Linearized Reed-Solomon Codes with Support-Constrained Generator Matrix

Hedongliang Liu*, Hengjia Wei†‡, Antonia Wachter-Zeh*, Moshe Schwartz§
*School of Computation, Information and Technology, Technical University of Munich, Germany
†Peng Cheng Laboratory, Shenzhen, China
‡ School of Mathematics and Statistics, Xi'an Jiaotong University, Xi'an, China
§School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Israel
lia.liu@tum.de, hjwei05@gmail.com, antonia.wachter-zeh@tum.de, schwartz@ee.bgu.ac.il

2023 IEEE Information Theory Workshop (ITW) | 979-8-3503-0149-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ITW55543.2023.10161635

***Abstract*—Linearized Reed-Solomon (LRS) codes are a class of evaluation codes based on skew polynomials. They achieve the Singleton bound in the sum-rank metric, and therefore are known as maximum sum-rank distance (MSRD) codes. In this work, we give necessary and sufficient conditions on the existence of MSRD codes with support-constrained generator matrix. These conditions are identical to those for MDS codes and MRD codes. Moreover, the required field size for an $[n,k]_{q^m}$ LRS codes with support-constrained generator matrix is $q \geqslant \ell+1$ and $m \geqslant \max_{l\in[\ell]}\{k-1+\log_q k, n_l\}$, where ℓ is the number of blocks and n_l is the size of the l-th block. The special cases of the result coincide with the known results for Reed-Solomon codes and Gabidulin codes.**

I. Introduction

Designing error-correcting codes with support-constrained generator matrices is motivated by its application in network coding for wireless cooperative data exchange [1], wireless sensor networks [2] and multiple access networks [3]. From both, the theoretical and the practical point of view, the objective is to design codes with support-constrained generator matrix achieving the maximum minimum distance. In Hamming metric, research has been done in developing and proving necessary and sufficient conditions such that there exists an MDS code fulfilling the support constraints. It was first conjectured in [4], referred as the *GM–MDS conjecture*, and finally proven by Yildiz and Hassibi [5] and independently by Lovett [6].

Theorem 1 (GM–MDS Condition [5], [6])**.** *Let $Z_1,\dots,Z_k \subseteq \{1,\dots,n\}$ be such that for any nonempty $\Omega \subseteq \{1,\dots,k\}$,*

$$\left|\bigcap_{i\in\Omega} Z_i\right| + |\Omega| \leqslant k \ . \tag{1}$$

Then for any $q \geqslant n+k-1$, there exists an $[n,k]_q$ Reed–Solomon (RS) code with a generator matrix $\boldsymbol{G} \in \mathbb{F}_q^{k\times n}$ fulfilling the support constraint:

$$\boldsymbol{G}_{ij} = 0 \ , \quad \forall i \in \{1,\dots,k\},\ \forall j \in Z_i \ . \tag{2}$$

Yildiz and Hassibi adapted the approach to Gabidulin codes in [7] and derived the following GM–MRD condition.

The work has been supported by the German Research Foundation (DFG) with a German Israeli Project Cooperation (DIP) under grants no. PE2398/1-1, KR3517/9-1.

Theorem 2 (GM–MRD Condition [7, Theorem 1])**.** *Let $Z_1,\dots,Z_k \subseteq \{1,\dots,n\}$ fulfill (1) for any nonempty $\Omega \subseteq \{1,\dots,k\}$. Then for any prime power q and integer $m \geqslant \max\{n, k-1+\log_q k\}$, there exists an $[n,k]_{q^m}$ Gabidulin code with a generator matrix $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k\times n}$ fulfilling (2).*

Linearized Reed-Solomon codes [8], [9] are a class of evaluation codes based on skew polynomials [10], achieving the Singleton bound in the sum-rank metric, and therefore known as maximum sum-rank distance (MSRD) codes. They have been applied in network coding [11], locally repairable codes [12] and code-based cryptography [13].

Motivated by the practical interest of codes with support-constrained generator matrix and the prosperous research on sum-rank metric codes (in particular, LRS codes), we investigate the existence of MSRD codes with a support-constrained generator matrix in this work. We present in Section III our main results on the necessary and sufficient conditions for the existence of MSRD codes with a support-constrained generator matrix as in (2) and the sufficient field size of an LRS code fulfilling the support constraint. Section IV provides the proof of the sufficient condition. Due to the page limit, some proofs are omitted and can be found in the full version [14].

II. Preliminaries

A. Notations

Denote by $[a,b]$ the set of integers $\{a, a+1, \dots, b-1, b\}$, and let $[b] := [1,b]$. Let $\mathbb{N}$ be the set of natural numbers and $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Denote by $\mathbb{F}_q$ the finite field of size q, and by $\mathbb{F}_{q^m}$ its extension field of extension degree m.

Given two vectors $\boldsymbol{a} = (a_1,\dots,a_n), \boldsymbol{b} = (b_1,\dots,b_n) \in \mathbb{F}^n$, we define their *star-product* as the entry-wise multiplication, i.e., $\boldsymbol{a} \star \boldsymbol{b} := (a_1b_1, a_2b_2, \dots, a_nb_n) \in \mathbb{F}^n$. Given a vector $\boldsymbol{a} \in \mathbb{F}^n$, let $\mathrm{diag}(\boldsymbol{a}) \in \mathbb{F}^{n\times n}$ be the diagonal matrix with entries of $\boldsymbol{a}$ on its diagonal.

Throughout the paper, unless specified otherwise, the indices of entries in vectors, elements in sets, etc., start from 1, while the coefficients of polynomials start from 0.

B. Skew Polynomials

Let $\mathbb{F}_{q^m}[X;\theta]$ be a skew polynomial ring over $\mathbb{F}_{q^m}$ with automorphism $\theta : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$. The degree of a skew polynomial $f(X) = \sum_i f_i X^i \in \mathbb{F}_{q^m}[X;\theta]$ is $\deg f(X) := \max\{i \mid f_i \neq 0\}$. The addition in $\mathbb{F}_{q^m}[X;\theta]$ is defined to be the usual addition of polynomials and the multiplication is defined by the basic rule $X \cdot \alpha = \theta(\alpha) \cdot X, \forall \alpha \in \mathbb{F}_{q^m}$ and extended to all elements of $\mathbb{F}_{q^m}[X;\theta]$ by associativity and distributivity. For two skew polynomials $f(X) = \sum_i f_i X^i$ and $g(X) = \sum_j g_j X^j$, their product is

$$f(X) \cdot g(X) = \sum_i \sum_j f_i \theta^i(g_j) X^{i+j}. \tag{3}$$

The degree of the product is $\deg(f(X) \cdot g(X)) = \deg f(X) + \deg g(X)$. For ease of notation, when it is clear from the context, we may omit the variable notation in $f(X)$ for $f \in \mathbb{F}_{q^m}[X;\theta]$, and write only f.

Since skew polynomials are non-commutative under multiplication and division, we denote by $|_r$ and $|_l$ the right and left division respectively. The powers of θ are $\theta^i(\alpha) = \theta(\theta^{i-1}(\alpha))$. For any $\alpha \in \mathbb{F}_{q^m}$, its *$i$-th truncated norm* is defined as $N_i(\alpha) := \prod_{j=0}^{i-1} \theta^j(\alpha)$ and $N_0(\alpha) = 1$. For the Frobenius automorphism, $\sigma : \alpha \mapsto \alpha^q$, $\sigma^i(\alpha) = \alpha^{q^i}$, and $N_i(\alpha) = \alpha^{(q^i-1)/(q-1)}$.

Definition 1 (θ-Conjugacy Classes)**.** *Two elements $a, b \in \mathbb{F}_{q^m}$ are called* θ-conjugate *if there exists a nonzero element $c \in \mathbb{F}_{q^m}$ such that $b = \theta(c)ac^{-1}$. Otherwise, they are called* θ-distinct*. The* conjugacy class *of a with respect to θ is the set*

$$C_\theta(a) := \{\theta(c)ac^{-1} \mid c \in \mathbb{F}_{q^m} \backslash \{0\}\} \ .$$

The remainder evaluation of $f \in \mathbb{F}_{q^m}[X;\theta]$ at $\alpha \in \mathbb{F}_{q^m}$ is $f(\alpha) = \sum_{i=0}^{\deg f} f_i N_i(\alpha)$ (see [15, Lemma 2.4]). With this form, α is a root of f if and only if $(X-\alpha)|_r f$. Similar to the evaluation of conventional polynomials, the evaluation of a $f \in \mathbb{F}_{q^m}[X;\theta]$ at $\Omega = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_{q^m}$ can be written as $(f(\alpha_1), \ldots, f(\alpha_n)) = \boldsymbol{f} \cdot \boldsymbol{V}_k^\theta(\Omega)$, where k is the degree of f, $\boldsymbol{f} = (f_0, \ldots, f_k)$ contains the coefficients of f, and $\boldsymbol{V}_{k+1}^\theta(\Omega)$ is the first $k+1$ rows of $\boldsymbol{V}^\theta(\Omega)$ defined below.

Definition 2 (θ-Vandermonde Matrix)**.** *Let θ be an automorphism $\theta : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$. Given a set $\Omega = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_{q^m}$, the θ-Vandermonde matrix of Ω is given by*

$$\boldsymbol{V}^\theta(\Omega) := \begin{pmatrix} N_0(\alpha_1) & N_0(\alpha_2) & \ldots & N_0(\alpha_n) \\ N_1(\alpha_1) & N_1(\alpha_2) & \ldots & N_1(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ N_{n-1}(\alpha_1) & N_{n-1}(\alpha_2) & \ldots & N_{n-1}(\alpha_n) \end{pmatrix},$$

where $N_0(\alpha) = 1$, and for $i \geqslant 1$, $N_i(\alpha) = \prod_{j=0}^{i-1} \theta^j(\alpha)$ is the i-th truncated norm of α.

Definition 3 (Minimal Polynomial)**.** *Given a nonempty set $\Omega \subseteq \mathbb{F}_{q^m}$, we define its* minimal polynomial *in $\mathbb{F}_{q^m}[X;\theta]$ as a monic polynomial $f_\Omega \in \mathbb{F}_{q^m}[X;\theta]$ of minimal degree such that $f_\Omega(\alpha) = 0$ for all $\alpha \in \Omega$.*

It was shown in [16, Lemma 5] (see also [17, Theorem 2.5]) that the minimal polynomial of any nonempty set $\Omega = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_{q^m}$ is unique. The minimal polynomial can be constructed by an iterative Newton interpolation approach as in [17, Proposition 2.6] or by computing

$$f_\Omega(X) = \operatorname*{lclm}_{\alpha \in \Omega}\{X - \alpha\}. \tag{4}$$

where lclm is defined as follows.

Definition 4. *The least common left multiple (lclm) of $g_i \in \mathbb{F}_{q^m}[X;\theta]$, denoted by $\mathrm{lclm}_i\{g_i\}$, is the unique monic polynomial $h \in \mathbb{F}_{q^m}[X;\theta]$ s.t. $g_i|_r h, \forall i$.*

The *polynomial independence* of a set is defined via its minimal polynomials.

Definition 5 (P-independent Set [17, Def. 2.6])**.** *A set $\Omega \subseteq \mathbb{F}_{q^m}$ is P-independent in $\mathbb{F}_{q^m}[X;\theta]$ if $\deg(f_\Omega) = |\Omega|$.*

Given a P-independent set $\Omega \subseteq \mathbb{F}_{q^m}$, $\deg(f_\Omega) = |\Omega| = \mathrm{rank}(\boldsymbol{V}^\theta(\Omega))$ [16, Theorem 8] and all of its subsets are P-independent [17, Corollary 2.8].

Lemma 1. *Given a P-independent set Ω, for any subset $\mathcal{Z} \subset \Omega$, let $f_\mathcal{Z}(x) \in \mathbb{F}_{q^m}[X;\theta]$ be the minimal polynomial of $\mathcal{Z}$. Then, for any element $\alpha \in \Omega \backslash \mathcal{Z}$, $f_\mathcal{Z}(\alpha) \neq 0$.*

Proof: Assume $f_\mathcal{Z}(\alpha) = 0$, then the minimal polynomial $f_{\mathcal{Z} \cup \{\alpha\}} = f_\mathcal{Z}$ and $\deg(f_{\mathcal{Z} \cup \{\alpha\}}) = |\mathcal{Z}| < |\mathcal{Z} \cup \{\alpha\}|$, which contradicts to that $\mathcal{Z} \cup \{\alpha\} \subseteq \Omega$ is P-independent. ■

C. Linearized Reed-Solomon Codes

The definition of LRS codes adopted in this paper follows from the *generalized skew evaluations codes* [8, Section III] with particular choices of the evaluation points and column multipliers.

Definition 6 (Linearized Reed-Solomon (LRS) Codes)**.** *Let $\ell \leqslant q-1, n_i \leqslant m$ be positive integers for all $i = 1, \ldots, \ell$ and $n := \sum_{i=1}^{\ell} n_i$. Let $a_1, \ldots, a_\ell \in \mathbb{F}_{q^m}$ be from distinct σ-conjugacy classes of $\mathbb{F}_{q^m}$, and called* block representatives. *Let*

$$\boldsymbol{b} = (\beta_{1,1}, \ldots, \beta_{1,n_1} \vdots \cdots \vdots \beta_{\ell,1}, \ldots, \beta_{\ell,n_\ell}) \in \mathbb{F}_{q^m}^n$$

be a vector of column multipliers*, where $\beta_{l,1}, \ldots, \beta_{l,n_l}$ are linearly independent over $\mathbb{F}_q, \forall l \in [\ell]$.*

Let the set of code locators *be*

$$\mathcal{L} = \{a_1\beta_{1,1}^{q-1}, \ldots, a_1\beta_{1,n_1}^{q-1} \vdots \cdots \vdots a_\ell\beta_{\ell,1}^{q-1}, \ldots, a_\ell\beta_{\ell,n_\ell}^{q-1}\} \ . \tag{5}$$

An $[n,k]_{q^m}$ linearized Reed-Solomon *code is defined as*

$$\mathcal{C}_k^\sigma(\mathcal{L}, \boldsymbol{b}) := \{\boldsymbol{b} \star (f(\alpha))_{\alpha \in \mathcal{L}} \mid f(X) \in \mathbb{F}_{q^m}[X;\sigma], \deg f(X) < k\},$$

where the evaluation $f(\alpha) = \sum_{i=0}^{\deg f} f_i N_i(\alpha)$ is the remainder evaluation.

The code locator set $\mathcal{L}$ of LRS codes is P-independent [17, Theorem 2.11]. A generator matrix of the LRS code in Definition 6 is given by

$$\boldsymbol{G}^{(\mathsf{LRS})} = \begin{pmatrix} \boldsymbol{G}_1^{(\mathsf{LRS})} & \vdots & \ldots & \vdots & \boldsymbol{G}_\ell^{(\mathsf{LRS})} \end{pmatrix} \in \mathbb{F}_{q^m}^{k \times n} \tag{6}$$

where for each $l \in [\ell]$,

$$
\begin{aligned}
&\boldsymbol{G}_l^{(\mathsf{LRS})} = \boldsymbol{V}_k^{\sigma}(\mathcal{L}^{(l)}) \cdot \operatorname{diag}(\boldsymbol{b}^{(l)}) \\
&= \begin{pmatrix} 1 & \dots & 1 \\ N_1(a_l\beta_{l,1}^{q-1}) & \dots & N_1(a_l\beta_{l,n_l}^{q-1}) \\ \vdots & \ddots & \vdots \\ N_{k-1}(a_l\beta_{l,1}^{q-1}) & \dots & N_{k-1}(a_l\beta_{l,n_l}^{q-1}) \end{pmatrix} \cdot \begin{pmatrix} \beta_{l,1} & & \\ & \ddots & \\ & & \beta_{l,n_l} \end{pmatrix} \\
&= \begin{pmatrix} 1 & & \\ & \ddots & \\ & & N_{k-1}(a_l) \end{pmatrix} \cdot \begin{pmatrix} \beta_{l,1} & \beta_{l,2} & \dots & \beta_{l,n_l} \\ \beta_{l,1}^{q^1} & \beta_{l,2}^{q^1} & \dots & \beta_{l,n_l}^{q^1} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{l,1}^{q^{k-1}} & \beta_{l,2}^{q^{k-1}} & \dots & \beta_{l,n_l}^{q^{k-1}} \end{pmatrix}, \qquad (7)
\end{aligned}
$$

where $\mathcal{L}^{(l)} := \{a_l\beta_{l,1}, \dots, a_l\beta_{l,n_l}\}$ and $\boldsymbol{b}^{(l)} := (\beta_{l,1}, \dots, \beta_{l,n_l})$. Eq. (7) holds because for $\sigma(a) = a^q$, $N_i(\beta_{l,t}^{q-1}) \cdot \beta_{l,t} = \left(\beta_{l,t}^{q-1}\right)^{(q^i-1)/(q-1)} \cdot \beta_{l,t} = \beta_{l,t}^{q^i}$.

III. LRS Codes with Support Constraints

In this section we show that (1) is also a necessary and sufficient condition that a matrix $\boldsymbol{G}$ fulfilling (2) generates an MSRD code.

Since the sum-rank weight is at most the Hamming weight for any vector in $\mathbb{F}_{q^m}^n$, an MSRD code is necessarily an MDS code. Therefore, (1) is also a necessary condition for $\boldsymbol{G}$ to generate an MSRD code.

Now we proceed to show the sufficiency of (1) for MSRD codes, in particular, LRS codes. Note that for any $\Omega = \{i\}$, we have $|Z_i| \leqslant k-1$. One can add elements from $[n]$ to each Z_i until $|Z_i|$ reaches $k-1$ while preserving (1) [7, Corollary 3]. This operation will only put more zero constraints on $\boldsymbol{G}$ but not remove any. This means that the code we design under the new Z_i's of size $k-1$ will also satisfy the original constraints. Therefore, without loss of generality, along with (1), we will further assume that

$$|Z_i| = k-1, \ \forall i \in [k] \ . \qquad (8)$$

Let $\boldsymbol{G}^{(\mathsf{LRS})}$ be a generator matrix of an LRS code as given in (6). Given the following matrix

$$\boldsymbol{G} = \boldsymbol{T} \cdot \boldsymbol{G}^{(\mathsf{LRS})}, \qquad (9)$$

if $\boldsymbol{T} \in \mathbb{F}_{q^m}^{k\times k}$ has full rank, then $\boldsymbol{G}$ is another generator matrix of the same LRS code generated by $\boldsymbol{G}^{(\mathsf{LRS})}$. Recall that $a_1, \dots, a_\ell \in \mathbb{F}_{q^m}$ are the block representatives, $\beta_{1,1}, \dots, \beta_{1,n_1}, \dots, \beta_{\ell,1}, \dots, \beta_{\ell,n_\ell} \in \mathbb{F}_{q^m}$ are the column multipliers, and $\mathcal{L} = \{\alpha_1, \dots, \alpha_n\}$ is the code locator set as defined in Definition 6, where $\alpha_j = a_l\beta_{l,t}^{q-1}$ for some $l \in [\ell]$ and $t \in [n_l]$, $\forall j \in [n]$. Let $n_0 = 0$. Define the following bijective map between the indices, $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$,

$$(l,t) \mapsto j = t + \sum_{r=0}^{l-1} n_r, \qquad (10)$$

such that $\alpha_j = a_l\beta_t^{q-1}$. The inverse map $\varphi^{-1} : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ is $j \mapsto (l,t)$, where $l = \max\{i \mid \sum_{r=1}^{i} n_r \leqslant j\}$ and $t = j - \sum_{r=0}^{l-1} n_r$.

For all $i \in [k]$, define the skew polynomials

$$f_i(X) := \sum_{j=0}^{k-1} T_{i,j+1} X^j \ \in \mathbb{F}_{q^m}[X;\sigma] \ , \qquad (11)$$

where $T_{i,j+1}$ is the entry at i-th ($1 \leqslant i \leqslant k$) row, $j+1$-th ($1 \leqslant j+1 \leqslant k$) column in $\boldsymbol{T}$. The entries of $\boldsymbol{G}$ will be $G_{ij} = f_i(a_l\beta_{l,t}^{q-1})\beta_{l,t}, i \in [k], j = \varphi(l,t) \in [n]$. Then, the zero constraints in (2) become root constraints on f_i's:

$$f_i(a_l\beta_{l,t}^{q-1}) = 0, \quad \forall i \in [k], \ \forall j = \varphi(l,t) \in Z_i \ . \qquad (12)$$

For brevity, we denote by

$$\mathcal{Z}_i := \{a_l\beta_{l,t}^{q-1} \mid \varphi(l,t) \in Z_i\} \qquad (13)$$

corresponding to the zero set Z_i. We simplify the notation, denoting by $f_i(X) := f_{\mathcal{Z}_i}(X)$, the minimal polynomial of $\mathcal{Z}_i$, which can be written in the form

$$f_i(X) = f_{\mathcal{Z}_i}(X) = \operatorname*{lclm}_{\alpha \in \mathcal{Z}_i}\{(X-\alpha)\}. \qquad (14)$$

Since $\mathcal{L}$ and any subset $\mathcal{Z}_i \subset \mathcal{L}$ are all P-independent, it follows from Lemma 1 that $f_i(\alpha) \neq 0$, for all $\alpha \in \mathcal{L}\backslash\mathcal{Z}_i$. Hence, there is no other zero in $\boldsymbol{G}$ than the required positions in Z_i's. Moreover, by the assumption in (8), $|\mathcal{Z}_i| = |Z_i| = k-1$, and $\deg f_i(X) = k-1, \forall i \in [k]$. Hence the coefficients of $f_i(X)$ in (11) are uniquely determined (up to scaling) in terms of $a_1\beta_{1,1}^{q-1}, \dots, a_\ell\beta_{\ell,n_\ell}^{q-1}$. In the following, we assume $a_1, \dots, a_\ell$ are fixed, non-zero, and from distinct σ-conjugacy classes. We see $\beta_{l,t}$'s as variables of the following commutative multivariate polynomial ring

$$R_n := \mathbb{F}_{q^m}[\beta_{1,1}, \dots, \beta_{\ell,n_\ell}], \qquad (15)$$

and the coefficients $T_{i,j+1}$ of $f_i(X)$ can be seen as polynomials in R_n. Then the problem of finding $\beta_{l,t}$'s such that $\boldsymbol{G}$ generates the same LRS code as $\boldsymbol{G}^{(\mathsf{LRS})}$ becomes finding $\beta_{l,t}$'s such that

$$
\begin{aligned}
P(\beta_{1,1}, \dots, \beta_{\ell,n_\ell}) :=& P_{\boldsymbol{T}}(\beta_{1,1}, \dots, \beta_{\ell,n_\ell}) \\
&\cdot \prod_{l=1}^{\ell} P_{\boldsymbol{M}_l}(\beta_{l,1}, \dots, \beta_{l,n_l}) \neq 0 \qquad (16)
\end{aligned}
$$

where $P_{\boldsymbol{T}}$ is the determinant of $\boldsymbol{T}$, whose entries are determined by the minimal polynomials f_i's, and

$$P_{\boldsymbol{M}_l} := \det \begin{pmatrix} \beta_{l,1} & \beta_{l,2} & \dots & \beta_{l,n_l} \\ \beta_{l,1}^{q^1} & \beta_{l,2}^{q^1} & \dots & \beta_{l,n_l}^{q^1} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{l,1}^{q^{n_l-1}} & \beta_{l,2}^{q^{n_l-1}} & \dots & \beta_{l,n_l}^{q^{n_l-1}} \end{pmatrix}.$$

Since the coefficient of the monomial $\prod_{i=1}^{n_l} \beta_{l,i}^{q^{i-1}}$ in $P_{\boldsymbol{M}_l}$ is 1, $P_{\boldsymbol{M}_l}$ is a nonzero polynomial in R_n. With Claim 1 below, we can conclude that $P(\beta_{1,1}, \dots, \beta_{\ell,n_\ell})$ is a nonzero polynomial in R_n.

Claim 1. *If the condition in* (1) *is satisfied, then* $P_{\boldsymbol{T}}$ *is a nonzero polynomial in* R_n.

Now we proceed to present the result on the field size by assuming Claim 1 is true. A more general version (Theorem 4) of the claim is given in Section IV-B.

For a fixed $l \in [\ell], t \in [n_\ell]$, the degree in $\beta_{l,t}$ of $P_{\boldsymbol{M}_l}$ is $\deg_{\beta_{l,t}} P_{\boldsymbol{M}_l} = q^{n_l-1}$ [18, Lemma 3.51]. Moreover, $\deg_{\beta_{l,t}} P_{\boldsymbol{T}} \leqslant (k-1)(q-1)\cdot q^{k-2}$, which can be shown by extending the analysis of linearized polynomials for Gabidulin codes in [7, Section II.F] to skew polynomials. The details of this extension are provided in [14, Appendix B]. Then, the degree of $P(\beta_{1,1},\dots,\beta_{\ell,n_\ell})$ in (16) as a polynomial in $\beta_{l,t}$ is

$$\deg_{\beta_{l,t}} P \leqslant (k-1)(q-1)\cdot q^{k-2} + q^{n_l-1} \ .$$

Theorem 3. *Let ℓ, n_l be positive integers and $n := \sum_{l=1}^{\ell} n_l$. Let $Z_1,\dots,Z_k \subset [n]$ fulfill (1) for any nonempty $\Omega \subseteq [k]$. Then for any prime power $q \geqslant \ell+1$ and integer $m \geqslant \max_{l\in[\ell]}\{k-1+\log_q k, n_l\}$, there exists an $[n,k]_{q^m}$ linearized Reed-Solomon code with ℓ blocks, and each block of length n_l, $l \in [\ell]$ with a generator matrix $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k\times n}$ fulfilling the support constraints in (2).*

Proof: Claim 1 has shown that $P(\beta_{1,1},\dots,\beta_{\ell,n_\ell})$ is a nonzero polynomial. By the Combinatorial Nullstellensatz [19, Theorem 1.2], there exist $\hat\beta_{1,1},\dots,\hat\beta_{\ell,n_\ell}$ in $\mathbb{F}_{q^m}$ such that

$$P(\hat\beta_{1,1},\dots,\hat\beta_{\ell,n_\ell}) \neq 0$$

if

$$\begin{aligned} q^m &> \max_{l\in[\ell],t\in[n_l]}\{\deg_{\beta_{l,t}} P\} \\ &= \max_{l\in[\ell]}\{(k-1)(q-1)\cdot q^{k-2}+q^{n_l-1}\} \ . \end{aligned} \tag{17}$$

If $m \geqslant \max_{l\in[\ell]}\{k-1+\log_q k \ , \ n_l\}$, we have

$$\begin{aligned} q^m =& (q-1)q^{m-1}+q^{m-1} \\ \geqslant& \max_{l\in[\ell]}\{k(q-1)\cdot q^{k-2}+q^{n_l-1}\} > (17) \ . \end{aligned}$$

To have $a_1,\dots,a_\ell$ from different nontrivial σ-conjugacy class of $\mathbb{F}_{q^m}$, by the structure of σ-conjugacy classes [17, Theorem 2.12], we require $q-1 \geqslant \ell$. ∎

Remark 1. *Consider the extreme cases:*

1) *For $\ell = 1$, the sum-rank metric is the rank metric and LRS codes are Gabidulin codes.*
2) *For $\ell = n$ and $n_l = 1, \forall l \in [\ell]$, the sum-rank metric is the Hamming metric. In addition, with $\theta = \mathrm{Id}$, LRS codes are generalized RS codes with distinct nonzero $a_1,\dots,a_\ell$ as code locators and nonzero $\beta_{l,t}$'s as column multipliers (see [17, Theorem 2.17], [11, Table II]).*

For the first case, our result on the field size in Theorem 3 coincides with [7, Theorem 1]. For the second case, by adapting the setup in (15)-(16) to $\theta = \mathrm{Id}$, and the proof in [14, Appendix B] with the usual evaluation of commutative polynomials, one can obtain the same results as in [5, Theorem 2].

IV. Proof of Claim 1

A. Problem Setup

Let R_n be the multivariate commutative polynomial ring as defined in (15). Note that $R_0 = \mathbb{F}_{q^m}$. Let σ be the Frobenius automorphism of R_0, which we extend to any $a = \sum_{\boldsymbol{i}\in\mathbb{N}_0^n} a_{\boldsymbol{i}} \cdot \beta_{1,1}^{i_1}\cdots\beta_{\ell,n_\ell}^{i_n} \in R_n$ by

$$\begin{aligned} \sigma \ : \ & R_n \to R_n \\ \sum_{\boldsymbol{i}\in\mathbb{N}_0^n} a_{\boldsymbol{i}}\cdot\beta_{1,1}^{i_1}\cdots\beta_{\ell,n_\ell}^{i_n} &\mapsto \sum_{\boldsymbol{i}\in\mathbb{N}_0^n}\sigma(a_{\boldsymbol{i}})\cdot\sigma(\beta_{1,1}^{i_1})\cdots\sigma(\beta_{\ell,n_\ell}^{i_n}) \ . \end{aligned}$$

Let $R_n[X;\sigma]$ be the univariate skew polynomial ring with indeterminate X, whose coefficients are from R_n, i.e.,

$$R_n[X;\sigma] := \left\{ \sum_{i=0}^{d} c_i X^i \ \middle| \ d \geqslant 0, c_0,\dots,c_d \in R_n, \right\} \ .$$

For ease of notation, when it is clear from the context, we may omit the variable notation in $f(X)$ for $f \in R_n[X;\sigma]$, and write only f. The degree of $f = \sum_{i=0}^{d} c_i X^i \in R_n[X;\sigma]$ is $\deg f = d$ if d is the largest integer such that $c_d \neq 0$. We define $\deg 0 = -\infty$.

Similar to skew polynomials over a finite field, addition is commutative and multiplication is defined using the commutation rule

$$X \cdot a = \sigma(a)\cdot X, \ \forall a \in R_n, \tag{18}$$

which is naturally extended by distributivity and associativity. Just like (3), the product of $f, g \in R_n[X;\sigma]$ with $\deg f = d_f$ and $\deg g = d_g$ is

$$f \cdot g = \sum_{i=0}^{d_f}\sum_{j=0}^{d_g} f_i \sigma^i(g_j) X^{i+j}, \tag{19}$$

and the degree of the product is $\deg(f\cdot g) = d_f + d_g$. Note that in general, $f\cdot g \neq g \cdot f$, for $f, g \in R_n[X;\sigma]$.

By abuse of notation, in the following, we also denote by

$$\mathcal{L} = \{a_1\beta_{1,1}^{q-1},\dots,a_1\beta_{1,n_1}^{q-1} \ \vdots \ \dots \ \vdots \ a_\ell\beta_{\ell,1}^{q-1},\dots,a_\ell\beta_{\ell,n_\ell}^{q-1}\} \subseteq R_n$$

the P-independent set as a subset of R_n. Let $\mathcal{Z}_i \subseteq \mathcal{L}$ be the set as in (13) corresponding to Z_i and $f_{\mathcal{Z}_i} \in R_n[X;\sigma]$ be the minimal polynomial of $\mathcal{Z}_i$ as in (14). In the main result in Theorem 4, we are interested in skew polynomials in the following form: for any $Z \subseteq [n], \tau \geqslant 0$

$$\mathsf{f}(Z,\tau) := X^\tau \cdot \operatorname*{lclm}_{\substack{\alpha\in\{a_l\beta_{l,t}^{q-1} | \\ \varphi(l,t)\in Z\}}}\{(X-\alpha)\} \in R_n[X;\sigma] \ , \tag{20}$$

where $\varphi(l,t)$ is as defined in (10).

Define the set of skew polynomials of this form:

$$\begin{aligned} \mathcal{S}_{n,k} := \{\mathsf{f}(Z,\tau) \mid \tau \geqslant 0, Z \subseteq [n] \\ \text{s.t. } |Z| + \tau \leqslant k-1\} \subseteq R_n[X;\sigma]. \end{aligned} \tag{21}$$

Note that $\deg f \leqslant k-1, \forall f \in \mathcal{S}_{n,k}$.

B. Main Result

The following theorem is a more general statement than Claim 1 and it is the analog of [7, Theorem 3.A] for skew polynomials.

Theorem 4. *Let $k \geqslant s \geqslant 1$ and $n \geqslant 0$. For any $f_1, f_2, \ldots, f_s \in \mathcal{S}_{n,k}$, the following are equivalent:*

(i) *For all $g_1, g_2, \ldots, g_s \in R_n[X;\sigma]$ such that $\deg(g_i \cdot f_i) \leqslant k-1$, we have*
$$\sum_{i=1}^{s} g_i \cdot f_i = 0 \quad \Longrightarrow \quad g_1 = g_2 = \cdots = g_s = 0 \ .$$

(ii) *For all nonempty $\Omega \subseteq [s]$, we have*
$$k - \deg(\operatorname*{gcrd}_{i\in\Omega} f_i) \geqslant \sum_{i\in\Omega}(k - \deg f_i) \ . \qquad (22)$$

The proof of Theorem 4 is given in [14, Appendix C]. We will show in Corollary 1 that Claim 1 is a special case of Theorem 4. For this purpose, we give an equivalent way of writing it in terms of matrices with entries from R_n. This is done in Theorem 5, which is an analog to [7, Theorem 3.B].

We first describe the multiplication between skew polynomials in matrix language. Let $u = \sum_i u_i X^i \in R_n[X;\sigma]$. For $b-a \geqslant \deg u$, define the following matrix in $R_n^{a\times b}$

$$\boldsymbol{S}_{a\times b}(u) \coloneqq \begin{pmatrix} u_0 & \cdots & u_{b-a} & & \\ & \sigma(u_0) & \cdots & \sigma(u_{b-a}) & \\ & \ddots & \ddots & \ddots & \\ & & \sigma^{a-1}(u_0) & \cdots & \sigma^{a-1}(u_{b-a}) \end{pmatrix}.$$

In particular, for $a=1$, denote by $R_n[X;\sigma]_{<b}$ the set of skew polynomials of degree strictly less than b. The map

$$\begin{aligned} \boldsymbol{S}_{1\times b}(\cdot) \ : \ R_n[X;\sigma]_{<b} &\to R_n^b \\ u &\mapsto (u_0, \ldots, u_{b-1}) \end{aligned} \qquad (23)$$

is bijective and $\boldsymbol{S}_{1\times b}(0) = \boldsymbol{0}, \forall b \in \mathbb{N}$. For any skew polynomial $v = \sum_i v_i X^i \in R_n[X;\sigma]$, we have

$$\boldsymbol{S}_{a\times b}(v\cdot u) = \boldsymbol{S}_{a\times c}(v)\cdot \boldsymbol{S}_{c\times b}(u) \ , \qquad (24)$$

where $a, b, c \in \mathbb{N}$ are such that $c - a \geqslant \deg v, b - c \geqslant \deg u$. As a special case, when $v = X^\tau, \tau \in \mathbb{N}$, we can write

$$\begin{aligned} \boldsymbol{S}_{a\times(b+\tau)}(X^\tau\cdot u) &= \boldsymbol{S}_{a\times(a+\tau)}(X^\tau)\cdot \boldsymbol{S}_{(a+\tau)\times(b+\tau)}(u) \\ &= (\boldsymbol{0}_{a\times\tau} \quad \boldsymbol{I}_{a\times a})\cdot \boldsymbol{S}_{(a+\tau)\times(b+\tau)}(u). \end{aligned} \qquad (25)$$

By the definition in (20), $\mathsf{f}(Z,\tau) = X^\tau \cdot u$ for some $u \in R_n[X;\sigma]$. It can be readily seen from (25) that the first τ columns of $\boldsymbol{S}_{a\times(b+\tau)}(\mathsf{f}(Z,\tau))$ are all zero.

For $s \in [k]$, $i \in [s]$, let $f_i = \mathsf{f}(Z_i, \tau_i) \in \mathcal{S}_{n,k}$. We write $\boldsymbol{S}(f_i)$ instead of $\boldsymbol{S}_{(k-\tau_i-|Z_i|)\times k}(f_i)$ for ease of notation. By (25), $\boldsymbol{S}(f_i)$ looks like

$$\boldsymbol{S}(f_i) = \left.\begin{pmatrix} 0 & \cdots & 0 & \times & \times & \cdots & \times & & & \\ 0 & \cdots & 0 & & \times & \times & \cdots & \times & & \\ \vdots & & \vdots & & & \ddots & \ddots & & \ddots & \\ 0 & \cdots & 0 & & & & \times & \times & \cdots & \times \end{pmatrix}\right\} k-\tau_i-|Z_i|$$
$$\underbrace{\qquad}_{\tau_i} \quad \underbrace{\qquad\qquad}_{k-1-\tau_i-|Z_i|} \quad \underbrace{\qquad\qquad}_{|Z_i|+1}$$

where the $\times$'s represent possibly non-zero entries. Then, applying (24) to the expression $g_i \cdot f_i$ in Theorem 4 yields

$$\boldsymbol{S}_{1\times k}(g_i\cdot f_i) = \boldsymbol{u}_i \cdot \boldsymbol{S}(f_i) \ ,$$

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

$$\boldsymbol{S}_{1\times k}\Big(\sum_{i=1}^{s} g_i\cdot f_i\Big) = (\boldsymbol{u}_1, \cdots, \boldsymbol{u}_s)\cdot \underbrace{\begin{pmatrix} \boldsymbol{S}(f_1) \\ \vdots \\ \boldsymbol{S}(f_s) \end{pmatrix}}_{=:\boldsymbol{M}(f_1,\ldots,f_s)} \qquad (26)$$

which is a linear combination of the rows of $\boldsymbol{M}(f_1, \ldots, fs)$.

The following theorem is an equivalent statement to Theorem 4, in matrix language.

Theorem 5. *Let $k \geqslant s \geqslant 1$ and $n \geqslant 0$. For $i \in [s]$, let $Z_i \in [n], \tau_i \geqslant 0$ such that $\tau_i + |Z_i| \leqslant k-1$ and $f_i = \mathsf{f}(Z_i, \tau_i) \in \mathcal{S}_{n,k}$. The matrix $\boldsymbol{M}(f_1, \ldots, f_s)$ defined in (26) has full row rank if and only if, for all nonempty $\Omega \subseteq [s]$,*

$$k - \Big|\bigcap_{i\in\Omega} Z_i\Big| - \min_{i\in\Omega}\tau_i \geqslant \sum_{i\in\Omega}(k - \tau_i - |Z_i|) \ . \qquad (27)$$

The proof of Theorem 5 is omitted here due to page limit. It can be found in the full version [14] of this paper.

As a special case, when $s = k, \tau_i = 0$ and $|Z_i| = k-1, \forall i \in [k]$, each block $\boldsymbol{S}(f_i)$ becomes a row vector with entries being the coefficients of $f_i = \mathsf{f}(Z_i, \tau_i) = \sum_{j=0}^{k-1} f_{i,j+1}X^j \in R_n[X;\sigma]$ and

$$\boldsymbol{M}(f_1, \ldots, f_k) = \begin{pmatrix} f_{11} & f_{12} & \cdots & f_{1k} \\ f_{21} & f_{22} & \cdots & f_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ f_{k1} & f_{k2} & \cdots & f_{kk} \end{pmatrix} \in R_n^{k\times k} \ . \qquad (28)$$

Note that $\boldsymbol{M}(f_1, \ldots, f_k)$ coincides with the matrix $\boldsymbol{T}$ in (9). Hence we have Corollary 1 below, which is Claim 1.

Corollary 1. *For $i \in [k]$, let $Z_i \subseteq [n]$ with $|Z_i| = k-1$. Then $\det \boldsymbol{M}(f_1, \ldots, f_k)$ is a nonzero polynomial in R_n if and only if for all nonempty $\Omega \subseteq [k]$, $k - |\bigcap_{i\in\Omega} Z_i| \geqslant |\Omega|$.*

References

[1] M. Yan and A. Sprintson, "Weakly secure network coding for wireless cooperative data exchange," in *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011*, pp. 1–5, IEEE, 2011.
[2] 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*, pp. 1889–1893, IEEE, 2013.
[3] 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, 2014.
[4] 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*, pp. 1787–1791, IEEE, 2014.
[5] H. Yildiz and B. Hassibi, "Optimum linear codes with support constraints over small fields," in *2018 IEEE Information Theory Workshop (ITW)*, pp. 1–5, IEEE, 2018.
[6] 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)*, pp. 194–199, IEEE, 2018.

[7] H. Yildiz and B. Hassibi, “Gabidulin codes with support constrained generator matrices,” *IEEE Transactions on Information Theory*, vol. 66, no. 6, pp. 3638–3649, 2020.

[8] S. Liu, F. Manganiello, and F. R. Kschischang, “Construction and decoding of generalized skew-evaluation codes,” in *2015 IEEE 14th Canadian Workshop on Information Theory (CWIT)*, pp. 9–13, IEEE, 2015.

[9] U. Martínez-Peñas, “Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring,” *Journal of Algebra*, vol. 504, pp. 587–612, 2018.

[10] O. Ore, “Theory of non-commutative polynomials,” *Annals of mathematics*, pp. 480–508, 1933.

[11] U. Martínez-Peñas and F. R. Kschischang, “Reliable and secure multishot network coding using linearized Reed-Solomon codes,” *IEEE Transactions on Information Theory*, 2019.

[12] U. Martínez-Peñas and F. R. Kschischang, “Universal and dynamic locally repairable codes with maximal recoverability via sum-rank codes,” *IEEE Transactions on Information Theory*, 2019.

[13] F. Hörmann, H. Bartz, and A.-L. Horlemann, “Security considerations for Mceliece-like cryptosystems based on linearized Reed-Solomon codes in the sum-rank metric,” in *CBCrypto 2022: International Workshop on Code-Based Cryptography, May 29-30, 2022, Trondheim, Norway.*, 2022.

[14] H. Liu, H. Wei, A. Wachter-Zeh, and M. Schwartz, “Linearized Reed–Solomon codes with support-constrained generator matrix.” Available at https://arxiv.org/abs/2212.07991, 2022.

[15] T.-Y. Lam and A. Leroy, “Vandermonde and Wronskian matrices over division rings,” *Journal of Algebra*, vol. 119, no. 2, pp. 308–336, 1988.

[16] T.-Y. Lam, “A general theory of Vandermonde matrices,” *Expositions Mathematicae*, vol. 4, pp. 193–215, 1986.

[17] U. Martínez-Peñas, M. Shehadeh, and F. R. Kschischang, “Codes in the sum-rank metric: Fundamentals and applications,” *Foundations and Trends® in Communications and Information Theory*, vol. 19, no. 5, pp. 814–1031, 2022.

[18] R. Lidl and H. Niederreiter, *Finite fields*. No. 20, Cambridge university press, 1997.

[19] N. Alon, “Combinatorial Nullstellensatz,” *Combinatorics, Probability and Computing*, vol. 8, no. 1-2, pp. 7–29, 1999.