Radboud University Nijmegen

Faculty of Science

The MCE problem given codes with non-trivial automorphism groups

Master Thesis in Mathematics

Daily supervisor:
Krijn Reijnders

Author:
Tjitske Koster

Supervisor:
Dr. Simona Samardjiska

Second reader:
Dr. Wieb Bosma

July 25, 2024

Contents

1 Introduction

Large scale quantum computers do not yet exist, but if one were to be built a quantum computer it would be able to break many of the public-key cryptosystems systems currently used [11]. Because scientist believe that a large scale quantum computer could be build in the not-too-distant future, there is a present need to construct cryptographic systems secure against a quantum computer. Constructing a cryptographic system, testing its security and then implementing it in everyday use, can take a long time [11]. Time we can not afford to waste.

To create a cryptographic system resistant to quantum attacks, one typically uses the hardness assumption of a mathematical problem. Equivalence problems are often used as the basis for such cryptographic systems. They take two mathematical objects and ask for an equivalence mapping relating the two. The equivalence map should preserve some structure of the objects. This preservation requirement makes it more difficult for an adversary to find an equivalence map given only the two objects.

For example, the code equivalence problem takes as input two codes with the Hamming metric and asks for an equivalence between the codes that preserves the metric. Finding a one-to-one map between the two finite codes can be easily done. Finding a one-to-one map that preserves the metric is more difficult. It is thus assumed that an adversary would not be able to construct such a map.

Given an equivalence problem one can construct a Sigma protocol. If the equivalence is hard to find for an adversary (using a quantum computer), multiple rounds of a Sigma protocol give a zero knowledge identification scheme. This identification scheme gives rise to a provable secure signature scheme with the Fiat-Shamir transform [7]. The security of the signature scheme relies on the hardness of finding the equivalence. Therefore, if a new equivalence problem is proposed for this signature scheme, it must be determined how difficult it is to find the equivalence.

In 2023 the Matrix Equivalence Digital Signature Scheme (MEDS) was submitted to the NIST post quantum cryptographic standardization process. This competition is created to select cryptographic systems that are secure against a quantum computer. MEDS is a signature scheme based on matrix codes and equivalences. This thesis aims to find the security of the signature scheme MEDS. By studying the hardness of the underlying problem.

The MEDS system relies on the equivalence problem for matrix codes, where the equivalence must preserve the so-called rank metric. This metric is defined by the rank distance between two codewords, two matrices $A, B \in \mathcal{M}_{n,m}(q)$. The rank distance is defined to be $d(A, B) = \mathrm{rnk}(A - B)$. A *matrix code* is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{n\times m}$ endowed with this rank metric. An isometry between two codes $\mathcal{C}$ and $\mathcal{D}$ is a mapping that preserves the rank metric.

Any isometry $\mu\colon \mathcal{C} \to \mathcal{D}$ can in fact be written as $\mu = (L, R)$ with $L, R \in \mathrm{GL}_n(q)$, where the mapping is given by $\mathbf{C} \mapsto L\mathbf{C}R$, or as matrix transposition, i.e., the mapping $\mathbf{C} \mapsto \mathbf{C}^\top$. Alternatively, the isometry may be a combination of both forms. Any isometry is of this form as proven in [9, 19]. In this thesis, we consider only isometries of the first form as commonly done, [2, 3, 5, 13].

The equivalence problem for two matrix codes $\mathcal{C}$ and $\mathcal{D}$ can now be defined and asks for an isometry between the codes.

Problem 1. The *Matrix Code Equivalence problem (MCE)*;
Given two equivalent matrix codes $\mathcal{C}$ and $\mathcal{D}$ over $\mathbb{F}_q^{n\times m}$;
Problem: find two matrices $L \in \mathrm{GL}_n(q)$ and $R \in \mathrm{GL}_m(q)$ such that $L\mathcal{C}R = \mathcal{D}$.

The hardness of the MCE problem is previously investigated in [5, 13], both for a classical and quantum computer. This thesis extends the research on the complexity of the MCE problem, providing further insights into its computational hardness.

The complexity of solving the MCE problem depends on the structure of the codes. In particular the presence of automorphisms. We define an *automorphism* of a matrix code $\mathcal{C} \subseteq \mathcal{M}_{n,m}(q)$ to be an isometry from a code onto itself. The *automorphism group* of $\mathcal{C}$, denoted as $\mathrm{Aut}(\mathcal{C})$, consists of all automorphisms of $\mathcal{C}$. The code has a *trivial automorphism group* if the only automorphism of the code is multiplication with a scalar from $\mathbb{F}_q$.

Reijnders, Samardjiska, and Trimoska in [13] investigated the hardness of the MCE problem with the assumption that the codes have trivial automorphisms. Under this assumption they were able to prove that the MCE problem is polynomial time equivalent to *Bilinear Maps Linear Equivalence* and the *Quadratic Maps Linear Equivalence* problem. Using the second reduction Reijnders, Samardjiska, and Trimoska could give an algorithm to solve the MCE problem in time complexity $\mathcal{O}\left(q^{\min\{n,m\}}\right)$ [13, Algorithm 2].

On the other hand, if the codes are guaranteed to have many automorphisms, the MCE problem becomes more easy to solve. If the codes are $\mathbb{F}_{q^n}$-linear, then there exists an algorithm that solves the MCE problem in polynomial time [5, Algorithm 3].

The same article investigates a variant of the MCE problem where the left side of the isometry is the identity matrix. This variant of the MCE problem is called the Matrix Code Right Equivalence problem and can be solved in polynomial time [5, Algorithm 2].

Problem 2. The *Matrix Code Right Equivalence problem (MCRE)*;
Given two matrix codes $\mathcal{C}$ and $\mathcal{D}$ over $\mathbb{F}_q^{n\times m}$;
Problem: find if there exists a matrix $R \in \mathrm{GL}_m(q)$ such that $\mathcal{C}R = \mathcal{D}$.

This thesis aims to describe the complexity of the MCE problem when the matrix codes have non-trivial automorphisms and the codes are not $\mathbb{F}_{q^n}$-linear. Using the structure of the automorphism groups this thesis develops the Sylvester algorithm. The Sylvester algorithm can be used to discover the isometry for two equivalent codes. This thesis moreover describes the computational complexity of this algorithm.

Contributions. Given two matrix codes, this thesis investigates the space of all isometries that exists between these codes, the isometry group. The size of this isometry group heavily depends on the automorphism groups of the codes. If the codes have many automorphisms, there are also many isometries connecting the codes. Even stronger, the structure of the automorphism groups relates to the structure of the isometry group. This thesis investigates the relation between these structures. As a result, we develop and present the Sylvester algorithm for the MCE problem. This algorithm does not require the codes to have non-trivial automorphism groups, but for codes with trivial automorphism groups the algorithm yields an exponential complexity.

The Sylvester algorithm uses the structure of the automorphism groups to form Sylvester equations. The isometry should be a solution to the Sylvester equation generated by the algorithm. A brute force approach is then used to search through all potential solutions to

the Sylvester equation, ensuring that at least one isometry is found. The complexity of the algorithm mostly depends on the size of solution space to the Sylvester equation, as the size of this solution space determines the complexity of the brute force attack.

The Sylvester algorithm presented in this thesis can be used to solve the MCE problem. The algorithm yields a polynomial time complexity if the codes are $\mathbb{F}_{q^n}$-linear. If the codes have trivial automorphism groups, the Sylvester algorithm yields a complexity comparable to that of a brute force attack. This high complexity is a direct consequence of the because brute force used during the Sylvester algorithm.

Furthermore, this thesis gives the complexity of finding the isometry in all other cases. This is to say for codes that have non-trivial automorphism groups that are not $\mathbb{F}_{q^n}$-linear. The complexity can be found in Theorem 8.1 and Theorem 8.2. It depends on the number of automorphisms that the codes have. If the codes have several automorphisms, the complexity moreover depends on the specific automorphism that is used during the Sylvester attack. A different automorphism leads to a different Sylvester equation which leads to a different number of solutions to this equation.

Outline. Section 2 introduces main objects and tools that we consider throughout the thesis. Section 3 provides background information on the matrix code equivalence problem. It explains the relation between the automorphism and isomorphism groups and introduces the outline of the Sylvester algorithm that uses this structure relation. Section 4 states some remarks about how we can obtain the automorphisms needed to find the isometry and thus to preform the Sylvester algorithm. Section 5 and Section 6 together give a detailed description of the Sylvester algorithm. Section 7 investigates the complexity to preform the Sylvester algorithm. Section 8 summarizes the Sylvester algorithm and the complexity. Section 9 concludes the thesis and addresses some points for further research.

Acknowledgments. Special thanks to my supervisors Simona Samardjiska and Krijn Reijnders for guiding me during the process of research and the writing of this thesis. Thanks as well to my second reader Wieb Bosma for reading this thesis. Special thanks to Ina de Vries, who kindly helped me find the courses that lie in my interest and which provided me with the right background to write this thesis.

Thanks to all the students in the master room: Eline, Gilan, Nathan, Robin, and Wouter, for providing me with distraction and laughter when I needed it. Thanks also for helping me correct my English mistakes and figure out the "trivial" proofs that I stumbled upon.

2 Preliminaries

We write $\mathbb{F}_q$ for the finite field of q elements with q a prime power. I.e. $q = p^n$ for some $n \geq 0$ and p a prime number. The characteristic of the finite field is then defined as p and denoted as $\text{Char}(\mathbb{F}_q)$. We define $\mathbb{F}_q^*$ to be $\mathbb{F}_q \backslash \{0\}$. We use capital calligraphic letters like $\mathcal{C}, \mathcal{D}$ to indicate codes, and capital bold letters like $\mathbf{C}, \mathbf{D}$ to denote codewords. Capital letters like A, B are used to denote matrices that are not considered as codewords.

The space of matrices over $\mathbb{F}_q$ of size $n \times m$ is denoted $\mathcal{M}_{n,m}(q)$ or $\mathcal{M}_n(q)$ if $m = n$. The space of non-singular $n \times n$ matrices over $\mathbb{F}_q$ is denoted $\text{GL}_n(q)$. The projective space of non-singular matrices is denoted $\text{PGL}_n(q)$. In this projective space multiplication by scalars is not considered. For the identity matrix we write $\mathbf{I}$. For prime numbers other than the characteristic of the field r is used.

In literature, it is commonly assumed that matrix multiplication can be performed in time $\mathcal{O}\left(n^3\right)$. This assumption is based on the standard and practical algorithm that yields this time complexity as noted in [16]. However, Strassen discovered a method to multiply two matrices in time $\mathcal{O}\left(n^{\log(7)}\right)$, which approximates to $\mathcal{O}\left(n^{2.81}\right)$ [17]. The fastest algorithm for matrix multiplication known is presented by Coppersmith and Winograd. They prove that two matrices can be multiplied in time $\mathcal{O}\left(n^{2.376}\right)$ [4]. In this thesis we follow [1] and denote $M(n)$ for the complexity of matrix multiplication, the complexity of Sylvester algorithm can then easily be calculated when the algorithm is implemented.

2.1 Basic properties of matrices

Non-singular matrices are used intensively, thus this section introduces general properties of $\text{GL}_n(q)$. The size of $\text{GL}_n(q)$ is well known, [8, page 381], [15, Proposition 1.10.1].

Lemma 2.1. *There are* $\prod_{k=0}^{n-1} q^n - q^k$ *different matrices in* $\text{GL}_n(q)$.

Proof. In the first column each of the n entries has q options. We exclude the zero column as it leads to a singular matrix. There are thus $q^n - 1$ options for the first column. For the second column there are again q^n options, except for the q multiples of the first column. Iterate this, for the $k+1$-th column there are q^n options, minus the vectors in the span of the first k columns. This span is of size q^k, providing $q^n - q^k$ options for the $k+1$-th column. □

We say that the order of a non-singular matrix $A \in \text{GL}_n(q)$ is the least number k for which $A^k = \mathbf{I}$. As a consequence, the inverse of the matrix A is A^{k-1}. This number k can not exceed $q^n - 1$, as the maximum order a matrix in $\text{GL}_n(q)$ can have is $q^n - 1$ [6]. When the order of a matrix $A \in \text{GL}_n(q)$ is known, the order of A^m for some natural number m is described in the following lemma. This lemma holds in more general; for numbers $a \in \mathbb{F}_q$ the order of a^m can be described by this lemma.

Lemma 2.2. *For any matrix* $A \in \text{GL}_n(q)$ *the order of* A^m *is exactly*

$$\text{Order}(A^m) = \frac{\text{Order}(A)}{\gcd(m, \text{Order}(A))}.$$

Proof. Let $\text{Order}(A) = k$ and $\text{Order}(A^m) = l$. Then it holds that $(A^m)^l = A^{ml} = \mathbf{I} = A^k$. From this equation it can be deduced that $ml \geq k$, otherwise ml would have been the order

of A. Moreover, ml is a multiple of k because otherwise $A^{ml} \neq \mathbf{I}$, leading to $k \mid ml$. Take $l = \frac{k}{\gcd(m,k)}$, then $k \mid ml$. This is moreover the least such l, concluding the argument. □

From this lemma it can be deduced that if the order of A is prime and $m < \text{Order}(A)$, then the order of A^m equals $\text{Order}(A)$. This can be deduced because the greatest common divisor of m and $\text{Order}(A)$ equals 1.

Definition 2.3. *The* span *of a matrix $A \in \text{GL}_n(q)$ is the set consisting of all possible terms $\sum_i a_i A^i$ or equivalently all matrices polynomial in A, i.e.*

$$\text{span}\langle A\rangle = \{f(A) \mid f \in \mathbb{F}_q[x]\}. \tag{2.1}$$

For a pair of matrices (A_1, A_2) we define the span to be

$$\text{span}\langle (A_1, A_2)\rangle = \left\{ \sum_i a_i (A_1^i, A_2^i) \mid a_i \in \mathbb{F}_q \right\}.$$

In the span sums are preserved. The subset of the span where we consider only multiplication is defined below.

Definition 2.4. *For a matrix $A \in \text{GL}_n(q)$ the subset of the span with only multiplication is the set*

$$\text{powers}\langle A\rangle = \{aA^i \mid a \in \mathbb{F}_q^*\}.$$

Equivalently to the span, we can define powers for a pair of matrices;

$$\text{powers}\langle (A_1, A_2)\rangle = \{a(A_1^i, A_2^i) \mid a \in \mathbb{F}_q^*\}.$$

The *characteristic polynomial* of a matrix $A \in \mathcal{M}_n(q)$ is defined as $\det(x\,\mathbf{I} - A)$, it is denoted $\Phi_A(x)$. The *minimal polynomial*, denoted $p_A(x)$, is the polynomial of least degree such that A vanishes. It divides the characteristic polynomial and has the exact same roots. The *eigenvalues* of a matrix $A \in \mathcal{M}_n(q)$ are the n roots of the characteristic polynomial $\Phi_A(x)$, denoted $\lambda_1, .., \lambda_n$. The characteristic polynomial $\Phi_A(x)$ might have double roots, corresponding to double eigenvalues. If these eigenvalues are counted double we say it is counted with multiplicity. For example, counted with multiplicity the characteristic polynomial of a matrix in $\text{GL}_n(q)$ has n roots.

For any $A \in \text{GL}_n(q)$ it holds that if λ is an eigenvalue of A then λ^n is an eigenvalue of A^n. Consequently, for any $A \in \text{GL}_n(q)$ if A has order r then all eigenvalues λ have $\lambda^r = 1$ and thus have an order that divides r. If r is prime then all eigenvalues have order r. A number is called an r-roots of unity if it has order r, there are r such numbers.

Lemma 2.5. *Given $\omega \neq 1$ an r-root of unity, with r prime, then the field $\mathbb{F}_q(\omega)$ contains all r-roots of unity.*

Proof. According to Lemma 2.2 for all a the order of ω^a is $\frac{\text{Order}(\omega)}{\gcd(a,\text{Order}(\omega))} = \frac{r}{\gcd(a,r)}$. If r is prime, then all $a < r$ are coprime with r. Thus, all $\omega, \omega^2, ..., \omega^{r-1}, \omega^r = 1 \in \mathbb{F}_q(\omega)$ have order r and are r-roots of unity. As these are r roots, these are all r-roots of unity. The field $\mathbb{F}_q(\omega)$ contains all r-roots of unity as $\omega \in \mathbb{F}_q(\omega)$ and the field is closed under multiplication. □

Throughout this thesis we will use matrices of prime order r, all eigenvalues have order r and all eigenvalues are in the same extension field as shown in Lemma 2.5. The size of this a field extension can be expressed as is done in Corollary 2.6.

Corollary 2.6. *The degree d of the smallest extension field $\mathbb{F}_q(\omega)$ containing all r-roots of unity is the least d such that $r \mid q^d - 1$.*

Proof. Let the extension field $\mathbb{F}_q(\omega)$ be isomorphic to $\mathbb{F}_{q^d}$. By definition $\omega^{q^d-1} = 1 \mod q^d$ and $\omega^r = 1$ by assumption, which implies $r \mid q^d - 1$. The degree of the smallest field extension is the least d for which it holds that $r \mid q^d - 1$. □

2.2 Normal forms and invariant factors

During this section we will work over the polynomial ring $\mathbb{F}[x]$. Definitions and theorems in this section are adapted from "The Theory of Matrices" [10], unless stated otherwise.

The Smith's normal form is a standard form for matrices defined over $\mathbb{F}_q[x]$. Each matrix is equivalent to a unique Smith normal form, so to introduce the subject of normal forms we introduce the notion of equivalence.

Definition 2.7. *A matrix A over $\mathbb{F}_q[x]$ is defined to be* equivalent *to matrix S over $\mathbb{F}_q[x]$ if there exist two non-singular matrices $P, Q \in \mathrm{GL}_n(q)$ such that $S = PAQ$.*

Theorem 2.8. *Every matrix $x\,\mathbf{I} - A$ over $\mathbb{F}_q[x]$ of rank r is equivalent to a diagonal matrix*

$$S = \begin{pmatrix} f_1 & 0 & \cdots & 0 & \dots & 0 \\ 0 & f_2 & \cdots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \\ 0 & 0 & \dots & f_r & \dots & 0 \\ \vdots & . & . & . & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{2.2}$$

where each f_i divides f_{i+1}. This is called Smith's normal form.

Note that the matrix S of the previous theorem can be established by elementary row operations on $x\,\mathbf{I} - A$. In particular, the determinant of the Smith normal form is a scalar multiple of the determinant of the original matrix. We can scale the matrix S to have the same determinant as $x\,\mathbf{I} - A$.

Definition 2.9. *An* i-minor *of a matrix $A \in \mathcal{M}_n(q)$ or $A \in \mathcal{M}_n(q)[x]$ with $i < n$ is the determinant of a submatrix of A consisting of i rows and i columns.*

Definition 2.10. *For any $A \in \mathcal{M}_n(q)$ let d_i be the greatest common divisor of all the i minors of the matrix $x\,\mathbf{I} - A$. The* invariant factors *of A are defined as:*

$$f_1 = d_1,\ f_2 = \frac{d_2}{d_1},\ \ldots.,\ f_n = \frac{d_n}{d_{n-1}}$$

The invariant factors f_i are the factors that appear in the Smith normal form. They are defined up to a unit factor. In particular, they are thus preserved under equivalence.

Remark. The index of the invariant factors is important as f_{n-1} divides f_n and so on, i.e. $f_1 \mid ... \mid f_{n-1} \mid f_n$. We assume and respect this order during the thesis.

The invariant factors are strongly related to the characteristic and minimal polynomial. In fact, the invariant factor f_n is the minimal polynomial. The characteristic polynomial of a matrix is the product $f_1 \cdot ... \cdot f_n$ of its invariant factors.

Example 2.11. Let matrix $A \in \mathrm{GL}_3(7)$ be given by

$$A = \begin{pmatrix} 4 & 4 & 6 \\ 0 & 0 & 1 \\ 0 & 6 & 6 \end{pmatrix}.$$

The product of the invariant factors equals the characteristic polynomial and the last invariant factor equals the minimal polynomial. These relations can be used to calculate the invariant factors. The characteristic polynomial is $\Phi_A(x) = (x+3)^2(x+5)$. The minimal polynomial equals $(x+3)(x+5)$, since $(A+3\,\mathbf{I})(A+5\,\mathbf{I}) = 0$. The invariant factors are thus $f_1 = 1$, $f_2 = (x+3)$ and $f_3 = (x+3)(x+5)$.

With the invariant factors of a matrix, the Smith normal form can be formed.

Example 2.12. Revisit the matrix $A \in \mathrm{GL}_3(7)$ from Example 2.11. The invariant factors are 1, $(x+3)$ and $(x+3)(x+5)$. The matrix is non-singular and thus of full rank. The Smith normal form is

$$\mathrm{SNF}(x\,\mathbf{I} - A) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & (x+3) & 0 \\ 0 & 0 & (x+3)(x+5) \end{pmatrix}. \tag{2.3}$$

The invariant factors are defined up to a unit factor as stated before. In particular, they can be assumed to be monic polynomials. For any monic polynomial there exist a companion matrix.

Definition 2.13. *Given a monic and non-zero polynomial $f(x)$ of degree d of the form*

$$f(x) = x^d + \sum_{i=0}^{d-1} c_i x^i.$$

Define the companion matrix C_f *of $f(x)$ as*

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{d-1} \end{pmatrix}.$$

For the definition of the companion matrix we followed [10], as this shape is commonly used, for example in Magma. Some authors define the companion as the transpose of the matrix described above, this is done in [16]. We do however follow [16] in the definition of the Frobenius normal form. If the transpose of the companion matrices is used, the Frobenius normal form is transposed as well.

Definition 2.14. *The* Frobenius normal form F *of a matrix* $A \in \mathrm{GL}_n(q)$ *is the block diagonal matrix in Equation* (2.4) *where each block* C_{f_i} *is the companion matrix of the invariant factor* f_i *of* A *with* $\deg(f_i) \geq 1$. *The other entries of the matrix are zero.*

$$F = \begin{pmatrix} C_{f_{n-l}} & & & & \\ & \ddots & & & \\ & & C_{f_{n-2}} & & \\ & & & C_{f_{n-1}} & \\ & & & & C_{f_n} \end{pmatrix}. \tag{2.4}$$

The invariant factor f_{n-l} *is the least invariant factor for which* $\deg(f_{n-l}) > 0$.

It is well known that any matrix can be transformed into its Frobenius normal form through left and right multiplication by a non-singular matrix P and its inverse P^{-1}, which is stated in [16].

Theorem 2.15. *For any matrix* $A \in \mathcal{M}_n(q)$ *there exists a matrix* $P \in \mathrm{GL}_n(q)$ *such that* PAP^{-1} *is the Frobenius normal form of the matrix* A.

Example 2.16. Revisit matrix $A \in \mathrm{GL}_3(7)$ from Example 2.11.

$$A = \begin{pmatrix} 4 & 4 & 6 \\ 0 & 0 & 1 \\ 0 & 6 & 6 \end{pmatrix}.$$

The invariant factors are 1, $(x+3)$ and $(x+3)(x+5)$. The trivial invariant factor 1 is not used in the Frobenius normal form. The invariant factors $x+3$ and $(x+3)(x+5) = x^2+x+1$ have the following companion matrices

$$C_{x+3} = \begin{pmatrix} 4 \end{pmatrix} \qquad\qquad C_{x^2+x+1} = \begin{pmatrix} 0 & 1 \\ 6 & 6 \end{pmatrix}.$$

This gives the following Frobenius normal form

$$\mathrm{FNF}(A) = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 6 & 6 \end{pmatrix}.$$

2.3 Similar matrices

For two different matrices $A, B \in \mathcal{M}_n(q)$ the Smith and Frobenius normal form can be the same. This introduces the subject of similar matrices.

Definition 2.17. *Two matrices* $A, B \in \mathcal{M}_n(q)$ *are called similar, denoted* $A \sim B$, *if there exists* $P \in \mathrm{GL}_n(q)$ *such that* $PAP^{-1} = B$.

By Theorem 2.15 any matrix is similar to its Frobenius normal form. Consequently, two matrices can be defined similar if and only if they share the same Frobenius normal form. Theorem 2.18 is a standard result, and it states several properties that are preserved under similarity.

Theorem 2.18. *For any matrix $A \in \mathrm{GL}_n(q)$ the following properties are preserved by similarity.*

- *Rank;*
- *Characteristic polynomial, minimal polynomial, determinant, trace and the eigenvalues;*
- *The Frobenius and Smith normal form;*
- *Order.*

Proof. Let $L \in \mathrm{GL}_n(q)$ and form the matrix B similar to A by $B = LAL^{-1}$. The multiplication of matrix A with matrices L, L^{-1} of full rank does not change the rank. It holds that;

$$\mathrm{rnk}(B) = \mathrm{rnk}((L \cdot A) \cdot L^{-1}) = \mathrm{rnk}(L \cdot A) = \mathrm{rnk}(A).$$

The characteristic polynomial of A, denoted $\Phi_A(x)$, is $\det(x\,\mathbf{I} - A)$. Using the multiplication rules for determinants of [8, page 96] we can deduce that;

$$\begin{aligned}
\det(x\,\mathbf{I} - A) &= \det(L \cdot L^{-1}(x\,\mathbf{I} - A)) \\
&= \det(L) \cdot \det(L^{-1}) \cdot \det(x\,\mathbf{I} - A) \\
&= \det(L) \cdot \det(x\,\mathbf{I} - A) \cdot \det(L^{-1}) \\
&= \det(L \cdot (x\,\mathbf{I} - A) \cdot L^{-1}) \\
&= \det(x\,\mathbf{I} - L \cdot A \cdot L^{-1}) \\
&= \det(x\,\mathbf{I} - B).
\end{aligned}$$

Properties derived from the characteristic polynomial are preserved as well, i.e. determinant, trace, eigenvalues and the minimal polynomial. The Frobenius normal form is preserved as noted before. The Smith's normal form is invariant under equivalence and therefore also under similarity. For the order, assume $A^k = I$ then:

$$B^k = (L \cdot A \cdot L^{-1})^k = L \cdot A^k \cdot L^{-1} = L \cdot I \cdot L^{-1} = I.$$

This implies that the order of B divides the order of A. The same calculation can be done with A and B swapped. This implies that the order of both matrices is equal. □

Theorem 2.18 specifies which properties of a matrix are invariant under similarity. This is a one-way argument, meaning that two non-similar matrices could share such a property without being similar. However, the converse is true under certain additional assumptions, one of which is stated in the following theorem and proven in [12].

Theorem 2.19. *Given two matrices $A, B \in \mathcal{M}_n(q)$. If they have the same characteristic and minimal polynomial that coincide, $p_A = \Phi_A = \Phi_B = p_B$, then A and B are similar.*

Proof. The minimal and characteristic polynomial of A and B coincide with their characteristic polynomial, which implies that there is only one block in the Frobenius normal form. Moreover, this normal form is the same for both A and B. As such we can conclude that the matrices are similar. □

Example 2.20. It is important to note that the minimal and characteristic polynomial of two matrices might be the same while the matrices are not similar. Take matrices $A, B \in \mathrm{GL}_5(7)$ to be

$$A = \begin{pmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 3 & 0 & 6 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 5 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 3 & 0 & 6 \end{pmatrix}.$$

Both matrices have characteristic polynomial $(x+3)^4(x+2)$. The minimal polynomial of both is $(x+3)^2(x+2)$, but the matrices are not similar. Matrix A has the invariant factors

$$f_1 = f_2 = 1,\ f_3 = (x+3),\ f_4 = (x+3),\ \text{ and } f_5 = (x+3)^2(x+2).$$

The matrix B has the invariant factors

$$f_1 = f_2 = f_3 = 1,\ f_4 = (x+3)^2 \text{ and } f_5 = (x+3)^2(x+2).$$

The invariant factors are different, and thus the matrices are not similar.

Lemma 2.21. *For any matrix $A \in \mathrm{GL}_n(q)$ with order coprime to q it holds that the characteristic polynomial of A is the same as the characteristic polynomial of A^q.*

Proof. This lemma follows from the notion that the eigenvalues of A^q are the eigenvalues of A raised to the power q. The characteristic polynomial $\Phi_A(x)$ is defined over $\mathbb{F}_q$ thus the Frobenius map $x \mapsto x^q$ leaves the roots invariant if the order of the roots is coprime with q. If on the contrary, the order of A and q have a non-trivial common divisor, then $\mathrm{Order}(A^q)$ is different from $\mathrm{Order}(A)$ by Lemma 2.2. The matrices can thus not be similar. □

Theorem 2.22. *Given $A \in \mathrm{GL}_n(q)$ with order coprime to q and where all roots of the minimal polynomial have multiplicity 1. Then A is similar to A^q.*

Proof. Let A have Frobenius normal form F, i.e. $A = QFQ^{-1}$, then A is similar to A^q if and only if F is similar to F^q, as demonstrated by the following calculation:

$$A^q = (QFQ^{-1})^q = QF^qQ^{-1}.$$

Thus, it is only needed to prove this theorem for a matrix F in FNF form. The matrix F has blocks $C_{f_1}, ..., C_{f_m}$ for some $m \leq n$ and F^q has blocks $C^q_{f_1}, ..., C^q_{f_m}$. The assumption that all roots of the minimal polynomial have multiplicity 1 implies that all invariant factors have roots with multiplicity 1. This implies that for any block C_f the minimal and characteristic polynomial coincide. By Lemma 2.21, C_f has the same characteristic polynomial as C^q_f. This characteristic polynomial also coincides with the minimal polynomial by the same assumption that the roots have multiplicity 1. The matrix C_f is thus similar to C^q_f by Theorem 2.19. This leads to the existence of matrices $P_{f_1}, ..., P_{f_r}$ such that

$$P_{f_1}C_{f_1}P^{-1}_{f_1} \sim C^q_{f_1},\ ...,\ P_{f_r}C_{f_r}P^{-1}_{f_1} \sim C^q_{f_r}.$$

In particular this implies the existence of the diagonal block matrix P with blocks $P_{f_1}, ..., P_{f_r}$ which shows the similarity of F and F^q as $PFP^{-1} = F^q$. □

3 Matrix Code Equivalence problem

The aim of this thesis is to evaluate the complexity of the matrix code equivalence problem. Specifically when the codes posses non-trivial automorphism groups. The objective of this section is to provide background information and insight into this problem.

Any matrix code is equipped with the rank metric and an isometry between two codes preserves this metric. The group of all isometries is defined below:

Definition 3.1. *The* isometry group *for two matrix codes* $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ *is defined to be*

$$\mathrm{Iso}(\mathcal{C}, \mathcal{D}) = \{\mu = (L, R) \mid L \in \mathrm{GL}_n(q),\ R \in \mathrm{GL}_m(q),\ L\mathcal{C}R = \mathcal{D}\}.$$

If the isometry is one-sided with a trivial right side we denote the isometry with $\mu = (L, \mathbf{I})$.

Definition 3.2. *The* conductor group *for two matrix codes* $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ *is the group*

$$\mathbf{Cond}(\mathcal{C}, \mathcal{D}) = \{M \in \mathcal{M}_n(q) \mid M\mathcal{C} \subseteq \mathcal{D}\}.$$

If the matrix M is singular, then $M\mathcal{C} \subsetneq \mathcal{D}$ is a strict subset. Equality holds if and only if $M \in \mathrm{GL}_n(q)$. Write $\mathbf{Cond}(\mathcal{C})$ to denote the conductor group of a code on itself i.e. $\mathbf{Cond}(\mathcal{C}, \mathcal{C})$. This group is called the *endomorphism group.*

Recall that automorphisms are isomorphisms from a code to itself. Automorphisms can also be one-sided. We write $\mathrm{Aut}_{\mathrm{L}}(\mathcal{C})$ for the group of automorphisms of the form $(A, \mathbf{I})$, and similarly, $\mathrm{Aut}_{\mathrm{R}}(\mathcal{C})$ denotes the group of automorphisms with a non-trivial right side. To stress the trivial side, in $\mathrm{Aut}_{\mathrm{L}}(\mathcal{C})$ and $\mathrm{Aut}_{\mathrm{R}}(\mathcal{C})$ we refer to these as *one-sided automorphism group. Two-sided automorphism groups* have a non-trivial matrix on both the left and the right side.

The groups Iso(), **Cond**() and Aut() are closely related. By definition the automorphism group of a code equals the isometry group of the code onto itself, $\mathrm{Aut}(\mathcal{C}) = \mathrm{Iso}(\mathcal{C}, \mathcal{C})$. If the isometry between two codes is one-sided with a trivial right side, the group $\mathrm{Iso}(\mathcal{C}, \mathcal{D})$ equals the set $\{(L, \mathbf{I}) \mid L \in \mathbf{Cond}(\mathcal{C}, \mathcal{D}) \text{ and } L \in \mathrm{GL}_n(q)\}$. The correspondence of the automorphism group with the conductor group is then evident;

$$\mathrm{Aut}_{\mathrm{L}}(\mathcal{C}) = \mathbf{Cond}(\mathcal{C}) \cap \mathrm{GL}_n(q).$$

The open question addressed in this thesis concerns the complexity of the MCE problem when $\mathcal{C}$ and $\mathcal{D}$ have non-trivial automorphisms.

Problem 3. The *Matrix code equivalence problem with non-trivial automorphisms*;

Given two equivalent matrix codes $\mathcal{C}$ and $\mathcal{D}$ over $\mathbb{F}_q^{n \times m}$ with non-trivial automorphism groups;

Problem: find two matrices $L \in \mathrm{GL}_n(q)$ and $R \in \mathrm{GL}_m(q)$ such that $L\mathcal{C}R = \mathcal{D}$.

The aim of the thesis is to describe the complexity of Problem 3.

3.1 Approach of the problem

To solve the Matrix code equivalence problem for codes with non-trivial automorphisms we use the structure of the automorphism groups of the codes. Given two equivalent matrix codes the automorphism groups of both are related by the isometry.

Proposition 3.3. *Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$. Any automorphism $(A_1, A_2) \in \mathrm{Aut}(\mathcal{C})$ relates by $\mu = (L, R)$ to a unique pair $(B_1, B_2) \in \mathrm{Aut}(\mathcal{D})$ as follows:*

$$B_1 = L \cdot A_1 \cdot L^{-1} \text{ and } B_2 = R^{-1} \cdot A_2 \cdot R.$$

Proof. This can be seen by the diagram below. Note that on the left side, multiplication is done to the left, and on the right side to the right.

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{(A_1,A_2)} & \mathcal{C} \\ {\scriptstyle (L^{-1},R^{-1})}\uparrow & & \downarrow{\scriptstyle (L,R)} \\ \mathcal{D} & \xrightarrow[(B_1,B_2)]{} & \mathcal{D} \end{array}$$

□

Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$. The proposition proves that any automorphism $A = (A_1, A_2) \in \mathrm{Aut}(\mathcal{C})$ is similar to an automorphism $B = (B_1, B_2) \in \mathrm{Aut}(\mathcal{D})$. This correspondence reveals crucial information about the isometry. The automorphisms satisfy the following equations and (L, R) is a solution,

$$\begin{cases} XA_1 &= B_1X \\ A_2Y &= YB_2. \end{cases} \tag{3.1}$$

These equations are called Sylvester equations as Sylvester in [18] was the first to investigate matrix equations of this form. These equations are the basis of the algorithm presented in this thesis, which therefore is called the Sylvester algorithm.

Outline Sylvester algorithm. To perform the Sylvester algorithm, one must first identify similar automorphisms $(A_1, A_2) \in \mathrm{Aut}(\mathcal{C})$ and $(B_1, B_2) \in \mathrm{Aut}(\mathcal{D})$. Given these automorphisms the Sylvester equations $B_1X = XA_1$ is solved. The space of solutions to $B_1X = XA_1$ is denoted $\mathrm{SolSp}(B_1, A_1)$. As explained, the isometry is non-singular and a solution to the Sylvester equation. However, the solution space contains also singular matrices which will thus not give rise to an isometry. We therefore reduce the space $\mathrm{SolSp}(B_1, A_1)$ to a smaller space which contains exactly the non-singular matrices of $\mathrm{SolSp}(B_1, A_1)$. This smaller space is denoted $\mathrm{SolSpNon\text{-}Sing}(B_1, A_1)$.

At least one of the matrices in the reduced space $\mathrm{SolSpNon\text{-}Sing}(B_1, A_1)$ is an isometry. To find this isometry we preform a brute force attack. The brute force picks a random matrix $L \in \mathrm{SolSpNon\text{-}Sing}(B_1, A_1)$. With a polynomial MCRE solver, the brute force can check if $L\mathcal{C}$ is right equivalent to $\mathcal{D}$. If no equivalence is found, the process needs to be repeated with a different matrix L. The complexity of this brute force attack is estimated at the end. This brute force approach is the bottleneck of the algorithm, and it heavily depends

on the amount of isometries there are in SolSpNon-Sing(B_1, A_1) and of the size of the space SolSpNon-Sing(B_1, A_1).

Outline Sylvester algorithm in the thesis During this thesis the Sylvester algorithm is developed and explained. Each section is a new step in the algorithm, the outline is stated below.

- Section 4 finds similar automorphisms $(A_1, A_2) \in \mathrm{Aut}(\mathcal{C})$ and $(B_1, B_2) \in \mathrm{Aut}(\mathcal{D})$.
- Section 5 finds the solution space $\mathrm{SolSp}(B_1, A_1)$ to the equation $B_1 X = X A_1$.
- Section 6 reduces $\mathrm{SolSp}(B_1, A_1)$ to the smaller space SolSpNon-Sing(B_1, A_1).
- Section 7 estimates the complexity of preforming a brute force attack.
- Section 8 describes the Sylvester algorithm and analysis the algorithm.

During the Sylvester algorithm only information of the left side of the automorphisms is used to find the left side of an isometry. Information of the codes is used to find the corresponding right side of the isometry.

3.2 Automorphism group

This section aims to investigate properties of the automorphism group for a matrix code $\mathcal{C} \subseteq \mathcal{M}_{n,m}(q)$. The automorphism group is a subset of $\mathrm{GL}_n(q) \times \mathrm{GL}_m(q)$. It is closed under multiplication with scalars of $\mathbb{F}_q$ and the group action. For automorphisms (A_1, A_2) and (A_1', A_2') of code $\mathcal{C}$, define scalar multiplication $a \in \mathbb{F}_q^*$ and the group operation $\circ$ to be

$$a(A_1, A_2) \circ (A_1', A_2') = (aA_1 \cdot A_1', A_2' \cdot A_2).$$

With these definitions the automorphism group forms a group. It does not matter if scalar multiplication is done on the left or right side as it commutes with the matrices.

By definition of composition of automorphisms for any automorphism $(A_1, A_2) \in \mathrm{Aut}(\mathcal{C})$ it holds that powers$\langle (A_1, A_2) \rangle \in \mathrm{Aut}(\mathcal{C})$. On the contrary, span$\langle (A_1, A_2) \rangle$ is in general not preserved for the two-sided automorphisms as the following calculation illustrates:

$$\begin{aligned}(A_1 + A_1', A_2 + A_2')\mathbf{C} &= (A_1 + A_1')\mathbf{C}(A_2 + A_2') \\ &= (A_1 + A_1')(\mathbf{C}A_2 + \mathbf{C}A_2') \\ &= A_1\mathbf{C}A_2 + A_1\mathbf{C}A_2' + A_1'\mathbf{C}A_2 + A_1'\mathbf{C}A_2'.\end{aligned}$$

The linear structure of $\mathcal{C}$ assures that the term $A_1\mathbf{C}A_2 + A_1'\mathbf{C}A_2'$ is in $\mathcal{C}$. The mixed terms $A_1\mathbf{C}A_2' + A_1'\mathbf{C}A_2$ however do not need to be preserved in the code. In general the two-sided automorphism group is thus not closed under addition. For one-sided automorphisms, addition is preserved in the conductor group.

Lemma 3.4. *For any $\mathcal{C} \subseteq \mathcal{M}_{n,m}(q)$ and $A \in \mathbf{Cond}(\mathcal{C})$ it holds that* span$\langle A \rangle \subseteq \mathbf{Cond}(\mathcal{C})$.

Proof. We need to prove that $\sum_i a_i(A^i, Id)$ is in $\mathbf{Cond}(\mathcal{C})$. It is clear that $a_i(A^i, \mathbf{I})$ is in $\mathbf{Cond}(\mathcal{C})$ by the argument that multiplication is preserved in automorphism group. To proof

that addition is preserved in the conductor group, take any $\mathbf{C} \in \mathcal{C}$. For any two matrices $A, A' \in \mathbf{Cond}(\mathcal{C})$ the sum of both is in the conductor group as the calculation illustrates;

$$\begin{aligned}(A + A', \mathbf{I})\mathbf{C} &= (A + A')\mathbf{C}\,\mathbf{I} \\ &= A\mathbf{C}\,\mathbf{I} + A'\mathbf{C}\,\mathbf{I}\,.\end{aligned}$$

Both automorphisms A, A' are in the left-sided automorphism group, thus both $A\mathbf{C}$ and $A'\mathbf{C}$ are in $\mathcal{C}$. The sum of both is in $\mathcal{C}$ by its linear structure. □

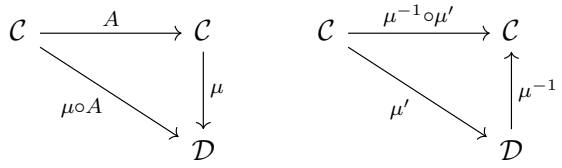
It is important to stress that non-singular elements of the conductor group are in the left one-sided automorphism group. This implies that for any two matrices $A, A' \in \mathbf{Cond}(\mathcal{C})$ it holds that if $(A + A')$ is non-singular, then this sum is in $\mathrm{Aut}_{\mathrm{L}}(\mathcal{C})$.

Given $\mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ and let $\mathcal{C}$ and $\mathcal{D}$ be two equivalent matrix codes. The automorphisms of $\mathcal{C}$ are strongly related to the automorphisms of $\mathcal{D}$ by the isometry $\mu\colon \mathcal{C} \to \mathcal{D}$ as noted in Proposition 3.3. This relation is two-sided; the isometry group $\mathrm{Iso}(\mathcal{C}, \mathcal{D})$ can also be described with use of the automorphisms of $\mathcal{C}$ as the following corollary explains.

Corollary 3.5. *Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$. If $\mathrm{Iso}(\mathcal{C}, \mathcal{D})$ is non-empty then $\#\mathrm{Aut}(\mathcal{D}) = \#\mathrm{Aut}(\mathcal{C}) = \#\mathrm{Iso}(\mathcal{C}, \mathcal{D})$ and the isometry group is:*

$$\mathrm{Iso}(\mathcal{C}, \mathcal{D}) = \{\mu \circ A \mid A \in \mathrm{Aut}(\mathcal{C})\}. \tag{3.2}$$

Proof. For any isomorphism μ it holds that $\mu \circ A$ is an isomorphism as can be seen in the diagram below. Similarly, given two isomorphisms the composition of both, $\mu^{-1} \circ \mu'$, gives an automorphism on $\mathcal{C}$.



From the structure of the isomorphism group it follows that the size of the automorphism groups is equal to the size of the isomorphism group. □

4 Algorithm to find similar automorphisms

Context - This thesis investigates the complexity of the MCE problem given that the codes have non-trivial automorphisms. To make use of the structure of the automorphisms, it is needed to find non-trivial similar automorphisms.

Goal - The goal of this section is to prove how similar automorphisms of two codes can be found given non-trivial automorphisms of both codes. This section thus aims solve the following problem.

Problem 4. Finding similar matrices;

Input: $A = (A_1, A_2)$ and $B = (B_1, B_2)$, two pairs of matrices where A_1 and B_1 are non-trivial, i.e. $A_1 \neq \mathbf{I} \neq B_1$, but A_2 and B_2 could be trivial;

Problem: find $A' = (A'_1, A'_2)$ and $B' = (B'_1, B'_2)$ with $A' \in \text{powers}\langle A \rangle$, $B' \in \text{powers}\langle B \rangle$, A' similar to B' and A'_1 prime order.

Given two matrices A, B Problem 4 finds similar matrices in the sets $\text{powers}\langle A \rangle$ and $\text{powers}\langle B \rangle$ as all matrices in these sets are in the automorphism group.

Motivation - Assume that the codes have non-trivial one-sided automorphisms. An automorphism of a code is an isometry from a code to itself. To find a one-sided automorphism intuitively a MCRE solver can be used with as input two times the same code.

One should require that the output of this solver is a non-trivial automorphism. This can be done by running the MCRE solver of [5] with input two times the same code described with a different basis. The algebraic algorithm for the MCE problem of [2] can also be used. This gives in fact all one-sided automorphisms.

For two-sided automorphisms however the reduction to the MCE problem does not help as we are trying to solve this problem. This thesis does not investigate if there exists a more sophisticated way to find two-sided automorphisms and assumes a two-sided automorphism is given before preforming the Sylvester algorithm.

The Sylvester algorithm presented in this thesis can be used with two and one-sided automorphisms. We will thus always write the automorphism as (A_1, A_2) where A_1 is assumed to be non-trivial. It will be clearly indicated where the algorithm differs for one-sided and two-sided automorphisms.

Proposition 4.1. *Problem 4 can be solved in time* $\mathcal{O}\left(n \cdot \text{Order}(B_1) + qn^3\right)$ *by Algorithm 1. Assuming that* $\text{Order}(A_1) \leq \text{Order}(B_1)$

Proof. The order of a matrix is the least common multiple of the order of its eigenvalues. Computing the order of the matrix can thus be done by computing the order of its eigenvalues. The eigenvalues can be found with the characteristic polynomial. The time complexity of finding the eigenvalues is $\mathcal{O}(M(n))$ as proven by Strassen. Finding the order of an eigenvalue λ can be done by brute forcing all powers until the order is found. This results thus in $\text{Order}(\lambda)$ multiplications. Note that this order might exceed $q-1$ if λ is not defined over $\mathbb{F}_q$. This needs to be repeated for all eigenvalues of both matrices. The time complexity is thus at most $\mathcal{O}(n \cdot \max\{\text{Order}(\lambda_1), .., \text{Order}(\lambda_n)\})$. Which has as upper-bound $\mathcal{O}(n \cdot \text{Order}(B_1))$.

Algorithm 1 Finding Similar Matrices

Input Two pairs of matrices (A_1, A_2), (B_1, B_2) in $\mathrm{GL}_n(q) \times \mathrm{PGL}_m(q)$.

Output If they exist, two pairs of matrices $M = (M_1, M_2) \in \text{powers}\langle(A_1, A_2)\rangle$ and $N = (N_1, N_2) \in \text{powers}\langle(B_1, B_2)\rangle$ such that $M \sim N$ and M_1 of prime power.

```
Order(A_1)                                                    ▷ O(n · Order(A_1))
Order(B_1)                                                    ▷ O(n · Order(B_1))
r_1, r_2, ..., r_l ← PrimeFactorization(Order(A_1))
r_1, r_2, ..., r_l' ← PrimeFactorization(Order(B_1)).
r := max{{r_1, r_2, ..., r_l} ∩ {r_1, r_2, ..., r_l'}}
M := A_1^{Order(A_1)/r}                                       ▷ O(M(n) log(Order(A_1)/r))
N := B_1^{Order(B_1)/r}                                       ▷ O(M(n) log(Order(B_1)/r))
m := min{r, q}.
for i in [1..m] do
    if FNF(M^i) equals FNF(N) then                            ▷ O(n^3)
        return (M^i, A_2^{i·Order(A_1)/r}), (N, B_2^{Order(B_1)/r})   ▷ O(M(n) log(Order(B_1)/r)
    end if
end for
return ⊥
```

On a quantum computer the factorization of $\mathrm{Order}(A_1)$ and $\mathrm{Order}(B_1)$ can be done efficiently with Shor's algorithm.

The maximum prime order of a matrix in $\text{powers}\langle A_1\rangle$ and $\text{powers}\langle B_1\rangle$ is r with

$$r := \max\left(\text{PrimeFactorization}(\mathrm{Order}(A_1)) \cap \text{PrimeFactorization}(\mathrm{Order}(B_1))\right).$$

The order of M and N is r by Lemma 2.2. For any matrix M of prime order r it holds that $M^2, .., M^{r-1}$ have order r. For all these matrices it needs to be checked if they are similar to N. The complexity of checking similarity is the complexity of finding the Frobenius normal form for M^i and comparing it to the Frobenius normal form of N. Finding the Frobenius normal form can be done in $\mathcal{O}\left(n^3\right)$ as proven in [16].

Lemma 6.9 states that all invariant factors of a matrix of prime order have roots with multiplicity 1. The matrix M^i is thus similar to M^{iq} by Theorem 2.22. The iteration thus finds a matrix M^i similar to N within q steps if it exists.

If none of the matrices $M, M^2, .., M^{q-1}$ are similar to N, then it is impossible to find similar matrices in $\text{powers}\langle(A_1, A_2)\rangle$ and $\text{powers}\langle(B_1, B_2)\rangle$. Namely, for each matrix A similar to B it holds that $A^i \sim B^i$ as $A = QBQ^{-1}$ implies $A^i = QB^iQ^{-1}$. If none of the matrices of $\text{powers}\langle M\rangle$ are similar to N an error is returned. Otherwise, the returned matrices are in the sets $\text{powers}\langle(A_1, A_2)\rangle$ and $\text{powers}\langle(B_1, B_2)\rangle$ as required. The overall complexity reads

$$\mathcal{O}\left(n \cdot \mathrm{Order}(B_1) + qn^3\right).$$

□

If Algorithm 1 has the right input, similar matrices will be returned. We will be preforming the algorithm with similar matrices. The question arises in which cases the returned similar automorphisms are related by an isometry.

Theorem 4.2. *Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ with isometry μ. Let $A = (A_1, A_2)$ in $\mathrm{Aut}(\mathcal{C})$ be similar to $B = (B_1, B_2) \in \mathrm{Aut}(\mathcal{D})$ by μ and let them both be similar to automorphism $B' = (B'_1, B'_2)$ in $\mathrm{Aut}(\mathcal{D})$. There always exists an isometry μ' such that $\mu'(A) = B'$ if and only if there exists $B'' \in \mathrm{Aut}(\mathcal{D})$ such that $B' = B'' \circ B$.*

Proof. This follows from Corollary 3.5. If there exists an isometry $\mu'(A) = B'$ and $\mu(A) = B$, then $B'' = \mu' \circ \mu^{-1}$ is an automorphism of $\mathcal{D}$. Moreover, $B'' \circ B = \mu' \circ \mu^{-1} \circ \mu(A) = \mu'(A) = B'$. To prove the statement the other way around, assume there is an isometry μ such that $\mu(A) = B$ and $B' = B'' \circ B$, then $B' = B'' \circ \mu(A)$. The isometry $\mu' = B'' \circ \mu$ thus relates the automorphisms A and B'. □

As a corollary it follows that it is unimportant whether the original isometry maps A to B or to B^q. This because $B^q = B^{q-1} \circ B$ and B^{q-1} is an automorphism as required. Algorithm 1 thus outputs two matrices that are similar by an isometry if the original isometry maps the automorphisms from powers$\langle A \rangle$ to powers$\langle B \rangle$.

We assume it to be unlikely that any $A \in \mathrm{Aut}(\mathcal{C})$ is similar to several automorphisms $B, B' \in \mathrm{Aut}(\mathcal{D})$ and that B and B' do not relate by an automorphism B''. We thus assume that any pair of similar matrices gives rise to an isometry.

Theorem 4.3. *Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$. Given non-trivial automorphisms $A = (A_1, A_2) \in \mathrm{Aut}(\mathcal{C})$ and $B = (B_1, B_2) \in \mathrm{Aut}(\mathcal{D})$. There exists an algorithm working in time $\mathcal{O}\left(n \cdot \mathrm{Order}(B_1) + qn^3\right)$ that finds $A' = (A_1, A_2) \in \mathrm{Aut}(\mathcal{C})$ and $B' = (B_1, B_2) \in \mathrm{Aut}(\mathcal{D})$ and assures that A' and B' are similar, are mapped by an isometry and both A'_1 and B'_1 have prime order.*

Proof. Proposition 4.1 finds two similar matrices in time complexity $\mathcal{O}\left(n \cdot \mathrm{Order}(B_1) + qn^3\right)$. If the algorithm succeeds it can be assumed that these are linked by an isometry by Theorem 4.2 and the remark afterwards. If the algorithm fails, other automorphisms should be provided. □

Theorem 4.4. *Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ with non-trivial one-sided automorphism groups. There exists an algorithm with time complexity $\mathcal{O}\left(n \cdot \mathrm{Order}(B) + qn^3\right)$ that finds $A' \in \mathrm{Aut}_{\mathrm{L}}(\mathcal{C})$ and $B' \in \mathrm{Aut}_{\mathrm{L}}(\mathcal{D})$ and assures that A' and B' are similar, are mapped by an isometry and both have prime order. Here B is an automorphism in $\mathrm{Aut}_{\mathrm{L}}(\mathcal{D})$ found in the first step of the algorithm.*

Proof. As noted before a non-trivial one-sided automorphism A of $\mathcal{C}$ and $B = (B_1, B_2)$ for $\mathcal{D}$ can be found in polynomial time. Use Algorithm 1 to find similar matrices. This can be done in time $\mathcal{O}\left(n \cdot \mathrm{Order}(B_1) + qn^3\right)$ by Proposition 4.1. If the one-sided automorphism groups are spanned by one matrix the algorithm terminates with similar matrices. If $\mathrm{Aut}_{\mathrm{L}}(\mathcal{C})$ is spanned by several automorphisms this procedure needs to be repeated with another input. □

5 The solution space of the Sylvester equation

Context - Recall the Sylvester algorithm we preform to find the equivalence between two matrix codes. At first, we find automorphisms of both codes that are similar, this is done in the previous section. From these similar automorphisms we form a Sylvester equation. One of the solutions of the Sylvester equation is the isometry. This section thus aims to investigate the structure of the solution space for two automorphisms.

Approach - The automorphisms are assumed to be similar, thus in particular we are interested in the solution space of the Sylvester equation for similar matrices. The main result of this section is Theorem 5.6.

Theorem 5.6. *For similar matrices $B \in \mathrm{GL}_n(q)$ and $A \in \mathrm{GL}_n(q)$ the solution space $\mathrm{SolSp}(B, A)$ of $BX = XA$ can be found in polynomial time $\mathcal{O}\left(\dim(\mathrm{SolSp}(B, A)) \cdot n \cdot M(n)\right)$. The solution space is $\mathrm{SolSp}(B, A) = \{LA' \mid A'A = AA'\}$ for some solution L and all matrices A' commuting with A. The space $\mathrm{SolSp}(B, A)$ has dimension of size*

$$\sum_{i=1}^{n} (2(n-i)+1) \cdot \deg(f_i),$$

for f_i the invariant factors of A.

Outline section - To prove Theorem 5.6, Section 5.1 states the size of the solution space for the Sylvester equation with arbitrary input. This section moreover looks into the size of the solution space for similar matrices. Section 5.2 investigates the structure of the solution space to the Sylvester equation.

5.1 Sylvester's equation

This section aims to find the number of solutions to the Sylvester equation, Equation (5.1)

$$BX = XA \tag{5.1}$$

for any two matrices $A, B \in \mathcal{M}_n(q)$. This number is described by Cecioni and Frobenius and depends on the invariant factors of the matrices. We cite the statement without proof, but a proof can be found in [10, Thm. 46.2].

Theorem 5.1 (Cecioni and Frobenius)**.** *For two matrices $A, B \in \mathcal{M}_n(q)$ the number of linearly independent solutions of the equation $BX = XA$ is $\sum_{i,j}^{n} \gcd(f_i, g_j)$ where f_i ranges over the invariant factors of A and g_j over the invariant factors of B.*

The invariant factors for similar matrices A and B are the same. The indexation of the invariant factors respects the order of division. This gives the formula in Theorem 5.1 a particular form, as described in Corollary 5.2.

Corollary 5.2. *Given similar matrices $A, B \in \mathrm{GL}_n(q)$, and let the f_i be the invariant factors of A. Then the number of linearly independent solutions of the equation $BX = XA$ is*

$$\sum_{i=1}^{n} (2(n-i)+1) \cdot \deg(f_i).$$

Proof. The invariant factors g_i of B are the exact same as the invariant factors of A, which implies that $\gcd(f_i, g_j)$ is the same as $\gcd(f_i, f_j)$. The indexation of the invariant factors respects division, i.e. $f_i \mid f_j$ for $i \leq j$ implying $\gcd(f_i, f_j) = f_i$. Write the Cecioni and Frobenius equation as:

$$\sum_{i,j=1}^{n} \gcd(f_i, f_j) = \sum_{i=1}^{n}\sum_{j>i}^{n} \gcd(f_i, f_j) + \sum_{i=1}^{n}\sum_{j<i}^{n} \gcd(f_i, f_j) + \sum_{i=1}^{n}\sum_{j=i}^{n} \gcd(f_i, f_j)$$

By symmetry $\sum_{i=1}^{n}\sum_{j>i}^{n} \deg(f_i) = \sum_{i=1}^{n}\sum_{j<i}^{n} \deg(f_j)$ thus conclude

$$\sum_{i,j=1}^{n} \gcd(f_i, f_j) = 2\sum_{i=1}^{n}\sum_{j>i}^{n} \deg(f_i) + \sum_{i=1}^{n} \deg(f_i).$$

The term $\deg(f_i)$ appears $n - i$ times in the first sum, plus 1 time in the second sum. This gives the desired result of $\sum_{i=1}^{n}(2(n-i)+1) \cdot \deg(f_i)$. □

The formula of Corollary 5.2 can in particular be used to count the solutions of $AX = XA$, as a matrix is always similar to itself. This is the number of matrices that commute with A and is known. The number of matrices that commute with a given matrix is described by Frobenius, as documented in [8, Theorem 3.16]. The formulation and formula of this theorem is slightly different from ours, but equivalent.

The solution space of $BX = XA$ is the smallest when the characteristic polynomial coincides with the minimal polynomial of A. This however is an exceptional case and does not hold in general. In general there would be more invariant factors leading to more solutions to $BX = XA$.

Corollary 5.3. *If for any $A \in \mathrm{GL}_n(q)$ the minimal polynomial equals the characteristic polynomial and A is similar to $B \in \mathrm{GL}_n(q)$, then there are q^n solutions to $BX = XA$.*

Proof. There is one non-constant invariant factor f_n of degree n. Using Corollary 5.2 one can prove that the number of linear independent solutions is therefore $(2(n-n)+1) \cdot n = n$. Name these solutions $X_1, .., X_n$. To form linear dependent solutions, sums can be taken as the solution space is closed under addition. The linear dependent solutions are of the form $a_1X_1 + .. + a_nX_n$ for $a_i \in \mathbb{F}_q$. For each a_i there are q options, giving a total of q^n solutions. □

Example 5.4. Consider the similar matrices $A, B \in \mathrm{GL}_3(7)$ given by:

$$A = \begin{pmatrix} 4 & 4 & 6 \\ 0 & 0 & 1 \\ 0 & 6 & 6 \end{pmatrix} \qquad B = \begin{pmatrix} 4 & 0 & 0 \\ 1 & 1 & 5 \\ 3 & 5 & 5 \end{pmatrix}. \tag{5.2}$$

The invariant factors of A are $f_1 = 1$, $f_2 = (x+3)$ and $f_3 = (x+3)(x+5)$ by Example 2.11. The matrices are similar, so the invariant factors of B are the same. By Corollary 5.2 the number of linear independent solutions for $BX = XA$ is $\sum_{i=1}^{n}(2(n-i)+1) \cdot \deg(f_i)$.

$$\begin{aligned}\sum_{i=1}^{3}(2(3-i)+1) \cdot \deg(f_i) &= 5 \cdot \deg(1) + 3 \cdot \deg(x+3) + \deg(x^2+x+1) \\ &= 5 \cdot 0 + 3 \cdot 1 + 2 = 5\end{aligned}$$

There are thus 5 linear independent solutions, hence $7^5 = 16807$ solutions to $BX = XA$.

5.2 Structure of the solution space

The number of solutions to the Sylvester equation is described in the previous section. This section investigates the structure of the solution space.

For two matrices $A, B \in \mathrm{GL}_n(q)$, the solution space of $BX = XA$ is denoted $\mathrm{SolSp}(B, A)$. $\mathrm{SolSp}(B, A)$ exhibits a clear structure; given one solution, all other solutions can be described using this initial solution and all matrices that commute with A, as expressed in Lemma 5.5.

Lemma 5.5. *Given two matrices $A, B \in \mathrm{GL}_n(q)$ and L be any non-singular solution to $BX = XA$, then all solutions are LA' for $A' \in \mathcal{M}_n(q)$ commuting with A.*

Proof. Let L be a solution to $BX = XA$. Consider the matrices commuting with A, i.e. solutions to $AX = XA$. Multiply both sides with L results in $LAX = LXA$ which equals $BLX = LXA$ because L satisfies $BL = LA$. Therefore, LX is a solution to $BX = XA$.

$$\mathrm{SolSp}(B, A) \supseteq \{LA' \mid A'A = AA'\}.$$

No other solution exists as both sides have the same size. The number of solutions to $BX = XA$ and $AX = XA$ is the same as the number of solutions to both equations depend on the invariant factors of A. □

The space $\mathrm{SolSp}(B, A)$ can be considered as a matrix code as it is closed under addition and scalar multiplication. This lemma relates the matrix code $\mathrm{SolSp}(B, A)$ to the matrix code $\mathrm{SolSp}(A, A)$ by a left equivalence. This left equivalence can be any element of $\mathrm{SolSp}(B, A)$ which also follows from the lemma. That implies that if one uses a matrix code left equivalence solver on the codes $\mathrm{SolSp}(B, A)$ and $\mathrm{SolSp}(A, A)$ the set $\mathrm{SolSp}(B, A)$ will be returned.

The main result of this section is stated in the following theorem.

Theorem 5.6. *For similar matrices $B \in \mathrm{GL}_n(q)$ and $A \in \mathrm{GL}_n(q)$ the solution space $\mathrm{SolSp}(B, A)$ of $BX = XA$ can be found in polynomial time $\mathcal{O}(\dim(\mathrm{SolSp}(B, A)) \cdot n \cdot M(n))$. The solution space is $\mathrm{SolSp}(B, A) = \{LA' \mid A'A = AA'\}$ for some solution L and all matrices A' commuting with A. The space $\mathrm{SolSp}(B, A)$ has dimension of size*

$$\sum_{i=1}^{n} (2(n-i)+1) \cdot \deg(f_i),$$

for f_i the invariant factors of A.

Proof. There are $\dim(\mathrm{SolSp}(B, A)) = \sum_{i=1}^{n} (2(n-i)+1) \cdot \deg(f_i)$ linear independent solutions to the equation $BX = XA$, proven in Corollary 5.2. Write this dimension to be m. If m values of X are fixed the other values are uniquely determinable by solving the equation.

The equation $BX = XA$ can be solved by solving $Bx_i = a_i$ for all column vectors x_i of X and a_i of A. Solving $Bx_i = a_i$ is of time complexity $\mathcal{O}(M(n))$ [1, Theorem 6.7]. This needs to be repeated for all n column vectors to find matrix X.

To find a basis of $\dim(\mathrm{SolSp}(B, A))$, m linear independent solutions should be found. This can be done by taking X_i to have m zero's on the first m entries except one 1 on the i-th entry. The other entries of the matrix are variables and can be found by solving the equation. Solving $BX_i = X_iA$ for m matrices X_i leads to an overall complexity of $\mathcal{O}(\dim(\mathrm{SolSp}(B, A)) \cdot n \cdot M(n))$.

The space $\mathrm{SolSp}(B, A)$ equals $\{LA' \mid A'A = AA'\}$ as shown by Lemma 5.5. □

6 Reduction of the solution space

Context - Recall the Sylvester algorithm that we preform for two equivalent matrix codes with non-trivial automorphism groups. We found similar automorphisms of the codes in Section 4. For these automorphisms we found the Sylvester equation and solved it in the previous section. In the solution space of this Sylvester equation we want to find the isometry. The isometry is non-singular and thus in particular we are interested in the number of non-singular solutions to the Sylvester equation. This section aims to find this number.

Approach - Theorem 5.6 states that the solution space for two different similar matrices is left equivalent to the matrices commuting with one of them. In particular, the number of non-singular solutions of both sets is thus equal. The number of non-singular matrices commuting with a given matrix is known, we evaluate this in Section 6.1.

Outline section - Section 6.1 gives the number of non-singular matrices commuting with a given matrix. For the Sylvester attack however we assume that the order of the matrices in the Sylvester equation is prime. Section 6.2 therefore evaluates the number of non-singular matrices commuting with a given matrix of prime order r for r not equal to the characteristic of the field. In the particular case that the matrices of the Sylvester equation have prime order equal to the characteristic of the field, the number of non-singular matrices commuting with A is investigated in Section 6.3.

6.1 The number of non-singular matrices commuting with a given matrix

Stanley [15] investigated the number of non-singular matrices that commute with a given matrix. This section presents this number, the preliminaries needed for it and some examples. The definitions of this section are adapted from [15].

Definition 6.1. *A partition of any natural number is an ordered set $\lambda = \{\lambda_1, \lambda_2, ...\}$ such that it holds that $\lambda_1 \geq \lambda_2 \geq \cdots \geq 0$. The natural number is the sum $\sum_i \lambda_i$ denoted with $|\lambda|$.*

Definition 6.2. *For any partition λ the conjugate partition is denoted λ'. The value λ'_i of λ' is the number of elements of λ that have value at least i.*

Example 6.3. A partition of 9 could be $\{4, 2, 1, 1, 1\}$ the conjugate partition is $\{5, 2, 1, 1\}$.

Theorem 6.4 is stated without proof. The proof can be found in [15, Theorem 1.10.7].

Theorem 6.4. *Given a matrix $A \in \mathrm{GL}_n(q)$ with characteristic polynomial $\Phi_A(x)$. Assume $\Phi_A(x)$ has one irreducible factor $f(x)$ of degree d and multiplicity $|\lambda|$. Let the partition λ describe the partition of the non-constant invariant factors, i.e. $f_n = f(x)^{\lambda_1}$, $f_{n-1} = f(x)^{\lambda_2}$, $...f_1 = f(x)^{\lambda_k}$. Let λ' be the conjugate partition of λ, let b_i be the number of parts of λ of size i, or equivalently $\lambda'_i - \lambda'_{i+1}$. Let $s_i = \lambda'_1 + ... + \lambda'_i$. Then the number of non-singular matrices, denoted $c_d(\lambda)$, that commute with A of size $n = d|\lambda|$ is*

$$c_d(\lambda) = \prod_{i \geq 1} \prod_{j=1}^{b_i} \left(q^{ds_i} - q^{(s_i - j)d} \right). \tag{6.1}$$

Any matrix $A \in \mathrm{GL}_n(q)$ in block-diagonal form commutes with a matrix B in block-diagonal form if and only if the blocks are of the same size and the blocks commute individually. This motivates the generalization of Theorem 6.4, the proof can be found in the proof of Theorem 1.10 in [15].

Theorem 6.5. *Take any matrix $A \in \mathrm{GL}_n(q)$. Denote with λ_f the partition in which the irreducible polynomial f appears in the invariant factors of A. The number of matrices commuting with A is*

$$\prod_{f \text{ irreducible}} c_d(\lambda_f). \tag{6.2}$$

Following the notation of Theorem 6.4 this is the same as

$$\prod_{f \text{ irreducible}} \prod_{i \geq 1} \prod_{j=1}^{b_i} \left(q^{ds_i} - q^{(s_i - j)d} \right). \tag{6.3}$$

Where s_i, b_i and d depend on the irreducible polynomial f as in Theorem 6.4.

If the matrix A has an irreducible characteristic polynomial the number of non-singular matrices commuting with A is calculated in Example 6.6.

Example 6.6. Given any matrix $A \in \mathrm{GL}_d(q)$ with an irreducible characteristic polynomial $f(x)$. Then $\deg(f) = d$, the size of A. Verify that $\lambda = \{1\}$, $\lambda' = \{1\}$, $b_1 = 1$, all other b_i are zero and $s_i = 1$ for all i. Using Theorem 6.4 the number of non-singular matrices that commute with A is

$$\begin{aligned} c_d(\{1\}) &= \prod_{i \geq 1} \prod_{j=1}^{b_i} \left(q^{ds_i} - q^{(s_i - j)d} \right) \\ &= q^{d \cdot 1} - q^{(1-1)d} = q^d - 1. \end{aligned}$$

The following example concerns a matrix $A \in \mathrm{GL}_n(q)$ where A has coinciding minimum and characteristic polynomial, but the characteristic polynomial is not irreducible. Example 6.7 expresses the number of non-singular matrices commuting with A. It shows moreover the difference in number of singular and non-singular commuting matrices.

Example 6.7. Take matrix $A \in \mathrm{GL}_3(7)$ to be

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 4 & 1 & 1 \end{pmatrix}.$$

The characteristic polynomial is $\Phi_A(x) = (x+3)(x+5)(x+6)$, and it coincides with the minimum polynomial because all roots have multiplicity 1. According to Corollary 5.3 there are $q^n = 7^3$ solutions to the equation $AX = XA$. With Theorem 6.5 in hand we can calculate the number of non-singular matrices commuting with A. It is the product of $c_d(\lambda)$ for all irreducible factors of $\Phi_A(x)$. Using Example 6.6 one can show that $c_1(\{1\}) = q - 1$ for all factors.

$$\prod_{f \in \{(x+3),\, (x+5),\, (x+6)\}} c_1(\{1\}) = (q-1)^3 = 6^3 = 216$$

This shows that there are $q^n = 343$ matrices commuting with A, of which 216 non-singular.

6.2 Non-singular matrices commuting with a matrix of prime order

For matrices with prime order, the structure of the characteristic polynomial can be described neatly. The number of non-singular matrices commuting with a matrix A of prime order is described in Theorem 6.10. The following lemma investigates the structure of the characteristic polynomial needed to do this. We give a sketch of the proof, for a detailed proof of the lemma we refer to [14].

Lemma 6.8. *Given a finite field $\mathbb{F}_q$ of characteristic p. Consider the polynomial $x^r - 1 \in \mathbb{F}_q[x]$ for prime number $r \neq p$. Let d be the least number such that $r \mid q^d - 1$ and $s = \frac{r-1}{d}$ then it holds that*

$$x^r - 1 = (x-1)\prod_{i=1}^{s} g_i(x)$$

where all $g_i(x)$ are irreducible and have same degree d. Each $g_i(x)$ over $\mathbb{F}_{q^d}$ splits as

$$g_i(x) = \prod_{j=1}^{t} x - \pi_p^j(\lambda_i)$$

where $\pi_p \colon x \mapsto x^p$ the Frobenius map and λ_i a d root of unity in $\mathbb{F}_{q^d}$.

Proof. All roots of $x^r - 1$ are r-roots of unity, and they are in the same extension field, say $\mathbb{F}_{q^d}$, as proven in Corollary 2.6. One of the roots is 1, the root of $x - 1$. The other roots of unity are roots of an irreducible polynomial of degree d over $\mathbb{F}_q$. This implies that $x^r - 1$ factors in $x - 1$ and parts of degree d. The second claim that all irreducible factors g_i of degree d split over the field $\mathbb{F}_{q^d}$ in this way is proven in [14]. □

The following lemma is adapted from [14].

Lemma 6.9. *If matrix $A \in \mathrm{GL}_n(q)$ is of prime order $r \neq \mathrm{Char}(\mathbb{F}_q)$, then the characteristic polynomial $\Phi_A(x)$ splits in irreducible factors g_i of the same degree d each of multiplicity α_i and the factor $x - 1$ of multiplicity α_0. For $\alpha_i \geq 0$ the characteristic polynomial $\Phi_A(x)$ is*

$$\Phi_A(x) = (x-1)^{\alpha_0}\prod_{i=1} g_i(x)^{\alpha_i},$$

with $\alpha_0 + d\sum_i \alpha_i = n$. The minimal polynomial has the same roots, each of multiplicity 1.

Proof. The order of A is r, $A^r = \mathbf{I}$ and A thus vanishes on the polynomial $x^r - 1$. This polynomial is of the form $x^r - 1 = (x-1)\prod_{i=1} g_i(x)$ where all g_i have degree d as in Lemma 6.8. The minimal polynomial $p_A(x)$ is the polynomial of least degree on which A vanishes. Thus, $p_A(x) \mid x^r - 1$, implying that $p_A(x)$ is the product of some factors $(x-1), g_1(x), ..., g_s(x)$. The characteristic polynomial has the exact same roots as the minimal polynomial, and therefore equals $(x-1)^{\alpha_0}\prod_{i=1} g_i(x)^{\alpha_i}$ with $\alpha_i = 0$ if g_k is not a factor of $p_A(x)$ and $\alpha_i > 0$ otherwise. Moreover, the degree of the characteristic polynomial is n, thus $\alpha_0 + d\sum_i \alpha_i = n$. □

Using the structure of the characteristic polynomial of a matrix A of prime order. The number of non-singular matrices commuting with A is described in the following theorem.

Theorem 6.10. *If $A \in \mathrm{GL}_n(q)$ has prime order $r \neq \mathrm{Char}(\mathbb{F}_q)$ then the number of non-singular matrices that commute with A is*

$$|GL_{\alpha_0}(q)| \prod_{g_k,\, k\geq 1} |GL_{\alpha_k}(q^d)|.$$

Were α_k for $k \geq 1$ is the number of times the factor g_k of degree d appears in $\Phi_A(x)$ and α_0 is the number of times $x-1$ appears.

Proof. Lemma 6.9 proofs that the characteristic polynomial of A is

$$\Phi_A(x) = (x-1)^{\alpha_0} \prod_{k=1} g_k(x)^{\alpha_k}$$

with each $\alpha_k \geq 0$, $\deg(g_k) = d$ and $\alpha_0 + d\sum_{k=1} \alpha_k = n$. For each factor g_k the partition is $\lambda_k = \{1, 1, ...\}$ with α_k times 1 because the minimal polynomial contains each irreducible factor exactly once. This implies that the irreducible factors appear at most once in all invariant factors. The conjugate partition is $\lambda_k' = \{\alpha_k\}$, thus $b_1 = \alpha_k$ and $b_i = 0$ for other i, $s_i = \alpha_k$ for all i. With Theorem 6.4 $c_d(\lambda_k)$ is thus

$$\begin{aligned} c_d(\lambda_k) &= \prod_{i\geq 1} \prod_{j=1}^{b_i} q^{ds_i} - q^{(s_i-j)d} \\ &= \prod_{j=1}^{\alpha_k} (q^d)^{\alpha_k} - (q^d)^{(\alpha_k - j)} \\ &= \prod_{j=0}^{\alpha_k - 1} (q^d)^{\alpha_k} - (q^d)^j \\ &= |GL_{\alpha_k}(q^d)|. \end{aligned}$$

With Theorem 6.5 the number of non-singular matrices commuting with A is

$$\prod_{f \text{ irreducible}} c_f(\lambda_f) = |GL_{\alpha_0}(q)| \cdot \prod_{g_k,\, k\geq 1} |GL_{\alpha_k}(q^d)|.$$

□

Example 6.11. Take $A \in \mathrm{GL}_4(5)$ of order 3 to be

$$A = \begin{pmatrix} 4 & 3 & 0 & 2 \\ 0 & 2 & 4 & 4 \\ 2 & 1 & 2 & 4 \\ 0 & 3 & 2 & 3 \end{pmatrix}.$$

It has minimal polynomial $(x-1)(x^2+x+1)$ and characteristic polynomial $(x-1)^2(x^2+x+1)$. The degree of (x^2+x+1) is $d = 2$ it appears once, so $\alpha_1 = 1$. The factor $x-1$ appears twice,

thus $\alpha_0 = 2$. The number of non-singular matrices commuting with A can be calculated with Theorem 6.10 and reads

$$\begin{aligned} |GL_2(q)| \cdot |GL_1(q^2)| &= \prod_{k=0}^{1}(q^2 - q^k) \cdot \prod_{k=0}^{0}(q^1 - q^k) \\ &= (q^2-1)(q^2-q) = 480. \end{aligned}$$

The number of matrices commuting with A is by Corollary 5.2

$$\begin{aligned} q^{\sum_{i=1}^{4}(2(4-i)+1)\cdot \deg(f_i)} &= q^{3+3} \\ &= q^6 = 15625. \end{aligned}$$

6.3 Non-singular matrices commuting with a matrix of prime order equal to the characteristic of the field

In the previous section we investigated the number of non-singular matrices commuting with a matrix of prime order. During that section it is assumed that the prime order is not equal to the characteristic of the field. This section aims to find the number of non-singular matrices for a matrix of prime order equal to the characteristic of the field.

The following statement and proof can be found in [14].

Lemma 6.12. *If matrix $A \in \mathrm{GL}_n(q)$ is of prime order p with p the characteristic of the field, then the characteristic polynomial $\Phi_A(x)$ is $(x-1)^n$.*

Proof. The order of A is p, so A vanishes on the polynomial $x^p - 1$. Over a field of characteristic p, $x^p - 1$ equals $(x-1)^p$. As A vanishes on this polynomial, it holds that $p_A(x) \mid (x-1)^p$. Therefore, the minimal polynomial only contains the factor $x - 1$ several times. The characteristic polynomial has the same roots and since it has degree n it equals $(x-1)^n$. □

A matrix of prime order r with r not the characteristic of the field has other factors then $(x-1)$ in the characteristic polynomial. This is proven in Lemma 3.3 of [14].

Lemma 6.13. *Given any matrix $A \in \mathrm{GL}_n(q)$ with characteristic polynomial $\Phi_A(x) = (x-1)^n$. Then A has order p^k for some $k \geq 0$.*

For matrices with as order the characteristic of the field the number of commuting matrices is can be described with Theorem 6.4. We can not say anything more precise; the minimal polynomial is at most degree p and the characteristic polynomial of degree n and the invariant can have different degrees. This leads to different numbers of commuting matrices and different number of non-singular commuting matrices. This is shown in the following two examples.

Example 6.14. Take matrix $A \in \mathrm{GL}_4(5)$ to be

$$A = \begin{pmatrix} 4 & 3 & 1 & 1 \\ 3 & 1 & 0 & 1 \\ 4 & 1 & 3 & 0 \\ 2 & 1 & 2 & 1 \end{pmatrix}$$

This matrix has order 5 and characteristic polynomial $(x-1)^4$. The minimal polynomial of this matrix is $(x-1)^4$. The number of non-singular matrices commuting with A is thus $q^n - 1$ by Example 6.6 which is $5^4 - 1 = 624$. The total number of matrices commuting with A is q^n with Corollary 5.3 these are $5^4 = 625$ matrices.

Example 6.15. Take matrix $A \in \mathrm{GL}_6(3)$ to be

$$A = \begin{pmatrix} 0 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 2 & 2 & 1 & 1 \\ 1 & 2 & 0 & 2 & 1 & 1 \\ 0 & 2 & 1 & 2 & 0 & 2 \\ 0 & 1 & 1 & 1 & 0 & 2 \\ 2 & 2 & 0 & 1 & 1 & 1 \end{pmatrix}$$

This matrix has order 3, characteristic polynomial $(x-1)^6$, minimal polynomial $f_6 = (x-1)^3$ and invariant factor $f_5 = (x-1)^3$ the other invariant factors are constant 1. The number of non-singular matrices commuting with A can be calculated with Theorem 6.4 in hand. The degree of $(x-1)$ is 1, the partition $\{3,3\}$, the conjugate partition $\{2,2,2\}$, $b_3 = 2$ and $b_i = 0$ for $i \neq 3$ and $s_1 = 2$, $s_2 = 4$ and $s_3 = 6$. This gives

$$\begin{aligned} c_1(\{3,3\}) &= \prod_{i \geq 1} \prod_{j=1}^{b_i} (q^{s_i} - q^{s_i - j}) \\ &= (3^6 - 3^{(6-1)})(3^6 - 3^{(6-2)}) \\ &= (3^6 - 3^5)(3^6 - 3^4) \\ &= 314.928 \end{aligned}$$

non-singular matrices that commute with A. This is around 3^{11} to 3^{12} matrices. The number of matrices commuting with A can be calculated with Corollary 5.2 and is:

$$\begin{aligned} 3^{\sum_{i=1}^{6}(2(6-i)+1)\cdot \deg(f_i)} &= 3^{3\cdot 3+3} \\ &= 3^{12} \\ &= 531.441. \end{aligned}$$

7 Fraction of the solution space that is the left side of an isometry

Context - Recall the Sylvester algorithm that we preform for two equivalent matrix codes with non-trivial automorphism groups. We found similar automorphisms of the codes in Section 4. For these automorphisms we found the Sylvester equation and solved it in Section 5. In the previous section we described the number of non-singular matrices in this solution space.

Approach - This section aims to describe the complexity of preforming a brute force on the solution space of the Sylvester equation. Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ with non-trivial automorphism groups. Let $(A_1, A_2) \in \mathrm{Aut}(\mathcal{C})$ be similar to $(B_1, B_2) \in \mathrm{Aut}(\mathcal{D})$. The Sylvester equation we get is $B_1X = XA_1$. The brute force attack samples non-singular matrices L from the solution space of $B_1X = XA_1$. For such a matrix L we check if $L\mathcal{C}$ is right equivalent to $\mathcal{D}$. This section aims to estimate how many samples need to be done.

Outline section - Section 7.1 describes which solutions to the Sylvester equation are the left side of an isometry. The complexity of the brute force attack thus depends on the number of left sides of an isometry in the solution space of the Sylvester equation. Section 7.2 and Section 7.3 together describe the complexity for the brute force Sylvester algorithm with two-sided automorphisms. Section 7.4 describes the same for one-sided automorphisms.

7.1 Commuting automorphisms

As mentioned, we solve a Sylvester equation to find the left side of an isometry between two codes. There is not a unique isometry and neither a unique left side of an isometry in the solution space of the Sylvester equation. This section aims to find the solutions we are interested in.

For two automorphism (A_1, A_2) and (B_1, B_2) of matrix codes $\mathcal{C},\ \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ the solution space to the Sylvester equation equals $\{LA' \mid A'A_1 = A_1A'\}$, proven in Lemma 5.5. The set with left sides of an isometry equals $\{LA' \mid A' \in \mathrm{Aut}_{\mathrm{L}}(\mathcal{C})\}$ as shown in Corollary 3.5. The intersection of both sets thus describes the solutions that are the left side of an isometry. This intersection depends on automorphisms that commute with A_1. The aim of this section is thus to describe what automorphisms commute with each other.

Lemma 7.1. *Any matrix A commutes with all matrices polynomial in A.*

Proof. Let the polynomial $f \in \mathbb{F}_q[x]$ of degree d be written as $f(x) = \sum_{i=0}^{d} a_i X^i$, then:

$$A \cdot f(A) = A \cdot \sum_{i=0}^{d} a_i A^i = \sum_{i=0}^{d} a_i A^{i+1} = \left(\sum_{i=0}^{d} a_i A^i \right) A = f(A) \cdot A.$$

It can be deduced that A commutes with $f(A)$ completing the proof. □

The statement of Lemma 7.1 is a one way statement. If matrix $A \in \mathcal{M}_n(q)$ commutes with matrix $B \in \mathcal{M}_n(q)$, then B does not necessarily need to be polynomial in A. For example all matrices commute with the identity matrix, but only scalar multiples of $\mathbf{I}$ are polynomial in $\mathbf{I}$. Next examples show the same for a non-trivial matrix.

Example 7.2. Revisit matrix $A \in \mathrm{GL}_6(3)$ from Example 6.15. This matrix has minimal polynomial $(x-1)^3$. All matrices polynomial in A are thus $a_0+a_1A+a_2A^2$ for $a_0, a_1, a_2 \in \mathbb{F}_q$. These are $q^3 = 3^3 = 27$ matrices. The matrices commuting with A on the other hand is 3^{12} with Corollary 5.3 which are many more matrices.

The example shows that if the degree of the minimal polynomial is low, then there are fewer matrices polynomial in A. On the other hand, the low degree of the minimal polynomial assures that there are other non-constant invariant factors. These factors lead to more matrices commuting with A as can be seen in the formula of Corollary 5.2.

If the minimal polynomial coincides with the characteristic polynomial, then all matrices commuting with A are polynomial in A.

Lemma 7.3. *If the minimal polynomial and characteristics polynomial of a matrix A in $\mathcal{M}_n(q)$ coincide, then $B \in \mathcal{M}_n(q)$ commutes with A if and only if B is polynomial in A.*

Proof. Lemma 7.1 gives an inclusion of the following two sets

$$\{B \mid B = f(A),\ f(x) \in \mathbb{F}_q[x]\} \subseteq \{B \mid AB = BA\}.$$

In order to prove equality we use a dimension argument. The minimal polynomial of A coincides with the characteristic polynomial, the right-hand side therefore has dimension n by Corollary 5.3. The dimension of the space of matrices polynomial in A depends on the degree of the minimal polynomial of A, n in this case. The basis of the space of matrices polynomial in A is $\{1, x, .., x^{\deg(p_A(x))-1} = x^{n-1}\}$. The left-hand side thus is also of dimension n. The dimension of the two spaces is equal and one is a subset of the other; therefore we can conclude that the sets are equal. □

Matrices that commute with an automorphism but are not in its polynomial span are difficult to describe. Therefore, we focus on matrices polynomial in the automorphism.

Addition is preserved in the conductor group; for a one-sided automorphism $(A_1, \mathbf{I})$ all matrices polynomial in A_1 are in the conductor group. This leads to the following corollary for one-sided automorphisms.

Corollary 7.4. *Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ with $A \in \mathrm{Aut}_{\mathrm{L}}(\mathcal{C})$ similar to $B \in \mathrm{Aut}_{\mathrm{L}}(\mathcal{D})$ be given. If the minimal polynomial and characteristics polynomial of A coincide then all non-singular solutions to $BX = XA$ are the left side of an isometry.*

Proof. This corollary can be proven with a dimension argument. The size of $BX = XA$ is q^n by Corollary 5.3. The matrices polynomial in A are also q^n as can be seen in the proof of Lemma 7.3. The non-singular elements of this set are the left side of an isometry. □

Remark. The coincidence of the minimal and characteristic polynomial is a sufficient and necessarily condition. If the minimal polynomial has degree lower than n, then the matrices polynomial in A are fewer than q^n and the matrices commuting with A are more than q^n.

Unfortunately addition is not preserved in the group of two-sided automorphisms. As a result, not all pairs of matrices in the span of a two-sided automorphism are in the automorphism group. Guaranteed is however that for any automorphism powers and scalar multiplications is preserved in the automorphism group as proven in Section 3.2.

7.2 Size of the set of powers of a given matrix

For two-sided automorphisms, it can be guaranteed that all elements of their set of powers are automorphisms. These automorphisms correspond one-to-one to the isometries that can be found via the Sylvester attack. The goal of this section is therefore to express the size of powers$\langle A \rangle$ for a given matrix $A \in \mathrm{GL}_n(q)$. Note there might be more automorphisms commuting with this two-sided automorphism. We focus only on the automorphisms in powers$\langle A \rangle$, which leads to an upper bound.

Lemma 7.5. *Given a matrix $A \in \mathrm{PGL}_n(q)$ and let p_A its minimal polynomial. Then;* powers$\langle A \rangle$ *evaluated in* $\mathrm{PGL}_n(q)$ *is of size k if and only if k is the least number such that $A^k = \mathbf{I}$.*

In $\mathrm{GL}_n(q)$, powers$\langle A \rangle$ *is of size $(q-1)k$ if and only if $A^k = a\,\mathbf{I}$ for some $a \in \mathbb{F}_q^*$ and k is the least number for which this holds.*

Proof. Let k be the least number such that $A^k = \mathbf{I}$ then clearly powers$\langle A \rangle = \{A, A^2, .., A^k\}$ is of size k in $\mathrm{PGL}_n(q)$. Over $\mathrm{GL}_n(q)$ it is of size $(q-1)k$ as we add $q-1$ scalar multiplications. If powers$\langle A \rangle$ is of size k, then necessarily A^{k+1} equals some A^l for $l \leq k$. The order of A is exactly the least number for which this sequence repeats and thus $A^k = \mathbf{I}$. If $A^k = \mathbf{I}$ over $\mathrm{PGL}_n(q)$ then A^k considered over $\mathrm{GL}_n(q)$ is $a\,\mathbf{I}$ for some scalar $a \in \mathbb{F}_q^*$. □

The number k of Lemma 7.5 depends on the eigenvalues and not just the order. Lemma 7.6 gives a lower bound for the size of powers$\langle A \rangle$ given only the order of the matrix.

Lemma 7.6. *The set* powers$\langle A \rangle$ *of a matrix $A \in \mathrm{GL}_n(q)$ over $\mathbb{F}_q$ is:*

- *Of size $q-1$ if A equals $\mathbf{I}$ in $\mathrm{PGL}_q(n)$.*
- *Of size $(q-1)\,\mathrm{Order}(A)$ if $\mathrm{Order}(A)$ is prime.*
- *At least of size $(q-1) \cdot \frac{\mathrm{Order}(A)}{\gcd(\mathrm{Order}(A), q-1)}$ otherwise.*

Proof. Lemma 7.5 states that powers$\langle A \rangle$ is of size k for $A \in \mathrm{PGL}_n(q)$ and k the least such that $A^k = \mathbf{I}$. If $A = \mathbf{I}$ in $\mathrm{PGL}_n(q)$ then $k = 1$. Over $\mathrm{GL}_n(q)$, powers$\langle A \rangle$ is of size $(q-1)k$.

For the remainder of the proof we assume $k \neq 1$, and we will be working over $\mathrm{GL}_n(q)$. The number k divides $\mathrm{Order}(A)$, if $\mathrm{Order}(A)$ is prime then $k = \mathrm{Order}(A)$. The result that powers$\langle A \rangle$ is of size $(q-1)k$ follows directly from Lemma 7.5.

If $\mathrm{Order}(A)$ is not prime, then k could be a non-trivial divisor of $\mathrm{Order}(A)$. It holds that $A^k = a\,\mathbf{I}$ for some $a \in \mathbb{F}_q$ and thus $(A^k)^{q-1} = \mathbf{I}$. It follows that $\mathrm{Order}(A)$ divides $k(q-1)$. The least k satisfying these constraints is $\frac{\mathrm{Order}(A)}{\gcd(\mathrm{Order}(A), q-1)}$, proven in Lemma 2.2. □

7.3 Two-sided automorphisms

Assume we are given two equivalent matrix codes and similar two-sided automorphisms to preform the Sylvester attack. The Sylvester equation is formed with the left sides of the automorphisms. The equation can be solved, and this section aims to describe the complexity of a brute force attack preformed in this solution space. In this section we focus only on the non-singular matrices in the solution space. The left side of the two-sided automorphism is assumed to be of prime order.

Theorem 7.7. *Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$. Let $(A_1, A_2) \in \mathrm{Aut}(\mathcal{C})$ be similar to $(B_1, B_2) \in \mathrm{Aut}(\mathcal{D})$. Assume A_1 has prime order $r \neq \mathrm{Char}(\mathbb{F}_q)$. Then the fraction of the non-singular matrices in the solution space $B_1X = XA_1$ that are the left side of an isometry is*

$$\frac{(q-1)r}{\prod_{j=0}^{\alpha_0-1}(q^{\alpha_0}-q^j)\prod_k\prod_{j=0}^{\alpha_k-1}((q^d)^{\alpha_k}-(q^d)^j)}. \tag{7.1}$$

Where α_0 is the number of times $(x-1)$ appears and α_k for $k \geq 1$ the number of times the factor g_k of degree d appears. The order of complexity of searching the space for a left side of an isometry is:

$$\mathcal{O}\left(\frac{1}{r}q^{S-1}\right) \tag{7.2}$$

with $S = \alpha_0^2 + \sum_k d\alpha_k^2$. For evaluations of S we refer to Table 1.

Proof. The number of matrices in powers$\langle A_1 \rangle$ is $(q-1)r$ by Lemma 7.6. This is the number of matrices that commute with A_1 and are in the automorphism group. This number corresponds to the number of elements LA' in $\mathrm{SolSp}(B_1, A_1)$ that are the left side of an isometry Lemma 5.5. The total number of non-singular matrices in the space $\mathrm{SolSp}(B_1, A_1)$ is the same as the number of non-singular matrices commuting with A_1 and is by Theorem 6.10

$$\prod_{j=0}^{\alpha_0-1}(q^{\alpha_0}-q^j)\prod_k\prod_{j=0}^{\alpha_k-1}(q^d)^{\alpha_k}-(q^d)^j.$$

Divide both numbers to get the fraction of solutions that are the left side of an isometry expressed in Equation (7.1). The order of complexity of finding the left side of an isometry is 1 divided by the fraction in Equation (7.1). The order of complexity of $\prod_{j=0}^{\alpha_0-1}(q^{\alpha_0}-q^j)$ is $\mathcal{O}\left(q^{\alpha_0^2}\right)$ this leads to the total complexity presented in Equation (7.2). □

Remark. We aim to estimate $S = \alpha_0^2 + d\sum_{k>1}\alpha_k^2$ in terms of n^2 and n, where n can be expressed as $n = \alpha_0 + d\sum_{k>1}\alpha_k$. For $d \neq 0$ it thus holds that $\sum_{k>1}\alpha_k = \frac{n-\alpha_0}{d}$. If $d = 0$, then α_0 equals n and $S = \alpha_0^2$. This only happens when the prime order equals $p = \mathrm{Char}(\mathbb{F}_q)$ by Lemma 6.13. Assume $d \neq 0$, then S is at most

$$\begin{aligned}
S &= \alpha_0^2 + d\sum_{k>1}\alpha_k^2 \\
&\leq \alpha_0^2 + d\left(\sum_{k>1}\alpha_k\right)^2 \\
&= \alpha_0^2 + d\left(\frac{n-\alpha_0}{d}\right)^2 \\
&= \frac{n^2}{d} - \frac{2n\alpha_0}{d} + \frac{\alpha_0^2}{d} + \alpha_0^2.
\end{aligned}$$

The complexity depends on the number of times $x-1$ appears in $\Phi_A(x)$, α_0, and the degree d of the other factors. If $\alpha_0 \to n$ it follows that d is less equal than $n - \alpha_0$ and thus $d \to 1$. The time complexity is small when α_0 is small and d relatively big in comparison to n.

α_0	$\mathbf{S \leq \frac{n^2}{d} - \frac{2n\alpha_0}{d} + \frac{\alpha_0^2}{d} + \alpha_0^2}$
0	$\frac{n^2}{d}$
1	$\frac{n^2}{d} - \frac{2n+1}{d} + 1 = \mathcal{O}\left(\frac{n^2-2n}{d}\right)$
$\frac{n}{2}$	$\frac{1}{4}\left(\frac{n^2}{d} + n^2\right) = \mathcal{O}\left(\frac{1}{2}n^2\right)$
n	n^2

Table 1: Estimations of S

Assume the Sylvester algorithm is preformed with similar automorphisms of which the left side has coinciding minimal and characteristic polynomial. The solution space that the Sylvester equation gives contains a high fraction of non-singular matrices. In fact reducing the space of all solutions to the non-singular solutions leads to at most a speedup of a factor q as the following proposition shows.

Proposition 7.8. *Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$. Let (A_1, A_2) in $\mathrm{Aut}(\mathcal{C})$ be similar to $(B_1, B_2) \in \mathrm{Aut}(\mathcal{D})$. Assume A_1 has prime order $r \neq \mathrm{Char}(\mathbb{F}_q)$. Assume moreover that the minimal polynomial of A_1 coincides with the characteristic polynomial, then the faction of non-singular matrices of the solution space $B_1X = XA_1$ is at most $\frac{1}{q}$, i.e.*

$$\frac{|\{X \mid BX = XA \text{ } X \text{ non-singular}\}|}{|\{X \mid BX = XA\}|} \leq \frac{1}{q}.$$

Proof. The minimal polynomial equals the characteristic polynomial, hence there are q^n solutions to the equation $B_1X = XA_1$. Moreover, all factors of the characteristic polynomial appear at most once, thus all α_i of Theorem 6.10 are either 0 or 1. We stress this by writing δ to indicate if $x - 1$ is a factor of $p_A(x)$. There are thus $\frac{n-\delta}{d}$ unique factors of degree d. The number of non-singular solutions can be evaluated with Theorem 6.10. The size of $\mathrm{GL}_{\alpha_i}(q^d)$ is $(q^d - 1)$ for $\alpha_i = 1$ and 0 otherwise. The number of non-singular matrices commuting with A_1 is thus $(q-1)^\delta (q^d - 1)^{\frac{n-\delta}{d}}$ by Theorem 6.10. The fraction of non-singular matrices is

$$\frac{(q-1)^\delta (q^d - 1)^{\frac{n-\delta}{d}}}{q^n}.$$

The numerator has degree n, the same degree as the denominator; they differ a constant factor. The quotient can thus never exceed $\frac{1}{q}$. □

Example 7.9. Revisit the matrix $A \in \mathrm{GL}_3(7)$ of Example 6.7. The number of non-singular matrices commuting with A are $6^3 = 216$, all matrices commuting with A are $7^3 = 343$ matrices. This difference is a factor $\frac{216}{343} \approx \frac{3}{2}$, which is indeed less than 3, the size of the field.

7.4 One-sided automorphisms

Assume we are again given two equivalent matrix codes but, in contrast with the previous section, we are given similar one-sided automorphisms to preform the Sylvester attack. The Sylvester equation is formed with the automorphisms. The equation can be solved, and this

section aims to describe the complexity of a brute force attack preformed in this solution space. In this section we again focus only on automorphisms of prime order, but we do not restrict to the non-singular matrices.

Working with left one-sided automorphism implies that addition is preserved in the conductor group. The non-singular matrices of the conductor group are in the automorphism group. The non-singular matrices of the conductor group are difficult to describe, thus we evaluate the fraction of the conductor group with all solutions to the Sylvester equation.

Theorem 7.10. *Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ and let $A \in \mathrm{Aut}_{\mathrm{L}}(\mathcal{C})$, $B \in \mathrm{Aut}_{\mathrm{L}}(\mathcal{D})$ similar automorphisms be given. Assume A, B have prime order $r \neq \mathrm{Char}(\mathbb{F}_q)$. Then the fraction of matrices in the solution space $BX = XA$ that are in $\mathbf{Cond}(\mathcal{C}, \mathcal{D})$ is*

$$\prod_{i=1}^{n-1} q^{-(2(n-i)+1)\cdot \deg(f_i)}. \tag{7.3}$$

Proof. The size of $\mathrm{span}\langle A \rangle$ depends on the minimal polynomial and is $q^{\deg(p_A)}$ which is $q^{\deg(f_n)}$. This expresses the number of matrices that commute with A and are guaranteed to be in the conductor group $\mathbf{Cond}(\mathcal{C})$. The total number of matrices in the space $\mathrm{SolSp}(B, A)$ equals $q^{\sum_{i=1}^{n}(2(n-i)+1)\cdot \deg(f_i)}$ by Theorem 5.1 which equals $\prod_{i=1}^{n} q^{(2(n-i)+1)\cdot \deg(f_i)}$. Divide both numbers to find the fraction of matrices in the solution space $BX = XA$ that are in the conductor group $\mathbf{Cond}(\mathcal{C}, \mathcal{D})$:

$$\prod_{i=1}^{n-1} q^{-(2(n-i)+1)\cdot \deg(f_i)}.$$

□

The degree of invariant factor f_n does not contribute to the fraction in the previous theorem. This implies that if the degree of $f_n = p_A(x)$ is high, then the degree of the other invariant factors is low and thus the sum $\sum_{i=1}^{n-1}(2(n-i)+1)\deg(f_i)$ is small.

If the degree of the minimal polynomial is high the fraction of Theorem 7.10 is big. There are thus more solutions that give rise to an isometry.

Remark. Theorem 7.10 yields a number of solutions, but some might be singular. This gives therefore an upper bound for the number of non-singular solutions that are the left side of an isometry. This does not pose a problem, on average most matrices are non-singular.

In the particular case that the minimal polynomial equals the characteristic polynomial the left sides of an isometry can be easily found.

Example 7.11. Take A, B as in Corollary 7.4 and assume moreover A has an irreducible characteristic polynomial. Then $\mathrm{SolSp}(B, A)$ has size q^n by Corollary 5.3. Moreover, $q^n - 1$ solutions are non-singular by Theorem 6.10; there is 1 invariant factor of degree n, the size of $|\mathrm{GL}_q(q^n)| = q^n - 1$. The only singular solution is thus the zero solution. An isometry can thus be found in polynomial time.

8 The Sylvester algorithm

This thesis explained a brute force algorithm for the MCE problem based on the Sylvester equation. The complexity of this algorithm is described in Section 7. The algorithm is presented in its entirety in this section. During this section we assume that the similar automorphisms are given. Some notes on the complexity of finding this is stated in Section 4. Similar matrices are easiest found for one-sided automorphism groups.

The MCRE problem is solvable in polynomial time as explained. During the algorithms presented below we do not chose a solver and denote the time of a solver by $p_1(m)$.

Theorem 8.1. *Given two equivalent matrix codes over $\mathcal{M}_{n,m}(q)$ with non-trivial one-sided automorphism groups and two non-trivial one-sided automorphisms that relate by the isometry. The MCE problem with this input can be solved in time complexity*

$$\mathcal{O}\left(nM(n) + M(n)p_1(m) \cdot q^{\sum_{i=1}^{n-1}(2(n-i)+1)\cdot \deg(f_i)}\right) \tag{8.1}$$

using the Randomized Sylvester algorithm described in Algorithm 2.

Algorithm 2 Randomized Sylvester algorithm one-sided automorphisms

Input Two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ with non-trivial one-sided automorphisms $A \in \mathrm{Aut}_{\mathrm{L}}(\mathcal{C})$ and $B \in \mathrm{Aut}_{\mathrm{L}}(\mathcal{D})$.

Output A pair $(L, R) \in \mathrm{GL}_n(q) \times \mathrm{GL}_m(q)$ such that $L\mathcal{C}R = \mathcal{D}$.

Find a basis of the Sylvester equation $BX = XA$ ▷ $\mathcal{O}(nM(n))$
repeat
  do
    $L \leftarrow \mathrm{SolSp}(B, A)$.
    Determinant(L) ▷ $\mathcal{O}(M(n))$
  while Determinant(L) equals 0
  Solve the MCRE problem with $L\mathcal{C}$ and $\mathcal{D}$ ▷ $\mathcal{O}(p_1(m))$
until L, R are found with $L\mathcal{C}R = \mathcal{D}$ ▷ $\mathcal{O}\left(q^{\sum_{i=1}^{n-1}(2(n-i)+1)\cdot \deg(f_i)}\right)$
return (L, R)

Proof. If A and B relate by an isometry Proposition 3.3 guarantees that some solution L to $BX = XA$ is the left side of an isometry. With this left side L an MCRE solver can find R and give the isometry. It is therefore clear that the algorithm succeeds.

To find a basis of the Sylvester equation Theorem 5.6 can be used. The basis can be found time complexity $\mathcal{O}(nM(n))$.

We are interested in non-singular solutions, and thus we implement a check for singularity. Strassen [17] demonstrates how any $\mathcal{O}(n^\alpha)$, $\alpha > 2$ algorithm for matrix multiplication can be used to obtain an $\mathcal{O}(n^\alpha)$ algorithm for computation of determinants. Checking a matrix for singularity is thus of complexity $\mathcal{O}(M(n))$.

Use a MCRE solver working in time $p_1(m)$ to find if a right equivalence between $L\mathcal{C}$ and $\mathcal{D}$ exists. If no right equivalence is found repeat this loop. Theorem 7.10 proves that this takes roughly $\mathcal{O}\left(q^{\sum_{i=1}^{n-1}(2(n-i)+1)\cdot \deg(f_i)}\right)$ repetitions. Together this gives the time complexity of Equation (8.1). □

Theorem 8.2. *Given two equivalent matrix codes over $\mathcal{M}_{n,m}(q)$ with non-trivial two-sided automorphism groups and two non-trivial two-sided automorphisms that relate by the isometry. The MCE problem with this input can be solved in time complexity*

$$\mathcal{O}\left(nM(n) + M(n) \cdot p_1(m) \cdot \frac{1}{r} q^{S-1}\right)$$

using the Randomized Sylvester algorithm described in Algorithm 3. With S as in Theorem 7.7 and Table 1.

Algorithm 3 Randomized Sylvester algorithm two-sided automorphisms

Input Two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ and similar non-trivial two-sided automorphisms $(A_1, A_2) \in \mathrm{Aut}(\mathcal{C})$ and $(B_1, B_2) \in \mathrm{Aut}(\mathcal{D})$.

Output A pair $(L, R) \in \mathrm{GL}_n(q) \times \mathrm{GL}_m(q)$ such that $L\mathcal{C}R = \mathcal{D}$.

```
Find a basis of the Sylvester equation B_1 X = X A_1                ▷ O(nM(n))
repeat
    do
        L ← SolSp(B_1, A_1).
        Determinant(L)                                              ▷ O(M(n))
    while L singular
    Solve the MCRE problem with LC and D                            ▷ O(p_1(m))
until L, R are found with LCR = D                                   ▷ O((1/r) q^{S-1})
return (L, R)
```

Proof. The proof is similar to Theorem 8.1. The expected number of repetitions to find an equivalence is $\mathcal{O}\left(\frac{1}{r} q^{S-1}\right)$ as proven in Theorem 7.7. □

To conclude this thesis we present some examples to evaluate the complexities described in Theorem 8.1 and Theorem 8.2. To this end we need to fix a solver for matrix multiplication and an MCRE solver.

We assume $M(n) = n^3$, this assumption is based on the standard and practical algorithm that yields this time complexity as pointed out in [16].

The MCRE solver of [5] is not very constructive, and the complexity is difficult to evaluate. The algebraic attack to the MCE problem described in [3] is constructive and moreover its complexity is easily evaluated. The MCE solver can be used to solve a right equivalence by choosing the matrix on the left to be the identity matrix. The complexity of this algebraic MCRE solver can be expressed in terms of m and the dimension of the code. It has time complexity $\mathcal{O}\left(M\left(m^2 + \dim(\mathcal{C})^2\right)\right)$. Without loss of generality we can assume that $m \leq \dim(\mathcal{C})$ [13, Lemma 26]. The complexity of solving the MCRE problem is thus assumed to be $\mathcal{O}\left(m^6\right)$.

If the codes are $\mathbb{F}_{q^n}$-linear, [5] proves that the MCE problem is solvable in polynomial time. This is equivalent to saying that the codes have one-sided left automorphisms group and a matrix with an irreducible characteristic polynomial in these left sided automorphism groups. This is expressed in the following theorem.

Theorem 8.3. *Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$. If there exists a matrix $A \in \mathrm{Aut}_{\mathrm{L}}(\mathcal{C})$ with an irreducible characteristic polynomial, then the codes are $\mathbb{F}_{q^n}$-linear.*

Proof. Definition 25 in [5] states that $A \in \mathcal{M}_n(q)$ with irreducible polynomial spans $\mathbb{F}_{q^n}$ as an algebra. Thus, if there exist a matrix $A \in \mathrm{Aut}_{\mathrm{L}}(\mathcal{C})$ with irreducible characteristic polynomial it spans $\mathbb{F}_{q^n}$. This implies that the code is $\mathbb{F}_{q^n}$-linear. □

To compare the Sylvester algorithm for $\mathbb{F}_{q^n}$-linear codes to the polynomial time algorithm of [5] we should evaluate the Sylvester algorithm for a matrix with irreducible characteristic polynomial. To illustrate this, consider the following example.

Example 8.4. Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ and $A \in \mathrm{Aut}_{\mathrm{L}}(\mathcal{C})$ and $B \in \mathrm{Aut}_{\mathrm{L}}(\mathcal{D})$ be similar. If the minimal polynomial of A equals its characteristic polynomial then Algorithm 2 terminates with this input in time $\mathcal{O}\left(n^4 + n^3 \cdot m^6\right)$ assuming that $n = m$ as commonly done [2, 3] the complexity reads $\mathcal{O}\left(n^9\right)$.

Note that the assumption for Example 8.4 is that the automorphisms have coinciding minimal and characteristic polynomial which is slightly less strict than the assumption that the characteristic polynomial irreducible. The example shows that the MCE problem can be solved in polynomial time under this assumption. In particular, the Sylvester algorithm solves the MCE problem in polynomial time if the codes are $\mathbb{F}_{q^n}$-linear.

The next example is presented to illustrate the complexity of the MCE problem if the matrix with irreducible characteristic polynomial is part of a two-sided automorphism.

Example 8.5. Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ and let similar two-sided automorphisms $(A_1, A_2) \in \mathrm{Aut}(\mathcal{C})$ and $(B_1, B_2) \in \mathrm{Aut}(\mathcal{D})$ be given. If A_1 has an irreducible characteristic polynomial, then Proposition 7.8 shows that the fraction of non-singular solutions to $B_1 X = X A_1$ is at most $\frac{1}{q}$. Corollary 7.4 shows that all non-singular solutions are the left side of an isometry. Assuming $m = n$ Algorithm 3 terminates in time

$$\mathcal{O}\left(n^4 + n^3 \cdot m^6 \cdot q\right) = \mathcal{O}\left(n^9 \cdot q\right).$$

The MCE problem given codes with trivial automorphism groups is solvable in time $\mathcal{O}\left(q^{\min\{n,m\}}\right)$ [13]. If the Sylvester algorithm is used with trivial automorphisms the algorithm is exponential slower than the algorithm of [5] and expressed by the following example.

Example 8.6. Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$. Take $(\mathbf{I}, \mathbf{I}) \in \mathrm{Aut}(\mathcal{C})$ and $(\mathbf{I}, \mathbf{I}) \in \mathrm{Aut}(\mathcal{D})$ the input for Algorithm 2. Then Algorithm 2 terminates in time $\mathcal{O}\left(q^{n^2-1}\right)$. Algorithm 3 terminates in the same time complexity.

The complexity of this example is the complexity of a brute force attack where all matrices are searched. This brute force complexity is inherited form the brute force attack on the solution space $\mathrm{SolSp}(B, A)$. To improve the Sylvester algorithm it should not use brute force.

The Sylvester algorithm can describe the complexity of the MCE problem where the matrix codes are not $\mathbb{F}_{q^n}$-linear and neither trivial. The Sylvester algorithm with a brute force search reaches time complexities between polynomial and q^{n^2}. Some examples can be found below.

Example 8.7. Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$ and $(A, \mathbf{I}) \in \mathrm{Aut}(\mathcal{C})$ and $(B, \mathbf{I}) \in \mathrm{Aut}(\mathcal{D})$. If A has two non-constant invariant factors, Algorithm 2 terminates in the worst case in time

$$\mathcal{O}\left(m^6 \cdot q^{\frac{3}{2}n}\right).$$

If there are at most 2 invariant factors, f_{n-1} has degree at most $\lfloor \frac{n}{2} \rfloor$. This leads to the highest value of the sum, $\sum_{i=1}^{n-1}(2(n-i)+1) \cdot \deg(f_i) = 3\deg(f_{n-1}) = \frac{3}{2}n$.

In the best case the degree of the invariant factor f_{n-1} is 1 and the algorithm terminates in time complexity

$$\mathcal{O}\left(m^6 \cdot q^3\right).$$

This can be seen by evaluating the sum, $\sum_{i=1}^{n-1}(2(n-i)+1) \cdot \deg(f_i) = 3\deg(f_{n-1}) = 3$.

Example 8.8. Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$. Let non-trivial two-sided automorphisms $(A_1, A_2) \in \mathrm{Aut}(\mathcal{C})$ similar to $(B_1, B_2) \in \mathrm{Aut}(\mathcal{D})$ be given. Assume A_1 has $p_A(x) = g(x)$ an irreducible polynomial of degree $d = \frac{n}{2}$. The characteristic polynomial is then $g(x)^2$. This gives $S = \frac{n}{2} \cdot 2^2 = 2n$ of Theorem 7.7. Algorithm 3 terminates in time

$$\mathcal{O}\left(m^6 \cdot \frac{1}{r} q^{2n}\right).$$

All eigenvalues are d roots of unity. The order of the matrix therefore divides $q^d - 1$. In the best case scenario the matrix has order $q^d - 1 = q^{\frac{n}{2}} - 1$ the algorithm then terminates in time complexity

$$\mathcal{O}\left(m^6 \cdot q^{\frac{3}{2}n}\right).$$

Example 8.9. Given two equivalent matrix codes $\mathcal{C}, \mathcal{D} \subseteq \mathcal{M}_{n,m}(q)$. Let $(A, \mathbf{I}) \in \mathrm{Aut}(\mathcal{C})$ and $(B, \mathbf{I}) \in \mathrm{Aut}(\mathcal{D})$ similar automorphisms be given. If A has 3 non-constant invariant factors, Algorithm 2 terminates in the worst case in time

$$\mathcal{O}\left(m^6 \cdot q^{\frac{8}{3}n}\right).$$

The invariant factors f_{n-2} and f_{n-1} have degree at most $\lfloor \frac{n}{3} \rfloor$. This leads to the highest value of the sum, $\sum_{i=1}^{n-1}(2(n-i)+1) \cdot \deg(f_i) = 5\deg(f_{n-2}) + 3\deg(f_{n-1}) = \frac{5}{3}n + \frac{3}{3}n$.

In the best case the degree of the invariant factors f_{n-2} and f_{n-1} is 1 and the algorithm terminates in time complexity

$$\mathcal{O}\left(m^6 \cdot q^8\right).$$

Remark. If the degree of the minimal polynomial is high then the complexity of solving the MCE problem with the Sylvester algorithm is lowest. On the other hand, if there are many invariant factors all invariant factors contribute to the sum and the complexity of solving the MCE problem with the Sylvester algorithm has a high complexity.

9 Conclusion

During this thesis, we demonstrated the correspondence between the automorphism and isomorphism groups of two equivalent matrix codes. Any isometry relates two automorphisms by similarity, and this relation can be used to find the isometry. Two automorphisms that are similar give rise to a Sylvester equation. The solution space of this Sylvester equation has a particular structure, which can be compared to the structure of the space of matrices that commute with a given matrix. Investigating the structure of this second space, thus provides insights into the structure of the solution space of the Sylvester equation. The structure reveals information on the number of isometries within the solution space, which in turn determines the complexity of a brute force attack.

The structure of the solution space to the Sylvester equation potentially contains more information. During the thesis we used the structure only to estimate the number of isometries in the solution space and, consequently, to estimate the complexity of a brute force attack. It might be interesting to explore this structure further to identify a more efficient searching method. If such a method could be developed, the Sylvester algorithm would become more efficient, allowing the MCE problem to be solved more quickly.

The Sylvester algorithm presented in this thesis can be used to solve the MCE problem. The analysis of its complexity allows us to understand the difference in complexity when solving the MCE problem for matrix codes with trivial versus non-trivial automorphism groups. We clearly demonstrated how the complexity depends on the automorphisms used in the algorithm.

The complexity of the Sylvester algorithm primarily depends on the automorphisms used in the algorithm. If the automorphism has on one side a matrix with a few invariant factors, the complexity of solving the MCE problem with the Sylvester algorithm is the lowest. On the other hand, if the automorphism used has on both sides matrices with many invariant factors, the complexity of solving the MCE problem with the Sylvester algorithm is the highest. This implies that for matrix codes with $\mathbb{F}_q^n$-linear automorphism groups, the MCE problem can be solved in polynomial time. Conversely, for two equivalent matrix codes with trivial automorphism groups, the Sylvester algorithm cannot efficiently find the equivalence, resulting in exponential complexity.

This thesis does not extensively address the complexity of finding automorphisms given two matrix codes. During this thesis we assumed that similar automorphisms were given. For one-sided automorphism groups, all automorphisms can be found efficiently, and it is a matter of searching to find similar automorphisms. However, for two-sided automorphism groups, finding similar automorphisms could be more complicated. Despite this, identifying these similar automorphisms is necessary for the algorithm to function. The complexity of finding these similar automorphism remains an open question.

References

[1] Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley Publishing Company, 1974. URL: https://api.semanticscholar.org/CorpusID:29599075.

[2] Tung Chou et al. *Matrix Equivalence Digital Signature*. 2023.

[3] Tung Chou et al. "Take your MEDS: Digital Signatures from Matrix Code Equivalence". In: *International Conference on Cryptology in Africa*. https://eprint.iacr.org/2022/1559. Springer. 2023, pp. 28–52.

[4] D. Coppersmith and S. Winograd. "Matrix multiplication via arithmetic progressions". In: *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*. STOC '87. New York, New York, USA: Association for Computing Machinery, 1987, pp. 1–6. ISBN: 0897912217. DOI: 10.1145/28395.28396. URL: https://doi.org/10.1145/28395.28396.

[5] Alain Couvreur, Thomas Debris-Alazard, and Philippe Gaborit. "On the hardness of code equivalence problems in rank metric". In: *arXiv preprint arXiv:2011.04611* (2020).

[6] MR Darafsheh. "Order of elements in the groups related to the general linear group". In: *Finite Fields and Their Applications* 11.4 (2005), pp. 738–747.

[7] A. Fiat and A. Shamir. "How to Prove Yourself: Practical Solutions to Identification and Signature Problems". In: *Proceedings on Advances in Cryptology—CRYPTO '86*. Santa Barbara, California, USA: Springer-Verlag, 1987, pp. 186–194. ISBN: 0387180478.

[8] Nathan Jacobson. *Basic algebra I*. W H Freeman & Co, 1989, p. 207.

[9] H Loo-Kengn. "A theorem on matrices over a sfield and its applications". In: *Bulletin of the American Mathematical Society* 55 (1951), pp. 1046–1046.

[10] CC MacDuffee. "The Theory of Matrices". In: *Co., New York* (1946), p. 104.

[11] NIST. *Post-Quantum Cryptography Background*. Created January 03, 2017, Updated June 24, 2024, Last accessed June 27 2024. 2024. URL: https://www.nist.gov/pqcrypto.

[12] Tovohery Hajatiana Randrianarisoa. "The number of matrices over $\mathbb{F}_q$ with irreducible characteristic polynomial". In: *arXiv: Commutative Algebra* (2014). arXiv: 1402.2794 [math.AC].

[13] Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. "Hardness estimates of the Code Equivalence Problem in the Rank Metric". Cryptology ePrint Archive, Paper 2022/276. https://eprint.iacr.org/2022/276. 2022.

[14] Krijn Reijnders et al. "Random Rank-Metric Codes have trivial automorphism groups". Preprint.

[15] Richard P Stanley. "What is enumerative combinatorics?" In: Springer, 1986. Chap. 1.10.

[16] Arne Storjohann. "An $\mathcal{O}(n^3)$ algorithm for the frobenius normal form". In: *Proceedings of the 1998 international symposium on Symbolic and algebraic computation*. 1998, pp. 101–105.

[17] Volker Strassen. "Gaussian elimination is not optimal". In: *Numerische mathematik* 13.4 (1969), pp. 354–356.

[18] James Joseph (1814-1897) Sylvester. "Sur l'équation en matrices $px = xq$". eng. In: (1912). URL: http://rcin.org.pl/Content/121877/PDF/WA35_145270-11371-4_Art25.pdf.

[19] Zhe-Xian Wan. "A proof of the automorphisms of linear groups over a sfield of characteristic 2". In: *Sci. Sinica* 11 (1962), pp. 1183–1194.