Gabidulin Codes with Support Constrained Generator Matrices

Hikmet Yildiz and Babak Hassibi
Department of Electrical Engineering
California Institute of Technology
Email: {hyildiz, hassibi}@caltech.edu

Abstract

Gabidulin codes are the only known general construction of linear codes that are maximum rank distant (MRD). They have found applications in linear network coding 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 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 this paper, we give necessary and sufficient conditions on the support of the generator matrix that guarantees the existence of Gabidulin codes and general MRD 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. When these conditions are 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. The necessary and sufficient conditions are identical to those that appear for MDS codes which were recently proven in [1, 2] in the context of settling the GM-MDS conjecture.

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.* [3], and referred to as the GM-MDS conjecture, which was proved in our previous work [1] and the independent work of Lovett [2].

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 [4] and Gabidulin [5] are the only known general constructions of it [6]. These codes require a field size of q^s, with $s \geq n$.

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.* [7] 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.* [8] 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 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 paper, 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 [8] 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 [1,2] 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 paper is organized as follows: In Section 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 1). Section 3 then proposes a purely algebraic problem on linearized polynomials that contains a more general theorem than Claim 1 and provides a detailed proof. The advantage of the generalization is that it leads itself to proof by induction. Finally, we conclude in Section 4.

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 are the only known general constructions of codes achieving 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 of this paper. Our proof relies on a claim (Claim 1), which will be proven in Section 3, and constitutes the major technical contribution of our work.

2.1 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

$$\operatorname{rank}(c) = \dim(\operatorname{span}\{c_1, \ldots, c_n\}) \tag{1}$$

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

$$\operatorname{rank}(c) \leq \|c\|_H \tag{2}$$

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

$$d_R = \min_{0 \neq c \in \mathcal{C}} \operatorname{rank}(c) \tag{3}$$

Then, by (2), the rank distance is less than or equal to the Hamming distance:

$$d_R \leq d_H \tag{4}$$

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

2.2 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:

$$\forall i \in [k],\ \forall j \in \mathcal{Z}_i, \quad \mathbf{G}_{ij} = 0 \tag{5}$$

It is well known that [1–3] a necessary condition for a code to be an MDS is

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

for all nonempty $\Omega \subset [k]$. Hence, it is also *necessary* for the existence of MRD–codes by Remark 1. Later, we will show that it is actually 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 [3, 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 (6) (We also provide a different proof in Appendix B). Note that this operation will only put more zero constraints on $\mathbf{G}$ but 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 (6), we will further assume that

$$|\mathcal{Z}_i| = k-1, \quad \forall i \in [k] \tag{7}$$

2.3 Gabidulin Codes

Gabidulin codes were introduced in [4] and [5] and are the only known general constructions (meaning for any n and k) of an MRD code [6]. Their generator matrices are of the following form:

$$\mathbf{G}_{\mathrm{GC}} = \begin{pmatrix} \alpha_1^{q^0} & \alpha_2^{q^0} & \cdots & \alpha_n^{q^0} \\ \alpha_1^{q^1} & \alpha_2^{q^1} & \cdots & \alpha_n^{q^1} \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{k-1}} & \alpha_2^{q^{k-1}} & \cdots & \alpha_n^{q^{k-1}} \end{pmatrix} \in \mathbb{F}_{q^s}^{k \times n} \tag{8}$$

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 $\mathbf{G}_{\mathrm{GC}}$ over $\mathbb{F}_{q^s}$ [9, Lemma 3.51]. This matrix is also known as the Moore matrix.

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

$$\mathbf{G} = \mathbf{T} \cdot \mathbf{G}_{\mathrm{GC}} \tag{9}$$

where $\mathbf{T} \in \mathbb{F}_{q^s}^{k \times k}$ is full rank. This will allow us to introduce zeros at the desired positions on $\mathbf{G}$.

Notice that if we define the polynomials

$$f_i(x) = \sum_{j=1}^{k} \mathbf{T}_{ij} x^{q^{j-1}} \tag{10}$$

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 (5) on $\mathbf{G}$ will become root constraints on the f_i's:

$$\forall i \in [k],\ \forall j \in \mathcal{Z}_i, \quad f_i(\alpha_j) = 0 \tag{11}$$

In the view of the above, the question we would like to ask is whether under condition (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 (11) holds. In other words, since $\mathbf{T}$ is invertible, $\mathbf{G}$ has the same MRD property of $\mathbf{G}_{\mathrm{GC}}$, and also satisfies the support constraints in (5).

We should mention that a similar question for the existence of MDS codes with support constraints on the generator matrix was asked by [3] and was referred to as the GM–MDS conjecture. This was recently resolved in [1, 2], where it was shown that under (6) MDS codes with small fields size could be constructed using Reed–Solomon codes. The current paper can be viewed as an extension of that result to rank-metric codes and Gabidulin codes.

2.4 Linearized Polynomials

Polynomials in the form of (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* [10]. Furthermore, for any $\gamma \in \mathbb{F}_q$, we have that $\gamma^{q^i} = \gamma$. Therefore, any linearized polynomial in the form of

$$f(x) = \sum_{i=0}^{d} c_i x^{q^i}, \quad c_i \in \mathbb{F}_{q^s} \tag{12}$$

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

$$f(x) = \prod_{\beta \in V} (x - \beta) \tag{13}$$

is a linearized polynomial, i.e. after expanding the product, the monomials whose exponent is not a power of q will vanish [9, Theorem 3.52].

The q-degree of the linearized polynomial f in (12) is defined as $\deg_q f = d$ if $c_d \neq 0$. Then, the q-degree of f in (13) 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, where more properties of them will be given.

2.5 Existence of Gabidulin Codes

Note that by the definition in (10), we have $\deg_q f_i \leq k-1$. Furthermore, since the α_j's are assumed to be linearly independent, by (7) and (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

$$f_i(x) = \prod_{\beta \in \operatorname{span}\{\alpha_j : j \in \mathcal{Z}_i\}} (x - \beta), \tag{14}$$

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

$$F(\alpha_1, \ldots, \alpha_n) \triangleq F_1(\alpha_1, \ldots, \alpha_n) F_2(\alpha_1, \ldots, \alpha_n) \neq 0 \tag{15}$$

where

$$F_1(\alpha_1, \ldots, \alpha_n) = \det \mathbf{T} \tag{16}$$

$$F_2(\alpha_1, \ldots, \alpha_n) = \begin{vmatrix} \alpha_1^{q^0} & \alpha_2^{q^0} & \cdots & \alpha_n^{q^0} \\ \alpha_1^{q^1} & \alpha_2^{q^1} & \cdots & \alpha_n^{q^1} \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \cdots & \alpha_n^{q^{n-1}} \end{vmatrix} \tag{17}$$

because α_i's are linearly independent if and only if $F_2(\alpha_1, \ldots, \alpha_n) \neq 0$ [9, Lemma 3.51].

It is known 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 1 below is true, we can conclude that F is not the zero polynomial.

Claim 1. $\det \mathbf{T}$ *is not the zero polynomial if (6) is satisfied.* $\diamond$

We will give the proof of Claim 1 later in Section 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 (17) 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 (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 (14). 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

$$f_i'(x) = \prod_{\beta \in \mathrm{span}\{\alpha_{j'} : j' \in \mathcal{Z}_i'\}} (x - \beta) \tag{18}$$

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 $\deg_{\alpha_j} f'(\alpha_j) = q^{k-2}$. Then,

$$\begin{aligned}
f_i(x) &= \prod_{\beta \in \mathrm{span}\{\alpha_{j'} : j' \in \mathcal{Z}_i\}} (x - \beta) && (19)\\
&= \prod_{\gamma \in \mathbb{F}_q} \prod_{\beta \in \mathrm{span}\{\alpha_{j'} : j' \in \mathcal{Z}_i'\}} (x - \gamma\alpha_j - \beta) && (20)\\
&= \prod_{\gamma \in \mathbb{F}_q} f_i'(x - \gamma\alpha_j) && (21)\\
&= \prod_{\gamma \in \mathbb{F}_q} (f_i'(x) - \gamma f_i'(\alpha_j)) && (22)\\
&= (f_i'(x))^q - (f_i'(\alpha_j))^{q-1} f_i'(x) && (23)
\end{aligned}$$

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,

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

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

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

$$q^s = q^{s-1} + (q-1)q^{s-1} \geq q^{n-1} + (q-1)kq^{k-2} > q^{n-1} + (k-1)(q-1)q^{k-2} \tag{24}$$

Theorem 1. *For any $s \geq \max\{n, k-1+\log_q k\}$, if (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 (5).* ◇

2.6 Subcodes of Gabidulin codes

If the necessary and sufficient condition in (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 sizes. In [1], the following upper bound on the Hamming distance is noted:

$$d_H \leq n - \ell + 1 \tag{25}$$

where

$$\ell \triangleq \max_{\emptyset \neq \Omega \subset [k]} \left(\left| \bigcap_{i \in \Omega} \mathcal{Z}_i \right| + |\Omega| \right) \geq k \tag{26}$$

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

$$d_R \leq n - \ell + 1 \tag{27}$$

Theorem 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 (5).* ◇

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

$$\left| \bigcap_{i \in \Omega} \mathcal{Z}_i \right| + |\Omega| \leq \ell \tag{28}$$

Hence, by Theorem 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 (27). □

3 Proof of Claim 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 1, namely Theorems 3.A and 3.B, which, in fact, arise when trying to apply a proof by induction to Claim 1. Our generalization will be written in two different forms. Theorem 3.A will be in terms of linearized polynomials, whereas Theorem 3.B will be in terms of matrices. However, both are equivalent and more general than Claim 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.A.

3.1 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.,

$$\mathsf{R}_n[x] \triangleq \left\{ \sum_{i=0}^{d} c_i x^i \middle| d \geq 0, c_0, \ldots, c_d \in \mathsf{R}_n \right\} \tag{29}$$

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

$$\mathsf{L}_n \triangleq \left\{ \sum_{i=0}^{d} c_i x^{q^i} \middle| d \geq 0, c_0, \ldots, c_d \in \mathsf{R}_n \right\} \subset \mathsf{R}_n[x] \tag{30}$$

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 [9, 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 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 $t \geq 0$,

$$f = \prod_{\beta \in V} (x - \beta)^{q^t} \in \mathsf{L}_n \tag{31}$$

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:

$$\mathsf{f}(\mathcal{Z}, t) \triangleq \prod_{\beta \in \mathrm{span}\{x_i : i \in \mathcal{Z}\}} (x - \beta)^{q^t} \in \mathsf{L}_n, \qquad t \geq 0, \mathcal{Z} \subset [n] \tag{32}$$

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,

$$\deg_q \mathsf{f}(\mathcal{Z}, t) = t + \dim(\mathrm{span}\{x_i : i \in \mathcal{Z}\}) = t + |\mathcal{Z}| \tag{33}$$

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

$$\mathcal{L}_{n,k} \triangleq \{\mathsf{f}(\mathcal{Z}, t) | t \geq 0, \mathcal{Z} \subset [n] \text{ s.t. } t + |\mathcal{Z}| \leq k - 1\} \subset \mathsf{L}_n \tag{34}$$

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

$$f' = \begin{cases} \mathsf{f}(\mathcal{Z}, t) & n \notin \mathcal{Z} \\ \mathsf{f}(\mathcal{Z} - \{n\}, t+1) & n \in \mathcal{Z} \end{cases} \tag{35}$$

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 analogue 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

$$\mathbf{S}_{a \times b}(f_1 \circ f_2) = \mathbf{S}_{a \times c}(f_1) \cdot \mathbf{S}_{c \times b}(f_2) \tag{36}$$

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 $b-a \geq d$,

$$\mathbf{S}_{a\times(b+t)}(f^{q^t}) = \mathbf{S}_{a\times(a+t)}(x^{q^t}) \cdot \mathbf{S}_{(a+t)\times(b+t)}(f) \tag{37}$$

$$= \begin{pmatrix} \mathbf{0}_{a\times t} & \mathbf{I}_{a\times a} \end{pmatrix} \cdot \mathbf{S}_{(a+t)\times(b+t)}(f) \tag{38}$$

$$= \begin{pmatrix} \underbrace{\begin{matrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{matrix}}_{t} & \begin{matrix} c_0^{q^t} & c_1^{q^t} & \cdots & c_{b-a}^{q^t} & & & \\ & c_0^{q^{t+1}} & c_1^{q^{t+1}} & \cdots & c_{b-a}^{q^{t+1}} & & \\ & & \ddots & \ddots & & \ddots & \\ & & & c_0^{q^{t+a-1}} & c_1^{q^{t+a-1}} & \cdots & c_{b-a}^{q^{t+a-1}} \end{matrix} \end{pmatrix} \tag{39}$$

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.

3.2 Main Result

Theorem 3.A is a more general statement than Claim 1 given in Section 2 and it is the analog of [1, Theorem 3] for linearized polynomials.

Theorem 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 followings 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

$$\sum_{i=1}^{m} g_i \circ x^{q^r} \circ f_i = 0 \implies g_1 = g_2 = \cdots = g_m = 0 \tag{40}$$

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

$$k - \deg_q \operatorname*{gcd}_{i\in\Omega} f_i \geq \sum_{i\in\Omega} (k - \deg_q f_i) \tag{41}$$

$\diamond$

Before moving to the proof, in order to see how Claim 1 becomes a special case of Theorem 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 [1, 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:

$$\mathbf{S}(f_i^{q^r}) = \left.\begin{pmatrix} \underbrace{\begin{matrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{matrix}}_{r+t_i} & \underbrace{\begin{matrix} \times & \times & \cdots & \times & & \\ & \times & \times & \cdots & \times & \\ & & \ddots & \ddots & & \ddots \end{matrix}}_{k-1-t_i-|\mathcal{Z}_i|} & \underbrace{\begin{matrix} & & & \\ & & & \\ & & & \\ \times & \times & \cdots & \times \end{matrix}}_{|\mathcal{Z}_i|+1} \end{pmatrix}\right\} k-t_i-|\mathcal{Z}_i| \tag{42}$$

(43)

Then, applying (36) to the expression $g_i \circ x^{q^r} \circ f_i = g_i \circ f_i^{q^r}$ in Theorem 3.A yields

$$\mathbf{S}_{1\times(k+r)}(g_i \circ x^{q^r} \circ f_i) = \mathbf{u}_i \cdot \mathbf{S}(f_i^{q^r}) \tag{44}$$

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

$$\mathbf{S}_{1\times(k+r)}\left(\sum_{i=1}^{m} g_i \circ x^{q^r} \circ f_i\right) = \begin{pmatrix}\mathbf{u}_1 & \cdots & \mathbf{u}_m\end{pmatrix} \cdot \begin{pmatrix}\mathbf{S}(f_1^{q^r}) \\ \vdots \\ \mathbf{S}(f_m^{q^r})\end{pmatrix} \tag{45}$$

which is a linear combination of the rows of

$$\mathbf{M}(r) = \begin{pmatrix}\mathbf{S}(f_1^{q^r}) \\ \vdots \\ \mathbf{S}(f_m^{q^r})\end{pmatrix}_{\sum_{i=1}^{m}(k-t_i-|\mathcal{Z}_i|)\times(k+r)} \tag{46}$$

Hence, (i) in Theorem 3.A is equivalent to saying the matrix $\mathbf{M}(r)$ has full row rank. Note that first r columns of $\mathbf{M}(r)$ are zero since first $r + t_i$ columns of $\mathbf{S}(f_i^{q^r})$ are so.

Furthermore, (ii) in Theorem 3.A can be written in terms of the $\mathcal{Z}_i$'s and the t_i's in lights of (33) and P7. Therefore, Theorem 3.A is equivalent to Theorem 3.B below.

Theorem 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 (46) has full row rank for all $r \geq 0$ if and only if for all nonempty $\Omega \subset [m]$,*

$$k - \left|\bigcap_{i\in\Omega} \mathcal{Z}_i\right| - \min_{i\in\Omega} t_i \geq \sum_{i\in\Omega}(k - t_i - |\mathcal{Z}_i|) \tag{47}$$

$\diamond$

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 1 below, which is Claim 1 in Section 2.

Corollary 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 $f_i = \mathsf{f}(\mathcal{Z}_i, t_i) = \sum_{i=1}^{k} c_{ij} x^{q^{j-1}}$. $\diamond$

3.3 Sketch of the proof of Theorem 3.B

The proof given here for Theorem 3.B omits certain steps that the interested reader can fill in. The complete proof of the equivalent Theorem 3.A is given in Section 3.4 and includes each and every step.

The following identity (48) will be very useful throughout the proof.

For any $\Omega \subset [m]$ (wlog assume $\Omega = \{1, 2, \ldots, \ell\}$), 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 $\mathbf{S}(\,\cdot\,)$)

$$\begin{pmatrix} \mathbf{S}(f_1^{q^r}) \\ \vdots \\ \mathbf{S}(f_\ell^{q^r}) \end{pmatrix} = \underbrace{\begin{pmatrix} \mathbf{S}(f_1'^{q^r}) \\ \vdots \\ \mathbf{S}(f_\ell'^{q^r}) \end{pmatrix}}_{\begin{bmatrix}\mathbf{0}_{*\times r} & \mathbf{B}'\end{bmatrix}} \cdot \underbrace{\mathbf{S}(f_0)}_{\begin{bmatrix}\times \\ \mathbf{S}(f_0^{q^r})\end{bmatrix}} = \mathbf{B}' \cdot \mathbf{S}(f_0^{q^r}) \tag{48}$$

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 (47).

Therefore, if (47) 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. (47) is tight for some $2 \le |\Omega| \le m - 1$.

Case 2. (47) is strict for all $2 \le |\Omega| \le m - 1$.

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

$$\begin{pmatrix} \mathbf{S}(f_1^{q^r}) \\ \vdots \\ \mathbf{S}(f_m^{q^r}) \end{pmatrix} = \begin{pmatrix} \mathbf{B}'\mathbf{S}(f_0^{q^r}) \\ \mathbf{S}(f_{\ell+1}^{q^r}) \\ \vdots \\ \mathbf{S}(f_m^{q^r}) \end{pmatrix} \tag{49}$$

$$= \begin{pmatrix} \mathbf{B}' & & & \\ & \mathbf{I} & & \\ & & \ddots & \\ & & & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{S}(f_0^{q^r}) \\ \mathbf{S}(f_{\ell+1}^{q^r}) \\ \vdots \\ \mathbf{S}(f_m^{q^r}) \end{pmatrix} \tag{50}$$

This will reduce the problem into two smaller problems: First one is showing that the matrix on the right in (50) 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 (48)), 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 (47).

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.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 (47) 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

$$\mathbf{M}(r) = \left(\begin{array}{cccccccccc} 0 & \cdots & 0 & \times & \times & \cdots & \times & & & \\ 0 & \cdots & 0 & 0 & \times & \times & \cdots & \times & & \\ \vdots & & \vdots & \vdots & & \ddots & \ddots & & \ddots & \\ 0 & \cdots & 0 & 0 & & & \times & \times & \cdots & \times \\ \hline 0 & \cdots & 0 & 0 & \times & \times & \cdots & \times & & \\ \vdots & & \vdots & \vdots & & \ddots & & & \ddots & \\ 0 & \cdots & 0 & 0 & & & \times & \times & \cdots & \times \\ \hline & & & & & \vdots & & & & \end{array}\right) \tag{51}$$

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 (47).

3.4 Proof of Theorem 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

$$f_\Omega = \mathsf{f}\left(\bigcap_{i\in\Omega} \mathcal{Z}_i,\ \min_{i\in\Omega} t_i\right) \tag{52}$$

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 wlog, 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 $g_1, \ldots, g_\ell \in \mathsf{L}_n$ such that $\deg_q(g_i \circ f_i) \leq k-1$, 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 $(k, m \geq 2, n = 0)$, (ii) never holds: Suppose $f_i = x^{q^{t_i}}$ and $t_1 \leq t_2$, then for $\Omega = \{1, 2\}$, (41) becomes $k - t_1 \geq (k - t_1) + (k - t_2)$, which contradicts with $|\mathcal{Z}_i| + t_i \leq k - 1$.

For $k \geq m \geq 2$ and $n \geq 1$ 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 $2 \leq |\Omega| \leq m - 1$ such that (41) holds with equality.

Case 2. $\forall\, \Omega \subset [m]$ with $2 \leq |\Omega| \leq m - 1$, (41) 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 nonzero 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: Wlog, 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 $0 \in \Omega$:

$$\begin{aligned}
k - \deg_q f_\Omega &= k - \deg_q \gcd\{f_0, f_{(\Omega - \{0\})}\} && (53)\\
&= k - \deg_q \gcd\{f_{\Omega'}, f_{(\Omega - \{0\})}\} && (54)\\
&\leq \sum_{i \in \Omega' \cup (\Omega - \{0\})} (k - \deg_q f_i) && (55)\\
&= \sum_{i \in \Omega'} (k - \deg_q f_i) + \sum_{i \in (\Omega - \{0\})} (k - \deg_q f_i) && (56)\\
&= (k - \deg_q f_0) + \sum_{i \in (\Omega - \{0\})} (k - \deg_q f_i) && (57)\\
&= \sum_{i \in \Omega} (k - \deg_q f_i) && (58)
\end{aligned}$$

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,

$$g_0 \circ x^{q^r} \circ f_0 = \sum_{i=1}^{\ell} g_i \circ x^{q^r} \circ f_i = 0 \tag{59}$$

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 $(k - 1, m, n)$.

(i) holds for $(f'_1, \ldots, f'_m)$: 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, (ii) holds for $(f'_1, \ldots, f'_m)$ 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,

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

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 $g_m = 0$. 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 $\deg_q f_m \leq k-2$, then,

$$0 = g_m' \circ x^{q^{r+1}} \circ f_m' + \sum_{i=1}^{m-1} g_i \circ x^{q^{r+1}} \circ f_i' \tag{60}$$

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

Case 2c: Wlog, 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 $\mathcal{Z}_m \neq [n]$. Wlog, 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

$$f_i' = \mathsf{f}(\mathcal{Z}_i', t_i') = \begin{cases} \mathsf{f}(\mathcal{Z}_i, t_i) & n \notin \mathcal{Z}_i \\ \mathsf{f}(\mathcal{Z}_i - \{n\}, t_i + 1) & n \in \mathcal{Z}_i \end{cases} \tag{61}$$

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

$$k - \deg_q f'_\Omega = k - \left|\bigcap_{i\in\Omega} \mathcal{Z}'_i\right| - \min_{i\in\Omega} t'_i \tag{62}$$

$$\leq k - \left(\left|\bigcap_{i\in\Omega} \mathcal{Z}_i\right| - 1\right) - \min_{i\in\Omega} t_i \tag{63}$$

$$= k + 1 - \deg_q f_\Omega \tag{64}$$

$$\leq \sum_{i\in\Omega} (k - \deg_q f_i) \tag{65}$$

$$= \sum_{i\in\Omega} (k - \deg_q f'_i) \tag{66}$$

where the last inequality is because we assume (41) 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 $|\Omega| = m$, (41) was not strict; however, there is no need to have the $+1$ in (64) 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

$$\sum_{i=1}^{m} g'_i \circ x^{q^r} \circ f'_i = \left(\sum_{i=1}^{m} g_i \circ x^{q^r} \circ f_i\right)\Bigg|_{x_n=0} = 0 \mid_{x_n=0} = 0 \tag{67}$$

Then, $g'_1 = \cdots = g'_m = 0$. Contradiction. □

4 Conclusion

In this paper, we extended our proof technique in [1] 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.* [8] can be applied to networks with any number of source nodes, which had been shown only for 3 source nodes.

Theorem 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.

References

[1] H. Yildiz and B. Hassibi, "Optimum linear codes with support constraints over small fields," in *2018 IEEE Information Theory Workshop (ITW)*. IEEE, 2018, pp. 1–5.

[2] 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.

[3] 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.

[4] 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.

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

[6] A.-L. Horlemann-Trautmann and K. Marshall, "New criteria for MRD and Gabidulin codes and some rank-metric code constructions," *Advances in Mathematics of Communications*, vol. 11, no. 3, pp. 533–548, 2017.

[7] 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.

[8] 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.

[9] R. Lidl and H. Niederreiter, *Finite fields*. Cambridge University Press, 1997.

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

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 $a, b \in \mathsf{R}_n[x]$,

$$(a+b)^q = a^q + b^q \tag{68}$$

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 (68), 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* $t \geq 0$,

$$f = \prod_{\beta \in V} (x - \beta)^{q^t} \in \mathsf{L}_n \tag{69}$$

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

$$\operatorname{span}\{x_j : j \in \mathcal{Z}_1\} \cap \operatorname{span}\{x_j : j \in \mathcal{Z}_2\} = \operatorname{span}\{x_j : j \in \mathcal{Z}_1 \cap \mathcal{Z}_2\},$$

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:

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

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

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

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

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*

$$f' = \begin{cases} \mathsf{f}(\mathcal{Z}, t) & n \notin \mathcal{Z} \\ \mathsf{f}(\mathcal{Z} - \{n\}, t+1) & n \in \mathcal{Z} \end{cases} \tag{70}$$

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

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

□

B Generalized Hall's Theorem

Let $G = (U, V, E)$ represent the bipartite graph with the bipartite sets of vertices U and V and the edges $E \subset U \times V$. Let $N_G(\Omega) \subset V$ denote the neighborhood of $\Omega \subset U$, i.e. the set of all vertices in V adjacent to some element of Ω.

Theorem 4 (Generalized Hall's Theorem)**.** *Let $G = (U, V, E)$ 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 $\Omega \subset U$,*

$$|N_G(\Omega)| \geq c + \sum_{i \in \Omega} d_i \tag{71}$$

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 $i \in U$. ◇

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

1. (71) is *tight* for some Ω with $2 \leq |\Omega| \leq n - 1$.

   Let $G_1 = (\Omega, V, E_1)$, where $E_1 = E \cap (\Omega \times V)$ and $G_2 = (\Omega^c \cup \{\Omega\}, V, E_2)$, where $\Omega^c = U - \Omega$ and

   $$E_2 = (E - E_1) \cup \{(\Omega, j) : j \in N_G(\Omega)\}$$

   In other words, to obtain G_2, we merge the vertices in Ω into a single vertex called Ω with the edges from that to every vertex in $N_G(\Omega)$. Furthermore, let $d_\Omega = \sum_{i \in \Omega} d_i$.

We will show that (71) holds for G_1 and G_2 if and only if it holds for G. ($\Leftarrow$ direction is trivial) Let $\Omega_1 \subset \Omega, \Omega_2 \subset \Omega^c$. Then,

$$\begin{aligned}
|N_G(\Omega_1 \cup \Omega_2)| &= |N_G(\Omega_1)| + |N_G(\Omega_2) - N_G(\Omega_1)| \\
&\geq |N_G(\Omega_1)| + |N_G(\Omega_2) - N_G(\Omega)| \\
&= |N_G(\Omega_1)| + |N_G(\Omega_2 \cup \Omega)| - |N_G(\Omega)| \\
&= |N_{G_1}(\Omega_1)| + |N_{G_2}(\Omega_2 \cup \{\Omega\})| - (c + d_\Omega) \\
&\geq \left(c + \sum_{i \in \Omega_1} d_i\right) + \left(c + d_\Omega + \sum_{i \in \Omega_2} d_i\right) - (c + d_\Omega) \\
&= c + \sum_{i \in \Omega_1 \cup \Omega_2} d_i
\end{aligned}$$

Since $|\Omega| \leq n-1$ and $|\Omega^c \cup \{\Omega\}| \leq n-1$, by the induction hypothesis, we can remove edges from G_1 and 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 G_2 will be removed since its degree is already $c + d_\Omega$.)

2. (71) is *strict* for all Ω with $2 \leq |\Omega| \leq n-1$.
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 (**??**) because all the inequalities are strict except for $|\Omega| = n$, in which case, the left hand side is not affected. Now, we can assume that if a vertex $i \in U$ has degree 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:

Corollary 2 (Hall's Theorem)**.** *Let $G = (U, V, E)$ be a bipartite graph. If $|N_G(\Omega)| \geq |\Omega|$ for all $\Omega \subset U$, then there is a one-to-one matching from U to V.* ◇

Letting $c = |V| - |U|$ and $d_i = 1$ for all i yields to the following corollary, which is also proved in [3, Theorem 2]:

Corollary 3. *Let $\mathcal{Z}_1, \mathcal{Z}_2, \ldots, \mathcal{Z}_k \subset [n]$ such that for all nonempty $\Omega \subset [k]$,*

$$\left|\bigcap_{i \in \Omega} \mathcal{Z}_i\right| + |\Omega| \leq k \tag{72}$$

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. ◇

Proof. Consider the bipartite graph $G = ([k], [n], E)$ where $E = \{(i,j) : j \notin \mathcal{Z}_i\}$. Then, $\left|\bigcap_{i \in \Omega} \mathcal{Z}_i\right| = n - |N_G(\Omega)|$ and the inequality becomes

$$|N_G(\Omega)| \geq (n-k) + |\Omega| \tag{73}$$

Note that removing edges from the graph corresponds to adding elements from $[n]$ to the subsets. □