Linear Codes with Constrained Generator Matrices

Thesis by
Hikmet Yildiz

In Partial Fulfillment of the Requirements for the
Degree of
Doctor of Philosophy

CALIFORNIA INSTITUTE OF TECHNOLOGY
Pasadena, California

2021
Defended December 1, 2020

Hikmet Yildiz
ORCID: 0000-0002-0891-3352

To my mother Ayşe,
my father Hasan,
my sister Büşra,
my brother Üsame

ACKNOWLEDGEMENTS

To begin with, I would like to thank my advisor Babak Hassibi. I will truly miss our long discussions on challenging problems. I cannot thank him enough for giving me the freedom, without which, I would not be able to solve any of these problems.

I would like to thank my thesis committee, Prof. Victoria Kostina, Prof. Jehoshua Bruck, and Prof. Christopher Umans for their valuable feedback. It was a great pleasure to have them in my committee.

I would like to thank my lab-mates and collaborators, Fariborz Salehi, Ehsan Abbasi, Anatoly Khina, Oron Sabag, Navid Azizan, Ahmed Douik, Sahin Lale, Taylan Kargin, and Netanel Raviv for the discussions and the fun we had.

I would like to thank my friends Şahin Lale, Oğuzhan Teke, Utkan Candoğan, Sinan Kefeli, Recep Yavaş, Kordağ Kılıç, and Taylan Kargın for making me feel at home.

Last but not least, I would like to thank my mother Ayşe, my father Hasan, my sister Büşra, and my brother Üsame for their love and support.

ABSTRACT

Designing good error correcting codes whose generator matrix has a support constraint, i.e., one for which only certain entries of the generator matrix are allowed to be nonzero, has found many recent applications, including in distributed coding and storage, linear network coding, multiple access networks, and weakly secure data exchange. The dual problem, where the parity check matrix has a support constraint, comes up in the design of locally repairable codes. The central problem here is to design codes with the largest possible minimum distance, subject to the given support constraint on the generator matrix. When the distance metric is the Hamming distance, the codes of interest are Reed-Solomon codes, for which case, the problem was formulated as the "GM-MDS conjecture." In the rank metric case, the same problem can be considered for Gabidulin codes. This thesis provides solutions to these problems and discusses the remaining open problems.

PUBLISHED CONTENT AND CONTRIBUTIONS

[1] H. Yildiz, N. Raviv, and B. Hassibi, "Support constrained generator matrices of Gabidulin codes in characteristic zero," in *2020 IEEE International Symposium on Information Theory (ISIT)*, IEEE, 2020, pp. 60–65. DOI: 10.1109/ISIT44484.2020.9174524,
H.Y. participated in the conception of the project, solved the problem, and participated in the writing of the manuscript.

[2] H. Yildiz and B. Hassibi, "Gabidulin codes with support constrained generator matrices," *IEEE Transactions on Information Theory*, vol. 66, no. 6, pp. 3638–3649, 2019. DOI: 10.1109/TIT.2019.2955106,
H.Y. participated in the conception of the project, solved the problem, and participated in the writing of the manuscript.

[3] ——, "Gabidulin codes with support constraints," in *2019 IEEE Information Theory Workshop (ITW)*, IEEE, 2019, pp. 1–5. DOI: 10.1109/ITW44776.2019.8988992,
H.Y. participated in the conception of the project, solved the problem, and participated in the writing of the manuscript.

[4] ——, "Optimum linear codes with support-constrained generator matrices over small fields," *IEEE Transactions on Information Theory*, vol. 65, no. 12, pp. 7868–7875, 2019. DOI: 10.1109/TIT.2019.2932663,
H.Y. participated in the conception of the project, solved the problem, and participated in the writing of the manuscript.

[5] ——, "Further progress on the GM-MDS conjecture for Reed–Solomon codes," in *2018 IEEE International Symposium on Information Theory (ISIT)*, IEEE, 2018, pp. 16–20. DOI: 10.1109/ISIT.2018.8437308,
H.Y. participated in the conception of the project, solved the problem, and participated in the writing of the manuscript.

[6] ——, "Optimum linear codes with support constraints over small fields," in *2018 IEEE Information Theory Workshop (ITW)*, IEEE, 2018, pp. 1–5. DOI: 10.1109/ITW.2018.8613535,
H.Y. participated in the conception of the project, solved the problem, and participated in the writing of the manuscript.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

Chapter 1

INTRODUCTION

1.1 Motivation

Linear codes are widely used in error correcting since they have efficient encoding and decoding algorithms compared to the other codes. In a block code, a message vector is encoded into a longer vector by introducing some redundancy so that it can be resilient to the errors. For a linear block code, this encoding operation is a linear map. In other words, for each entry in the encoded vector, a weighted sum of the message entries is computed. This requires to have an access to each entry of the message that has a nonzero weight. However, in some scenarios where the encoded vector is computed distributively, there may not be an access to each message symbol from each device that computes a single entry of the encoded vector due to some physical constraints or privacy issues. Therefore, these constraints would require some particular weights in the encoding operation to be zero. Hence, a linear code with these constraints is needed to be designed in these scenarios.

1.2 Background

Linear Block Codes

A linear code $\mathcal{C}$ of length n and dimension k is a k dimensional linear space of the n dimensional space $\mathbb{F}^n$ over a field $\mathbb{F}$. The elements $\mathbf{c} \in \mathcal{C}$ are called the codewords of $\mathcal{C}$. The encoding operation is a linear map, which maps a given message vector $\mathbf{m} \in \mathbb{F}^k$ to a codeword $\mathbf{c} \in \mathcal{C}$. The objective is to send the message $\mathbf{m}$ to a receiver by transmitting the encoded codeword $\mathbf{c}$ through a noise channel. For an additive noise channel, the receiver will receive the vector $\mathbf{y} = \mathbf{c} + \mathbf{e}$ and need to decode the original message $\mathbf{m}$.

The encoding operation in a linear code can be defined in terms of the generator matrix $\mathbf{G} \in \mathbb{F}^{k \times n}$ of the code:

$$\mathbf{c} = \mathrm{enc}(\mathbf{m}) = \mathbf{m}\mathbf{G}. \tag{1.1}$$

The parity check matrix $\mathbf{H} \in \mathbb{F}^{(n-k)\times n}$ is a full rank matrix such that for any codeword $\mathbf{c} \in \mathcal{C}$,

$$\mathbf{H}\mathbf{c}^{\mathsf{T}} = 0. \tag{1.2}$$

Hence, we have that

$$\mathbf{G}\mathbf{H}^{\mathsf{T}} = 0. \tag{1.3}$$

The code itself can be written as the row space of the generator matrix or the null space of the parity check matrix:

$$\mathcal{C} = \mathrm{rowsp}(\mathbf{G}) = \mathrm{null}(\mathbf{H}) \tag{1.4}$$

i.e. the rows of $\mathbf{G}$ define a basis for the code.

The decoding operation usually depends on a distance metric. One such metric is the Hamming distance, which is defined as

$$d_H(\mathcal{C}) = \min_{\mathbf{c}\neq\mathbf{c}'\in\mathcal{C}} \|\mathbf{c}-\mathbf{c}'\|_H \tag{1.5}$$

where $\|\cdot\|_H$ is the Hamming weight, i.e. the number of nonzero entries. For linear codes, it can be also written as

$$d_H(\mathcal{C}) = \min_{0\neq\mathbf{c}\in\mathcal{C}} \|\mathbf{c}\|_H. \tag{1.6}$$

For a code with distance d, if $\|\mathbf{e}\|_H \leq \lfloor \frac{d-1}{2} \rfloor$, the receiver can recover the message uniquely. This distance is upper bounded by the Singleton bound in terms of n and k:

$$d_H(\mathcal{C}) \leq n-k+1. \tag{1.7}$$

The codes that achieve this upper bound are called Maximum Distance Separable (MDS).

Another metric is the rank distance, which is defined in terms of a subfield $\mathbb{F}' \subset \mathbb{F}$. Note that the field $\mathbb{F}$ can be viewed as a vector space over the subfield $\mathbb{F}'$. Then, the rank distance is defined as

$$d_R(\mathcal{C}) = \min_{0\neq c\in\mathcal{C}} \dim_{\mathbb{F}'}(\mathrm{span}_{\mathbb{F}'}\{c_1,\ldots,c_n\}) \tag{1.8}$$

where $c_1,\ldots,c_n \in \mathbb{F}$ represent the entries of $\mathbf{c}\in\mathbb{F}^n$. By fixing an ordered basis of $\mathbb{F}$ over $\mathbb{F}'$, the elements of $\mathbb{F}$ can be considered as vectors with entries from $\mathbb{F}'$; hence the codewords can be viewed as matrices over $\mathbb{F}'$. Then, this definition of the rank distance is equivalent to the minimum of the rank of the matrix representation of a nonzero codeword.

Notice that $\dim_{\mathbb{F}'}(\mathrm{span}_{\mathbb{F}'}\{c_1, \ldots, c_n\})$ can be upper bounded by the number of nonzero c_i's, i.e. $\|\mathbf{c}\|_H$. Hence, we have that

$$d_R(\mathcal{C}) \leq d_H(\mathcal{C}) \leq n - k + 1. \tag{1.9}$$

Therefore, we have the same upper bound for the rank distance as well. The codes that achieve a rank distance $d_R(\mathcal{C}) = n - k + 1$ are called Maximum Rank Distance (MRD).

Reed–Solomon Codes

Reed–Solomon codes are a family of algebraic MDS codes. Their generator matrices can be described by a Vandermonde matrix:

$$\mathbf{V} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{k-1} & x_2^{k-1} & \cdots & x_n^{k-1} \end{bmatrix} \tag{1.10}$$

where $x_1, \ldots, x_n \in \mathbb{F}$ are distinct parameters. In a more general form, a generator matrix of a Reed–Solomon code is

$$\mathbf{G} = \mathbf{TV} \tag{1.11}$$

where $\mathbf{T} \in \mathbb{F}^{k \times k}$ is an invertible transformation matrix. Note that the matrix $\mathbf{T}$ does not change the code itself but the encoding operation (it can be considered as a change of basis for the code).

Gabidulin Codes

Gabidulin codes are the first discovered family of rank metric codes that are MRD. Their generator matrices are in the form of

$$\mathbf{G} = \mathbf{TM} \tag{1.12}$$

where $\mathbf{T} \in \mathbb{F}^{k \times k}$ is an invertible matrix and

$$\mathbf{M} = \begin{bmatrix} x_1^{q^0} & x_2^{q^0} & \cdots & x_n^{q^0} \\ x_1^{q^1} & x_2^{q^1} & \cdots & x_n^{q^1} \\ x_1^{q^2} & x_2^{q^2} & \cdots & x_n^{q^2} \\ \vdots & \vdots & & \vdots \\ x_1^{q^{k-1}} & x_2^{q^{k-1}} & \cdots & x_n^{q^{k-1}} \end{bmatrix} \tag{1.13}$$

where $x_1, \ldots, x_n \in \mathbb{F}$ are linearly independent over the subfield $\mathbb{F}' \subset \mathbb{F}$ and $q = |\mathbb{F}'|$. This definition of Gabidulin codes, as originally defined by Delsarte [7] and Gabidulin [8], is only over the finite fields. Later, they are extended to fields of characteristic zero by replacing the matrix $\mathbf{M}$ above by

$$\mathbf{M} = \begin{bmatrix} \theta^0(x_1) & \theta^0(x_2) & \cdots & \theta^0(x_n) \\ \theta^1(x_1) & \theta^1(x_2) & \cdots & \theta^1(x_n) \\ \vdots & \vdots & & \vdots \\ \theta^{k-1}(x_1) & \theta^{k-1}(x_2) & \cdots & \theta^{k-1}(x_n) \end{bmatrix} \tag{1.14}$$

where $\theta^i(\cdot) = \theta(\theta^{i-1}(\cdot))$ for $i \geq 1$, θ^0 is the identity function, and θ is an automorphism of the cyclic field extension $\mathbb{F}/\mathbb{F}'$ [9]. Note that in the case of finite fields, setting $\theta(x) = x^q$ gives the matrix in (1.13), where $q = |\mathbb{F}'|$.

Conjectures on MDS codes

A linear code is desired to be MDS so that it can be more resilient to the errors. However, MDS codes do not exist over every field. For example, the standard Reed–Solomon codes require a field size of $|\mathbb{F}| \geq n$. The MDS conjecture specifies a bound on the field sizes over which an MDS code exists:

Conjecture 1.1 (MDS Conjecture)**.** *There exists an MDS code of length n and dimension k over a field $\mathbb{F}$ with $k < |\mathbb{F}|$ if and only if either*

(i) $n \leq |\mathbb{F}| + 1$ *and* $2 \leq k \leq |\mathbb{F}| - 1$ *or*

(ii) $n \leq |\mathbb{F}| + 2$*,* $k \in \{3, |\mathbb{F}| - 1\}$*, and* $|\mathbb{F}|$ *is even.*

It is well known that if either of the above conditions is satisfied, then there exist such an MDS code, which is constructed using the generalized Reed–Solomon codes [10] although the correctness of the opposite direction is still unknown.

On the other hand, the GM–MDS conjecture [11] considers the existence of MDS codes when there are additional constraints on the generator matrix of the code. When some particular entries of the generator matrix are required to be zero, a necessary condition (MDS condition, see Definition A.2) for the existence of such an MDS code is described in terms of the required zero pattern [2], [3], [11], [12]. Then, the question is for what field sizes there exists an MDS code with support constrained generator matrices if these constraints satisfy the MDS condition. It is shown that for very large fields ($|\mathbb{F}| \geq \binom{n-1}{k-1}$), the MDS condition is also sufficient

for the existence of MDS codes with constrained generator matrices [11]. The GM–MDS conjecture claims the existence of such MDS codes over much smaller field sizes ($|\mathbb{F}| \geq n + k - 1$):

Conjecture 1.2 (GM–MDS conjecture)**.** *There exists an MDS code of length n and dimension k over a field of size $|\mathbb{F}| \geq n + k - 1$ under a support constraint on the generator matrix if this constraint satisfies the MDS condition.*

1.3 Literature Review

The problem of designing good error correcting codes whose generator matrix has a support constraint, i.e., one for which only certain entries of the generator matrix are allowed to be nonzero, has found many recent applications, including in distributed coding and storage [13], linear network coding [14], multiple access networks [15], and weakly secure data exchange [16], [17]. The dual problem, where the parity check matrix has a support constraint, comes up in the design of locally repairable codes [18]–[20]. In this section, we will review some related problems on the linear codes having a support constraint on their generator matrices.

Distributed Reed–Solomon Codes

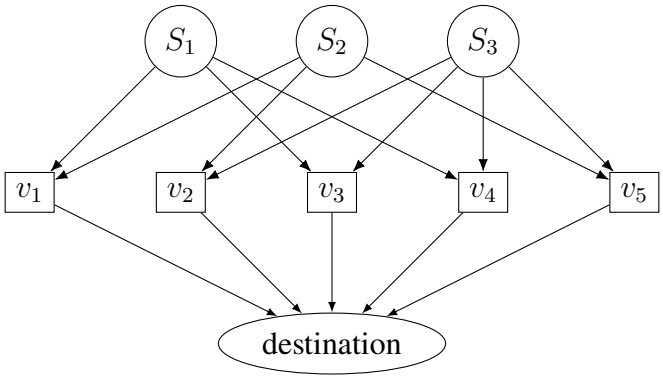

Figure 1.1: A simple multiple access network.

Halbawi *et al.* [13] and Dau *et al.* [15] consider a simple multiple access network (SMAN), where a destination node receives information from multiple source nodes S_i with information rates r_i via a set of relay nodes v_j. While Halbawi *et al.* [13] assumes r_i to be a positive integer, Dau *et al.* [15] further assumes that $r_i = 1$ by showing that the problem can be reduced to this case. If (linear) coding is employed at the relay nodes, each relay node will convey a linear combination of the messages coming only from the source nodes that it has access to, which puts a support constraint on the generator matrix of the code. Furthermore, since the number of

relay errors that can be tolerated is related to the minimum distance of the code, in order to tolerate as many relay errors as possible, one should design a linear code with the largest possible minimum distance under the support constraints on the generator matrix dictated by the network. To achieve this, both of these works use so called distributed Reed–Solomon codes, which are subcodes of Reed–Solomon codes with a generator matrix having a particular zero pattern. However, the existence of such a code relies on the GM–MDS conjecture.

Weakly Secure Cooperative Data Exchange

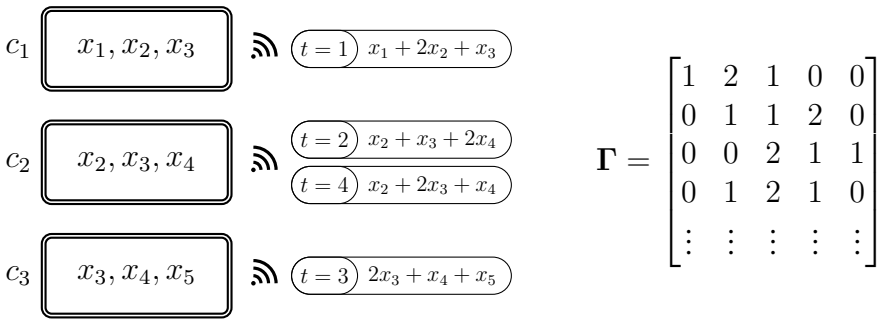

Figure 1.2: At each time, a linear combination of packets is sent by one of the clients. The corresponding encoding matrix is shown on the right.

In the weakly secure data exchange problem [16], [17], a number of clients c_i want to exchange a set of packets x_i by revealing as little information as possible to eavesdroppers. Each client holds a subset of the packets and at each time one of the clients broadcasts a weighted sum of the packets that it possesses. An encoding matrix $\mathbf{\Gamma}$ is defined by these weights such that $\mathbf{\Gamma}_{ij}$ is the coefficient of the packet x_j transmitted at time $t = j$. Since each client has only a subset of the packets, some of these entries are required to be zero, i.e. the matrix $\mathbf{\Gamma}$ has a support constraint. Yan *et al.* [16] showed that minimizing the information that eavesdroppers can capture is equivalent to maximizing the minimum distance of the linear code generated by $\mathbf{\Gamma}^{\mathsf{T}}$. Therefore, this problem is also equivalent to the GM–MDS conjecture [15].

Distributed Gabidulin Codes

In a random linear network, every node passes a random linear combination of the messages it has received to the nodes to which it is connected. In this model, the destination node will get a number of random linear combinations of the messages sent from different sources. Silva *et al.* [21] showed that subspace codes or Gabidulin codes can be used to transfer messages through this network model. In the absence of

errors, the random linear combinations in the network cannot alter the transmitted subspace. In the presence of errors, or adversaries, a few nodes may transmit codewords that are not linear combinations of what they receive. This will alter the subspace by a small rank (given by the number of erroneous nodes or adversaries) and can be corrected by an MRD code. Halbawi *et al.* [14] studied a scenario, where each of the source nodes has access to only a subset of all messages. They showed that so called distributed Gabidulin codes, which are subcodes of Gabidulin codes with generator matrices that have particular zero pattern (depending on what subset each source has access to), can be used under this scenario. They showed the existence and the code design only for networks that have up to 3 source nodes. More specifically, they designed subcodes of Gabidulin codes with the largest rank distance under a support constraint on the generator matrix such that the rows can be divided into 3 groups, where the rows in each group have the same zero pattern.

Partial Results on the GM–MDS conjecture

In the past years, progress had been reported on the GM–MDS conjecture after Dau *et al.* [11] showed that it is equivalent to a simplified conjecture that equates the non-singularity of a matrix with some combinatorial inequalities (See Theorem 2.3). The proof technique that was most commonly employed to attack this new algebraic-combinatorial conjecture was proof by induction. However, the first attempts by researchers were not able to perform the induction step, i.e. to reduce the problem to one of a smaller size, in every case. Therefore, the previous works on this conjecture either gave partial induction steps or were only able to prove it up to a small parameter. For instance, Halbawi *et al.* [13] proved the statement for $m \leq 3$, where m is the number of distinct support sets on the rows of the generator matrix. Yan *et al.* [17] described an induction step only for a special case. Heidarzadeh *et al.* [22] proved the conjecture only for dimensions $k \leq 5$. In our previous work [1], the statement was proven for $m \leq 6$, where m is defined as above. The main idea there was to write a more general problem which enables us to reduce the problem (i.e. apply the induction step) in much broader cases, which also constitutes the main technique we later applied to prove the conjecture. Besides these attempts to proving the conjecture, we should also mention that Halbawi *et al.* [23], [24] and Song *et al.* [25] also studied the problem when the generator matrix is sparsest and balanced (i.e. the numbers of zeros in each row (column) are as large as possible and differ at most by 1) and established the conjecture in this special case.

1.4 Summary of Contributions

This thesis provides a proof for the GM–MDS conjecture and a solution to the rank metric analog of the same problem. In this section, an outline of the main contributions is presented.

Reed–Solomon Codes with Support Constrained Generator Matrices

In Chapter 2, we study the problem of designing optimal linear codes (in terms of having the largest minimum distance) subject to a support constraint on the generator matrix. We show that the largest minimum distance can be achieved by a subcode of a Reed—Solomon code of small field size and with the same minimum distance. In particular, if the code has length n and maximum minimum distance d (over all generator matrices with the given support), then an optimal code exists for any field size $q \geq 2n - d$. As a by-product of this result, we settle the GM–MDS conjecture in the affirmative.

Gabidulin Codes with Support Constrained Generator Matrices

Gabidulin codes are the first general construction of linear codes that are maximum rank distant (MRD). They have found applications in linear network coding, for example, when the transmitter and receiver are oblivious to the inner workings and topology of the network (the so-called incoherent regime). The reason is that Gabidulin codes can be used to map information to linear subspaces, which in the absence of errors cannot be altered by linear operations, and in the presence of errors can be corrected if the subspace is perturbed by a small rank. Furthermore, in distributed coding and distributed systems, one is led to the design of error correcting codes whose generator matrix must satisfy a given support constraint.

In Chapter 3, we give a necessary and sufficient condition on the support of the generator matrix that guarantees the existence of Gabidulin codes and general MRD codes. This condition is identical to the one that appears in the GM–MDS conjecture when the distance metric is the Hamming distance. When this condition is not satisfied, we characterize the largest possible rank distance under the support constraints and show that they can be achieved by subcodes of Gabidulin codes. When the rate of the code is not very high, this is achieved with the same field size necessary for Gabidulin codes with no support constraint.

Gabidulin codes are also recently extended to the fields of characteristic zero by Augot et al. [9], whenever the Galois group of the underlying field extension is cyclic. However, the proof given in Chapter 3 does not apply to the fields of

characteristic zero. Therefore, in Chapter 4, we complete the picture by showing that the same condition is also necessary and sufficient for Gabidulin codes over fields of characteristic zero. Our proof builds upon and extends tools from the finite field case, combines them with a variant of the Schwartz–Zippel lemma over automorphisms, and provides a simple randomized construction algorithm whose probability of success can be arbitrarily close to one. In addition, potential applications for low-rank matrix recovery are discussed.

Chapter 2

SUPPORT CONSTRAINED REED–SOLOMON CODES

2.1 Introduction

The problem of designing a linear code with the largest possible minimum distance, subject to support constraints on the generator matrix, has recently found several applications. These include multiple access networks [13], [15] as well as weakly secure data exchange [16], [17]. In a simple multiple access network [13], [15], a destination node receives information from multiple source nodes via a set of relay nodes. If (linear) coding is employed at the relay nodes, each relay node will convey a linear combination of the messages coming only from the source nodes that it has access to, which puts a support constraint on the generator matrix of the code. Furthermore, since the number of relay errors that can be tolerated is related to the minimum distance of the code, in order to tolerate as many relay errors as possible, one should design a linear code with the largest possible minimum distance under the support constraints on the generator matrix dictated by the network. In the weakly secure data exchange problem [16], [17], a number of clients want to exchange a set of packets by revealing as little information as possible to eavesdroppers. Each transmission is done by one of the clients as a weighted sum of the packets that it possesses. Therefore, one needs to design an encoding matrix representing these weights under a support constraint. Yan *et al.* [16] showed that minimizing the information that eavesdroppers can capture is equivalent to maximizing the minimum distance of the linear code generated by the transpose of this encoding matrix, which has support constraints. We should also mention that support constraints on the generator matrix also arise in distributed storage scenarios where each of the storage elements has access only to a subset of the information to be stored.

A simple upper bound on the minimum distance of a linear code subject to a support constraint on the generator matrix can be obtained through a sequence of Singleton bounds on its subcodes. This upper bound can be achieved (with high probability) by randomly choosing the nonzero elements of the generator matrix from a field of a large enough size. A natural question to ask is whether the above maximum minimum distance can be achieved with a smaller field size, and in particular with a structured, possibly algebraic, construction. This question is equivalent to a

recently proposed conjecture by Dau *et al.* [11], which is commonly referred to as the GM–MDS (generator matrix, maximum distance separable) conjecture [22]. It conjectures the necessary and sufficient conditions for the existence of a Reed–Solomon code with dimension k and length n over a finite field $\mathbb{F}_q$ with $q \geq n+k-1$ under a support constraint on the generator matrix, which enforces certain entries of the generator matrix to be zero. These conditions are actually the same as the necessary and sufficient conditions on the support of a $k \times n$ generator matrix for the existence of a maximum distance separable (MDS) code in some field.

We should mention that when there is no support constraint on the generator matrix, this problem is related to the well-known MDS conjecture, which states that there exists an MDS code with dimension k and length n over $\mathbb{F}_q$ if and only if $n \leq q+1$ for all q and $2 \leq k \leq q-1$, except when q is even and $k \in \{3, q-1\}$, in which case $n \leq q+2$. Although the converse part is still open, the achievability part of the MDS conjecture is well known. In particular, it is known that if the above conditions are satisfied, there exist (extended) generalized Reed–Solomon codes [11].

In the past years, progress had been reported on the GM–MDS conjecture after Dau *et al.* [11] showed that it is equivalent to a simplified conjecture that equates the non-singularity of a matrix with some combinatorial inequalities (See Theorem 2.3). The proof technique that was most commonly employed to attack this new algebraic-combinatorial conjecture was proof by induction. However, researchers were not able to perform the induction step, i.e. to reduce the problem to one of a smaller size, in every case. Therefore, the previous works on this conjecture either gave partial induction steps or were only able to prove it up to a small parameter. For instance, Halbawi *et al.* [13] proved the statement for $m \leq 3$, where m is the number of distinct support sets on the rows of the generator matrix. Yan *et al.* [17] described an induction step only for a special case. Heidarzadeh *et al.* [22] proved the conjecture only for dimensions $k \leq 5$. In our previous work [1], the statement was proven for $m \leq 6$, where m is defined as above. The main idea there was to write a more general problem which enables us to reduce the problem (i.e. apply the induction step) in much broader cases, which also constitutes the main technique used here to prove the conjecture. Besides these attempts to proving the conjecture, we should also mention that Halbawi *et al.* [23], [24] and Song *et al.* [25] also studied the problem when the generator matrix is sparsest and balanced (i.e. the numbers of zeros in each row (column) are as large as possible and differ at most by 1) and established the conjecture in this special case.

In this chapter, we prove the GM–MDS conjecture, namely we show the existence of Reed–Solomon codes in a field of size $q \geq n+k-1$ with dimension k and length n under support constraints on the generator matrix as long as those constraints do not preclude the existence of an MDS code in every field. Furthermore, in general (without any condition on these constraints), we show that the largest minimum distance under support constraints on the generator matrix can be achieved by a subcode of a Reed–Solomon code of small field size, in fact as low as $2n-d$, where n is the code length and d is the maximum minimum distance dictated by the support constraints.

Remark: The results presented in this chapter were first announced in [2]. Concurrently and independently, the GM–MDS conjecture was proven by Lovett in [26]. The two proofs bear some resemblances and exhibit some differences. Both [2] and [26] refer to and build on the earlier paper [1] and define a more general statement than the GM–MDS conjecture that is more amenable to a proof by induction. These statements are mathematically equivalent: In [2], they are expressed in terms of the nonsingularity of a certain generalized Sylvester matrix, whereas in [26], they are expressed as the linear independence of a certain collection of polynomials (the reader may want to compare Theorem 3 in [2] and Theorem 1.7 in [26]). As a consequence, the proof in [2] is more in the language of matrices and that of [26] in the language of polynomials. There are differences in details of the proofs and the order in which statements in the induction arguments are performed, but it is possible to relate the proofs to one another.

Outline

The remainder of this chapter is organized as follows. In Section 2.2, we characterize the generator matrices of subcodes of Reed–Solomon codes. In Section 2.3, we define our main problem, namely maximizing the minimum distance d subject to support constraints on the generator matrix, where we show the achievability of the maximum possible minimum distance d by the subcodes of Reed–Solomon codes by assuming the correctness of the GM–MDS conjecture, which is a special case of our main problem (the MDS case). In Section 2.4, we prove the GM–MDS conjecture by proposing a more general statement than an equivalent conjecture (simplified GM–MDS conjecture) proposed in [11]. Our generalized theorem is not directly related to the coding problem, but more readily lends itself to an inductive argument. In Section 2.5, we discuss potential avenues to obtain explicit code constructions as the GM–MDS conjecture only conjectures the existence of the Reed–Solomon

codes. We conclude in Section 2.6.

Notation

Matrices are shown by bold capital letters and vectors are shown by bold lower case letters. For $n \geq 0$, we denote by $[n]$ the set $\{1, 2, \ldots, n\}$ by admitting $[0] = \emptyset$. For $n \geq 1$, we write $[\theta_i]_{i=1}^n$ to represent the ordered list of objects $\theta_1, \ldots, \theta_n$. For a finite nonempty $S \subset \mathbb{Z}$, $[\theta_i]_{i \in S}$ is the ordered list of θ_i's for $i \in S$ in the ascending order of their indices.

Given a collection of sets $S_1, S_2, \ldots, S_k$, for any nonempty $\Omega \subset [k]$, S_Ω represents the intersection $\bigcap_{i \in \Omega} S_i$.

$\mathbb{F}[x]$ represents the polynomial ring over the field $\mathbb{F}$, i.e. the set of polynomials with coefficients in $\mathbb{F}$. $\mathbb{F}(x)$ represents the field of rational functions in x over the field $\mathbb{F}$, i.e. the set of functions that can be written as a ratio of two polynomials in $\mathbb{F}[x]$ such that the denominator is not the zero polynomial.

When representing multivariate polynomials, for the ease of notation, we usually omit the parameters (e.g. we write p instead of $p(x_1, \ldots, x_n)$).

$[n, k, d]_q$ represent a linear code over $\mathbb{F}_q$ with length n, dimension k, and minimum distance d. In the case of MDS codes, where $d = n - k + 1$, we omit d and write $[n, k]_q$.

2.2 Subcodes of Reed–Solomon Codes

An $[n, \ell]_q$ Reed–Solomon code can be generated by a Vandermonde matrix

$$\mathbf{V} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{\ell-1} & \alpha_2^{\ell-1} & \cdots & \alpha_n^{\ell-1} \end{pmatrix} \in \mathbb{F}_q^{\ell \times n} \tag{2.1}$$

for distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$. Reed–Solomon codes have efficient decoders that can correct up to $\lfloor \frac{n-\ell+1}{2} \rfloor$ errors.

For $n \geq \ell \geq k$, $[n, k, d]_q$ subcodes of $[n, \ell]_q$ Reed–Solomon codes have generator matrices of the following form:

$$\mathbf{G} = \mathbf{T} \cdot \mathbf{V} \tag{2.2}$$

where $\mathbf{T} \in \mathbb{F}_q^{k \times \ell}$ is full rank and $\mathbf{V}$ is given in (2.1). Since the minimum distance of a subcode is at least that of the parent code, we have that $d \geq n - \ell + 1$.

We should mention that every $[n, k, d]_q$ linear code is actually a subcode of an $[n, n]_q$ Reed–Solomon code. However, we are interested in the subcodes of Reed–Solomon codes with the *same* minimum distance as the Reed–Solomon code. In other words, we want to design ℓ, $\mathbf{T}$, and $\mathbf{V}$ such that $d = n - \ell + 1$. Note that in that case, we can use the same decoder of the Reed–Solomon code with the generator matrix $\mathbf{V}$ to correct up to $\lfloor \frac{d}{2} \rfloor$ errors.

2.3 Support Constraint on the Generator Matrix

In this section, first we will derive an upper bound on the minimum distance of a linear code under support constraints on the generator matrix. Then, we will give the GM–MDS conjecture of Dau *et al.*, which claims the existence of Reed–Solomon codes in any field of size $q \geq n + k - 1$ with support constrained generator matrices when this upper bound on the minimum distance is equal to the Singleton bound $(n - k + 1)$. Finally, we will use this conjecture to show that the largest minimum distance is achieved by subcodes of Reed–Solomon codes for any support constraint.

Upper bound on the minimum distance

We will describe the support constraints on the generator matrix $\mathbf{G}$ through the subsets $S_1, S_2, \ldots, S_k \subset [n]$ as follows:

$$\forall i \in [k], \forall j \in S_i, \quad \mathbf{G}_{ij} = 0. \tag{2.3}$$

For any nonempty $\Omega \subset [k]$, the rows of $\mathbf{G}$ indexed in Ω have zeros in all their entries indexed in S_Ω. Consider the submatrix of $\mathbf{G}$ consisting of the rows indexed in Ω and the columns indexed in $[n] - S_\Omega$. The minimum distance d of $\mathbf{G}$ is at most the minimum distance of the code generated by this submatrix, which is at most $n - |S_\Omega| - |\Omega| + 1$ by the Singleton bound. Hence, we have the following upper bound on the minimum distance:

$$d \leq n + 1 - \max_{\emptyset \neq \Omega \subset [k]} (|S_\Omega| + |\Omega|). \tag{2.4}$$

Note that this upper bound is less than or equal to the Singleton bound as $|S_\Omega| + |\Omega| \geq k$ for $\Omega = [k]$.

Existence of MDS codes (GM–MDS conjecture)

For the existence of MDS codes, a straightforward *necessary* condition is that the upper bound in (2.4) is equal to the Singleton bound, i.e.

$$\max_{\emptyset \neq \Omega \subset [k]} (|S_\Omega| + |\Omega|) = k. \tag{2.5}$$

Theorem 2.1, which has been known as the GM–MDS conjecture, declares this as also a *sufficient* condition for the existence of Reed–Solomon codes in any field of size $q \geq n + k - 1$. The proof of Theorem 2.1 is given in Section 2.4.

Theorem 2.1 (GM–MDS Conjecture)**.** *Let $S_1, S_2, \ldots, S_k \subset [n]$ and $q \geq n + k - 1$ be a field size. Then, there exists an $[n, k]_q$ Reed–Solomon code with a generator matrix satisfying (2.3) if and only if for any nonempty $\Omega \subset [k]$,*

$$|S_\Omega| + |\Omega| \leq k. \tag{2.6}$$

$\diamond$

Achievability for any support constraint

Theorem 2.1 can be extended to any support constraint, for which, the upper bound is achieved by the subcodes of Reed–Solomon codes for any field size $q \geq 2n - d$.

Theorem 2.2. *Let $S_1, S_2, \ldots, S_k \subset [n]$,*

$$\ell \triangleq \max_{\emptyset \neq \Omega \subset [k]} (|S_\Omega| + |\Omega|) \tag{2.7}$$

and $q \geq n + \ell - 1$ be a field size. Then, there exists an $[n, k, d]_q$ subcode of a Reed–Solomon code that achieves $d = n - \ell + 1$ with a generator matrix satisfying (2.3). $\diamond$

Proof. For $\Omega = [k]$, we have $\ell \geq k$. Define $S_{k+1}, \ldots, S_\ell = \emptyset$. We can now appeal to Theorem 2.1 which states that there exists an $[n, \ell]_q$ Reed–Solomon code that has a generator matrix $\mathbf{G}'$ such that $\mathbf{G}'_{ij} = 0$ for $j \in S_i, i \in [\ell]$. The subcode with the generator matrix $\mathbf{G}$ consisting of the first k rows of $\mathbf{G}'$ satisfies the desired constraints and has the same minimum distance. $\square$

2.4 Proof of GM–MDS Conjecture

Simplified GM–MDS Conjecture

Dau *et al.* [11] showed that GM–MDS conjecture (Theorem 2.1) is equivalent to the simplified conjecture below, which equates the non-singularity of a matrix with some combinatorial inequalities. We should remark that for the ease of notation, we replaced α_j with $-\alpha_j$ and put the columns in the reversed order in the matrix below unlike the one given in [11] as they do not affect the singularity of the matrix.

Theorem 2.3. *Let $S_1, S_2, \ldots, S_k \subset [n]$ such that $|S_i| = k-1$. Then, the determinant of the $k \times k$ matrix*

$$\begin{pmatrix} 1 & \sum\limits_{j\in S_1} \alpha_j & \cdots & \prod\limits_{j\in S_1} \alpha_j \\ 1 & \sum\limits_{j\in S_2} \alpha_j & \cdots & \prod\limits_{j\in S_2} \alpha_j \\ \vdots & \vdots & & \vdots \\ 1 & \sum\limits_{j\in S_k} \alpha_j & \cdots & \prod\limits_{j\in S_k} \alpha_j \end{pmatrix}, \tag{2.8}$$

where the ith row consists of the coefficients of $\prod_{j\in S_i}(x + \alpha_j)$, is not the zero polynomial if and only if for any nonempty $\Omega \subset [k]$,

$$|S_\Omega| + |\Omega| \leq k. \tag{2.9}$$

$\diamond$

More general theorem

The inequalities in (2.9) are very similar to those given in Hall's marriage theorem, which is proven by induction by considering two cases: (i) the inequality is tight for at least one Ω, (ii) all the inequalities are strict [27]. In order to apply a similar proof technique to Theorem 2.3, it would be favorable to define a more general statement like [1, Conjecture 2], where the first case can be proven more readily. In fact, the induction step for the first case of [1, Conjecture 2] was already given in [1, Lemma 2] of the same paper. However, the induction step for the second case remained incomplete. In this section, we will propose a slightly more general statement (Theorem 2.4) than [1, Conjecture 2], which gives the necessary and sufficient conditions for the singularity of a more general matrix. It is also more general than Theorem 2.3.

Since we are interested in whether a determinant of a matrix, which is a multivariate polynomial, is the zero polynomial or not, it will be easier to work on the field of rational functions and define the matrix in this field. Let $\mathbb{K}_0 = \mathbb{F}_q$ be a finite field and $\mathbb{K}_n = \mathbb{F}_q(\alpha_1, \ldots, \alpha_n)$ be the field of rational functions in $\alpha_1, \ldots, \alpha_n$ over $\mathbb{F}_q$. For $k \geq m \geq 1$ and $n \geq 0$, define

$$\mathcal{S}_{k,m,n} = \left\{ [(S_i, r_i)]_{i=1}^m \middle| \forall i \in [m],\ S_i \subset [n], r_i \in \mathbb{Z}^+, |S_i| + r_i \leq k, \sum_{i=1}^m r_i = k \right\}. \tag{2.10}$$

Define the matrix $\mathbf{M} \in \mathbb{K}_n^{k\times k}$ in terms of the parameters $[(S_i, r_i)]_{i=1}^m \in \mathcal{S}_{k,m,n}$ as follows (we will often write $\mathbf{M}[(S_i, r_i)]_{i=1}^m$ to indicate its parameters):

$$\mathbf{M} = \left(\begin{array}{c} \left.\begin{array}{cccccccc} 1 & \sum\limits_{j\in S_1}\alpha_j & \dots & \prod\limits_{j\in S_1}\alpha_j & 0 & \cdots & & \\ & \ddots & & & \ddots & & & \\ 0 & & 1 & \sum\limits_{j\in S_1}\alpha_j & \dots & \prod\limits_{j\in S_1}\alpha_j & 0 & \cdots \end{array}\right\} r_1 \\ \hline \vdots \\ \hline \left.\begin{array}{cccccccc} 1 & \sum\limits_{j\in S_m}\alpha_j & \dots & \prod\limits_{j\in S_m}\alpha_j & 0 & \cdots & & \\ & \ddots & & & \ddots & & & \\ 0 & & 1 & \sum\limits_{j\in S_m}\alpha_j & \dots & \prod\limits_{j\in S_m}\alpha_j & 0 & \cdots \end{array}\right\} r_m \end{array}\right) \begin{array}{c} \\ \\ \\ \\ \vdots \\ \\ \\ \\ \end{array} .$$

The rows are partitioned into m blocks and for $i \in [m]$, the ith block is an $r_i \times k$ upper triangular Toeplitz matrix, whose first row consists of the coefficients of the polynomial $x^{k-|S_i|-1}\prod_{j\in S_i}(x+\alpha_j)$ in descending order with respect to the degree. This matrix can be also thought of as a generalized Sylvester matrix that is constructed by m polynomials while a classical Sylvester matrix is constructed by the coefficients of only two polynomials (a similar definition of generalized Sylvester matrix is given in [28]–[30]). The condition $|S_i| + r_i \le k$ in (2.10) ensures that the rows are not shifted too much to lose a nonzero entry in the last row of the ith Toeplitz block. Also, notice that the bottom-right entry of the ith block is nonzero iff we have the equality $|S_i| + r_i = k$. We want to point out that the matrix $\mathbf{M}$ above is slightly more general than the one given in [1] since it allows the bottom-right entry to be zero unlike the one in [1], where $|S_i| + r_i = k$ is required for all i.

Theorem 2.4 gives necessary and sufficient conditions on the parameters $[(S_i, r_i)]_{i=1}^m$ for $\det \mathbf{M}$ to be nonzero. Note that letting $k = m$, $r_i = 1$, and $|S_i| = k - 1$ in Theorem 2.4 yields Theorem 2.3.

Theorem 2.4. *Let* $k \ge m \ge 1$, $n \ge 0$, $[(S_i, r_i)]_{i=1}^m \in \mathcal{S}_{k,m,n}$. *Then,* $\det \mathbf{M}[(S_i, r_i)]_{i=1}^m \neq 0$ *if and only if for any nonempty* $\Omega \subset [m]$,

$$|S_\Omega| + \sum_{i\in\Omega} r_i \le \max_{i\in\Omega}(|S_i| + r_i). \tag{2.11}$$

$\diamond$

Remark: We should mention that Theorem 2.4 is mathematically equivalent to Conjecture 2 in [26], where the nonsingularity of $\mathbf{M}$ is replaced by the linear

independence of the polynomials with coefficients defined by the rows of $\mathbf{M}$. Furthermore, these polynomials in [26] are allowed to have repeated zeros at the origin. In fact, the multiplicity of the zeros at the origin is equal to $k - |S_i| - r_i$ in our notation; hence the maximization on the right hand side of (2.11) can be described in terms of the multiplicity of the common zeros at the origin of a collection of these polynomials. Therefore, one can translate the inequalities in (2.11) to the one given in [26].

Before moving to the proof of Theorem 2.4, we will give a useful lemma, where we give an equivalent way of writing $\det \mathbf{M} = 0$ in terms of the polynomials that we use when constructing $\mathbf{M}$.

Lemma 2.1. *Let* $[(S_i, r_i)]_{i=1}^m \in \mathcal{S}_{k,m,n}$. *For* $i \in [m]$, *define*

$$p_i = x^{k-|S_i|-r_i} \prod_{j \in S_i} (x + \alpha_j). \tag{2.12}$$

Then, $\det \mathbf{M}[(S_i, r_i)]_{i=1}^m = 0$ *if and only if there exist* $q_1, \ldots, q_m \in \mathbb{K}_n[x]$, *not all zero, such that* $\deg q_i \leq r_i - 1$ *for* $i \in [m]$ *and* $\sum_{i=1}^m p_i q_i = 0$. $\diamond$

Proof. For each q_i, construct a row vector of size r_i consisting of the coefficients of $x^{r_i-1}, \ldots, x, 1$ in q_i and merge them into one row vector $\mathbf{y} \in \mathbb{K}_n^{1\times k}$. Then, $\sum_{i=1}^m p_i q_i = 0$ iff $\mathbf{y} \cdot \mathbf{M} = 0$. The statement follows from $\det \mathbf{M} = 0$ iff there exists nonzero $\mathbf{y} \in \mathbb{K}_n^{1\times k}$ such that $\mathbf{y} \cdot \mathbf{M} = 0$. $\square$

Proof of Theorem 2.4

Proof of ($\Longrightarrow$)

Suppose that for some nonempty $\Omega \subset [m]$, the condition (2.11) is not true. Let $S_0 = S_\Omega$, $r_0 = \sum_{i\in\Omega} r_i$, $k' = \max_{i\in\Omega}(|S_i| + r_i)$. Then, $|S_0| + r_0 > k'$. Consider the r_0 rows of $\mathbf{M}$ in the blocks indexed in Ω. They all have zeros in their last $k - k'$ entries. Let $\mathbf{M}_0 \in \mathbb{K}_n^{r_0\times k'}$ be the submatrix consisting of these rows without including the last $k - k'$ columns. We will prove that $\operatorname{rank} \mathbf{M}_0 < r_0$, which implies $\det \mathbf{M} = 0$. Let $\mathbf{W} = ((-\alpha_j)^{1-i})_{i\in[k'],j\in S_0}$ be $k' \times |S_0|$ Vandermonde matrix. Then, $\mathbf{M}_0 \cdot \mathbf{W} = 0$ because the polynomials with the coefficients in the rows of $\mathbf{M}_0$ vanish at $-\alpha_j$ for $j \in S_0$. Hence,

$$\operatorname{rank} \mathbf{M}_0 \leq k' - \operatorname{rank} \mathbf{W} \leq k' - \min\{k', |S_0|\} < r_0 \tag{2.13}$$

which proves the first direction.

Proof of ($\Longleftarrow$)

For the other direction, we will apply induction on the parameters (k, m, n) considered in the lexicographical order. For $m = 1$, $\mathcal{S}_{k,1,n} = \{[(\emptyset, k)]\}$ and $\det \mathbf{M}[(\emptyset, k)] = \det \mathbf{I}_k = 1$. For $n = 0$, all of S_i's are empty; hence, for $\Omega = [m]$, (2.11) yields $m = 1$, for which, we already showed $\det \mathbf{M} = 1$.

For $k \geq m \geq 2$ and $n \geq 1$, assume that the statement is true for parameters (k', m', n') that are smaller than (k, m, n) with respect to lexicographical order.

Take any $[(S_i, r_i)]_{i=1}^m \in \mathcal{S}_{k,m,n}$ that satisfies the condition (2.11). We will prove that $\det \mathbf{M}[(S_i, r_i)]_{i=1}^m \neq 0$ under three cases. In fact, under each case, we will try to reduce a parameter and use the induction hypothesis.

1. There exists $\Omega_1 \subset [m]$ such that $2 \leq |\Omega_1| \leq m - 1$ and
$$|S_{\Omega_1}| + \sum_{i \in \Omega_1} r_i = \max_{i \in \Omega_1} (|S_i| + r_i). \tag{2.14}$$
2. There exists a unique $i \in [m]$ such that $|S_i| + r_i = k$.
3. Else (i.e. 1 and 2 are false).

In Case 1, 2, and 3, we will try to reduce the parameters m, k, and n, respectively. Furthermore, in Case 1 and 2, $\det \mathbf{M}$ will be written as a product of two quantities, which are nonzero by the induction hypothesis; whereas in Case 3, it will be shown that substituting $\alpha_j = 0$ in $\det \mathbf{M}$ results in a quantity that is nonzero by the induction hypothesis.

Case 1:

In this case, we will try to reduce the problem into two smaller problems (with smaller m).

Let $\Omega_2 = \{0\} \cup [m] - \Omega_1$. Note that $2 \leq |\Omega_1|, |\Omega_2| \leq m - 1$. Define
$$S_0 = S_{\Omega_1}, \quad r_0 = \sum_{i \in \Omega_1} r_i. \tag{2.15}$$
Then, (2.14) becomes
$$|S_0| + r_0 = \max_{i \in \Omega_1} (|S_i| + r_i). \tag{2.16}$$
Define $S_i' = S_i - S_0$ for $i \in \Omega_1$. Now, we will show that
$$[(S_i', r_i)]_{i \in \Omega_1} \in \mathcal{S}_{r_0, |\Omega_1|, n}, \quad [(S_i, r_i)]_{i \in \Omega_2} \in \mathcal{S}_{k, |\Omega_2|, n}. \tag{2.17}$$

The first one is true because by (2.15), $r_0 = \sum_{i\in\Omega_1} r_i$ and by (2.16), for any $i \in \Omega_1$,

$$|S_i'| + r_i = |S_i| + r_i - |S_0| \le r_0. \tag{2.18}$$

The second one is true because by (2.10), (2.15), and the definition of Ω_2,

$$k = \sum_{i=1}^{m} r_i = r_0 + \sum_{i\in[m]-\Omega_1} r_i = \sum_{i\in\Omega_2} r_i, \tag{2.19}$$

$|S_i| + r_i \le k$ for $i \in [m] - \Omega_1$ and $|S_0| + r_0 \le k$ due to (2.16).

By the induction hypothesis, the statement is true for $[(S_i', r_i)]_{i\in\Omega_1}$ and $[(S_i, r_i)]_{i\in\Omega_2}$. We will show that both satisfy the condition (2.11):

1. For any nonempty $\Omega \subset \Omega_1$,

$$\begin{aligned} |S_\Omega'| + \sum_{i\in\Omega} r_i &= |S_\Omega| - |S_0| + \sum_{i\in\Omega} r_i \\ &\le \max_{i\in\Omega}(|S_i| + r_i) - |S_0| \\ &= \max_{i\in\Omega}(|S_i'| + r_i) \end{aligned}$$

   where the first and last equalities are by definition of the S_i''s and the inequality is due to (2.11).

2. For any nonempty $\Omega \subset \Omega_2$, if $0 \notin \Omega$, then $\Omega \subset [m]$ and (2.11) holds trivially. Assume $\Omega = \{0\} \cup \Omega'$ for some $\Omega' \subset [m] - \Omega_1$. Then,

$$\begin{aligned} |S_\Omega| + \sum_{i\in\Omega} r_i &= |S_0 \cap S_{\Omega'}| + r_0 + \sum_{i\in\Omega'} r_i \\ &= |S_{\Omega_1\cup\Omega'}| + \sum_{i\in\Omega_1\cup\Omega'} r_i \\ &\le \max_{i\in\Omega_1\cup\Omega'}(|S_i| + r_i) \\ &= \max\{\max_{i\in\Omega_1}(|S_i| + r_i), \max_{i\in\Omega'}(|S_i| + r_i)\} \\ &= \max\{(|S_0| + r_0), \max_{i\in\Omega'}(|S_i| + r_i)\} \\ &= \max_{i\in\Omega}(|S_i| + r_i) \end{aligned}$$

   where the first and last equalities are due to $\Omega = \{0\} \cup \Omega'$, the second equality is due to (2.15), the inequality is due to (2.11), and the fourth equality is due to (2.16).

Hence, both $[(S_i', r_i)]_{i\in\Omega_1}$ and $[(S_i, r_i)]_{i\in\Omega_2}$ satisfy (2.11) and by the induction hypothesis, we have that

$$\det \mathbf{M}[(S_i', r_i)]_{i\in\Omega_1} \neq 0, \quad \det \mathbf{M}[(S_i, r_i)]_{i\in\Omega_2} \neq 0. \tag{2.20}$$

Now, we will use Lemma 2.1 to show that $\det \mathbf{M}[(S_i, r_i)]_{i=1}^m \neq 0$ (In fact, without appealing to Lemma 2.1, one can show that this determinant is the product of the two determinants in (2.20) by using row operations). Define for $i \in \{0\} \cup [m]$,

$$p_i = x^{k-|S_i|-r_i} \prod_{j\in S_i} (x + \alpha_j) \tag{2.21}$$

and for $i \in \Omega_1$,

$$p_i' = x^{r_0-|S_i'|-r_i} \prod_{j\in S_i'} (x + \alpha_j). \tag{2.22}$$

Note that for $i \in \Omega_1$, $p_i = p_i' p_0$.

Consider any $q_1, \ldots, q_m \subset \mathbb{K}_n[x]$ such that $\deg q_i \leq r_i - 1$ for $i \in [m]$ and $\sum_{i=1}^m p_i q_i = 0$. We need to prove that $q_i = 0$ for all $i \in [m]$. Define

$$q_0 = \sum_{i\in\Omega_1} p_i' q_i. \tag{2.23}$$

Note that $\deg q_0 \leq r_0 - 1$:

$$\deg q_0 \leq \max_{i\in\Omega_1} (\deg p_i' + \deg q_i) \tag{2.24}$$

$$\leq \max_{i\in\Omega_1} ((r_0 - r_i) + (r_i - 1)) \tag{2.25}$$

$$= r_0 - 1. \tag{2.26}$$

Also, we can write that

$$0 = \sum_{i=1}^m p_i q_i = p_0 \sum_{i\in\Omega_1} p_i' q_i + \sum_{i\in[m]-\Omega_1} p_i q_i = \sum_{i\in\Omega_2} p_i q_i. \tag{2.27}$$

Then, by Lemma 2.1, we get $q_i = 0$ for all $i \in \Omega_2$. Then, $q_0 = \sum_{i\in\Omega_1} p_i' q_i = 0$. Then, by Lemma 2.1, $q_i = 0$ for all $i \in \Omega_1$. Hence, $q_i = 0$ for all $i \in [m]$. By Lemma 2.1, $\det \mathbf{M}[(S_i, r_i)]_{i=1}^m \neq 0$.

Case 2:

In this case, we will try to reduce the parameter k.

W.l.o.g., let m be the unique i such that $|S_i| + r_i = k$. Then, for $i \in [m-1]$,

$$k = |S_m| + r_m > |S_i| + r_i. \tag{2.28}$$

Then, by the definition of $\mathbf{M}$, the last column of $\mathbf{M}[(S_i, r_i)]_{i=1}^m$ is all zero except the last entry, which is $\prod_{j \in S_m} \alpha_j$.

Notice that the upper left $(k-1) \times (k-1)$ block of $\mathbf{M}[(S_i, r_i)]_{i=1}^m$ actually defines another matrix $\mathbf{M}$ with different parameters. More precisely, we have that

$$\det \mathbf{M}[(S_i, r_i)]_{i=1}^m = \det \mathbf{M}[(S_i, r_i')]_{i=1}^m \cdot \prod_{j \in S_m} \alpha_j \tag{2.29}$$

where $r_m' = r_m - 1$ and $r_i' = r_i$ for $i \in [m-1]$ assuming that $r_m \geq 2$. (If $r_m = 1$, the first multiplier above would be replaced by $\det \mathbf{M}[(S_i, r_i)]_{i=1}^{m-1}$, which would be nonzero by the induction hypothesis, and we would be done.)

Note that $[(S_i, r_i')]_{i=1}^m \in \mathcal{S}_{k-1,m,n}$ since $\sum_{i=1}^m r_i' = k-1$ and $|S_i| + r_i' \leq k-1$ for any $i \in [m]$ due to (2.28).

By the induction hypothesis, the statement is true for $[(S_i, r_i')]_{i=1}^m$. Hence, all we need to prove is that $[(S_i, r_i')]_{i=1}^m$ satisfies (2.11) to conclude by (2.29) that

$$\det \mathbf{M}[(S_i, r_i')]_{i=1}^m \neq 0 \implies \det \mathbf{M}[(S_i, r_i)]_{i=1}^m \neq 0.$$

For any nonempty $\Omega \subset [m]$, if $m \notin \Omega$, then (2.11) holds trivially. Assume $m \in \Omega$.

$$|S_\Omega| + \sum_{i \in \Omega} r_i' = |S_\Omega| - 1 + \sum_{i \in \Omega} r_i \tag{2.30}$$

$$\leq \max_{i \in \Omega} (|S_i| + r_i) - 1 \tag{2.31}$$

$$= k - 1 \tag{2.32}$$

$$= \max_{i \in \Omega} (|S_i| + r_i') \tag{2.33}$$

where the first equality is by definition of r_i', the inequality is due to (2.11), and the second and last equalities are by (2.28).

Case 3:

In this case, we will try to reduce the parameter n by removing an element j from all the sets containing it and substituting $\alpha_j = 0$ in the matrix $\mathbf{M}$.

Since Case 1 is false, for any nonempty $\Omega \subset [m]$ such that $|\Omega| \neq 1, m$, we have

$$|S_\Omega| + \sum_{i \in \Omega} r_i \leq \max_{i \in \Omega} (|S_i| + r_i) - 1. \tag{2.34}$$

Since Case 2 is false, there exist at least two values of i such that $|S_i| + r_i = k$. W.l.o.g., assume that

$$k = |S_m| + r_m = |S_{m-1}| + r_{m-1}. \tag{2.35}$$

If $S_m = S_{m-1}$, we get a contradiction in (2.11) for $\Omega = \{m, m-1\}$:

$$r_m + r_{m-1} \leq \max\{r_m, r_{m-1}\}. \tag{2.36}$$

Then, either $S_{m-1} \neq [n]$ or $S_m \neq [n]$. W.l.o.g., we can assume that $n \notin S_m$.

By the definition of matrix $\mathbf{M}$, notice that substituting $\alpha_n = 0$ in the matrix $\mathbf{M}[(S_i, r_i)]_{i=1}^m$ will only remove the element n from all the S_i's containing n. Hence,

$$\det \mathbf{M}[(S_i, r_i)]_{i=1}^m|_{\alpha_n=0} = \det \mathbf{M}[(S_i', r_i)]_{i=1}^m \tag{2.37}$$

where $S_i' = S_i - \{n\}$.

Note that $[(S_i', r_i)]_{i=1}^m \in \mathcal{S}_{k,m,n-1}$ since $S_i' \subset [n-1]$ and $|S_i'| + r_i \leq |S_i| + r_i \leq k$ for $i \in [m]$.

By the induction hypothesis, the statement is true for $[(S_i', r_i)]_{i=1}^m$. Hence, all we need to prove is that $[(S_i', r_i)]_{i=1}^m$ satisfies (2.11) to conclude by (2.37) that

$$\det \mathbf{M}[(S_i', r_i)]_{i=1}^m \neq 0 \implies \det \mathbf{M}[(S_i, r_i)]_{i=1}^m \neq 0.$$

For $|\Omega| = 1$, (2.11) holds trivially. For $|\Omega| \neq 1, m$, we have

$$|S_\Omega'| + \sum_{i\in\Omega} r_i \leq |S_\Omega| + \sum_{i\in\Omega} r_i \tag{2.38}$$

$$\leq \max_{i\in\Omega}(|S_i| + r_i) - 1 \tag{2.39}$$

$$\leq \max_{i\in\Omega}(|S_i'| + r_i) \tag{2.40}$$

where the first and last inequalities follow trivially by the definition of the S_i's and the second inequality is due to (2.34).

For $\Omega = [m]$, it is sufficient to show that $k = \max_{i\in[m]}(|S_i'| + r_i)$, which is true because

$$|S_m'| + r_m = |S_m| + r_m = k. \tag{2.41}$$

□

2.5 Discussion of Explicit Constructions

Since a linear code achieving the maximum minimum distance under support constraints on the generator matrix can be designed as a subcode of a Reed–Solomon code as described in the proof of Theorem 2.2, we can focus on designing Reed–Solomon codes with support constraints satisfying the conditions in (2.6). As shown

in [11], this is equivalent to finding distinct $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$ such that the matrix in (2.8) is nonsingular. However, our result only guarantees the *existence* of these evaluation points. Hence, to design the code, explicit construction of them still remains to be studied.

Since our proof is inductive, one may hope that it can be used to recursively generate suitable α_i. Unfortunately, we have not been able to do so. To see why, denote $\det \mathbf{M}$ by the multivariate polynomial $F(\alpha_1, \ldots, \alpha_n)$, and note that in Case 1 of the proof of Theorem 2.4, $F(\alpha_1, \ldots, \alpha_n)$ is nonzero if two determinants, corresponding to smaller problems (with smaller m), $F_1(\alpha_1, \ldots, \alpha_n)$ and $F_2(\alpha_1, \ldots, \alpha_n)$ are nonzero. While each of these two determinants can then be studied separately, the fact that they share variables means that we need to find α_i that makes both determinants nonzero simultaneously. This creates a roadblock stopping us from having a recursive construction.

In the absence of an explicit construction, one can of course choose $\alpha_i \in \mathbb{F}_q$ at random and evaluate $\det \mathbf{M}$ until a nonzero determinant is found. Currently, we do not know whether this will efficiently find a suitable set of α_i's or whether it will require something akin to an exhaustive search.

Explicit constructions have been obtained in the literature for special instances of the problem: notably in [23]–[25] when the support constraints are sparsest and balanced (i.e. the numbers of zeros in each row (and column) are as large as possible and differ at most by 1), and in [31] when the sets are further required to satisfy $|S_{[i]}| \leq k - i$ for every $i \in [k]$.

2.6 Conclusion

We have established an upper bound on the minimum distance of linear codes with support constraints on the generator matrix by applying a sequence of Singleton bounds and have shown that it can be achieved by a subcode of a Reed–Solomon code of the same minimum distance, as long as the field size is not smaller than $2n - d$, by proving a more general statement than the GM–MDS conjecture (namely, Theorem 2.4). The work presented here suggests some research directions that should be fruitful to further explore. We briefly describe some of them.

First as discussed in Section V, our result only ensures the *existence* of evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n$ for which we can design a subcode of a Reed–Solomon code. Finding an efficient deterministic algorithm which explicitly finds these evaluation points would be of interest. At present, the best one can do is to choose the

$\alpha_1, \alpha_2, \ldots, \alpha_n$ at random and check whether the matrix $\mathbf{M}$ is full rank.

A second direction is the dual problem, where the support constraints are on the parity check matrix. In other words, we would like to find a code with the largest possible minimum distance, subject to support constraints on the parity check matrix. A special case of this problem has been studied in the context of locally repairable codes [18]–[20]. For example, when the repair sets are all of equal sizes, this imposes a very particular structure on the parity check matrix and it has been shown that the optimal code is a subcode of a Reed Solomon code of the same minimum distance [18]. In the case of general support constraints, it is not hard to derive an upper bound on the minimum distance that is achievable by a random code, which requires large field sizes and potentially does not have an efficient decoder. Therefore, a question one may ask is whether one can design an algebraic code on a small field size with a minimum distance that achieves the upper bound. If the code is MDS, the problem is clearly equivalent to the one we have studied here. However, if the support constraints on the parity check matrix preclude the existence of a MDS code, then the question of whether such an algebraic code exists remains open.

Another interesting question is whether it is possible to further reduce the field size by considering other code families with or without sacrificing the minimum distance. For instance, it might be worth looking at whether algebraic–geometric codes can be designed with support constrained generator matrices with a desired minimum distance and field size.

Finally, one may consider the problem of maximizing a different distance metric (instead of Hamming distance) of the code under a given support constraint. For instance, the rank metric is studied in [5], where it is shown that the same conditions are necessary and sufficient for the existence of Gabidulin codes by extending the proof used in this chapter. It remains open to study other distance metrics as well.

Chapter 3

SUPPORT CONSTRAINED GABIDULIN CODES OVER FINITE FIELDS

3.1 Introduction

Linear codes are desired to have the maximum minimum distance, for some distance measure, in order to be more resistant to errors in the channel. If the objective is to detect and correct as many error symbols as possible, the distance measure to be used is the Hamming distance. The Singleton bound $(n-k+1)$ is an upper bound on the largest value for the minimum Hamming distance d_H a code can have, where n is the length and k is the dimension of the code. Codes achieving it are called Maximum Distance Separable (MDS) codes and a well known example for an MDS code is the Reed–Solomon code. The necessary and sufficient conditions for the existence of Reed–Solomon codes in terms of the zero structure of the generator matrix were conjectured by Dau *et al.* [11], and referred to as the GM-MDS conjecture, which was worked on by many researchers in [1], [13], [15], [17], [22]–[25], [31] and finally proved in our previous work [2] and in the independent work of Lovett [26].

In some other scenarios, different distance metrics can be more desirable. For instance, the rank distance, d_R, is another metric which can be used to design linear codes in random linear network coding or in scenarios where the transmitter and receiver are oblivious to the topology and inner workings of the network (this is often called the incoherent regime). To see why, suppose the code is defined over an extension field $\mathbb{F}_{q^s}$, which can be thought of as a vector space over a base field $\mathbb{F}_q$, then the rank of a codeword in $\mathbb{F}_{q^s}^n$ is defined as the dimension of the span of the entries of the codeword over $\mathbb{F}_q$. Since the dimension of the span is at most the number of nonzero elements, we have $d_R \leq d_H$. Hence, a similar Singleton bound $(n-k+1)$ can be derived for the largest rank distance for a fixed code length n and dimension k. A code achieving this is called a Maximum Rank Distance (MRD) code and Gabidulin codes due to Delsarte [7] and Gabidulin [8] are the first general constructions of it. These codes require a field size of q^s, with $s \geq n$. Very recently, a new class of MRD codes, called twisted Gabidulin codes, have been constructed by Sheekey [32], which have been further generalized in [33]–[35].

In a random linear network, every node passes a random linear combination of the

messages it has received to the nodes to which it is connected. In this model, the destination node will get a number of random linear combinations of the messages sent from different sources. Silva *et al.* [21] showed that subspace codes or Gabidulin codes can be used to transfer messages through this network model. In the absence of errors, the random linear combinations in the network cannot alter the transmitted subspace. In the presence of errors, or adversaries, a few nodes may transmit codewords that are not linear combinations of what they receive. This will alter the subspace by a small rank (given by the number of erroneous nodes or adversaries) and can be corrected by an MRD code. Halbawi *et al.* [14] studied a scenario, where each of the source nodes has access to only a subset of all messages. They showed that subcodes of Gabidulin codes with generator matrices that have a particular zero pattern (depending on what subset each source has access to) can be used under this scenario. However, they showed the existence and the code design only for networks that have up to 3 source nodes. More specifically, they designed subcodes of Gabidulin codes with the largest rank distance under a support constraint on the generator matrix such that the rows can be divided into 3 groups, where the rows in each group have the same zero pattern.

In this chapter, we will give necessary and sufficient conditions for the existence of Gabidulin codes with support constrained generator matrices. Furthermore, if these constraints are not satisfied, we show that the largest possible rank distance can be achieved by subcodes of Gabidulin codes. Our result generalizes the result in [14] to any number of source nodes in the network. The necessary and sufficient conditions on the support constraints to guarantee the existence of Gabidulin codes and general MRD codes is identical to the conditions for MDS codes (that was recently established in [2], [26] in the context of the GM-MDS conjecture). Furthermore, the field size is now q^s, with $s \geq \max\{n, k-1+\log_q k\}$. When the rate of the code is not too large ($r = \frac{k}{n} \leq 1 - \frac{\log_q k - 1}{n}$), there is no penalty in field size compared to a Gabidulin code with no support constraints.

The rest of the chapter is organized as follows. In Section 3.2, after defining the rank metric and characterizing the generator matrices of Gabidulin codes, we define our problem, namely finding necessary and sufficient conditions for the existence of the Gabidulin codes with support constrained generator matrices. Then, we solve this problem by relying on a claim (Claim 3.1). Section 3.3 then proposes a purely algebraic problem on linearized polynomials that contains a more general theorem than Claim 3.1 and provides a detailed proof. The advantage of the generalization

is that it lends itself to proof by induction. Finally, we conclude in Section 3.4.

3.2 Gabidulin Codes with Support Constraints

In this section, first we will define the rank distance of a linear code, show its relation with the Hamming distance, and give its largest possible value in terms of the length n and dimension k of the code. Secondly, we will write some necessary conditions on the support of the generator matrix of a code for the rank distance to achieve this largest possible value. Thirdly, we will characterize the generator matrices of Gabidulin codes, which achieve the largest possible rank distance. Then, we will prove that those necessary conditions are also sufficient for the existence of Gabidulin codes, which is the main result in this chapter. Our proof relies on a claim (Claim 3.1), which will be proven in Section 3.3, and constitutes the major technical contribution of our work.

Rank distance

Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_{q^s}$ be an extension field of $\mathbb{F}_q$. Then, $\mathbb{F}_{q^s}$ forms a linear space over $\mathbb{F}_q$. Hence, for any $c = (c_1, \ldots, c_n) \in \mathbb{F}_{q^s}^n$, we can define the rank of c as

$$\mathrm{rank}(c) = \dim(\mathrm{span}\{c_1, \ldots, c_n\}). \tag{3.1}$$

Note that $\mathrm{rank}(c)$ is at most the Hamming weight of c, i.e. the number of nonzero entries of c:

$$\mathrm{rank}(c) \leq \|c\|_H. \tag{3.2}$$

Let $\mathcal{C} \subset \mathbb{F}_{q^s}^n$ be a linear code with $\dim \mathcal{C} = k$. The rank distance of $\mathcal{C}$ is defined as

$$d_R = \min_{0 \neq c \in \mathcal{C}} \mathrm{rank}(c). \tag{3.3}$$

Then, by (3.2), the rank distance is less than or equal to the Hamming distance:

$$d_R \leq d_H. \tag{3.4}$$

Hence, the Singleton bound on d_H also holds for the rank distance: $d_R \leq n - k + 1$. The codes achieving this bound are called Maximum Rank Distance (MRD) codes.

Remark 3.1. An MRD–code is also an MDS–code, but the opposite is not true in general.

Support constraints (zero constraints)

Suppose that we want to design an MRD–code under a support constraint on the generator matrix $\mathbf{G} \in \mathbb{F}_{q^s}^{k \times n}$. We describe these support constraints through the

subsets $\mathcal{Z}_1, \mathcal{Z}_2, \ldots, \mathcal{Z}_k \subset [n]$ as follows:

$$\forall i \in [k],\ \forall j \in \mathcal{Z}_i, \quad \mathbf{G}_{ij} = 0. \tag{3.5}$$

It is well known [2], [11], [26] that a necessary condition for a code to be MDS is

$$\left| \bigcap_{i \in \Omega} \mathcal{Z}_i \right| + |\Omega| \leq k \tag{3.6}$$

for all nonempty $\Omega \subset [k]$. Hence, (3.6) is also *necessary* for the existence of MRD–codes by Remark 3.1. Later, we will show that it is also a *sufficient* condition to design MRD–codes for fields of size q^s, with $s \geq \max\{n, k - 1 + \log_q k\}$.

Note that for $\Omega = \{i\}$, we have $|\mathcal{Z}_i| \leq k-1$. In [11, Theorem 2], Dau *et al.* showed that one can add elements from $[n]$ to each of these subsets until each has exactly $k-1$ elements by preserving (3.6) (we also provide a different proof in Chapter A). Note that this operation will only put more zero constraints on $\mathbf{G}$, but will not remove any. This means that the code we design under the new constraints will also satisfy the original constraints. Therefore, without loss of generality, along with (3.6), we will further assume that

$$|\mathcal{Z}_i| = k - 1, \quad \forall i \in [k]. \tag{3.7}$$

Gabidulin codes

Gabidulin codes were introduced in [7] and [8] and are the first general constructions (meaning for any n and k) of an MRD code. Their generator matrices are of the following form:

$$\mathbf{G}_{\text{GC}} = \begin{pmatrix} \alpha_1^{q^0} & \alpha_2^{q^0} & \cdots & \alpha_n^{q^0} \\ \alpha_1^{q^1} & \alpha_2^{q^1} & \cdots & \alpha_n^{q^1} \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{k-1}} & \alpha_2^{q^{k-1}} & \cdots & \alpha_n^{q^{k-1}} \end{pmatrix} \in \mathbb{F}_{q^s}^{k \times n} \tag{3.8}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_{q^s}$ are linearly independent over $\mathbb{F}_q$ and hence, $s \geq n$. We remark that the linear independence of the α_i's over $\mathbb{F}_q$ is equivalent to the linear independence of any k columns of $\mathbf{G}_{\text{GC}}$ over $\mathbb{F}_{q^s}$ [36, Lemma 3.51]. This matrix is also known as the Moore matrix.

Furthermore, multiplying $\mathbf{G}_{\text{GC}}$ by an invertible matrix from the left will not change the code (i.e. the row span), but will only change the basis:

$$\mathbf{G} = \mathbf{T} \cdot \mathbf{G}_{\text{GC}} \tag{3.9}$$

where $\mathbf{T} \in \mathbb{F}_{q^s}^{k\times k}$ is full rank. Hence, $\mathbf{G}$ can be also used as a generator matrix of the same Gabidulin code. This will allow us to introduce zeros at the desired positions on the generator matrix.

Notice that if we define the polynomials

$$f_i(x) = \sum_{j=1}^{k} \mathbf{T}_{ij} x^{q^{j-1}} \tag{3.10}$$

for $i \in [k]$, then the entries of $\mathbf{G}$ will be the values of the f_i's evaluated at the α_j's i.e. $\mathbf{G}_{ij} = f_i(\alpha_j)$. Then, the support constraints in (3.5) on $\mathbf{G}$ will become root constraints on the f_i's:

$$\forall i \in [k],\ \forall j \in \mathcal{Z}_i, \quad f_i(\alpha_j) = 0. \tag{3.11}$$

In view of the above, the question we would like to ask is whether under condition (3.6), there exist an invertible matrix $\mathbf{T}$ and linearly independent $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_{q^s}$ such that (3.11) holds. In other words, since $\mathbf{T}$ is invertible, $\mathbf{G}$ has the same MRD property of $\mathbf{G}_{\text{GC}}$, and also satisfies the support constraints in (3.5).

We should mention that a similar question for the existence of MDS codes with support constraints on the generator matrix was asked by [11] and was referred to as the GM–MDS conjecture. This was recently resolved in [2] and [26], where it was shown that under (3.6), MDS codes with small fields size could be constructed using Reed–Solomon codes. This chapter can be viewed as an extension of that result to rank-metric codes and Gabidulin codes.

Example

Let $q = 2, s = 4, k = 3, n = 4$. Suppose we have the following support constraints: $\mathcal{Z}_1 = \{1, 2\}, \mathcal{Z}_2 = \{2, 3\}, \mathcal{Z}_3 = \{3, 4\}$, i.e.,

$$\mathbf{G} = \begin{pmatrix} 0 & 0 & \times & \times \\ \times & 0 & 0 & \times \\ \times & \times & 0 & 0 \end{pmatrix}. \tag{3.12}$$

Note that these constraints satisfy (3.6). We need to find $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{F}_{16}$ that are linearly independent over $\mathbb{F}_2$ and an invertible matrix $\mathbf{T} \in \mathbb{F}_{16}^{3\times 3}$ such that

$$\mathbf{T} \cdot \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 \\ \alpha_1^4 & \alpha_2^4 & \alpha_3^4 & \alpha_4^4 \end{pmatrix} = \begin{pmatrix} 0 & 0 & \times & \times \\ \times & 0 & 0 & \times \\ \times & \times & 0 & 0 \end{pmatrix}. \tag{3.13}$$

The following matrix satisfies these zero constraints (later, we will show that this matrix is actually unique up to a scaling):

$$\mathbf{T} = \begin{pmatrix} \alpha_1\alpha_2(\alpha_1+\alpha_2) & \alpha_1^2+\alpha_2^2+\alpha_1\alpha_2 & 1 \\ \alpha_2\alpha_3(\alpha_2+\alpha_3) & \alpha_2^2+\alpha_3^2+\alpha_2\alpha_3 & 1 \\ \alpha_3\alpha_4(\alpha_3+\alpha_4) & \alpha_3^2+\alpha_4^2+\alpha_3\alpha_4 & 1 \end{pmatrix}. \tag{3.14}$$

Let us choose $\alpha_1 = 1, \alpha_2 = a, \alpha_3 = a^2, \alpha_4 = a^3$ in $\mathbb{F}_{16}$ with the primitive polynomial $a^4 + a + 1$. Then, they are linearly independent over $\mathbb{F}_2$ and $\det \mathbf{T} = a^{13} \neq 0$; so, $\mathbf{T}$ is invertible. Therefore,

$$\mathbf{G} = \begin{pmatrix} 0 & 0 & a^{10} & a^3 \\ a^7 & 0 & 0 & a^{14} \\ a^5 & a^{11} & 0 & 0 \end{pmatrix} \tag{3.15}$$

is the generator matrix for a Gabidulin code, which satisfies the support constraints.

Note that there are other choices of the α_i that can solve our problem, too. However, the primary focus of this chapter will be to show the existence of such a choice in general.

Linearized polynomials

Polynomials in the form of (3.10) are called *linearized polynomials* (q-polynomials) and it is beneficial to give some of their properties before moving forward. First, we should note that for any $a, b \in \mathbb{F}_{q^s}$ and $i \geq 0$, we have that $(a+b)^{q^i} = a^{q^i} + b^{q^i}$, which is commonly referred to as the *Freshman's Dream* [37]. Furthermore, for any $\gamma \in \mathbb{F}_q$, we have that $\gamma^{q^i} = \gamma$. Therefore, any linearized polynomial in the form of

$$f(x) = \sum_{i=0}^{d} c_i x^{q^i}, \quad c_i \in \mathbb{F}_{q^s} \tag{3.16}$$

is actually a linear map $f : \mathbb{F}_{q^s} \to \mathbb{F}_{q^s}$ when $\mathbb{F}_{q^s}$ is considered as a linear space over $\mathbb{F}_q$. Hence, the roots of f form a subspace over $\mathbb{F}_q$.

Conversely, it can be shown that for any subspace $V \subset \mathbb{F}_{q^s}$, the polynomial

$$f(x) = \prod_{\beta \in V} (x - \beta) \tag{3.17}$$

is a linearized polynomial, i.e. after expanding the product, the monomials whose exponent is not a power of q will vanish [36, Theorem 3.52].

The q-degree of the linearized polynomial f in (3.16) is defined as $\deg_q f = d$ if $c_d \neq 0$. Then, the q-degree of f in (3.17) can be expressed as $\deg_q f = \dim V$.

We will now move on to our main problem and later revisit linearized polynomials in Section 3.3, where more of their properties will be given.

Existence of Gabidulin codes

Note that by the definition in (3.10), we have $\deg_q f_i \leq k-1$. Furthermore, since the α_j's are assumed to be linearly independent, by (3.7) and (3.11), each f_i is enforced to have $|\mathcal{Z}_i| = k-1$ linearly independent roots. Therefore, the $f_1, \ldots, f_k$ are uniquely defined up to a scaling, and so in monic form

$$f_i(x) = \prod_{\beta \in \text{span}\{\alpha_j : j \in \mathcal{Z}_i\}} (x - \beta), \tag{3.18}$$

which, in turn, uniquely determines all the entries of $\mathbf{T}$ in terms of $\alpha_1, \ldots, \alpha_n$ due to (3.10).

Then, the problem becomes finding linearly independent $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^s}$ over $\mathbb{F}_q$ such that $\det \mathbf{T} \neq 0$. In other words, we need to find $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^s}$ such that

$$F(\alpha_1, \ldots, \alpha_n) \triangleq F_1(\alpha_1, \ldots, \alpha_n) F_2(\alpha_1, \ldots, \alpha_n) \neq 0 \tag{3.19}$$

where

$$F_1(\alpha_1, \ldots, \alpha_n) = \det \mathbf{T} \tag{3.20}$$

$$F_2(\alpha_1, \ldots, \alpha_n) = \begin{vmatrix} \alpha_1^{q^0} & \alpha_2^{q^0} & \cdots & \alpha_n^{q^0} \\ \alpha_1^{q^1} & \alpha_2^{q^1} & \cdots & \alpha_n^{q^1} \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \cdots & \alpha_n^{q^{n-1}} \end{vmatrix} \tag{3.21}$$

because α_i's are linearly independent if and only if $F_2(\alpha_1, \ldots, \alpha_n) \neq 0$ [36, Lemma 3.51].

It is known, by the Schwartz-Zippel Lemma, that there exist such α_j's in $\mathbb{F}_{q^s}$ if F is not the zero polynomial and for all $j \in [n]$, $\deg_{\alpha_j} F < q^s$. Note that F_2 is not the zero polynomial since the coefficient of the monomial $\prod_{i=1}^{n} \alpha_i^{q^{i-1}}$ in F_2 is 1 because it can only be obtained through multiplication of the diagonals. Furthermore, if Claim 3.1 below is true, we can conclude that F is not the zero polynomial.

Claim 3.1. $\det \mathbf{T}$ *is not the zero polynomial if (3.6) is satisfied.* $\diamond$

We will give the proof of Claim 3.1 later in Section 3.3 by proving a slightly more general statement. Therefore, in this section, we will proceed by assuming that it is

true. Then, F is not the zero polynomial and the only question that remains is "what is the largest value of $\deg_{\alpha_j} F$ over all $j \in [n]$?", whose answer, in turn, can be used as a sufficient lower bound on the size of the extension field where such α_j's exist.

Notice from (3.21) that for a fixed α_j, the degree of F_2 as a polynomial in α_j is

$$\deg_{\alpha_j} F_2 = q^{n-1}.$$

Now, we will compute $\deg_{\alpha_j} F_1$. From (3.10), recall that for any $i, \ell \in [k]$, $\mathbf{T}_{i\ell}$ is the coefficient of $x^{q^{\ell-1}}$ in $f_i(x)$. Since $f_i(x)$ is monic, $\mathbf{T}_{ik} = 1$. For $\ell < k$, $\mathbf{T}_{i\ell}$ is a polynomial in α_j and $\deg_{\alpha_j} \mathbf{T}_{i\ell} \leq \deg_{\alpha_j} f_i(x)$ (when writing $\deg_{\alpha_j} f_i(x)$, we consider $f_i(x)$ as a polynomial in α_j).

To find $\deg_{\alpha_j} f_i$, consider the definition of f_i in (3.18). Suppose that $j \in \mathcal{Z}_i$ (otherwise, $\deg_{\alpha_j} f_i = 0$). Let $\mathcal{Z}_i' = \mathcal{Z}_i - \{j\}$ and define f_i' as

$$f_i'(x) = \prod_{\beta \in \text{span}\{\alpha_{j'} : j' \in \mathcal{Z}_i'\}} (x - \beta) \tag{3.22}$$

which is a linearized polynomial with $\deg_q f_i' = |\mathcal{Z}_i'| = k - 2$ and hence as a usual polynomial $\deg_x f_i'(x) = q^{k-2}$. Since $j \notin \mathcal{Z}_i'$, $f_i'(x)$ is independent of α_j; therefore, we can also write $\deg_{\alpha_j} f_i'(\alpha_j) = q^{k-2}$. Furthermore, we can write that

$$\begin{aligned}
f_i(x) &= \prod_{\beta \in \text{span}\{\alpha_{j'} : j' \in \mathcal{Z}_i\}} (x - \beta) && (3.23)\\
&= \prod_{\gamma \in \mathbb{F}_q} \prod_{\beta \in \text{span}\{\alpha_{j'} : j' \in \mathcal{Z}_i'\}} (x - \gamma\alpha_j - \beta) && (3.24)\\
&= \prod_{\gamma \in \mathbb{F}_q} f_i'(x - \gamma\alpha_j) && (3.25)\\
&= \prod_{\gamma \in \mathbb{F}_q} (f_i'(x) - \gamma f_i'(\alpha_j)) && (3.26)\\
&= (f_i'(x))^q - (f_i'(\alpha_j))^{q-1} f_i'(x) && (3.27)
\end{aligned}$$

where the last step is because of the identity $\prod_{\gamma \in \mathbb{F}_q} (x - a\gamma) = x^q - a^{q-1}x$.

Hence, $\deg_{\alpha_j} \mathbf{T}_{i\ell} \leq \deg_{\alpha_j} f_i(x) \leq (q-1) \deg_{\alpha_j} f_i'(\alpha_j) = (q-1)q^{k-2}$. Then,

$$\begin{aligned}
\deg_{\alpha_j} F_1 &= \deg_{\alpha_j} \det \mathbf{T} && (3.28)\\
&\leq \max_{\sigma \in S_k} \sum_{\ell=1}^{k} \deg_{\alpha_j} \mathbf{T}_{\sigma(\ell),\ell} && (3.29)\\
&\leq (k-1)(q-1)q^{k-2} && (3.30)
\end{aligned}$$

where S_k denotes the set of permutations of $[k]$ and in the last inequality, recall that $\mathbf{T}_{ik} = 1$, whose degree is 0. As a result,

$$\deg_{\alpha_j} F \leq q^{n-1} + (k-1)(q-1)q^{k-2}. \tag{3.31}$$

So, if the field size is larger than this bound, i.e. $q^s > q^{n-1} + (k-1)(q-1)q^{k-2}$, then there exist $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^s}$ such that $F(\alpha_1, \ldots, \alpha_n) \neq 0$. As a result, we have the following theorem. Note that if $s \geq n$ and $s \geq k - 1 + \log_q k$, then

$$q^s = q^{s-1} + (q-1)q^{s-1} \geq q^{n-1} + (q-1)kq^{k-2} > q^{n-1} + (k-1)(q-1)q^{k-2}. \tag{3.32}$$

Theorem 3.1. *For any $s \geq \max\{n, k - 1 + \log_q k\}$, if (3.6) is satisfied, then there exists a Gabidulin code in $\mathbb{F}_{q^s}$ of length n and dimension k such that its generator matrix satisfies the support constraints in (3.5).* ◇

Subcodes of Gabidulin codes

If the necessary and sufficient condition in (3.6) is not satisfied, we cannot have an MDS code with the prescribed support constraints, and by fiat we cannot have an MRD code or a Gabidulin code. However, we can still ask whether a code with the largest possible rank distance can be achieved. In fact, we can show that the largest rank distance can be achieved by subcodes of Gabidulin codes for a large enough field size. In [2], the following upper bound on the Hamming distance is noted:

$$d_H \leq n - \ell + 1 \tag{3.33}$$

where

$$\ell \triangleq \max_{\emptyset \neq \Omega \subset [k]} \left(\left| \bigcap_{i \in \Omega} \mathcal{Z}_i \right| + |\Omega| \right) \geq k. \tag{3.34}$$

Since the rank distance of the code is upper bounded by the Hamming distance, we have that

$$d_R \leq n - \ell + 1. \tag{3.35}$$

Theorem 3.2. *Suppose $s \geq \max\{n, \ell - 1 + \log_q \ell\}$. Then, there exists a subcode of a Gabidulin code in $\mathbb{F}_{q^s}$ with length n, dimension k, and rank distance $d_R = n - \ell + 1$ such that its generator matrix satisfies (3.5).* ◇

Proof. Define $\mathcal{Z}_{k+1} = \cdots = \mathcal{Z}_\ell = \emptyset$. Then, for any nonempty $\Omega \subset [\ell]$,

$$\left| \bigcap_{i \in \Omega} \mathcal{Z}_i \right| + |\Omega| \leq \ell. \tag{3.36}$$

Hence, by Theorem 3.1, there exists a Gabidulin code of dimension ℓ with an $\ell \times n$ generator matrix $\mathbf{G}$ having zeros dictated by $\mathcal{Z}_1, \ldots, \mathcal{Z}_\ell$. Since it is an MRD–code, its rank distance is $n - \ell + 1$. The first k rows of $\mathbf{G}$ will generate a subcode whose rank distance d_R is as good as the Gabidulin code: $d_R \geq n - \ell + 1$. Hence, this subcode achieves the largest possible rank distance given in (3.35). □

3.3 Proof of Claim 3.1 (and More)

In this section, first we will extend the definition of linearized polynomials by allowing their coefficients to be multivariate polynomials. Then, we will propose a more general statement than Claim 3.1, namely Theorems 3.3.A and 3.3.B, which, in fact, arise when trying to apply a proof by induction to Claim 3.1. Our generalization will be written in two different forms. Theorem 3.3.A will be in terms of linearized polynomials, whereas Theorem 3.3.B will be in terms of matrices. However, both are equivalent and more general than Claim 3.1. We will give a sketch of the proof in the language of matrices while the detailed proof will be given in the language of polynomials. We should emphasize that the material presented here in the matrix language is only for a better illustration of Theorem 3.3.A.

Problem Setup

Consider a finite field $\mathbb{F}_q$ and an extension field $\mathsf{R}_0 = \mathbb{F}_{q^s}$. For $n \geq 1$, let $\mathsf{R}_n \triangleq \mathbb{F}_{q^s}[x_1, \ldots, x_n]$ be the ring of multivariate polynomials in the indeterminates $x_1, x_2 \ldots, x_n$ over $\mathbb{F}_{q^s}$.

Recall that the notation $\mathsf{R}_n[x]$ denotes the ring of polynomials in the indeterminate x, whose coefficients are drawn from R_n (the coefficients are multivariate polynomials in $x_1, \ldots, x_n$), i.e.,

$$\mathsf{R}_n[x] \triangleq \left\{ \sum_{i=0}^{d} c_i x^i \middle| d \geq 0, c_0, \ldots, c_d \in \mathsf{R}_n \right\}. \tag{3.37}$$

The set of linearized polynomials over R_n is a subset of $\mathsf{R}_n[x]$, which we define as:

$$\mathsf{L}_n \triangleq \left\{ \sum_{i=0}^{d} c_i x^{q^i} \middle| d \geq 0, c_0, \ldots, c_d \in \mathsf{R}_n \right\} \subset \mathsf{R}_n[x]. \tag{3.38}$$

The q-degree of $f \in \mathsf{L}_n$ is defined as $\deg_q f = d$ if $f = \sum_{i=0}^{d} c_i x^{q^i}$ and $c_d \neq 0$. We also take $\deg_q 0 = -\infty$. Since $\mathsf{L}_n \subset \mathsf{R}_n[x]$, for any $f, g \in \mathsf{L}_n$, we will continue to use $\gcd\{f, g\}$ and $f \mid g$ notations by treating as $f, g \in \mathsf{R}_n[x]$.

We note the following properties of L_n (see [36, Chapter 3] as a reference textbook, where these properties are proven for L_0, i.e., when the coefficients of the linearized polynomials are from $\mathbb{F}_{q^s}$. The same proofs can be extended to L_n. We also give the proofs of P1 and P3 in Appendix 3.A as the other properties are obvious):

P1. L_n is a ring with no zero divisors under the addition and the composition operation $\circ$.

P2. For any $f, g \in \mathsf{L}_n$, $\deg_q(f \circ g) = \deg_q(f) + \deg_q(g)$.

P3. For any finite-dimensional subspace $V \subset \mathsf{R}_n$ over $\mathbb{F}_q$ and $t \geq 0$,

$$f = \prod_{\beta \in V} (x - \beta)^{q^t} \in \mathsf{L}_n \tag{3.39}$$

and $\deg_q f = t + \dim V$.

P4. For any $f \in \mathsf{L}_n$, if $x^{q^t} \mid f$, then $\exists f' \in \mathsf{L}_n$ such that $f = f' \circ x^{q^t}$.

P5. For any $f, g \in \mathsf{L}_n$, if $x^{q^t} \mid f$, then $x^{q^t} \mid f \circ g$ and $x^{q^t} \mid g \circ f$.

P6. For any $f, g \in \mathsf{L}_n$, if $x^q \nmid f$ and $x^{q^t} \mid g \circ f$, then $x^{q^t} \mid g$.

We are interested in linearized polynomials of the following form:

$$\mathsf{f}(\mathcal{Z}, t) \triangleq \prod_{\beta \in \text{span}\{x_i : i \in \mathcal{Z}\}} (x - \beta)^{q^t} \in \mathsf{L}_n, \qquad t \geq 0, \mathcal{Z} \subset [n]. \tag{3.40}$$

Note that these are linearized polynomials in light of P3 above. Furthermore, since the x_i's are assumed to be indeterminates, any nontrivial linear combination of them is nonzero, i.e. the x_i's are linearly independent. Hence,

$$\deg_q \mathsf{f}(\mathcal{Z}, t) = t + \dim(\text{span}\{x_i : i \in \mathcal{Z}\}) = t + |\mathcal{Z}|. \tag{3.41}$$

For $k \geq 1$, we define the set of linearized polynomials in this form with q-degree at most $k - 1$:

$$\mathcal{L}_{n,k} \triangleq \{\mathsf{f}(\mathcal{Z}, t) | t \geq 0, \mathcal{Z} \subset [n] \text{ s.t. } t + |\mathcal{Z}| \leq k - 1\} \subset \mathsf{L}_n. \tag{3.42}$$

We also note the following properties with regard to $\mathcal{L}_{n,k}$, whose proofs appear in Appendix 3.A.

P7. For any $f_1 = \mathsf{f}(\mathcal{Z}_1, t_1), f_2 = \mathsf{f}(\mathcal{Z}_2, t_2) \in \mathcal{L}_{n,k}$, we have

$$\gcd\{f_1, f_2\} = \mathsf{f}(\mathcal{Z}_1 \cap \mathcal{Z}_2, \min\{t_1, t_2\}) \in \mathcal{L}_{n,k}.$$

P8. For any $f_1, f_2 \in \mathcal{L}_{n,k}$, if $f_2 \mid f_1$, then $\exists f_1' \in \mathsf{L}_n,\ f_1 = f_1' \circ f_2$.

P9. Let $f = \mathsf{f}(\mathcal{Z}, t) \in \mathcal{L}_{n,k}$ and let $f' = f|_{x_n=0} \in \mathsf{L}_{n-1}$ (substitute $x_n = 0$ in each coefficient of f). Then, $f' \in \mathcal{L}_{n-1,k}$ and

$$f' = \begin{cases} \mathsf{f}(\mathcal{Z}, t) & n \notin \mathcal{Z} \\ \mathsf{f}(\mathcal{Z} - \{n\}, t+1) & n \in \mathcal{Z} \end{cases}. \tag{3.43}$$

As a final note, it will be insightful to describe the composition operation between linearized polynomials in matrix language. It is known that multiplying two polynomials is equivalent to multiplying two Toeplitz matrices since both perform the convolution operation. Now, we will give the analog when composing two linearized polynomials. Let $f = \sum_{i=0}^{d} c_i x^{q^i} \in \mathsf{L}_n$. For $b - a \geq d$, we define the following matrix:

$$\mathbf{S}_{a\times b}(f) = \begin{pmatrix} c_0^{q^0} & c_1^{q^0} & \cdots & c_{b-a}^{q^0} & & \\ & c_0^{q^1} & c_1^{q^1} & \cdots & c_{b-a}^{q^1} & \\ & & \ddots & \ddots & & \ddots \\ & & & c_0^{q^{a-1}} & c_1^{q^{a-1}} & \cdots & c_{b-a}^{q^{a-1}} \end{pmatrix}$$

where $c_i = 0$ for $i > d$. Note that a and b are parameters that define the dimensions of the matrix $\mathbf{S}_{a\times b}(f)$, which is why we subscript $\mathbf{S}$ by $a \times b$. For any linearized polynomials $f_1, f_2 \in \mathsf{L}_n$, we have that

$$\mathbf{S}_{a\times b}(f_1 \circ f_2) = \mathbf{S}_{a\times c}(f_1) \cdot \mathbf{S}_{c\times b}(f_2) \tag{3.44}$$

for any a, b, c such that $c - a \geq \deg_q f_1$ and $b - c \geq \deg_q f_2$. The proof follows straightforward calculations by definition. As a special case, when $f_1 = x^{q^t}$, $f_2 = f = \sum_{i=0}^{d} c_i x^{q^i}$, and $f_1 \circ f_2 = f^{q^t}$, we can write for $b - a \geq d$,

$$\mathbf{S}_{a\times(b+t)}(f^{q^t}) = \mathbf{S}_{a\times(a+t)}(x^{q^t}) \cdot \mathbf{S}_{(a+t)\times(b+t)}(f) \tag{3.45}$$

$$= \begin{pmatrix} \mathbf{0}_{a\times t} & \mathbf{I}_{a\times a} \end{pmatrix} \cdot \mathbf{S}_{(a+t)\times(b+t)}(f) \tag{3.46}$$

$$= \begin{pmatrix} \underbrace{\begin{matrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{matrix}}_{t} & \begin{matrix} c_0^{q^t} & c_1^{q^t} & \cdots & c_{b-a}^{q^t} & & \\ & c_0^{q^{t+1}} & c_1^{q^{t+1}} & \cdots & c_{b-a}^{q^{t+1}} & \\ & & \ddots & \ddots & & \ddots \\ & & & c_0^{q^{t+a-1}} & c_1^{q^{t+a-1}} & \cdots & c_{b-a}^{q^{t+a-1}} \end{matrix} \end{pmatrix}. \tag{3.47}$$

Since by definition, $\mathsf{f}(\mathcal{Z},t)=f'^{q^t}$ for some $f'\in\mathsf{L}_n$, we have the following property:

P10. Let $f=\mathsf{f}(\mathcal{Z},t)$ and $r\geq 0$. Then the first $r+t$ columns of $\mathbf{S}_{a\times(b+r)}(f^{q^r})$ are all zero.

Main Result

Theorem 3.3.A is a more general statement than Claim 3.1 given in Section 3.2 and it is the analog of [2, Theorem 3] for linearized polynomials.

Theorem 3.3.A. *Let $k\geq m\geq 1$ and $n\geq 0$. Then, for any $f_1,f_2,\ldots,f_m\in\mathcal{L}_{n,k}$, the following are equivalent:*

(i) For all $g_1,g_2,\ldots,g_m\in\mathsf{L}_n$ and $r\geq 0$ such that $\deg_q(g_i\circ f_i)\leq k-1$, we have

$$\sum_{i=1}^{m} g_i\circ x^{q^r}\circ f_i=0 \implies g_1=g_2=\cdots=g_m=0. \tag{3.48}$$

(ii) For all nonempty $\Omega\subset[m]$, we have

$$k-\deg_q \gcd_{i\in\Omega} f_i\geq \sum_{i\in\Omega}(k-\deg_q f_i). \tag{3.49}$$

$\diamond$

Before moving to the proof, in order to see how Claim 3.1 becomes a special case of Theorem 3.3.A, we will give an equivalent way of writing it in terms of matrices with entries from R_n. This will also allow us to see its connection with [2, Theorem 3].

For $i\in[m]$, let $f_i=\mathsf{f}(\mathcal{Z}_i,t_i)\in\mathcal{L}_{n,k}$ (i.e. $\mathcal{Z}_i\subset[n], t_i\geq 0$ such that $|\mathcal{Z}_i|+t_i\leq k-1$). For $r\geq 0$, we will write $\mathbf{S}(f_i^{q^r})$ instead of $\mathbf{S}_{(k-t_i-|\mathcal{Z}_i|)\times(k+r)}(f_i^{q^r})$ for the ease of notation. By P10, $\mathbf{S}(f_i^{q^r})$ will look like as follows, where the $\times$'s represent the nonzero entries:

$$\mathbf{S}(f_i^{q^r})=\left.\begin{pmatrix} \underbrace{0 & \cdots & 0}_{r+t_i} & \underbrace{\times & \times & \cdots}_{k-1-t_i-|\mathcal{Z}_i|} & \underbrace{\times & & & \\ \times & \times & \cdots & \times & & & \\ & & \ddots & \ddots & & \ddots & \\ & & & \times & \times & \cdots & \times}_{|\mathcal{Z}_i|+1} \end{pmatrix}\right\} k-t_i-|\mathcal{Z}_i|. \tag{3.50}$$

Then, applying (3.44) to the expression $g_i \circ x^{q^r} \circ f_i = g_i \circ f_i^{q^r}$ in Theorem 3.3.A yields

$$\mathbf{S}_{1\times(k+r)}(g_i \circ x^{q^r} \circ f_i) = \mathbf{u}_i \cdot \mathbf{S}(f_i^{q^r}) \tag{3.51}$$

where $\mathbf{u}_i = \mathbf{S}_{1\times(k-t_i-|\mathcal{Z}_i|)}(g_i)$ is a row vector. Therefore, we can write

$$\mathbf{S}_{1\times(k+r)}\left(\sum_{i=1}^{m} g_i \circ x^{q^r} \circ f_i\right) = \begin{pmatrix}\mathbf{u}_1 & \cdots & \mathbf{u}_m\end{pmatrix} \cdot \begin{pmatrix}\mathbf{S}(f_1^{q^r}) \\ \vdots \\ \mathbf{S}(f_m^{q^r})\end{pmatrix} \tag{3.52}$$

which is a linear combination of the rows of

$$\mathbf{M}(r) = \begin{pmatrix}\mathbf{S}(f_1^{q^r}) \\ \vdots \\ \mathbf{S}(f_m^{q^r})\end{pmatrix}_{\sum_{i=1}^{m}(k-t_i-|\mathcal{Z}_i|)\times(k+r)} . \tag{3.53}$$

Hence, (i) in Theorem 3.3.A is equivalent to saying the matrix $\mathbf{M}(r)$ has full row rank. Note that the first r columns of $\mathbf{M}(r)$ are zero since the first $r + t_i$ columns of $\mathbf{S}(f_i^{q^r})$ are so.

Furthermore, (ii) in Theorem 3.3.A can be written in terms of the $\mathcal{Z}_i$'s and the t_i's in lights of (3.41) and P7. Therefore, Theorem 3.3.A is equivalent to Theorem 3.3.B below.

Theorem 3.3.B. *For $i \in [m]$, let $\mathcal{Z}_i \subset [n], t_i \geq 0$ such that $|\mathcal{Z}_i| + t_i \leq k-1$. Then, the matrix $\mathbf{M}(r)$ defined in (3.53) has full row rank for all $r \geq 0$ if and only if for all nonempty $\Omega \subset [m]$,*

$$k - \left|\bigcap_{i\in\Omega} \mathcal{Z}_i\right| - \min_{i\in\Omega} t_i \geq \sum_{i\in\Omega}(k - t_i - |\mathcal{Z}_i|). \tag{3.54}$$

$\diamond$

As a special case, when $m = k$, $|\mathcal{Z}_i| = k-1$, $t_i = 0$, and $r = 0$, each block in $\mathbf{M}(r)$ becomes a row vector with coefficients of $f_i = \mathsf{f}(\mathcal{Z}_i, t_i) = \sum_{i=1}^{k} c_{ij} x^{q^{j-1}}$:

$$\mathbf{S}_{(k-t_i-|\mathcal{Z}_i|)\times(k+r)}(f_i^{q^0}) = \mathbf{S}_{1\times(k+r)}(f_i) = \begin{pmatrix}c_{i1} & c_{i2} & \cdots & c_{ik}\end{pmatrix}.$$

Hence, we have Corollary 3.1 below, which is Claim 3.1 in Section 3.2.

Corollary 3.1. *For $i \in [k]$, let $\mathcal{Z}_i \subset [n]$ with $|\mathcal{Z}_i| = k-1$. Then,*

$$k \geq \left|\bigcap_{i\in\Omega} \mathcal{Z}_i\right| + |\Omega|, \qquad \forall\, \emptyset \neq \Omega \subset [k]$$

if and only if

$$\det \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1k} \\ c_{21} & c_{22} & \dots & c_{2k} \\ \vdots & \vdots & & \vdots \\ c_{k1} & c_{k2} & \dots & c_{kk} \end{pmatrix} \neq 0$$

where c_{ij}'s are defined as the coefficients of $f_i = \mathsf{f}(\mathcal{Z}_i, 0) = \sum_{i=1}^{k} c_{ij} x^{q^{j-1}}$. $\diamond$

Sketch of the proof of Theorem 3.3.B

The proof given here for Theorem 3.3.B omits certain steps that the interested reader can fill in. The complete proof of the equivalent Theorem 3.3.A is given in Section 3.3 and includes each and every step.

The following identity (3.55) will be very useful throughout the proof.

For any $\Omega \subset [m]$ (w.l.o.g. assume $\Omega = \{1, 2, \dots, \ell\}$), we have $f_i = f_i' \circ f_0$ for $i \in [\ell]$, where $f_0 = \gcd_{i \in \Omega} f_i$. Then, we can write (with the appropriate dimensions for $\mathbf{S}(\,\cdot\,)$)

$$\begin{pmatrix} \mathbf{S}(f_1^{q^r}) \\ \vdots \\ \mathbf{S}(f_\ell^{q^r}) \end{pmatrix} = \underbrace{\begin{pmatrix} \mathbf{S}(f_1'^{q^r}) \\ \vdots \\ \mathbf{S}(f_\ell'^{q^r}) \end{pmatrix}}_{\begin{bmatrix} \mathbf{0}_{* \times r} & \mathbf{B}' \end{bmatrix}} \cdot \underbrace{\mathbf{S}(f_0)}_{\begin{bmatrix} \times \\ \mathbf{S}(f_0^{q^r}) \end{bmatrix}} = \mathbf{B}' \cdot \mathbf{S}(f_0^{q^r}) \tag{3.55}$$

where the matrix $\mathbf{B}'$ has $(k - \left|\bigcap_{i \in \Omega} \mathcal{Z}_i\right| - \min_{i \in \Omega} t_i)$ columns and $\sum_{i \in \Omega}(k - t_i - |\mathcal{Z}_i|)$ rows. Note that these are respectively the left and right hand sides in (3.54).

Therefore, if (3.54) does not hold, then $\mathbf{B}'$ will be a tall matrix and will not have full row rank, which solves $\implies$ direction. For the other direction, we will try to reduce the problem to the one that has a smaller k, m, or n in order to do an inductive proof. We look into two cases:

Case 1. (3.54) is tight for some $2 \leq |\Omega| \leq m - 1$.

Case 2. (3.54) is strict for all $2 \leq |\Omega| \leq m - 1$.

In the first case, the matrix $\mathbf{B}'$ becomes a square matrix. Hence,

$$\begin{pmatrix} \mathbf{S}(f_1^{q^r}) \\ \vdots \\ \mathbf{S}(f_m^{q^r}) \end{pmatrix} = \begin{pmatrix} \mathbf{B}'\mathbf{S}(f_0^{q^r}) \\ \mathbf{S}(f_{\ell+1}^{q^r}) \\ \vdots \\ \mathbf{S}(f_m^{q^r}) \end{pmatrix} \tag{3.56}$$

$$= \begin{pmatrix} \mathbf{B}' & & & \\ & \mathbf{I} & & \\ & & \ddots & \\ & & & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{S}(f_0^{q^r}) \\ \mathbf{S}(f_{\ell+1}^{q^r}) \\ \vdots \\ \mathbf{S}(f_m^{q^r}) \end{pmatrix}. \tag{3.57}$$

This will reduce the problem into two smaller problems: The first one is showing that the matrix on the right in (3.57) has full row rank. The second one is showing that $\mathbf{B}'$ is non-singular or that $\mathbf{B}' \cdot \mathbf{S}(f_0^{q^r})$, which is equal to the first ℓ blocks (see (3.55)), has full row rank. Both are smaller problems (in terms of the number of blocks) and one can show that both satisfy the inequalities in (3.54).

In the second case, since the inequalities are strict except for $|\Omega| = 1, m$, we have some flexibility to play with the sets. For example, we can remove an element j from all the sets $\mathcal{Z}_i$'s containing j and increase t_i by 1 (this corresponds to Case 2c in the proof of Theorem 3.3.A). This operation sets $x_j = 0$ in the matrix $\mathbf{M}(r)$ and we can claim that if $\mathbf{M}(r)|_{x_j=0}$ has full row rank, then so does $\mathbf{M}(r)$. Hence, it reduces n in the problem to $n-1$. Furthermore, it can be shown that except for two corner cases (see Case 2a and 2b), one can carefully choose such an element j so that removing it from the sets will not break (3.54) for $|\Omega| = m$.

The only two corner cases are when none or only one of the t_i's is zero. If $t_i \geq 1$ for all $i \in [m]$ (i.e. the first $r+1$ columns of $\mathbf{M}(r)$ are all zero), then decreasing k and each t_i by 1 and increasing r by 1 will reduce the problem into a smaller one (see Case 2a). If there is a unique zero, say $t_1 = 0$ (see Case 2b), then the first $r+1$ columns of $\mathbf{S}(f_i^{q^r})$ will be zero only for $i \geq 2$. Then, the matrix will look like

$$\mathbf{M}(r) = \left(\begin{array}{cccccccccc} 0 & \cdots & 0 & \times & \times & \cdots & \times & & & \\ 0 & \cdots & 0 & 0 & \times & \times & \cdots & \times & & \\ \vdots & & \vdots & \vdots & & \ddots & \ddots & & \ddots & \\ 0 & \cdots & 0 & 0 & & & \times & \times & \cdots & \times \\ \hline 0 & \cdots & 0 & 0 & \times & \times & \cdots & \times & & \\ \vdots & & \vdots & \vdots & & \ddots & & & \ddots & \\ 0 & \cdots & 0 & 0 & & & \times & \times & \cdots & \times \\ \hline & & & & & \vdots & & & & \end{array}\right). \tag{3.58}$$

Hence, the first row is definitely not in the span of the other rows because it contains a nonzero in the $(r+1)$th column while the others do not. So, we can reduce the problem by removing the first row. This will decrease k and every t_i except t_1 by 1

(and maybe m too if there is a single row in the first block). Again, it can be shown that this operation does not violate (3.54).

Proof of Theorem 3.3.A

Let $f_i = \mathsf{f}(\mathcal{Z}_i, t_i)$. For the ease of notation, we will write $f_\Omega \triangleq \gcd_{i\in\Omega} f_i$, which, by P7, is equal to

$$f_\Omega = \mathsf{f}\left(\bigcap_{i\in\Omega} \mathcal{Z}_i,\ \min_{i\in\Omega} t_i\right). \tag{3.59}$$

We will first show the trivial direction ($(i) \implies (ii)$), then do induction for the other direction ($(ii) \implies (i)$).

$(i) \implies (ii)$:

Suppose that (ii) does not hold and w.l.o.g., assume that for $\Omega = \{1, 2, \ldots, \ell\}$,

$$k - \deg_q f_\Omega < \sum_{i\in\Omega} (k - \deg_q f_i).$$

For $i \in \Omega$, let $f_i = f_i' \circ f_\Omega$ for some $f_i' \in \mathsf{L}_n$ (see P8). Then, for $r = 0$ and for $g_1, \ldots, g_\ell \in \mathsf{L}_n$ such that $\deg_q(g_i \circ f_i) \le k-1$, in (i), the equation $\sum_{i\in\Omega} g_i \circ f_i' = 0$ defines homogeneous linear equations in coefficients of g_i's. The number of variables is $\sum_{i\in\Omega} k - \deg_q f_i$ and the number of equations is at most $k - \deg_q f_\Omega$. So, one can find $g_1, \ldots, g_\ell$, not all zero, that solves this linear system.

$(ii) \implies (i)$:

We will do induction on parameters (k, m, n) considered in the lexicographical order.

For $(k, m = 1, n)$, (i) always holds due to P1: $g_1 \circ x^{q^r} \circ f_1 = 0 \implies g_1 = 0$.

For $(k, m \ge 2, n = 0)$, (ii) never holds: $n = 0 \implies f_i = x^{q^{t_i}}$ for some t_i for every i. Suppose $t_1 \le t_2$, then for $\Omega = \{1, 2\}$, (3.49) becomes $k - t_1 \ge (k - t_1) + (k - t_2)$, which contradicts with $|\mathcal{Z}_i| + t_i \le k - 1$.

For $k \ge m \ge 2$ and $n \ge 1$, assume that the statement ($(ii) \implies (i)$) is true for parameters $(k', m', n') < (k, m, n)$. Take any $f_1, \ldots, f_m \in \mathcal{L}_{n,k}$ for which (ii) is true. We will prove that (i) holds under the following cases:

Case 1. $\exists\, \Omega \subset [m]$ with $2 \le |\Omega| \le m - 1$ such that (3.49) holds with equality.

Case 2. $\forall\, \Omega \subset [m]$ with $2 \le |\Omega| \le m - 1$, (3.49) holds strictly and any of these three:

Case 2a. For all $i \in [m]$, $t_i \geq 1$.

Case 2b. There exists a unique $i \in [m]$ such that $t_i = 0$.

Case 2c. There exist at least two zero t_i.

We will reduce m in Case 1, k in Case 2a and 2b, and n in Case 2c. Note that since $k \geq m$, reducing k sometimes may also reduce m, which may happen in Case 2b but will not happen in Case 2a, where we show $k \geq m + 1$.

Case 1: W.l.o.g., assume that for $\Omega' = \{1, 2, \ldots, \ell\}$,

$$k - \deg_q f_0 = \sum_{i \in \Omega'} (k - \deg_q f_i)$$

where $f_0 = f_{\Omega'}$. By P8, for $i \in [\ell]$, there exists $f_i' \in \mathsf{L}_n$ such that $f_i = f_i' \circ f_0$.

We will look at two smaller problems: $(f_1, \ldots, f_\ell) \in \mathcal{L}_{n,k}^{\ell}$ and $(f_0, f_{\ell+1}, \ldots, f_m) \in \mathcal{L}_{n,k}^{m-\ell+1}$. Since $\ell < m$ and $m - \ell + 1 < m$, the statement holds for both by the induction hypothesis.
It is trivial that (ii) holds for $(f_1, \ldots, f_\ell)$ and for $(f_0, f_{\ell+1}, \ldots, f_m)$ when $0 \notin \Omega$. We will show that it also holds for $(f_0, f_{\ell+1}, \ldots, f_m)$ when $0 \in \Omega$:

$$\begin{aligned}
k - \deg_q f_\Omega &= k - \deg_q \gcd\{f_0, f_{(\Omega - \{0\})}\} && (3.60)\\
&= k - \deg_q \gcd\{f_{\Omega'}, f_{(\Omega - \{0\})}\} && (3.61)\\
&\leq \sum_{i \in \Omega' \cup (\Omega - \{0\})} (k - \deg_q f_i) && (3.62)\\
&= \sum_{i \in \Omega'} (k - \deg_q f_i) + \sum_{i \in (\Omega - \{0\})} (k - \deg_q f_i) && (3.63)\\
&= (k - \deg_q f_0) + \sum_{i \in (\Omega - \{0\})} (k - \deg_q f_i) && (3.64)\\
&= \sum_{i \in \Omega} (k - \deg_q f_i). && (3.65)
\end{aligned}$$

Hence, by the induction hypothesis, (i) holds for both $(f_1, \ldots, f_\ell)$ and $(f_0, f_{\ell+1}, \ldots, f_m)$. Now, we will show that it also holds for $(f_1, \ldots, f_m)$:

Suppose that for some $r \geq 0$ and $g_1, \ldots, g_m \in \mathsf{L}_n$ with $\deg_q g_i \circ f_i \leq k - 1$ for $i \in [m]$, we have

$$\sum_{i=1}^{m} g_i \circ x^{q^r} \circ f_i = 0.$$

Since $x^{q^r} \mid \sum_{i=1}^{\ell} g_i \circ x^{q^r} \circ f_i'$, by P4, we can write

$$\sum_{i=1}^{\ell} g_i \circ x^{q^r} \circ f_i' = g_0 \circ x^{q^r}$$

for some $g_0 \in \mathsf{L}_n$. Then,

$$\begin{aligned} 0 &= \sum_{i=1}^{m} g_i \circ x^{q^r} \circ f_i \\ &= \sum_{i=1}^{\ell} g_i \circ x^{q^r} \circ f_i' \circ f_0 + \sum_{i=\ell+1}^{m} g_i \circ x^{q^r} \circ f_i \\ &= g_0 \circ x^{q^r} \circ f_0 + \sum_{i=\ell+1}^{m} g_i \circ x^{q^r} \circ f_i. \end{aligned}$$

Hence, $g_0 = g_{\ell+1} = \cdots = g_m = 0$. Then,

$$g_0 \circ x^{q^r} \circ f_0 = \sum_{i=1}^{\ell} g_i \circ x^{q^r} \circ f_i = 0. \tag{3.66}$$

Hence, $g_1 = \cdots = g_\ell = 0$. Then, all g_i's are zero.

Case 2a: For all $i \in [m]$, $f_i = x^q \circ f_i'$, where $f_i' = \mathsf{f}(\mathcal{Z}_i, t_i - 1) \in \mathcal{L}_{n,k-1}$. Note that since $\min_{i\in[m]} t_i \geq 1$, we have $\deg_q f_{[m]} \geq 1$ and for $\Omega = [m]$, (ii) implies

$$k - 1 \geq k - \deg_q f_{[m]} \geq \sum_{i\in[m]} (k - \deg_q f_i) \geq m.$$

By the induction hypothesis, the statement is true for $(f_1', \ldots, f_m')$ with parameters $(k-1, m, n)$.

(ii) holds for $(f_1', \ldots, f_m')$ because for any nonempty $\Omega \subset [m]$,

$$\begin{aligned} k - 1 - \deg_q f_\Omega' &= k - \deg_q f_\Omega \\ &\geq \sum_{i\in\Omega} (k - \deg_q f_i) \\ &= \sum_{i\in\Omega} (k - 1 - \deg_q f_i'). \end{aligned}$$

Hence, (i) holds for $(f_1', \ldots, f_m')$ too and we will show that it also holds for $(f_1, \ldots, f_m)$:

Suppose that for some $r \geq 0$ and $g_1, \ldots, g_m \in \mathsf{L}_n$ with $\deg_q g_i \circ f_i \leq k - 1$ for $i \in [m]$, we have

$$\sum_{i=1}^{m} g_i \circ x^{q^r} \circ f_i = 0.$$

Then,

$$\begin{aligned} 0 &= \sum_{i=1}^{m} g_i \circ x^{q^r} \circ f_i \\ &= \sum_{i=1}^{m} g_i \circ x^{q^r} \circ x^q \circ f_i' \\ &= \sum_{i=1}^{m} g_i \circ x^{q^{r+1}} \circ f_i'. \end{aligned}$$

Hence, $g_1 = \cdots = g_m = 0$.

Case 2b: Suppose that $t_m = 0$ and for $i \in [m-1]$, $t_i \geq 1$. For $i \in [m-1]$, let $f_i = x^q \circ f_i'$, where $f_i' = \mathsf{f}(\mathcal{Z}_i, t_i - 1) \in \mathcal{L}_{n,k-1}$ and let $f_m' = f_m \in \mathcal{L}_{n,k}$. Note that $f_m' \in \mathcal{L}_{n,k-1}$ if and only if $\deg_q f_m' \leq k-2$, in which case for $\Omega = [m]$, (ii) implies

$$k \geq k - \deg_q f_{[m]} \geq \sum_{i \in [m]} (k - \deg_q f_i) \geq m + 1.$$

By the induction hypothesis, the statement is true for $(f_1', \ldots, f_m')$ with parameters $(k-1, m, n)$ if $k \geq m+1$ (or $\deg_q f_m' \leq k-2$) and for $(f_1', \ldots, f_{m-1}')$ with parameters $(k-1, m-1, n)$.

We will show that (ii) holds for $(f_1', \ldots, f_m')$ when k is replaced by $k-1$. If $m \notin \Omega$, it is similar to Case 2a. For $m \in \Omega$, first observe that since each root of f_m has a multiplicity of 1, we have $\gcd\{f_m, f_i'\} = \gcd\{f_m, f_i\}$ for $i \in [m-1]$; hence, $f_\Omega = f_\Omega'$. Then,

$$\begin{aligned} (k-1) - \deg_q f_\Omega' &= -1 + k - \deg_q f_\Omega \\ &\geq -1 + \sum_{i \in \Omega} (k - \deg_q f_i) \\ &= (k - 1 - \deg_q f_m) + \sum_{i \in \Omega - \{m\}} (k - \deg_q f_i) \\ &= (k - 1 - \deg_q f_m') + \sum_{i \in \Omega - \{m\}} (k - 1 - \deg_q f_i') \\ &= \sum_{i \in \Omega} (k - 1 - \deg_q f_i'). \end{aligned}$$

Hence, (i) also holds for f_i''s.

Suppose that for some $r \geq 0$ and $g_1, \ldots, g_m \in \mathsf{L}_n$ with $\deg_q(g_i \circ f_i) \leq k-1$, we have

$$\sum_{i=1}^{m} g_i \circ x^{q^r} \circ f_i = 0.$$

Then,

$$\begin{aligned} 0 &= \sum_{i=1}^{m} g_i \circ x^{q^r} \circ f_i \\ &= g_m \circ x^{q^r} \circ f_m + \sum_{i=1}^{m-1} g_i \circ x^{q^r} \circ x^q \circ f_i' \\ &= g_m \circ x^{q^r} \circ f_m + \underbrace{\sum_{i=1}^{m-1} g_i \circ x^{q^{r+1}} \circ f_i'}_{\text{divisible by } x^{q^{r+1}} \text{ due to P5}} . \end{aligned}$$

Hence, $g_m \circ x^{q^r} \circ f_m$ is divisible by $x^{q^{r+1}}$ and since $x^q \nmid f_m$ (because $t_m = 0$), by P6, $x^{q^{r+1}} \mid g_m \circ x^{q^r}$. Then, by P4, we can write $g_m = g_m' \circ x^q$ for some $g_m' \in \mathsf{L}_n$ with $\deg_q g_i' = \deg_q g_i - 1$.

If $\deg_q f_m = k-1$, then $\deg_q g_m' \leq -1$, which implies that $g_m = 0$. Then, $g_1, \ldots, g_{m-1}$ are also zero since (i) holds for $(f_1', \ldots, f_{m-1}')$ with parameters $(k-1, m-1, n)$.

If $\deg_q f_m \leq k-2$,

$$0 = g_m' \circ x^{q^{r+1}} \circ f_m' + \sum_{i=1}^{m-1} g_i \circ x^{q^{r+1}} \circ f_i'. \tag{3.67}$$

Hence, $g_1 = \cdots = g_{m-1} = g_m' = 0$ since (i) holds for $(f_1', \ldots, f_m')$ with parameters $(k-1, m, n)$. Then all g_i's are zero.

Case 2c: W.l.o.g., assume that $t_{m-1} = t_m = 0$. If $\mathcal{Z}_{m-1} = \mathcal{Z}_m$, then for $\Omega = \{m-1, m\}$, (ii) implies

$$k - \deg_q f_m = k - \deg_q \gcd\{f_{m-1}, f_m\} \geq (k - \deg_q f_{m-1}) + (k - \deg_q f_m)$$

which contradicts with $\deg_q f_{m-1} \leq k-1$. Hence, either $\mathcal{Z}_{m-1} \neq [n]$ or $\mathcal{Z}_m \neq [n]$. W.l.o.g., assume $\mathcal{Z}_m \neq [n]$ and $n \notin \mathcal{Z}_m$.

Now, we will substitute $x_n = 0$. Let $f_i' = f_i \mid_{x_n=0}$. By P9, $f_i' \in \mathcal{L}_{n-1,k}$ and

$$f_i' = \mathsf{f}(\mathcal{Z}_i', t_i') = \begin{cases} \mathsf{f}(\mathcal{Z}_i, t_i) & n \notin \mathcal{Z}_i \\ \mathsf{f}(\mathcal{Z}_i - \{n\}, t_i + 1) & n \in \mathcal{Z}_i \end{cases}. \tag{3.68}$$

By the induction hypothesis, the statement is true for $(f_1', \ldots, f_m')$ with parameters $(k, m, n-1)$. We will show that it satisfies (ii):

For $|\Omega| = 1$, it is trivial.

For $2 \leq |\Omega| \leq m-1$, then

$$k - \deg_q f'_\Omega = k - \left|\bigcap_{i\in\Omega} \mathcal{Z}'_i\right| - \min_{i\in\Omega} t'_i \tag{3.69}$$

$$\leq k - \left(\left|\bigcap_{i\in\Omega} \mathcal{Z}_i\right| - 1\right) - \min_{i\in\Omega} t_i \tag{3.70}$$

$$= k + 1 - \deg_q f_\Omega \tag{3.71}$$

$$\leq \sum_{i\in\Omega}(k - \deg_q f_i) \tag{3.72}$$

$$= \sum_{i\in\Omega}(k - \deg_q f'_i) \tag{3.73}$$

where the last inequality is because we assume that (3.49) holds strictly for $2 \leq |\Omega| \leq m-1$ and the first inequality is because $t'_i \geq t_i$ and

$$\left|\bigcap_{i\in\Omega} \mathcal{Z}'_i\right| = \left|\bigcap_{i\in\Omega} \mathcal{Z}_i - \{n\}\right| \geq \left|\bigcap_{i\in\Omega} \mathcal{Z}_i\right| - 1.$$

For $|\Omega| = m$, (3.49) was not strict; however, there is no need to have the $+1$ in (3.71) since

$$n \notin \mathcal{Z}_m \implies n \notin \bigcap_{i\in[m]} \mathcal{Z}_i \implies \left|\bigcap_{i\in\Omega} \mathcal{Z}'_i\right| = \left|\bigcap_{i\in\Omega} \mathcal{Z}_i\right|.$$

Therefore, (ii) holds for f'_i's. Hence, so does (i).

Suppose that for some $g_1, \ldots, g_m \in \mathsf{L}_n$, not all zero, with $\deg_q(g_i \circ f_i) \leq k-1$, we have

$$\sum_{i=1}^{m} g_i \circ x^{q^r} \circ f_i = 0.$$

We can further assume that at least one coefficient of one g_i is not divisible by x_n. (Otherwise, divide them by x_n.) Define $g'_i = g_i \mid_{x_n=0} \in \mathsf{L}_{n-1}$. Then, the g'_i's are not all zero. We can write

$$\sum_{i=1}^{m} g'_i \circ x^{q^r} \circ f'_i = \left(\sum_{i=1}^{m} g_i \circ x^{q^r} \circ f_i\right)\Bigg|_{x_n=0} = 0 \mid_{x_n=0} = 0. \tag{3.74}$$

Then, $g'_1 = \cdots = g'_m = 0$, which gives a contradiction. □

3.4 Conclusion

In this chapter, we extended our proof technique in [2] for Reed–Solomon codes to Gabidulin codes by writing an analog of the algebraic-combinatorial problem presented there. The main challenge in extending the result to Gabidulin codes was that, unlike polynomial multiplication, the composition operation between linearized polynomials is not commutative. As a result, we showed that the work of Halbawi *et al.* [14] can be applied to networks with any number of source nodes, which had been shown only for 3 source nodes.

Theorem 3.1 only claims the existence of Gabidulin codes since its proof is based on the multivariate polynomial $F(\alpha_1, \ldots, \alpha_n)$ being not identically zero. The same observation applies to subcodes of Gabidulin codes. In order to explicitly construct a Gabidulin code, we need to explicitly specify the evaluations points $\alpha_1, \ldots, \alpha_n$ for which F takes a nonzero value. One possible algorithm could be to generate random evaluation points until F takes a nonzero value. However, currently, we do not know the average complexity of this algorithm. Hence, how to construct such codes efficiently remains an important open problem. As a special case, when the generator matrix is systematic (i.e. $\mathcal{Z}_i = [k] \backslash \{i\}$), constructions of Gabidulin codes are given in [38].

3.A Proofs of some properties of linearized polynomials

P1. L_n *is a ring with no zero divisors under the addition and the composition operation* $\circ$.

Proof. Note that for any $a, b \in \mathsf{R}_n[x]$,

$$(a+b)^q = a^q + b^q. \tag{3.75}$$

Let $f = \sum_{i=0}^{d_1} f_i x^{q^i},\ g = \sum_{i=0}^{d_2} g_i x^{q^i} \in \mathsf{L}_n$. Then,

$$\begin{aligned} f \circ g &= f\left(\sum_{i=0}^{d_2} g_i x^{q^i}\right) \\ &= \sum_{i=0}^{d_2} f(g_i x^{q^i}) \\ &= \sum_{i=0}^{d_2} \sum_{j=0}^{d_1} f_j g_i^{q^j} x^{q^{i+j}} \in \mathsf{L}_n. \end{aligned}$$

Furthermore, if $f, g \neq 0$, then $f \circ g \neq 0$ since the leading coefficient, $f_{d_1} g_{d_2}^{q^{d_1}}$ is nonzero. Hence, L_n has no zero divisors.

By (3.75), for any $f, g, h \in \mathsf{L}_n$,

$$\begin{aligned} f \circ (g + h) &= f(g(x) + h(x)) \\ &= f(g(x)) + f(h(x)) \\ &= f \circ g + f \circ h. \end{aligned}$$

The other ring properties are trivial. □

P3. *For any finite-dimensional subspace $V \subset \mathsf{R}_n$ over $\mathbb{F}_q$ and $t \geq 0$,*

$$f = \prod_{\beta \in V} (x - \beta)^{q^t} \in \mathsf{L}_n \tag{3.76}$$

and $\deg_q f = t + \dim V$.

Proof. It is sufficient to prove it for $t = 0$ because

$$\prod_{\beta \in V} (x - \beta)^{q^t} = x^{q^t} \circ \prod_{\beta \in V} (x - \beta).$$

We do induction on $\dim V$. If $\dim V = 1$, then $V = \{\alpha a : \alpha \in \mathbb{F}_q\}$ for some $a \in \mathsf{R}_n$ and

$$\begin{aligned} \prod_{\beta \in V} (x - \beta) &= \prod_{\alpha \in \mathbb{F}_q} (x - \alpha a) \\ &= x^q - a^{q-1} x \in \mathsf{L}_n. \end{aligned}$$

Suppose $V' \subset V$ is a subspace such that $\dim V' = \dim V - 1$ and suppose $f' = \prod_{\beta \in V'} (x - \beta) \in \mathsf{L}_n$. Then, $V = \{\alpha a + b : \alpha \in \mathbb{F}_q, b \in V'\}$ for some $a \in \mathsf{R}_n$ and

$$\begin{aligned} \prod_{\beta \in V} (x - \beta) &= \prod_{\alpha \in \mathbb{F}_q, b \in V'} (x - \alpha a - b) \\ &= \prod_{\alpha \in \mathbb{F}_q} \prod_{b \in V'} ((x - \alpha a) - b) \\ &= \prod_{\alpha \in \mathbb{F}_q} f'(x - \alpha a) \\ &= \prod_{\alpha \in \mathbb{F}_q} (f'(x) - \alpha f'(a)) \\ &= [x^q - (f'(a))^{q-1} x] \circ f' \in \mathsf{L}_n. \end{aligned}$$

□

P7. *For any* $f_1 = \mathsf{f}(\mathcal{Z}_1, t_1), f_2 = \mathsf{f}(\mathcal{Z}_2, t_2) \in \mathcal{L}_{n,k}$*, we have*

$$\gcd\{f_1, f_2\} = \mathsf{f}(\mathcal{Z}_1 \cap \mathcal{Z}_2, \min\{t_1, t_2\}) \in \mathcal{L}_{n,k}.$$

Proof. Note that each root of f_i has a multiplicity of q^{t_i}. Therefore, the roots of gcd of f_1 and f_2 will be the elements of $\mathrm{span}\{x_j : j \in \mathcal{Z}_1\} \cap \mathrm{span}\{x_j : j \in \mathcal{Z}_2\} = \mathrm{span}\{x_j : j \in \mathcal{Z}_1 \cap \mathcal{Z}_2\}$, each with a multiplicity of $\min\{t_1, t_2\}$. □

P8. *If* $f_1, f_2 \in \mathcal{L}_{n,k}$ *and* $f_2 \mid f_1$*, then* $\exists f_1' \in \mathsf{L}_n,\ f_1 = f_1' \circ f_2$.

Proof. Let $f_1 = \mathsf{f}(\mathcal{Z}_1, t_1)$ and $f_2 = \mathsf{f}(\mathcal{Z}_2, t_2)$. Since each root of f_i has a multiplicity of q^{t_i}, we have $t_2 \leq t_1$. Furthermore, the roots of f_2 are also roots of f_1:

$$\mathrm{span}\{x_j : j \in \mathcal{Z}_2\} \subset \mathrm{span}\{x_j : j \in \mathcal{Z}_1\}.$$

Hence, $\mathcal{Z}_2 \subset \mathcal{Z}_1$. Then,

$$\begin{aligned}
f_1 &= \prod_{\beta \in \mathrm{span}\{x_j : j \in \mathcal{Z}_1\}} (x - \beta)^{q^{t_1}} \\
&= \prod_{a \in \mathrm{span}\{x_j : j \in \mathcal{Z}_1 - \mathcal{Z}_2\}} \ \prod_{b \in \mathrm{span}\{x_j : j \in \mathcal{Z}_2\}} (x - a - b)^{q^{t_1}} \\
&= \prod_{a \in \mathrm{span}\{x_j : j \in \mathcal{Z}_1 - \mathcal{Z}_2\}} (f_2(x - a))^{q^{t_1 - t_2}} \\
&= \prod_{a \in \mathrm{span}\{x_j : j \in \mathcal{Z}_1 - \mathcal{Z}_2\}} (f_2(x) - f_2(a))^{q^{t_1 - t_2}} \\
&= \prod_{\beta \in \mathrm{span}\{f_2(x_j) : j \in \mathcal{Z}_1 - \mathcal{Z}_2\}} (f_2(x) - \beta)^{q^{t_1 - t_2}} \\
&= f' \circ f_2
\end{aligned}$$

where $f' = \prod_{\beta \in \mathrm{span}\{f_2(x_j) : j \in \mathcal{Z}_1 - \mathcal{Z}_2\}} (x - \beta)^{q^{t_1 - t_2}} \in \mathsf{L}_n$. □

P9. *Let* $f = \mathsf{f}(\mathcal{Z}, t) \in \mathcal{L}_{n,k}$ *and let* $f' = f|_{x_n = 0} \in \mathsf{L}_{n-1}$ *(substitute* $x_n = 0$ *in each coefficient of* f*). Then,* $f' \in \mathcal{L}_{n-1,k}$ *and*

$$f' = \begin{cases} \mathsf{f}(\mathcal{Z}, t) & n \notin \mathcal{Z} \\ \mathsf{f}(\mathcal{Z} - \{n\}, t + 1) & n \in \mathcal{Z} \end{cases}. \tag{3.77}$$

Proof. It is trivial when $n \notin \mathcal{Z}$. So, suppose $n \in \mathcal{Z}$. Then,

$$\begin{aligned}
f' &= \left(\prod_{\beta \in \mathrm{span}\{x_i : i \in \mathcal{Z}\}} (x-\beta)^{q^t} \right) \Bigg|_{x_n=0} \\
&= \left(\prod_{\beta \in \mathrm{span}\{x_i : i \in \mathcal{Z}-\{n\}\}} \prod_{\alpha \in \mathbb{F}_q} (x-\beta-\alpha x_n)^{q^t} \right) \Bigg|_{x_n=0} \\
&= \prod_{\beta \in \mathrm{span}\{x_i : i \in \mathcal{Z}-\{n\}\}} \prod_{\alpha \in \mathbb{F}_q} (x-\beta)^{q^t} \\
&= \prod_{\beta \in \mathrm{span}\{x_i : i \in \mathcal{Z}-\{n\}\}} (x-\beta)^{q^{t+1}} \\
&= \mathsf{f}(\mathcal{Z}-\{n\}, t+1) \in \mathcal{L}_{n-1,k}.
\end{aligned}$$

□

Chapter 4

SUPPORT CONSTRAINED GABIDULIN CODES OVER CHARACTERISTIC ZERO

4.1 Introduction

Over finite fields, Gabidulin codes [7], [8] can be seen as a rank-metric equivalent of Reed–Solomon codes, where instead of evaluating ordinary polynomials, one uses *linearized polynomials* (i.e., whose only nonzero coefficients are for monomials whose degree is a nonnegative integer power of the field characteristic). To properly generalize this definition to fields of characteristic zero, it was recently suggested in [9] to employ θ–polynomials, which are linear combinations of compositions of a generator θ of the underlying Galois group of the field extension (that must be cyclic).

Independently, there has been a surge of interest lately in constructing sparsest generator matrices for Reed–Solomon and Gabidulin codes [3], [5], [11], [13], [26], for several applications in distributed computing. Since the rows of a generator matrix are codewords, each row cannot contain more than $k-1$ zeros according to the Singleton bound, where k is the dimension of the code. The so-called GM–MDS conjecture, posed by [11] and solved by [3] and [26], asserts that this maximum number of zeros at every row is attainable, as long as a certain condition regarding the position of zeros is satisfied. Specifically, this condition requires the zero-entries at every set of rows to intersect in at most k minus the number of rows in the intersection.

In this chapter, we complete the picture by showing that the same condition is necessary and sufficient for the existence of sparse generator matrices for Gabidulin codes over fields of characteristic zero. We note that while the proof of the equivalent condition for Reed–Solomon is identical for finite fields and fields of characteristic zero, for Gabidulin codes this is *not* the case, and the proof from [5] fails over the latter fields. However, by adopting notions from the Reed–Solomon equivalent (the "Simplified GM–MDS conjecture" [3, Thm. 3]), and combining it with a variant of the well-known Schwartz–Zippel lemma, we are able to resolve the problem over fields of characteristic zero. Moreover, our proof also provides a randomized construction algorithm whose probability of success can be arbitrarily high; similar

randomized construction algorithms exist for the finite variants of the problem, but their probability of success is lower.

Beyond their application in network coding [21], space-time codes [39], and cryptography [40], Gabidulin codes have applications in *low rank matrix recovery* [41] (LRMR), which is normally performed over fields of characteristic zero. In this problem, one reconstructs a low-rank matrix from a given set of linear measurements. If these linear measurements are given by multiplication of the unknown matrix by a parity-check matrix of a Gabidulin code, this problem reduces to syndrome decoding of the respective zero codeword. Since the parity-check matrix of a Gabidulin code has a similar structure to that of the generator matrix [9, Prop. 8], our results imply that when performing LRMR with Gabidulin codes, one may employ linear measurements that depend on a small number of entries of the unknown matrix.

The problem is formally stated in Section 4.2, along necessary mathematical background. Our main results are summarized in Section 4.3, and proved in Section 4.5 by using auxiliary claims given in Section 4.4.

Notations

Let $[n] = \{1, 2, \ldots, n\}$. Denote the dimension of a subspace V over a field F by $\dim_{\mathsf{F}} V$ and the span of the elements in a set S over the field F by $\mathrm{span}_{\mathsf{F}} S$. The (total) degree of a (multivariate) polynomial f is denoted by $\deg f$ (e.g. $\deg(x^2y^2 + x^3) = 4$). For an $m \times n$ matrix $\mathbf{X}$ and $I \subseteq [m], J \subseteq [n]$, $\mathbf{X}_{I,J}$ is the submatrix with the columns and rows indexed in I and J respectively. Let $\mathbf{X}_{I,:} = \mathbf{X}_{I,[n]}$ and $\mathbf{X}_{:,J} = \mathbf{X}_{[m],J}$ and when I or J has a single element, we sometimes write the element only, instead of the set.

4.2 Problem Setup

In this section, we will first provide a brief background on cyclic Galois extensions. Then, we will define rank metric codes and Gabidulin codes. Finally, we will define our problem, namely, finding Gabidulin codes with support constrained generator matrices over a field of characteristic zero.

Field extensions

Let E/F be a field extension of finite degree, i.e. the dimension of E as a vector space over F is finite, and let $\dim_{\mathsf{F}} \mathsf{E} = m$. The automorphism group of E/F, $\mathrm{Aut}(\mathsf{E}/\mathsf{F})$,

is the set of automorphisms of E that fix F, i.e.

$$\mathrm{Aut}(\mathsf{E}/\mathsf{F}) = \{\theta : \mathsf{E} \to \mathsf{E} \text{ automorphism} \mid \forall x \in \mathsf{F}, \theta(x) = x\},$$

with the group operation of function composition $\circ$. If $|\mathrm{Aut}(\mathsf{E}/\mathsf{F})| = m$, E/F is called a Galois extension, in which case, $\mathrm{Aut}(\mathsf{E}/\mathsf{F})$ is also denoted by $\mathrm{Gal}(\mathsf{E}/\mathsf{F})$ and is called the Galois group of E/F.

In this chapter, we will focus on cyclic Galois extensions, whose Galois group is a cyclic group of order m:

$$\mathrm{Gal}(\mathsf{E}/\mathsf{F}) = \{\theta^0, \theta^1, \ldots, \theta^{m-1}\}$$

where the automorphism θ is the generator and $\theta^{i+1} = \theta \circ \theta^i$ for every $i \geq 0$. Notice that $\theta^m = \theta^0$ is the identity automorphism.

For example, for finite fields, when $\mathsf{F} = \mathbb{F}_q$ and $\mathsf{E} = \mathbb{F}_{q^m}$, the Galois group is cyclic of order m with the generator automorphism $\theta(x) = x^q$:

$$\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \left\{x, x^q, x^{q^2}, \ldots, x^{q^{m-1}}\right\}.$$

For infinite fields, when $\mathsf{F} = \mathbb{Q}$ is the set of rational numbers and $\mathsf{E} = \mathbb{Q}(\zeta_n)$, where ζ_n is the n'th root of unity, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension of degree $\varphi(n)$, where $\varphi(n)$ is the Euler's phi function ($\mathbb{Q}(\zeta_n)$ is called the n'th cyclotomic field and an interested reader can refer to [42]). Its Galois group is isomorphic to the multiplicative group $\mathbb{Z}_n^*$ of integers modulo n. Since $\mathbb{Z}_n^*$ is cyclic for $n = p^a, 2p^a$ [43], where p is any odd prime and a is any positive integer, it follows that for these values of n, we have that $\mathbb{Q}(\zeta_n)$ is a cyclic Galois extension of degree $m = \varphi(n) = p^{a-1}(p-1)$. It is also possible to define cyclic extensions of $\mathbb{Q}$ for any degree m by considering subfields of $\mathbb{Q}(\zeta_p)$ for an odd prime p such that $p-1$ is divisible by m.

Rank metric codes

A linear rank metric code, $[n, k, d]_{\mathsf{E}/\mathsf{F}}$, over a field extension E/F is an E–subspace $\mathcal{C}$ of E^n of dimension k with the rank distance

$$d = d_R(\mathcal{C}) \triangleq \min_{0 \neq \mathbf{c} \in \mathcal{C}} \dim_{\mathsf{F}}(\mathrm{span}_{\mathsf{F}}\{c_1, \ldots, c_n\}) \tag{4.1}$$

where $c_1, \ldots, c_n \in \mathsf{E}$ represent the entries of $\mathbf{c} \in \mathsf{E}^n$. By fixing an ordered basis of E over F, the elements of E can be considered as vectors in F^m, and then the codewords (i.e. the elements of $\mathcal{C} \subset \mathsf{E}^n$) can be viewed as $m \times n$ matrices over F.

Then, this definition of the rank distance in (4.1) is equivalent to the minimum of the rank of the matrix representation of a nonzero codeword.

Notice that, by definition in (4.1), the rank distance of $\mathcal{C}$ can be upper bounded by the Hamming distance, $d_H(\mathcal{C}) \triangleq \min_{0 \neq c \in \mathcal{C}} \|c\|_0$, where $\|c\|_0$ is the number of nonzero entries of c. Therefore, the Singleton bound can be written for the rank distance as well:

$$d_R(\mathcal{C}) \leq d_H(\mathcal{C}) \leq n - k + 1. \tag{4.2}$$

The codes with $d_R(\mathcal{C}) = n - k + 1$ are called maximum rank distance (MRD), for which we write $[n, k]_{\mathsf{E/F}}$ by omitting d. A generator matrix for an $[n, k, d]_{\mathsf{E/F}}$ code $\mathcal{C}$ is a $k \times n$ matrix over E whose rows form a basis for $\mathcal{C}$.

Gabidulin codes

Gabidulin codes are defined as the row space of the $k \times n$ matrix

$$\begin{bmatrix} \theta^0(x_1) & \theta^0(x_2) & \cdots & \theta^0(x_n) \\ \theta^1(x_1) & \theta^1(x_2) & \cdots & \theta^1(x_n) \\ \vdots & \vdots & & \vdots \\ \theta^{k-1}(x_1) & \theta^{k-1}(x_2) & \cdots & \theta^{k-1}(x_n) \end{bmatrix} \in \mathsf{E}^{k \times n} \tag{4.3}$$

where $\theta \in \mathrm{Aut}(\mathsf{E/F})$ and $x_1, \ldots, x_n \in \mathsf{E}$ are F–linearly independent (notice that this requires $n \leq m = \dim_{\mathsf{F}} \mathsf{E}$). Note that Gabidulin codes can be seen as evaluation codes of the so-called θ–polynomials; a θ–polynomial is a function $f : \mathsf{E} \to \mathsf{E}$ of the form $f(x) = \sum_i f_i \theta^i(x)$ for $f_i \in \mathsf{E}$, and every codeword in a Gabidulin code is the evaluations of some θ–polynomial of θ–degree at most $k - 1$. Note also that the generator matrix can be chosen as the product of any $k \times k$ invertible matrix over E and the matrix in (4.3).

Originally, this was defined by Delsarte [7] and Gabidulin [8] for the finite fields, when $\mathsf{F} = \mathbb{F}_q$, $\mathsf{E} = \mathbb{F}_{q^m}$, and $\theta(x) = x^q$, as the first general constructions of MRD codes over finite fields. Later [9], it was extended to fields of characteristic zero, and it was shown that when $\mathsf{E/F}$ is a cyclic Galois extension and θ is the generator of $\mathrm{Gal}(\mathsf{E/F})$, this extension of Gabidulin codes also gives an $[n, k]_{\mathsf{E/F}}$ MRD code [9]. In the rest of the chapter, we will assume that $\mathsf{E/F}$ is a cyclic Galois extension of order m and F is of characteristic zero.

Problem definition

We consider the problem of finding an $[n, k]_{\mathsf{E/F}}$ MRD code whose generator matrix $\mathbf{G} \in \mathsf{E}^{k \times n}$ has support constraints. We describe the support constraints through the

subsets $\mathcal{Z}_1, \mathcal{Z}_2, \ldots, \mathcal{Z}_k \subset [n]$ as

$$\mathbf{G}_{ij} = 0, \qquad \forall j \in \mathcal{Z}_i, i = 1, 2, \ldots, k. \tag{4.4}$$

Over finite fields, this problem was studied in [5] and it was shown that a necessary and sufficient condition for the existence of MRD codes under support constraints described by the $\mathcal{Z}_i$ is

$$\left|\bigcap_{i\in\Omega} \mathcal{Z}_i\right| + |\Omega| \leq k, \quad \forall \varnothing \neq \Omega \subseteq [k]. \tag{4.5}$$

The same condition also appears in the GM–MDS conjecture for MDS codes (i.e. $d_H = n - k + 1$, see [11], and also [13], [16]) which was proven in [3] and [26].

Over infinite fields, the fact that (4.5) is necessary can be shown similar to [3], since MRD codes are also MDS (4.2), and since the proof in [3] applies to both finite and infinite fields. However, a similar proof to [5] cannot be applied to show that (4.5) is sufficient when F has characteristic zero. The reason is that in finite fields, since the generator matrix in (4.3) consists of entries in the form of polynomials in the x_i's, which, in one step of the proof, allows to reduce the problem to a similar one with a smaller parameter, whereas in the characteristic zero, the entries are in the form of θ–polynomials (defined in [9]) and applying the same step turns the problem into one of a different kind. Hence, in this chapter, we will show that (4.5) is sufficient for the existence of $[n, k]_{\mathsf{E/F}}$ MRD codes under the support constraints on the generator matrix given in (4.4) when F has characteristic zero.

4.3 Main Results

In this section, we present our main results on the existence of MRD codes in characteristic zero (see Theorem 4.1) and the best achievable rank distance for the cases where there does not exist any (see Corollary 4.1). Also, we will give a randomized algorithm for the code construction. The proofs of the theorems will be given in Section 4.5.

Theorem 4.1. *Let $\mathsf{E/F}$ be a cyclic Galois extension of degree m such that F has characteristic zero. For some $k \leq n \leq m$, let $\mathcal{Z}_1, \ldots, \mathcal{Z}_k \subset [n]$ satisfy (4.5). Then, there exists an $[n, k]_{\mathsf{E/F}}$ Gabidulin code with a generator matrix satisfying the constraints in (4.4).*

If the $\mathcal{Z}_i$'s do not satisfy (4.5), then as given in [5] and [3], $d_R \leq d_H \leq n + 1 - \max\limits_{\varnothing\neq\Omega\subseteq[k]} \left(\left|\bigcap_{i\in\Omega} \mathcal{Z}_i\right| + |\Omega|\right) < n-k+1$, and hence, an MRD code does not exist. For

this case, Corollary 4.1 below (which is the analog of [5, Thm. 2]) shows that this upper bound is achievable by the subcodes (i.e the subspaces) of Gabidulin codes.

Corollary 4.1. *In Theorem 4.1, if the $\mathcal{Z}_i$'s do not satisfy (4.5), then there exists an $[n, k, n-\ell+1]_{\mathsf{E/F}}$ subcode of an $[n, \ell]_{\mathsf{E/F}}$ Gabidulin code, which satisfies (4.4), where*

$$\ell = \max_{\varnothing \neq \Omega \subseteq [k]} \left(\left| \bigcap_{i \in \Omega} \mathcal{Z}_i \right| + |\Omega| \right). \tag{4.6}$$

Proof. Define $\mathcal{Z}_{k+1} = \cdots = \mathcal{Z}_\ell = \varnothing$. Then, for any nonempty $\Omega \subseteq [\ell]$, we have that $\left|\bigcap_{i\in\Omega} \mathcal{Z}_i\right| + |\Omega| \leq \ell$. Hence, by Theorem 4.1, there exists an $[n, \ell, n-\ell+1]_{\mathsf{E/F}}$ Gabidulin code with an $\ell \times n$ generator matrix $\mathbf{G}$ having zeros dictated by $\mathcal{Z}_1, \ldots, \mathcal{Z}_\ell$. The first k rows of $\mathbf{G}$ will generate a subcode whose rank distance d_R is as good as the Gabidulin code: $d_R \geq n - \ell + 1$. Furthermore, $n - \ell + 1$ is an upper bound on d_H [3]. Therefore, $n - \ell + 1 \leq d_R \leq d_H \leq n - \ell + 1$. Hence, $d_R = n - \ell + 1$. □

Code Construction

Fix an F–basis $\{b_1, \ldots, b_m\}$ for E and assume that the conditions for the $\mathcal{Z}_i$ in Theorem 4.1 are satisfied, i.e. $\mathcal{Z}_1, \ldots, \mathcal{Z}_k \subset [n]$ satisfy (4.5). Then, each $\mathcal{Z}_i$ has at most $k-1$ elements by applying (4.5) with $|\Omega| = 1$. In [11, Thm. 2] and [5, Corollary 3], it is shown that one can keep adding elements to these sets from $[n]$ without violating any of the inequalities in (4.5) until each $\mathcal{Z}_i$ has exactly $k-1$ elements. Note that adding elements to these sets will only put more zero constraints on the generator matrix. Therefore, without loss of generality, we can assume that $|\mathcal{Z}_i| = k - 1$ for all i along with (4.5). Then, we construct a generator matrix for a rank metric code in a randomized manner as described below:

Inputs: A finite nonempty set $S \subset \mathsf{F}$ and subsets $\mathcal{Z}_1, \ldots, \mathcal{Z}_k \subset [n]$ satisfying (4.5).

Steps:

- Add elements to the $\mathcal{Z}_i$'s from $[n]$ (if necessary) by following the algorithm given in [11, Thm. 2] so that they all have *exactly* $k-1$ elements and *still* satisfy (4.5).
- Choose $(\gamma_{ij})_{i\in[n],j\in[m]}$ uniformly at random from S.
- Let $x_i = \sum_{j=1}^{m} \gamma_{ij} b_j$ for $i \in [n]$.
- Construct $\mathbf{A} \in \mathsf{E}^{k\times n}$ as in (4.3) in terms of $x_1, \ldots, x_n$.
- Define $\mathbf{T} \in \mathsf{E}^{k\times k}$ as

$$\mathbf{T}_{ij} = \det\begin{bmatrix}\mathbf{e}_j & \mathbf{A}_{:,\mathcal{Z}_i}\end{bmatrix}, \quad i,j \in [k] \tag{4.7}$$

  where $\mathbf{e}_j$ is the column vector with 1 at the jth entry and 0's elsewhere (Note that $|\mathcal{Z}_i| = k-1$).

Output: The generator matrix $\mathbf{G} = \mathbf{T}\cdot\mathbf{A} \in \mathsf{E}^{k\times n}$.

By Lemma 4.1 below, $\mathbf{G}$ in the above construction is guaranteed to satisfy (4.4) for any inputs.

Lemma 4.1. *Let $\mathcal{Z}_1, \ldots, \mathcal{Z}_k \subset [n]$ be subsets of size $k-1$. For a given $k\times n$ matrix $\mathbf{A}$, a $k\times k$ matrix $\mathbf{T}$ (over the same field as $\mathbf{A}$) satisfying $(\mathbf{T}\cdot\mathbf{A})_{ij} = 0$ for every $j \in \mathcal{Z}_i$ and $i \in [k]$ can be given as in (4.7).*

Proof. For a fixed $i \in [k]$, the statement $(\mathbf{T}\cdot\mathbf{A})_{ij} = 0$ for every $j \in \mathcal{Z}_i$ is equivalent to the equation $\mathbf{T}_{i,:}\cdot\mathbf{A}_{:,\mathcal{Z}_i} = 0$. A solution $\mathbf{T}_{i,:}$ to this equation can be described in terms of the adjugate of the $k\times k$ square matrix $\mathbf{P} = \begin{bmatrix}0_{k\times 1} & \mathbf{A}_{:,\mathcal{Z}_i}\end{bmatrix}$. Recall that $\operatorname{adj}\mathbf{P}$ is the transpose of the cofactor matrix $\left[(-1)^{i+j}\det(\mathbf{P}_{[k]\setminus\{i\},[k]\setminus\{j\}})\right]_{i,j\in[k]}$ and satisfies $\operatorname{adj}(\mathbf{P})\mathbf{P} = \det(\mathbf{P})\mathbf{I}_{k\times k}$. Since $\mathbf{P}$ has an all zero column, we have $\det\mathbf{P} = 0$, which implies $\operatorname{adj}(\mathbf{P})\mathbf{P} = 0$. Furthermore, due to the zero column in $\mathbf{P}$, the entries of $\operatorname{adj}\mathbf{P}$ are zero except the first row, whose entries are for $j \in [k]$,

$$(\operatorname{adj}\mathbf{P})_{1,j} = (-1)^{j+1}\det(\mathbf{P}_{[k]\setminus\{j\},[k]\setminus\{1\}})$$

$$= (-1)^{j+1} \det(\mathbf{A}_{[k]\setminus\{j\},\mathcal{Z}_i})$$
$$= \det \begin{bmatrix} \mathbf{e}_j & \mathbf{A}_{:,\mathcal{Z}_i} \end{bmatrix} = \mathbf{T}_{i,j}.$$

Since $(\operatorname{adj} \mathbf{P})_{1,:} \cdot \mathbf{P} = 0$ and $(\operatorname{adj} \mathbf{P})_{1,:} \cdot \mathbf{A}_{:,\mathcal{Z}_i} = 0$, the row vector $\mathbf{T}_{i,:} = (\operatorname{adj} \mathbf{P})_{1,:}$ satisfies $\mathbf{T}_{i,:} \cdot \mathbf{A}_{:,\mathcal{Z}_i} = 0$. □

Furthermore, if $x_1, \ldots, x_n$ are F–linearly independent and the matrix $\mathbf{T}$ is invertible (i.e. $\det \mathbf{T} \neq 0$), then the code generated by $\mathbf{G}$ is an $[n, k]_{\mathsf{E}/\mathsf{F}}$ Gabidulin code since the row spaces of $\mathbf{A}$ and $\mathbf{G} = \mathbf{T} \cdot \mathbf{A}$ are identical. In Theorem 4.2, we give a lower bound on the probability of this construction giving an MRD code.

Theorem 4.2. *If the conditions in Theorem 4.1 are satisfied, then the generator matrix* $\mathbf{G}$ *randomly constructed as described above will satisfy (4.4) and generate an* $[n, k]_{\mathsf{E}/\mathsf{F}}$ *Gabidulin code with probability at least* $1 - \frac{n+k(k-1)}{|S|}$.

Since F is infinite, S can be arbitrarily large. Therefore, the probability of constructing an MRD code can be arbitrarily close to 1.

Furthermore, if the $\mathcal{Z}_i$ do not satisfy (4.5), then by following the proof of Corollary 4.1, we can construct a rank metric code achieving the largest possible rank distance for the given support constraints.

4.4 More on Cyclic Galois Extensions

Before moving to the proofs of the theorems, in this section, we will give some useful properties of the automorphisms in $\operatorname{Gal}(\mathsf{E}/\mathsf{F}) = \{\theta^0, \theta^1, \ldots, \theta^{m-1}\}$.

Linear independence of the elements in E

Lemma 4.2 lists some equivalent conditions to the F–linear dependence of the elements of E in terms of the automorphisms in $\operatorname{Gal}(\mathsf{E}/\mathsf{F})$. The first two of these conditions can be also seen as a special case of [9, Prop. 5], where the authors give equivalent rank metrics for the elements of E^n, whereas Lemma 4.2 only claims that these rank metrics simultaneously declare rank deficiency (i.e. return a rank less than n) for a given element of E^n. It is worth noting, as shown by Augot *et al.* [9], that the assumption that the extension E/F is cyclic plays an important role in Lemma 4.2. This is since its proof relies on the fact that θ fixes *only* the elements of F (i.e. for any $x \in \mathsf{E}$, $\theta(x) = x$ if and only if $x \in \mathsf{F}$), which is the case for the cyclic extensions.

Lemma 4.2. *Let* $n \leq m = \dim_{\mathsf{F}} \mathsf{E}$*,* $x_1, \ldots, x_n \in \mathsf{E}$*, and*

$$\mathbf{M} = \begin{bmatrix} \theta^0(x_1) & \theta^0(x_2) & \cdots & \theta^0(x_n) \\ \theta^1(x_1) & \theta^1(x_2) & \cdots & \theta^1(x_n) \\ \vdots & \vdots & & \vdots \\ \theta^{m-1}(x_1) & \theta^{m-1}(x_2) & \cdots & \theta^{m-1}(x_n) \end{bmatrix} \in \mathsf{E}^{m \times n}. \tag{4.8}$$

Then, the following are equivalent:

(i) $x_1, \ldots, x_n$ *are* F*–linearly dependent.*

(ii) The columns of $\mathbf{M}$ *are* E*–linearly dependent.*

(iii) The top $n \times n$ *minor of* $\mathbf{M}$ *is zero, i.e.* $\det \mathbf{M}_{[n],[n]} = 0$*.*

Proof. If $x_i = 0$ for some i, then the claim is trivial, and hence assume that $x_i \neq 0$ for every i.

$(ii) \implies (i)$: Let ℓ be the minimum number of columns of $\mathbf{M}$ that are E–linearly dependent and w.l.o.g. assume that

$$\mathbf{M}_{:,\ell} = \sum_{i=1}^{\ell-1} \beta_i \mathbf{M}_{:,i}$$

for some unique $\beta_1, \ldots, \beta_{\ell-1} \in \mathsf{E}$, which implies that $\theta^{j-1}(x_\ell) = \sum_{i=1}^{\ell-1} \beta_i \theta^{j-1}(x_i)$ for every $j \in [m]$. Then, applying θ to both sides gives $\theta^j(x_\ell) = \sum_{i=1}^{\ell} \theta(\beta_i)\theta^j(x_i)$, which implies that $\mathbf{M}_{:,\ell} = \sum_{i=1}^{\ell-1} \theta(\beta_i)\mathbf{M}_{:,i}$ as $\theta^m = \theta^0$. Since the β_i's are unique, it follows that $\theta(\beta_i) = \beta_i$, which implies that $\beta_i \in \mathsf{F}$. Since $\theta^0(x) = x$, we have $x_\ell = \sum_{i=1}^{\ell} \beta_i x_i$ for $\beta_i \in \mathsf{F}$.

$(iii) \implies (ii)$: If the top $n \times n$ minor of $\mathbf{M}$ is zero, then there exists $\ell \leq n$ such that the ℓ'th row of $\mathbf{M}$ is in the E–span of the first $\ell - 1$ rows. By induction, it can be shown that for any $i \geq \ell$, the i'th row is in the span of the first $\ell - 1$ rows. To see how, assume for some $\beta_1, \ldots, \beta_{\ell-1} \in \mathsf{E}$, $\theta^{i-1}(x_j) = \sum_{t=1}^{\ell-1} \beta_t \theta^{t-1}(x_j)$ for all j. Then, by applying θ to both sides, it follows that the $(i+1)$'th row is a linear combination of the first ℓ rows; hence it is also in the span of the first $\ell - 1$ rows. As a result, $\operatorname{rank} \mathbf{M} \leq \ell - 1 < n$, which implies (ii).

$(i) \implies (iii)$: Assume that $\sum_{i=1}^{n} \beta_i x_i = 0$ for some $\beta_i \in \mathsf{F}$. Then, for any j, applying θ^j to both sides yields $\sum_{i=1}^{n} \beta_i \theta^j(x_i) = 0$ since $\theta^j(\beta_i) = \beta_i$, which implies (iii). □

Schwartz–Zippel Lemma for automorphisms

Recall the Schwartz–Zippel Lemma, which states that for a nonzero multivariate polynomial f in n variables over a field, a point uniformly chosen at random from S^n, where S is a nonempty finite subset of this field, will be a root of f with probability at most $\frac{\deg f}{|S|}$. In this section, we will give an extension of the Schwartz–Zippel Lemma for a special type of functions from E^n to E. More precisely, for a given multivariate polynomial f over E in mn variables (seen as an $m \times n$ matrix), we will consider the function $g(x_1, \ldots, x_n) = f([\theta^{i-1}(x_j)]_{i\in[m],j\in[n]})$ and give a bound on the probability of a randomly chosen point being a zero of g. Later, this will help us to derive the bound on the probability given in Theorem 4.2.

Lemma 4.3. *Let $\{b_1, \ldots, b_m\}$ be an F–basis for E. Let f be a nonzero multivariate polynomial over E in mn variables. Let $\mathbf{M} \in \mathsf{E}^{m\times n}$ be defined as in (4.8) for $x_j = \sum_{i=1}^{m} \mathbf{\Gamma}_{ij} b_i$, where the $\mathbf{\Gamma}_{ij}$ are independently uniformly chosen at random from a finite nonempty subset $S \subset \mathsf{F}$. Then,*

$$\mathbb{P}(f(\mathbf{M}) = 0) \leq \frac{\deg f}{|S|}.$$

Proof. Define another polynomial f' as $f'(\mathbf{X}) = f(\mathbf{BX})$ in the variables $\mathbf{X}_{ij}$, $i \in [m], j \in [n]$, where $\mathbf{B} = [\theta^{i-1}(b_j)]_{i,j\in[m]}$ is an $m \times m$ matrix defined as in (4.8) for $b_1, \ldots, b_m$. Since $\{b_1, \ldots, b_m\}$ is an F–basis, the b_i are F–linearly independent and by Lemma 4.2, $\mathbf{B}$ is invertible. Then, f can be also written as $f(\mathbf{X}) = f'(\mathbf{B}^{-1}\mathbf{X})$. Hence, f' is also nonzero and $\deg f = \deg f'$. Furthermore, $f'(\mathbf{\Gamma}) = f(\mathbf{B\Gamma}) = f(\mathbf{M})$ since

$$\begin{aligned}
\mathbf{M}_{ij} &= \theta^{i-1}(x_j) \\
&= \theta^{i-1}\left(\textstyle\sum_{t=1}^{m} b_t \mathbf{\Gamma}_{tj}\right) \\
&= \textstyle\sum_{t=1}^{m} \theta^{i-1}(b_t)\mathbf{\Gamma}_{tj} \\
&= (\mathbf{B\Gamma})_{ij}
\end{aligned}$$

where we use $\theta^{i-1}(\mathbf{\Gamma}_{tj}) = \mathbf{\Gamma}_{tj}$ since $\mathbf{\Gamma}_{tj} \in \mathsf{F}$. Now, applying the Schwartz–Zippel Lemma to the polynomial f' gives $\mathbb{P}(f'(\mathbf{\Gamma}) = 0) \leq \frac{\deg f'}{|S|}$. Hence, $\mathbb{P}(f(\mathbf{M}) = 0) \leq \frac{\deg f}{|S|}$. □

4.5 Proofs of Theorem 4.1 and Theorem 4.2

First of all, notice that it is sufficient to prove Theorem 4.2 since it implies Theorem 4.1 when S is chosen sufficiently large. Assume $x_1, \ldots, x_n$ are chosen as

described in Theorem 4.2. We know that the code with the generator matrix $\mathbf{T} \cdot \mathbf{A}$, which satisfies (4.4) by Lemma 4.1, is an $[n,k]_{\mathsf{E/F}}$ Gabidulin code if the x_i's are F–linearly independent and $\mathbf{T}$ is invertible. Define $\mathbf{M} \in \mathsf{E}^{m \times n}$ as in Lemma 4.2, by which the x_i's are F–linearly independent iff $\det \mathbf{M}_{[n],:} \neq 0$. Furthermore, since $\mathbf{A} = \mathbf{M}_{[k],:}$, we have that

$$\mathbf{T} = \left[\det \begin{bmatrix} \mathbf{e}_j & \mathbf{A}_{:,\mathcal{Z}_i} \end{bmatrix}\right]_{i,j \in [k]} = \left[\det \begin{bmatrix} \mathbf{e}_j & \mathbf{M}_{[k],\mathcal{Z}_i} \end{bmatrix}\right]_{i,j \in [k]}.$$

Therefore, it is sufficient to show that $\mathbb{P}(\det \mathbf{T} \cdot \det \mathbf{M}_{[n],:} \neq 0) \geq 1 - \frac{n+k(k-1)}{|S|}$ or that $\mathbb{P}(\det \mathbf{T} \cdot \det \mathbf{M}_{[n],:} = 0) \leq \frac{n+k(k-1)}{|S|}$.

In order to show this, we will appeal to Lemma 4.3. Define the multivariate polynomial

$$f(\mathbf{X}) = \det \left(\left[\det \begin{bmatrix} \mathbf{e}_j & \mathbf{X}_{[k],\mathcal{Z}_i} \end{bmatrix}\right]_{i,j \in [k]} \right) \cdot \det \mathbf{X}_{[n],:} \tag{4.9}$$

for the variables $\mathbf{X}_{ij}$, $i \in [m], j \in [n]$ seen as an $m \times n$ matrix $\mathbf{X}$. Then, it suffices to show that $\mathbb{P}(f(\mathbf{M}) = 0) \leq \frac{n+k(k-1)}{|S|}$. Hence, by Lemma 4.3, all we need to show is that f is a nonzero polynomial with total degree at most $n + k(k-1)$.

To show the bound on the degree of f, recall the Leibniz formula for the determinant of an $n \times n$ square matrix $\mathbf{Z}$, which is $\det \mathbf{Z} = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} \mathbf{Z}_{\pi(i),i}$, where S_n is the permutation group of size n and $\operatorname{sgn}(\pi)$ is the sign of the permutation π. Thus, when the entries of $\mathbf{Z}$ are polynomials, we can write

$$\deg \det \mathbf{Z} \leq \sum_{j \in [n]} \max_{i \in [n]} \deg \mathbf{Z}_{i,j}. \tag{4.10}$$

Hence, $\deg \det \mathbf{X}_{[n],:} \leq n$ since each entry of $\mathbf{X}$ has degree one. Furthermore, $\deg \det \begin{bmatrix} \mathbf{e}_j & \mathbf{X}_{[k],\mathcal{Z}_i} \end{bmatrix} \leq k-1$; hence, $\deg \det \left(\left[\det \begin{bmatrix} \mathbf{e}_j & \mathbf{X}_{[k],\mathcal{Z}_i} \end{bmatrix}\right]_{i,j \in [k]} \right) \leq k(k-1)$. As a result, $\deg f \leq n + k(k-1)$.

To show that f is a nonzero polynomial, we will use the simplified GM–MDS conjecture of Dau *et al.* [11], which was proved in [3] and [26].

Lemma 4.4 (Simplified GM–MDS conjecture [3, Thm. 3][1])**.** *Let $\mathcal{Z}_1, \ldots, \mathcal{Z}_k \subset [n]$ be subsets of size $k-1$. Then, they satisfy (4.5) if and only if the determinant of the*

[1] Compared to [3, Thm. 3], in the statement of Lemma 4.4, the variable α_j is replaced with $-\alpha_j$ and the matrix $\mathbf{P}$ is flipped about its vertical axis, which may only change the sign of the determinant.

$k \times k$ matrix

$$\mathbf{P} = \begin{bmatrix} \prod_{t\in\mathcal{Z}_1}(-\alpha_t) & \cdots & \sum_{t\in\mathcal{Z}_1}(-\alpha_t) & 1 \\ \prod_{t\in\mathcal{Z}_2}(-\alpha_t) & \cdots & \sum_{t\in\mathcal{Z}_2}(-\alpha_t) & 1 \\ \vdots & & \vdots & \vdots \\ \prod_{t\in\mathcal{Z}_k}(-\alpha_t) & \cdots & \sum_{t\in\mathcal{Z}_k}(-\alpha_t) & 1 \end{bmatrix} \tag{4.11}$$

with entries $\mathbf{P}_{ij} = \sum_{\mathcal{S}\subseteq\mathcal{Z}_i,|\mathcal{S}|=k-j} \prod_{t\in\mathcal{S}}(-\alpha_t)$ is not the zero polynomial in the variables $\alpha_1, \ldots, \alpha_n$.

Notice that the i'th row of $\mathbf{P}$ in (4.11) consists of the coefficients of the polynomial

$$\prod_{j\in\mathcal{Z}_i}(X - \alpha_j) = \sum_{j=1}^{k} \mathbf{P}_{ij} X^{j-1} \tag{4.12}$$

in the variable X. We will also show that $\mathbf{P}$ can be written in the form of (4.7). To see how, define the $m \times n$ Vandermonde matrix $\mathbf{V} = \left[\alpha_j^{i-1}\right]_{i\in[m],j\in[n]}$. Fix $i \in [k]$ and consider the determinant of the $k \times k$ Vandermonde matrix $\mathbf{W} = \begin{bmatrix} \mathbf{v} & \mathbf{V}_{[k],\mathcal{Z}_i} \end{bmatrix}$, where $\mathbf{v}$ is a column vector whose j'th entry is X^{j-1} for $j \in [k]$:

$$\det \mathbf{W} = c_i \prod_{j\in\mathcal{Z}_i}(X - \alpha_j) \overset{(4.12)}{=} c_i \sum_{j\in[k]} \mathbf{P}_{ij} X^{j-1}$$

where $c_i = \prod_{j_1<j_2\in\mathcal{Z}_i}(\alpha_{j_1} - \alpha_{j_2}) \neq 0$. On the other hand, by the linearity of the determinant in the first column, we can write

$$\det \mathbf{W} = \sum_{j\in[k]} \det \begin{bmatrix} \mathbf{e}_j & \mathbf{V}_{[k],\mathcal{Z}_i} \end{bmatrix} X^{j-1},$$

since $\mathbf{v} = \sum_{j\in[k]} \mathbf{e}_j X^{j-1}$. As a result, the entries of $\mathbf{P}$ satisfy

$$c_i \mathbf{P}_{ij} = \det \begin{bmatrix} \mathbf{e}_j & \mathbf{V}_{[k],\mathcal{Z}_i} \end{bmatrix}. \tag{4.13}$$

Now, let us evaluate f in (4.9) at $\mathbf{V}$, which will give a multivariate polynomial in the variables α_j:

$$\begin{aligned} f(\mathbf{V}) &= \det\left(\left[\det\begin{bmatrix} \mathbf{e}_j & \mathbf{V}_{[k],\mathcal{Z}_i} \end{bmatrix}\right]_{i,j\in[k]}\right) \cdot \det \mathbf{V}_{[n],:} \\ &\overset{(4.13)}{=} \det\left(\left[c_i \mathbf{P}_{ij}\right]_{i,j\in[k]}\right) \cdot \det \mathbf{V}_{[n],:} \\ &= \det \mathbf{P} \cdot \left(\prod_{i\in[k]} c_i\right) \cdot \det \mathbf{V}_{[n],:}. \end{aligned}$$

By Lemma 4.4, $\det \mathbf{P}$ is a nonzero polynomial. Furthermore, we have that $c_i \neq 0$ and $\det \mathbf{V}_{[n],:} = \prod_{j_1<j_2\in[n]}(\alpha_{j_1} - \alpha_{j_2}) \neq 0$. Hence, $f(\mathbf{V})$ is not the zero polynomial in the variables α_j. Therefore, $f(\mathbf{X})$ itself cannot be the zero polynomial in the variables $\mathbf{X}_{ij}$. $\square$

Chapter 5

CONCLUDING REMARKS AND FUTURE DIRECTIONS

5.1 Central Problem: Generator Matrix under Support Constraints

The central problem in this thesis was to design linear codes with generator matrices under support constraints. For the Hamming metric, if the MDS condition holds, the existence of the Reed–Solomon codes over fields of size at least $n+k-1$ is shown. For the rank metric, if the MDS condition holds, the existence of the Gabidulin codes over the finite field extensions $\mathbb{F}_{q^s}/\mathbb{F}_q$ with $s \geq \max\{n, k-1+\log_q k\}$ and the field extensions of characteristic zero is shown. These results suggest some research directions to explore. We briefly describe two future directions for this problem.

Explicit Constructions

In order to design a Reed–Solomon code with support constraints satisfying the MDS condition, one needs to find distinct evaluation points $\alpha_1, \ldots, \alpha_n$ such that the matrix $\mathbb{M}$ in (2.8) is nonsingular. Similarly, to design a Gabidulin code with the same support constraints, one needs to find evaluation points $\alpha_1, \ldots, \alpha_n$ such that the multivariate polynomial F in (3.19) evaluates to a nonzero value. However, our results only guarantee the *existence* of these evaluation points. Hence, to design the code, explicit constructions of them still remain to be studied.

In the absence of an explicit construction, one can of course choose $\alpha_i \in \mathbb{F}$ at random and evaluate $\det \mathbf{M}$ or F until a nonzero value is obtained. Currently, we do not know whether this will efficiently find a suitable set of α_i's or whether it will require something akin to an exhaustive search.

Explicit constructions have been obtained in the literature for special instances of the problem: Notably in [23]–[25] when the support constraints are sparsest and balanced (i.e. the numbers of zeros in each row (and column) are as large as possible and differ at most by 1), and in [31] when the sets are further required to satisfy $\left|\bigcap_{j=1}^{i} \mathcal{Z}_j\right| \leq k-i$ for every $i \in [k]$.

Further Reducing the Field Size

Another interesting question is whether it is possible to further reduce the field size for the existence of MDS codes with support constrained generator matrices. Note that if the MDS conjecture is true, without sacrificing the minimum distance, the best one can hope is to reduce the field size from $n+k-1$ to $n-1$. However, if much smaller field sizes are required, one can consider other code families with sacrificing the minimum distance. For instance, it might be worth looking at whether algebraic–geometric codes can be designed with support constrained generator matrices with a desired minimum distance and field size.

5.2 Dual Problem: Parity Check Matrix under Support Constraints

A related problem to the main problem of this thesis is the dual problem, where the support constraints are on the parity check matrix. In other words, we would like to find a code with the largest possible minimum distance, subject to support constraints on the parity check matrix.

Similarly, if we represent these constraints through subsets $\mathcal{Z}_1, \ldots, \mathcal{Z}_{n-k} \subset [n]$, the entry $\mathbf{H}_{ij}$ is required to be zero for every $j \in \mathcal{Z}_i$:

$$\mathbf{H}_{(n-k)\times n} = \begin{bmatrix} \times & 0 & \times & \cdots & 0 \\ 0 & 0 & \times & \cdots & \times \\ \vdots & \vdots & \vdots & & \vdots \\ \times & \times & 0 & \cdots & 0 \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} \rightarrow \mathcal{Z}_1 \\ \rightarrow \mathcal{Z}_2 \\ \vdots \\ \rightarrow \mathcal{Z}_{n-k} \end{matrix} . \tag{5.1}$$

The distance of the code with the parity check matrix $\mathbf{H}$ can be written in terms of the Kruskal rank of $\mathbf{H}$:

$$d_H(\mathcal{C}) = \mathrm{kr}(\mathbf{H}) + 1 \tag{5.2}$$

where $\mathrm{kr}(\mathbf{H})$, the Kruskal rank of $\mathbf{H}$, is the largest integer r such that any r columns of $\mathbf{H}$ are linearly independent. This is because $\mathbf{c} \in \mathcal{C} \iff \mathbf{H}\mathbf{c}^{\mathsf{T}} = 0$, which implies that the columns of $\mathbf{H}$ corresponding to the nonzero entries of a codeword $\mathbf{c}$ are linearly dependent.

Let us drive an upper bound on the distance in terms of the given zero pattern. Notice that permuting the rows or columns of $\mathbf{H}$ does not affect its Kruskal rank. Hence, for a fixed nonempty $\Omega \subset [n-k]$, permute the rows such that the rows indexed in Ω are on the top, and then permute the columns such that all the common

zeros of the rows indexed in Ω are shifted to the right (denote $\mathcal{Z}_\Omega = \bigcap_{i\in\Omega} \mathcal{Z}_i$):

$$\mathbf{H}' = \begin{bmatrix} \times & \mathbf{0} \\ \times & \times \end{bmatrix} \begin{matrix} \} \, |\Omega| \\ \} \, n-k-|\Omega| \end{matrix} . \tag{5.3}$$
$$\underbrace{}_{n-|\mathcal{Z}_\Omega|} \quad \underbrace{}_{|\mathcal{Z}_\Omega|}$$

If $|\mathcal{Z}_\Omega| > n-k-|\Omega|$, then the last $n-k-|\Omega|+1$ columns would be linearly dependent because they only have nonzero entries in their last $n-k-|\Omega|$ rows; hence the Kruskal rank could be at most $n-k-|\Omega|$:

$$|\mathcal{Z}_\Omega| > n-k-|\Omega| \implies \mathrm{kr}(\mathbf{H}) \leq n-k-|\Omega|. \tag{5.4}$$

As a result, we can upper bound the distance of the code as follows:

$$\begin{aligned} d_H(\mathcal{C}) &\leq \min_{\Omega\subset[n-k]} n-k-|\Omega|+1 && (5.5)\\ &\qquad \text{s.t.} \quad |\mathcal{Z}_\Omega| > n-k-|\Omega| \\ &= n-k+1-\max_{\Omega\subset[n-k]} |\Omega| && (5.6)\\ &\qquad\qquad \text{s.t.} \quad |\mathcal{Z}_\Omega| > n-k-|\Omega|. \end{aligned}$$

Locally Repairable Codes

A special case of this problem has been studied in the context of locally repairable codes [18]–[20]. For example, when the repair sets are all of equal size r (i.e. locality of r), this imposes a very particular structure on the parity check matrix. If $\mathcal{Z}_i$ is the set of positions of the zeros in the ith row of $\mathbf{H}$, then for all $j \in [n]$, there exists $i \in [n-k]$ such that $j \in \mathcal{Z}_i^{\mathsf{c}}$ and $|\mathcal{Z}_i^{\mathsf{c}}| \leq r+1$. Now, let us simplify the upper bound in (5.6) for these subsets. Let

$$\Omega_0 = \{i \in [n-k] : |\mathcal{Z}_i^{\mathsf{c}}| \leq r+1\}. \tag{5.7}$$

Then, $\bigcup_{i\in\Omega_0} \mathcal{Z}_i^{\mathsf{c}} = [n]$ and

$$n = \left|\bigcup_{i\in\Omega_0} \mathcal{Z}_i^{\mathsf{c}}\right| \leq \sum_{i\in\Omega_0} |\mathcal{Z}_i^{\mathsf{c}}| \leq |\Omega_0|(r+1). \tag{5.8}$$

Hence, $|\Omega_0| \geq \lceil \frac{n}{r+1} \rceil$. Note that locally repairable codes do not impose any constraints on the rows indexed in Ω_0^{c}. For any $\Omega \subset \Omega_0$ such that $|\Omega| < \frac{k}{r}$, we have that

$$\left|\bigcup_{i\in\Omega} \mathcal{Z}_i^{\mathsf{c}}\right| \leq \sum_{i\in\Omega} |\mathcal{Z}_i^{\mathsf{c}}| \leq |\Omega|(r+1) < |\Omega| + k \tag{5.9}$$

which is equivalent to the constraint in (5.6) by De Morgan's law. If n is large enough, we can choose $\Omega \subset \Omega_0$ such that $|\Omega| = \lceil \frac{k}{r} \rceil - 1 \leq \lceil \frac{n}{r+1} \rceil \leq |\Omega_0|$. Hence, by (5.6), we get the well-known bound on the minimum distance of a locally repairable code with locality r:

$$d_H(\mathcal{C}) \leq n - k + 2 - \left\lceil \frac{k}{r} \right\rceil . \tag{5.10}$$

It has been shown that this is achievable by a subcode of a Reed–Solomon code [18].

General Case

In the case of general support constraints, this upper bound (5.6) is achievable by a random code, which requires large field sizes and potentially does not have an efficient decoder. Therefore, a question one may ask is whether one can design an algebraic code on a small field size with a minimum distance that achieves the upper bound. If the code is MDS, the problem is clearly equivalent to the one we have studied here. However, if the support constraints on the parity check matrix preclude the existence of a MDS code, then the question of whether such an algebraic code under a general support constraint exists remains open.

Appendix A

RELEVANT MATERIALS AND INSPIRING PROBLEMS

In this chapter, we will go over some relevant materials for our problems and some related problems inspiring us in our solutions, from a pure mathematical perspective. Firstly, we will define the MDS matrices, which are in fact the generator matrices of MDS codes. We will derive a necessary condition (MDS condition) for a matrix to be an MDS matrix in terms of the positions of its zero entries. Secondly, we will go over a famous combinatorial problem, the Hall's Marriage Theorem, which involves a very similar condition to the MDS condition, and we will give some generalizations of it. The generalization of the Hall's Theorem will be later useful in simplifying the GM–MDS conjecture. Thirdly, we will give the proofs of the Hall's Theorem and its generalization. The ideas behind these proofs are, in fact, very similar to those used in the main problems of this thesis. Therefore, they may help the reader to have a taste of the main idea behind the proof of the GM–MDS conjecture.

A.1 MDS Matrix

Definition A.1 (MDS Matrix)**.** An MDS Matrix is a $k \times n$ matrix ($k \leq n$) over a field $\mathbb{F}$ such that every k columns of it are linearly independent.

A Vandermonde matrix with distinct parameters $x_1, x_2, \ldots, x_n \in \mathbb{F}$ is an example of an MDS matrix:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{k-1} & x_2^{k-1} & \cdots & x_n^{k-1} \end{bmatrix}. \tag{A.1}$$

This is because any $k \times k$ minor of it is a Vandermonde determinant, which is nonzero when the parameters x_i are distinct. More precisely, the $k \times k$ minor that is defined by the columns indexed in $t_1, t_2, \ldots, t_k$ is

$$\prod_{1 \leq i < j \leq k} (x_{t_j} - x_{t_i}) \neq 0. \tag{A.2}$$

The MDS property of a matrix is preserved after multiplying with an invertible matrix from left:

Theorem A.1. *Let* $\mathbf{G}$ *be* $k \times n$ *and* $\mathbf{T}$ *be* $k \times k$ *invertible. Then,* $\mathbf{G}$ *is an MDS matrix if and only if* $\mathbf{TG}$ *is an MDS matrix.*

MDS condition for a zero pattern

MDS matrices cannot admit every zero pattern. For example, a matrix having a column with all zero entries cannot be an MDS matrix since a $k \times k$ minor involving this column is zero. We will represent a zero pattern by subsets $\mathcal{Z}_1, \ldots, \mathcal{Z}_k \subset [n]$. For $i \in [k]$, $\mathcal{Z}_i$ denotes the set of positions of some zeros in the ith row of $\mathbf{G}$:

$$\mathbf{G}_{k\times n} = \begin{bmatrix} \times & 0 & \times & \cdots & 0 \\ 0 & 0 & \times & \cdots & \times \\ \vdots & \vdots & \vdots & & \vdots \\ \times & \times & 0 & \cdots & 0 \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \to \mathcal{Z}_1 \\ \to \mathcal{Z}_2 \\ \vdots \\ \to \mathcal{Z}_k \end{matrix}. \tag{A.3}$$

We say that $\mathbf{G}$ admits this zero pattern if

$$\mathbf{G}_{ij} = 0 \qquad \forall j \in \mathcal{Z}_i. \tag{A.4}$$

Note that $\mathbf{G}$ may have other zeros as well in its entries shown with $\times$.

Let us derive a necessary condition for a matrix $\mathbf{G}_{k\times n}$ to be an MDS matrix in terms of its zero entries. Notice that permuting the rows or columns of $\mathbf{G}$ will not change the MDS property. Hence, for a fixed nonempty $\Omega \subset [k]$, permute the rows such that the rows indexed in Ω are on the top, and then permute the columns such that all the common zeros of the rows indexed in Ω are moved to the right (denote $\mathcal{Z}_\Omega = \bigcap_{i\in\Omega} \mathcal{Z}_i$):

$$\mathbf{G}' = \begin{bmatrix} \times & \mathbf{0} \\ \times & \times \end{bmatrix} \begin{matrix} \} \, |\Omega| \\ \} \, k-|\Omega| \end{matrix} \quad \begin{matrix} \\ \\ \end{matrix} \quad \begin{matrix} \overbrace{}^{n-|\mathcal{Z}_\Omega|} & \overbrace{}^{|\mathcal{Z}_\Omega|} \end{matrix}. \tag{A.5}$$

If $|\mathcal{Z}_\Omega| > k - |\Omega|$, then the last $k - |\Omega| + 1$ columns would be linearly dependent because they only have nonzero entries in their last $k - |\Omega|$ rows. Therefore, for $\mathbf{G}'$ to be an MDS matrix, $\mathcal{Z}_\Omega$ can have at most $k - |\Omega|$ elements. Hence, a necessary condition for $\mathbf{G}$ to be an MDS matrix is given as:

Definition A.2 (MDS Condition)**.** For any nonempty $\Omega \subset [k]$,

$$\left| \bigcap_{i\in\Omega} \mathcal{Z}_i \right| + |\Omega| \leq k. \tag{A.6}$$

For large enough fields, the MDS condition on a zero pattern is also a sufficient condition to find an MDS matrix admitting this zero pattern. For example, when $|\mathbb{F}| \geq \binom{n-1}{k-1}$, it is shown that for any zero pattern satisfying the MDS condition, there exists an MDS matrix admitting this zero pattern [12]. The GM–MDS conjecture claims the same for smaller field sizes, in fact as low as $n + k - 1$.

A.2 Hall's Marriage Theorem

Let $\mathcal{G} = (U, V, E)$ represent the bipartite graph with the disjoint sets of vertices U and V and the edges $E \subset U \times V$ such that $|U| \leq |V|$. Let $N_{\mathcal{G}}(\Omega) \subset V$ denote the neighborhood of $\Omega \subset U$, i.e. the set of all vertices in V adjacent to some element of Ω.

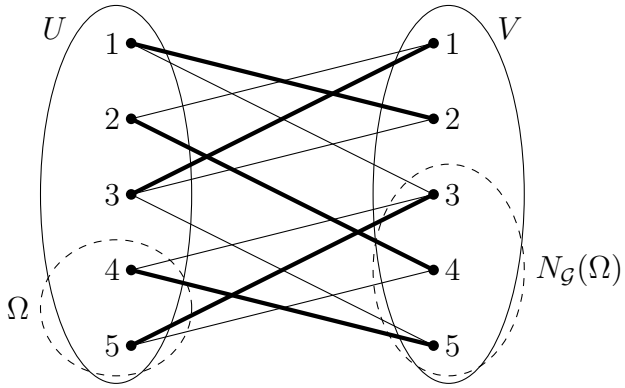

Figure A.1: A bipartite graph with a perfect matching (bold), a subset Ω of the left nodes, and its neighborhood $N_{\mathcal{G}}(\Omega)$.

We are interested in finding a perfect matching in $\mathcal{G}$, which means a one-to-one mapping from U to V using the edges in E. A straightforward necessary condition for the existence of a perfect matching in $\mathcal{G}$ can be given as the neighborhood of any $\Omega \subset U$ should have at least as many elements as Ω:

Definition A.3 (Marriage Condition)**.** For any $\Omega \subset U$,

$$|N_{\mathcal{G}}(\Omega)| \geq |\Omega|. \tag{A.7}$$

Hall's Marriage Theorem states that the Marriage Condition is also a sufficient condition for the existence of a perfect matching.

Theorem A.2.A (Hall's Theorem)**.** *Let $\mathcal{G} = (U, V, E)$ be a bipartite graph. There is a perfect matching in $\mathcal{G}$ if and only if $|N_{\mathcal{G}}(\Omega)| \geq |\Omega|$ for all $\Omega \subset U$.*

Relation to the MDS condition

The marriage condition is in fact very similar to the MDS condition given in Definition A.2. To see how, let us define $\mathcal{S}_i = N_{\mathcal{G}}(\{i\})$ as the neighbors of $i \in U$. Then, $N_{\mathcal{G}}(\Omega) = \bigcup_{i\in\Omega} \mathcal{S}_i$ and equation (A.7) can be written as:

$$\left| \bigcup_{i\in\Omega} \mathcal{S}_i \right| \geq |\Omega|. \tag{A.8}$$

This form is not quite the same as the MDS condition; however, if we rewrite it in terms of the complements $\mathcal{Z}_i \triangleq V \backslash \mathcal{S}_i$ by assuming $U = [k]$ and $V = [n]$, we get:

$$\left| \bigcap_{i\in\Omega} \mathcal{Z}_i \right| + |\Omega| \leq n, \tag{A.9}$$

which is the same as the MDS condition when $n = k$.

$$\begin{bmatrix} 0 & \times & \times & 0 & 0 \\ \times & 0 & 0 & \times & 0 \\ \times & \times & 0 & 0 & \times \\ 0 & 0 & \times & 0 & \times \\ 0 & 0 & \times & \times & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Figure A.2: The zero pattern and the permutation matrix corresponding to the bipartite graph and the perfect matching illustrated in Figure A.1.

In fact, when $n = k$, Hall's Marriage Theorem says that any zero pattern satisfying the MDS condition for a $k \times k$ square matrix can be achieved by a permutation matrix[1], which is an invertible matrix and therefore, an MDS matrix. To see how, first notice that finding a perfect matching can be viewed as removing edges from the graph until each node in U has only one neighbor while the Marriage Condition is still satisfied (note that when each node has a single neighbor, the Marriage Condition only says that these neighbors are distinct, i.e. it is a perfect matching). Furthermore, note that $\mathcal{Z}_i$ is the set of nodes to which i is not connected. Hence, removing edges corresponds to adding elements from $[n]$ to the subsets $\mathcal{Z}_i$. Therefore, in terms of the subsets $\mathcal{Z}_1, \ldots, \mathcal{Z}_k \subset [n]$, Hall's Marriage Theorem can be rewritten as

[1]By using this idea, it can be shown that the Birkhoff–Von Neumann theorem is a logical equivalence of the Hall's theorem.

Theorem A.2.B (Hall's Theorem)**.** *Let* $\mathcal{Z}_1, \mathcal{Z}_2, \ldots, \mathcal{Z}_k \subset [n]$ *such that for all nonempty* $\Omega \subset [k]$*,*

$$\left| \bigcap_{i \in \Omega} \mathcal{Z}_i \right| + |\Omega| \leq n. \tag{A.10}$$

Then, one can keep adding elements from $[n]$ *to these subsets without violating any of the inequalities until each subset has exactly* $n-1$ *elements.*

Hence, when $n = k$, for a given zero pattern satisfying the MDS condition, we can add more zeros if necessary and obtain a zero pattern that has $k-1$ zeros in each row. Then, if we put 1 to the remaining nonzero entries, we will obtain a permutation matrix.

Generalization of Hall's Marriage Theorem

Heretofore Hall's Marriage Theorem relates to the MDS matrices only when $n = k$. In order to have a relation in a more general case, let us consider a generalization of the statement [11, Thm. 2]:

Theorem A.3.A (Generalized Hall's Theorem)**.** *Let* $\mathcal{Z}_1, \mathcal{Z}_2, \ldots, \mathcal{Z}_k \subset [n]$ *such that for all nonempty* $\Omega \subset [k]$*,*

$$\left| \bigcap_{i \in \Omega} \mathcal{Z}_i \right| + |\Omega| \leq k. \tag{A.11}$$

Then, one can keep adding elements from $[n]$ *to these subsets without violating any of the inequalities until each subset has exactly* $k-1$ *elements.*

Note that this only generalizes the special case (when $n = k$) of the Hall's Theorem. In other words, setting $n = k$ in both Theorem A.2.B and Theorem A.3.A gives the same statement.

In relation to the zero patterns of the MDS matrices, Theorem A.3.A says that to a given zero pattern satisfying the MDS condition, we can add more zeros and obtain an extended zero pattern which also satisfies the MDS condition and has exactly $k-1$ zeros in each row. Note that the MDS condition only requires that each row can have at most $k-1$ zeros. Hence, Theorem A.3.A can help us to convert any zero pattern of an MDS matrix to one that has exactly $k-1$ zeros in each row by introducing more zeros. This will be very useful later when simplifying the GM–MDS conjecture.

A.3 Proof of Hall's Theorem and its generalization

In this section, first we will provide a very nice inductive proof of Hall's Marriage Theorem. Then, we will try to mimic this proof for its generalization. When doing so, we will need to write down an even more general statement. This idea is actually very similar to those in Chapter 2 (the proof of the GM–MDS conjecture) and Chapter 3. Therefore, it may help to understand the main ideas behind the proofs given in those chapters.

Proof of Hall's Theorem

We will show that from a given graph $\mathcal{G} = (U, V, E)$ satisfying the marriage condition, we can remove edges until we get a perfect matching. Let us do induction on $|U|$. If $|U| = 1$, it is trivial. Let $k \geq 2$ and suppose it is true when $|U| < k$. Let $|U| = k$. We consider two cases:

1. (A.7) holds with equality for some Ω with $2 \leq |\Omega| \leq k-1$.

   We will remove all the edges between $\Omega^{\mathsf{c}} = U \backslash \Omega$ and $N_{\mathcal{G}}(\Omega)$. This will split $\mathcal{G}$ into two disconnected parts: $\mathcal{G}_1 = (U_1, V_1, E_1)$, $\mathcal{G}_2 = (U_2, V_2, E_2)$, where $U_1 = \Omega$, $U_2 = \Omega^{\mathsf{c}}$, $V_1 = N_{\mathcal{G}}(\Omega)$, $V_2 = V \backslash V_1$, and $E_i = E \cap (U_i \times V_i)$.

   Clearly, $\mathcal{G}_1$ satisfies (A.7). We will show that so does $\mathcal{G}_2$: For any $\Omega' \subset U_2$,

   $$|N_{\mathcal{G}_2}(\Omega')| = |N_{\mathcal{G}}(\Omega \cup \Omega')| - |N_{\mathcal{G}}(\Omega)| \tag{A.12}$$
   $$\geq |\Omega| + |\Omega'| - |\Omega| \tag{A.13}$$
   $$= |\Omega'|. \tag{A.14}$$

   Hence, by the induction hypothesis, we can find perfect matching in both disconnected parts of $\mathcal{G}$.

2. (A.7) is strict for all Ω with $2 \leq |\Omega| \leq k-1$.

   If there is at least one node $i \in U$ with a degree bigger than one (otherwise it is a perfect matching), remove one of the edges from i. Since all inequalities are strict this will not violate (A.7).

First attempt to prove the Generalized Hall's Theorem

First let us rewrite the Generalized Hall's Theorem in terms of the bipartite graphs:

Theorem A.3.B (Generalized Hall's Theorem)**.** *Let $\mathcal{G} = (U, V, E)$ be a bipartite graph with $|U| = k, |V| = n$. Suppose that for any nonempty $\Omega \subset U$,*

$$|N_{\mathcal{G}}(\Omega)| \geq n - k + |\Omega|. \tag{A.15}$$

Then, one can keep removing edges from E without violating any of the inequalities until the degree of i is exactly $n-k+1$ for all $i \in U$.

Note that adding extra dummy nodes to V should not have any effect on this property, but the size of $|V|$ appears in these inequalities. Also, when we try to mimic a similar proof, another thing to observe is that if the equality holds for some Ω, the subgraph $\mathcal{G}_\Omega = (\Omega, N_\mathcal{G}(\Omega), E \cap (\Omega \times N_\mathcal{G}(\Omega)))$ has fewer nodes on the right side than $|V| = n$ while the inequalities still carry the information about the size of the bigger graph. Therefore, it is natural to remove this dependency to the number of nodes and focus on a bit more general version of it:

Theorem A.4. *Let $\mathcal{G} = (U, V, E)$ be a bipartite graph. Suppose that there exists an integer $c \geq 0$ such that, for any nonempty $\Omega \subset U$,*

$$|N_\mathcal{G}(\Omega)| \geq c + |\Omega|. \tag{A.16}$$

Then, one can keep removing edges from E without violating any of the inequalities until the degree of i is exactly $c+1$ for all $i \in U$.

Now, assuming again that the equality holds for some Ω (i.e. $|N_\mathcal{G}(\Omega)| = c + |\Omega|$), the subgraph $\mathcal{G}_\Omega$ can be resolved by the induction hypothesis. However, we still need to guarantee that while removing edges from these subgraphs, we do not break the inequality

$$|N_\mathcal{G}(\Omega_1 \cup \Omega_2)| \geq c + |\Omega_1| + |\Omega_2| \tag{A.17}$$

for any $\Omega_1 \subset \Omega$ and $\Omega_2 \subset \Omega^\mathsf{c}$. Note that by the induction hypothesis, we are able to assume that after removing an edge, the inequality $|N_\mathcal{G}(\Omega_1)| \geq |\Omega_1|$ will still hold. Then,

$$\begin{aligned}
|N_\mathcal{G}(\Omega_1 \cup \Omega_2)| &= |N_\mathcal{G}(\Omega_1)| + |N_\mathcal{G}(\Omega_2) - N_\mathcal{G}(\Omega_1)| \\
&\geq |N_\mathcal{G}(\Omega_1)| + |N_\mathcal{G}(\Omega_2) - N_\mathcal{G}(\Omega)| \\
&= |N_\mathcal{G}(\Omega_1)| + |N_\mathcal{G}(\Omega_2 \cup \Omega)| - |N_\mathcal{G}(\Omega)| \\
&\geq c + |\Omega_1| + |N_\mathcal{G}(\Omega_2 \cup \Omega)| - c - |\Omega| \\
&= |N_\mathcal{G}(\Omega_2 \cup \Omega)| + |\Omega_1| - |\Omega| \\
&\overset{?}{\geq} c + |\Omega_1| + |\Omega_2|.
\end{aligned}$$

Hence, it is sufficient to guarantee that $|N_\mathcal{G}(\Omega_2 \cup \Omega)| \geq c + |\Omega_2| + |\Omega|$ is not violated (instead of $|N_\mathcal{G}(\Omega_1 \cup \Omega_2)| \geq c + |\Omega_1| + |\Omega_2|$ for every $\Omega_1 \subset \Omega$). Therefore, the

individual nodes inside Ω do not have any role anymore, which suggests us to define a new graph, where we merge all the nodes in Ω into a single node called Ω:

$\mathcal{G}' = (\Omega^{\mathsf{c}} \cup \{\Omega\}, V, E')$, where

$$E' = (E \cap (\Omega^{\mathsf{c}} \times V)) \cup (\{\Omega\} \times N_{\mathcal{G}}(\Omega)).$$

Note that the node Ω is a placeholder for $|\Omega|$ nodes. Therefore, our new problem now may have nodes that represent multiple nodes. Hence, this suggests us to generalize the problem even more by assigning a weight to each of the nodes in U. The whole point in working on a more general problem is that we want to benefit from the induction hypothesis and generalizing the problem also makes the induction hypothesis to cover the cases that we need.

A further generalization of Hall's Theorem and Proof of Theorem A.3.B

Theorem A.5. *Let $\mathcal{G} = (U, V, E)$ be a bipartite graph. Suppose that there exist integers $c \geq 0$ and $d_i \geq 1$ for $i \in U$ such that for any nonempty $\Omega \subset U$,*

$$|N_{\mathcal{G}}(\Omega)| \geq c + \sum_{i \in \Omega} d_i. \tag{A.18}$$

Then, one can keep removing edges from E without violating any of the inequalities until the degree of i is exactly $c + d_i$ for all $i \in U$. $\diamond$

Proof. We will do induction on $|U|$. If $|U| = 1$, it is trivial. Let $k \geq 2$ and suppose it is true when $|U| < k$. Let $|U| = k$. We consider two cases:

1. (A.18) is *tight* for some Ω with $2 \leq |\Omega| \leq k - 1$.

   Let $\mathcal{G}_1 = (\Omega, V, E_1)$, where $E_1 = E \cap (\Omega \times V)$ and $\mathcal{G}_2 = (\Omega^{\mathsf{c}} \cup \{\Omega\}, V, E_2)$, where $\Omega^{\mathsf{c}} = U - \Omega$ and

   $$E_2 = (E - E_1) \cup \{(\Omega, j) : j \in N_{\mathcal{G}}(\Omega)\}.$$

   In other words, to obtain $\mathcal{G}_2$, we merge the vertices in Ω into a single vertex called Ω with the edges from that to every vertex in $N_{\mathcal{G}}(\Omega)$. Furthermore, let $d_\Omega = \sum_{i \in \Omega} d_i$.

   We will show that (A.18) holds for $\mathcal{G}_1$ and $\mathcal{G}_2$ if and only if it holds for $\mathcal{G}$ (the other direction $\Leftarrow$ is trivial). Let $\Omega_1 \subset \Omega, \Omega_2 \subset \Omega^{\mathsf{c}}$. Then,

   $$|N_{\mathcal{G}}(\Omega_1 \cup \Omega_2)| = |N_{\mathcal{G}}(\Omega_1)| + |N_{\mathcal{G}}(\Omega_2) - N_{\mathcal{G}}(\Omega_1)|$$

$$
\begin{aligned}
&\geq |N_{\mathcal{G}}(\Omega_1)| + |N_{\mathcal{G}}(\Omega_2) - N_{\mathcal{G}}(\Omega)| \\
&= |N_{\mathcal{G}}(\Omega_1)| + |N_{\mathcal{G}}(\Omega_2 \cup \Omega)| - |N_{\mathcal{G}}(\Omega)| \\
&= |N_{\mathcal{G}_1}(\Omega_1)| + |N_{\mathcal{G}_2}(\Omega_2 \cup \{\Omega\})| - (c + d_\Omega) \\
&\geq \left(c + \sum_{i \in \Omega_1} d_i \right) + \left(c + d_\Omega + \sum_{i \in \Omega_2} d_i \right) - (c + d_\Omega) \\
&= c + \sum_{i \in \Omega_1 \cup \Omega_2} d_i.
\end{aligned}
$$

Since $|\Omega| \leq k-1$ and $|\Omega^{\mathsf{c}} \cup \{\Omega\}| \leq k-1$, by the induction hypothesis, we can remove edges from $\mathcal{G}_1$ and $\mathcal{G}_2$ until the degree of i is $c + d_i$ for all $i \in U$. (Note that none of the edges from the vertex Ω in $\mathcal{G}_2$ will be removed since its degree is already $c + d_\Omega$.)

2. (A.18) is *strict* for all Ω with $2 \leq |\Omega| \leq k-1$.
   If there exists an edge $(i, j) \in E$ such that the degree of i is at least $c + d_i + 1$ and the degree of j is at least 2, then removing (i, j) will not violate (A.18) because all the inequalities are strict except for $|\Omega| = k$, in which case, the left hand side is not affected. Now, we can assume that if a vertex $i \in U$ has a degree of at least $c + d_i + 1$, then it is disconnected from the other vertices in U. Then, removing any edge from such a vertex i will not violate any of the inequalities. □

As a special case, letting $c = 0$ and $d_i = 1$ for all i yields to the Hall's Marriage Theorem (Theorem A.2.A-A.2.B). Letting $c = |V| - |U|$ and $d_i = 1$ for all i yields to its generalization (Theorem A.3.A-A.3.B and [11, Thm. 2]). Hence, Theorem A.5 covers all the other theorems given in Sections A.2 and A.3.

BIBLIOGRAPHY

[1] H. Yildiz and B. Hassibi, "Further progress on the GM-MDS conjecture for Reed–Solomon codes," in *2018 IEEE International Symposium on Information Theory (ISIT)*, IEEE, 2018, pp. 16–20. DOI: 10.1109/ISIT.2018.8437308,

[2] ——, "Optimum linear codes with support constraints over small fields," in *2018 IEEE Information Theory Workshop (ITW)*, IEEE, 2018, pp. 1–5. DOI: 10.1109/ITW.2018.8613535,

[3] ——, "Optimum linear codes with support-constrained generator matrices over small fields," *IEEE Transactions on Information Theory*, vol. 65, no. 12, pp. 7868–7875, 2019. DOI: 10.1109/TIT.2019.2932663,

[4] ——, "Gabidulin codes with support constraints," in *2019 IEEE Information Theory Workshop (ITW)*, IEEE, 2019, pp. 1–5. DOI: 10.1109/ITW44776.2019.8988992,

[5] ——, "Gabidulin codes with support constrained generator matrices," *IEEE Transactions on Information Theory*, vol. 66, no. 6, pp. 3638–3649, 2019. DOI: 10.1109/TIT.2019.2955106,

[6] H. Yildiz, N. Raviv, and B. Hassibi, "Support constrained generator matrices of Gabidulin codes in characteristic zero," in *2020 IEEE International Symposium on Information Theory (ISIT)*, IEEE, 2020, pp. 60–65. DOI: 10.1109/ISIT44484.2020.9174524,

[7] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory, Series A*, vol. 25, no. 3, pp. 226–241, 1978.

[8] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problemy Peredachi Informatsii*, vol. 21, no. 1, pp. 3–16, 1985.

[9] D. Augot, P. Loidreau, and G. Robert, "Generalized Gabidulin codes over fields of any characteristic," *Designs, Codes and Cryptography*, vol. 86, no. 8, pp. 1807–1848, 2018.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Elsevier, 1977, vol. 16.

[11] S. H. Dau, W. Song, and C. Yuen, "On the existence of MDS codes over small fields with constrained generator matrices," in *2014 IEEE International Symposium on Information Theory*, IEEE, 2014, pp. 1787–1791.

[12] S. H. Dau, W. Song, Z. Dong, and C. Yuen, "Balanced sparsest generator matrices for MDS codes," in *2013 IEEE International Symposium on Information Theory*, IEEE, 2013, pp. 1889–1893.

[13] W. Halbawi, T. Ho, H. Yao, and I. Duursma, "Distributed Reed–Solomon codes for simple multiple access networks," in *2014 IEEE International Symposium on Information Theory*, IEEE, 2014, pp. 651–655.

[14] W. Halbawi, T. Ho, and I. Duursma, "Distributed Gabidulin codes for multiple-source network error correction," in *2014 International Symposium on Network Coding (NetCod)*, IEEE, 2014, pp. 1–6.

[15] S. H. Dau, W. Song, and C. Yuen, "On simple multiple access networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 2, pp. 236–249, 2015.

[16] M. Yan and A. Sprintson, "Algorithms for weakly secure data exchange," in *2013 International Symposium on Network Coding (NetCod)*, IEEE, 2013, pp. 1–6.

[17] M. Yan, A. Sprintson, and I. Zelenko, "Weakly secure data exchange with generalized Reed–Solomon codes," in *2014 IEEE International Symposium on Information Theory*, IEEE, 2014, pp. 1366–1370.

[18] I. Tamo and A. Barg, "A family of optimal locally recoverable codes," *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 4661–4676, 2014.

[19] I. Tamo, A. Barg, and A. Frolov, "Bounds on the parameters of locally recoverable codes," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3070–3083, 2016.

[20] D. S. Papailiopoulos and A. G. Dimakis, "Locally repairable codes," *IEEE Transactions on Information Theory*, vol. 60, no. 10, pp. 5843–5855, 2014.

[21] D. Silva, F. R. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE transactions on information theory*, vol. 54, no. 9, pp. 3951–3967, 2008.

[22] A. Heidarzadeh and A. Sprintson, "An algebraic-combinatorial proof technique for the GM-MDS conjecture," in *2017 IEEE International Symposium on Information Theory (ISIT)*, IEEE, 2017, pp. 11–15.

[23] W. Halbawi, Z. Liu, and B. Hassibi, "Balanced Reed–Solomon codes," in *2016 IEEE International Symposium on Information Theory (ISIT)*, IEEE, 2016, pp. 935–939.

[24] ——, "Balanced Reed–Solomon codes for all parameters," in *2016 IEEE Information Theory Workshop (ITW)*, IEEE, 2016, pp. 409–413.

[25] W. Song and K. Cai, "Generalized Reed–Solomon codes with sparsest and balanced generator matrices," in *2018 IEEE International Symposium on Information Theory (ISIT)*, IEEE, 2018, pp. 1–5.

[26] S. Lovett, "MDS matrices over small fields: A proof of the GM-MDS conjecture," in *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE, 2018, pp. 194–199.

[27] P. R. Halmos and H. E. Vaughan, "The marriage problem," *American Journal of Mathematics*, vol. 72, pp. 214–215, 1950.

[28] J. Maroulas and D. Dascalopoulos, "Applications of the generalized Sylvester matrix," *Applied Mathematics and Computation*, vol. 8, no. 2, pp. 121–135, 1981.

[29] E. W. Cheney, *Introduction to Approximation Theory*. McGraw-Hill, 1966.

[30] S. Barnett, "Greatest common divisors from generalized Sylvester resultant matrices," *Linear and Multilinear Algebra*, vol. 8, no. 4, pp. 271–279, 1980.

[31] G. Greaves and J. Syatriadi, "Reed–Solomon codes over small fields with constrained generator matrices," *IEEE Transactions on Information Theory*, 2019.

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

[33] G. Lunardon, R. Trombetti, and Y. Zhou, "Generalized twisted Gabidulin codes," *Journal of Combinatorial Theory, Series A*, vol. 159, pp. 79–106, 2018.

[34] S. Puchinger, J. Sheekey, *et al.*, "Further generalisations of twisted Gabidulin codes," *arXiv preprint arXiv:1703.08093*, 2017.

[35] J. Sheekey, "New semifields and new MRD codes from skew polynomial rings," *arXiv preprint arXiv:1806.00251*, 2018.

[36] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge University Press, 1997.

[37] T. W. Hungerford, *Algebra*. Springer, 1974.

[38] A. Neri, "Systematic encoders for generalized Gabidulin codes and the q-analogue of Cauchy matrices," *arXiv preprint arXiv:1805.06706*, 2018.

[39] P. Lusina, E. Gabidulin, and M. Bossert, "Maximum rank distance codes as space-time codes," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2757–2760, 2003.

[40] E. M. Gabidulin, A. Paramonov, and O. Tretjakov, "Ideals over a non-commutative ring and their application in cryptology," in *Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, 1991, pp. 482–489.

[41] S. Müelich, S. Puchinger, and M. Bossert, "Low-rank matrix recovery using Gabidulin Codes in characteristic zero," *Electronic Notes in Discrete Mathematics*, vol. 57, pp. 161–166, 2017.

[42] D. A. Marcus, *Number fields*. Springer, 1977.

[43] E. W. Weisstein, "Modulo multiplication group," *MathWorld–A Wolfram Web Resource*, 2020. [Online]. Available: `http://mathworld.wolfram.com/ModuloMultiplicationGroup.html`.