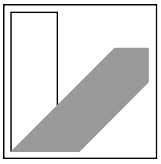


UNIVERSITÄT
BAYREUTH

**Faculty for Mathematics, Physics, and Computer Science**

# MASTER'S THESIS

**in Mathematics**

# Rank Metric Codes

**submitted by**

**Miriam Schmidt**

**Mat.-No. 1204821**

**March 30, 2016**

**— corrected version —**

**Supervisor: Prof. Dr. Michael Stoll**
**Advisor: Dr. Michael Kiermaier**
**Second Assessor: apl. Prof. Dr. Alfred Wassermann**

## Acknowledgments

I would like to express my gratitude to my advisor Michael Kiermaier for the useful comments, remarks, and inspirations throughout this thesis. His door was always open and whenever I had a question, I got appropriate help.

I also want to thank Kai-Uwe Schmidt for providing his unpublished LP-bounds. Last but not least, I would like to thank my husband Alexander for guarding my back throughout the process of writing this thesis.

# Contents

# List of Algorithms



# List of Tables



# List of Figures

# 1 Introduction

A problem in transmitting or storing information is that the transmission can be disturbed or the storage medium can be damaged. Bad weather or a scratch in a CD are only two examples of many. This is often referred to having a "noisy channel".

The common solution to this problem is to translate the message into a sequence of codewords which differ enough from each other that a certain number of errors in transmission can be corrected or at least recognized. To tell when codewords differ enough, a concept of distance suitable for the transmission channel or storage medium is needed.

The set of codewords is called a *code* and the *minimum distance* of a code is the minimal pairwise distance of codewords. This minimum distance is a measurement of how many errors a code can recognize or correct. The main goal is to find—in a fixed space of possible codewords—a code that contains as many codewords as possible while having a minimum distance as large as possible. The most common example for measuring distance in coding theory is the *Hamming distance* $\mathrm{d}_H$ which counts the number of entries in which two vectors (or more general: strings) differ. This distance is suitable, for example, for binary symmetric channels where vectors of $\mathbb{F}_2^n$ are transmitted and there is a certain probability that a "0" is flipped into a "1" or vice versa.

If there is not a single point-to-point connection but a network which, in general, has multiple sources and several sinks, for example, in the distribution of software updates, network coding is used to improve the information flow. Here, *subspace codes* [35, 37, 61] are an appropriate choice. Instead of vectors, they consist of subspaces of a given vector space and are equipped, for example, with the subspace metric

$$\mathrm{d}_S(U,V) = \dim(U) + \dim(V) - 2\dim(U \cap V)$$

or with the injection distance

$$\mathrm{d}_I(U,V) = \max\{\dim(U), \dim(V)\} - \dim(U \cap V).$$

When all codewords of a subspace code have the same dimension, the code is called *constant dimension code*. In this important case, $\mathrm{d}_S(U,V) = 2\,\mathrm{d}_I(U,V)$.

Such constant dimension codes can be constructed, for example, from *rank metric codes*. These are codes consisting of matrices and equipped with the *rank metric*

$$\mathrm{d}_{\mathrm{rk}}(A,B) = \mathrm{rk}(A-B).$$

This metric is first introduced by Loo-Keng Hua (in 1945 for symmetric matrices [31] and in 1951 for general matrices [32, Section 7]) as "arithmetic distance" and introduced into coding theory by Delsarte [13] in 1978 and Gabidulin [21] in 1985.

To construct a constant dimension code from a rank metric code, a subspace $\Lambda(A)$ of $\mathbb{F}_q^{m+n}$ is generated by the rows of the $n \times (n+m)$ matrix $(I_n \mid A)$ composed as a block matrix from the identity matrix $I_n$ and an element $A$ of the rank metric code in $\mathbb{F}_q^{n\times m}$. This mapping is injective and it holds that

$$\mathrm{d}_S(\Lambda(A),\Lambda(B)) = 2\,\mathrm{d}_I(\Lambda(A),\Lambda(B)) = 2\,\mathrm{d}_{\mathrm{rk}}(A,B).$$

This construction is first proposed in 2003 for linear authentication codes in [66] and rediscovered by Kschischang and Kötter in 2008 in [37].

Additionally, rank metric codes have an application in space-time coding [23] and in the GPT (Gabidulin, Paramonov, Tretjakov) cryptosystem [24, 22].

Also rank metric codes with certain additional properties are of interest, for example, containing linear subcodes of symmetric matrices improves the error correcting capability of linear rank metric codes [25].

In odd characteristic, from a rank metric code $Y$ consisting only of symmetric matrices in $\mathbb{F}_q^{n\times n}$, two codes $\mathcal{C}_1(Y), \mathcal{C}_2(Y) \subset \mathbb{F}_q^{q^n-1}$, both classical codes in Hamming metric, of size $\#Y$ and $q^m \cdot \#Y$, respectively, can be constructed [56]. For this, functions $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$ with $f(0) = 0$ are identified with vectors in $\mathbb{F}_q^{q^n-1}$ which contain the function values $f(v)$ for all $v \neq 0$. Then $\mathcal{C}_1(Y)$ is defined to consist of the quadratic forms associated with the matrices in $Y$ and $\mathcal{C}_2(Y)$ is defined as $\mathcal{C}_2(Y) = \{a+b \mid a \in \mathcal{C}_1(Y), b \in \mathcal{L}\}$ where $\mathcal{L}$ denotes the set of linear forms on $\mathbb{F}_q^n$. The codes $\mathcal{C}_1(Y)$ and $\mathcal{C}_2(Y)$ thus are subcodes of the shortened generalized second-order Reed-Muller code, that is, the code resulting when taking all codewords of the generalized second-order Reed-Muller code $\mathrm{GRM}(2, m)$ whose first entry is zero and omitting the first entry (cf. also [58]). In [56, Section 5], it is described how the distance enumerators of $\mathcal{C}_1(Y)$ and $\mathcal{C}_2(Y)$ which are polynomials defined by

$$\beta_{\mathcal{C}_i(Y)}(z) = \frac{1}{\#\mathcal{C}_i(Y)} \sum_{b,c\in\mathcal{C}_i(Y)} z^{\mathrm{d}_H(b,c)}$$

can be obtained from a property of the rank distance code $Y$ which is called inner distribution. In the case of $\mathbb{F}_2$, there exists a similar construction of subsets of $\mathrm{ZRM}(2,m)/\mathrm{ZRM}(1,m)$ where $\mathrm{ZRM}(d, m)$ refers to quaternary Reed–Muller codes of order $d$ [54, 55, 58].

Rank metric codes of skew-symmetric matrices have been studied in [14] and rank metric codes of Hermitian matrices in [57].

Those rank metric codes—which are also referred to as rank codes, matrix codes, or rank distance codes—are subject of this thesis, in particular codes consisting only of symmetric or Hermitian matrices over finite fields. The aim is—given a prescribed matrix space and a fixed number as lower bound for the minimum distance—to classify codes which reach the maximum possible size and to improve lower bounds for this maximum code size in cases where the exact maximum size has not been determined.

The thesis is structured as follows:

Section 2 contains the fundamental concepts needed to understand this thesis.

Section 3 summarizes known upper and lower bounds for the size of maximum codes. The subsections on symmetric and Hermitian matrices are mainly based on the works [55, 56, 57] by Kai-Uwe Schmidt.

Section 4 is based on the book "Geometry of Matrices" [65] by Zhe-Xian Wan which summarizes results mainly by him and his teacher Loo-Keng Hua. It is dedicated to the groups of isometries of matrix spaces and develops a concept of isomorphism for rank metric codes. This section also provides a way to put this concept into practice.

Based on the results of Section 4, Section 5 deals with the determination of automorphism groups of codes.

Section 6 contains the main part of this thesis. Here, constructions for symmetric and Hermitian codes are provided. This is subdivided into four subsections. In the first subsection, two new infinite series of Hermitian codes are described of which one improves the lower bounds for all spaces of Hermitian $n \times n$ matrices over finite fields where $n \geq 4$ is an even number when the minimum distance is two. In the next two subsections, two exact

algorithms are presented which are able to find and classify maximum codes. It is shown that the best known lower bound for the size of maximum codes in the space of Hermitian $2 \times 2$ matrices over the field $\mathbb{F}_{25}$ actually already coincides with the maximum code size for this case. Besides classification, it is also an aim to find "nice" representatives of each isomorphism class and give (geometric) interpretations. In the last subsection, a heuristic approach is applied to cases where the search space becomes too big for the presented exact algorithms. By this, the lower bounds can be increased in some further particular cases.

In Section 7, the results of this thesis are summarized and further work is inspired.

# 2 Preliminaries

Very generally, a *code* $\mathcal{C}$ can be defined as a subset of a metric space $(M, \mathrm{d})$.

If $\#\mathcal{C} > 1$, then the *minimum distance* of $\mathcal{C}$ is $\mathrm{d}(\mathcal{C}) = \min\{\mathrm{d}(c_1, c_2) \mid c_1 \neq c_2 \in \mathcal{C}\}$. If $\#\mathcal{C} \leq 1$, we set $\mathrm{d}(\mathcal{C}) = \infty$.

**Definition 2.1.** Let $F$ be a field and let $\mathcal{M} \subset F^{m\times n}$ be a set of matrices. For two matrices $A, B \in \mathcal{M}$, we define their *rank distance* to be

$$\mathrm{d}_{\mathrm{rk}}(A, B) = \mathrm{rk}(A - B).$$

As observed, for example, in [21], the rank distance is indeed a metric on $\mathcal{M}$. Subsets of $(\mathcal{M}, \mathrm{d}_{\mathrm{rk}})$ are called *rank metric codes* and are the subject of this thesis. Consequently, from now on by code we mean rank metric code and distance refers to the rank distance.

By

$$\mathcal{S}_n(F) = \left\{(m_{i,j})_{1\leq i,j\leq n} \in F^{n\times n} \mid m_{i,j} = m_{j,i}\ \forall 1 \leq i, j, \leq n\right\},$$

we denote the set of *symmetric $n \times n$ matrices* over the field $F$.

A nontrivial involution of a field $F$ is a field automorphism of order 2, or, in other words, a field automorphism $\overline{\ }\colon F \to F$ with $\overline{\overline{a}} = a$ for all $a \in F$ which not equals $\mathrm{id}_F$. For a field $F$ with a fixed nontrivial involution $\overline{\ }\colon F \to F$, we define by

$$\mathcal{H}_n(F) = \left\{(m_{i,j})_{1\leq i,j\leq n} \in F^{n\times n} \mid m_{i,j} = \overline{m_{j,i}}\ \forall 1 \leq i, j, \leq n\right\}$$

the set of *Hermitian $n \times n$ matrices*.

It is well known (see, e.g., [27]) that the automorphism group of $\mathbb{F}_{p^n}$, $p$ prime, is cyclic of order $n$ and generated by the Frobenius automorphism $\sigma\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}\ , x \mapsto x^p$. This means that the finite field with $q = p^n$ elements possesses a nontrivial involution if and only if $2 \mid n$, that is, if $q$ is a square. In this case, the nontrivial involution is unique and given by $\sigma^{n/2} = \overline{\ }\colon \mathbb{F}_q \to F_q,\ x \mapsto x^{\sqrt{q}}$.

Transposition of a matrix $M$ is denoted by $M^{\mathsf{T}}$. Whenever a field automorphism is applied to a matrix, we mean applying it to every matrix entry.

Furthermore, $I_n$ stands for the $n \times n$-identity matrix, $\mathbb{N} = \{1, 2, 3, \dots\}$, and $\mathbb{F}_q$ denotes the field with $q$ elements. For non-prime fields, the following representations are used:

$$\mathbb{F}_4 = {}^{\mathbb{F}_2[x]}\!/_{(x^2+x+1)} \qquad \mathbb{F}_{16} = {}^{\mathbb{F}_2[x]}\!/_{(x^4+x^3+x^2+x+1)}$$
$$\mathbb{F}_9 = {}^{\mathbb{F}_3[x]}\!/_{(x^2+1)} \qquad \mathbb{F}_{25} = {}^{\mathbb{F}_5[x]}\!/_{(x^2+3)}$$

The residue class of $x$ is denoted by $X$.

Throughout this thesis, $\#S$ denotes the cardinality of a set $S$ and $2^S$ its power set.

A *graph* $\Gamma = (V, E)$ consists of a (finite) vertex set $V$ and a set $E \subset \binom{V}{2} = \{e \subset V \mid \#e = 2\}$ of edges. We say that the edge $\{i, j\}$ *connects* the vertices $i$ and $j$ or that $i$ and $j$ are *adjacent*. A *clique* $C$ in the graph $\Gamma$ is a subset of the vertex set $V$ such that $\{i, j\} \in E$ for all $i, j \in C$.

In this thesis, we are searching for codes of maximum possible size amongst all codes in a given matrix space with minimum distance at least a fixed number. So we want to introduce the terms maximal and maximum as they are commonly used in graph theory [4, p. xvi]:

**Definition 2.2.** Let $S$ be a set and $\mathcal{T} \subset 2^S$ be a collection of subsets of $S$. Then $A \in \mathcal{T}$ is called

- *maximal* if there is no $B \in \mathcal{T}$ with $A \subsetneq B$ and
- *maximum* if $\#B \leq \#A$ for all $B \in \mathcal{T}$.

**Definition 2.3.** A (*left*) *group action* of a group $G$ on a set $X$ is a map

$$G \times X \to X,\ (g, x) \mapsto g.x$$

with the property that

1. $e.x = x\ \forall x \in X$ where $e$ is the identity element of $G$ and
2. $(gh).x = g.(h.x)\ \forall g, h \in G, x \in X$.

We denote the *$G$-orbit* of $x \in X$ by $G.x = \{g.x \mid g \in G\}$ and, additionally, $g.Y = \{g.y \mid y \in Y\}$ for $Y \subset X$. The set of all $G$-orbits is a partition of $X$. For $Y \subset X$, the *setwise stabilizer* is defined as $G_Y = \{g \in G \mid g.y \in Y\ \forall y \in Y\}$. It is a subgroup of $G$. For singletons, we use the abbreviation $G_x = G_{\{x\}}$.

**Definition 2.4.** Cf., e.g., [20, section 1.1.1], [29, p. 36ff.]. Let $G$ be a group acting on the set $X$. A *transversal* is a set containing exactly one representative from each $G$-orbit of $X$.

For a fixed transversal $T$, a map $\tau\colon X \to G$ with the property that $\tau(x).x \in T$ for all $x \in X$ is called *canonicalizing* (also: *canonizing*) *map* with respect to $T$. The element $\tau(x).x$ is called *canonical representative* of the orbit $G.x$.

# 3 Bounds for the Size of Maximum Codes

Throughout this section, let $2 \leq d \leq n$ be natural numbers.

## 3.1 Unrestricted Matrices

**Theorem 3.1** (Delsarte)**.** *[13, Thm. 5.4] Let $\mathcal{C} \subset \mathbb{F}_q^{m \times n}$ be a code with minimum distance $\geq d$. Without loss of generality, let $m \leq n$ (otherwise transpose). Then*

$$\#\mathcal{C} \leq q^{(m-d+1)n}.$$

For the case of linear codes, this bound can also be found in the work of Gabidulin [21] and Roth [52].

A code reaching this bound is called *maximum rank distance (MRD) code*. The bound itself is, for example, referred to as the Singleton bound for codes with the rank metric (see [26]) or Singleton-like bound (see [40]).

In [21, Section 4], Gabidulin presents a class of linear MRD codes in vector representation (he deals with codes in $\mathbb{F}_{q^m}^n$ instead of $\mathbb{F}_q^{m\times n}$—which is equivalent) for all $d \leq m \leq n$ and any finite field $\mathbb{F}_q$. So does Roth in [52] independently. In [13], Delsarte also gives a construction for linear MRD codes, though from the perspective of bilinear forms. Both constructions are essentially the same (see, e.g., [10, Section 5]) and commonly known as *Gabidulin codes*.

In [39], Kshevetskiy and Gabidulin present a new construction for MRD codes that includes the construction of [21] as a special case. Other constructions for MRD codes different from Gabidulin codes are given in [11], [48], and [60].

Since the size of maximum codes in $\mathbb{F}_q^{m\times n}$ is clear in all cases, this thesis will concentrate on symmetric and Hermitian matrices.

## 3.2 Symmetric Matrices

### 3.2.1 Upper Bounds

**Theorem 3.2** (K.-U. Schmidt)**.** *[55, Cor. 7], [56, Lemma 3.5] Let $\mathcal{C} \subset \mathcal{S}_n(\mathbb{F}_q)$ be a code with minimum distance $\geq d$. Then*

$$\#\mathcal{C} \leq \begin{cases} q^{(n+1)(n-d+2)/2}, & n, d \text{ even}, \\ q^{n(n-d+3)/2}, & n \text{ odd and } d \text{ even}, \\ q^{(n+1)(n-d+1)/2}, & n \text{ even and } d \text{ odd}, \\ q^{n(n-d+2)/2}, & n, d \text{ odd}. \end{cases}$$

The proof in the case of even characteristic can be found in [55, Cor. 7] and is based on the work of Delsarte and Goethals on alternating bilinear forms [14]. The case of odd characteristic is treated in [56, Lemma 3.5] for odd $d$ and can be easily derived for even $d$ since a code with minimum distance $\geq d$ is also a code with minimum distance $\geq d-1$. The key idea of both proofs is the use of association schemes as pioneered by Delsarte [12]. For a survey on association schemes in coding theory, see, e.g., [15].

In the case of odd characteristic and even $d$ this bound can be improved as follows:

**Theorem 3.3** (K.-U. Schmidt)**.** *[56, Prop. 3.7] Let $q$ be an odd prime power and $\mathcal{C} \subset \mathcal{S}_n(\mathbb{F}_q)$ be a code with minimum distance $\geq d$ with $d$ even. Then*

$$\#\mathcal{C} \leq \begin{cases} q^{(n+1)(n-d+2)/2} \cdot \frac{1+q^{-n+d-1}}{q+1}, & n \text{ even}, \\ q^{n(n-d+3)/2} \cdot \frac{1+q^{-n+1}}{q+1}, & n \text{ odd}. \end{cases}$$

Since in the case $d = 2$, the bound of Theorem 3.2 equals the number $q^{n(n+1)/2}$ of symmetric matrices, there is also a slight but easy improvement possible in the case where $q$ is even.

**Proposition 3.4.** *Let $\mathcal{C} \subset \mathcal{S}_n(\mathbb{F}_q)$ be a code with minimum distance $\geq 2$. Then*

$$\#\mathcal{C} \leq q^{n(n+1)/2} - q^n + 1.$$

Table 1: LP-bounds calculated by K.-U. Schmidt [59] compared to the (rounded down) upper bounds for the size of codes in $\mathcal{S}_n(\mathbb{F}_q)$ given in Theorem 3.3.

| | $n=5, d=4$ | | $n=7, d=6$ | | $n=7, d=4$ | |
|---|---|---|---|---|---|---|
| | $q=3$ | $q=5$ | $q=3$ | $q=5$ | $q=3$ | $q=5$ |
| Theorem 3.3 | 14944 | 1630208 | 1197382 | 1017317708 | 2618675528 | 79477945963541 |
| LP-bound [59] | 10044 | 1304791 | 798984 | 813869792 | 2328242882 | 76299072265609 |

*Proof.* Since $\mathcal{S}_n(\mathbb{F}_q)$ is an additive group, we can assume without loss of generality that the zero matrix is an element of $\mathcal{C}$. This means that there must not be any matrices of rank one in $\mathcal{C}$. By [41], the number of symmetric $n \times n$ matrices of rank 1 is $q^n - 1$. Thus the claim follows. □

There also can be considered Delsarte's linear programming (LP) bound [12] which (according to current knowledge) has to be calculated for each triple $(q, n, d)$ separately. K.-U. Schmidt conjectures [59] that this LP-bound equals $q^5 - q^4 + 2q^3 - 2q^2 + q$ in the case $n = 3$, $d = 2$ and $q$ odd. He verified this formula for all odd prime powers $q \leq 113$. This would improve the bound of Theorem 3.3 by the additive term $q - 2$, as can be easily shown by polynomial division. Additionally, he calculated some values for $q = 3$ and $q = 5$ as shown in Table 1. In those cases, the LP-bound improves the bound given by Theorem 3.3 additively by approximately

$$\begin{cases} q^8 - q^7, & n = 5, d = 2, \\ q^{12} - q^{11}, & n = 7, d = 6, \\ q^{18} - q^{17}, & n = 7, d = 4, \end{cases}$$

where $q \in \{3, 5\}$. When $n$ and $d$ are even and $q$ is odd, K.-U. Schmidt expects the LP-bound to coincide with the bound of Theorem 3.3 [56, remark after Prop. 3.7].

### 3.2.2 Lower Bounds

The most obvious way to obtain lower bounds on the maximum size of codes is to explicitly give a code of a certain size. In the case of codes in $\mathcal{S}_n(\mathbb{F}_q)$, K.-U. Schmidt does this by constructing additive codes.

**Theorem 3.5** (K.-U. Schmidt)**.** *[55, Thm. 12 and Thm. 16], [56, Thm. 4.1 and Thm. 4.4] There exists an additive code $\mathcal{C} \subset \mathcal{S}_n(\mathbb{F}_q)$ with minimum distance $d$ and*

$$\#\mathcal{C} = \begin{cases} q^{(n+1)(n-d+1)/2}, & n-d \text{ odd}, \\ q^{n(n-d+2)/2}, & n-d \text{ even}. \end{cases}$$

The construction for $q$ even is given in [55] and for odd characteristic in [56]. Both constructions use the trace function

$$\mathrm{Tr}\colon \mathbb{F}_{q^m} \to \mathbb{F}_q, \quad \mathrm{Tr}(x) = \sum_{k=0}^{m-1} x^{q^k}$$

Table 2: Upper and lower bounds for the maximum code size in $\mathcal{S}_n(\mathbb{F}_q)$ with minimum distance at least an even number $d$ for some small values of $n$, $q$, and $d < n$.

| | $n=3,\ d=2$ | | | | | | | $n=4,\ d=2$ | | $n=5,\ d=4$ | | | $n=5,\ d=2$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $q=2$ | $q=3$ | $q=4$ | $q=5$ | $q=7$ | $q=8$ | $q=9$ | $q=2$ | $q=3$ | $q=2$ | $q=3$ | $q=4$ | $q=2$ |
| lower bound | $22^a$ | $90^b$ | $256^c$ | $625^c$ | $2401^c$ | $4096^c$ | $6561^c$ | $256^c$ | $6561^c$ | $64^c$ | $729^c$ | $4096^c$ | $4096^c$ |
| upper bound | $22^a$ | $201^d$ | $4033^e$ | $2705^d$ | $15001^d$ | $261633^e$ | $53793^d$ | $1009^e$ | $15309^f$ | $1024^g$ | $10044^d$ | $1048576^g$ | $32737^e$ |

[a] [36], [b] [58], [c] Theorem 3.5, [d] [59], [e] Proposition 3.4, [f] Theorem 3.3, [g] Theorem 3.2

and symmetric bilinear forms

$$B_\lambda \colon \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} \to \mathbb{F}_q, \quad B_\lambda(x,y) = \mathrm{Tr}\left(\lambda_0 xy + \sum_{j=1}^{t} \lambda_j \left(x^{q^{s\cdot j}} y + x y^{q^{s\cdot j}}\right)\right),$$

where $0 \leq t \leq \frac{m-1}{2}$, $\lambda \in \mathbb{F}_{q^m}^{t+1}$, and $s = 1$ in the case of characteristic 2 or $s$ coprime to $m$ in the case of odd characteristic.

Actually, in case of odd characteristic, these are the largest possible additive codes in $\mathcal{S}_n(\mathbb{F}_q)$ [56, Thm. 3.3] where additive means forming an additive subgroup of the ambient matrix space. For not necessarily additive codes, the upper and lower bound coincide in the case where $d$ is odd (or $d = n$) but K.-U. Schmidt leaves it an open problem ([55, Section 5], [56, remark after Prop. 3.7]) whether larger non-additive codes exist in the case where $d$ is even and $d < n$. This is answered by M. Kiermaier [36] who found that the maximum code size in $\mathcal{S}_3(\mathbb{F}_2)$ is 22 ($d = 2$) and that there exists a code with minimum distance $d = 2$ in $\mathcal{S}_3(\mathbb{F}_3)$ of size 90 (cf. [58, slide 15]). The largest additive codes in those cases are of size 16 and 81, respectively. Further new lower bounds for the size of maximum codes in $\mathcal{S}_n(\mathbb{F}_q)$ are produced in section 6.4.

For some small values of $n$, $q$, and $d < n$, where $d$ even, Table 2 summarizes the in each case best lower and upper bounds of those presented up to this point for the maximum code size of codes in $\mathcal{S}_n(\mathbb{F}_q)$ with minimum distance $\geq d$.

## 3.3 Hermitian Matrices

### 3.3.1 Partial Spread Sets

**Definition 3.6.** [28, Section 1] Let $F$ be a field. $U \subset F^{n\times n}$ is called *partial spread set* if

1. $\mathrm{rk}(A - B) = n \quad \forall A, B \in U, A \neq B$ and
2. $\mathrm{rk}(A) = n \quad \forall A \in U, A \neq 0$.

As we can see, the case where we are looking for maximum codes in $\mathcal{H}_n(\mathbb{F}_{q^2})$ with minimum rank distance $d = n$ can be viewed as the problem of finding maximal partial spread sets in $\mathcal{H}_n(\mathbb{F}_{q^2})$. Those are closely related to partial spreads in the Hermitian polar space $H(2n-1, q^2)$ [28]. For definitions of polar geometry, see appendix A.

In [28], we find the following lemma.

**Lemma 3.7.** *[28, Lemma 1] There exists a partial spread set in $\mathcal{H}_n(\mathbb{F}_{q^2})$ of size $N$ if and only if there exists a partial spread in $H(2n-1, q^2)$ of size $N+1$.*

The connection of partial spreads and partial spread sets can be traced back to [6, Section 5].

Additionally, partial spreads in $H(3,q^2)$ correspond to partial ovoids in the elliptic quadric $Q^-(5,q)$ (see, e.g., [28, p. 14]), so we can use known bounds for those too.

However, the concepts of isomorphism of partial spreads and partial ovoids do not coincide with the notion of isomorphism of codes introduced in Section 4. Indeed, all maximum partial spreads in $H(3,9)$ are isomorphic (see [18, Section 4]) as well as all maximum codes in $\mathcal{H}_2(\mathbb{F}_9)$ with minimum distance 2 are (see section 6.2.2). On the other side, there are only 3 non-isomorphic maximum partial ovoids in $Q^-(5,4)$ (see [8, Table 1]) but 7 non-isomorphic maximum codes in $\mathcal{H}_2(\mathbb{F}_{16})$ as we will see in section 6.2.3.

### 3.3.2 Upper Bounds

**Theorem 3.8** (K.-U. Schmidt)**.** *[57, Thm. 1, Thm. 2] Let $\mathcal{C} \subset \mathcal{H}_n(\mathbb{F}_{q^2})$ be a code with minimum distance $\geq d$. Then*

$$\#\mathcal{C} \leq \begin{cases} q^{n(n-d+1)}, & d \text{ odd}, \\ (-1)^{n+1} \cdot q^{n(n-d+1)} \cdot \frac{\left((-q)^{n-d+2}-1\right)+(-q)^n\left((-q)^{n-d+1}-1\right)}{(-q)^{n-d+2}-(-q)^{n-d+1}}, & d \text{ even}. \end{cases}$$

In the case where $n = d$ odd, this bound is already proven by Vanhove in 2009 in [63] in the context of partial spreads. In the case where $n$ even, K.-U. Schmidt conjectures that this bound coincides with the LP-bound [57, remark after Thm. 2].

By means of Lemma 3.7, we can use the upper bounds for partial spreads collected in the work of Ihringer [33] for the case $n = d$:

**Theorem 3.9** (De Beule, Klein, Metsch, Storme)**.** *[9, Thm. 4.2] Let $S$ be a partial spread of $H(2n-1,q^2)$ where $n$ is even. Then*

$$\#S \leq \begin{cases} \frac{1}{2}(q^3+q+2), & n = 2 \\ q^{2n-1} - q^{3n/2}(\sqrt{q}-1), & n \geq 4 \end{cases}.$$

If $n = 4$ and $q = 2, 3$ or if $n > 4$, this bound can be improved by the following theorem.

**Theorem 3.10** (Ihringer)**.** *[33, Thm. 1.5] Let $S$ be a partial spread of $H(2n-1,q^2)$, $n > 1$. Then*

$$\#S \leq q^{2n-1} - q\frac{q^{2n-2}-1}{q+1}.$$

Summing up the best upper bounds known to Ihringer in 2014 for a partial spread of $H(2n-1,q^2)$, $n$ even, and using Lemma 3.7, we gain the following upper bounds for the size of a code $\mathcal{C} \subset \mathcal{H}_n(\mathbb{F}_{q^2})$, $n$ even, with minimum distance $n$ (see [33, table on p. 3]):

$$\#\mathcal{C} \leq \begin{cases} \frac{1}{2}(q^3+q), & n = 2, q \neq 4, \\ 24, & n = 2, q = 4 \text{ (taken from [8])}, \\ q^{2n-1} - q\frac{q^{2n-2}-1}{q+1} - 1, & n = 4, q \leq 3, \\ q^{2n-1} - q^{3n/2}(\sqrt{q}-1) - 1, & n = 4, q > 3, \\ q^{2n-1} - q\frac{q^{2n-2}-1}{q+1} - 1, & n > 4. \end{cases}$$

The bound 24 in the case $n = 2, q = 4$ comes from an exhaustive computer search in [8] which has shown that the largest size of a maximal partial ovoid in $Q^-(5,4)$ is 25. In the same article, we come across another bound which is better in a few cases than those gathered by Ihringer and is already known since 1995: In a quadric, a cap is the same as a partial ovoid (comparing the definitions in [8] and [2]), so we can use the following result of Blokhuis and Moorhouse.

**Theorem 3.11** (Blokhuis, Moorhouse)**.** *[2, Thm. 1.3] If $S$ is any cap on a nondegenerate quadric in* $\mathrm{PG}(n, p^e)$*, then*

$$\#S \leq \left( \binom{p+n-1}{n} - \binom{p+n-3}{n} \right)^e + 1.$$

Applying this theorem to $Q^-(5,q)$ we gain the following corollary.

**Corollary 3.12.** *Let $\mathcal{C} \subset \mathcal{H}_2(\mathbb{F}_{q^2})$ be a code with minimum distance 2 and $q = p^e$ with $p$ prime. Then*

$$\#\mathcal{C} \leq \left( \binom{p+4}{5} - \binom{p+2}{5} \right)^e = \left( \frac{(p+2)(p+1)^2 p}{12} \right)^e.$$

*Proof.* Since a cap, that is, a partial ovoid, in $Q^-(5,q)$ corresponds to a partial spread in $H(3,q^2)$, we only have to subtract one from the bound of Theorem 3.11 and substitute $n = 5$ to obtain the bound for the size of $\mathcal{C}$ using Lemma 3.7. The equality is a straightforward computation:

$$\begin{aligned}
\binom{p+4}{5} - \binom{p+2}{5} &= \prod_{j=1}^{5} \frac{p+4+1-j}{j} - \prod_{k=1}^{5} \frac{p+2+1-k}{k} \\
&= \frac{p(p+1)(p+2)}{5!} \cdot \big( (p+3)(p+4) - (p-2)(p-1) \big) \\
&= \frac{p(p+1)(p+2)}{5!} \cdot \big( 10p + 10 \big) \\
&= \frac{p(p+1)^2(p+2)}{12}.
\end{aligned}$$

□

**Proposition 3.13.** *The bound of Corollary* 3.12 *is stronger than $\frac{1}{2}(q^3+q)$ if and only if $p \leq 7$ and*

$$\begin{cases} e \geq 3, & \text{if } p \leq 3, \\ e \geq 4, & \text{if } p = 5, \\ e \geq 34, & \text{if } p = 7. \end{cases}$$

*Proof.* Define $\mathrm{BKMS}(p,e) = \frac{1}{2}(p^{3e} + p^e)$ and $\mathrm{BM}(p,e) = \left( \frac{(p+2)(p+1)^2 p}{12} \right)^e$.

For $p > 7$, we have $p \geq 11$ and so

$$\begin{aligned}
\mathrm{BM}(p,e) &= \left( \frac{p+2}{12} \right)^e (p^2+2p+1)^e p^e \\
&> (p^2+1)^e p^e \\
&> \mathrm{BKMS}(p,e).
\end{aligned}$$

So in this case, the bound of De Beule, Klein, Metsch, and Storme is tighter for any $e$.

For $p \leq 7$, we want to show that $\frac{\mathrm{BKMS}(p,e)}{\mathrm{BM}(p,e)}$ is monotonically increasing in $e$ and that the smallest value for $e$ such that the fraction is greater than 1 is 3 resp. 4 resp. 34. For this, we define the functions

$$f_p \colon \mathbb{N} \to \mathbb{Q},\ e \mapsto \frac{\mathrm{BKMS}(p,e)}{\mathrm{BM}(p,e)}$$

for $p \in \{2,3,5,7\}$:

$$\begin{aligned}
f_2(e) &= \frac{1}{2}\left(\left(\frac{4}{3}\right)^e + \left(\frac{1}{3}\right)^e\right), & f_2(2) &\approx 0.944, & f_2(3) &\approx 1.204\\
f_3(e) &= \frac{1}{2}\left(\left(\frac{27}{20}\right)^e + \left(\frac{3}{20}\right)^e\right), & f_3(2) &\approx 0.923, & f_2(3) &\approx 1.232\\
f_5(e) &= \frac{1}{2}\left(\left(\frac{25}{21}\right)^e + \left(\frac{1}{21}\right)^e\right), & f_5(3) &\approx 0.844, & f_5(4) &\approx 1.004\\
f_7(e) &= \frac{1}{2}\left(\left(\frac{49}{48}\right)^e + \left(\frac{1}{48}\right)^e\right), & f_7(33) &\approx 0.987, & f_7(34) &\approx 1.008
\end{aligned}$$

We can see, that the fractions $f_p(e)$ are of the form

$$\frac{1}{2}\left(\left(\frac{a}{b}\right)^e + \left(\frac{c}{b}\right)^e\right)$$

with $a, b, c \in \mathbb{N}$, $a - b \geq c$. For the proof of the monotonicity, we can neglect the factor $\frac{1}{2}$ and use that $e$ can only take natural numbers:

$$\begin{aligned}
2f_p(e+1) &= \left(\frac{a}{b}\right)^{e+1} + \left(\frac{c}{b}\right)^{e+1}\\
&= \frac{a}{b}\left(\frac{a}{b}\right)^e + \frac{c}{b}\left(\frac{c}{b}\right)^e\\
&= \left(\frac{a}{b}\right)^e + \frac{a-b}{b}\left(\frac{a}{b}\right)^e + \frac{c}{b}\left(\frac{c}{b}\right)^e && \text{use } a-b \geq c\\
&\geq \left(\frac{a}{b}\right)^e + \frac{c}{b}\left(\frac{a}{c}\right)^e\left(\frac{c}{b}\right)^e + \frac{c}{b}\left(\frac{c}{b}\right)^e && \text{use } a > c, e \geq 1\\
&\geq \left(\frac{a}{b}\right)^e + \frac{c}{b}\cdot\frac{a}{c}\left(\frac{c}{b}\right)^e + \frac{c}{b}\left(\frac{c}{b}\right)^e\\
&= \left(\frac{a}{b}\right)^e + \frac{a+c}{b}\left(\frac{c}{b}\right)^e && \text{use } a+c \geq 2c+b > b\\
&> \left(\frac{a}{b}\right)^e + \left(\frac{c}{b}\right)^e = 2f_p(e)
\end{aligned}$$

So for $q \leq 7$, the bound of Blokhuis and Moorhouse is better exactly for the values of $e$ that are proposed. □

### 3.3.3 Lower Bounds

In [57, Section 4], K.-U. Schmidt gives constructions for additive codes $\mathcal{C} \subset \mathcal{H}_n(\mathbb{F}_{q^2})$ with minimum distance $d$ and $\#\mathcal{C} = q^{n(n-d+1)}$ for the cases $n-d$ odd [57, Thm. 4] and $n$ and $d$ both odd [57, Thm. 5]. He also mentions that linear codes of cardinality $q^n$ with minimum distance $n$ in $\mathcal{H}_n(\mathbb{F}_{q^2})$ are easy to obtain from Theorem 3.5 (since $\mathcal{S}_n(\mathbb{F}_q) \hookrightarrow \mathcal{H}_n(\mathbb{F}_{q^2})$ via

Table 3: Upper and lower bounds for the maximum code size in $\mathcal{H}_n(\mathbb{F}_{q^2})$ with minimum distance at least an even number $d$ for some small numbers $n$ and $q$.

| | $n=2,\ d=2$ | | | | | | | | | | $n=3,\ d=2$ | $n=4,\ d=4$ | | $n=6,\ d=6$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $q=2$ | $q=3$ | $q=4$ | $q=5$ | $q=7$ | $q=8$ | $q=9$ | $q=11$ | $q=13$ | $q=16$ | $q=2$ | $q=2$ | $q=3$ | $q=2$ |
| lower bound | $5^a$ | $15^a$ | $24^b$ | $47^b$ | $97^b$ | $125^b$ | $145^b$ | $215^b$ | $272^b$ | $271^c$ | $64^d$ | $16^e$ | $81^e$ | $64^e$ |
| upper bound | $5^f$ | $15^f$ | $24^b$ | $65^f$ | $175^f$ | $216^g$ | $369^f$ | $671^f$ | $1105^f$ | $1296^g$ | $176^h$ | $86^i$ | $1641^i$ | $1366^i$ |

[a] [9], [b] [8], [c] [28], [d] [57], [e] Theorem 3.5, [17], [f] Theorem 3.9, [g] Corollary 3.12, [h] Theorem 3.8, [i] Theorem 3.10

$\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^2}$) or are constructed, for example, in [17, Thm. 4]. This means that the bound of Theorem 3.8 is tight for $d$ odd. Since a code with minimum distance $d+1$ is a fortiori a code with minimum distance at least $d$, we have a code of cardinality at least $q^{n(n-d)}$ in the case $d < n$ with $d, n$ both even. K.-U. Schmidt leaves it an open problem if, in general, there exist additive codes of size $q^{n(n-d+1)}$ when $d < n$ both even and how to construct them [57, remark after Thm. 5]. In this thesis, a construction for maximum (meaning of size $q^{n(n-1)}$ [57, Thm. 1]) additive codes with $d = 2$ is provided in Theorem 6.1.

It is also known (see, e.g., [9, Remark 4.4]) that the bound of Theorem 3.9 is tight for $n = 2$ and $q = 2, 3$ and, as already mentioned in section 3.3.2, that there is a code of size 24 in $\mathcal{H}_2(\mathbb{F}_{16})$.

Gow et al. [28] give a construction for partial spread sets in $\mathcal{H}_2(\mathbb{F}_{q^2})$ of size $q^2 + q - 1$.

By heuristic search, Cimráková and Fack found partial ovoids of size 48 in $Q^-(5,5)$, of size 98 in $Q^-(5,7)$, of size 126 in $Q^-(5,8)$, of size 146 in $Q^-(5,9)$, of size 216 in $Q^-(5,11)$, and of size 273 in $Q^-(5,13)$ (see [8, Table 2]) which leads to lower bounds for the maximum code size in $\mathcal{H}_2(\mathbb{F}_{q^2})$, $d = 2$, for $q \in \{5, 7, 8, 9, 11, 13\}$.

For some small values of $n$, $q$, and $d \leq n$, where $d$ even, Table 3 summarizes the in each case best lower and upper bounds of those presented up to this point for the maximum code size of codes in $\mathcal{H}_n(\mathbb{F}_{q^2})$ with minimum distance $\geq d$.

# 4 Isometries of Matrix Spaces and Isomorphisms of Rank Metric Codes

The matrix spaces of unrestricted, symmetric, or Hermitian matrices come with natural symmetries to which this section is dedicated. This leads to a concept of isomorphism which will be used for classifying codes in Sections 6.2 and 6.3.

**Definition 4.1.** Let $\mathcal{M} \subset \mathbb{F}_q^{m\times n}$. We shall call two rank metric codes $C_1, C_2 \subset \mathcal{M}$ *isomorphic* if there is a bijective map $f\colon \mathcal{M} \to \mathcal{M}$ from the ambient space $\mathcal{M}$ to itself that is an isometry in terms of the rank distance and fulfills $f(C_1) = C_2$.

For a map $f$ to be an isometry in terms of distance $d$, we actually only demand that $d(a,b) = d(f(a), f(b))$ for all $a$ and $b$. Note that at least Berger [1] uses a stricter definition for the rank distance as he additionally demands (semi-)linearity.

This section shows that the isometries of unrestricted, symmetric, and Hermitian matrices can be described by matrices. Also a possibility to compute the group of isometries in those cases using a graph automorphism program is explained.

The following lemma is useful in all three cases.

**Lemma 4.2.** *Let $\mathcal{M} \subset \mathbb{F}_q^{m\times n}$ and $f\colon \mathcal{M} \to \mathcal{M}$ a bijective map. If $f$ preserves rank distance one, then so does $f^{-1}$.*

*Proof.* Cf. [65, p. 302]. The map

$$f \times f\colon \mathcal{M} \times \mathcal{M} \to \mathcal{M} \times \mathcal{M},\ (A, B) \mapsto (f(A), f(B))$$

is bijective and—since $\mathrm{d_{rk}}(f(A), f(B)) = 1$ if $\mathrm{d_{rk}}(A, B) = 1$—it maps the set

$$\Delta_1 = \{(A, B) \in \mathcal{M} \times \mathcal{M} \mid \mathrm{d_{rk}}(A, B) = 1\}$$

to itself. Thanks to the finiteness of $\mathcal{M} \times \mathcal{M}$, this yields that $(f \times f)|_{\Delta_1}\colon \Delta_1 \to \Delta_1$ is surjective. So if we have $A, B \in \mathcal{M}$ with $\mathrm{d_{rk}}(A, B) = 1$, then $\mathrm{d_{rk}}(f^{-1}(A), f^{-1}(B)) = 1$ as claimed. □

## 4.1 Unrestricted Matrices

**Proposition 4.3.** *Cf. [65, Cor. 3.6]. For a bijection $f\colon \mathbb{F}_q^{m\times n} \to \mathbb{F}_q^{m\times n}$ to be an isometry in terms of the rank distance, it is sufficient to demand that it preserves rank distance one.*

*Proof.* Cf. [65, p. 91ff.]. Let $A, B \in \mathbb{F}_q^{m\times n}$ with $\mathrm{d_{rk}}(A, B) = d$. Then there are matrices $S \in \mathrm{GL}_m(\mathbb{F}_q), T \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $S(A - B)T = \begin{pmatrix} I_d & 0 \\ 0 & 0 \end{pmatrix}$ (see, e.g., [65, Prop. 1.17]). Then it holds for the matrices $C_i = A - S^{-1}\begin{pmatrix} I_i & 0 \\ 0 & 0 \end{pmatrix} T^{-1}$, $i = 0, \ldots, d$, that $\mathrm{d_{rk}}(C_{i-1}, C_i) = 1$, $i = 1, \ldots, d$. Hence, according to the hypothesis, $\mathrm{d_{rk}}(f(C_{i-1}), f(C_i)) = 1$, $i = 1, \ldots, d$. Since $C_0 = A$ and $C_d = B$, it follows that

$$\begin{aligned}
\mathrm{d_{rk}}(f(A), f(B)) &= \mathrm{rk}\left(\sum_{i=1}^{d} \big(f(C_{i-1}) - f(C_i)\big)\right) \\
&\leq \sum_{i=1}^{d} \mathrm{rk}\left(f(C_{i-1}) - f(C_i)\right) \\
&= \mathrm{d_{rk}}(A, B).
\end{aligned}$$

By Lemma 4.2, we also have that $f^{-1}$ preserves rank distance one, so we can use the same argument for $f^{-1}$ and conclude that

$$\mathrm{d_{rk}}(A, B) = \mathrm{d_{rk}}(f^{-1}(f(A)), f^{-1}(f(B))) \leq \mathrm{d_{rk}}(f(A), f(B)) \leq \mathrm{d_{rk}}(A, B). \qquad \square$$

Now that we know that in fact, we are looking for rank distance one preserving bijections, we can use the Fundamental Theorem of Rectangular Matrices. It can be found in the more general setting of matrices over division rings in the book of Wan [65].

**Theorem 4.4** (Fundamental Theorem of Rectangular Matrices)**.** *See, e.g., [65, Thm. 3.4]. Let $m, n \in \mathbb{N}_{\geq 2}$, and $f\colon \mathbb{F}_q^{m\times n} \to \mathbb{F}_q^{m\times n}$ be a bijective map such that $f$ and $f^{-1}$ both preserve rank distance one. Then there are matrices $P \in \mathrm{GL}_m(\mathbb{F}_q)$, $Q \in \mathrm{GL}_n(\mathbb{F}_q)$, and $R \in \mathbb{F}_q^{m\times n}$ and an automorphism $\sigma$ of $\mathbb{F}_q$ such that if $m \neq n$, then*

$$f(X) = P\sigma(X)Q + R \quad \forall X \in \mathbb{F}_q^{m\times n} \tag{1}$$

*and if $m = n$, then either $f$ is of the form (1) or*

$$f(X) = P\sigma(X^{\mathsf{T}})Q + R \quad \forall X \in \mathbb{F}_q^{m\times n}. \tag{2}$$

*Conversely, any map of the form (1) or (2) is bijective and preserves rank distance one.*

The proof uses the concept of maximal sets of rank 1 and maximal sets of rank 2 (for definitions, see [65, Def. 3.3 and Def. 3.5] ). Reproducing this (long) proof is beyond the scope of this thesis. The interested reader is referred to [65, p. 106ff.].

## 4.2 Hermitian Matrices

The case of Hermitian matrices is similar to that of unrestricted matrices.

**Proposition 4.5.** *See, e.g., [65, Cor. 6.6]. For a bijection $f\colon \mathcal{H}_n(\mathbb{F}_{q^2}) \to \mathcal{H}_n(\mathbb{F}_{q^2})$ to be an isometry in terms of the rank distance, it is sufficient to demand that it preserves rank distance one.*

*Proof.* Cf. [65, p. 91ff.]. Let $A, B \in \mathcal{H}_n(\mathbb{F}_{q^2})$ with $\mathrm{d_{rk}}(A, B) = d$. Then there is a matrix $Q \in \mathrm{GL}_n(\mathbb{F}_{q^2})$ such that

$$\overline{Q}^{\mathsf{T}}(A - B)Q = \begin{pmatrix} a_1 & & & & \\ & \ddots & & & \\ & & a_d & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}$$

with $a_i \in \mathbb{F}_q, i = 1, \ldots, d$ (see, e.g., [65, Prop. 1.32]). Thus it holds for the matrices

$$C_i = A - \left(\overline{Q}^{\mathsf{T}}\right)^{-1} \begin{pmatrix} a_1 & & & & \\ & \ddots & & & \\ & & a_i & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} Q^{-1},$$

$i = 0, \ldots, d$, that $\mathrm{d_{rk}}(C_{i-1}, C_i) = 1$, $i = 1, \ldots, d$, and that $C_i \in \mathcal{H}_n(\mathbb{F}_{q^2})$, $i = 0, \ldots, d$. The rest of the proof is analogous to the proof of Proposition 4.3. □

The Fundamental Theorem of Hermitian Matrices is also stated in [65] in the more general context of division rings $D$ possessing an involution $\bar{}\colon D \to D$ fulfilling some properties. It is asserted in [65, Example 1.2] that it holds for $D = \mathbb{F}_{q^2}$ with $\overline{a} = a^q$.

**Theorem 4.6** (Fundamental Theorem of Hermitian Matrices)**.** *[65, Thm. 6.4] Let $q$ be a power of a prime, $n \in \mathbb{N}_{\geq 2}$, and $f\colon \mathcal{H}_n(\mathbb{F}_{q^2}) \to \mathcal{H}_n(\mathbb{F}_{q^2})$ a bijective map such that $f$ and $f^{-1}$ both preserve rank distance one. Then there are matrices $P \in \mathrm{GL}_n(\mathbb{F}_{q^2})$, $H \in \mathcal{H}_n(\mathbb{F}_{q^2})$, $a \in \mathbb{F}_q^*$, and an automorphism $\sigma$ of $\mathbb{F}_{q^2}$ such that*

$$f(X) = a\overline{P}^{\mathsf{T}}\sigma(X)P + H \quad \forall X \in \mathcal{H}_n(\mathbb{F}_{q^2}). \tag{3}$$

*Conversely, any map of the form (3) and its inverse preserves rank distance one.*

The proof is similar to that of Theorem 4.4 and is also omitted. It can be found in [65, p. 323ff.] for the case $n \geq 3$ and in [65, p. 348ff.] for the case $n = 2$.

## 4.3 Symmetric Matrices

For symmetric matrices, there exists a fundamental theorem too, but this case is more complicated.

**Theorem 4.7** (Fundamental Theorem of Symmetric Matrices)**.** *[65, Thm. 5.4] Let $F$ be any field, $n \in \mathbb{N}_{\geq 2}$, and $f\colon \mathcal{S}_n(F) \to \mathcal{S}_n(F)$ a bijective map such that $f$ and $f^{-1}$ both preserve rank distance one. If $\mathcal{S}_n(F) \neq \mathcal{S}_3(\mathbb{F}_2)$, then there are $a \in F^*$, matrices $P \in \mathrm{GL}_n(F)$, $S \in \mathcal{S}_n(F)$, and an automorphism $\sigma$ of $F$ such that*

$$f(X) = aP^{\mathsf{T}}\sigma(X)P + S \quad \forall X \in \mathcal{S}_n(F). \tag{4}$$

*If $\mathcal{S}_n(F) = \mathcal{S}_3(\mathbb{F}_2)$ then $f$ can additionally be a composition of maps of form (4) and the following extra bijective map $\widetilde{f}$:*

$$\widetilde{f}\colon \mathcal{S}_3(\mathbb{F}_2) \to \mathcal{S}_3(\mathbb{F}_2),\ \begin{cases} \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{12} & x_{22} & 0 \\ x_{13} & 0 & x_{33} \end{pmatrix} \mapsto \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{12} & x_{22} & 0 \\ x_{13} & 0 & x_{33} \end{pmatrix} \\ \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{12} & x_{22} & 1 \\ x_{13} & 1 & x_{33} \end{pmatrix} \mapsto \begin{pmatrix} x_{11}+1 & x_{12}+1 & x_{13}+1 \\ x_{12}+1 & x_{22} & 1 \\ x_{13}+1 & 1 & x_{33} \end{pmatrix} \end{cases} \tag{5}$$

*Conversely, the map $\widetilde{f}$ and all maps of the form (4) preserve rank distance one and so do their inverses.*

The proof is similar to that for unrestricted or Hermitian matrices, but more complicated and treats the cases

- $\mathrm{char}(F) \neq 2$,
- $\mathrm{char}(F) = 2$ and $F \neq \mathbb{F}_2$,
- $F = \mathbb{F}_2$ and $n \neq 3$, and
- $F = \mathbb{F}_2$ and $n = 3$

separately. It can be found in [65, p. 231ff., p. 252ff., p. 270ff., and p. 276ff.]. The difficulties of the proof are linked with the fact that the statement of Proposition 4.3 and Proposition 4.5 is not true for symmetric matrices in general which becomes clear by the following:

The map $\widetilde{f}$ preserves rank distance one (see [65, Lemma 5.34]), but is not an isometry in terms of the rank distance as one can see in the following example taken from [65, p. 275]: The zero matrix and $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ obviously have rank distance 2 whereas their images under $\widetilde{f}$, $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, have rank distance 3.

**Proposition 4.8.** *Any map of form (4) is an isometry in terms of the rank distance.*

In the book of Wan, it is proven that maps $f\colon \mathcal{S}_n(F) \to \mathcal{S}_n(F)$ such that both $f$ and $f^{-1}$ preserve rank distance one are isometries in terms of the rank distance in the cases where $\mathrm{char}(F) \neq 2$ (see [65, Cor. 5.6]) and where $F = \mathbb{F}_2$ and $2 \leq n \neq 3$ (see [65, Lemma 5.31]). Here we give a different simple proof for the general case. However, this proof is entirely built on the explicit description in form (4) while in [65], the proof of Theorem 4.7 uses on the statements of [65, Lemma 5.31 and Cor. 5.6].

*Proof.* Let $X, Y \in \mathcal{S}_n(F)$ arbitrary. Then

$$\begin{aligned} f(X) - f(Y) &= \big(aP^{\mathsf{T}}\sigma(X)P + S\big) - \big(aP^{\mathsf{T}}\sigma(Y)P + S\big) = aP^{\mathsf{T}}\big(\sigma(X) - \sigma(Y)\big)P \\ &= aP^{\mathsf{T}}\sigma(X - Y)P. \end{aligned}$$

Since $\sigma$ is a field automorphism, $\mathrm{rk}(X - Y) = \mathrm{rk}(\sigma(X - Y))$. The matrices $P$ and $P^{\mathsf{T}}$ are invertible, so $\mathrm{rk}(P^{\mathsf{T}}\sigma(X - Y)P) = \mathrm{rk}(\sigma(X - Y))$. This implies that $\mathrm{d_{rk}}(f(X), f(Y)) = \mathrm{d_{rk}}(X, Y)$ because $a \in F^*$. □

Actually, those are the only isometries also in the case of $\mathcal{S}_3(\mathbb{F}_2)$ as the following theorem states.

**Theorem 4.9.** *[65, Prop. 5.32] If $f$ is an isometry of $\mathcal{S}_3(\mathbb{F}_2)$, $f$ is of form (4).*

This is proven together with the case $F = \mathbb{F}_2$, $n \neq 3$ of Theorem 4.7 in [65, p. 270ff.].

Summing up, we can state now the converse of Proposition 4.8:

**Theorem 4.10.** *Let $F$ be any field, $n \in \mathbb{N}_{\geq 2}$, and $f\colon \mathcal{S}_n(F) \to \mathcal{S}_n(F)$ an isometry in terms of the rank distance. Then there are $a \in F^*$, matrices $P \in \mathrm{GL}_n(F)$, $S \in \mathcal{S}_n(F)$, and an automorphism $\sigma$ of $F$ such that*

$$f(X) = aP^{\mathsf{T}}\sigma(X)P + S \quad \forall X \in \mathcal{S}_n(F).$$

*Proof.* This follows directly from Theorem 4.7 and Theorem 4.9 together with the fact that any isometry (and its inverse map) in particular preserves rank distance one. □

## 4.4 Connection to Graph Automorphisms

Since it is a nontrivial problem to determine whether two codes are isomorphic, we want to use nauty [44]—which is a well known tool to find graph isomorphisms—to do this for us. For this, we have to translate the matrix spaces $\mathbb{F}_q^{m\times n}$, $\mathcal{S}_n(\mathbb{F}_q)$, and $\mathcal{H}_n(\mathbb{F}_{q^2})$ into graphs in a way that asserts that the group of isometries of the matrix space is isomorphic to the automorphism group of the associated graph. For testing whether two codes are isomorphic, the graph associated to the ambient space—which has to be the same for both codes—is "colored" (a formal definition is given below) for both codes separately. This way, the vertices corresponding to code matrices are distinguishable for nauty. Two codes are isomorphic then if and only if the associated colored graphs are isomorphic. The algorithm used by nauty is described in [42] and [45].

**Definition 4.11.** [44, Section 1] A *graph automorphism* is a permutation of the vertices of a graph such that two vertices $i, j$ are adjacent if and only if their images are adjacent.

**Definition 4.12.** [45, Section 2.1] Let $\Gamma$ be a graph with vertex set $V$. A *coloring* of $\Gamma$ is a surjective function $\pi\colon V \to \{1, \dots, k\}$ for some $k \in \mathbb{N}$. This means that the colors of the vertices are represented by natural numbers.

A *cell* of $\pi$ is the set of vertices with some given color, that is, the preimage $\pi^{-1}(j)$ of some given $j \in \{1, \dots, k\}$.

A *colored graph* $(\Gamma, \pi)$ is a graph $\Gamma$ together with a coloring $\pi$ of $\Gamma$.

**Definition 4.13.** Cf. [45, Section 2.2] An *automorphism of a colored graph* $(\Gamma, \pi)$ is a graph automorphism $g$ with the property that $\pi(g(v)) = \pi(v)$ for all vertices $v$ of $\Gamma$.

This means that an automorphism of a colored graph preserves the colors of the vertices.

The automorphisms of a graph $\Gamma$ (of a colored graph $(\Gamma, \pi)$) form a group under composition. The automorphism group of a colored graph is denoted by $\mathrm{Aut}(\Gamma, \pi)$. In the uncolored case or if the coloring is clear from the context, this group is denoted by $\mathrm{Aut}(\Gamma)$.

Let $\mathcal{M}$ be one of the sets $\mathbb{F}_q^{m\times n}, \mathcal{H}_n(\mathbb{F}_{q^2}), \mathcal{S}_n(\mathbb{F}_q)$ except for $\mathcal{S}_3(\mathbb{F}_2)$. Then the bijections of $\mathcal{M}$ preserving rank distance one are exactly the isometries of $\mathcal{M}$ (see Proposition 4.3, Proposition 4.5, and Theorem 4.7 together with Proposition 4.8) and thus the isometries of $\mathcal{M}$ match the graph automorphisms of the following graph $\Gamma_{\mathcal{M}}$ consisting of:

- $\#\mathcal{M}$ vertices which are numbered by $0, \dots, \#\mathcal{M} - 1$,
- edges connecting vertices $i$ and $j$ for all $0 \leq i, j \leq \#\mathcal{M} - 1$ with $\mathrm{d_{rk}}(M_i, M_j) = 1$ (for the numbering of the matrices which is used for the calculations in this thesis, see appendix B)

To harmonize the subsequent notation, we equip graph $\Gamma_{\mathcal{M}}$ with the trivial coloring

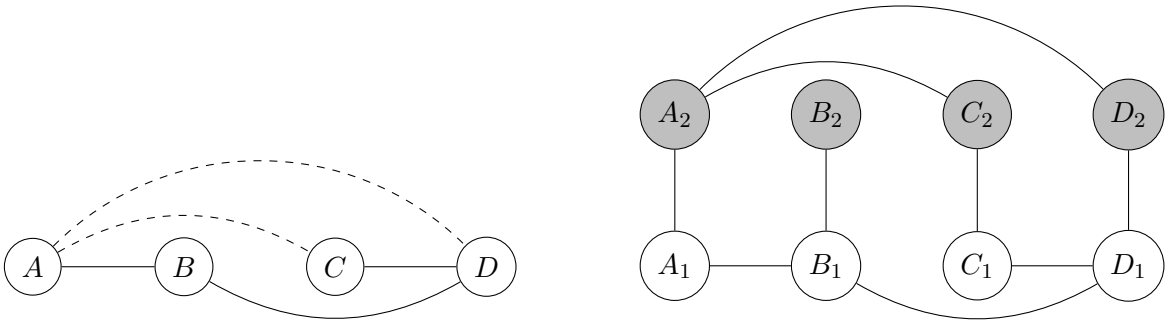
$$\pi\colon \{0, \dots, \#\mathcal{M} - 1\} \to \{1\}.$$

This correspondence between maps that preserve rank distance one and automorphisms of the graph where two vertices are adjacent if and only if the corresponding matrices have rank distance one is easy to justify: Let $g$ be a graph automorphism of $\Gamma_{\mathcal{M}}$ and let $M_i, M_j \in \mathcal{M}$ with $\mathrm{d_{rk}}(M_i, M_j) = 1$ corresponding to the adjacent vertices $i$ and $j$. Those vertices are mapped by $g$ to two adjacent vertices $g(i)$ and $g(j)$, which again correspond to matrices $M_{g(i)}$ and $M_{g(j)}$ with $\mathrm{d_{rk}}(M_{g(i)}, M_{g(j)}) = 1$. Hence the bijection on $\mathcal{M}$ induced by $g$ preserves rank distance one. The other direction is just the same.

Now let $\mathcal{M} = \mathcal{S}_3(\mathbb{F}_2)$. We are interested in creating a graph such that the graph automorphisms correspond to the isomorphisms of $\mathcal{S}_3(\mathbb{F}_2)$ to determine the group of graph automorphisms with nauty [45]. To achieve this graph, every matrix is represented by a vertex and the vertices corresponding to matrices with rank distance one are connected with one kind of edges while the vertices corresponding to matrices with rank distance two are connected by another kind of edge. Then the vertices that are not adjacent automatically correspond to matrices with rank distance three.

This graph has the desired property that its graph automorphisms (which preserve the color of the edges) correspond exactly to the isometries of $\mathcal{S}_3(\mathbb{F}_2)$, but nauty can not handle graphs with different types of edges. Since nauty can handle different types (colors) of vertices instead, the user guide of nauty recommends the following workaround [44, p.58] which is illustrated in Figure 1: For every vertex in the original graph, there are two vertices

Figure 1: Illustration of the workaround for graphs with colored edges in nauty as recommended by the nauty user guide [44]: Edges of different colors (graph on the left) are represented as edges in different layers (graph on the right).




in the new graph—partitioned in two layers with different vertex colors. Each two vertices arising from the same original vertex are connected by an edge. Then the original edges of the first and second color are inserted between the corresponding vertices of the first and second layer, respectively, of the new graph. Then the action of the new automorphism group on the first layer of the new graph is the same as the action of the original automorphism group on the original graph.

Following those instructions, we gain the following nauty-compatible graph $(\Gamma_{\mathcal{S}_3(\mathbb{F}_2)}, \pi)$ consisting of:

- $2 \cdot \#\mathcal{S}_3(\mathbb{F}_2) = 128$ vertices, numbered by $0, \dots, 127$,
- a coloring $\pi\colon \{0, \dots, 127\} \to \{1, 2\}$ with

$$\pi(v) = \begin{cases} 1, & v < 64 \\ 2, & v \geq 64 \end{cases},$$

- edges connecting vertices $i$ and $i + 64$ for all $i = 0, \dots, 63$,
- edges connecting vertices $i$ and $j$ for all $0 \leq i, j \leq 63$ with $\mathrm{d_{rk}}(M_i, M_j) = 1$, and
- edges connecting vertices $i + 64$ and $j + 64$ for all $0 \leq i, j \leq 63$ with $\mathrm{d_{rk}}(M_i, M_j) = 2$.

We can use this graph $\Gamma_{\mathcal{S}_3(\mathbb{F}_2)}$ to confirm Theorem 4.9: Computing $\mathrm{Aut}(\Gamma_{\mathcal{S}_3(\mathbb{F}_2)})$ with nauty reveals that this graph has an automorphism group of size 10752—which is exactly $\#\,\mathrm{GL}_3(\mathbb{F}_2) \cdot \#\mathcal{S}_3(\mathbb{F}_2)$— generated by the permutations $g_0, \dots, g_4$ where

$$\begin{aligned} g_0 = &(1,2)(5,6)(9,10)(13,14)(16,32)(17,34) \\ &(18,33)(19,35)(20,36)(21,38)(22,37)(23,39) \\ &(24,40)(25,42)(26,41)(27,43)(28,44)(29,46) \\ &(30,45)(31,47)(49,50)(53,54)(57,58)(61,62) \end{aligned}$$

$$
\begin{aligned}
&(65,66)(69,70)(73,74)(77,78)(80,96)(81,98)\\
&(82,97)(83,99)(84,100)(85,102)(86,101)(87,103)\\
&(88,104)(89,106)(90,105)(91,107)(92,108)(93,110)\\
&(94,109)(95,111)(113,114)(117,118)(121,122)(125,126),\\
g_1 =&(8,25)(9,24)(10,27)(11,26)(12,29)(13,28)\\
&(14,31)(15,30)(32,36)(33,37)(34,38)(35,39)\\
&(40,61)(41,60)(42,63)(43,62)(44,57)(45,56)\\
&(46,59)(47,58)(48,52)(49,53)(50,54)(51,55)\\
&(72,89)(73,88)(74,91)(75,90)(76,93)(77,92)\\
&(78,95)(79,94)(96,100)(97,101)(98,102)(99,103)\\
&(104,125)(105,124)(106,127)(107,126)(108,121)(109,120)\\
&(110,123)(111,122)(112,116)(113,117)(114,118)(115,119),\\
g_2 =&(1,2,7)(3,5,6)(9,10,15)(11,13,14)(16,32,48)\\
&(17,34,55)(18,39,49)(19,37,54)(20,36,52)(21,38,51)\\
&(22,35,53)(23,33,50)(24,40,56)(25,42,63)(26,47,57)\\
&(27,45,62)(28,44,60)(29,46,59)(30,43,61)(31,41,58)\\
&(65,66,71)(67,69,70)(73,74,79)(75,77,78)(80,96,112)\\
&(81,98,119)(82,103,113)(83,101,118)(84,100,116)(85,102,115)\\
&(86,99,117)(87,97,114)(88,104,120)(89,106,127)(90,111,121)\\
&(91,109,126)(92,108,124)(93,110,123)(94,107,125)(95,105,122),\\
g_3 =&(2,8)(3,9)(4,16)(5,17)(6,24)(7,25)\\
&(12,18)(13,19)(14,26)(15,27)(22,28)(23,29)\\
&(34,40)(35,41)(36,48)(37,49)(38,56)(39,57)\\
&(44,50)(45,51)(46,58)(47,59)(54,60)(55,61)\\
&(66,72)(67,73)(68,80)(69,81)(70,88)(71,89)\\
&(76,82)(77,83)(78,90)(79,91)(86,92)(87,93)\\
&(98,104)(99,105)(100,112)(101,113)(102,120)(103,121)\\
&(108,114)(109,115)(110,122)(111,123)(118,124)(119,125),\ \text{and}\\
g_4 =&(0,1)(2,3)(4,5)(6,7)(8,9)(10,11)(12,13)\\
&(14,15)(16,17)(18,19)(20,21)(22,23)(24,25)(26,27)\\
&(28,29)(30,31)(32,33)(34,35)(36,37)(38,39)\\
&(40,41)(42,43)(44,45)(46,47)(48,49)(50,51)\\
&(52,53)(54,55)(56,57)(58,59)(60,61)(62,63)\\
&(64,65)(66,67)(68,69)(70,71)(72,73)(74,75)(76,77)\\
&(78,79)(80,81)(82,83)(84,85)(86,87)(88,89)(90,91)\\
&(92,93)(94,95)(96,97)(98,99)(100,101)(102,103)\\
&(104,105)(106,107)(108,109)(110,111)(112,113)(114,115)\\
&(116,117)(118,119)(120,121)(122,123)(124,125)(126,127).
\end{aligned}
$$

Here the additional vertices of the second color are written in gray.

A simple brute force computer calculation shows that the generators $g_i$ correspond to maps

$$f_i \colon \mathcal{S}_3(\mathbb{F}_2) \to \mathcal{S}_3(\mathbb{F}_2),\ X \mapsto {P_i}^{\mathsf{T}} X P_i + S_i, \quad i = 0, \ldots, 4,$$

where

$$P_0 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, P_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, P_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, P_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, P_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$S_0 = S_1 = S_2 = S_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \text{and} \quad S_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

This means that any isometry of $\mathcal{S}_3(\mathbb{F}_2)$ can be written in the form (4) which is the statement of Theorem 4.9.

# 5 Automorphism Groups of Codes

To understand the structure of a code, it is useful to consider its automorphism group as it gives information about the symmetries of the code.

**Definition 5.1.** Let $\mathcal{M} \subset \mathbb{F}_q^{m \times n}$ and $\mathcal{C} \subset \mathcal{M}$ be a code in $\mathcal{M}$. Denote the group of isometries from $\mathcal{M}$ to itself by $\mathrm{Aut}(\mathcal{M})$. The *automorphism group of* $\mathcal{C}$ *(with respect to* $\mathcal{M}$*)* $\mathrm{Aut}_{\mathcal{M}}(\mathcal{C})$ is defined to be the setwise stabilizer of $\mathcal{C}$ in $\mathrm{Aut}(\mathcal{M})$. If the ambient space $\mathcal{M}$ is clear from the context, we simply write $\mathrm{Aut}(\mathcal{C})$.

By definition, the automorphism group of a code depends on the ambient space if only because it consists of maps from the ambient space to itself. That is, $\mathrm{Aut}_{\mathcal{M}_1}(\mathcal{C}) \neq \mathrm{Aut}_{\mathcal{M}_2}(\mathcal{C})$ whenever $\mathcal{C} \subset \mathcal{M}_1, \mathcal{M}_2$ and $\mathcal{M}_1 \neq \mathcal{M}_2$. This is not surprising but one should note that even the restriction of those automorphism groups to the code are not isomorphic in general, that is,

$$\{f|_{\mathcal{C}} : \mathcal{C} \to \mathcal{C} \mid f \in \mathrm{Aut}_{\mathcal{M}_1}(\mathcal{C})\} \ncong \{g|_{\mathcal{C}} : \mathcal{C} \to \mathcal{C} \mid g \in \mathrm{Aut}_{\mathcal{M}_2}(\mathcal{C})\}.$$

The following examples shows this:

Let $\mathcal{C} \subset \mathcal{S}_2(\mathbb{F}_3) \subset \mathbb{F}_3^{2\times 2}$,

$$\mathcal{C} = \left\{ A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, C = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\}.$$

From section 4, particularly from formulas (1) and (4), it is clear that every isometry of $\mathcal{S}_2(\mathbb{F}_3)$ can be extended to an isometry of $\mathbb{F}_3^{2\times 2}$. But there exist isometries of $\mathbb{F}_3^{2\times 2}$ such that there exists no isometry of $\mathcal{S}_2(\mathbb{F}_3)$ that acts in the same way on $\mathcal{C}$. Consider the map

$$f \colon \mathbb{F}_3^{2\times 2} \to \mathbb{F}_3^{2\times 2},\ X \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \cdot X \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

This is an isometry of $\mathbb{F}_3^{2\times 2}$ such that $f(\mathcal{C}) = \mathcal{C}$. More precisely, it holds that $f(A) = A$, $f(B) = C$, $f(C) = B$. So it is to show that there is no isometry $g$ of $\mathcal{S}_2(\mathbb{F}_3)$ such that

$g(A) = A$, $g(B) = C$, and $g(C) = B$. We know from section 4.3 that such a map has the form $g(X) = \alpha \begin{pmatrix} a & c \\ b & d \end{pmatrix} X \begin{pmatrix} a & b \\ c & d \end{pmatrix} + S$ with $\alpha \in \mathbb{F}_3^* = \{1, 2\}$. By $g(A) = A$, it is determined that $S$ is the zero matrix. Assume $\alpha = 1$. Then the equations

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 + c^2 & ab + cd \\ ab + cd & b^2 + d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \tag{6}$$

and

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 + 2c^2 & ab + 2cd \\ ab + 2cd & b^2 + 2d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{7}$$

follow from $g(B) = C$ and $g(C) = B$. Note that in $\mathbb{F}_3$, squares can only equal 0 or 1. So it follows from $a^2 + 2c^2 = 1$—which follows from equation (7)—that $a \neq 0, c = 0$. Equation (6) implies that $b^2 + d^2 = 2$ which means that neither $b$ nor $d$ can be 0. Together with $a \neq 0$ and $c = 0$, it follows that $ab + cd \neq 0$ which is a contradiction to equation (6).

Now assume that $\alpha = 2$. Then $g(B) = C$ and $g(C) = B$ result in

$$2 \cdot \begin{pmatrix} a^2 + c^2 & ab + cd \\ ab + cd & b^2 + d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

and

$$2 \cdot \begin{pmatrix} a^2 + 2c^2 & ab + 2cd \\ ab + 2cd & b^2 + 2d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

which—equations multiplied by 2—implies that

$$\begin{pmatrix} a^2 + c^2 & ab + cd \\ ab + cd & b^2 + d^2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \tag{8}$$

and

$$\begin{pmatrix} a^2 + 2c^2 & ab + 2cd \\ ab + 2cd & b^2 + 2d^2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \tag{9}$$

hold. Using the same reasoning as above, the bottom right matrix entry of equation (9) implies that $b = 0, d \neq 0$ and from the top left matrix entry of expression (8) it follows that $a, c \neq 0$. Putting these together results in $ab + cd \neq 0$ which is a contradiction to (8) and since $\alpha \in \{1, 2\}$, it is proved that there exists no isometry $g$ of $\mathcal{S}_2(\mathbb{F}_3)$ such that $g|_{\mathcal{C}} = f|_{\mathcal{C}}$ even though $\mathcal{C} \subset \mathcal{S}_2(\mathbb{F}_3)$.

As checking whether two codes are isomorphic, it is also a nontrivial problem to determine the automorphism group of a code. This problem can be outsourced to nauty in a similar way since the automorphism group $\mathrm{Aut}_{\mathcal{M}}(\mathcal{C})$ can be identified in a natural way with the automorphism group of the colored graph $(\Gamma_{\mathcal{M}}, \pi_{\mathcal{C}})$ where $(\Gamma_{\mathcal{M}}, \pi)$ is the colored graph associated to the ambient space $\mathcal{M}$ and

$$\pi_{\mathcal{C}}(i) = \begin{cases} 1, & M_i \in \mathcal{C} \\ \pi(i) + 1, & M_i \notin \mathcal{C} \end{cases}$$

is a coloring that distinguishes the vertices corresponding to code matrices from the remaining vertices. Nauty provides a set of generators of the automorphism group. Those generators are translated into a matrix representation of form (3) or (4) using a simple brute force computer calculation.

Magma [5] is a useful tool for analyzing the automorphism groups of the classified codes. For instance, it is used to find "nicer" sets of generators—meaning smaller or better illustratable.

# 6 Constructions

For constructing codes, different approaches—depending on the problem size—are used and described in this section. Firstly, two series of Hermitian codes are presented of which one improves the general lower bound on the maximum code size when $2 = d < n$, $n$ even. Secondly, two different exact algorithms for finding the maximum code size are described which entail a classification of maximum codes. The first exact algorithm is a successive execution of an orderly algorithm while the second one utilizes Cliquer. The resulting code representatives are converted using maps from Section 4 in order to obtain "nicer" representatives. Since the exact algorithms are unsuitable for larger fields or matrix sizes, the last subsection is dedicated to a heuristic clique search approach.

## 6.1 Two Series of Hermitian Codes

**Theorem 6.1.** *$\mathcal{C} = \{(m_{i,j})_{1\le i,j\le n} \in \mathcal{H}_n(\mathbb{F}_{q^2}) \mid m_{i,i} = 0\ \forall 1 \le i \le n\}$ is an additive code with minimum distance 2 of size $q^{n(n-1)}$ in $\mathcal{H}_n(\mathbb{F}_{q^2})$.*

*Proof.* It is obvious that $\mathcal{C}$ is an additive subgroup of $\mathcal{H}_n(\mathbb{F}_{q^2})$ and that $\#\mathcal{C} = q^{n(n-1)}$. So there is only to show that $\mathrm{rk}(M) \ge 2$ for all $M \in \mathcal{C} \setminus \{0\}$. Let $M = (m_{i,j})_{1\le i,j\le n} \in \mathcal{C} \setminus \{0\}$. Then there are $k$ and $l$ $(k < l)$ such that $m_{k,l} = a \neq 0$. Thus, the submatrix $M_{k,l} = (m_{i,j})_{i,j\in\{k,l\}} = \begin{pmatrix} 0 & a \\ \overline{a} & 0 \end{pmatrix}$ has rank 2 and therefore $M$ has rank at least 2. □

Theorem 6.1 shows that K.-U. Schmidt's upper bound for additive codes [57, Thm. 1] is tight not only if $n$ or $d$ is odd or if $n = d$ but also in the case $d = 2$. However, it remains unknown whether the bound is tight for $4 \le d < n$ both even.

**Theorem 6.2.** *Let $\mathcal{D} = \left\{ \begin{pmatrix} 1 & a \\ \overline{a} & 0 \end{pmatrix} \mid a \in \mathbb{F}_{q^2}^* \right\}$. Then $\mathcal{C} = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \cup \mathcal{D}$ is a code in $\mathcal{H}_2(\mathbb{F}_{q^2})$ with minimum distance 2 of size $q^2 + 1$.*

*Proof.* This is obvious since the difference matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & a \\ \overline{a} & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & a \\ \overline{a} & -1 \end{pmatrix}$, and $\begin{pmatrix} 0 & a-b \\ \overline{a}-\overline{b} & 0 \end{pmatrix}$ have full rank for all $a, b \in \mathbb{F}_{q^2}^*$, $a \neq b$. □

In case of $\mathbb{F}_4$, this construction is optimal; additionally, we have the following statement:

**Theorem 6.3.** *The construction from Theorem 6.2 can not be augmented.*

*Proof.* Let $M = \begin{pmatrix} g & b \\ \overline{b} & h \end{pmatrix} \in \mathcal{H}_n(\mathbb{F}_{q^2})$ be an arbitrary Hermitian matrix and $D_a = \begin{pmatrix} 1 & a \\ \overline{a} & 0 \end{pmatrix}$. Consider $\det(M - D_a) = (g-1)h - (b-a)\overline{(b-a)}$. If $g = 1$ or $h = 0$, then either $b \neq 0$, so we can choose $a = b$ and found a matrix $D_b \in \mathcal{D} \subset \mathcal{C}$ with $\mathrm{d_{rk}}(M, D_b) < 2$, or $b = 0$, so $M$

has rank distance less than 2 to the zero or identity matrix. So assume $g \neq 1$ and $h \neq 0$. Then $(g-1)h \in \mathbb{F}_q^*$ and since the norm map $x \mapsto x\overline{x}$ is a surjective group homomorphism from $\mathbb{F}_{q^2}^*$ to $\mathbb{F}_q^*$ (see, e.g., [46, Thm. 1.4.9]), there are $\frac{q^2-1}{q-1} = q+1$ elements $x \in \mathbb{F}_{q^2}^*$ such that $x\overline{x} = (g-1)h$. Hence, there are $q+1$ different choices for $a$ such that $\det(M - D_a) = 0$, and at least $q$ of them are in $\mathbb{F}_{q^2}^*$, so we again found a matrix in $\mathcal{D}$ that prevents $M$ from augmenting the code $\mathcal{C}$. □

In [28, Thm. 17], a similar construction of maximal partial spread sets in $\mathcal{H}_2(\mathbb{F}_{q^2})$ of size $N$ is given for every integer $N$ in the interval $[q^2, q^2+q-1]$.

## 6.2 An Orderly Generation Approach

One way to gain a classification of maximum codes with minimum distance $\geq d$ in the matrix space $\mathcal{M}$ is the orderly generation approach. The aim of this approach is to reject isomorphic copies as early as possible in the generation process. The setting is as follows:

**Definition 6.4.** See, e.g., [53, p. 106]. A property $\mathscr{P}$ of sets is called *hereditary* if whenever $S$ satisfies property $\mathscr{P}$ then also all subsets of $S$ satisfy property $\mathscr{P}$.

Let $G$ be a group acting on the set $V$. Let $\mathscr{P}$ be a hereditary property of subsets of $V$ which is independent of the group action, that is, a subset $X$ of $V$ fulfills $\mathscr{P}$ if and only if $g.X$ fulfills $\mathscr{P}$ for all $g \in G$. We denote $M_k = \{X \subset V \mid \#X = k \text{ and } X \text{ fullfills } \mathscr{P}\}$. Then $G$ acts on each set $M_k$ by

$$G \times M_k \to M_k,\ (g, X) \mapsto g.X$$

which we call the *induced group action* of $G$ on $M_k$. Let $S_k \subset M_k$ be a transversal. An orderly algorithm creates a transversal $S_{k+1} \subset M_{k+1}$ from $S_k$ by taking advantage of total orders on each set $M_k$ which are mutually compatible in some sense. The theory of orderly generation was developed by Read [50] in a very general context.

In the following, the orderly algorithm by Royle [53] is presented in Algorithm 1. It is a specialized and simplified version of the general framework by McKay [43] and is completely sufficient for our purpose. In this algorithm, the underlying orders are not obvious but they are implicitly contained in a function $\theta\colon 2^V \to 2^V$ satisfying

1. $\theta(X)$ is an orbit of $G_X$ on X for all $X \subset V$ and
2. $\theta(g.X) = g.\theta(X)$ for all $g \in G$ and all $X \subset V$.

The correctness of Algorithm 1 is proven by the following theorem.

**Theorem 6.5.** *See [53, Thm. 2.1]. Let $G$ be a group acting on a set $V$, $\mathscr{P}$ a hereditary property of subsets of $V$ that is independent of the group action, and $S_k$ a set containing precisely one representative from each $G$-orbit on $k$-sets of $V$ that have property $\mathscr{P}$. Additionally, let $\theta\colon 2^V \to 2^V$ be a function satisfying*

1. *$\theta(X)$ is an orbit of $G_X$ on $X$ for all $X \subset V$ and*
2. *$\theta(g.X) = g.\theta(X)$ for all $g \in G$ and all $X \subset V$.*

*Then the set $S_{k+1}$ as defined by Algorithm 1 has the stated properties, that is, it contains precisely one representative from each $G$-orbit on $(k+1)$-sets of $V$ that have property $\mathscr{P}$.*

**Algorithm 1:** Orderly Algorithm by Royle, see [53, p. 7].

**Input**: Set $V$,
group $G$ acting on $V$,
function $\theta\colon 2^V \to 2^V$ satisfying properties 1 and 2,
hereditary property $\mathscr{P}$ that is independent of the group action,
set $S_k$ containing precisely one representative from each $G$-orbit on $k$-sets of $V$ that have property $\mathscr{P}$

**Output**: Set $S_{k+1}$ containing precisely one representative from each $G$-orbit on $(k+1)$-sets of $V$ that have property $\mathscr{P}$

```
S_{k+1} ← ∅;
foreach X ∈ S_k do
    foreach orbit representative x of G_X on V \ X do
        if x ∈ θ(X ∪ {x}) and X ∪ {x} has property 𝒫 then
            S_{k+1} ← S_{k+1} ∪ {X ∪ {x}};
        end
    end
end
return S_{k+1};
```

In [53], Royle does not explicitly demand that $\mathscr{P}$ should be independent of the group action, but otherwise this search for representatives makes no sense.

Theorem 6.5 means that Algorithm 1 is an orderly algorithm (see [53, p. 107]). Here the map $\theta$ takes responsibility that the set $S_{k+1}$ contains exactly one representative of each isomorphism class.

*Proof.* See, [53, p. 107]. Let $X' \subset V$ be a set of cardinality $k+1$ satisfying property $\mathscr{P}$. We have to show that $S_{k+1}$ contains exactly one isomorphic copy of $X'$.

First we show that $S_{k+1}$ contains at least one isomorphic copy of $X'$. Let $x \in \theta(X')$. Since $\theta(X') \subset X'$, $X = X' \setminus \{x\}$ has cardinality $k$. Remember that $\mathscr{P}$ is hereditary, so $X$ satisfies $\mathscr{P}$. Therefore there is a set $Y$ in the same $G$-orbit as $X$ contained in $S_k$, say $Y = g.X$.

Augmenting $Y$, at some stage, we consider an element $y \in V$ that is in the same orbit under $G_Y$ as $g.x$, that is, there is an element $g' \in G$ such that $y = (g'g).x$ and $Y = g'.Y = (g'g).X$. Then $Y \cup \{y\} = (g'g).X'$, so $Y \cup \{y\}$ satisfies property $\mathscr{P}$ and from $x \in \theta(X')$ follows

$$y = (g'g).x \in (g'g).\theta(X') = \theta((g'g).X') = \theta(Y \cup \{y\}).$$

This means that $Y \cup \{y\} = (g'g).X'$ is contained in $S_{k+1}$.

Now suppose that $S_{k+1}$ contains at least two different isomorphic copies $Y'$ and $Z'$ of $X'$, that is, $Y' = g.X'$ and $Z' = h.X'$ for some $g, h \in G$. Then there exist $y \in Y'$ and $z \in Z'$ such that $Y'$ is augmented from $Y = Y' \setminus \{y\} \in S_k$ and $Z'$ is augmented from $Z = Z' \setminus \{z\} \in S_k$. Hence $y \in \theta(Y')$ and $z \in \theta(Z')$. Reformulating this gives that $g^{-1}.y$ and $h^{-1}.z$ both are in $\theta(X')$, so there is an element $f \in G_{X'}$ such that

$$g^{-1}.y = (fh^{-1}).z. \tag{10}$$

Now we see that

$$\begin{aligned} Y &= g.(X' \setminus \{g^{-1}.y\}) \\ &= g.(X' \setminus \{(fh^{-1}).z\}) \\ &= (gf).(X' \setminus \{h^{-1}.z\}) \\ &= (gfh^{-1}).Z. \end{aligned}$$

So $Z$ is an isomorphic copy of $Y$ and since $Y, Z \in S_k$, this means that $Y = Z$ and $gfh^{-1} \in G_Y$. Together with (10), this means that $y$ and $z$ are in the same orbit under $G_Y$ which is a contradiction to line 3 of Algorithm 1. □

**Procedure** `Augment`$(S_k; \mathcal{M}, (\Gamma_\mathcal{M}, \pi), d)$.

```
1  G ← Aut(Γ_M, π);
2  S_{k+1} ← ∅;
3  forall the X ∈ S_k do
4  |  forall the v ∈ M \ X do
5  |  |  if v has the lowest label in its orbit under G_X then
6  |  |  |  if d_rk(v, v') ≥ d for all v' ∈ X then
7  |  |  |  |  if v is in the same orbit under G_{X∪{v}} as the vertex with canonical
   |  |  |  |  label 0 then
8  |  |  |  |  |  S_{k+1} ← S_{k+1} ∪ {X ∪ {v}};
9  |  |  |  |  end
10 |  |  |  end
11 |  |  end
12 |  end
13 end
14 return S_{k+1};
```

We now want to use this orderly algorithm to find all isomorphism classes of maximum codes with a minimum distance at least a fixed number $d$ in a matrix space $\mathcal{M} \in \{\mathbb{F}_q^{m\times n}, \mathcal{S}_n(\mathbb{F}_q), \mathcal{H}_n(\mathbb{F}_{q^2})\}$. For this, we need to specify $V$, $G$, $\mathscr{P}$, and $\theta$.

As set $V$ and group $G$, we use the vertex set of the colored graph $(\Gamma_\mathcal{M}, \pi)$ described in section 4.4 and its automorphism group. The property $\mathscr{P}$ is a pairwise rank distance of at least $d$, which is obviously hereditary. In case $\mathcal{M} = \mathcal{S}_3(\mathbb{F}_2)$, we additionally demand that the set is a subset of the vertices of the first color. It remains to define the map $\theta$ such that it fulfills properties 1 and 2 required by Theorem 6.5.

Royle describes in [53, p. 107] how $\theta$ can be defined in the case that $V$ is the vertex set of a graph $\Gamma$ and $G$ is the automorphism group of $\Gamma$. For this, we need to know that—besides determining the automorphism group of a graph—nauty can perform an operation called canonical labeling. A canonical labeling of a (colored) graph is a renumeration of the vertices in a manner that is independent of the initial labeling and such that isomorphic graphs become identical by canonical labeling (see [44, p. 3]). There are different possibilities to define a canonical labeling; the one used by nauty is designed to be computed efficiently, see, e.g., [53, p. 106]. In addition, the coloring (remember Definition 4.12) of a canonical colored graph as produced by nauty has the property to be nondecreasing, see [44, p 3].

**Algorithm 2:** Algorithm for classification of maximum codes, based on Algorithm 1.

**Input**: Matrix set $\mathcal{M} \in \{\mathbb{F}_q^{m\times n}, \mathcal{S}_n(\mathbb{F}_q), \mathcal{H}_n(\mathbb{F}_{q^2})\}$, lower bound $d$ for the minimum distance

**Output**: Maximum code size $m$ and set $\mathcal{S}_m$ containing precisely one representative of each isomorphism class of maximum codes

```
Create colored graph (Γ_M, π);
S_0 ← {∅};
k ← 0;
while S_k ≠ ∅ do
    S_{k+1} ← Augment(S_k; M, (Γ_M, π), d);
    k ← k + 1;
end
return (k − 1, S_{k−1});
```

With this knowledge, Royle defines $\theta$ in the following way: For a fixed set $X \in 2^V$, equip graph $\Gamma$ with the coloring

$$\pi(v) = \begin{cases} 1, & v \in X \\ 2, & v \notin X \end{cases}$$

and label this colored graph canonically using nauty. Let $v$ be the vertex of $\Gamma$ that is mapped to 0 by canonical labeling. Then define $\theta(X)$ to be the orbit of $G_X$ which contains $v$. Procedure `Augment()` is the adaption of Algorithm 1. Algorithm 2 executes Procedure `Augment()` repeatedly, each with the output of the preceding step and starting with $S_0 = \emptyset$.

Algorithm 1 and therefore Procedure `Augment()` can be parallelized by partitioning the input set $S_k$ and combining the output sets. Using this, the implementation of Algorithm 2 is split up via Bash script into 8 processes. Anyway, it turns out that this approach is pointless in almost all symmetric and Hermitian cases. Table 4 lists the cardinality of $S_k$ and the computation time on an Intel Core i7 3770 for each single augmentation step for each completed and three aborted calculations. The calculation time in the case $\mathcal{M} = \mathcal{H}_2(\mathbb{F}_{16})$ adds up to approximately 15 hours. In Figure 2, the values of $\#S_k$ are plotted for the completely computed runs (black lines) and the aborted ones (gray lines). Note the logarithmic scale. The dashed continuation of case $\mathcal{H}_2(\mathbb{F}_{25})$ is an estimation based on the augmentation of two of the 55,691,107 representatives of size eight. On the basis of those two computation times which amount to approximately 11.5 and 49.5 hours it is estimated that the total computation time of this case would reach 200,000 years.

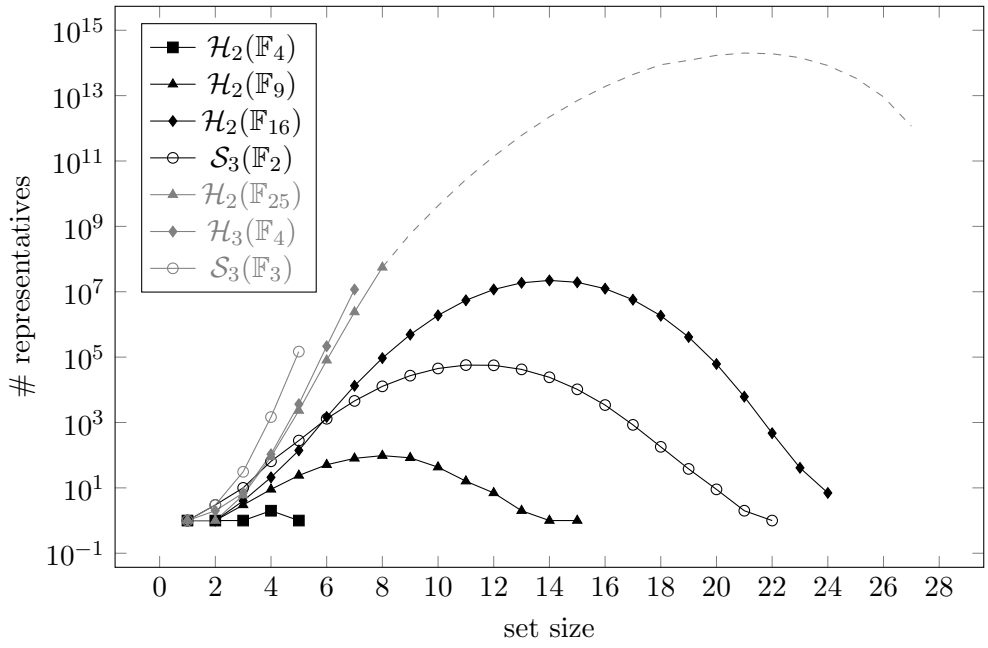
In the following, the codes classified by the orderly algorithm are described in detail. At this, a code of size $N$ is denoted by $\mathcal{C}_N$ and by $\mathcal{C}_N^{(i)}$ if there is more than one isomorphism class. Orbits that are significant for the description of the code are denoted by $\mathcal{O}_M$, where $M$ is the length of the orbit, or $\mathcal{O}_M^{(j)}$ if there is more than one interesting orbit of that length.

Since $\mathcal{H}_n(\mathbb{F}_{q^2})$ is a vector space over $\mathbb{F}_q$ (but not over $\mathbb{F}_{q^2}$), in case $q > 2$, it makes sense to say that matrices are collinear or to speak about lines. It should be noted that collinearity is invariant under the action of $\mathrm{Aut}_{\mathcal{M}}(\mathcal{C})$ if $\mathcal{M} \in \{\mathbb{F}_q^{m\times n}, \mathcal{S}_n(\mathbb{F}_q), \mathcal{H}_n(\mathbb{F}_{q^2})\}$ since the automorphisms then are of the form (1), (2), (3), or (4).

Table 4: Number of representatives ($\#S_k$) and computing time in seconds seperately for each set size $k$ in all completed (on the left) and aborted (on the right) cases.

| $k$ | $\mathcal{H}_2(\mathbb{F}_4)$ | | $\mathcal{H}_2(\mathbb{F}_9)$ | | $\mathcal{H}_2(\mathbb{F}_{16})$ | | $\mathcal{S}_3(\mathbb{F}_2)$ | | $\mathcal{H}_2(\mathbb{F}_{25})$ | | $\mathcal{H}_3(\mathbb{F}_4)$ | | $\mathcal{S}_3(\mathbb{F}_3)$ | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | # repr. | time | # repr. | time | # repr. | time | # repr. | time | # repr. | time | # repr. | time | # repr. | time |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 2 | 1 | 3 |
| 2 | 1 | 0 | 1 | 0 | 1 | 0 | 3 | 0 | 1 | 1 | 2 | 6 | 3 | 4 |
| 3 | 1 | 0 | 3 | 0 | 4 | 1 | 10 | 0 | 6 | 2 | 7 | 6 | 31 | 5 |
| 4 | 2 | 0 | 9 | 0 | 21 | 0 | 65 | 0 | 89 | 2 | 107 | 6 | 1467 | 10 |
| 5 | 1 | 0 | 24 | 0 | 140 | 1 | 280 | 0 | 2317 | 11 | 3646 | 17 | 147559 | 203 |
| 6 | – | – | 51 | 1 | 1473 | 1 | 1304 | 0 | 80105 | 159 | 215129 | 370 | ?? | ?? |
| 7 | | | 80 | 0 | 13275 | 5 | 4575 | 1 | 2395603 | 3566 | 11732851 | 17996 | | |
| 8 | | | 97 | 0 | 93442 | 31 | 12762 | 2 | 55691107 | 82018 | ?? | ?? | | |
| 9 | | | 83 | 0 | 489215 | 170 | 27103 | 4 | ?? | ?? | | | | |
| 10 | | | 43 | 0 | 1900458 | 706 | 44940 | 7 | | | | | | |
| 11 | | | 16 | 0 | 5477871 | 2205 | 57069 | 10 | | | | | | |
| 12 | | | 7 | 0 | 11750349 | 5140 | 56194 | 11 | | | | | | |
| 13 | | | 2 | 1 | 18757108 | 8949 | 42183 | 10 | | | | | | |
| 14 | | | 1 | 0 | 22235145 | 11472 | 24183 | 6 | | | | | | |
| 15 | | | 1 | 0 | 19450778 | 10945 | 10335 | 3 | | | | | | |
| 16 | | | – | – | 12424803 | 7695 | 3421 | 1 | | | | | | |
| 17 | | | | | 5705868 | 3937 | 847 | 1 | | | | | | |
| 18 | | | | | 1848255 | 1452 | 180 | 0 | | | | | | |
| 19 | | | | | 412293 | 386 | 38 | 0 | | | | | | |
| 20 | | | | | 61675 | 75 | 9 | 0 | | | | | | |
| 21 | | | | | 6157 | 11 | 2 | 0 | | | | | | |
| 22 | | | | | 471 | 2 | 1 | 0 | | | | | | |
| 23 | | | | | 41 | 0 | – | – | | | | | | |
| 24 | | | | | 7 | 1 | | | | | | | | |
| 25 | | | | | – | – | | | | | | | | |

Figure 2: Number of representatives for each set size $k$ in all completed (black) and aborted (gray) cases. The dashed continuation is an estimate.



### 6.2.1 Maximum Code in $\mathcal{H}_2(\mathbb{F}_4)$ with $d = 2$

In $\mathcal{H}_2(\mathbb{F}_4)$, the maximum code size is 5 and there exists only one isomorphism class. One representative

$$\mathcal{C}_5 = \left\{ M_4 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, M_8 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, M_{13} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, M_{14} = \begin{pmatrix} 1 & 1+X \\ X & 1 \end{pmatrix}, M_{15} = \begin{pmatrix} 1 & X \\ 1+X & 1 \end{pmatrix} \right\}$$

consists of all five rank-1-matrices.

The size of the automorphism group is 120, there are three orbits: The zero matrix is a fixed point, the second orbit consists of the code (5 rank-1-matrices) and the third orbit consists of the 10 rank-2-matrices.

The automorphism group is generated by the two maps

$$g_1 \colon \mathcal{H}_2(\mathbb{F}_4) \to \mathcal{H}_2(\mathbb{F}_4), \quad C \mapsto \overline{P_1}^{\mathsf{T}} \cdot C \cdot P_1 \quad \text{with } P_1 = \begin{pmatrix} 0 & X \\ 1 & 1 \end{pmatrix}$$

and

$$g_2 \colon \mathcal{H}_2(\mathbb{F}_4) \to \mathcal{H}_2(\mathbb{F}_4), \quad C \mapsto \overline{C}.$$

The restrictions of the automorphisms to the code, generated by

$$\begin{aligned} g_1|_{\mathcal{C}_5} &= (M_4, M_8, M_{13}, M_{14}, M_{15}) \text{ and} \\ g_2|_{\mathcal{C}_5} &= (M_{14}, M_{15}), \end{aligned}$$

form the full symmetric group on the 5 elements of the code.

### 6.2.2 Maximum Code in $\mathcal{H}_2(\mathbb{F}_9)$ with $d = 2$

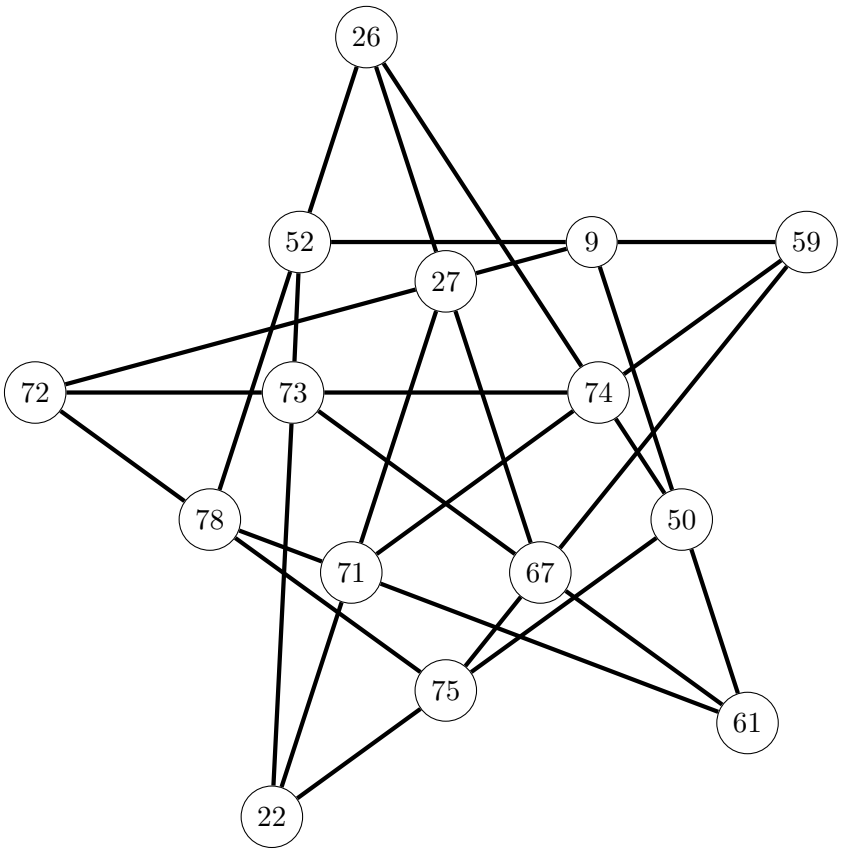
In $\mathcal{H}_2(\mathbb{F}_9)$, a maximum code with minimum distance 2 is of size 15 and there is only one isomorphism class of maximum codes. Via the connection given by Lemma 3.7, this confirms the result of Ebert and Hirschfeld [18, Section 4] who found that a maximum partial spread in $H(3, 9)$ has size 16.

The following set constitutes a representative of a maximum code:

$$\begin{aligned} \mathcal{C}_{15} = \Bigg\{ & M_9 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, && M_{22} = \begin{pmatrix} 2 & 1+2X \\ 1+X & 0 \end{pmatrix}, && M_{26} = \begin{pmatrix} 2 & 2+X \\ 2+2X & 0 \end{pmatrix}, \\ & M_{27} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, && M_{50} = \begin{pmatrix} 2 & 2+2X \\ 2+X & 1 \end{pmatrix}, && M_{52} = \begin{pmatrix} 2 & 1+X \\ 1+2X & 1 \end{pmatrix}, \\ & M_{59} = \begin{pmatrix} 0 & 2+2X \\ 2+X & 2 \end{pmatrix}, && M_{61} = \begin{pmatrix} 0 & 1+X \\ 1+2X & 2 \end{pmatrix}, && M_{67} = \begin{pmatrix} 1 & 1+2X \\ 1+X & 2 \end{pmatrix}, \\ & M_{71} = \begin{pmatrix} 1 & 2+X \\ 2+2X & 2 \end{pmatrix}, && M_{72} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, && M_{73} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \\ & M_{74} = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}, && M_{75} = \begin{pmatrix} 2 & 2X \\ X & 2 \end{pmatrix}, && M_{78} = \begin{pmatrix} 2 & X \\ 2X & 2 \end{pmatrix} \Bigg\} \end{aligned}$$

The 15 matrices of $\mathcal{C}_{15}$ lie on 15 lines, such that every matrix lies on three lines and every line goes through three matrices. Figure 3 is a stellar realization (cf., e.g., [3, fig. 2]) of this configuration known as Cremona-Richmond configuration. This geometrical configuration is

Figure 3: Stucture of maximum code in $\mathcal{H}_2(\mathbb{F}_9)$.




described in detail in [51]. Richmond shows that if one chooses six points in general linear position, that is, such that no five of them lie in one hyperplane, from a four-dimensional space (according to [16, 38], Richmond means projective space), then the intersection points of a line through two points and a space through the remaining four points (he calls those intersection points diagonal points) lie by threes on 15 lines. For the history of the Cremona-Richmond configuration, see [3, chapter 6].

By the relation of section 3.3.1, the code $\mathcal{C}_{15}$ corresponds to a maximal partial spread in $H(3,9)$ which is related to the Kummer surface (see [18, Sections 4, 5]). We remark that a connection between the Kummer surface and the Cremona-Richmond configuration is also given in [19] in a different context.

The automorphism group of $\mathcal{C}_{15}$ has size 720 and is generated by the following two maps:

$$g_1 \colon \mathcal{H}_2(\mathbb{F}_9) \to \mathcal{H}_2(\mathbb{F}_9), \qquad C \mapsto \overline{P_1}^{\mathsf{T}} \cdot \overline{C} \cdot P_1 \qquad \text{with } P_1 = \begin{pmatrix} 1+X & 2X \\ 1+X & 1+X \end{pmatrix}$$

$$g_2 \colon \mathcal{H}_2(\mathbb{F}_9) \to \mathcal{H}_2(\mathbb{F}_9), \qquad C \mapsto \overline{P_2}^{\mathsf{T}} \cdot \overline{C} \cdot P_2 + I_2 \qquad \text{with } P_2 = \begin{pmatrix} 0 & 1+X \\ 2+2X & 0 \end{pmatrix}$$

Their restrictions to $\mathcal{C}_{15}$ are as follows:

$$g_1|_{\mathcal{C}_{15}} = (M_{26}, M_{59}, M_{61}, M_{22}, M_{72})\,(M_9, M_{50}, M_{75}, M_{78}, M_{52})\,(M_{27}, M_{74}, M_{67}, M_{71}, M_{73})$$
$$g_2|_{\mathcal{C}_{15}} = (M_{26}, M_{71})\,(M_{59}, M_{50})\,(M_{61}, M_{52})\,(M_{22}, M_{67})$$

Applying $g_1$ to $\mathcal{C}_{15}$ as illustrated in Figure 3 means rotating the figure by 72°. The second generator $g_2$ is not visualizable that nice. However, the fixed points of $g_2|_{\mathcal{C}_{15}}$ are $M_{72}$ and those six matrices that together form the three lines through $M_{72}$, namely $M_9$ and $M_{27}$, $M_{73}$ and $M_{74}$, and $M_{75}$ and $M_{78}$.

Outside of the code, there is an orbit $\mathcal{O}_6$ of length 6. The representative of the maximum code is chosen such that $\mathcal{O}_6$ contains the zero matrix and the identity matrix.

$$\mathcal{O}_6 = \Bigg\{ M_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, M_{13} = \begin{pmatrix} 1 & 1+2X \\ 1+X & 0 \end{pmatrix}, M_{17} = \begin{pmatrix} 1 & 2+X \\ 2+2X & 0 \end{pmatrix},$$
$$M_{32} = \begin{pmatrix} 0 & 2+2X \\ 2+X & 1 \end{pmatrix}, M_{34} = \begin{pmatrix} 0 & 1+X \\ 1+2X & 1 \end{pmatrix}, M_{36} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Bigg\}$$

Looking at the restrictions of $g_1$ and $g_2$ to $\mathcal{O}_6$,

$$g_1|_{\mathcal{O}_6} = (M_{13}, M_{34}, M_{32}, M_{17}, M_{36})$$

and

$$g_2|_{\mathcal{O}_6} = (M_0, M_{36}),$$

one can see that the restriction of the automorphism group to $\mathcal{O}_6$ is the symmetric group on 6 elements.

This orbit of length 6 attracts our attention since Richmond's construction starts with six points. Indeed, it turns out that the fifteen matrices of the code are determined by the orbit of length 6 in the following way: Choose two matrices of $\mathcal{O}_6$ (note that $\binom{6}{2} = 15$), put a line through these two matrices, and the third point on each of these lines is exactly one element in the code $\mathcal{C}_{15}$. Equivalently, one can construct the points of $\mathcal{C}_{15}$ by intersecting a line through two matrices of $\mathcal{O}_6$ with the space trough the remaining four matrices of $\mathcal{O}_6$. This accords exactly with Richmond's construction. Which matrix of $\mathcal{C}_{15}$ lays on which line through matrices of $\mathcal{O}_6$ is illustrated in Table 5.

When partitioning $\mathcal{O}_6 = \{M_{a_1}, M_{a_2}\} \cup \{M_{b_1}, M_{b_2}\} \cup \{M_{c_1}, M_{c_2}\}$ into three sets of size two, the three matrices $M_a, M_b, M_c \in \mathcal{C}_{15}$ which are the third points on a line through each two matrices of one subset are collinear. Since there are exactly 15 possibilities of partitioning $\mathcal{O}_6$ in sets of 2, this corresponds precisely to the 15 lines of $\mathcal{C}_{15}$.

Table 5: Construction of $\mathcal{C}_{15}$: The matrices of $\mathcal{O}_6$ to put a line through to obtain a matrix in the code $\mathcal{C}_{15}$ are marked with an "X".

| | Matrix | $M_9$ | $M_{22}$ | $M_{26}$ | $M_{27}$ | $M_{50}$ | $M_{52}$ | $M_{59}$ | $M_{61}$ | $M_{67}$ | $M_{71}$ | $M_{72}$ | $M_{73}$ | $M_{74}$ | $M_{75}$ | $M_{78}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| lies on line through matrices | $M_0$ | | X | X | | | | X | X | | | X | | | | |
| | $M_{13}$ | X | | X | | | | | | | X | | X | | X | |
| | $M_{17}$ | X | X | | | | | | | X | | | | X | | X |
| | $M_{32}$ | | | | X | | X | | X | | | | | X | X | |
| | $M_{34}$ | | | | X | X | | X | | | | | X | | | X |
| | $M_{36}$ | | | | | X | X | | | X | X | X | | | | |

### 6.2.3 The Isomorphism Classes of Maximum Codes in $\mathcal{H}_2(\mathbb{F}_{16})$ with $d = 2$

In $\mathcal{H}_2(\mathbb{F}_{16})$, the maximum size of a code with minimum distance 2 is 24 and there are seven isomorphism classes of maximum codes. Figures 4, 5, 7, 8, and 9 show collinearity (as thin lines) and full lines (as thick lines) in the codes of type 1, 2, 3, 6, and 7. In those figures, additionally, the orbits of the automorphisms groups are shaded in gray. Type 4 contains no collinear points and type 5 only a single full line. For each type a representative is described in detail in the following.

**Type 1:** The automorphism group of $\mathcal{C}_{24}^{(1)}$ is of size 12 and has one orbit $\mathcal{O}_4$ of length 4 outside the code. The representative can be chosen such that $\mathcal{O}_4 = \{M_0, M_{16}, M_{32}, M_{48}\}$ consists of the matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, where $a \in \{0, 1, X^2 + X^3, 1 + X^2 + X^3\} = \mathbb{F}_4 \subset \mathbb{F}_{16}$.

The code $\mathcal{C}_{24}^{(1)}$ itself is partitioned in two orbits of length 12:

$$\begin{aligned}
\mathcal{O}_{12}^{(1)} = \Big\{ M_1 &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, & M_2 &= \begin{pmatrix} 0 & 1+X+X^2+X^3 \\ X & 0 \end{pmatrix}, \\
M_6 &= \begin{pmatrix} 0 & 1+X+X^2 \\ X+X^2 & 0 \end{pmatrix}, & M_8 &= \begin{pmatrix} 0 & X^2 \\ X^3 & 0 \end{pmatrix}, \\
M_{12} &= \begin{pmatrix} 0 & X^2+X^3 \\ X^2+X^3 & 0 \end{pmatrix}, & M_{13} &= \begin{pmatrix} 0 & 1+X^2+X^3 \\ 1+X^2+X^3 & 0 \end{pmatrix}, \\
M_{23} &= \begin{pmatrix} 1 & X+X^2 \\ 1+X+X^2 & 0 \end{pmatrix}, & M_{31} &= \begin{pmatrix} 1 & X \\ 1+X+X^2+X^3 & 0 \end{pmatrix}, \\
M_{41} &= \begin{pmatrix} X^2+X^3 & 1+X^2 \\ 1+X^3 & 0 \end{pmatrix}, & M_{43} &= \begin{pmatrix} X^2+X^3 & X+X^3 \\ 1+X+X^3 & 0 \end{pmatrix}, \\
M_{51} &= \begin{pmatrix} 1+X^2+X^3 & X+X^2+X^3 \\ 1+X & 0 \end{pmatrix}, & M_{53} &= \begin{pmatrix} 1+X^2+X^3 & 1+X^3 \\ 1+X^2 & 0 \end{pmatrix} \Big\}
\end{aligned}$$

and

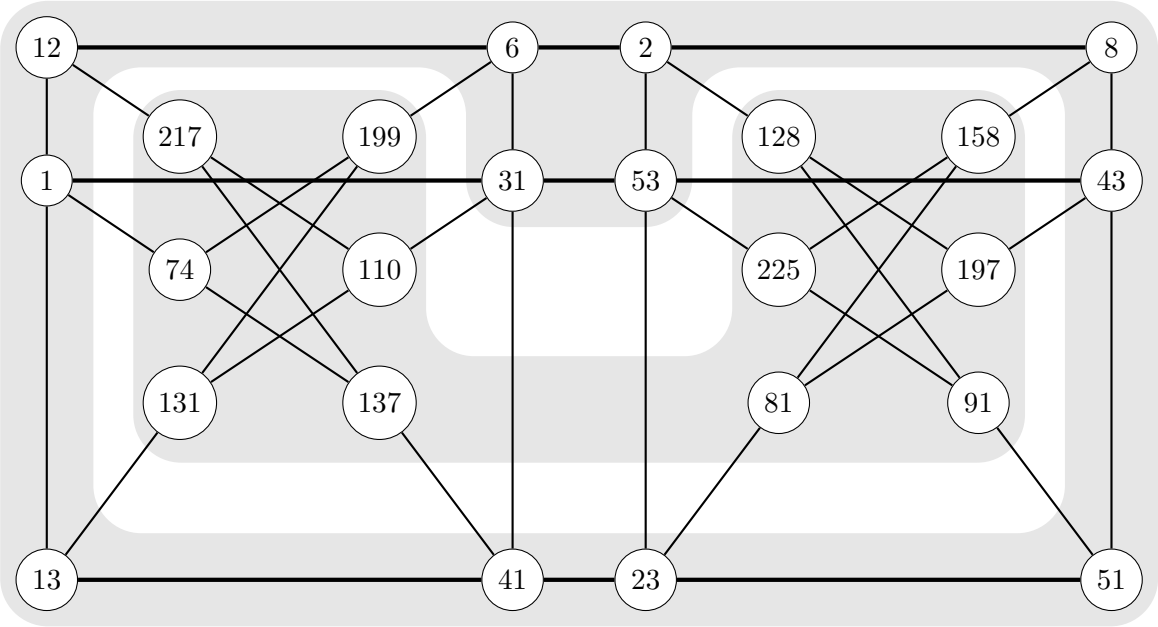
$$\begin{aligned}
\mathcal{O}_{12}^{(2)} = \Big\{ M_{74} &= \begin{pmatrix} 0 & 1+X+X^3 \\ X+X^3 & 1 \end{pmatrix}, & M_{81} &= \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \\
M_{91} &= \begin{pmatrix} 1 & X+X^3 \\ 1+X+X^3 & 1 \end{pmatrix}, & M_{110} &= \begin{pmatrix} X^2+X^3 & 1+X \\ X+X^2+X^3 & 1 \end{pmatrix}, \\
M_{128} &= \begin{pmatrix} 0 & 0 \\ 0 & X^2+X^3 \end{pmatrix}, & M_{131} &= \begin{pmatrix} 0 & X+X^2+X^3 \\ 1+X & X^2+X^3 \end{pmatrix}, \\
M_{137} &= \begin{pmatrix} 0 & 1+X^2 \\ 1+X^3 & X^2+X^3 \end{pmatrix}, & M_{158} &= \begin{pmatrix} 1 & 1+X \\ X+X^2+X^3 & X^2+X^3 \end{pmatrix}, \\
M_{197} &= \begin{pmatrix} 0 & 1+X^3 \\ 1+X^2 & 1+X^2+X^3 \end{pmatrix}, & M_{199} &= \begin{pmatrix} 0 & X+X^2 \\ 1+X+X^2 & 1+X^2+X^3 \end{pmatrix}, \\
M_{217} &= \begin{pmatrix} 1 & 1+X^2 \\ 1+X^3 & 1+X^2+X^3 \end{pmatrix}, & M_{225} &= \begin{pmatrix} X^2+X^3 & 1 \\ 1 & 1+X^2+X^3 \end{pmatrix} \Big\}.
\end{aligned}$$

The orbit $\mathcal{O}_{12}^{(1)}$ consists of three full lines whereas the second orbit $\mathcal{O}_{12}^{(2)}$ considered separately contains no collinear points (see Figure 4). Outside of the code $\mathcal{C}_{24}^{(1)}$, there are further 19 orbits of size 12 additionally to the already mentioned orbit $\mathcal{O}_4$.

The automorphism group $\mathrm{Aut}(\mathcal{C}_{24}^{(1)})$ is generated by the maps

$$g_1 \colon \mathcal{H}_2(\mathbb{F}_{16}) \to \mathcal{H}_2(\mathbb{F}_{16}), \qquad C \mapsto \overline{P_1}^{\mathsf{T}} \cdot \sigma(C) \cdot P_1 + S_1$$
$$\text{with} \qquad P_1 = \begin{pmatrix} 1+X+X^3 & 0 \\ 1+X^2 & 1 \end{pmatrix} \text{ and } S_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Figure 4: Stucture of maximum code in $\mathcal{H}_2(\mathbb{F}_{16})$, type 1.




where $\sigma\colon \mathbb{F}_{16} \to \mathbb{F}_{16}$, $x \mapsto x^2$ is the Frobenius automorphism and

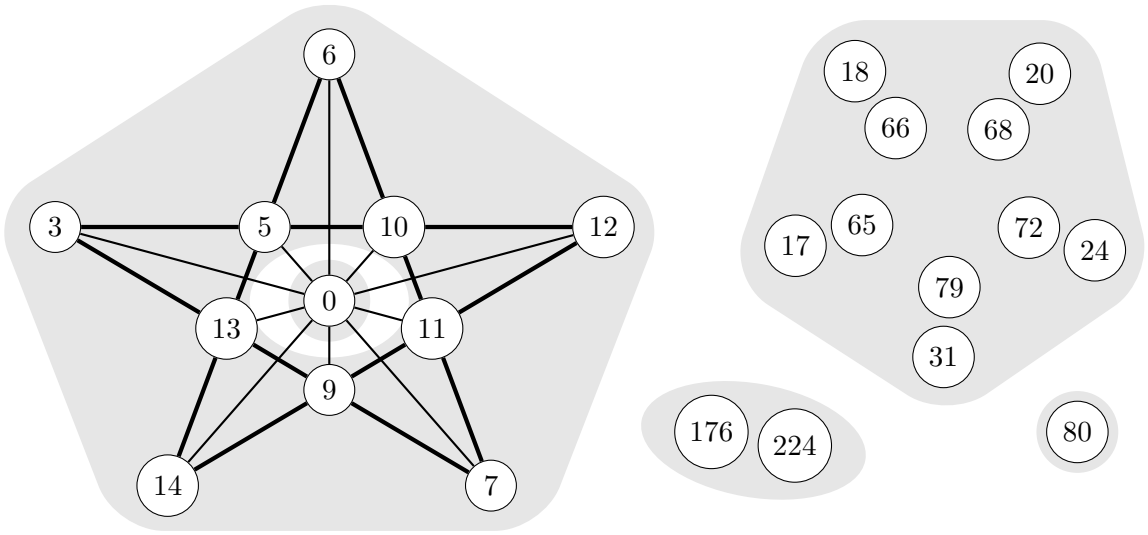
$$g_2\colon \mathcal{H}_2(\mathbb{F}_{16}) \to \mathcal{H}_2(\mathbb{F}_{16}), \qquad C \mapsto \overline{P_2}^{\mathsf{T}} \cdot \overline{C} \cdot P_2 + S_2$$
$$\text{with} \qquad P_2 = \begin{pmatrix} 1 & 0 \\ X + X^3 & 1 + X^2 \end{pmatrix} \text{ and } S_2 = \begin{pmatrix} 1 + X^2 + X^3 & 0 \\ 0 & 0 \end{pmatrix}.$$

Magma tells that $\mathrm{Aut}(\mathcal{C}_{24}^{(1)})$ is isomorphic to the dicyclic group $\mathrm{Dic}_3 \cong C_3 \rtimes C_4$ where $C_n$ denotes the cyclic group of order $n$. The restrictions of the generators to $\mathcal{O}_4$ and $\mathcal{C}_{24}^{(1)}$ are as follows:

$$\begin{aligned}
g_1|_{\mathcal{O}_4} &= (M_0, M_{16}, M_{48}, M_{32}),\\
g_2|_{\mathcal{O}_4} &= (M_0, M_{48})(M_{16}, M_{32}),\\
g_1|_{\mathcal{C}_{24}^{(1)}} &= (M_1, M_{43}, M_{31}, M_{53})(M_2, M_{13}, M_8, M_{41})(M_6, M_{23}, M_{12}, M_{51})\\
&\quad (M_{74}, M_{81}, M_{110}, M_{91})(M_{128}, M_{199}, M_{158}, M_{217})(M_{131}, M_{225}, M_{137}, M_{197}),\\
g_2|_{\mathcal{C}_{24}^{(1)}} &= (M_1, M_{41}, M_{12}, M_{31}, M_{13}, M_6)(M_2, M_{43}, M_{23}, M_8, M_{53}, M_{51})\\
&\quad (M_{74}, M_{137}, M_{217}, M_{110}, M_{131}, M_{199})(M_{81}, M_{158}, M_{225}, M_{91}, M_{128}, M_{197}).
\end{aligned}$$

**Type 2:** $\mathrm{Aut}(\mathcal{C}_{24}^{(2)})$ decomposes $\mathcal{C}_{24}^{(2)}$ into the following orbits: Two fixed points—the representative is chosen such that those are the zero matrix $M_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and the identity

Figure 5: Stucture of maximum code in $\mathcal{H}_2(\mathbb{F}_{16})$, type 2.




matrix $M_{80} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$—, an orbit

$$\mathcal{O}_2 = \left\{ M_{176} = \begin{pmatrix} 1+X^2+X^3 & 0 \\ 0 & X^2+X^3 \end{pmatrix}, \quad M_{224} = \begin{pmatrix} X^2+X^3 & 0 \\ 0 & 1+X^2+X^3 \end{pmatrix} \right\},$$

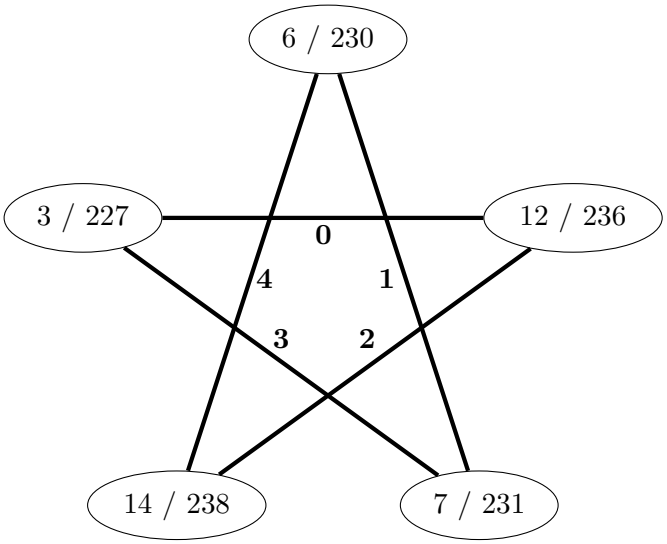
of length 2 and two orbits of length 10, namely

$$\begin{aligned} \mathcal{O}_{10}^{(1)} = \Big\{ M_3 &= \begin{pmatrix} 0 & X+X^2+X^3 \\ 1+X & 0 \end{pmatrix}, & M_5 &= \begin{pmatrix} 0 & 1+X^3 \\ 1+X^2 & 0 \end{pmatrix}, \\ M_6 &= \begin{pmatrix} 0 & 1+X+X^2 \\ X+X^2 & 0 \end{pmatrix}, & M_7 &= \begin{pmatrix} 0 & X+X^2 \\ 1+X+X^2 & 0 \end{pmatrix}, \\ M_9 &= \begin{pmatrix} 0 & 1+X^2 \\ 1+X^3 & 0 \end{pmatrix}, & M_{10} &= \begin{pmatrix} 0 & 1+X+X^3 \\ X+X^3 & 0 \end{pmatrix}, \\ M_{11} &= \begin{pmatrix} 0 & X+X^3 \\ 1+X+X^3 & 0 \end{pmatrix}, & M_{12} &= \begin{pmatrix} 0 & X^2+X^3 \\ X^2+X^3 & 0 \end{pmatrix}, \\ M_{13} &= \begin{pmatrix} 0 & 1+X^2+X^3 \\ 1+X^2+X^3 & 0 \end{pmatrix}, & M_{14} &= \begin{pmatrix} 0 & 1+X \\ X+X^2+X^3 & 0 \end{pmatrix} \Big\} \end{aligned}$$

and

$$\begin{aligned} \mathcal{O}_{10}^{(2)} = \Big\{ M_{17} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, & M_{18} &= \begin{pmatrix} 1 & 1+X+X^2+X^3 \\ X & 0 \end{pmatrix}, \\ M_{20} &= \begin{pmatrix} 1 & X^3 \\ X^2 & 0 \end{pmatrix}, & M_{24} &= \begin{pmatrix} 1 & X^2 \\ X^3 & 0 \end{pmatrix}, \\ M_{31} &= \begin{pmatrix} 1 & X \\ 1+X+X^2+X^3 & 0 \end{pmatrix}, & M_{65} &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \\ M_{66} &= \begin{pmatrix} 0 & 1+X+X^2+X^3 \\ X & 1 \end{pmatrix}, & M_{68} &= \begin{pmatrix} 0 & X^3 \\ X^2 & 1 \end{pmatrix}, \\ M_{72} &= \begin{pmatrix} 0 & X^2 \\ X^3 & 1 \end{pmatrix}, & M_{79} &= \begin{pmatrix} 0 & X \\ 1+X+X^2+X^3 & 1 \end{pmatrix} \Big\}. \end{aligned}$$

Figure 6: The lines of the pentagram of Figure 5 resp. Figure 9 as elements of $\mathbb{F}_5$.




The matrices in $\mathcal{O}_{10}^{(1)}$ form five full lines and the zero matrix lies on further five lines spanned by matrices of $\mathcal{O}_{10}^{(1)}$ as Figure 5 shows. However, the other orbits of $\mathcal{C}_{24}^{(2)}$ contain no collinear points.

Outside of the code, there are each two orbits of lengths 2, 4, and 5, five orbits of length 10, and eight orbits of length 20.

The automorphism group $\mathrm{Aut}(\mathcal{C}_{24}^{(2)})$ has order 40 and is generated by the three maps $g_1$, $g_2$, and $g_3$ with

$$g_i \colon \mathcal{H}_2(\mathbb{F}_{16}) \to \mathcal{H}_2(\mathbb{F}_{16}), \quad C \mapsto \overline{P_i}^{\mathsf{T}} \cdot \sigma_i(C) \cdot P_i$$
$$\text{with} \quad P_1 = \begin{pmatrix} X^2+X+1 & 0 \\ 0 & 1 \end{pmatrix}, P_2 = \begin{pmatrix} X & 0 \\ 0 & 1 \end{pmatrix}, \text{ and } P_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

where $\sigma_1 = \mathrm{id}_{\mathbb{F}_{16}}$ is the identity on $\mathbb{F}_{16}$, $\sigma_2 \colon \mathbb{F}_{16} \to \mathbb{F}_{16}$, $x \mapsto x^2$ is the Frobenius automorphism, and $\sigma_3 \colon \mathbb{F}_{16} \to \mathbb{F}_{16}$, $x \mapsto \overline{x}$ is the conjugation.

Their restrictions to $\mathcal{C}_{24}^{(2)}$ are the following:

$$\begin{aligned}
g_1|_{\mathcal{C}_{24}^{(2)}} =& (M_3, M_6, M_{12}, M_7, M_{14})(M_5, M_{10}, M_{11}, M_9, M_{13}) \\
& (M_{17}, M_{18}, M_{20}, M_{24}, M_{31})(M_{65}, M_{66}, M_{68}, M_{72}, M_{79}) \\
g_2|_{\mathcal{C}_{24}^{(2)}} =& (M_3, M_{10}, M_{12}, M_5)(M_6, M_9)(M_7, M_{11}, M_{14}, M_{13}) \\
& (M_{17}, M_{18}, M_{24}, M_{20})(M_{65}, M_{66}, M_{72}, M_{68}) \\
& (M_{176}, M_{224}) \\
g_3|_{\mathcal{C}_{24}^{(2)}} =& (M_{17}, M_{65})(M_{18}, M_{66})(M_{20}, M_{68})(M_{24}, M_{72})(M_{31}, M_{79}) \\
& (M_{176}, M_{224})
\end{aligned}$$

In Figure 5, $g_1$ acts as a rotation by 72° of the pentagram and the pentagonal orbit, $g_2^2$

as a reflection with respect to the vertical axis of the pentagram and the inner pentagon, and $g_3$ as the transposition of the inner and the outer pentagon and the two matrices of $\mathcal{O}_2$.

Magma tells that $\mathrm{Aut}(\mathcal{C}_{24}^{(2)})$ is isomorphic to $C_2 \times (\mathbb{F}_5 \rtimes \mathbb{F}_5^*)$ where $C_2$ is the cyclic group of order 2 and $\mathbb{F}_5 \rtimes \mathbb{F}_5^*$ is the Frobenius group of order 20. The group of the restrictions of the automorphisms to the orbit $\mathcal{O}_{10}^{(1)}$ is isomorphic to $\mathbb{F}_5 \rtimes \mathbb{F}_5^*$ and generated by $g_1|_{\mathcal{O}_{10}^{(1)}}$ and $g_2|_{\mathcal{O}_{10}^{(1)}}$. If one identifies the lines of the pentagram of Figure 5 with $\mathbb{F}_5$ as done in Figure 6, the actions of those two restrictions on the lines of the pentagram correspond to the actions of "+1" and "·2". This means that we can identify $\mathbb{F}_5 \rtimes \mathbb{F}_5^*$ explicitly with the affine general linear group $\mathrm{AGL}_1(\mathbb{F}_5)$.

**Type 3:** The decomposition of $\mathcal{C}_{24}^{(3)}$ into orbits under its automorphism group also contains two fixed points that were chosen to be the zero matrix $M_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and the identity matrix $M_{80} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Besides them, this code contains seven orbits of length 2, namely

$$\mathcal{O}_2^{(1)} = \left\{ M_3 = \begin{pmatrix} 0 & X+X^2+X^3 \\ 1+X & 0 \end{pmatrix}, \quad M_{12} = \begin{pmatrix} 0 & X^2+X^3 \\ X^2+X^3 & 0 \end{pmatrix} \right\},$$

$$\mathcal{O}_2^{(2)} = \left\{ M_5 = \begin{pmatrix} 0 & 1+X^3 \\ 1+X^2 & 0 \end{pmatrix}, \quad M_{10} = \begin{pmatrix} 0 & 1+X+X^3 \\ X+X^3 & 0 \end{pmatrix} \right\},$$

$$\mathcal{O}_2^{(3)} = \left\{ M_7 = \begin{pmatrix} 0 & X+X^2 \\ 1+X+X^2 & 0 \end{pmatrix}, \quad M_{14} = \begin{pmatrix} 0 & 1+X \\ X+X^2+X^3 & 0 \end{pmatrix} \right\},$$

$$\mathcal{O}_2^{(4)} = \left\{ M_{11} = \begin{pmatrix} 0 & X+X^3 \\ 1+X+X^3 & 0 \end{pmatrix}, \quad M_{13} = \begin{pmatrix} 0 & 1+X^2+X^3 \\ 1+X^2+X^3 & 0 \end{pmatrix} \right\},$$

$$\mathcal{O}_2^{(5)} = \left\{ M_{22} = \begin{pmatrix} 1 & 1+X+X^2 \\ X+X^2 & 0 \end{pmatrix}, \quad M_{70} = \begin{pmatrix} 0 & 1+X+X^2 \\ X+X^2 & 1 \end{pmatrix} \right\},$$

$$\mathcal{O}_2^{(6)} = \left\{ M_{31} = \begin{pmatrix} 1 & X \\ 1+X+X^2+X^3 & 0 \end{pmatrix}, \quad M_{79} = \begin{pmatrix} 0 & X \\ 1+X+X^2+X^3 & 1 \end{pmatrix} \right\},$$

and

$$\mathcal{O}_2^{(7)} = \left\{ M_{41} = \begin{pmatrix} X^2+X^3 & 1+X^2 \\ 1+X^3 & 0 \end{pmatrix}, \quad M_{137} = \begin{pmatrix} 0 & 1+X^2 \\ 1+X^3 & X^2+X^3 \end{pmatrix} \right\}$$

and two orbits of length 4 which are

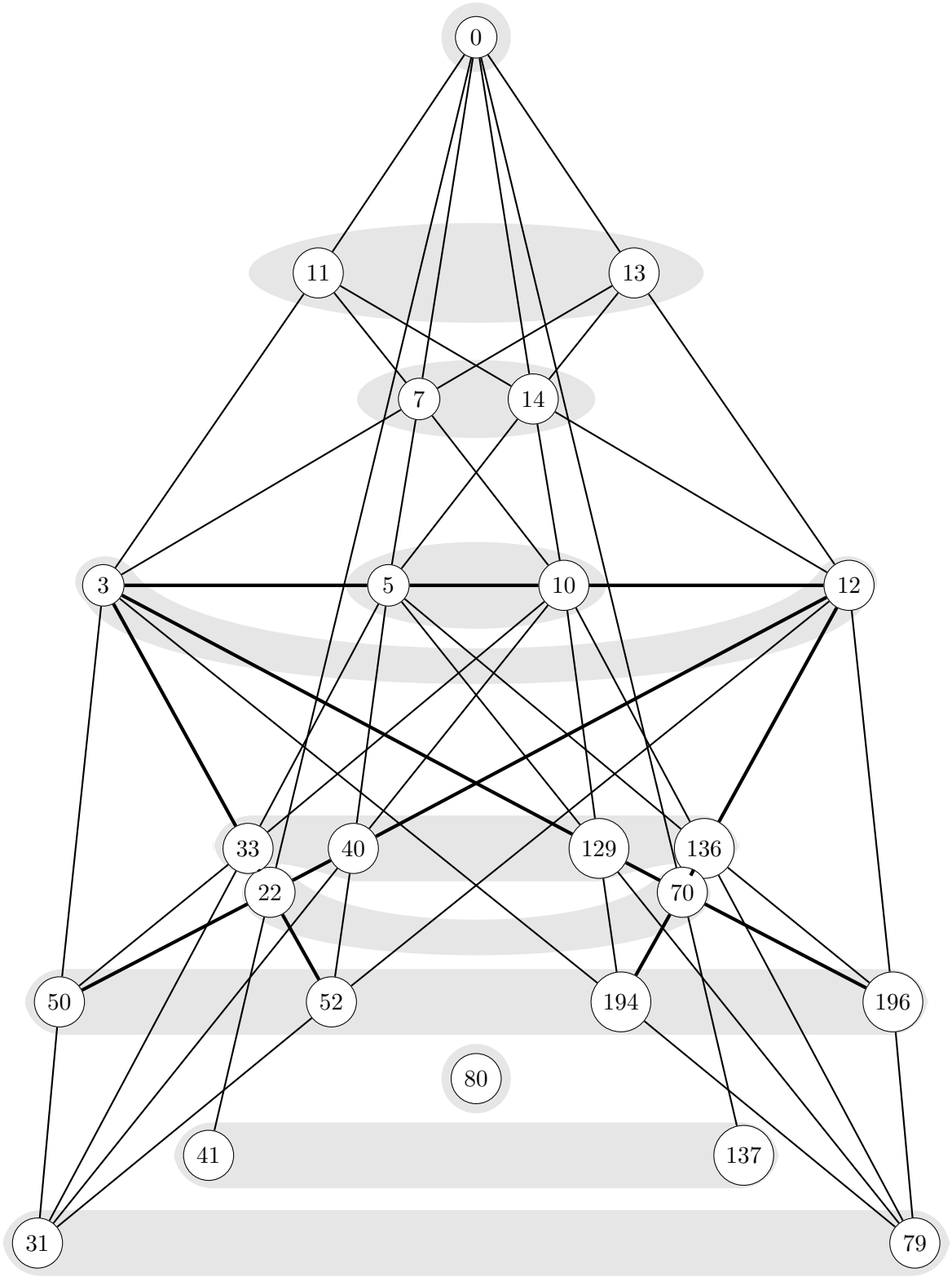
$$\mathcal{O}_4^{(1)} = \left\{ M_{33} = \begin{pmatrix} X^2+X^3 & 1 \\ 1 & 0 \end{pmatrix}, \quad M_{40} = \begin{pmatrix} X^2+X^3 & X^2 \\ X^3 & 0 \end{pmatrix}, \right.$$
$$\left. M_{129} = \begin{pmatrix} 0 & 1 \\ 1 & X^2+X^3 \end{pmatrix}, \quad M_{136} = \begin{pmatrix} 0 & X^2 \\ X^3 & X^2+X^3 \end{pmatrix} \right\}$$

and

$$\mathcal{O}_4^{(2)} = \left\{ M_{50} = \begin{pmatrix} 1+X^2+X^3 & 1+X+X^2+X^3 \\ X & 0 \end{pmatrix}, \quad M_{52} = \begin{pmatrix} 1+X^2+X^3 & X^3 \\ X^2 & 0 \end{pmatrix}, \right.$$
$$\left. M_{194} = \begin{pmatrix} 0 & 1+X+X^2+X^3 \\ X & 1+X^2+X^3 \end{pmatrix}, \quad M_{196} = \begin{pmatrix} 0 & X^3 \\ X^2 & 1+X^2+X^3 \end{pmatrix} \right\}.$$

Those matrices are arranged in lines as Figure 7 shows. Note that, although it looks differently, the matrices $M_0$ and $M_7$ lie on a different line with $M_5$ as the matrices $M_{40}$ and

Figure 7: Stucture of maximum code in $\mathcal{H}_2(\mathbb{F}_{16})$, type 3.



$M_{52}$. The same applies to the lines through $M_0$, $M_{14}$, and $M_{10}$ and through $M_{10}$, $M_{129}$, and $M_{194}$.

Outside of the code, there are further 14 fixed points, 41 orbits of length 2, and 34 orbits of length 4. The overall 16 fixed points of $\mathrm{Aut}(\mathcal{C}_{24}^{(3)})$ are exactly the matrices $\begin{pmatrix} a & b \\ \overline{b} & a \end{pmatrix}$ with $a \in \mathbb{F}_4 = \{0, 1, X^2+X^3, 1+X^2+X^3\}$ and $b \in \{0, X, 1+X+X^2, 1+X^2\} = X \cdot \mathbb{F}_4$.

The automorphism group has order 4 and is isomorphic to the Klein four-group $C_2 \times C_2$. It is generated by the two maps

$$g_1 \colon \mathcal{H}_2(\mathbb{F}_{16}) \to \mathcal{H}_2(\mathbb{F}_{16}), \qquad C \mapsto \overline{P_1}^{\mathsf{T}} \cdot C \cdot P_1 \qquad \text{with } P_1 = \begin{pmatrix} 0 & X^2 \\ 1 & 0 \end{pmatrix}$$

and

$$g_2 \colon \mathcal{H}_2(\mathbb{F}_{16}) \to \mathcal{H}_2(\mathbb{F}_{16}), \qquad C \mapsto \overline{P_2}^{\mathsf{T}} \cdot \overline{C} \cdot P_2 \qquad \text{with } P_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In Figure 7,

$$\begin{aligned} g_1|_{\mathcal{C}_{24}^{(3)}} =& (M_3, M_{12})(M_5, M_{10})(M_7, M_{14})(M_{11}, M_{13}) \\ & (M_{22}, M_{70})(M_{31}, M_{79})(M_{33}, M_{136})(M_{40}, M_{129})(M_{41}, M_{137})(M_{50}, M_{196})(M_{52}, M_{194}) \end{aligned}$$

acts as a reflection with respect to the vertical axis while

$$g_2|_{\mathcal{C}_{24}^{(3)}} = (M_{22}, M_{70})(M_{31}, M_{79})(M_{33}, M_{129})(M_{40}, M_{136})(M_{41}, M_{137})(M_{50}, M_{194})(M_{52}, M_{196})$$

interchanges the two lower spikes.

**Type 4:** The code $\mathcal{C}_{24}^{(4)}$ contains no collinear points at all. $\mathrm{Aut}(\mathcal{C}_{24}^{(4)})$ partitions it into an orbit

$$\begin{aligned} \mathcal{O}_4 = \Big\{ M_0 &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, & M_{18} &= \begin{pmatrix} 1 & 1+X+X^2+X^3 \\ X & 0 \end{pmatrix}, \\ M_{66} &= \begin{pmatrix} 0 & 1+X+X^2+X^3 \\ X & 1 \end{pmatrix}, & M_{80} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Big\} \end{aligned}$$

of length 4 and an orbit of length 20, namely

$$\begin{aligned} \mathcal{O}_{20} = \Big\{ M_{37} &= \begin{pmatrix} X^2+X^3 & 1+X^3 \\ 1+X^2 & 0 \end{pmatrix}, & M_{55} &= \begin{pmatrix} 1+X^2+X^3 & X+X^2 \\ 1+X+X^2 & 0 \end{pmatrix}, \\ M_{103} &= \begin{pmatrix} X^2+X^3 & X+X^2 \\ 1+X+X^2 & 1 \end{pmatrix}, & M_{117} &= \begin{pmatrix} 1+X^2+X^3 & 1+X^3 \\ 1+X^2 & 1 \end{pmatrix}, \\ M_{129} &= \begin{pmatrix} 0 & 1 \\ 1 & X^2+X^3 \end{pmatrix}, & M_{132} &= \begin{pmatrix} 0 & X^3 \\ X^2 & X^2+X^3 \end{pmatrix}, \\ M_{138} &= \begin{pmatrix} 0 & 1+X+X^3 \\ X+X^3 & X^2+X^3 \end{pmatrix}, & M_{141} &= \begin{pmatrix} 0 & 1+X^2+X^3 \\ 1+X^2+X^3 & X^2+X^3 \end{pmatrix}, \\ M_{147} &= \begin{pmatrix} 1 & X+X^2+X^3 \\ 1+X & X^2+X^3 \end{pmatrix}, & M_{150} &= \begin{pmatrix} 1 & 1+X+X^2 \\ X+X^2 & X^2+X^3 \end{pmatrix}, \\ M_{152} &= \begin{pmatrix} 1 & X^2 \\ X^3 & X^2+X^3 \end{pmatrix}, & M_{159} &= \begin{pmatrix} 1 & X \\ 1+X+X^2+X^3 & X^2+X^3 \end{pmatrix}, \\ M_{195} &= \begin{pmatrix} 0 & X+X^2+X^3 \\ 1+X & 1+X^2+X^3 \end{pmatrix}, & M_{198} &= \begin{pmatrix} 0 & 1+X+X^2 \\ X+X^2 & 1+X^2+X^3 \end{pmatrix}, \end{aligned}$$

$$
\begin{aligned}
M_{200} &= \begin{pmatrix} 0 & X^2 \\ X^3 & 1+X^2+X^3 \end{pmatrix}, & M_{207} &= \begin{pmatrix} 0 & X \\ 1+X+X^2+X^3 & 1+X^2+X^3 \end{pmatrix}, \\
M_{209} &= \begin{pmatrix} 1 & 1 \\ 1 & 1+X^2+X^3 \end{pmatrix}, & M_{212} &= \begin{pmatrix} 1 & X^3 \\ X^2 & 1+X^2+X^3 \end{pmatrix}, \\
M_{218} &= \begin{pmatrix} 1 & 1+X+X^3 \\ X+X^3 & 1+X^2+X^3 \end{pmatrix}, & M_{221} &= \begin{pmatrix} 1 & 1+X^2+X^3 \\ 1+X^2+X^3 & 1+X^2+X^3 \end{pmatrix} \Bigg\}.
\end{aligned}
$$

Outside of $\mathcal{C}_{24}^{(4)}$, there are each one orbits of lengths 4, 8, 20, and 80 and three orbits of length 40.

The automorphism group $\mathrm{Aut}(\mathcal{C}_{24}^{(4)})$ has order 160 and—according to Magma—is isomorphic to $D_4 \times (\mathbb{F}_5 \rtimes \mathbb{F}_5^*)$ where $D_4$ is the dihedral group of order 8 and $(\mathbb{F}_5 \rtimes \mathbb{F}_5^*)$ is the Frobenius group of order 20. It is generated by the maps

$$
\begin{aligned}
g_1 \colon \mathcal{H}_2(\mathbb{F}_{16}) &\to \mathcal{H}_2(\mathbb{F}_{16}), & C &\mapsto \overline{P_1}^{\mathsf{T}} \cdot \sigma(C) \cdot P_1 \\
&\text{with} & P_1 &= \begin{pmatrix} 1+X & 1+X^2+X^3 \\ 1+X+X^3 & X^2+X^3 \end{pmatrix}, \\
g_2 \colon \mathcal{H}_2(\mathbb{F}_{16}) &\to \mathcal{H}_2(\mathbb{F}_{16}), & C &\mapsto \overline{P_2}^{\mathsf{T}} \cdot C \cdot P_2 + S_2 \\
&\text{with} & P_2 &= \begin{pmatrix} 1 & 0 \\ X & 1 \end{pmatrix} \text{ and } S_2 = \begin{pmatrix} 1 & 1+X+X^2+X^3 \\ X & 0 \end{pmatrix},
\end{aligned}
$$

and

$$
\begin{aligned}
g_3 \colon \mathcal{H}_2(\mathbb{F}_{16}) &\to \mathcal{H}_2(\mathbb{F}_{16}), & C &\mapsto \overline{P_3}^{\mathsf{T}} \cdot \sigma(C) \cdot P_3 + S_3 \\
&\text{with} & P_3 &= \begin{pmatrix} 1 & 0 \\ X^2 & X \end{pmatrix} \text{ and } S_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},
\end{aligned}
$$

where $\sigma \colon \mathbb{F}_{16} \to \mathbb{F}_{16}$, $x \mapsto x^2$ is the Frobenius automorphism. Restricting those generators to $\mathcal{C}_{24}^{(4)}$ gives

$$
\begin{aligned}
g_1|_{\mathcal{C}_{24}^{(4)}} =& (M_{37}, M_{159}, M_{138}, M_{198})(M_{55}, M_{141}, M_{152}, M_{212})(M_{103}, M_{221}, M_{200}, M_{132}) \\
& (M_{117}, M_{207}, M_{218}, M_{150})(M_{129}, M_{147})(M_{195}, M_{209}), \\
g_2|_{\mathcal{C}_{24}^{(4)}} =& (M_0, M_{18})(M_{37}, M_{55})(M_{129}, M_{132})(M_{138}, M_{159})(M_{141}, M_{152}) \\
& (M_{147}, M_{150})(M_{195}, M_{212})(M_{198}, M_{209})(M_{200}, M_{207})(M_{218}, M_{221}),
\end{aligned}
$$

and

$$
\begin{aligned}
g_3|_{\mathcal{C}_{24}^{(4)}} =& (M_0, M_{80}, M_{18}, M_{66})(M_{37}, M_{103}, M_{55}, M_{117})(M_{129}, M_{138}, M_{150}, M_{159}) \\
& (M_{132}, M_{141}, M_{147}, M_{152})(M_{195}, M_{218}, M_{212}, M_{207})(M_{198}, M_{221}, M_{209}, M_{200}).
\end{aligned}
$$

**Type 5:** The only difference between $\mathcal{C}_{24}^{(5)}$ and $\mathcal{C}_{24}^{(4)}$ is that the matrices $M_{18}$ and $M_{66}$ are replaced by $M_{160}$ and $M_{240}$, such that the orbit $\mathcal{O}_4$ forms a line in $\mathcal{C}_{24}^{(5)}$. The orbits

$$
\begin{aligned}
\mathcal{O}_4 = \Bigg\{ M_0 &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, & M_{80} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\
M_{160} &= \begin{pmatrix} X^2+X^3 & 0 \\ 0 & X^2+X^3 \end{pmatrix}, & M_{240} &= \begin{pmatrix} 1+X^2+X^3 & 0 \\ 0 & 1+X^2+X^3 \end{pmatrix} \Bigg\}
\end{aligned}
$$

and

$$\mathcal{O}_{20} = \Bigg\{ M_{37} = \begin{pmatrix} X^2+X^3 & 1+X^3 \\ 1+X^2 & 0 \end{pmatrix}, \quad M_{55} = \begin{pmatrix} 1+X^2+X^3 & X+X^2 \\ 1+X+X^2 & 0 \end{pmatrix},$$
$$M_{103} = \begin{pmatrix} X^2+X^3 & X+X^2 \\ 1+X+X^2 & 1 \end{pmatrix}, \quad M_{117} = \begin{pmatrix} 1+X^2+X^3 & 1+X^3 \\ 1+X^2 & 1 \end{pmatrix},$$
$$M_{129} = \begin{pmatrix} 0 & 1 \\ 1 & X^2+X^3 \end{pmatrix}, \quad M_{132} = \begin{pmatrix} 0 & X^3 \\ X^2 & X^2+X^3 \end{pmatrix},$$
$$M_{138} = \begin{pmatrix} 0 & 1+X+X^3 \\ X+X^3 & X^2+X^3 \end{pmatrix}, \quad M_{141} = \begin{pmatrix} 0 & 1+X^2+X^3 \\ 1+X^2+X^3 & X^2+X^3 \end{pmatrix},$$
$$M_{147} = \begin{pmatrix} 1 & X+X^2+X^3 \\ 1+X & X^2+X^3 \end{pmatrix}, \quad M_{150} = \begin{pmatrix} 1 & 1+X+X^2 \\ X+X^2 & X^2+X^3 \end{pmatrix},$$
$$M_{152} = \begin{pmatrix} 1 & X^2 \\ X^3 & X^2+X^3 \end{pmatrix}, \quad M_{159} = \begin{pmatrix} 1 & X \\ 1+X+X^2+X^3 & X^2+X^3 \end{pmatrix},$$
$$M_{195} = \begin{pmatrix} 0 & X+X^2+X^3 \\ 1+X & 1+X^2+X^3 \end{pmatrix}, \quad M_{198} = \begin{pmatrix} 0 & 1+X+X^2 \\ X+X^2 & 1+X^2+X^3 \end{pmatrix},$$
$$M_{200} = \begin{pmatrix} 0 & X^2 \\ X^3 & 1+X^2+X^3 \end{pmatrix}, \quad M_{207} = \begin{pmatrix} 0 & X \\ 1+X+X^2+X^3 & 1+X^2+X^3 \end{pmatrix},$$
$$M_{209} = \begin{pmatrix} 1 & 1 \\ 1 & 1+X^2+X^3 \end{pmatrix}, \quad M_{212} = \begin{pmatrix} 1 & X^3 \\ X^2 & 1+X^2+X^3 \end{pmatrix},$$
$$M_{218} = \begin{pmatrix} 1 & 1+X+X^3 \\ X+X^3 & 1+X^2+X^3 \end{pmatrix}, \quad M_{221} = \begin{pmatrix} 1 & 1+X^2+X^3 \\ 1+X^2+X^3 & 1+X^2+X^3 \end{pmatrix} \Bigg\}$$

(which is exactly the same as $\mathcal{O}_{20}$ of type 4) are (re)printed for the sake of completeness.

Outside of $\mathcal{C}_{24}^{(5)}$, there are three orbits of length 4—one of them coinciding with the orbit of length 4 outside of $\mathcal{C}_{24}^{(4)}$—, seven orbits of length 20, and two orbits of length 40.

The automorphism group $\mathrm{Aut}(\mathcal{C}_{24}^{(4)})$ has order 80 and Magma states that it is isomorphic to the semidirect product $(C_2 \times C_2) \rtimes (\mathbb{F}_5 \rtimes \mathbb{F}_5^*)$ of the Klein four-group and the Frobenius group of order 20.

The generators of $\mathrm{Aut}(\mathcal{C}_{24}^{(4)})$ are

$$g_1 \colon \mathcal{H}_2(\mathbb{F}_{16}) \to \mathcal{H}_2(\mathbb{F}_{16}), \quad C \mapsto \overline{P_1}^{\mathsf{T}} \cdot \sigma(C) \cdot P_1 + S_1$$
$$\text{with} \quad P_1 = \begin{pmatrix} 0 & X^2 \\ 1 & 0 \end{pmatrix} \text{ and } S_1 = \begin{pmatrix} 1+X^2+X^3 & 0 \\ 0 & 1+X^2+X^3 \end{pmatrix},$$

and

$$g_2 \colon \mathcal{H}_2(\mathbb{F}_{16}) \to \mathcal{H}_2(\mathbb{F}_{16}), \quad C \mapsto \overline{P_2}^{\mathsf{T}} \cdot \sigma(C) \cdot P_2 + S_2$$
$$\text{with} \quad P_2 = \begin{pmatrix} 1+X & 1+X^3 \\ X+X^3 & 1+X \end{pmatrix} \text{ and } S_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

where $\sigma \colon \mathbb{F}_{16} \to \mathbb{F}_{16}$, $x \mapsto x^2$ is the Frobenius automorphism. The action of these generators on $\mathcal{C}_{24}^{(5)}$ is given by

$$g_1|_{\mathcal{C}_{24}^{(5)}} = (M_0, M_{240}, M_{80}, M_{160})(M_{37}, M_{55}, M_{117}, M_{103})(M_{129}, M_{200}, M_{212}, M_{159})$$
$$(M_{132}, M_{207}, M_{209,152})(M_{138}, M_{198}, M_{221}, M_{147})(M_{141}, M_{195}, M_{218}, M_{150})$$

and

$$g_2|_{\mathcal{C}_{24}^{(5)}} = (M_0, M_{80})(M_{37}, M_{200}, M_{141}, M_{147})(M_{55}, M_{218}, M_{159}, M_{129})(M_{103}, M_{138}, M_{207}, M_{209})$$
$$(M_{117}, M_{152}, M_{221}, M_{195})(M_{132}, M_{198})(M_{150}, M_{212}).$$

**Type 6:** $\mathcal{C}_{24}^{(6)}$ consists of two fixed points—again chosen to be the zero matrix $M_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and the identity matrix $M_{80} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$—,three orbits of length 2

$$\begin{aligned}
\mathcal{O}_2^{(1)} = \Big\{ & M_{10} = \begin{pmatrix} 0 & 1+X+X^3 \\ X+X^3 & 0 \end{pmatrix}, && M_{14} = \begin{pmatrix} 0 & 1+X \\ X+X^2+X^3 & 0 \end{pmatrix} \Big\} \\
\mathcal{O}_2^{(2)} = \Big\{ & M_{20} = \begin{pmatrix} 1 & X^3 \\ X^2 & 0 \end{pmatrix}, && M_{68} = \begin{pmatrix} 0 & X^3 \\ X^2 & 1 \end{pmatrix} \Big\} \\
\mathcal{O}_2^{(3)} = \Big\{ & M_{176} = \begin{pmatrix} 1+X^2+X^3 & 0 \\ 0 & X^2+X^3 \end{pmatrix}, && M_{224} = \begin{pmatrix} X^2+X^3 & 0 \\ 0 & 1+X^2+X^3 \end{pmatrix} \Big\},
\end{aligned}$$

two orbits of length 4

$$\begin{aligned}
\mathcal{O}_4^{(1)} = \Big\{ & M_5 = \begin{pmatrix} 0 & 1+X^3 \\ 1+X^2 & 0 \end{pmatrix}, && M_6 = \begin{pmatrix} 0 & 1+X+X^2 \\ X+X^2 & 0 \end{pmatrix} \\
& M_{11} = \begin{pmatrix} 0 & X+X^3 \\ 1+X+X^3 & 0 \end{pmatrix}, && M_{12} = \begin{pmatrix} 0 & X^2+X^3 \\ X^2+X^3 & 0 \end{pmatrix} \Big\} \\
\mathcal{O}_4^{(2)} = \Big\{ & M_3 = \begin{pmatrix} 0 & X+X^2+X^3 \\ 1+X & 0 \end{pmatrix}, && M_7 = \begin{pmatrix} 0 & X+X^2 \\ 1+X+X^2 & 0 \end{pmatrix} \\
& M_9 = \begin{pmatrix} 0 & 1+X^2 \\ 1+X^3 & 0 \end{pmatrix}, && M_{13} = \begin{pmatrix} 0 & 1+X^2+X^3 \\ 1+X^2+X^3 & 0 \end{pmatrix} \Big\},
\end{aligned}$$

and one orbit of length 8

$$\begin{aligned}
\mathcal{O}_8 = \Big\{ & M_{34} = \begin{pmatrix} X^2+X^3 & 1+X+X^2+X^3 \\ X & 0 \end{pmatrix}, && M_{40} = \begin{pmatrix} X^2+X^3 & X^2 \\ X^3 & 0 \end{pmatrix}, \\
& M_{49} = \begin{pmatrix} 1+X^2+X^3 & 1 \\ 1 & 0 \end{pmatrix}, && M_{63} = \begin{pmatrix} 1+X^2+X^3 & X \\ 1+X+X^2+X^3 & 0 \end{pmatrix}, \\
& M_{130} = \begin{pmatrix} 0 & 1+X+X^2+X^3 \\ X & X^2+X^3 \end{pmatrix}, && M_{136} = \begin{pmatrix} 0 & X^2 \\ X^3 & X^2+X^3 \end{pmatrix}, \\
& M_{193} = \begin{pmatrix} 0 & 1 \\ 1 & 1+X^2+X^3 \end{pmatrix}, && M_{207} = \begin{pmatrix} 0 & X \\ 1+X+X^2+X^3 & 1+X^2+X^3 \end{pmatrix} \Big\}
\end{aligned}$$

under its automorphism group. The collinearity of those matrices is shown in Figure 8.

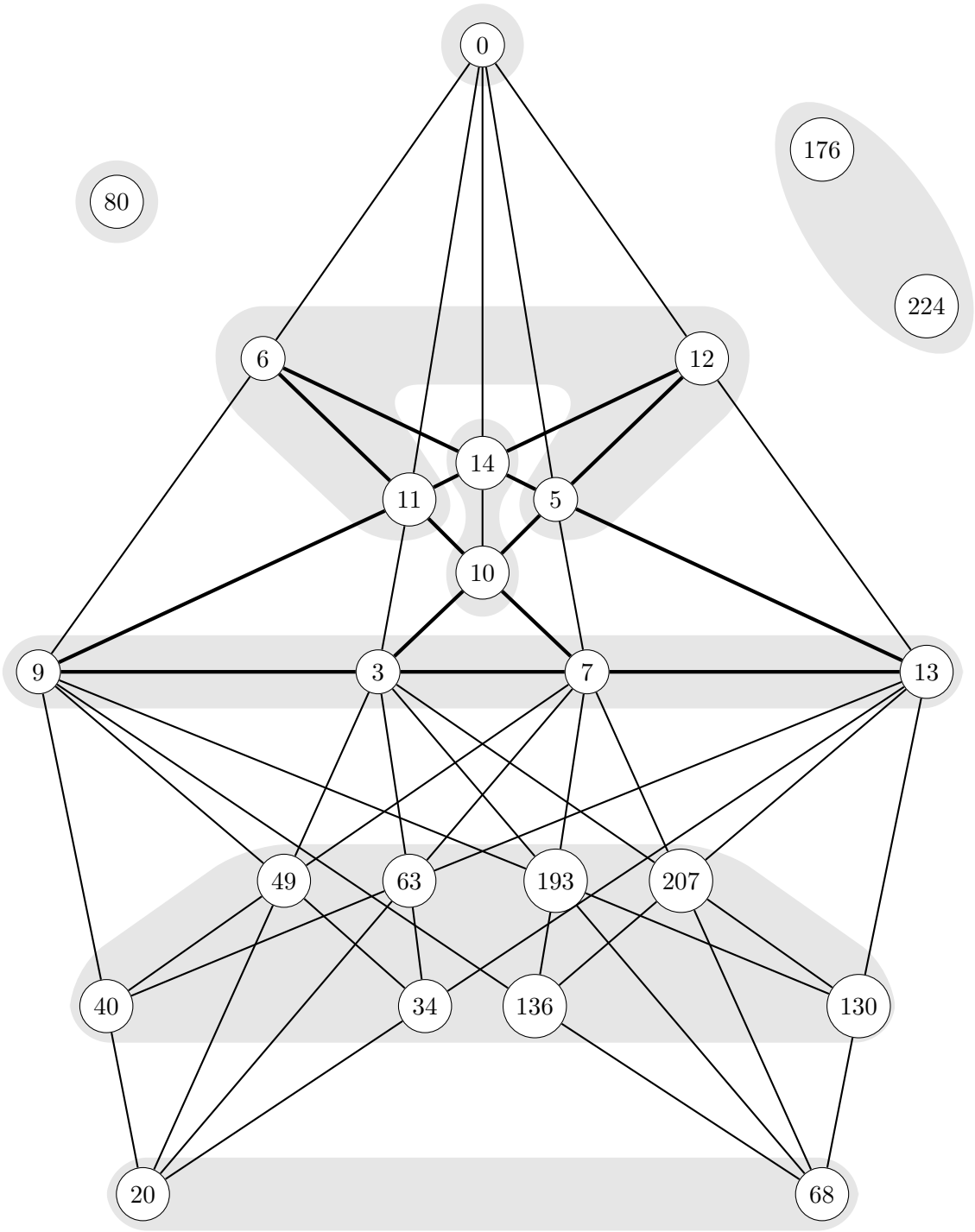
Outside of $\mathcal{C}_{24}^{(6)}$, there are two further fixed points, seven orbits of length 2, 20 orbits of length 4, and 17 orbits of length 8. The all in all four fixed points do not lie on one line but fulfill that their sum is the zero matrix. This property is independent of the representative since a different representative always arises by application of a map of form (4), $4 \cdot S = 0$ in characteristic 2, and the rest of the map can be placed outside brackets.

The automorphism group is isomorphic to $C_2 \times C_4$ and thereby has order 8. It is generated by the two maps $g_1$ and $g_2$,

$$\begin{aligned}
g_i \colon \mathcal{H}_2(\mathbb{F}_{16}) \to \mathcal{H}_2(\mathbb{F}_{16}), \qquad & C \mapsto \overline{P_i}^{\mathsf{T}} \cdot \sigma_i(C) \cdot P_i \\
\text{with} \qquad & P_1 = \begin{pmatrix} X & 0 \\ 0 & 1 \end{pmatrix} \text{ and } P_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},
\end{aligned}$$

where $\sigma_1 \colon \mathbb{F}_{16} \to \mathbb{F}_{16}$, $x \mapsto x^8$ and $\sigma_2 \colon \mathbb{F}_{16} \to \mathbb{F}_{16}$, $x \mapsto \overline{x}$.

Figure 8: Stucture of maximum code in $\mathcal{H}_2(\mathbb{F}_{16})$, type 6.



The restrictions of those generators to $\mathcal{C}_{24}^{(6)}$ are

$$\begin{aligned} g_1|_{\mathcal{C}_{24}^{(6)}} =&(M_3, M_{13}, M_7, M_9)(M_5, M_6, M_{11}, M_{12})(M_{10}, M_{14}) \\ &(M_{34}, M_{63}, M_{40}, M_{49})(M_{130}, M_{207}, M_{136}, M_{193})(M_{176}, M_{224}) \end{aligned}$$

and

$$g_2|_{\mathcal{C}_{24}^{(6)}} =(M_{20}, M_{68})(M_{34}, M_{130})(M_{40}, M_{136})(M_{49}, M_{193})(M_{63}, M_{207})(M_{176}, M_{224}).$$

In Figure 8, $g_1^2$ acts by reflecting each of the three spikes with respect to its vertical axis while $g_2$ interchanges the two bottom spikes and the points 176 and 224.

**Type 7:** The code $\mathcal{C}_{24}^{(7)}$ contains two fixed points $M_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $M_{80} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ again. The remaining orbits inside $\mathcal{C}_{24}^{(7)}$ are

$$\begin{aligned} \mathcal{O}_2 = \Big\{ & M_{160} = \begin{pmatrix} X^2+X^3 & 0 \\ 0 & X^2+X^3 \end{pmatrix}, && M_{240} = \begin{pmatrix} 1+X^2+X^3 & 0 \\ 0 & 1+X^2+X^3 \end{pmatrix} \Big\}, \\ \mathcal{O}_{10}^{(1)} = \Big\{ & M_{33} = \begin{pmatrix} X^2+X^3 & 1 \\ 1 & 0 \end{pmatrix}, && M_{34} = \begin{pmatrix} X^2+X^3 & 1+X+X^2+X^3 \\ X & 0 \end{pmatrix}, \\ & M_{36} = \begin{pmatrix} X^2+X^3 & X^3 \\ X^2 & 0 \end{pmatrix}, && M_{40} = \begin{pmatrix} X^2+X^3 & X^2 \\ X^3 & 0 \end{pmatrix}, \\ & M_{47} = \begin{pmatrix} X^2+X^3 & X \\ 1+X+X^2+X^3 & 0 \end{pmatrix}, && M_{193} = \begin{pmatrix} 0 & 1 \\ 1 & 1+X^2+X^3 \end{pmatrix}, \\ & M_{194} = \begin{pmatrix} 0 & 1+X+X^2+X^3 \\ X & 1+X^2+X^3 \end{pmatrix}, && M_{196} = \begin{pmatrix} 0 & X^3 \\ X^2 & 1+X^2+X^3 \end{pmatrix}, \\ & M_{200} = \begin{pmatrix} 0 & X^2 \\ X^3 & 1+X^2+X^3 \end{pmatrix}, && M_{207} = \begin{pmatrix} 0 & X \\ 1+X+X^2+X^3 & 1+X^2+X^3 \end{pmatrix} \Big\}, \end{aligned}$$

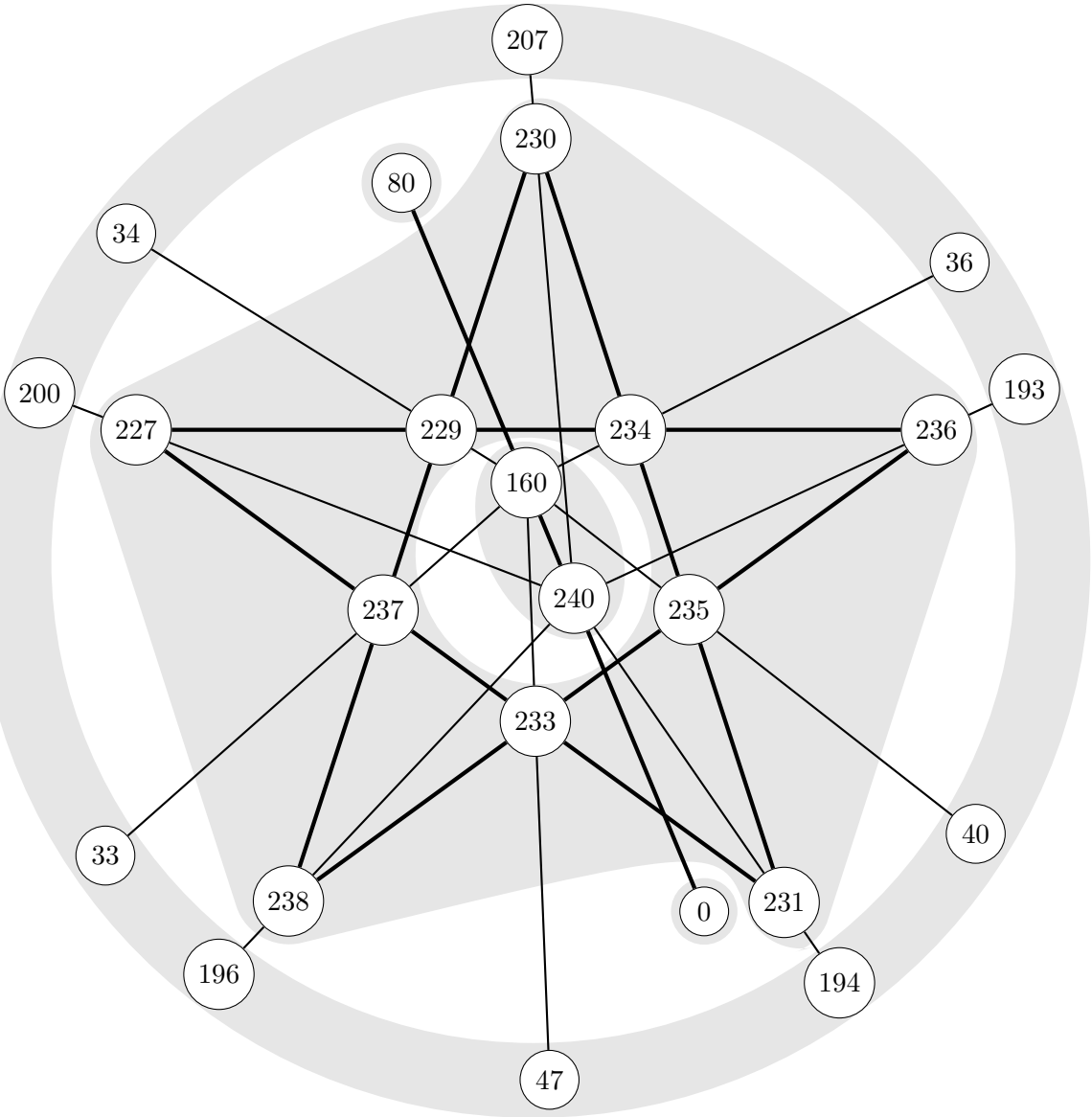
and

$$\begin{aligned} \mathcal{O}_{10}^{(2)} = \Big\{ & M_{227} = \begin{pmatrix} X^2+X^3 & X+X^2+X^3 \\ 1+X & 1+X^2+X^3 \end{pmatrix}, && M_{229} = \begin{pmatrix} X^2+X^3 & 1+X^3 \\ 1+X^2 & 1+X^2+X^3 \end{pmatrix}, \\ & M_{230} = \begin{pmatrix} X^2+X^3 & 1+X+X^2 \\ X+X^2 & 1+X^2+X^3 \end{pmatrix}, && M_{231} = \begin{pmatrix} X^2+X^3 & X+X^2 \\ 1+X+X^2 & 1+X^2+X^3 \end{pmatrix}, \\ & M_{233} = \begin{pmatrix} X^2+X^3 & 1+X^2 \\ 1+X^3 & 1+X^2+X^3 \end{pmatrix}, && M_{234} = \begin{pmatrix} X^2+X^3 & 1+X+X^3 \\ X+X^3 & 1+X^2+X^3 \end{pmatrix}, \\ & M_{235} = \begin{pmatrix} X^2+X^3 & X+X^3 \\ 1+X+X^3 & 1+X^2+X^3 \end{pmatrix}, && M_{236} = \begin{pmatrix} X^2+X^3 & X^2+X^3 \\ X^2+X^3 & 1+X^2+X^3 \end{pmatrix}, \\ & M_{237} = \begin{pmatrix} X^2+X^3 & 1+X^2+X^3 \\ 1+X^2+X^3 & 1+X^2+X^3 \end{pmatrix}, && M_{238} = \begin{pmatrix} X^2+X^3 & 1+X \\ X+X^2+X^3 & 1+X^2+X^3 \end{pmatrix} \Big\}. \end{aligned}$$

The matrices of $\mathcal{O}_{10}^{(2)}$ form five full lines while $\mathcal{O}_2$ forms a line together with the fixed points. The matrices of $\mathcal{O}_{10}^{(1)}$ all lie on a line through a matrix of $\mathcal{O}_2$ and a matrix of $\mathcal{O}_{10}^{(2)}$ as Figure 9 shows.

Outside of $\mathcal{C}_{24}^{(7)}$, we have two further fixed points that do not lie on a line with $M_0$ and $M_{80}$ but fulfill that the sum of all four fixed points is the zero matrix. Additionally, there are five orbits of length 2, four orbits of length 5, and 20 orbits of length 20 outside of the code.

Figure 9: Stucture of maximum code in $\mathcal{H}_2(\mathbb{F}_{16})$, type 7.



The automorphism group of $\mathcal{C}_{24}^{(7)}$ has size 20 and is generated by the two maps

$$g_1 \colon \mathcal{H}_2(\mathbb{F}_{16}) \to \mathcal{H}_2(\mathbb{F}_{16}), \qquad C \mapsto \overline{P_1}^{\mathsf{T}} \cdot C \cdot P_1 \qquad \text{with } P_1 = \begin{pmatrix} X & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$g_2 \colon \mathcal{H}_2(\mathbb{F}_{16}) \to \mathcal{H}_2(\mathbb{F}_{16}), \qquad C \mapsto \overline{P_2}^{\mathsf{T}} \cdot \sigma(C) \cdot P_2 \qquad \text{with } P_2 = \begin{pmatrix} 0 & 1 \\ X & 0 \end{pmatrix}$$

where $\sigma(x) = x^8 \ \forall x \in \mathbb{F}_{16}$. According to Magma, $\mathrm{Aut}(\mathcal{C}_{24}^{(7)})$ is isomorphic to the Frobenius group $\mathbb{F}_5 \rtimes \mathbb{F}_5^*$. The restrictions of the generators to the code are

$$\begin{aligned} g_1|_{\mathcal{C}_{24}^{(7)}} =& (M_{230}, M_{236}, M_{231}, M_{238}, M_{227})(M_{229}, M_{234}, M_{235}, M_{233}, M_{237}) \\ & (M_{207}, M_{193}, M_{194}, M_{196}, M_{200})(M_{36}, M_{40}, M_{47}, M_{33}, M_{34}) \end{aligned}$$

and

$$\begin{aligned} g_2|_{\mathcal{C}_{24}^{(7)}} =& (M_{230}, M_{233})(M_{236}, M_{229}, M_{227}, M_{234})(M_{231}, M_{235}, M_{238}, M_{237}) \\ & (M_{207}, M_{47})(M_{36}, M_{193}, M_{34}, M_{200})(M_{40}, M_{196}, M_{33}, M_{194}) \\ & (M_{160}, M_{240}). \end{aligned}$$

In Figure 9, $g_1$ acts as a rotation by 72° and $g_2^2$ as a reflection with respect to the vertical axis. Considering the edges of the pentagram instead and identifying them with elements of $\mathbb{F}_5$ in the way Figure 6 shows (as we already did analyzing type 2), $g_1$ corresponds to "+1" and $g_2$ to "·2".

### 6.2.4 Maximum Code in $\mathcal{S}_3(\mathbb{F}_2)$ with $d = 2$

For the case $\mathcal{S}_3(\mathbb{F}_2)$, the implementation of Algorithm 2 had to be adjusted such that it is using the special graph $\Gamma_{S_3(\mathbb{F}_2)}$ described on page 17. It then delivered the result that a maximum code in $\mathcal{S}_3(\mathbb{F}_2)$ with $d = 2$ has size 22 (which is already found by Kiermaier [36] as previously mentioned in section 3.2.2) and all maximum codes are isomorphic.

The automorphism group $\mathrm{Aut}(\mathcal{C}_{22})$ has order 168 and, according to Magma, is a simple group. Every simple group of order 168 is isomorphic to $\mathrm{GL}_3(\mathbb{F}_2)$ (see, e.g., [64]) and so is $\mathrm{Aut}(\mathcal{C}_{22})$.

The action of $\mathrm{Aut}(\mathcal{C}_{22})$ partitions $\mathcal{C}_{22}$ into one fixed point and one orbit of length 21. After moving the fixed point to the zero matrix, we gain a representative consisting exactly of the zero matrix $M_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and the set of the 21 non-alternate rank-2-matrices

$$\begin{aligned} \mathcal{O}_{21} = \Bigg\{ & M_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad M_5 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad M_6 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \\ & M_9 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad M_{10} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad M_{15} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \\ & M_{17} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad M_{21} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad M_{24} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \end{aligned}$$

$$M_{27} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad M_{30} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad M_{34} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$
$$M_{38} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad M_{40} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad M_{43} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$
$$M_{45} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad M_{51} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad M_{55} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix},$$
$$M_{56} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \quad M_{61} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \quad M_{62} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \Bigg\}$$

Besides the fixed point and the orbit $\mathcal{O}_{21}$ within the code, $\mathrm{Aut}(\mathcal{C}_{22})$ has an orbit of length 7 consisting of the rank-1-matrices, an orbit of length 7 consisting of the alternate rank-2-matrices, and an orbit of length 28 consisting of the rank-3-matrices outside of $\mathcal{C}_{22}$.

The automorphism group of $C_{22}$ then is generated by the three maps $g_1$, $g_2$, and $g_3$ where

$$g_i \colon \mathcal{S}_3(\mathbb{F}_2) \to \mathcal{S}_3(\mathbb{F}_2), \qquad C \mapsto P_i^{\mathsf{T}} \cdot C \cdot P_i$$
$$\text{with} \qquad P_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, P_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \text{ and } P_3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

so the automorphism group consists exactly of the maps $C \mapsto P^{\mathsf{T}} \cdot C \cdot P$ with $P \in \mathrm{GL}_3(\mathbb{F}_2)$. In other words, the automorphism group of $C_{22}$ is the stabilizer subgroup of the isometries of $\mathcal{S}_3(\mathbb{F}_2)$ with respect to the zero matrix.

The restrictions of the generators to $\mathcal{C}_{22}$ are

$$\begin{aligned} g_1|_{\mathcal{C}_{22}} =& (M_5, M_6)(M_9, M_{10})(M_{17}, M_{34})(M_{21}, M_{38}) \\ & (M_{24}, M_{40})(M_{27}, M_{43})(M_{30}, M_{45})(M_{61}, M_{62}), \\ g_2|_{\mathcal{C}_{22}} =& (M_3, M_9)(M_5, M_{17})(M_6, M_{24})(M_{15}, M_{27}) \\ & (M_{34}, M_{40})(M_{38}, M_{56})(M_{45}, M_{51})(M_{55}, M_{61}), \end{aligned}$$

and

$$\begin{aligned} g_3|_{\mathcal{C}_{22}} =& (M_3, M_5)(M_9, M_{15})(M_{17}, M_{55})(M_{21}, M_{51}) \\ & (M_{24}, M_{56})(M_{27}, M_{61})(M_{30}, M_{62})(M_{43}, M_{45}). \end{aligned}$$

### 6.3 An Algorithm Using Cliquer

Since the orderly algorithm computes intermediate sets with strongly increasing size, another algorithm is discussed which does not have this drawback. In this, a set of C-routines, called Cliquer [47], is used. Cliquer can be used to find all maximum cliques in a given graph but also has a wider range of application, see, e.g., [47].

The key idea of Cliquer is a branch-and-bound approach. For description of the underlying algorithm, see [67, algorithm 2]. Cliquer can be used with different predefined orderings of vertices, e.g., the greedy vertex coloring which seems to perform well in many cases (see, e.g., [47, Section 2.4] which is based on discussion in [67]).

To translate the problem of finding maximum codes with minimum distance at least a fixed number $d$ in a space of matrices $\mathcal{M} \subset \mathbb{F}_q^{m \times n}$ into a maximum clique problem, we

generate a graph $\Delta_{\mathcal{M},d}$ with vertices $0, \ldots, \#\mathcal{M} - 1$ that has an edge connecting vertices $i$ and $j$ if and only if $\mathrm{d_{rk}}(M_i, M_j) \geq d$. This graph $\Delta_{\mathcal{M},d}$ is not to be confused with the graph $\Gamma_{\mathcal{M}}$ described in section 4.4.

But passing the whole graph $\Delta_{\mathcal{M},d}$ to Cliquer would take too much time consumption and also the provided source code is not parallelized. So the idea is to use a "hybrid approach" as suggested by Royle (see [53, Section 2]). Instead of $\Delta_{\mathcal{M},d}$, Cliquer is given the induced subgraph $\Delta^{(S)}_{\mathcal{M},d}$ consisting of all vertices adjacent to a predefined small clique $S$. Note that, if the vertices of $\Delta^{(S)}_{\mathcal{M},d}$ are relabeled with consecutive numbers, they have to be translated back into vertices of $\Delta_{\mathcal{M},d}$ at the end of calculation. Using Cliquer on $\Delta^{(S)}_{\mathcal{M},d}$ for each possible clique $S$ with a fixed small size would imply that all maximum cliques are found—possibly besides cliques $S \cup S'$, where $S'$ is a maximum clique in $\Delta^{(S)}_{\mathcal{M},d}$, that are maximal but nevertheless not maximum in $\Delta_{\mathcal{M},d}$.

Since we are only interested in non-isomorphic codes, it is sufficient to restrict ourself to starting configurations that are not isomorphic in the sense of Definition 4.1. These starting configurations are created with the orderly algorithm. At the end, it is necessary to check all maximum codes for isomorphism.

**Procedure** `IsIsomorphic`$(C_1, C_2; (\Gamma_{\mathcal{M}}, \pi))$: `Canon()` refers to the canonical labeled graph computed by nauty.

```
1  forall the v in the vertex set of Γ_M do
2  |  for i ← 1 to 2 do
3  |  |  if v ∈ C_i then
4  |  |  |  π_i(v) ← 1;
5  |  |  else
6  |  |  |  π_i(v) ← π(v) + 1;
7  |  |  end
8  |  end
9  end
10 if Canon(Γ_M, π_1)=Canon(Γ_M, π_2) then
11 |  return true;
12 else
13 |  return false;
14 end
```

Algorithm 3 consolidates the whole approach. Up to line 10, the orderly algorithm is applied to generate the starting configurations. If the size of the starting configurations is chosen larger than the maximum code size, the result is output and the algorithm terminated in line 8. In lines 11 to 18, for each starting configuration $S$, the graph $\Delta^{(S)}_{\mathcal{M},d}$ is created and passed to Cliquer for solving the problem of finding all maximum cliques. The maximum clique size is increased by $s$ and the vertices of $S$ are added to each clique found. If $s$ is chosen appropriate, lines 11 to 18 contain the main effort of this algorithm. Since the starting configurations $S$ and thus the subgraphs $\Delta^{(S)}_{\mathcal{M},d}$ are independent, this part is quite easy to parallelize. In lines 19 and 20, the maximum code size is determined and all cliques of that size are combined in the set $M$. In lines 21 to 32, one representative of each isomorphism class is added to the set $S_m$ which is subsequently returned along with $m$. The test for

**Algorithm 3:** Algorithm for classification of maximum codes, based on Cliquer [47]. Here `CliquerFindAllMaximumCliques()` stands for the procedure which is outsourced to Cliquer and returns a pair $(m, M)$ where $m$ is the maximum clique size and $M$ is the set of all maximum cliques in the input graph.

**Input**: Matrix set $\mathcal{M} \in \{\mathbb{F}_q^{m\times n}, \mathcal{S}_n(\mathbb{F}_q), \mathcal{H}_n(\mathbb{F}_{q^2})\}$,
lower bound $d$ for the minimum distance,
size of starting configurations $s$

**Output**: Maximum code size $m$ and set $\mathcal{S}_m$ containing precisely one representative of each isomorphism class of maximum codes

Create colored graph $(\Gamma_{\mathcal{M}}, \pi)$;
$S_0 \leftarrow \{\emptyset\}$;
$k \leftarrow 0$;
**while** $k < s$ **do**
  $S_{k+1} \leftarrow$ `Augment(`$S_k; \mathcal{M}, (\Gamma_{\mathcal{M}}, \pi), d$`)`;
  $k \leftarrow k + 1$;
  **if** $S_k = \emptyset$ **then**
    **return** $(k-1, S_{k-1})$;
  **end**
**end**
**forall the** $S \in S_s$ **do**
  Create graph $\Delta^{(S)}_{\mathcal{M},d}$;
  $(m_S, M_S) \leftarrow$ `CliquerFindAllMaximumCliques(`$\Delta^{(S)}_{\mathcal{M},d}$`)`;
  $m_S \leftarrow m_S + s$;
  **forall the** $C \in M_S$ **do**
    $C \leftarrow C \cup S$;
  **end**
**end**
$m \leftarrow \max\{m_S \mid S \in \mathcal{S}_s\}$;
$M \leftarrow \bigcup_{S:m_S=m} M_S$;
$S_m \leftarrow \emptyset$;
**forall the** $C \in M$ **do**
  $b \leftarrow$**true**;
  **forall the** $T \in S_m$ **do**
    **if** `IsIsomorphic(`$C, T; \Gamma_{\mathcal{M}}$`)` **then**
      $b \leftarrow$ **false**;
    **end**
  **end**
  **if** $b$ **then**
    $S_m \leftarrow S_m \cup \{C\}$;
  **end**
**end**
**return** $(m, S_m)$;

Table 6: Computation time of `CliquerFindAllMaximumCliques(`$\Delta^{(S)}_{\mathcal{H}_2(\mathbb{F}_{25}),2}$`)` for one starting configuration $S$ of each of the sizes 4 to 6 and deduced estimated total computation time.

| $k = \#S$ | time (min) | $\#S_k$ | extrapolated total time |
|---|---|---|---|
| 4 | 1487 | 89 | 92 days |
| 5 | 39 | 2317 | 63 days |
| 6 | 6 | 80105 | 361 days |

isomorphism is done using Procedure `IsIsomorphic()`. This procedure equips the graph $(\Gamma_{\mathcal{M}}, \pi)$ with two different new colorings

$$\pi_1(v) = \begin{cases} 1, & v \in C_1 \\ \pi(v) + 1, & v \notin C_1 \end{cases}$$

and

$$\pi_2(v) = \begin{cases} 1, & v \in C_2 \\ \pi(v) + 1, & v \notin C_2 \end{cases}$$

and tests the colored graphs $(\Gamma_{\mathcal{M}}, \pi_1)$ and $(\Gamma_{\mathcal{M}}, \pi_2)$ for isomorphism.

To get an idea how big the starting cliques $S$ should be in the case $\mathcal{M} = \mathcal{H}_2(\mathbb{F}_{25})$, the graph $\Delta^{(S)}_{\mathcal{M},d}$ is passed to cliquer for each one clique $S$ of the sizes 4, 5, and 6. Then the resulting computing time on an Intel Core i7 3770 is multiplied by the number of non-isomorphic cliques of that size (taken from Table 4). The results are listed in Table 6. Due to inaccuracy in the first time measurement, start sets of size 4 are used instead of start sets of size 5. Table 6 contains the corrected data.

Though the extrapolated total computation time takes a minimum at $\#S = 5$, it is not sure that this would be really the best choice. This is mainly due to the fact that the computation time varies widely for different starting configurations of the same size as we will see below. Additionally, the computation time is lengthened when 8 processes are computing at the same time (by a factor of 1.66 for the set of size 4 tested).

In the case $\mathcal{M} = \mathcal{H}_2(\mathbb{F}_{25})$, $d = 2$, 88 of the 89 starting configurations led to the maximum clique size of 47. The distribution of the computation time of `CliquerFindAllMaximumCliques(`$\Delta^{(S)}_{\mathcal{H}_2(\mathbb{F}_{25}),2}$`)` is described in Table 7. Besides the maximum size of 47—which was already known to be a lower bound [8]—, Algorithm 3 revealed that all maximum cliques are isomorphic in this case. One representative of this isomorphism class is analyzed in section 6.3.1.

Table 7: Distribution (quantiles, maximum, and average) of the computation time in hours of `CliquerFindAllMaximumCliques(`$\Delta^{(S)}_{\mathcal{H}_2(\mathbb{F}_{25}),2}$`)` for all starting configurations $S$ of size 4 leading to the overall maximum clique size.

| $Q_{10}$ | $Q_{25}$ | $Q_{50}$ | $Q_{75}$ | $Q_{90}$ | $Q_{95}$ | $Q_{99}$ | max | av. |
|---|---|---|---|---|---|---|---|---|
| 30 | 42 | 54 | 93 | 121 | 180 | 203 | 489 | 74 |

An attempt to apply Algorithm 3 to $\mathcal{M} = \mathcal{H}_3(\mathbb{F}_4)$, $d = 2$ with parameter $s = 4$ has been aborted after nearly three weeks. By then, the largest clique found by Cliquer in 44 of the 107 graphs $\Delta^{(S)}_{\mathcal{H}_3(\mathbb{F}_4),2}$ is of size 84. Adding the 4 start vertices, this gives a code of size 88. As we will see in Section 6.4, this calculation has been far away from completion since a maximum code in $\mathcal{H}_3(\mathbb{F}_4)$ with minimum distance $\geq 2$ has size at least 120.

### 6.3.1 Maximum Code in $\mathcal{H}_2(\mathbb{F}_{25})$ with $d = 2$

The code $\mathcal{C}_{47}$ consists of one fixed point under its automorphism group—which is chosen to be the zero matrix $M_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$—, three orbits

$$\begin{aligned}
\mathcal{O}_6^{(1)} = \Bigg\{ & M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, && M_4 = \begin{pmatrix} 0 & 4 \\ 4 & 0 \end{pmatrix}, \\
& M_{180} = \begin{pmatrix} 2 & 4X \\ X & 1 \end{pmatrix}, && M_{195} = \begin{pmatrix} 2 & X \\ 4X & 1 \end{pmatrix}, \\
& M_{580} = \begin{pmatrix} 3 & 4X \\ X & 4 \end{pmatrix}, && M_{595} = \begin{pmatrix} 3 & X \\ 4X & 4 \end{pmatrix} \Bigg\}, \\
\mathcal{O}_6^{(2)} = \Bigg\{ & M_{85} = \begin{pmatrix} 3 & 3X \\ 2X & 0 \end{pmatrix}, && M_{90} = \begin{pmatrix} 3 & 2X \\ 3X & 0 \end{pmatrix}, \\
& M_{135} = \begin{pmatrix} 0 & 3X \\ 2X & 1 \end{pmatrix}, && M_{140} = \begin{pmatrix} 0 & 2X \\ 3X & 1 \end{pmatrix}, \\
& M_{477} = \begin{pmatrix} 4 & 2 \\ 2 & 3 \end{pmatrix}, && M_{478} = \begin{pmatrix} 4 & 3 \\ 3 & 3 \end{pmatrix} \Bigg\},
\end{aligned}$$

and

$$\begin{aligned}
\mathcal{O}_6^{(3)} = \Bigg\{ & M_{105} = \begin{pmatrix} 4 & 4X \\ X & 0 \end{pmatrix}, && M_{120} = \begin{pmatrix} 4 & X \\ 4X & 0 \end{pmatrix}, \\
& M_{380} = \begin{pmatrix} 0 & 4X \\ X & 3 \end{pmatrix}, && M_{395} = \begin{pmatrix} 0 & X \\ 4X & 3 \end{pmatrix}, \\
& M_{551} = \begin{pmatrix} 2 & 1 \\ 1 & 4 \end{pmatrix}, && M_{554} = \begin{pmatrix} 2 & 4 \\ 4 & 4 \end{pmatrix} \Bigg\}
\end{aligned}$$

of length 6, two orbits

$$\begin{aligned}
\mathcal{O}_8^{(1)} = \Bigg\{ & M_7 = \begin{pmatrix} 0 & 2+4X \\ 2+X & 0 \end{pmatrix}, && M_8 = \begin{pmatrix} 0 & 3+4X \\ 3+X & 0 \end{pmatrix}, \\
& M_{22} = \begin{pmatrix} 0 & 2+X \\ 2+4X & 0 \end{pmatrix}, && M_{23} = \begin{pmatrix} 0 & 3+X \\ 3+4X & 0 \end{pmatrix}, \\
& M_{177} = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}, && M_{178} = \begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix}, \\
& M_{577} = \begin{pmatrix} 3 & 2 \\ 2 & 4 \end{pmatrix}, && M_{578} = \begin{pmatrix} 3 & 3 \\ 3 & 4 \end{pmatrix} \Bigg\}
\end{aligned}$$

and

$$\mathcal{O}_8^{(2)} = \Big\{ \begin{aligned} M_{11} &= \begin{pmatrix} 0 & 1+3X \\ 1+2X & 0 \end{pmatrix}, & M_{14} &= \begin{pmatrix} 0 & 4+3X \\ 4+2X & 0 \end{pmatrix}, \\ M_{16} &= \begin{pmatrix} 0 & 1+2X \\ 1+3X & 0 \end{pmatrix}, & M_{19} &= \begin{pmatrix} 0 & 4+2X \\ 4+3X & 0 \end{pmatrix}, \\ M_{351} &= \begin{pmatrix} 4 & 1 \\ 1 & 2 \end{pmatrix}, & M_{354} &= \begin{pmatrix} 4 & 4 \\ 4 & 2 \end{pmatrix}, \\ M_{401} &= \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}, & M_{404} &= \begin{pmatrix} 1 & 4 \\ 4 & 3 \end{pmatrix} \end{aligned} \Big\}$$

of length 8, and one orbit

$$\mathcal{O}_{12} = \Big\{ \begin{aligned} M_{62} &= \begin{pmatrix} 2 & 2+3X \\ 2+2X & 0 \end{pmatrix}, & M_{63} &= \begin{pmatrix} 2 & 3+3X \\ 3+2X & 0 \end{pmatrix}, \\ M_{67} &= \begin{pmatrix} 2 & 2+2X \\ 2+3X & 0 \end{pmatrix}, & M_{68} &= \begin{pmatrix} 2 & 3+2X \\ 3+3X & 0 \end{pmatrix}, \\ M_{225} &= \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}, & M_{280} &= \begin{pmatrix} 1 & 4X \\ X & 2 \end{pmatrix}, \\ M_{295} &= \begin{pmatrix} 1 & X \\ 4X & 2 \end{pmatrix}, & M_{450} &= \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \\ M_{512} &= \begin{pmatrix} 0 & 2+3X \\ 2+2X & 4 \end{pmatrix}, & M_{513} &= \begin{pmatrix} 0 & 3+3X \\ 3+2X & 4 \end{pmatrix}, \\ M_{517} &= \begin{pmatrix} 0 & 2+2X \\ 2+3X & 4 \end{pmatrix}, & M_{518} &= \begin{pmatrix} 0 & 3+2X \\ 3+3X & 4 \end{pmatrix} \end{aligned} \Big\}$$

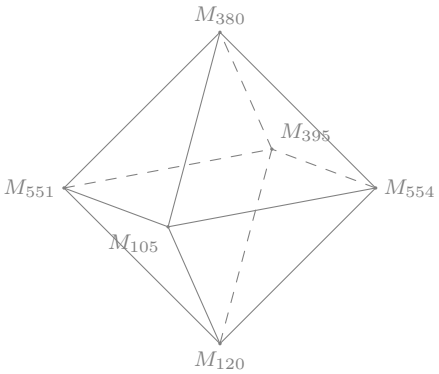
of length 12. The matrices of $\mathcal{O}_8^{(1)}$ are all of the form

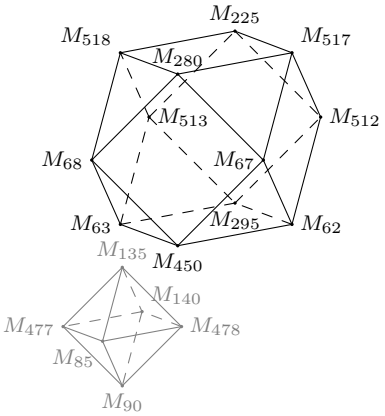
$$\begin{pmatrix} 3 & 2 \\ 2 & 4 \end{pmatrix} + \alpha \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \beta \begin{pmatrix} 2 & X \\ 4X & 1 \end{pmatrix} + \gamma \begin{pmatrix} 2 & 4X \\ X & 1 \end{pmatrix}$$

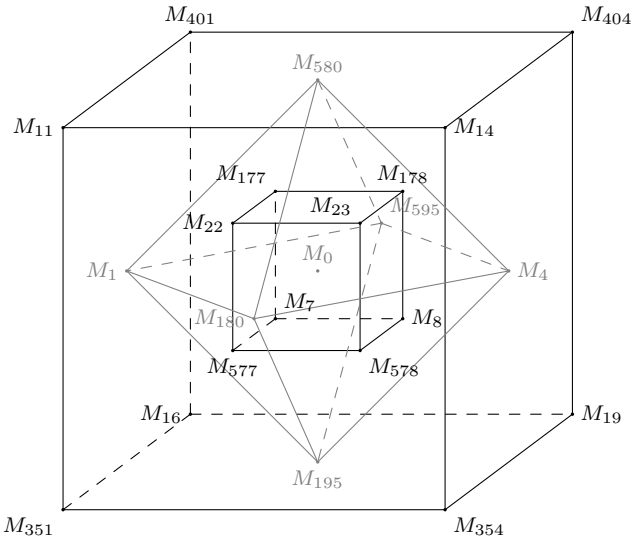
where $\alpha, \beta, \gamma \in \{0, 1\}$. This is a parallelepiped whose space diagonals intersect at the zero matrix $M_0$. The orbit $\mathcal{O}_8^{(2)}$ arises from $\mathcal{O}_8^{(1)}$ by central dilation with scaling center $M_0$ and scale factor 3. The matrices of $\mathcal{O}_6^{(1)}$ are obtained as the centers of the faces of the parallelepiped $\mathcal{O}_8^{(2)}$. Shifting $\mathcal{O}_6^{(1)}$ by $\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$ yields $\mathcal{O}_6^{(3)}$ and $\mathcal{O}_6^{(2)}$ results from $\mathcal{O}_6^{(3)}$ by central dilation with scaling center $M_0$ and scale factor $\frac{1}{3} = 2$. Finally, the twelve matrices of $\mathcal{O}_{12}$ can be constructed from the twelve edges of the bipyramids $\mathcal{O}_6^{(1)}$ and $\mathcal{O}_6^{(3)}$ by intersecting the lines through the end points of one edge of $\mathcal{O}_6^{(1)}$ and the respective opposite end points of the corresponding edge of $\mathcal{O}_6^{(3)}$, for example, $M_{518}$ is the intersection point of the line through $M_{580}$ and $M_{551}$ and the line through $M_1$ and $M_{380}$.

Outside of $\mathcal{C}_{47}$, there are further four fixed points that are all multiples (with coefficients in $\mathbb{F}_5^*$) of $\begin{pmatrix} 4 & 0 \\ 0 & 3 \end{pmatrix}$ which is the midpoint of $\mathcal{O}_6^{(2)}$. The matrix $\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} = 3 \cdot \begin{pmatrix} 4 & 0 \\ 0 & 3 \end{pmatrix}$ is the center of $\mathcal{O}_6^{(3)}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = 4 \cdot \begin{pmatrix} 4 & 0 \\ 0 & 3 \end{pmatrix}$—where the factor 4 can be thought of as $\frac{3}{2}$ with regard to the construction of $\mathcal{O}_{12}$ and figure 10—is the center of $\mathcal{O}_{12}$. Besides, there are seven orbits of length 6, eight orbits of length 8, nine orbits of length 12, and fifteen orbits of length 24.

Figure 10: Stucture of maximum code in $\mathcal{H}_2(\mathbb{F}_{25})$.



In Figure 10, the orbits in $\mathcal{C}_{47}$ are illustrated as octahedra, cubes, and cuboctahedron in view of the automorphism group $\mathrm{Aut}(\mathcal{C}_{47})$ which has order 48 and is isomorphic to the symmetry group of a cube. It is generated by the three maps

$$\begin{aligned} g_i \colon \mathcal{H}_2(\mathbb{F}_{25}) \to \mathcal{H}_2(\mathbb{F}_{25}), \quad & C \mapsto \overline{P_i}^{\mathsf{T}} \cdot \sigma_i(C) \cdot P_i \\ \text{with} \quad & P_1 = \begin{pmatrix} 0 & 3X \\ X & 0 \end{pmatrix}, P_2 = \begin{pmatrix} 2+X & 4+3X \\ 3+X & 3X \end{pmatrix}, \\ \text{and} \quad & P_3 = \begin{pmatrix} 2+X & 4X \\ 2X & 2+4X \end{pmatrix} \end{aligned}$$

where $\sigma_1 \colon \mathbb{F}_{25} \to \mathbb{F}_{25}$, $x \mapsto \overline{x}$, and $\sigma_2 = \sigma_3 = \mathrm{id}_{\mathbb{F}_{25}}$.

In Figure 10, those maps act simultaneous on $\mathcal{O}_6^{(2)}$, $\mathcal{O}_6^{(3)}$, $\mathcal{O}_{12}$, and the union of the three orbits $\mathcal{O}_6^{(1)}$, $\mathcal{O}_8^{(1)}$, and $\mathcal{O}_8^{(2)}$ in the following way:

$$\begin{aligned} g_1|_{\mathcal{C}_{47}} =& (M_1, M_4)(M_{180}, M_{595})(M_{195}, M_{580}) \\ & (M_{85}, M_{140})(M_{90}, M_{135})(M_{477}, M_{478}) \\ & (M_{105}, M_{395})(M_{120}, M_{380})(M_{551}, M_{554}) \\ & (M_7, M_{23})(M_8, M_{22})(M_{177}, M_{578})(M_{178}, M_{577}) \\ & (M_{11}, M_{19})(M_{14}, M_{16})(M_{351}, M_{404})(M_{354}, M_{401}) \\ & (M_{62}, M_{518})(M_{63}, M_{517})(M_{67}, M_{513})(M_{68}, M_{512})(M_{225}, M_{450})(M_{280}, M_{295}) \end{aligned}$$

is a point reflection,

$$\begin{aligned} g_2|_{\mathcal{C}_{47}} =& (M_1, M_{595}, M_4, M_{180}) \\ & (M_{85}, M_{477}, M_{140}, M_{478}) \\ & (M_{105}, M_{551}, M_{395}, M_{554}) \\ & (M_7, M_8, M_{578}, M_{577})(M_{22}, M_{177}, M_{178}, M_{23}) \\ & (M_{11}, M_{401}, M_{404}, M_{14})(M_{16}, M_{19}, M_{354}, M_{351}) \\ & (M_{62}, M_{450}, M_{63}, M_{295})(M_{67}, M_{68}, M_{513}, M_{512})(M_{225}, M_{517}, M_{280}, M_{518}) \end{aligned}$$

is a rotation by 90° with respect to the vertical axis, and

$$\begin{aligned} g_3|_{\mathcal{C}_{47}} =& (M_1, M_{195}, M_{180})(M_4, M_{580}, M_{595}) \\ & (M_{85}, M_{477}, M_{90})(M_{135}, M_{140}, M_{478}) \\ & (M_{105}, M_{551}, M_{120})(M_{380}, M_{395}, M_{554}) \\ & (M_7, M_{578}, M_{22})(M_8, M_{23}, M_{177}) \\ & (M_{11}, M_{16}, M_{354})(M_{14}, M_{401}, M_{19}) \\ & (M_{62}, M_{280}, M_{513})(M_{63}, M_{450}, M_{68})(M_{67}, M_{518}, M_{295})(M_{225}, M_{512}, M_{517}) \end{aligned}$$

is a rotation by 120° with respect to the space diagonal axis which runs from the front bottom left to the back top right.

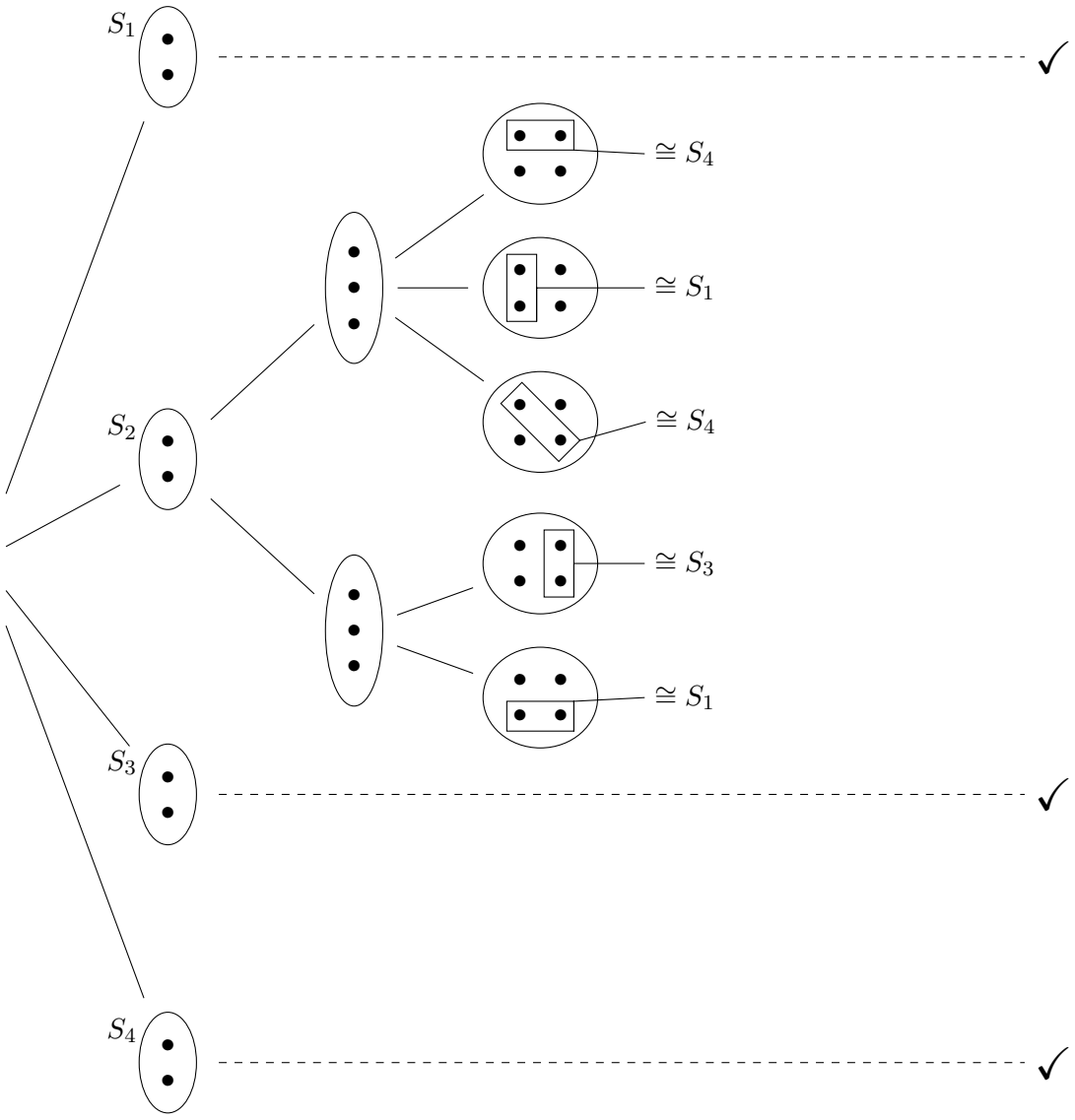
### 6.3.2 Improvement of the Method

It is desirable to exclude a part of the starting configurations without affecting the correctness of the result—not only because the computation time of `CliquerFindAllMaximumCliques(`$\Delta_{\mathcal{M},d}^{(S)}$`)` varies widely but also since the total computation time is approximately

linear in the number of starting configurations. This motivates us to develop a criterion for a starting configuration to be negligible.

Figure 11 illustrates the idea in a simple example: There are four starting configurations $S_1, \ldots, S_4$ of size 2. The computation of `CliquerFindAllMaximumCliques(`$\Delta_{\mathcal{M},d}^{(S_i)}$`)` is already completed for $i \in \{1, 3, 4\}$ and we want to decide whether we can neglect the starting configuration $S_2$. For this, Procedure `Augment()` is applied twice to $S_2$ (to be more precise, it is first applied to $(\{S_2\}; \mathcal{M}, (\Gamma_M, \pi), d)$ and then to $(T; \mathcal{M}, (\Gamma_M, \pi), d)$ where $T$ is the result of the first execution) to obtain all starting configurations of size 4 which result from $S_2$ in the orderly generation. Then we check if each of these configurations of size 4 contains a subset of size 2 which is isomorphic to one of the starting configurations $S_1$, $S_3$ or $S_4$.

Figure 11: Illustration of the improvement strategy for Algorithm 3.



Since this is the case, we in fact can exclude $S_2$ without influencing the classification result. This can be explained in the following way: It is permissible to mix the sizes of the starting configurations as long as all leaves of a subtree of the orderly generation tree are used as starting configurations since the results of `CliquerFindAllMaximumCliques(`$\Delta_{\mathcal{M},d}^{(S)}$`)` for all leaves $S$ include the results of Algorithm 2. In our example, this means that we could use $S_1$, $S_3$, $S_4$ and the five shown sets of size 4 as starting configurations. But each of the starting configurations of size 4 can be neglected since any clique arising from them contains a subset of size 2 which is isomorphic to $S_i$, $i \in \{1, 3, 4\}$, and thus is isomorphic to a (subset of a) clique arising from this set $S_i$.

Transferring this rule to the general case where the sets in $S_k$ are used as starting configurations, gives the following criterion: Let $S \in S_k$ be a starting configuration of size $k$ and let $T$ be the set of configurations of size $m > k$ obtained by subsequently applying Procedure `Augment()` to $S$. Then $S$ can be neglected if every set in $T$ contains a subset of size $k$ which is isomorphic to a configuration $\widetilde{S} \in S_k$ for which the computation of `CliquerFindAllMaximumCliques(`$\Delta_{\mathcal{M},d}^{(\widetilde{S})}$`)` is already completed.

Since the excluded configurations can be considered completed, we can use already excluded configurations of size $k$ for the isomorphism tests additionally to those configurations $S \in S_k$ for which the computation of `CliquerFindAllMaximumCliques(`$\Delta_{\mathcal{M},d}^{(S)}$`)` is already completed. There is a chance that configurations can be neglected this way that otherwise could not.

There are also different further developments of this idea. If one starting configuration can not be excluded completely, either the augmented sets which prevent the set from being excluded can be used as starting configurations instead or they can be augmented further to see if they can be excluded then.

In the case $\mathcal{H}_2(\mathbb{F}_{25})$, the starting configuration which had by far the longest computation time could be excluded by augmenting to size 6.

### 6.4 Heuristic Clique Search

Since the possibilities of the algorithms described in sections 6.2 and 6.3—which are capable of proving the maximum code size including classification—are exhausted quickly, the problem is approached heuristically too. The aim is to at least increase the lower bounds for the maximum code size.

Algorithm 4 is a heuristic approach that seizes the idea of the DLS-MC (dynamic local search for the maximum clique problem) algorithm from [49]. Again, it is used that the problem of finding maximum codes can be translated into a maximum clique problem. The strategy is to first expand a clique as long as possible (improvement phase) and then exchange single vertices in the hope of being able to add vertices again (plateau search phase).

In order to prevent the algorithm from cycling, there is a flag for each vertex which can take the values “available” and “unavailable” and a vertex is set “unavailable” if it is selected during the plateau search phase.

For each non-empty clique $\mathcal{C}$ in a graph with vertex set $V$, there are defined two sets:

$$N_I(\mathcal{C}) = \{v \in V \setminus \mathcal{C} \mid v \text{ is adjacent to all vertices of } \mathcal{C}\}$$

is the set of vertices the current clique $\mathcal{C}$ can be expanded by and

$$N_L(\mathcal{C}) = \{v \in V \setminus \mathcal{C} \mid v \text{ is adjacent to all vertices of } \mathcal{C} \text{ except for one}\}$$

is the set of vertices that can be used to exchange one single vertex in $\mathcal{C}$.

**Algorithm 4:** Heuristic clique search seizing the idea of DLS-MC [49].

**Input**: graph $\Gamma$ with vertex set $V$
**Output**: increasing numbers $m$ and cliques of size $m$

```
1  m ← 0;
2  set all vertices "available";
3  C ← {random(V)};
4  initialize N_I(C) and N_L(C);
5  repeat
6      while N_I(C) ≠ ∅ do
7          v ← random(N_I(C));
8          C ← C ∪ {v};
9          update N_I(C) and N_L(C);
10     end
11     if #C > m then
12         m ← #C;
13         output (m, C);
14     end
15     n_{C∩C'} ← #C;
16     while {w ∈ N_L(C) | w available} ≠ ∅ and n_{C∩C'} > 0 do
17         v ← random({w ∈ N_L(C) | w available});
18         set v "unavailable";
19         w ← vertex in C not adjacent to v;
20         C ← (C \ {w}) ∪ {v};
21         update N_I(C) and N_L(C);
22         n_{C∩C'} ← n_{C∩C'} − 1;
23         if N_I(C) ≠ ∅ then
24             goto line 6;
25         end
26     end
27     v ← random(V \ C);
28     C ← {w ∈ C | w adjacent to v} ∪ {v};
29     update N_I(C) and N_L(C);
30     set all vertices "available";
31 until forever;
```

Algorithm 4 proceeds as follows: At the beginning, the size of the largest clique found so far is initialized with 0 and all vertices are set "available". Then the clique $\mathcal{C}$ is initialized with a set containing only one random vertex. The rest of the algorithm is an infinite loop and can be terminated at any time. In the improvement phase (lines 6 to 10), successively random vertices of the set $N_I(\mathcal{C})$ are added to the clique $\mathcal{C}$ until $\mathcal{C}$ is maximal. After each change of $\mathcal{C}$, the sets $N_I(\mathcal{C})$ and $N_L(\mathcal{C})$ have to be updated to ensure that $\mathcal{C}$ always is a clique.

When the improvement phase is completed, the current clique and its size are output if it is larger than the largest clique found before. In this case, also the variable for the size

of the largest clique found is refreshed. We remark that the output contains only maximal cliques.

In line 15, the variable $n_{\mathcal{C}\cap\mathcal{C}'}$ is set to the size of the current clique. This variable originates from the following termination condition for the plateau search phase of the DLS-MC algorithm: At the beginning of the plateau search phase, the current clique is saved in the variable $\mathcal{C}'$ and the plateau search is terminated when the intersection of $\mathcal{C}$ and $\mathcal{C}'$ becomes empty. Pullan and Hoos adopt this criterion from [34]. In [49, p. 163], it is remarked that this criterion can be realized by decreasing $n_{\mathcal{C}\cap\mathcal{C}'}$ by one each time a vertex is selected and terminating when $n_{\mathcal{C}\cap\mathcal{C}'} = 0$ since—as we will see—the plateau search phase is designed such that each vertex can only be chosen once. We note that those criteria are not exactly equivalent since if a vertex which is not in $\mathcal{C}'$ is first swapped into $\mathcal{C}$ and later swapped out again, $n_{\mathcal{C}\cap\mathcal{C}'}$ decreases faster than $\#(\mathcal{C}\cap\mathcal{C}')$.

The plateau search phase contains the lines 16 to 26. Here, an available vertex is chosen at random from $N_L(\mathcal{C})$ and exchanges the only vertex of $\mathcal{C}$ to which it is not adjacent. Each vertex selected during the plateau search phase of the algorithm is set "unavailable". This prevents the algorithm from choosing the same vertex twice in the plateau search phase. Anyway, we do not prevent an unavailable vertex from enlarging the clique in the improvement phase. After each replacement of an element in $\mathcal{C}$, the sets $N_I(\mathcal{C})$ and $N_L(\mathcal{C})$ are updated and $n_{\mathcal{C}\cap\mathcal{C}'}$ is decreased by one. Those steps are repeated until there are no available vertices left in $N_L(\mathcal{C})$, $n_{\mathcal{C}\cap\mathcal{C}'}$ becomes zero, or $N_I(\mathcal{C})$ becomes non-empty. In the last case, the algorithm jumps back to the improvement phase, in the first two cases, the clique $\mathcal{C}$ is truncated by adding a random vertex $v$ and removing all vertices which are not adjacent to $v$ from $\mathcal{C}$. Before the algorithm starts the improvement phase again, all vertices are made available again.

To reduce the search space and avoid unnecessary symmetries, the graph $\Delta_{\mathcal{M}}^{(\{0\})}$, i.e., the subgraph of $\Delta_{\mathcal{M},d}$ induced by all vertices adjacent to 0, is passed to Algorithm 4 instead of $\Delta_{\mathcal{M},d}$. When outputting $(m,\mathcal{C})$, $m$ has to be increased by one and $\mathcal{C}$ has to be completed with vertex 0. This is not an actual restriction since every code can be offset to include the zero matrix provided that its surrounding matrix space $\mathcal{M}$ forms a group under addition.

Besides Algorithm 4, there is also implemented a greedy variant. A greedy algorithm is one that makes locally the best choice. In our case, this means adding a vertex to the clique which fulfills that the set of vertices which could be added next is as large as possible instead of just a random one. For this, line 7 was exchanged by

---

7 | | $v \leftarrow \text{random}(\{v' \in N_I(\mathcal{C}) \mid \#N_I(\mathcal{C}\cup\{v'\}) \text{ maximal}\})$;

---

It turns out that none of the two versions is essentially better. The greedy variant has its advantage in finding cliques of most sizes faster but with the drawback that it does not find some "hidden" cliques.

The sizes of the largest cliques found are summarized in Table 8 and compared with the upper and lower bounds from section 3. In all attempted symmetric cases, the lower bound could be improved. In the cases $\mathcal{H}_2(\mathbb{F}_{q^2})$, $7 \le q \le 13$, $d = 2$, the lower bounds originate from heuristic search done by Cimráková and Fack in [8]. For $q \in \{7,8,9\}$, we confirm their results, in the case $q = 11$, we can improve it, while in the case $q = 13$ we do not reach their result. In all remaining attempted Hermitian cases, the lower bound is exceeded. The best

Table 8: Sizes of the largest codes found by Algorithm 4 or its greedy version in comparison to the lower and upper bounds summarized in Section 3. Improvements on the lower bounds are marked bold.

| $\mathcal{S}_n(\mathbb{F}_q)$ | $n=3,\ d=2$ | | | | $n=4,\ d=2$ | $n=5,\ d=4$ |
|---|---|---|---|---|---|---|
| | $q=3$ | $q=4$ | $q=5$ | $q=7$ | $q=2$ | $q=2$ |
| lower bound | 90 | 256 | 625 | 2401 | 256 | 64 |
| heuristic result | **135** | **428** | **934** | **3100** | **320** | **96** |
| upper bound | 201 | 4033 | 2705 | 15001 | 1009 | 1024 |

| $\mathcal{H}_n(\mathbb{F}_{q^2})$ | $n=2,\ d=2$ | | | | | | $n=3,\ d=2$ | $n=4,\ d=4$ |
|---|---|---|---|---|---|---|---|---|
| | $q=7$ | $q=8$ | $q=9$ | $q=11$ | $q=13$ | $q=16$ | $q=2$ | $q=2$ |
| lower bound | 97 | 125 | 145 | 215 | 272 | 271 | 64 | 16 |
| heuristic result | 97 | 125 | 145 | **239** | 194 | **289** | **120** | **37** |
| upper bound | 175 | 216 | 369 | 671 | 1105 | 1296 | 176 | 86 |

codes found by our heuristic search are recorded on a disc attached to this thesis.

Altogether, the heuristic computations lasted about five weeks utilizing several computers. In the smallest cases, almost all runs reached the best result while in the others, mostly only one amongst several runs did. In those cases, the best result often outdistances the rest which indicates a hidden solution which is only found if the algorithm is lucky.

In Figure 12, the new lower bounds for the sizes maximum codes in $\mathcal{H}_2(\mathbb{F}_{q^2})$ with minimum distance 2 (for $q \leq 5$ these are the sizes of maximum codes) are compared to the function $2q^2$. The plot suggests the assumption that the maximum code size grows like $2q^2$, though the heuristics (including the one in [8] for $q = 13$) did not find sizes near this value for $q \geq 13$. Actually, all found codes are of size $< 2q^2$. This possibly might be true for all codes with minimum distance 2 in $\mathcal{H}_2(\mathbb{F}_{q^2})$.

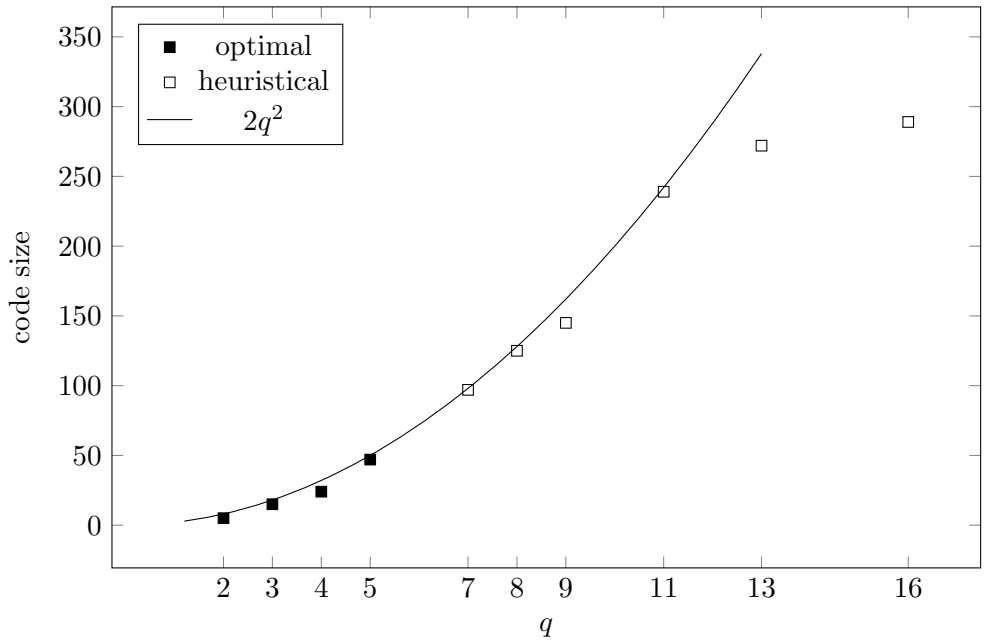
# 7 Conclusion

## 7.1 Results

In this thesis, the maximum codes in $\mathcal{H}_2(\mathbb{F}_4)$, $\mathcal{H}_2(\mathbb{F}_9)$, $\mathcal{H}_2(\mathbb{F}_{16})$, $\mathcal{S}_3(\mathbb{F}_2)$, and $\mathcal{H}_2(\mathbb{F}_{25})$, each with minimum distance $\geq 2$ have been classified. In latter case, this implied the proof that the lower bound on the maximum code size, 47, which was given by Cimráková and Fack in [8] by heuristic search, is tight. In each of the matrix spaces $\mathcal{H}_2(\mathbb{F}_4)$, $\mathcal{H}_2(\mathbb{F}_9)$, $\mathcal{S}_3(\mathbb{F}_2)$, and $\mathcal{H}_2(\mathbb{F}_{25})$, it was shown that the maximum code is unique up to isomorphism and those codes could be interpreted quite satisfyingly: A maximum code in $\mathcal{H}_2(\mathbb{F}_4)$ is isomorphic to the set of rank-1-matrices while a maximum code in $\mathcal{S}_3(\mathbb{F}_2)$ with minimum distance 2 is isomorphic to the set which contains the zero matrix and all non-alternate rank-2 matrices. A maximum code in $\mathcal{H}_2(\mathbb{F}_9)$ is closely related to the Cremona-Richmond configuration and a maximum code in $\mathcal{H}_2(\mathbb{F}_{25})$ features an octahedral symmetry. In $\mathcal{H}_2(\mathbb{F}_{16})$, there are seven different isomorphism classes of maximum codes.

In some more cases, it was possible to construct new codes which improve the known

Figure 12: Optimal and best heuristical code sizes for codes in $\mathcal{H}_2(\mathbb{F}_{q^2})$ with minimum distance $\geq 2$ in comparison to the function $2q^2$.




lower bounds on the maximum code size by heuristic search.

Furthermore, a construction for additive codes with minimum distance 2 of size $q^{n(n-1)}$ in $\mathcal{H}_n(\mathbb{F}_{q^2})$ was given. This provides a partial answer to the question whether additive codes of size $q^{n(n-d+1)}$ with minimum distance $d < n$ where $n$ and $d$ are both even exist in $\mathcal{H}_n(\mathbb{F}_{q^2})$ and how to construct them [57, remark after Thm. 5]. The question remains open for $4 \leq d < n$ where $n$ and $d$ are both even.

This construction also improves the lower bound on the maximum code size in $\mathcal{H}_n(\mathbb{F}_{q^2})$ in the cases where $d = 2$ and $n \geq 4$ even. All improvements on lower bounds are summarized in Table 9.

Table 9: Improvements on lower bounds for the maximum code size.

| $\mathcal{S}_n(\mathbb{F}_q)$ | $n=3,\ d=2$ | | | | $n=4,\ d=2$ | $n=5,\ d=4$ |
|---|---|---|---|---|---|---|
| | $q=3$ | $q=4$ | $q=5$ | $q=7$ | $q=2$ | $q=2$ |
| previous | 90 | 256 | 625 | 2401 | 256 | 64 |
| new | **135** | **428** | **934** | **3100** | **320** | **96** |

| $\mathcal{H}_n(\mathbb{F}_{q^2})$ | $n=2,\ d=2$ | | $n=3,\ d=2$ | $n=4,\ d=4$ | $n \geq 4$ even, $d=2$ |
|---|---|---|---|---|---|
| | $q=11$ | $q=16$ | $q=2$ | $q=2$ | $q$ arbitrary prime power |
| previous | 215 | 271 | 64 | 16 | $q^{n(n-2)}$ |
| new | **239** | **289** | **120** | **37** | $\boldsymbol{q^{n(n-1)}}$ |

It was also possible to slightly improve the upper bound for the size of a maximum code with minimum distance 2 in $\mathcal{S}_n(\mathbb{F}_q)$. The new upper bound in this case is $q^{n(n+1)/2} - q^n + 1$ whereas the previous bound equaled the number $q^{n(n+1)/2}$ of symmetric matrices in $\mathcal{S}_n(\mathbb{F}_q)$.

Besides this research on bounds and classification, it was also shown that in general, the automorphism group of a code depends on its ambient space in a nontrivial way.

## 7.2 Further Work

For further research, the following ideas are suggested:

- Improve the known upper bound for the maximum code size in $\mathcal{H}_2(\mathbb{F}_{q^2})$. The best known bound is $\min\left\{\frac{1}{2}(q^3+q), \left(\frac{(p+2)(p+1)^2p}{12}\right)^e\right\}$, where $q = p^e$, $p$ prime. Our results suggest that $2q^2$ might be a good upper bound.

- Though the maximum code size is known in the unrestricted case, those codes should be classified with respect to the concept of isomorphism presented in section 4.1. No such research is known to the author of this thesis.

- Classify codes in the symmetric and Hermitian cases, where the known upper and lower bounds coincide. For symmetric matrices, this is the case when $d$ is odd or $d = n$. For Hermitian matrices, the upper and lower bounds coincide when $d$ is odd.

- Apply the heuristic presented in section 6.4 using starting configurations bigger than $\{0\}$. This could also solve the problem that (for example in the case $\mathcal{H}_4(\mathbb{F}_9)$, $d = 4$) the graph $\Delta_{\mathcal{M}}^{(\{0\})}$ is too large to fit into 32 GB RAM and 108.5 GB swap.

- A strategy which was not pursued in this thesis is formulating the maximum clique search in $\Delta_{\mathcal{M},d}$ as an integer linear programming (ILP) problem and pass it to an appropriate solver. This has the advantage that the solver successively improves both the upper and lower bounds. However, the resulting ILPs are quite big and computationally hard to solve. In the orientation phase of this thesis, this was checked out using Gurobi [30] for the case $\mathcal{S}_3(\mathbb{F}_3)$. After about 4.5 days, the upper bound was reduced from 201 to 198 while the lower bound was raised from 90 to 135. Also the performance did not improve considerably by prescribing small starting configurations. It should be noted that even if the solver finds an exact solution, this does not involve a classification.

- The approach which looks most promising for further classification results is to extend the improvement ideas of Section 6.3.2, for example, in the following way: Starting with a full set $S_k$ of starting configurations of size $k$, each time the computation of `CliquerFindAllMaximumCliques(`$\Delta_{\mathcal{M},d}^{(S)}$`)` finishes for some $S$ in $S_k$, the unfinished starting configurations are checked for redundancy. This can be done by extending step by step rather than extending to a predefined size $m$ and checking for subsets isomorphic to completed or excluded sets $\widetilde{S} \in S_k$ after each augmentation step.

  For the next case in reach, $\mathcal{H}_3(\mathbb{F}_4)$, $d = 2$, $k$ should be chosen at least 5 since the computation time for single starting configurations of size 4 exceeds three weeks by far, see page 48 in Section 6.3.

# A Partial Spreads and Partial Ovoids in Classical Polar Spaces

**Definition A.1.** [7, Section 1.4] A *polar space* S is a set of points together with distinguished subsets called subspaces such that:

(i) a subspace together with the subspaces it contains is a $d$-dimensional projective space with $-1 < d < n-1$ for some integer n which is called the rank of S;

(ii) the intersection of any two subspaces is a subspace;

(iii) given a subspace $L$ of dimension $n-1$ and a point $p \in S \setminus L$ , there exists a unique subspace $M$ containing $p$ such that $\dim(M \cap L) = n-2$ and it contains all points of $L$ which are joined to $p$ by some subspace of dimension one;

(iv) there exist disjoint subspaces of dimension $n-1$.

**Definition A.2.** [9, Section 1] The *generators* of a classical polar space are the subspaces of maximal dimension.

**Definition A.3.** [62, Section 1.1]

1. $H(n, q^2)$ is the polar space formed by the points and lines of a non-singular Hermitian variety $H$ in $\mathrm{PG}(n, q^2)$, $n \geq 3$. Its rank is $\lceil \frac{n}{2} \rceil$.

2. $Q^-(2n+1, q)$ is the polar space formed by the points and lines of a non-singular elliptic quadric $Q^-$ in $\mathrm{PG}(2n+1, q)$, $n \geq 2$. Its rank is $n$.

**Theorem A.4.** *[62, Thm. 5] $Q^-(5, q)$ is isomorphic to the dual of $H(3, q^2)$.*

**Definition A.5.** [9, Section 1]

1. A *partial spread* of a classical polar space $\mathcal{P}$ is a set $\mathcal{S}$ of pairwise disjoint generators of $\mathcal{P}$.

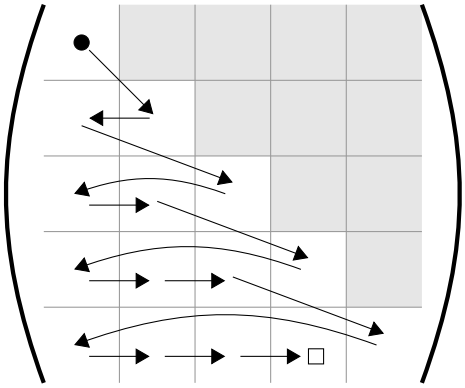
2. A *partial ovoid* of a classical polar space $\mathcal{P}$ is a set $\mathcal{O}$ of points of $\mathcal{P}$ such that every generator contains at most one point of $\mathcal{O}$.

# B Numbering of the Matrices

The basis of the numbering of the matrices is a numbering of the field elements. Since we represent a non-prime field $\mathbb{F}_q$, $q = p^e$ with $p$ prime, as $\mathbb{F}_p[x]/(g)$ where $g$ is an irreducible polynomial, the field elements $a_i \in \mathbb{F}_q$ $(0 \leq i < q)$ are represented as polynomials $f_i \in \mathbb{F}_p[X]$ with degree at most $e-1$. These polynomials can also be considered as polynomials $\widetilde{f_i} \in \mathbb{Z}[x]$ with degree at most $e-1$ and coefficients in $\{0, \ldots, p-1\}$. Thinking of the positional notation system with base $p$, it is easy to see that $\widetilde{f_i}(p)$ takes all values in $\{0, \ldots, p^e - 1\}$ as $i$ varies from 0 to $q-1$. Now the numbering of the field elements $a_i$ is chosen such that $\widetilde{f_i}(p) = i$ for all $0 \leq i < q$. Note that, in the case of non-prime fields, this numbering of the field elements depends on the irreducible polynomial $g$.

For the matrix spaces used in calculations of this thesis, the numbering of the matrices is explicitly given on the disc attached to this thesis. The numbering of symmetric and Hermitian matrices in the general case is described in the following.

Figure B.1: The order of matrix entries used in the numbering of symmetric matrices using the example $\mathcal{S}_5(\mathbb{F}_q)$.



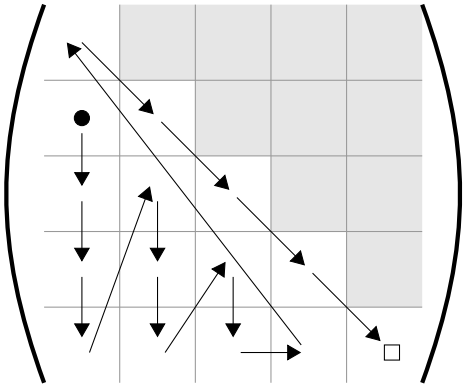
## B.1 Symmetric Matrices

There are $q^{n(n+1)/2}$ symmetric $n \times n$ matrices with entries in $\mathbb{F}_q$. To obtain the matrix $M_i$ where $i \in \{0, \ldots, q^{n(n+1)/2} - 1\}$, proceed as follows: Write the number $i$ in positional notation with base $q$. Then—beginning with the least significant digit—fill the matrix entries in the order illustrated in Figure B.1 with the field elements $a_j \in \mathbb{F}_q$ corresponding to the digits $j$ of $i$ in this notation. Finally, the gray fields have to be filled such that the resulting matrix is symmetric.

## B.2 Hermitian Matrices

Since, in a Hermitian matrix in $\mathcal{H}_n(\mathbb{F}_{q^2})$, the $n$ entries on the main diagonal can only take values in $\mathbb{F}_q \subset \mathbb{F}_{q^2}$ while the remaining $n(n-1)$ entries can take all values in $\mathbb{F}_{q^2}$, the numbering of Hermitian matrices is a bit more complicated than the numbering of symmetric matrices. To proceed similar to the latter, we need a mixed radix positional notation system where the $\frac{n(n-1)}{2}$ least significant digits can take values from 0 to $q^2 - 1$ while the more significant digits can only take values up to $q - 1$. Besides the numbering of the field elements of $\mathbb{F}_{q^2} = \{a_0, \ldots, a_{q^2-1}\}$ which is taken as described above, we additionally need a numbering of the subfield $\mathbb{F}_q = \{b_0, \ldots, b_{q-1}\} \subset \mathbb{F}_{q^2}$ which is obtained by numbering the elements of $\mathbb{F}_q$ in the order they show up in $\mathbb{F}_{q^2}$, that is, such that $b_j = a_{i_j} = \overline{a_{i_j}}$ and $i_0 < \cdots < i_{q-1}$.

Figure B.2: The order of matrix entries used in the numbering of Hermitian matrices using the example $\mathcal{H}_5(\mathbb{F}_{q^2})$.



To obtain the matrix $M_i$ where $i \in \{0, \ldots, q^{(n^2)} - 1\}$, we write this number $i$ in the mixed radix notation described above and fill the matrix entries in the order illustrated by Figure B.2 with the field elements $a_j \in \mathbb{F}_{q^2}$ or alternatively $b_j = a_{i_j} \in \mathbb{F}_q$ determined by the digits $j$ of $i$, depending on whether the entry lies on the main diagonal or not. At the end, the gray entries have to be filled such that the resulting matrix is Hermitian.

## References


[1] T. P. Berger. Isometries for rank distance and permutation group of gabidulin codes. *IEEE Transactions on Information Theory*, 49(11):3016–3019, Nov 2003.

[2] A. Blokhuis and G. E. Moorhouse. Some p-ranks related to orthogonal spaces. *Journal of Algebraic Combinatorics*, 4(4):295–316, 1995.

[3] M. Boben, B. Grunbaum, T. Pisanski, and A. Zitnik. Small triangle-free configurations of points and lines. *Discrete & Computational Geometry*, 35(3):405–427, 2006.

[4] B. Bollobás. *Extremal Graph Theory*. Dover Books on Mathematics. Dover Publications, 2013.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[6] R. Bruck and R. Bose. The construction of translation planes from projective spaces. *Journal of Algebra*, 1(1):85 – 102, 1964.

[7] F. Buekenhout and E. Shult. On the foundations of polar geometry. *Geometriae Dedicata*, 3(2):155–170, August 1974.

[8] M. Cimráková and V. Fack. Searching for maximal partial ovoids and spreads in generalized quadrangles. *Bull. Belg. Math. Soc. Simon Stevin*, 12(5):697–706, 2005.

[9] J. De Beule, A. Klein, K. Metsch, and L. Storme. Partial ovoids and partial spreads in hermitian polar spaces. *Des. Codes Cryptography*, 47(1-3):21–34, 2008.

[10] J. de la Cruz, E. Gorla, H. H. Lopez, and A. Ravagnani. Rank distribution of delsarte codes. *arXiv preprint arXiv:1510.01008*, 2015.

[11] J. de la Cruz, M. Kiermaier, A. Wassermann, and W. Willems. Algebraic structures of MRD codes. *arXiv preprint arXiv:1502.02711v1*, 2015.

[12] P. Delsarte. *An algebraic approach to the association schemes of coding theory*. PhD thesis, Philips Research Laboratories, 1973.

[13] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25(3):226 – 241, 1978.

[14] P. Delsarte and J. Goethals. Alternating bilinear forms over GF(q). *Journal of Combinatorial Theory, Series A*, 19(1):26 – 50, 1975.

[15] P. Delsarte and V. Levenshtein. Association schemes and coding theory. *Information Theory, IEEE Transactions on*, 44(6):2477–2504, Oct 1998.

[16] I. Dolgachev. Abstract configurations in algebraic geometry. *arXiv preprint math/0304258*, 2003.

[17] J.-G. Dumas, R. Gow, and J. Sheekey. Rank properties of subspaces of symmetric and hermitian matrices over finite fields. *Finite Fields and Their Applications*, 17(6):504–520, 2011.

[18] G. Ebert and J. Hirschfeld. Complete systems of lines on a hermitian surface over a finite field. *Designs, Codes and Cryptography*, 17(1-3):253–268, 1999.

[19] W. L. Edge. Fundamental figures, in four and six dimensions, over GF(2). *Mathematical Proceedings of the Cambridge Philosophical Society*, 60:183–195, 4 1964.

[20] T. Feulner. Computergestützte Berechnung eines eindeutigen Repräsentanten der semilinearen Isometrieklasse eines fehlerkorrigierenden, linearen Codes und Bestimmung der Automorphismengruppe. Diploma thesis, Universität Bayreuth, January 2008. available at `http://www.algorithm.uni-bayreuth.de/de/team/Feulner_Thomas/Diplomarbeit.pdf`.

[21] E. Gabidulin. Theory of codes with maximum rank distance. *Probl. Inf. Transm.*, 21:1–12, 1985.

[22] E. M. Gabidulin. Attacks and counter-attacks on the gpt public key cryptosystem. *Designs, Codes and Cryptography*, 48(2):171–177, 2008.

[23] E. M. Gabidulin, M. Bossert, and P. Lusina. Space-time codes based on rank codes. In *Information Theory, 2000. Proceedings. IEEE International Symposium on*, page 284. IEEE, 2000.

[24] E. M. Gabidulin, A. Paramonov, and O. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In *Advances in Cryptology—EUROCRYPT'91*, pages 482–489. Springer, 1991.

[25] E. M. Gabidulin and N. I. Pilipchuk. Symmetric matrices and codes correcting rank errors beyond the $\lfloor (d-1)/2 \rfloor$ bound. *Discrete applied mathematics*, 154(2):305–312, 2006.

[26] M. Gadouleau and Z. Yan. Properties of rank metric codes. *CoRR*, abs/cs/0702077, 2007.

[27] D. J. H. Garling. *A course in Galois theory*. Cambridge University Press, 1986.

[28] R. Gow, M. Lavrauw, J. Sheekey, and F. Vanhove. Constant rank-distance sets of hermitian matrices and partial spreads in hermitian polar spaces. *Electr. J. Comb.*, 21(1):P1.26, 2014.

[29] R. Gugisch. *Konstruktion von Isomorphieklassen orientierter Matroide*. Dissertation, Universität Bayreuth, 2005. available at `http://www.mathe2.uni-bayreuth.de/ralfg/papers/diss.pdf`.

[30] I. Gurobi Optimization. Gurobi optimizer reference manual, 2015.

[31] L.-K. Hua. Geometries of matrices. i. generalizations of von staudt's theorem. *Transactions of the American Mathematical Society*, 57(3):441–481, 1945.

[32] L.-K. Hua. A theorem on matrices over a sfield and its applications. *Acta Math. Sinica*, 1(2):109–163, 1951.

[33] F. Ihringer. A new upper bound for constant distance codes of generators on hermitian polar spaces of type $H(2d-1,q^2)$. *Journal of Geometry*, 105(3):457–464, 2014.

[34] K. Katayama, A. Hamamoto, and H. Narihisa. Solving the maximum clique problem by k-opt local search. In *Proceedings of the 2004 ACM Symposium on Applied Computing*, SAC '04, pages 1021–1025, New York, NY, USA, 2004. ACM.

[35] A. Khaleghi, D. Silva, and F. R. Kschischang. Subspace codes. In M. Parker, editor, *Cryptography and Coding*, volume 5921 of *Lecture Notes in Computer Science*, pages 1–21. Springer Berlin Heidelberg, 2009.

[36] M. Kiermaier, 2015. personal communication.

[37] R. Koetter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, Aug 2008.

[38] D. Král', E. Máčajová, O. Pangrác, A. Raspaud, J.-S. Sereni, and M. Škoviera. Projective, affine, and abelian colorings of cubic graphs. *European Journal of Combinatorics*, 30(1):53 – 69, 2009.

[39] A. Kshevetskiy and E. Gabidulin. The new construction of rank codes. In *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*, pages 2105–2108, Sept 2005.

[40] P. Loidreau. Properties of codes in rank metric. *CoRR*, abs/cs/0610057, 2006.

[41] J. MacWilliams. Orthogonal matrices over finite fields. *The American Mathematical Monthly*, 76(2):152–164, 1969.

[42] B. D. McKay. Practical graph isomorphism. *Congressus Numerantium*, 30:45–87, 1981.

[43] B. D. McKay. Isomorph-free exhaustive generation. *Journal of Algorithms*, 26(2):306 – 324, 1998.

[44] B. D. McKay and A. Piperno. Nauty and traces user's guide (version 2.5). *Computer Science Department, Australian National University, Canberra, Australia*, 2013.

[45] B. D. McKay and A. Piperno. Practical graph isomorphism, II. *CoRR*, abs/1301.1493, 2013.

[46] G. L. Mullen and C. Mummert. *Finite fields and applications*. American Math. Soc., 2007.

[47] S. Niskanen and P. R. Östergård. Cliquer User's Guide, Version 1.0. Technical Report T48, Communications Laboratory, Helsinki University of Technology, 2003.

[48] K. Otal and F. Özbudak. Some non-Gabidulin MRD codes. talk at ALCOMA 2015, slides available at `http://alcoma15.uni-bayreuth.de/files/slides/contributed/otal_20.pdf`, 2015.

[49] W. Pullan and H. H. Hoos. Dynamic local search for the maximum clique problem. *Journal of Artificial Intelligence Research*, pages 159–185, 2006.

[50] R. C. Read. Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations. *Annals of Discrete Mathematics*, 2:107–120, 1978.

[51] H. W. Richmond. On the figure of six points in space of four dimensions. *The quarterly journal of pure and applied mathematics*, 31:125–160, 1900.

[52] R. Roth. Maximum-rank array codes and their application to crisscross error correction. *Information Theory, IEEE Transactions on*, 37(2):328–336, Mar 1991.

[53] G. F. Royle. An orderly algorithm and some applications in finite geometry. *Discrete Mathematics*, 185(1):105–115, 1998.

[54] K. U. Schmidt. $\mathbb{Z}_4$-valued quadratic forms and quaternary sequence families. *IEEE Transactions on Information Theory*, 55(12):5803–5810, Dec 2009.

[55] K.-U. Schmidt. Symmetric bilinear forms over finite fields of even characteristic. *Journal of Combinatorial Theory, Series A*, 117(8):1011–1026, 2010.

[56] K.-U. Schmidt. Symmetric bilinear forms over finite fields with applications to coding theory. *CoRR*, abs/1410.7184, 2014.

[57] K.-U. Schmidt. Hermitian rank distance codes. personal communication, May 2015.

[58] K.-U. Schmidt. Symmetric rank distance codes. talk at ALCOMA 2015, slides available at `http://alcoma15.uni-bayreuth.de/files/slides/contributed/schmidt.pdf`, 2015.

[59] K.-U. Schmidt, February 2016. personal communication.

[60] J. Sheekey. A new family of linear maximum rank distance codes. *arXiv preprint arXiv:1504.01581*, 2015.

[61] D. Silva and F. R. Kschischang. On metrics for error correction in network coding. *IEEE Transactions on Information Theory*, 55(12):5479–5490, Dec 2009.

[62] J. Thas. Old and new results on spreads and ovoids of finite classical polar spaces. In P. C. A. Barlotti, A. Bichara and G. Tallini, editors, *Combinatorics '90Recent Trends and ApplicationsProceedings of the Conference on Corn binatorics, Gaeta*, volume 52 of *Annals of Discrete Mathematics*, pages 529 – 544. Elsevier, 1992.

[63] F. Vanhove. The maximum size of a partial spread in $H(4n+1, q^2)$ is $q^{2n+1}+1$. *Electr. J. Comb.*, 16(1), 2009.

[64] T. Vis. The existence and uniqueness of a simple group of order 168. available at `http://math.ucdenver.edu/~tvis/Coursework/Fano.pdf`, accessed 3 December 2015, February 2007.

[65] Z. Wan. *Geometry of Matrices*. World Scientific, Jan. 1996.

[66] H. Wang, C. Xing, and R. Safavi-Naini. Linear authentication codes: bounds and constructions. *IEEE Transactions on Information Theory*, 49(4):866–872, April 2003.

[67] P. R. Östergård. A fast algorithm for the maximum clique problem. *Discrete Applied Mathematics*, 120(1):197–207, 2002.

## Affirmation

Hereby I affirm that I have written this thesis independently and without using other sources or means than those explicitly stated. This thesis or parts of it have not previously been submitted in order to obtain any academic degree and have also not yet been published.

Langenzenn, March 30, 2016