T. Uyematsu, "Relative generalized rank weight of linear codes and its applications to network coding," 2013. [Online]. Available: arxiv:1301.5482

[28] J. Kurihara, T. Uyematsu, and R. Matsumoto, "Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight," *IEICE Trans. Fundamentals*, vol. E95-A, no. 11, pp. 2067–2075, Nov. 2012. [Online]. Available: doi:10.1587/transfun.E95.A.2067

[29] Z. Liu, W. Chen, and Y. Luo, "The relative generalized Hamming weight of linear q-ary codes and their subcodes," *Des. Codes Cryptogr.*, vol. 48, no. 2, pp. 111–123, 2008. [Online]. Available: http://dx.doi.org/10.1007/s10623-008-9170-1

[30] Y. Luo, C. Mitrpant, A. J. H. Vinck, and K. Chen, "Some new characters on the wire-tap channel of type II," *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 1222–1229, 2005. [Online]. Available: http://dx.doi.org/10.1109/TIT.2004.842763

[31] J. L. Massey, "Some applications of coding theory in cryptography," in *Codes and Ciphers: Cryptography and Coding IV*, 1995, pp. 33–47.

[32] R. Matsumoto and S. Miura, "On the Feng-Rao bound for the $\mathcal{L}$-construction of algebraic geometry codes," *IEICE Trans. Fundamentals*, vol. E83-A, no. 5, pp. 926–930, May 2000. [Online]. Available: http://www.rmatsumoto.org/repository/e83-a_5_923.pdf

[33] C. Munuera and D. Ramirez, "The second and third generalized Hamming weights of Hermitian codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 709–712, 1999. [Online]. Available: http://dx.doi.org/10.1109/18.749019

[34] W. Olaya-León and C. Munuera, "On the minimum distance of castle codes," *Finite Fields Appl.*, vol. 20, pp. 55–63, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.ffa.2012.12.001

[35] M. E. O'Sullivan, "New codes for the Berlekamp-Massey-Sakata algorithm," *Finite Fields Appl.*, vol. 7, no. 2, pp. 293–317, 2001. [Online]. Available: http://dx.doi.org/10.1006/ffta.2000.0283

[36] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Advances in cryptology (Paris, 1984)*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 1985, vol. 209, pp. 33–50. [Online]. Available: http://dx.doi.org/10.1007/3-540-39757-4_5

[37] R. Pellikaan, "On the efficient decoding of algebraic-geometric codes," *Eurocode*, vol. 92, pp. 231–253, 1993.

[38] G. Salazar, D. Dunn, and S. B. Graham, "An improvement of the Feng-Rao bound on minimum distance," *Finite Fields Appl.*, vol. 12, pp. 313–335, 2006.

[39] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[40] H. Stichtenoth, "A note on Hermitian codes over GF(q^2)," *Information Theory, IEEE Transactions on*, vol. 34, no. 5, pp. 1345–1348, 1988.

[41] A. Subramanian and S. W. McLaughlin, "MDS codes on the erasure-erasure wiretap channel," *arXiv preprint arXiv:0902.3286*, 2009.

[42] H. J. Tiersma, "Remarks on codes from Hermitian curves," *IEEE Trans. Inform. Theory*, vol. 33, no. 4, pp. 605–609, 1987. [Online]. Available: `http://dx.doi.org/10.1109/TIT.1987.1057327`

[43] M. Tsfasman and S. G. Vladut, *Algebraic-geometric codes*. Kluwer Academic Publishers, 1991.

[44] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 5, pp. 1412–1418, 1991.

[45] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[46] H. Yamamoto, "Secret sharing system using (k, L, n) threshold scheme," *Electron. Comm. Jpn. Pt. I*, vol. 69, no. 9, pp. 46–54, 1986. [Online]. Available: `doi:10.1002/ecja.4410690906`

[47] K. Yang and P. V. Kumar, "On the true minimum distance of Hermitian codes," in *Coding theory and algebraic geometry*. Springer, 1992, pp. 99–107.

[48] Z. Zhuang, Y. Luo, and B. Dai, "Code constructions and existence bounds for relative generalized Hamming weight," *Des. Codes Cryptogr.*, vol. 69, no. 3, pp. 275–297, dec 2013.

PAPER V

Relative generalized Hamming weights of q-ary Reed-Muller codes

Martin Stefano Geil Olav

Martin Stefano and Geil Olav, "Relative generalized Hamming weights of q-ary Reed-Muller codes", *submitted*, 2014, preprint at arXiv:1407.6185v2 [cs.IT]

Relative generalized Hamming weights of q-ary Reed-Muller codes

Stefano Martin[1] and Olav Geil[2]

Department of Mathematical Sciences, Aalborg University, Denmark

[1]stefano@math.aau.dk
[2]olav@math.aau.dk

Abstract

Coset constructions C_1/C_2, where $C_2 \subsetneq C_1$ are linear codes, serve as useful primitives in connection with wire-tap channels of type II and ramp secret sharing. The corresponding relative generalized Hamming weights describe the information leakage and security, respectively [2, 19, 17, 10]. In this paper we show how to compute relative generalized Hamming weights when both the involved codes are q-ary Reed-Muller codes. Our work is a non-trivial extension of material in [13] on generalized Hamming weights.

Keywords: q-ary Reed-Muller code, relative generalized Hamming weight, secret sharing, wire-tap channel of type II

Chapter 1

Introduction

Relative generalized Hamming weights (RGHWs) are useful tools for estimating the information leakage from wire-tap channels of type II when linear codes are used [19]. Similarly they describe the security in linear ramp secret sharing schemes [2, 17, 10]. We shall give a brief overview of their use in connection with secret sharing schemes. A linear ramp secret sharing scheme with n participants, secrets in $(\mathbb{F}_q)^\ell$, and shares belonging to $\mathbb{F}_q$ can be described as follows [5]. Consider linear codes $C_2 \subsetneq C_1 \subset (\mathbb{F}_q)^n$ with $\ell = \dim(C_1) - \dim(C_2)$ and let $L \subseteq (\mathbb{F}_q)^n$ be (a linear code) such that $C_1 = L \oplus C_2$, where $\oplus$ is the direct sum. Consider a vector space isomorphism $\psi : (\mathbb{F}_q)^\ell \to L$. A secret $\vec{s} \in (\mathbb{F}_q)^\ell$ is mapped to $\vec{x} = \psi(\vec{s}) + \vec{c}_2 \in C_1$, where $\vec{c}_2 \in C_2$ is chosen by random. The n shares distributed among the n participants are the n coordinates of $\vec{x}$. The parameters t and r of the scheme are the unique numbers such that:

1. No group of t participants can recover any information about $\vec{s}$, but some groups of size $t+1$ can.

2. All groups of size r can recover the secret in full, but some groups of size $r-1$ cannot.

Only for $\ell = 1$ we can hope for $r = t+1$ in which case we have a complete picture of the security. Such schemes are called t-threshold secret sharing schemes. For general linear ramp secret sharing schemes we have the parameters $t_1, \ldots, t_\ell, r_1, \ldots, r_\ell$ where for $m = 1, \ldots, \ell$, t_m and r_m are the unique numbers such that the following hold:

1. No group of t_m participants can recover m q-bits of information about $\vec{s}$, but some groups of size $t_m + 1$ can.

2. All groups of size r_m can recover m q-bits of information about $\vec{s}$, but some groups of size $r_m - 1$ cannot.

Clearly, $t = t_1$ and $r = r_\ell$. From [2, Th. 6.7], [17, Th. 4] and [10, Th. 6] we have the following characterization of these parameters:

$$t_m = M_m((C_2)^\perp, (C_1)^\perp) - 1 \tag{1.1}$$
$$r_m = n - M_{\ell-m+1}(C_1, C_2) + 1, \tag{1.2}$$

where $M_m(C_1, C_2)$ is the m-th relative generalized Hamming weight for C_1 with respect to C_2 and $(C)^\perp$ denotes the dual code of C.
Unfortunately, it is not easy to find the hierarchy of RGHWs of two general linear codes and only for a few classes of codes these parameters have been found or estimated. Actually – until recently – only for a single class of codes the parameters were known, namely MDS codes for which the situation is particular simple [19]. Recently a general method for estimating RGHWs of one-point algebraic geometric codes was proposed in [10] leading to a bound for Hermitian codes which is tight in some cases. In the present paper we show how to calculate RGHWs when both C_1 and C_2 are q-ary Reed-Muller codes. Such codes are particularly suited for secret sharing as the dual of a q-ary Reed-Muller code is also a q-ary Reed-Muller code – and by (1.1) and (1.2) we therefore can determine t_m as well as r_m, $m = 1, \ldots, \ell$. Also if one wants to apply such a scheme for the purpose of secure multiparty computation [7, 8, 4, 9] then one would need to know the product $C^2 = C * C$ of the involved codes. Here, $C^2 = \{\vec{a} * \vec{b} \mid \vec{a}, \vec{b} \in C\}$ where for $\vec{a} = (a_1, \ldots, a_n)$, $\vec{b} = (b_1, \ldots, b_n)$, $\vec{a} * \vec{b} = (a_1 b_1, \ldots, a_n b_n)$. Also one might need to know higher powers C^p. For a q-ary Reed-Muller code C the code C^p is again a q-ary Reed-Muller code which is easy to determine.
Our work is a non-trivial generalization of results by Heijnen and Pellikaan [13] who showed how to calculate generalized Hamming weights of q-ary Reed-Muller codes. Similar to Heijnen and Pellikaan we propose a low complexity method to derive the parameters, and for the situation where the codes are defined from polynomials in two variables we furthermore give closed formula expressions.

The paper is organized as follows. In Section 2 we introduce RGHWs and show how to estimate them using the footprint bound from Gröbner basis theory. This method is then applied to q-ary Reed-Muller codes in Section 3. In Section 4 we elaborate on the method and formalize our findings into an algorithm. For the special case of q-ary Reed-Muller codes defined from polynomials in two variables we then in Section 5 provide closed formula expressions. Finally, Section 6 is the conclusion.

Chapter 2

Relative generalized Hamming weights

In this section we give the definition of relative generalized Hamming weights. We also introduce the footprint bound which will be useful when we want to calculate the RGHWs of q-ary Reed-Muller codes and we take the first step in this direction. A well-know concept in coding theory is the generalized Hamming weights [16, 14, 22] which we start by introducing. Recall that for $D \subseteq (\mathbb{F}_q)^n$ the support of D is defined as

$$\operatorname{supp}(D) = \{i \mid c_i \neq 0 \text{ for some } \vec{c} = (c_1, \ldots, c_n) \in D\}.$$

Definition 1. *Let C be a linear code and k its dimension. For $r = 1, \ldots, k$, the r-th generalized Hamming weight (GHW) of C is defined by*

$$d_r(C) = \min\{|\operatorname{supp}(D)| \mid D \text{ is a linear subcode of } C, \dim(D) = r\}.$$

The sequence $(d_1(C), \ldots, d_k(C))$ is called the hierarchy of the GHWs of C.

In particular $d_1(C)$ is the minimum distance of C. The problem of computing the GHWs for binary Reed-Muller codes was solved in [22] and for general q-ary Reed-Muller codes in [13]. A further generalization of GHWs was introduced by Luo et al. in [19].

Definition 2. *Let $C_2 \subsetneq C_1$ be linear codes, $\ell = \dim(C_1) - \dim(C_2)$ the codimension of C_1 and C_2, and n the length of the codes. For $m = 1, \ldots, \ell$, the m-th relative generalized Hamming weight (RGHW) of C_1 with respect to C_2 is defined by*

$$M_m(C_1, C_2) = \min_{J \subseteq \{1,\ldots,n\}} \{|J| \mid \dim((C_1)_J) - \dim((C_2)_J) = m\}$$

where $(C_i)_J = \{\vec{c} \in C_i \mid c_t = 0 \text{ for } t \notin J\}$ for $i = 1, 2$. The sequence $(M_1(C_1, C_2), \ldots, M_\ell(C_1, C_2))$ is called the hierarchy of the RGHWs of C_1 with respect to C_2.

If C_2 is the zero code $\{\vec{0}\}$ then the m-th RGHW of C_1 with respect to C_2 is equivalent to the m-th GHW of C_1. This fact should be more clear from the following result [18, Lem. 1].

Theorem 3. *Let $C_2 \subsetneq C_1$ be linear codes and $\ell = \dim(C_1) - \dim(C_2)$ be the codimension of C_1 and C_2. For $m = 1, \ldots, \ell$ we have that*

$$M_m(C_1, C_2) = \min\{|\mathrm{supp}(D)| \mid D \text{ is a linear subcode of } C_1, \\ D \cap C_2 = \{\vec{0}\} \text{ and } \dim(D) = m\}.$$

This alternative characterization of RGHWs is useful when one considers q-ary Reed-Muller codes which we now define.

Definition 4. *Let q be a power of a prime, u an integer, s a positive integer, and write $n = q^s$. We enumerate the elements of $(\mathbb{F}_q)^s$ as $\{P_1, \ldots, P_n\}$ and consider the evaluation map $\varphi : \mathbb{F}_q[X_1, \ldots, X_s] \to (\mathbb{F}_q)^n$, $\varphi(f) = (f(P_1), \ldots, f(P_n))$. The q-ary Reed-Muller code of order u in s variables is defined by*

$$\begin{aligned} RM_q(u, s) &= \{\varphi(f) : f \in \mathbb{F}_q[X_1, \ldots, X_s], \deg(f) \leq u\} \\ &= \mathrm{span}_{\mathbb{F}_q}\{\varphi(X_1^{a_1} \cdots X_s^{a_s}) \mid 0 \leq a_1, \ldots, a_s < q, a_1 + \cdots + a_s \leq u\} \end{aligned} \tag{2.1}$$

In this paper we shall use the convention $\deg(0) = -1$ and $\mathrm{span}_{\mathbb{F}_q}\{\} = \{\vec{0}\}$. Hence $RM_q(-1, s) = \{\vec{0}\}$.

Throughout the rest of the paper we shall always write $n = q^s$. Observe that the equality in (2.1) is a consequence of the fact that

$$\varphi(f) = \varphi(f \text{ rem } \{X_1^q - X_1, \ldots, X_s^q - X_s\}) \tag{2.2}$$

for any $f \in \mathbb{F}_q[X_1, \ldots, X_s]$. Here, the argument on the right side of (2.2) means the remainder of f after division with $\{X_1^q - X_1, \ldots, X_s^q - X_s\}$ (see [6, Sec. 2.3] for the multivariate division algorithm). Furthermore note that φ is surjective which is seen by applying Lagrange interpolation. Dimension considerations now show that the restriction of φ to the span of

$$R_q^s = \{X_1^{a_1} \cdots X_s^{a_s} \mid 0 \leq a_i < q, i = 1, \ldots, s\}$$

is a bijection and $\{\varphi(M) \mid M \in R_q^s\}$ therefore is a basis for $(\mathbb{F}_q)^n$ as a vector space. We write

$$Q_q^s = \{(a_1, \ldots, a_s) \in \mathbb{N}_0^s \mid 0 \leq a_i < q, i = 1, \ldots, s\}$$

and $\vec{X}^{\vec{a}} = X_1^{a_1} \cdots X_s^{a_s}$ for $\vec{a} = (a_1, \ldots, a_s) \in \mathbb{N}_0^s$. Hence, $R_q^s = \{\vec{X}^{\vec{a}} \mid \vec{a} \in Q_q^s\}$.

Remark 5. *From the above discussion we conclude that if $D \subseteq RM_q(u, s)$ is a subspace of dimension m then without loss of generality we may assume that $D = span_{\mathbb{F}_q}\{\varphi(F_1), \ldots, \varphi(F_m)\}$ where the leading monomials (with respect to the given fixed monomial ordering $\prec$) satisfy $lm(F_i) \in R_q^s$, $lm(F_i) \neq lm(F_j)$ for $i \neq j$, and $\deg(F_i) \leq u$ for $i = 1, \ldots m$. For given D and fixed $\prec$ these leading monomials are unique.*

We could calculate the RGHWs of q-ary Reed-Muller codes using the technique from [10] where the Feng-Rao bound for primary codes is employed. However, the simple algebraic structure of the q-ary Reed-Muller codes suggests that instead we should apply the footprint bound which we now introduce.

Definition 6. *Let k be a field and consider an ideal $J \subseteq k[X_1, \ldots, X_s]$ and a fixed monomial ordering $\prec$. Let $\mathcal{M}(X_1, \ldots, X_s)$ denote the set of monomials in the variables $X_1, \ldots, X_s$. The footprint of J with respect to $\prec$ is the set*

$$\Delta_\prec(J) = \{M \in \mathcal{M}(X_1, \ldots, X_s) \mid M \text{ is not the leading monomial of any polynomial in } J\}.$$

Example 1. *We see immediately that $\Delta_\prec(\langle X_1^q - X_1, \ldots, X_s^q - X_s\rangle) \subseteq R_q^s$.*

From [6, Th. 6] we have the following well-known result.

Theorem 7. *Let the notation be as in Definition 6. The set $\{M+J \mid M \in \Delta_\prec(J)\}$ is a basis for $k[X_1, \ldots, X_s]/J$ as a vector space over k.*

Example 2. *This is a continuation of Example 1. From Theorem 7 and the fact that $\varphi : R_q^s \to (\mathbb{F}_q)^n$ is a bijection we conclude $\Delta_\prec(\langle X_1^q - X_1, \ldots, X_s^q - X_s\rangle) = R_q^s$.*

Consider polynomials $F_1, \ldots, F_m \in \mathbb{F}_q[X_1, \ldots, X_s]$. Let $\{Q_1, \ldots, Q_N\}$ be their common zeros over $\mathbb{F}_q$ and define the vector space homomorphism $\psi : \mathbb{F}_q[X_1, \ldots, X_s] \to (\mathbb{F}_q)^N$, $\psi(f) = (f(Q_1), \ldots, f(Q_s))$. This map is surjective (Lagrange interpolation again) and as a corollary to Theorem 7 we therefore obtain the following incidence of the footprint bound. (For the general version of the footprint bound see [15] and [6, Pro. 8, Sec. 5.3]).

Lemma 8. *Let $F_1, \ldots, F_m \in \mathbb{F}_q[X_1, \ldots, X_s]$. The number of common zeros of $F_1, \ldots, F_m$ over $\mathbb{F}_q$ is at most equal to $|\Delta_\prec(\langle F_1, \ldots, F_m, X_1^q - X_1, \ldots, X_s^q - X_s\rangle)|$ (here, $\prec$ is any monomial ordering).*

We note that actually equality holds in Lemma 8 (see [6, Pro. 8, Sec. 5.3]), but we shall not need this fact. To make Lemma 8 operational we recall the following notation from [3].

Definition 9. *The partial ordering $\preceq_{\mathrm{P}}$ on the monomials in R_q^s and on the elements in Q_q^s is defined by*

$$\vec{X}^{\vec{a}} \preceq_{\mathrm{P}} \vec{X}^{\vec{b}} \text{ (or } \vec{a} \preceq_{\mathrm{P}} \vec{b}) \iff a_i \leq b_i \text{ for all } i \in \{1, \ldots, s\}.$$

The upward shadow of $\vec{a} \in Q_q^s$ is $\nabla\vec{a} = \{\vec{b} \in Q_q^s \mid \vec{b} \succeq_{\mathrm{P}} \vec{a}\}$.
The lower shadow of $\vec{a} \in Q_q^s$ is $\Delta\vec{a} = \{\vec{b} \in Q_q^s \mid \vec{b} \preceq_{\mathrm{P}} \vec{a}\}$.
Let $A \subseteq Q_q^s$, we define $\nabla A = \bigcup_{\vec{a} \in A} \nabla\vec{a}$ and $\Delta A = \bigcup_{\vec{a} \in A} \Delta\vec{a}$.

Example 3. *For $\vec{a} = (2, 3) \in Q_4^2$ we have that*

$$\nabla\vec{a} = \{(2, 3), (3, 3)\}$$

$$\Delta\vec{a} = \{(2, 3), (1, 3), (0, 3), (2, 2), (1, 2), (0, 2), (2, 1), (1, 1), (0, 1), (2, 0), (1, 0), (0, 0)\}.$$

The partial ordering is not a total ordering; for example we neither have $(3, 2) \preceq_{\mathrm{P}} (2, 3)$ nor $(3, 2) \succeq_{\mathrm{P}} (2, 3)$.

An important tool for calculating RGHWs of q-ary Reed-Muller codes is the following corollary to Lemma 8.

Corollary 10. *Consider any monomial ordering and let* $D = \operatorname{span}_{\mathbb{F}_q}\{\varphi(F_1), \ldots, \varphi(F_m)\}$ *be a subspace of* $(\mathbb{F}_q)^n$ *of dimension* m *where without loss of generality we assume* $\operatorname{lm}(F_i) = \vec{X}^{\vec{a}_i} \in R_q^s$ *for* $i = 1, \ldots, m$ *and* $\vec{a}_i \neq \vec{a}_j$ *for* $i \neq j$ *(Remark 5). Writing* $A = \{\vec{a}_1, \ldots, \vec{a}_m\}$ *we have* $|\operatorname{supp}(D)| \geq |\nabla A|$.

Proof. The elements of D are linear combination of $\varphi(F_1), \ldots, \varphi(F_m)$, hence $|\operatorname{supp}(D)|$ equals the length n minus the number of common zeros of $F_1, \ldots, F_m$ over $\mathbb{F}_q$. By Lemma 8 we get

$$\begin{aligned}
& |\operatorname{supp}(D)| \\
\geq\ & n - |\Delta_\prec(\langle F_1, \ldots, F_m, X_1^q - X_1, \ldots, X_s^q - X_s\rangle)| \\
\geq\ & n - \Big|\Big(\Delta_\prec(\langle X_1^q - X_1, \ldots, X_s^q - X_s\rangle) \\
& \setminus \cup_{i=1}^m \{\vec{X}^{\vec{a}} \in \Delta_\prec(\langle X_1^q - X_1, \ldots, X_s^q - X_s\rangle) \mid \vec{X}^{\vec{a}} \text{ is divisible by } \vec{X}^{\vec{a}_i}\}\Big)\Big| \\
=\ & n - |R_q^s| + |\bigcup_{i=1}^m \{\vec{a} \in Q_q^s \mid \vec{a} \succeq_{\mathrm{P}} \vec{a}_i\}| = |\bigcup_{i=1}^m \nabla\vec{a}_i| = |\nabla A|
\end{aligned}$$

and the proof is complete. □

Interestingly for any choice of A as in Corollary 10 there exists some subspaces D for which the bound is sharp.

Proposition 11. *Consider any monomial ordering and* $A = \{\vec{a}_1, \ldots, \vec{a}_m\} \subseteq Q_q^s$ *where* $\vec{a}_i \neq \vec{a}_j$ *for* $i \neq j$. *Then*

$$\min\{|\operatorname{supp}(D)| \mid D = \operatorname{span}_{\mathbb{F}_q}\{\varphi(F_1), \ldots, \varphi(F_m)\} \text{ for some } F_1, \ldots, F_m \text{ with } lm(F_i) = \vec{X}^{\vec{a}_i}, i = 1, \ldots, m\} = |\nabla A|.$$

Proof. From Corollary 10 we know that

$$\min\{|\operatorname{supp}(D)| \mid D = \operatorname{span}_{\mathbb{F}_q}\{\varphi(F_1), \ldots, \varphi(F_m)\} \text{ for some } F_1, \ldots, F_m \text{ with } \operatorname{lm}(F_i) = \vec{X}^{\vec{a}_i}, i = 1, \ldots, m\} \geq |\nabla A|.$$

Now we want to prove the other inequality. Let $\mathbb{F}_q = \{\gamma_0, \ldots, \gamma_{q-1}\}$ and $\vec{a} = (a_1, \ldots, a_s) \in Q_q^s$, we write $\vec{\gamma}_{\vec{a}} = (\gamma_{a_1}, \ldots, \gamma_{a_s})$. For $i = 1, \ldots, m$, we write the coordinates of $\vec{a}_i$ as $(a_{i,1}, a_{i,2}, \ldots, a_{i,s})$. We define the following subspace of $(\mathbb{F}_q)^n$:

$$\tilde{D} = \operatorname{span}_{\mathbb{F}_q}\{\varphi(G_1), \ldots, \varphi(G_m)\} \text{ with}$$

$$G_i = \prod_{t=1}^{s} \prod_{j=0}^{a_{i,t}-1} (X_t - \gamma_j) \text{ for } i = 1, \ldots, m.$$

For $i = 1, \ldots, m$ we have $\mathrm{lm}(G_i) = \vec{X}^{\vec{a}_i}$. Furthermore $G_i(\gamma_{\vec{a}}) \neq 0$ if and only if $\vec{a} \in Q_q^s$ satisfies $\vec{a}_i \preceq_{\mathrm{P}} \vec{a}$. The last result is equivalent to saying that $G_i(\gamma_{\vec{a}}) \neq 0$ if and only if $\vec{a} \in \nabla\vec{a}_i$. The support of $\tilde{D}$ is the union of all positions where some $\varphi(G_i)$ does not equal 0. Hence, $|\mathrm{supp}(\tilde{D})| = |\bigcup_{i=1}^{m} \nabla\vec{a}_i| = |\nabla A|$. The proof is complete. □

Chapter 3

GHWs and RGHWs of q-ary Reed-Muller codes

In this section we employ Proposition 11 to compute the hierarchy of RGHWs in the case that C_1 and C_2 are both q-ary Reed-Muller codes. The main result is Theorem 20. Recall that a q-ary Reed-Muller code is defined as

$$RM_q(u,s) = \mathrm{span}_{\mathbb{F}_q}\{\varphi(f) \mid f \in R_q^s, \deg(f) \leq u\}.$$

Our method for calculating the hierarchy of RGHWs involves the anti lexicographic ordering on the monomials in R_q^s (and on the elements in Q_q^s). To relate our findings to Heijnen and Pellikaan's work on GHWs we also need the lexicographic ordering on the same sets.

Definition 12. *The lexicographic ordering $\prec_{\mathrm{Lex}}$ on the monomials in R_q^s and on the elements in Q_q^s is defined by*

$$\vec{X}^{\vec{a}} \prec_{\mathrm{Lex}} \vec{X}^{\vec{b}} \text{ (or } \vec{a} \prec_{\mathrm{Lex}} \vec{b}) \iff \begin{array}{l} a_1 = b_1, \ldots, a_{l-1} = b_{l-1} \text{ and} \\ a_l < b_l \text{ for some } l. \end{array}$$

The anti lexicographic ordering $\prec_{\mathrm{A}}$ on the monomials in R_q^s and on the elements in Q_q^s is defined by

$$\vec{X}^{\vec{a}} \prec_{\mathrm{A}} \vec{X}^{\vec{b}} \text{ (or } \vec{a} \prec_{\mathrm{A}} \vec{b}) \iff \begin{array}{l} a_s = b_s, \ldots, a_{s-l+1} = b_{s-l+1} \text{ and} \\ a_{s-l} > b_{s-l} \text{ for some } l. \end{array}$$

Example 4. *For $s = 2$, $q = 3$ with $X = X_1$ and $Y = X_2$ we have*

$$1 \prec_{\mathrm{Lex}} Y \prec_{\mathrm{Lex}} Y^2 \prec_{\mathrm{Lex}} X \prec_{\mathrm{Lex}} XY \prec_{\mathrm{Lex}} XY^2 \prec_{\mathrm{Lex}} X^2 \prec_{\mathrm{Lex}} X^2Y \prec_{\mathrm{Lex}} X^2Y^2,$$

$$X^2Y^2 \prec_{\mathrm{A}} XY^2 \prec_{\mathrm{A}} Y^2 \prec_{\mathrm{A}} X^2Y \prec_{\mathrm{A}} XY \prec_{\mathrm{A}} Y \prec_{\mathrm{A}} X^2 \prec_{\mathrm{A}} X \prec_{\mathrm{A}} 1.$$

From this example it is easy to see that the anti lexicographic ordering is not the inverse ordering of the lexicographic ordering. Recalling from Definition 9 the ordering $\preceq_{\mathrm{P}}$ we note that if $\vec{X}^{\vec{a}} \preceq_{\mathrm{P}} \vec{X}^{\vec{b}}$ (or $\vec{a} \preceq_{\mathrm{P}} \vec{b}$) then $\vec{X}^{\vec{a}} \preceq_{\mathrm{Lex}} \vec{X}^{\vec{b}}$ and $\vec{X}^{\vec{a}} \succeq_{\mathrm{A}} \vec{X}^{\vec{b}}$ (or $\vec{a} \preceq_{\mathrm{Lex}} \vec{b}$ and $\vec{a} \succeq_{\mathrm{A}} \vec{b}$).

The following concepts will be used extensively throughout our exposition.

Definition 13. *Given $\vec{a} = (a_1, \ldots, a_s) \in Q_q^s$, we call $\deg(\vec{a}) = \deg(\vec{X}^{\vec{a}}) = \sum_{t=1}^{s} a_t$ the degree of $\vec{a}$. Let a, b be two integers with $0 \leq a \leq b \leq s(q-1)$, then we define*

$$F_q((a,b),s) = \{\vec{a} \in Q_q^s \mid a \leq \deg(\vec{a}) \leq b\} \text{ and}$$

$$W_q((a,b),s) = \{\vec{X}^{\vec{a}} \in R_q^s \mid \vec{a} \in F_q((a,b),s)\}.$$

The index q and the value s will be omitted in the rest of this section, thus instead we will use the notations $F(a,b)$ and $W(a,b)$, respectively.

Definition 14. *Let $m \in \{1, \ldots, |F(a,b)|\}$, we denote by $L_{(a,b)}(m)$ the set of the first m elements of $F(a,b)$ using the lexicographic ordering and by $N_{(a,b)}(m)$ the set of the first m elements of $F(a,b)$ using the anti lexicographic ordering.*

The sets $N_{(a,b)}(m)$ will play a crucial role in the following derivation of a formula for the RGHWs of q-ary Reed-Muller codes. The sets $L_{(a,b)}(m)$ shall help us establish the connection to the work by Heijnen and Pellikaan on GHWs. Their main result [13, Th. 5.10] is as follows:

Theorem 15. *Let $\vec{a} = (a_1, \ldots, a_s)$ be the r-th element in $F(s(q-1)-u_1, s(q-1))$ with respect to the lexicographic ordering. Then*

$$d_r(RM_q(u_1,s)) = |\Delta L_{(s(q-1)-u_1, s(q-1))}(r)| = \sum_{i=1}^{s} a_{s-i+1} q^{i-1} + 1. \tag{3.1}$$

Before continuing our work on establishing the RGHWs we reformulate the expressions in (3.1). We shall need the following result corresponding to [13, Lem. 5.8].

Lemma 16. *Let t be an integer satisfying $1 \leq t \leq q^s$. Write $t-1 = \sum_{i=1}^{s} a_{s-i+1} q^{i-1}$. Then $(a_1, \ldots, a_s)$ is the t-th element of Q_q^s with respect to the lexicographic ordering.*

Also we shall need the bijection $\mu : Q_q^s \to Q_q^s$ given by $\mu(a_1, \ldots, a_s) = (q-1-a_s, \ldots, q-1-a_1)$. Observe that μ has the properties

- $\vec{a} \prec_{\mathrm{A}} \vec{b} \iff \mu(\vec{a}) \prec_{\mathrm{Lex}} \mu(\vec{b})$,
- $\mu(F(a,b)) = F(s(q-1)-b, s(q-1)-a)$,
- $\mu(\nabla N_{(a,b)}(m)) = \Delta L_{(s(q-1)-b, s(q-1)-a)}(m)$.

For the proofs and other properties of μ we refer to Lemma 28 in Appendix A. Note that by the first property an element $\vec{a}$ in a subset A of Q_q^s is the t-th element in A using the anti lexicographic ordering if and only if $\mu(\vec{a})$ is the t-th element in $\mu(A)$ using the lexicographic ordering. We can now reformulate Theorem 15 into the following result which is not stated in [13].

Theorem 17. *Let $\vec{a}$ be the r-th element in $F(0,u_1)$ using the anti lexicographic ordering. Because $F(0,u_1) \subseteq Q_q^s$ there exists t such that $\vec{a}$ is the t-th element in Q_q^s using the anti lexicographic ordering. We have*

$$d_r(RM_q(u_1,s)) = |\nabla N_{(0,u_1)}(r)| = t.$$

Proof. By the properties of μ and using the lexicographic ordering, we have that $\mu(\vec{a}) = (\tilde{a}_1, \ldots, \tilde{a}_s)$ is the r-th element in $F(s(q-1)-u_1, s(q-1))$ and the t-th element in Q_q^s. From Theorem 15 we get

$$d_r(RM_q(u_1,s)) = |\Delta L_{(s(q-1)-u_1,s(q-1))}(r)| = \sum_{i=1}^{s} \tilde{a}_{s-i+1} q^{i-1} + 1$$

where by Lemma 16 the last expression can be rewritten as $\sum_{i=1}^{s} \tilde{a}_{s-i+1} q^{i-1} + 1 = t - 1 + 1 = t$.
From the third listed property of μ we obtain

$$|\nabla N_{(0,u_1)}(r)| = |\mu(\nabla N_{(0,u_1)}(r))| = |\Delta L_{(s(q-1)-u_1,s(q-1))}(r)|.$$

□

Having reformulated the formula by Heijnen and Pellikaan for GHWs we now continue our work on establishing a formula for the RGHWs. Consider $C_2 = RM_q(u_2,s) \subsetneq C_1 = RM_q(u_1,s)$. Let ℓ be the codimension of C_1 and C_2, then for $m = 1, \ldots, \ell$ we have that

$$\begin{aligned} M_m(C_1,C_2) &= \min\{|\mathrm{supp}(D)| \mid D \text{ is a linear subcode of } C_1, \\ &\quad D \cap C_2 = \{\vec{0}\} \text{ and } \dim(D) = m\} \qquad (3.2) \\ &= \min\{|\mathrm{supp}(D)| \mid D = \mathrm{span}_{\mathbb{F}_q}\{\varphi(F_1), \ldots, \varphi(F_m)\}, \\ &\quad \mathrm{lm}(F_1) = \vec{X}^{\vec{a}_1}, \ldots, \mathrm{lm}(F_m) = \vec{X}^{\vec{a}_m},\ \vec{a}_i \neq \vec{a}_j \text{ for } i \neq j \\ &\quad \text{and } \vec{X}^{\vec{a}_i} \in W(u_2+1,u_1) \text{ for } i = 1, \ldots, m\} \qquad (3.3) \end{aligned}$$

Equation (3.2) corresponds to Theorem 3. Equation (3.3) follows from Remark 5 and the fact that $D \subseteq C_1$ implies $\mathrm{lm}(F_i) \in W(0,u_1)$, $i = 1, \ldots, m$ and from the fact that $D \cap C_2 = \{\vec{0}\}$ implies $\mathrm{lm}(F_i) \notin W(0,u_2)$, $i = 1, \ldots, m$. In conclusion $\mathrm{lm}(F_i) \in W(u_2+1,u_1)$, $i = 1, \ldots, m$. Combining (3.3) with Proposition 11 we get

$$\begin{aligned} M_m(C_1,C_2) &= \min\{|\bigcup_{i=1}^{m} \nabla \vec{a}_i| \mid \vec{a}_i \in F(u_2+1,u_1), i = 1, \ldots m \\ &\quad \text{and } \vec{a}_i \neq \vec{a}_j, \text{ for } i \neq j\} \\ &= \min\{|\nabla A| \mid A \subseteq F(u_2+1,u_1), |A| = m\}. \qquad (3.4) \end{aligned}$$

The following lemma – which can be viewed as a generalization of [12, Th. 3.7.7] – is proved in Appendix A.

Lemma 18. *Let A be a subset of $F(a,b)$ consisting of m elements. Then $|\nabla N_{(a,b)}(m)| \leq |\nabla A|$.*

Proposition 19. *Let $C_2 = RM_q(u_2, s) \subsetneq C_1 = RM_q(u_1, s)$. We have*

$$M_m(C_1, C_2) \quad = \quad |\nabla N_{(u_2+1,u_1)}(m)|$$

Proof. Follows from (3.4) and Lemma 18. □

We are now ready to present the generalization of Theorem 17 to RGHWs.

Theorem 20. *Given $C_2 = RM_q(u_2, s) \subsetneq C_1 = RM_q(u_1, s)$, let $\vec{a}$ be the m-th element in $F(u_2 + 1, u_1)$ with respect to the anti lexicographic ordering. Because $F(u_2+1, u_1) \subseteq F(0, u_1) \subseteq Q_q^s$ there exist r and t such that $\vec{a}$ is the r-th element in $F(0, u_1)$ and the t-th element in Q_q^s with respect to the anti lexicographic ordering. We have*

$$M_m(C_1, C_2) = t - r + m.$$

Proof. By Proposition 19 we have already proved that $M_m(C_1, C_2) = |\nabla N_{(u_2+1,u_1)}(m)|$. It remains to be proved that $|\nabla N_{(u_2+1,u_1)}(m)| = t - r + m$. Because $\vec{a}$ is the m-th element in $F(u_2 + 1, u_1)$ and the r-th element in $F(0, u_1)$ we have

$$N_{(0,u_1)}(r) = N_{(0,u_2)}(r - m) \cup N_{(u_2+1,u_1)}(m)$$

from which we derive

$$\begin{aligned} \nabla N_{(0,u_1)}(r) &= \nabla N_{(u_2+1,u_1)}(m) \cup \nabla N_{(0,u_2)}(r - m) \\ &= \nabla N_{(u_2+1,u_1)}(m) \cup (\nabla N_{(0,u_2)}(r - m) \backslash \nabla N_{(u_2+1,u_1)}(m)). \end{aligned}$$

The last union involves two disjoint sets. Hence,

$$|\nabla N_{(u_2+1,u_1)}(m)| = |\nabla N_{(0,u_1)}(r)| - |\nabla N_{(0,u_2)}(r - m) \backslash \nabla N_{(u_2+1,u_1)}(m)|.$$

From Theorem 17 we have $|\nabla N_{(0,u_1)}(r)| = t$. Hence, we will be through if we can prove that

$$|\nabla N_{(0,u_2)}(r - m) \backslash \nabla N_{(u_2+1,u_1)}(m)| = r - m. \tag{3.5}$$

We enumerate $N_{(0,u_2)}(r-m) = \{\vec{a}_1, \ldots, \vec{a}_{r-m}\}$ according to the anti lexicographic ordering. We have

$$\begin{aligned} &\nabla N_{(0,u_2)}(r - m) \backslash \nabla N_{(u_2+1,u_1)}(m) = \left(\nabla \bigcup_{i=1}^{r-m} \{\vec{a}_i\} \right) \backslash \nabla N_{(u_2+1,u_1)}(m) \\ = \quad & \left(\bigcup_{i=1}^{r-m} \nabla \vec{a}_i \right) \backslash \nabla N_{(u_2+1,u_1)}(m) = \left(\bigcup_{i=1}^{r-m} \nabla \vec{a}_i \backslash \nabla \{\vec{a}_t \mid t < i\} \right) \backslash \nabla N_{(u_2+1,u_1)}(m) \\ = \quad & \bigcup_{i=1}^{r-m} \left(\nabla \vec{a}_i \backslash \left(\nabla \{\vec{a}_t \mid t < i\} \cup \nabla N_{(u_2+1,u_1)}(m) \right) \right). \end{aligned} \tag{3.6}$$

We will prove that

$$\nabla \vec{a}_i \backslash \left(\nabla \{\vec{a}_t \mid t < i\} \cup \nabla N_{(u_2+1,u_1)}(m) \right) = \{\vec{a}_i\} \tag{3.7}$$

holds for $i = 1, \ldots, r-m$.
As $\vec{a}_i \succ_{\mathrm{A}} \vec{a}_t$ for $t < i$, we have $\vec{a}_i \notin \nabla\{\vec{a}_t \mid t < i\}$. Furthermore from $\deg(\vec{a}_i) \leq u_2$ and $\deg(\vec{c}) \geq u_2+1$ for any $\vec{c} \in \nabla N_{(u_2+1,u_1)}(m)$, we conclude $\vec{a}_i \notin \nabla N_{(u_2+1,u_1)}(m)$. It follows that

$$\{\vec{a}_i\} \subseteq \nabla\vec{a}_i \backslash \left(\nabla\{\vec{a}_t \mid t < i\} \cup \nabla N_{(u_2+1,u_1)}(m)\right).$$

Now we prove the other inclusion. Assume first $\vec{a}_i \in F(u_2, u_2)$. For $t = 1, \ldots, s$ we define $\vec{b}_t = \vec{a}_i + \vec{e}_t$ where $\vec{e}_t$ is the standard vector with 1 in the t-th position. If $\vec{b}_t \in Q_q^s$ then $\vec{b}_t \in N_{(u_2+1,u_1)}(m)$ because $\deg(\vec{b}_t) = u_2 + 1$ and $\vec{a}_i \succ_{\mathrm{A}} \vec{b}_t \succeq_{\mathrm{A}} \vec{a}$. It follows that

$$\nabla\vec{a}_i \backslash \left(\nabla\{\vec{a}_t \mid t < i\} \cup \nabla N_{(u_2+1,u_1)}(m)\right) \subseteq$$
$$\subseteq \nabla\vec{a}_i \backslash \nabla(\{\vec{b}_1, \ldots, \vec{b}_s\} \cap Q_q^s) = \{\vec{a}_i\}.$$

Assume next $\vec{a}_i \notin F(u_2, u_2)$. Again we define $\vec{b}_t = \vec{a}_i + \vec{e}_t$ for $t = 1, \ldots, s$. If $\vec{b}_t \in Q_q^s$ then $\vec{b}_t \in \{\vec{a}_t \mid t < i\}$ because $\deg(\vec{b}_t) \leq u_2$ and $\vec{a}_i \succ_{\mathrm{A}} \vec{b}_t$. Hence,

$$\nabla\vec{a}_i \backslash \left(\nabla\{\vec{a}_t \mid t < i\} \cup \nabla N_{(u_2+1,u_1)}(m)\right) \subseteq$$
$$\subseteq \nabla\vec{a}_i \backslash \nabla(\{\vec{b}_1, \ldots, \vec{b}_s\} \cap Q_q^s) = \{\vec{a}_i\}.$$

We have established (3.7).
Combining finally (3.7) and (3.6) we obtain

$$\nabla N_{(0,u_2)}(r-m) \backslash \nabla N_{(u_2+1,u_1)}(m) = \bigcup_{i=1}^{r-m} \{\vec{a}_i\} = N_{(0,u_2)}(r-m).$$

By Definition 14 the last set is of size $r - m$ and (3.5) follows. The proof is complete. □

Consider the special case of Theorem 20 where $C_2 = \{\vec{0}\} = \mathrm{RM}_q(-1, s)$. In this particular case we have – as already noted – $d_m(C_1) = M_m(C_1, C_2)$. If we apply Theorem 20 and the notion in there then we obtain $r = m$ and consequently $M_m(C_1, C_2) = t$. Theorem 17 gives us the same information $d_m(C_1) = t$.

We illustrate the use of Theorem 17 and Theorem 20 with an example.

Example 5. *In this example we consider Reed-Muller codes in two variables over* $\mathbb{F}_5$. *We first consider the case* $C_1 = RM_5(5, 2)$ *and* $C_2 = RM_5(3, 2)$. *Figure 3.1 illustrates how to find* r *and* m *for any given* t *and how to calculate* $d_r(C_1)$ *and* $M_m(C_1, C_2)$ *from this information. The elements of* Q_5^2 *are depicted in Part 3.1.1. In Parts 3.1.2, 3.1.3, and 3.1.4 we illustrate how the elements of* Q_5^2, $F(0, 5)$ *and* $F(4, 5)$, *respectively, are ordered. Finally, Part 3.1.5 illustrates how to determine* $d_r(C_1)$ *and* $M_m(C_1, C_2)$ *from Theorem 17 and Theorem 20, respectively.*

$(0,4)$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$
$(0,3)$	$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$
$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$
$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$
$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$

Part 3.1.1 : Q_5^2

5	4	3	2	1
10	9	8	7	6
15	14	13	12	11
20	19	18	17	16
25	24	23	22	21

Part 3.1.2: t-th positions in Q_5^2

2	1			
5	4	3		
9	8	7	6	
14	13	12	11	10
19	18	17	16	15

Part 3.1.3: r-th positions in $F(0,5)$

2	1			
	4	3		
		6	5	
			8	7
				9

Part 3.1.4: m-th positions in $F(4,5)$

Q_5^2	t	r	m	$d_r(C_1)$ $= t$	$M_m(C_1, C_2)$ $= t - r + m$
$(4,4)$	1	-	-	-	-
$(3,4)$	2	-	-	-	-
$(2,4)$	3	-	-	-	-
$(1,4)$	4	1	1	4	4
$(0,4)$	5	2	2	5	5
$(4,3)$	6	-	-	-	-
$(3,3)$	7	-	-	-	-
$(2,3)$	8	3	3	8	8
$(1,3)$	9	4	4	9	9
$(0,3)$	10	5	-	10	-
$(4,2)$	11	-	-	-	-
$(3,2)$	12	6	5	12	11
$(2,2)$	13	7	6	13	12
$(1,2)$	14	8	-	14	-
$(0,2)$	15	9	-	15	-
$(4,1)$	16	10	7	16	13
$(3,1)$	17	11	8	17	14
$(2,1)$	18	12	-	18	-
$(1,1)$	19	13	-	19	-
$(0,1)$	20	14	-	20	-
$(4,0)$	21	15	9	21	15
$(3,0)$	22	16	-	22	-
$(2,0)$	23	17	-	23	-
$(1,0)$	24	18	-	24	-
$(0,0)$	25	19	-	25	-

Part 3.1.5

Figure 3.1: Calculation of GHWs and RGHWs for $C_1 = \mathrm{RM}_5(5,2)$ and $C_2 = \mathrm{RM}_5(3,2)$.

$r = m$	$d_r(C_1)$	$M_m(C_1, C_2)$
1	15	15
2	19	19
3	20	22

Table 3.1: $C_1 = \mathrm{RM}_5(2, 2), C_2 = \mathrm{RM}_5(1, 2)$.

$r = m$	$d_r(C_1)$	$M_m(C_1, C_2)$
1	10	10
2	14	14
3	15	17
4	18	19

Table 3.2: $C_1 = \mathrm{RM}_5(3, 2), C_2 = \mathrm{RM}_5(2, 2)$.

For the above choice of C_1 and C_2 most of the time the GHWs and RGHWs are the same. This however, is not the general situation for q-ary Reed-Muller codes as the following choices of C_1 and C_2 illustrate.
In the remaining part of this example we concentrate on q-ary Reed-Muller codes $C_1 = RM_5(u_1, 2)$, $C_2 = RM_5(u_2, 2)$ where $u_1 = u_2 + 1$. In Table 3.1, Table 3.2, Table 3.3, Table 3.4, and Table 3.5, respectively, we present parameters $d_r(C_1)$ and $M_m(C_1, C_2)$ for (u_1, u_2) equal to $(2, 1)$, $(3, 2)$, $(4, 3)$, $(5, 4)$, and $(6, 5)$ respectively.

$r = m$	$d_r(C_1)$	$M_m(C_1, C_2)$
1	5	5
2	9	9
3	10	12
4	13	14
5	14	15

Table 3.3: $C_1 = \mathrm{RM}_5(4, 2), C_2 = \mathrm{RM}_5(3, 2)$.

$r = m$	$d_r(C_1)$	$M_m(C_1, C_2)$
1	4	4
2	5	7
3	8	9
4	9	10

Table 3.4: $C_1 = \mathrm{RM}_5(5,2), C_2 = \mathrm{RM}_5(4,2)$.

$r = m$	$d_r(C_1)$	$M_m(C_1, C_2)$
1	3	3
2	4	5
3	5	6

Table 3.5: $C_1 = \mathrm{RM}_5(6,2), C_2 = \mathrm{RM}_5(5,2)$.

Chapter 4

An algorithm to compute RGHWs

By Theorem 20 there are still two questions that need to be addressed:

Q1 Given $m \in \{1, \ldots, |F_q((a,b),s)|\}$, how can we find the m-th element $\vec{a}$ of $F_q((a,b),s)$ with respect to the anti lexicographic ordering?

Q2 Given $\vec{a} \in F_q((a,b),s)$ how can we find the corresponding position t and r – with respect to the anti lexicographic ordering – in Q_q^s and in $F_q((0,b),s)$, respectively?

In this section we give answers to these two questions. We start by providing an algorithm that solves the problem from question Q1. This algorithm is a generalizing of a method proposed in [13, Sec. 6]. Due to the nature of the algorithm from now on we will – in contrast to the previous section – use the full notation $F_q((a,b),s)$, rather than just $F_q((a,b))$ (Definition 13).

Definition 21. *Let $0 \leq a \leq b \leq s(q-1)$ and $0 \leq v \leq w < q$ be integers. We define*

$$F_q((a,b),(v,w),s) = \{(a_1, \ldots, a_s) \in F_q((a,b),s) \mid v \leq a_s \leq w\}.$$

We denote by $\rho_q((a,b),s)$ and $\rho_q((a,b),(v,w),s)$ the cardinality of $F_q((a,b),s)$ and $F_q((a,b),(v,w),s)$, respectively. Most of the time the index q will be omitted.

Theorem 22. *Let q be a fixed prime power and consider non-negative integers a, b, v, s, m with*

$$a \leq b \leq s(q-1),\ v \leq q-1,\ 1 \leq s,\ \text{and } m \in \{1, \ldots, |F_q((a,b),(0,v),s)|\}.$$

If these numbers are used as input to the procedure VECA in Figure 4.1 then the output is the m-th element $\vec{a} = (a_1, \ldots, a_s)$ of $F_q((a,b),(0,v),s)$ with respect to the anti lexicographic ordering.

1: **procedure** VECA(A, B, V, S, M, q: Non-negative integers with $A \leq B \leq S(q-1)$, $V \leq q-1$, $1 \leq S$, and $M \in \{1, \ldots, |F_q((A,B),(0,V),S)|\}$)
2: **if** $V > B$ **then**
3: VECA$(A, B, V, S, M, q) \leftarrow$ VECA(A, B, B, S, M, q)
4: **else**
5: **if** $S \neq 1$ **then**
6: $\alpha \leftarrow \max\{A - V, 0\}$
7: $r \leftarrow \rho_q((\alpha, B - V), S - 1)$
8: **if** $M > r$ **then**
9: VECA$(A, B, V, S, M, q) \leftarrow$ VECA$(A, B, V - 1, S, M - r, q)$
10: **else if** $M < r$ **then**
11: VECA$(A, B, V, S, M, q) \leftarrow$
12: (VECA$(\alpha, B - V, q - 1, S - 1, M, q), V)$
13: **else**
14: $\theta_1 \leftarrow \alpha$ rem $(q-1)$
15: $\theta_2 \leftarrow (\alpha - \theta_1)/(q-1)$
16: **if** $\theta_2 < S - 1$ **then**
17: VECA$(A, B, V, S, M, q) \leftarrow$
18: $(\underbrace{q-1, \ldots, q-1}_{\theta_2}, \theta_1, \underbrace{0, \ldots, 0}_{S-\theta_2-2}, V)$
19: **else**
20: VECA$(A, B, V, S, M, q) \leftarrow (\underbrace{q-1, \ldots, q-1}_{\theta_2}, V)$
21: **end if**
22: **end if**
23: **else**
24: VECA$(A, B, V, S, M, q) \leftarrow (V - M + 1)$
25: **end if**
26: **end if**
27: **end procedure**

Figure 4.1: The recursive algorithm VECA. We use the notation $((\beta_1, \ldots, \beta_{\kappa-1}), \beta_\kappa) = (\beta_1, \ldots, \beta_{\kappa-1}, \beta_\kappa)$ for concatenation.

Proof. Consider the condition

C1: A, B, V, S, M are non-negative integers with $A \leq B \leq S(q-1)$, $V \leq q-1$, $1 \leq S$ and $M \in \{1, \ldots, |F_q((A,B),\,(0,V),\,S)|\}$.

We first show that the following loop invariant holds true:

- If $V > B$ and A, B, V, S, M satisfy Condition C1 then the elements of $(\tilde{A}, \tilde{B}, \tilde{V}, \tilde{S}, \tilde{M}) = (A, B, B, S, M)$ satisfy Condition C1.
- If $V \leq B$, $S \neq 1$ and A, B, V, S, M satisfy Condition C1 then:
  - for $M > r$ the elements in $(\tilde{A}, \tilde{B}, \tilde{V}, \tilde{S}, \tilde{M}) = (A, B, V-1, S, M-r)$ satisfy Condition C1,
  - for $M < r$ the elements in $(\tilde{A}, \tilde{B}, \tilde{V}, \tilde{S}, \tilde{M}) = (\alpha, B-V, q-1, S-1, M)$ satisfy Condition C1. Here $\alpha = \max\{A-V, 0\}$.

Assume first $V > B$. We have $F_q((A,B),(0,V),S) = F_q((A,B),\,(0,\,B),S)$ and the result follows. Assume next $V \leq B$ and $S \neq 1$. We consider the case $M > r$ (line 8–9) and leave the case $M < r$ for the reader. By inspection $\tilde{A} \leq \tilde{B} \leq \tilde{S}(q-1)$, $\tilde{V} \leq q-1$, $1 \leq \tilde{S}$, and $\tilde{A}, \tilde{B}, \tilde{S}, \tilde{M}$ are non-negative. Aiming for a contradiction we assume that $V = 0$ is possible (which would cause $\tilde{V}$ to be negative). But then

$$\begin{aligned} r &= \rho((\alpha, B-V), S-1) = \rho((A,B), S-1) \\ &= \rho((A,B),(0,0),S) = \rho((A,B),(0,V),S) \geq M \end{aligned}$$

where the inequality follows by the assumption that A, B, V, S, M satisfy Condition C1. We have reached a contradiction. Hence, we conclude $0 < V$ and therefore $\tilde{V}$ is non-negative. We next show that $\tilde{M} = M - r$ is in the desired interval. Clearly $\tilde{M} = M - r \geq 1$. To demonstrate that $\tilde{M} \leq |F_q((\tilde{A}, \tilde{B}), (0, \tilde{V}), \tilde{S})|$ we note that

$$\begin{aligned} M &\leq \rho((A,B),(0,V),S) \\ &= \rho((A,B),(0,V-1),S) + \rho((A,B),(V,V),S) \\ &= \rho((A,B),(0,V-1),S) + \rho((\alpha, B-V), S-1) \\ &= \rho((\tilde{A},\tilde{B}),(0,\tilde{V}),\tilde{S}) + r \end{aligned}$$

and the last part of Condition C1 is established.
Let (A_i, B_i, S_i, M_i) be the value of (A, B, S, M) before entering the loop the i-th time. The sequence $\big((A_1,B_1,S_1,M_1),(A_2,B_2,\,S_2,\,M_2),\ldots\big)$ is strictly decreasing with respect to the partial ordering $\preceq_{\mathrm{P}}$, and as A, B, S, M are upper bounded as well as lower bounded the sequence must be finite, meaning that the algorithm terminates.
We next give an induction proof that the algorithm returns the M-th element of $F_q((A,B),(0,V),S)$ with respect to the anti lexicographic ordering.

Basis step:
First assume $V \leq B$, $S \neq 1$ and let θ_1 and θ_2 be as in line 14 and 15 of the

algorithm. Observe that $\theta_2 \leq S-1$ as $\theta_2 = S$ would imply $V = 0$ and consequently $F_q((A,B),(0,V),S) = \emptyset$. This is not possible as by Condition C1, $M \in \{1,\ldots,|F_q((A,B),(0,V),S)|\}$. Consider the last element of $F_q((\alpha, B-V),(V,V),S)$ i.e.

$$(\underbrace{q-1,\ldots,q-1}_{\theta_2},\theta_1,\underbrace{0,\ldots,0}_{S-\theta_2-2},V)$$

if $\theta_2 < S-1$, and

$$(\underbrace{q-1,\ldots,q-1}_{\theta_2},V)$$

if $\theta_2 = S-1$ (in which case $\theta_1 = 0$). This element is the r-th element of $F_q((A,B),(0,V),S)$ where r is as in line 7. Hence, if $M = r$ (lines 13–22) then indeed VECA(A,B,V,S,M,q) equals the element in position M of $F_q((A,B),(0,V),S)$. Assume next $V \leq B$ and $S = 1$. We see that the M-th element of $F_q((A,B),(0,V),1)$ equals $(V-(M-1))$ which corresponds to line 24.

Induction step:
If $V > B$ then as already noted $F_q((A,B),(0,V),S) = F_q((A,B),\ (0,B),S)$. For $V \leq B$, $S \neq 1$ we next consider the two cases $M > r$ and $M < r$ seperately.
We first consider $M > r$ corresponding to lines 8–9 of the algorithm. We have

$$\rho((A,B),(V,V),S) = \rho((\alpha,B-V),(0,q-1),S-1) = r.$$

But $M > r$ and therefore the M-th element of $F_q((A,B),(0,V),S)$ equals the $(M-r)$-th element of $F_q((A,B),(0,V-1),S)$.
We next consider the case $M < r$. Using similar arguments as above we see that the M-th element of $F_q((A,B),(0,V),S)$ is in $F_q((A,B),(V,V),S)$. Therefore it equals $(\beta_1,\ldots,\beta_{S-1},V)$ where $(\beta_1,\ldots,\beta_{S-1})$ is the M-th element of $F_q((\alpha,B-V),(0,q-1),S-1)$.

The proof is complete. □

Note that for our purpose (that is, to answer Q1), the input V in the algorithm VECA shall always be equal to $q-1$. The procedure VECA in Figure 4.1 uses the value $\rho_q((A,B),S)$ for various choices of A,B,S. We therefore need an algorithm to compute this number.

Lemma 23. *Let q be a prime power and onsider integers a,b,s with $0 \leq a \leq b \leq s(q-1)$ and $s \geq 1$. We have*

$$\rho_q((a,b),s) = \sum_{i=a}^{b}\sum_{j=0}^{\lfloor i/q \rfloor}(-1)^j\binom{s}{j}\binom{s-1+i-qj}{s-1}.$$

Proof. We rewrite the first expression as follows

$$\begin{aligned}\rho_q((a,b),s) &= |F_q((a,b),s)| = |W_q((a,b),s)| = \\ &= |W_q((0,b),s)\backslash W_q((0,a-1),s)| \\ &= |W_q(0,b),s)| - |W_q((0,a-1),s)| \\ &= \dim(RM_q(b,s)) - \dim(RM_q(a-1,s)).\end{aligned}$$

```
1: procedure RHO(a, b, s, q: Non-negative integers with 0 ≤ a ≤ b ≤ s(q − 1) and
   1 ≤ s.)
2:     sum ← 0
3:     for i := a, . . . , b do
4:         for j := 0, . . . , ⌊i/q⌋ do
5:             sum ← sum + (−1)^j C(s, j) C(s − 1 + i − qj, s − 1)
6:         end for
7:     end for
8:     return sum
9: end procedure
```

Figure 4.2: The algorithm RHO.

By [20] and by Exercise 1.2.8 of [21] we have that

$$\dim(RM_q(u,s)) = \sum_{i=0}^{u} \sum_{j=0}^{\lfloor i/q \rfloor} (-1)^j \binom{s}{j} \binom{s-1+i-qj}{s-1}$$

and the proof follows. □

Theorem 24. *Let q be a prime power and consider a, b, s as in Lemma 23. If the procedure RHO (see Figure 4.2) is used with input a, b, s, q then it returns $\rho_q((a,b),s)$.*

Proof. By Lemma 23. □

Example 6. *We use the algorithm VECA in Figure 4.1 to find the 34-th element $\vec{a} = (a_1, \ldots, a_7)$ of $F_7((20,22),7)$. The procedure takes as input $(A,B,V,S,M) = (20,22,6,7,34)$. The notation $\tilde{A}$, $\tilde{B}$, $\tilde{V}$, $\tilde{S}$, $\tilde{M}$ is as in the proof of Theorem 22.*

$(A,B,V,S,M) = (20,22,6,7,34)$*:*
$\rho_7((14,16),6) = 23415 > 34$ *(lines 10–12). Thus* $a_7 = 6$, $\tilde{A} = \max\{0, 20-6\} = 14$, $\tilde{B} = 22 - 6 = 16$, $\tilde{V} = q - 1 = 6$ *and* $\tilde{S} = 7 - 1 = 6$.

$(A,B,V,S,M) = (14,16,6,6,34)$*:*
$\rho_7((8,10),5) = 1936 > 34$ *(lines 10–12). Thus* $a_6 = 6$, $\tilde{A} = \max\{0, 14-6\} = 8$, $\tilde{B} = 16 - 6 = 10$, $\tilde{V} = q - 1 = 6$ *and* $\tilde{S} = 6 - 1 = 5$.

$(A,B,V,S,M) = (8,10,6,5,34)$*:*
$\rho_7((2,4),4) = 64 > 34$ *(lines 10–12). Thus* $a_5 = 6$, $\tilde{A} = \max\{0, 8-6\} = 2$, $\tilde{B} = 10 - 6 = 4$, $\tilde{V} = q - 1 = 6$ *and* $\tilde{S} = 5 - 1 = 4$.

$(A,B,V,S,M) = (2,4,6,4,34)$*:*
$6 > 4$ *(lines 2–3). Thus* $\tilde{V} = B = 4$.

$\underline{(A,B,V,S,M)=(2,4,4,4,34)}$*:*
$\rho_7((0,0),3)=1<34$ *(lines 8–9). Thus* $\tilde{M}=34-1=33$ *and* $\tilde{V}=4-1=3$.

$\underline{(A,B,V,S,M)=(2,4,3,4,33)}$*:*
$\rho_7((0,1),3)=4<33$ *(lines 8–9). Thus* $\tilde{M}=33-4=29$ *and* $\tilde{V}=3-1=2$.

$\underline{(A,B,V,S,M)=(2,4,2,4,29)}$*:*
$\rho_7((0,2),3)=10<29$ *(lines 8–9). Thus* $\tilde{M}=29-10=19$ *and* $\tilde{V}=2-1=1$.

$\underline{(A,B,V,S,M)=(2,4,1,4,19)}$*:*
$\rho_7((1,3),3)=19=19$ *(lines 13–17). We have* $\theta_1=1$ *and* $\theta_2=0$*, thus* $(a_1,a_2,a_3,a_4)=(1,0,0,1)$ *and the algorithm ends.*

In conclusion the 34*-th element of* $F_7((20,22),7)$ *is* $(a_1,a_2,a_3,a_4,\ a_5,a_6,a_7)=(1,0,0,1,6,6,6)$.

Having answered question Q1 from the beginning of the section we now turn to question Q2. Given $\vec{a}\in F_q((a,b),s)$ we need a method to determine what are the corresponding positions r and t in $F_q((0,b),s)$ and Q_q^s, respectively. The following proposition tells us how to find r. This is done by applying the formula (4.1) in there in combination with the algorithm RHO.

Proposition 25. *The element* $\vec{a}=(a_1,\ldots,a_s)\in F_q((a,b),s)$ *is the* r*-th element of* $F_q((a,b),s)$ *with respect to the anti lexicographic ordering, where*

$$r=\sum_{j=0}^{s-1}\sum_{i=0}^{q-a_{s-j}-2}\rho_q((\max\{0,a-\sum_{t=0}^{j}a_{s-t}-i-1\},b-\sum_{t=1}^{j}a_{s-t}-i-1),s-j-1)+1.$$

In particular if $a=0$ *then*

$$r=\sum_{j=0}^{s-1}\sum_{i=0}^{q-a_{s-j}-2}\rho_q((0,b-\sum_{t=1}^{j}a_{s-t}-i-1),s-j-1)+1. \tag{4.1}$$

Proof. We must count the number of elements $\vec{b}=(b_1,\ldots,b_s)$ in $F_q((a,b),s)$ which are smaller than or equal to $\vec{a}$ with respect to the anti lexicographic ordering. This

number equals

$$\begin{aligned}
r &= |\{\vec{b} \in F_q((a,b),s) \mid \vec{b} \preceq_{\mathrm{A}} \vec{a}\}| \\
&= |\{\vec{b} \in F_q((a,b),s) \mid b_s > a_s\}| + |\{\vec{b} \in F_q((a,b),s) \mid \vec{a} \preceq_{\mathrm{A}} \vec{b}, b_s = a_s\}| \\
&= \rho((a,b),(a_s+1,q-1),s) + |\{\vec{b} \in F_q((a,b),s) \mid b_{s-1} > a_{s-1}, b_s = a_s\}| \\
&\quad + |\{\vec{b} \in F_q((a,b),s) \mid \vec{a} \preceq_{\mathrm{A}} \vec{b}, b_{s-1} = a_{s-1}, b_s = a_s\}| \\
&= \rho((a,b),(a_s+1,q-1),s) + \rho((\max\{0,a-a_s\},b-a_s),(a_{s-1}+1,q-1),s-1) \\
&\quad + |\{\vec{b} \in F_q((a,b),s) \mid \vec{a} \preceq_{\mathrm{A}} \vec{b}, b_{s-1} = a_{s-1}, b_s = a_s\}| \\
&= \cdots \\
&= \sum_{j=0}^{s-1} \rho((\max\{0, a - \sum_{t=0}^{j-1} a_{s-t}\}, b - \sum_{t=0}^{j-1} a_{s-t}), (a_{s-j}+1, q-1), s-j) + |\{\vec{a}\}| \\
&= \sum_{j=0}^{s-1} \rho((\max\{0, a - \sum_{t=0}^{j-1} a_{s-t}\}, b - \sum_{t=0}^{j-1} a_{s-t}), (a_{s-j}+1, q-1), s-j) + 1.
\end{aligned}$$

By the below Lemma 26, for $j = 0, \ldots, s-1$ we have

$$\begin{aligned}
&\rho((\max\{0, a - \sum_{t=0}^{j-1} a_{s-t}\}, b - \sum_{t=0}^{j-1} a_{s-t}), (a_{s-j}+1, q-1), s-j) \\
= &\sum_{i=0}^{q-a_{s-j}-2} \rho((\max\{0, a - \sum_{t=0}^{j} a_{s-t} - i - 1\}, b - \sum_{t=1}^{j} a_{s-t} - i - 1), s-j-1)
\end{aligned}$$

and the proof is complete. □

Lemma 26. *Given a prime power q, let $0 \le a \le b \le s(q-1)$ and $0 \le v \le w < \min\{b, q\}$ be integers. Then $\rho_q((a,b),(v,w),s) = \sum_{i=0}^{w-v} \rho_q((\max\{0, a-v-i\}, b-v-i), s-1)$.*

Proof.

$$\begin{aligned}
\rho((a,b),(v,w),s) &= |F_q((a,b),(v,w),s)| \\
&= |\{(a_1,\ldots,a_s) \in F_q((a,b),s) \mid v \le a_s \le w\}| \\
&= |\bigcup_{i=0}^{w-v} \{(a_1,\ldots,a_s) \in F_q((a,b),s) \mid a_s = v+i\}| \\
&= |\bigcup_{i=0}^{w-v} F_q((a,b),(v+i,v+i),s)| \\
&= \sum_{i=0}^{w-v} \rho((a,b),(v+i,v+i),s) \\
&= \sum_{i=0}^{w-v} \rho((\max\{0,a-v-i\}, b-v-i), s-1).
\end{aligned}$$

□

Setting $a = 0$ and $b = s(q-1)$ in Proposition 25 we could of course compute the t such that $\vec{a}$ is the t-th element of Q_q^s, but with the following reformulation of Lemma 25 we can calculate it much easier.

Lemma 27. *The element $(a_1, \ldots, a_s) \in Q_q^s$ is the t-th element of Q_q^s with respect to the anti lexicographic ordering where*

$$t = q^s - \sum_{i=1}^{s} a_i q^{i-1}.$$

Proof. Recall from Section 3 the map $\mu : Q_q^s \to Q_q^s$, $\mu(a_1, \ldots, a_s) = (q-1-a_s, \ldots, q-1-a_1)$. By Lemma 16 $\mu(a_1, \ldots, a_s) = (q-1-a_s, \ldots, q-1-a_1)$ is the t element of Q_q^s using the lexicographic ordering where $t-1 = \sum_{i=1}^{s}(q-1-a_i)q^{i-1} = q^s - 1 - \sum_{i=1}^{s} a_i q^{i-1}$. Recall from Section 3 that $\vec{c} \prec_{\mathrm{A}} \vec{d} \iff \mu(\vec{c}) \prec_{\mathrm{Lex}} \mu(\vec{d})$. Therefore $(a_1, \ldots, a_s)$ is the t-th element of Q_q^s using the anti lexicographic ordering. □

Summarizing this section: to find the m-th RGHW of $C_1 = RM_q(u_1, s)$ with respect to $C_2 = RM_q(u_2, s)$, we perform the following steps.

1. Find the m-th element $(a_1, \ldots, a_s)$ of $F_q((u_2+1, u_1), s)$ by using the algorithm VECA in Theorem 22 with input $A = u_2 + 1$, $B = u_1$, $V = q-1$, $S = s$, and $M = m$.

2. Find the r-th position of $(a_1, \ldots, a_s)$ in $F_q((0, u_1), s)$ using Proposition 25 in combination with the algorithm RHO.

3. Find the t-th position of $(a_1, \ldots, a_s)$ in Q_q^s using Lemma 27.

4. Compute $M_m(C_1, C_2) = t - r + m$ (Theorem 20).

Example 7. *This is a continuation of Example 5, in the beginning of which we considered $C_1 = RM_5(5, 2)$ and $C_2 = RM_5(3, 2)$. Applying the above procedure to establish the 8-th RGHW we first use Theorem 22 to establish that the 8-th element of $F_5((4, 5), 2)$ is $(3, 1)$. Using Proposition 25 we then find that $(3, 1)$ is the 11-th element of $F_5((0, 5), 2)$ and Lemma 27 next tells us that it is the 17-th element of Q_5^2. Hence, $M_8(C_1, C_2) = 17 - 11 + 8 = 14$.*

Example 8. *We consider $C_1 = RM_{16}(90, 7)$ and $C_2 = RM_{16}(88, 7)$. We want to compute the 1000-th RGHW of C_1 with respect to C_2. Applying the algorithm VECA in Theorem 22 we find that that $(9, 10, 14, 11, 15, 15, 15)$ is the 1000-th element of $F_{16}((88, 90), 7)$. Applying next Proposition 25 and Lemma 27 we find that it is the 14557-th element of $F_{16}((0, 90), 7)$ and the 16727-th element of Q_{16}^7. Hence, $M_{1000}(C_1, C_2) = 16727 - 14557 + 1000 = 3170$. To find the 1000-th GHW of C_1, we use Theorem 22 with $C_2 = RM_{16}(-1, 7)$ and we find that $(5, 1, 10, 15, 15, 15, 15)$ is the 1000-th element of $F_{16}((0, 90), 7)$. By Lemma 27 it is the 1515-th element of Q_{16}^7. Hence, from Theorem 17 we deduce $d_{1000}(C_1) = 1515$.*

Chapter 5

Closed formula expressions for q-ary Reed-Muller codes in two variables

In the previous section we presented a method to calculate RGHWs for any set of q-ary Reed-Muller codes $C_i = \mathrm{RM}_q(u_i, s)$, $i = 1, 2$. As an alternative, for q-ary Reed-Muller codes in two variables (which by Definition 4 means that $s = 2$) it is a manageable task to list closed formula expressions for all possible situations. This is done in the first half of the present section. Letting next $u_2 = -1$, corresponding to $C_2 = \{\vec{0}\}$, we in particular get closed formula expressions for the GHWs (such formulas – to the best of our knowledge – cannot be found in the literature). The formulas in the present section can be derived by applying Proposition 19 directly. We shall leave the details for the reader. To simplify the description we use the notation $t = u_1 - u_2$ which of course implies that $u_1 = u_2 + t$. Hence, throughout this section $C_2 = \mathrm{RM}_q(u_2, 2)$ and $C_1 = \mathrm{RM}_q(u_2 + t, 2)$.

5.1 Formulas for RGHW

We have the following three cases.

5.1.1 First case: $u_2 - q + 2 \geq 0$

In this case the codimension is $\ell = t(2q - u_2 - t - 2) + \frac{t(t+1)}{2}$.

- If $m = 1, \ldots, t(2q-u_2-t-2)$ then there exist $a \in \{0, \ldots, 2(q-1)-u_2-t-1\}$ and $b \in \{1, \ldots, t\}$ such that $m = at + b$. We have

$$M_m(C_1, C_2) = \left(2q - 2 - u_2 - \frac{a}{2}\right)(a+1) + b - t.$$

$$\begin{array}{ccccc} Y^4 & \underline{XY^4} & \underline{X^2Y^4} & X^3Y^4 & X^4Y^4 \\ Y^3 & XY^3 & \underline{X^2Y^3} & \underline{X^3Y^3} & X^4Y^3 \\ Y^2 & XY^2 & X^2Y^2 & \underline{X^3Y^2} & \underline{X^4Y^2} \\ Y & XY & X^2Y & X^3Y & \underline{X^4Y} \\ 1 & X & X^2 & X^3 & X^4 \end{array}$$

$W_5(5,6)$ underlined, i.e. $u_2 = 4$ and $t = 2$
(First case)

- If $m = t(2q - u_2 - t - 2) + 1, \ldots, t(2q - u_2 - t - 2) + \frac{t(t+1)}{2}$, then there exists $c \in \left\{1, \ldots, \frac{t(t+1)}{2}\right\}$ such that $m = t(2q - u_2 - t - 2) + c$. We have

$$M_m(C_1, C_2) = \frac{1}{2}(2q - u_2 - t - 2)(2q - u_2 + t - 1) + c.$$

5.1.2 Second case: $u_2 - q + t + 1 \leq 0$

$$\begin{array}{ccccc} Y^4 & XY^4 & X^2Y^4 & X^3Y^4 & X^4Y^4 \\ \underline{Y^3} & XY^3 & X^2Y^3 & X^3Y^3 & X^4Y^3 \\ \underline{Y^2} & \underline{XY^2} & X^2Y^2 & X^3Y^2 & X^4Y^2 \\ Y & \underline{XY} & \underline{X^2Y} & X^3Y & X^4Y \\ 1 & X & \underline{X^2} & \underline{X^3} & X^4 \end{array}$$

$W_5(2,3)$ underlined, i.e. $u_2 = 1$ and $t = 2$
(Second case)

In this case the codimension is $\ell = \frac{t(t+1)}{2} + t(u_2 + 1)$.

- If $m = 1, \ldots, \frac{t(t+1)}{2}$ then there exist $a \in \{0, \ldots, t-1\}$ and $b \in \{1, \ldots, a+1\}$ such that $m = \frac{a(a+1)}{2} + b$. We have

$$M_m(C_1, C_2) = q(q - u_2 - t + a) + b - a - 1.$$

- If $m = \frac{t(t+1)}{2} + 1, \ldots, \frac{t(t+1)}{2} + t(u_2 + 1)$, then there exist $a \in \{0, \ldots, u_2\}$ and $b \in \{1, \ldots, t\}$ such that $m = \frac{t(t+1)}{2} + at + b$. We have

$$M_m(C_1, C_2) = q(q + a - u_2) + b - t - 1 - \frac{a(a+3)}{2}.$$

$$\begin{array}{ccccc}
\underline{Y^4} & \underline{XY^4} & X^2Y^4 & X^3Y^4 & X^4Y^4 \\
\underline{Y^3} & \underline{XY^3} & \underline{X^2Y^3} & X^3Y^3 & X^4Y^3 \\
Y^2 & \underline{XY^2} & \underline{X^2Y^2} & \underline{X^3Y^2} & X^4Y^2 \\
Y & XY & \underline{X^2Y} & \underline{X^3Y} & \underline{X^4Y} \\
1 & X & X^2 & \underline{X^3} & \underline{X^4}
\end{array}$$

$W_5(3,5)$ underlined, i.e. $u_2 = 2$ and $t = 3$
(Third case)

5.1.3 Third case: $u_2 - q + 2 < 0$ and $u_2 - q + t + 1 > 0$

In this case the codimension is $\ell = (2q - u_2)(u_2 + t) + 3(q - u_2) - q^2 - 2 - \frac{t(t+3)}{2}$.

- If $m = 1, \ldots, \frac{1}{2}(q-u_2-2)(2t-q+u_2+1)+t$ then there exist $a \in \{0, \ldots, q-u_2-2\}$ and $b \in \{1, \ldots, u_2+t-q+a+2\}$ such that $m = a(u_2+t-q+1)+\frac{a(a+1)}{2}+b$. We have
$$M_m(C_1, C_2) = (a+2)(q-1) - u_2 - t + b.$$

- If $m = \frac{1}{2}(q-u_2-2)(2t-q+u_2+1)+t+1, \ldots, \frac{1}{2}(q-u_2-2)(2t-q+u_2+1)+t(q-t)$ then there exist $a \in \{0, \ldots, q-t-2\}$ and $b \in \{1, \ldots, t\}$ such that $m = \frac{1}{2}(q-u_2-2)(2t-q+u_2+1) + (a+1)t + b$. We have
$$M_m(C_1, C_2) = q(q - u_2 + a) - \frac{a(a+3)}{2} - t + b - 1.$$

- If $m = \frac{1}{2}(q-u_2-2)(2t-q+u_2+1)+t(q-t)+1, \ldots, (2q-u_2)(u_2+t)+3(q-u_2)-q^2-2-\frac{t(t+3)}{2}$ then there exists $c \in \{1, \ldots, \frac{1}{2}((t+1)^2-(q-u_2-1)^2+q-u_2-t-2)\}$ such that $m = \frac{1}{2}(q-u_2-2)(2t-q+u_2+1)+t(q-t)+c$. We have
$$M_m(C_1, C_2) = \frac{1}{2}(3q^2 - 2u_2q - 3q - t^2 - t) + c.$$

5.2 Formulas for GHW

Applying the formulas from the previous section to the special case of $u_2 = -1$ and consequently $u_1 = t - 1$ we get by letting $u = u_1$ the following results concerning the GHWs of $\mathrm{RM}_q(u, s)$.

5.2.1 The case $u - q + 1 \leq 0$

In this case the dimension of C_1 is $k_1 = \frac{(u+1)(u+2)}{2}$.

m	1	2	3	4	5	6	7	8	9	10
diff(m)	0	0	14	15	29	43	45	59	73	87
$M_m(C_1, C_2)$	16	31	46	61	76	91	106	121	136	151

m	11	12	13	14	15	16
diff(m)	90	104	118	132	146	150
$M_m(C_1, C_2)$	166	181	196	211	226	241

Table 5.1: The special case $u_2 = q - 2$ and $t = 1$ with $q = 16$. That is, $C_1 = \mathrm{RM}_{16}(15, 2)$ and $C_2 = \mathrm{RM}_{16}(14, 2)$. The function diff($m$) equals $M_m(C_1, C_2) - d_m(C_1)$.

- For $r = 1, \ldots, \frac{(u+1)(u+2)}{2}$ there exist $a \in \{0, \ldots, u\}$ and $b \in \{1, \ldots, a+1\}$ such that $r = \frac{a(a+1)}{2} + b$. We have

$$d_r(C_1) = q(q - u + a) + b - a - 1.$$

5.2.2 The case $u - q + 1 > 0$

In this case the dimension of C_1 is $k_1 = q(2u_1 - q + 3) - \frac{u_1(u_1+3)}{2} - 1$.

- For $r = 1, \ldots, q(u+2) - \frac{u(u+3)}{2} - 1$ there exist $a \in \{0, \ldots, 2(q-1) - u\}$ and $b \in \{1, \ldots, u - q + 2 + a\}$ such that $r = a(u - q + 1) + \frac{a(a+1)}{2} + b$. We have

$$d_r(C_1) = (a+2)(q-1) - u + b.$$

- For $r = q(u+2) - \frac{u(u+3)}{2}, \ldots, q(2u - q + 3) - \frac{u(u+3)}{2} - 1$ there exists $c \in \{1, \ldots, q(u - q + 1)\}$ such that $r = q(u+2) - \frac{u(u+3)}{2} - 1 + c$. We have

$$d_r(C_1) = q(2q - u - 1) + c.$$

5.3 Comparing RGHW and GHW in a special case

Consider the special case $u_2 = q - 2$ and $t = 1$. If $m = 1, \ldots, q$ then there exist $a \in \{0, \ldots, q-1\}$ and $b \in \{1, \ldots, a+1\}$ such that $m = \frac{a(a+1)}{2} + b$. We have

$$M_m(C_1, C_2) = \frac{m}{2}(2q - m + 1) \text{ and } d_m(C_1) = (q-1)(a+1) + b$$

Thus

$$M_m(C_1, C_2) - d_m(C_1) = \frac{1}{8}(-a^4 - 2a^3 + (-4b + 4q + 1)a^2$$
$$+(-4b - 4q + 10)a - 4b^2 + 8bq - 4b - 8q + 8).$$

For the particular case that $q = 16$ we get the values listed in Table 5.1

Chapter 6

Concluding remarks

In this paper we found the RGHWs of q-ary Reed-Muller codes by using the footprint bound. There is a very strong connection between the footprint bound and the Feng-Rao bound for primary codes [1, 11] which is the bound that we used in [10] to estimate RGHWs of one-point algebraic geometric codes. Using in the present paper the footprint bound rather than the Feng-Rao bound for primary or dual codes helped us save some cumbersome notation (which is difficult to avoid in the case of one-point algebraic geometric codes).

The authors gratefully acknowledge the support from the Danish National Research Foundation and the National Natural Science Foundation of China (Grant No. 11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography. Also the authors gratefully acknowledge the support from The Danish Council for Independent Research (Grant No. DFF–4002-00367). Part of this work was done while the first listed order was visiting East China Normal University. We are grateful to Professor Hao Chen for his hospitality. Finally the authors would like to thank Diego Ruano and Ruud Pellikaan for helpful discussions.

Appendix A

Proof of Lemma 18

To prove Lemma 18 we start by generalizing [12, Th. 3.7.7] which corresponds to Lemma 28 below in the particular case that $b = s(q-1)$. The proof of [12, Th. 3.7.7] was given in [12, App. B.1].

Lemma 28. *Let A be a subset of $F_q(a,b)$ consisting of m elements. Then $|\Delta L_{(a,b)}(m)| \leq |\Delta A|$.*

Proof. In Appendix B.1 of [12] a proof for Lemma 28 is given in the particular case that $b = s(q-1)$. We indicate how this proof can be modified to cover all possible choices of b. First note that [12] uses v where we use a, uses m where we use s, and uses r where we use m. With the following modifications the proof in [12] is lifted to a proof of Lemma 28.

- In [12, Rem. B.1.2]: Replace $F_{\geq v}$ with $F_q(v,b)$ and let the parameter k go from v to b.
- In [12, Def. B.1.6]: Replace $F_{\geq l}$ with $F_q(l,b)$.
- In [12, Lem. B.1.10]: Replace $F_{\geq v}$ with $F_q(v,b)$ and let the summation end with A_b rather than $A_{s(q-1)}$.
- In [12, Lem. B.1.13, Lem. B.1.14 and their proofs]: Replace $F_{\geq l}$, $F_{\geq (l-1)}$, $F_{\geq v}$, $L_{\geq l-1}(r)$ and $L_{\geq l}(r)$ with $F_q(l,b)$, $F_q(l-1,b)$, $F_q(v,b)$, $L_{(l,b)}(r)$ and $L_{(l-1,b)}(r)$, respectively.

□

Recall from Section 3 the map $\mu : Q_q^s \to Q_q^s$ given by $\mu(a_1,\ldots,a_s) = (q-1-a_s,\ldots,q-1-a_1)$. To translate Lemma 28 into Lemma 18 we need the following results.

Lemma 29. *Let $0 \leq a \leq b \leq s(q-1)$ be integers, $\vec{a},\vec{b} \in Q_q^s$ and $m \in \{1,\ldots,|F_q(a,b)|\}$, then we have that*

1. $\vec{a} \prec_{\mathrm{Lex}} \vec{b} \iff \mu(\vec{a}) \prec_{\mathrm{A}} \mu(\vec{b})$,

2. $\vec{a} \prec_{\mathrm{A}} \vec{b} \iff \mu(\vec{a}) \prec_{\mathrm{Lex}} \mu(\vec{b})$,

3. $\vec{a} \preceq_{\mathrm{P}} \vec{b} \iff \mu(\vec{a}) \succeq_{\mathrm{P}} \mu(\vec{b})$,

4. $\mu(\nabla \vec{a}) = \Delta \mu(\vec{a})$,

5. $\mu(\nabla A) = \Delta \mu(A)$,

6. $\mu(F_q(a,b)) = F_q(s(q-1)-b, s(q-1)-a)$,

7. $A \subseteq F_q(a,b) \iff \mu(A) \subseteq F_q(s(q-1)-b, s(q-1)-a)$,

8. $\mu(N_{(a,b)}(m)) = L_{(s(q-1)-b, s(q-1)-a)}(m)$,

9. $\mu(\nabla N_{(a,b)}(m)) = \Delta L_{(s(q-1)-b, s(q-1)-a)}(m)$.

Proof. Let $\vec{a} = (a_1, \ldots, a_s)$ and $\vec{b} = (b_1, \ldots, b_s)$.

1. $\vec{a} \prec_{\mathrm{Lex}} \vec{b} \iff a_1 = b_1, \ldots, a_{l-1} = b_{l-1}, a_l < b_l$ for some $l \iff q-1-a_1 = q-1-b_1, \ldots, q-1-a_{l-1} = q-1-b_{l-1}, q-1-a_l > q-1-b_l$ for some $l \iff \mu(\vec{a}) \prec_{\mathrm{A}} \mu(\vec{b})$.

2. Similar to 1.

3. $\vec{a} \preceq_{\mathrm{P}} \vec{b} \iff a_1 \leq b_1, \ldots, a_s \leq b_s \iff q-1-a_1 \geq q-1-b_1, \ldots, q-1-a_s \geq q-1-b_s \iff \mu(\vec{a}) \succeq_{\mathrm{P}} \mu(\vec{b})$.

4. $\vec{b} \in \mu(\nabla \vec{a}) \iff \exists \vec{b_1} = \mu^{-1}(b) \in \nabla \vec{a} \iff \vec{b_1} \preceq_{\mathrm{P}} \vec{a} \iff \mu(\vec{b_1}) \succeq_{\mathrm{P}} \mu(\vec{a}) \iff \vec{b} \succeq_{\mathrm{P}} \mu(\vec{a}) \iff \vec{b} \in \Delta \mu(\vec{a})$.

5. $\mu(\nabla A) = \mu(\bigcup_{\vec{a} \in A} \nabla \vec{a}) = \bigcup_{\vec{a} \in A} \mu(\nabla \vec{a}) = \bigcup_{\vec{a} \in A} \Delta \mu(\vec{a}) = \Delta \bigcup_{\vec{a} \in A} \mu(\vec{a}) = \Delta \mu(A)$.

6. $\vec{a} \in F_q(a,b) \iff a \leq \deg(\vec{a}) \leq b \iff a \leq \sum_{i=1}^{s} a_i \leq b \iff s(q-1)-a \geq s(q-1) - \sum_{i=1}^{s} a_i \geq s(q-1)-b \iff s(q-1)-b \leq \sum_{i=1}^{s}(q-1-a_i) \leq s(q-1)-a \iff \mu(\vec{a}) \in F_q(s(q-1)-b, s(q-1)-a)$.

7. Similar to 6.

8. Follows from 1,2 and 7 by induction.

9. $\mu(\nabla N_{(a,b)}(m)) = \Delta \mu(N_{(a,b)}(m)) = \Delta L_{(s(q-1)-b, s(q-1)-a)}(m)$.

□

We are now ready to prove Lemma 18.

Proof of Lemma 18. By 7. in Lemma 29 he have $\mu(A) \subseteq F_q(s(q-1)-b, s(q-1)-a)$. It follows that

$$\begin{aligned} |\nabla N_{(a,b)}(m)| &= |\mu(\nabla N_{(a,b)}(m))| \\ &= |\Delta L_{(s(q-1)-b,s(q-1)-a)}(m)| \\ &\leq |\Delta\mu(A)| \\ &= |\mu(\nabla A)| \\ &= |\nabla A|, \end{aligned}$$

where the first and the last line is a consequence of the fact that μ is bijective, the second line follows from 9. in Lemma 29,the third line follows from Lemma 28, and the fourth line follows from 5. in Lemma 29. □

Bibliography

[1] H. E. Andersen and O. Geil. Evaluation codes from order domain theory. *Finite Fields and Their Applications*, 14(1):92–123, 2008.

[2] T. Bains. Generalized Hamming weights and their applications to secret sharing schemes. Master's thesis, Univ. Amsterdam, 2008.

[3] S. L. Bezrukov and U. Leck. Macaulay posets. *The Electronic Journal of Combinatorics*, 1000:DS12–Jan, 2005.

[4] I. Cascudo, R. Cramer, and C. Xing. The arithmetic codex. In *Information Theory Workshop (ITW), 2012 IEEE*, pages 75–79. IEEE, 2012.

[5] H. Chen, R. Cramer, S. Goldwasser, R. De Haan, and V. Vaikuntanathan. Secure computation from random error correcting codes. In *Advances in Cryptology-EUROCRYPT 2007*, pages 291–310. Springer, 2007.

[6] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer, third edition, 2012.

[7] R. Cramer. Introduction to secure computation. In *Lectures on Data Security*, pages 16–62. Springer, 1999.

[8] R. Cramer. The arithmetic codex: Theory and applications. In *Advances in Cryptology–EUROCRYPT 2011*, pages 1–1. Springer, 2011.

[9] I. Duursma and J. Shen. Multiplicative secret sharing schemes from Reed-Muller type codes. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 264–268. IEEE, 2012.

[10] O. Geil, S. Martin, R. Matsumoto, D. Ruano, and Y. Luo. Relative generalized Hamming weights of one-point algebraic geometric codes. *arXiv preprint arXiv:1403.7985*, 2014.

[11] O. Geil, R. Matsumoto, and D. Ruano. Feng–Rao decoding of primary codes. *Finite Fields and their Applications*, 23:35–52, 2013.

[12] P. Heijnen. Some classes of linear codes. In *Ph.D. Thesis*. Technische Universiteit Eindhoven, 1999.

[13] P. Heijnen and R. Pellikaan. Generalized Hamming weights of q-ary Reed-Muller codes. In *IEEE Trans. Inform. Theory*. Citeseer, 1998.

[14] T. Helleseth, T. Kløve, and J. Mykkeltveit. The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l - 1)/n)$. *Discrete Mathematics*, 18(2):179–211, 1977.

[15] T. Høholdt. On (or in) Dick Blahut's footprint. *Codes, Curves and Signals*, pages 3–9, 1998.

[16] T. Kløve. The weight distribution of linear codes over $GF(q^l)$ having generator matrix over $GF(q)^*$. *Discrete Mathematics*, 23(2):159–168, 1978.

[17] J. Kurihara, T. Uyematsu, and R. Matsumoto. Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 95(11):2067–2075, 2012.

[18] Z. Liu, W. Chen, and Y. Luo. The relative generalized Hamming weight of linear q-ary codes and their subcodes. *Designs, Codes and Cryptography*, 48(2):111–123, 2008.

[19] Y. Luo, C. Mitrpant, A. H. Vinck, and K. Chen. Some new characters on the wire-tap channel of type II. *Information Theory, IEEE Transactions on*, 51(3):1222–1229, 2005.

[20] A. B. Sørensen. Projective Reed-Muller codes. *Information Theory, IEEE Transactions on*, 37(6):1567–1576, 1991.

[21] M. Tsfasman and S. G. Vladut. *Algebraic-geometric codes*. Kluwer Academic Publishers, 1991.

[22] V. K. Wei. Generalized Hamming weights for linear codes. *Information Theory, IEEE Transactions on*, 37(5):1412–1418, 1991.