Maximum Sum-Rank Distance Codes over Finite Chain Rings

Umberto Martínez-Peñas[1] and Sven Puchinger[2]

[1] IMUVa-Mathematics Research Institute, University of Valladolid, Spain
umberto.martinez@uva.es
[2] Inst. Electrical and Computer Eng., Technical University of Munich, Germany
sven.puchinger@tum.de

Abstract. In this work, maximum sum-rank distance (MSRD) codes and linearized Reed-Solomon codes are extended to finite chain rings. It is proven that linearized Reed-Solomon codes are MSRD over finite chain rings, extending the known result for finite fields. For the proof, several results on the roots of skew polynomials are extended to finite chain rings. These include the existence and uniqueness of minimum-degree annihilator skew polynomials and Lagrange interpolator skew polynomials. An efficient Welch-Berlekamp decoder with respect to the sum-rank metric is then provided for finite chain rings.

Keywords: Finite chain rings · linearized Reed-Solomon codes · MSRD codes · sum-rank metric · Welch-Berlekamp decoding.

1 Introduction

The sum-rank metric [19] generalizes the Hamming and rank metrics. Codes in the sum-rank metric over finite fields have applications in multishot Network Coding [19, 16], Space-Time Coding with multiple fading blocks [14, 23] and Distributed Storage [17]. However, codes over rings may be more suitable for physical-layer Network Coding [4], and finite rings from the complex field allows for more choices of constellations for Space-Time codes [7, 6].

Maximum sum-rank distance (MSRD) codes are those whose minimum sum-rank distance attains the Singleton bound. Linearized Reed-Solomon codes [15] are the MSRD codes with smallest finite-field sizes (thus more computationally efficient) for the main parameter regimes. They cover a wide range of parameter values and are the only known MSRD codes compatible with square matrices. Linearized Reed-Solomon codes recover both generalized Reed-Solomon codes [22] and Gabidulin codes [5], whenever the sum-rank metric recovers the Hamming metric and the rank metric, respectively. Reed-Solomon codes over rings were systematically studied for the first time in [21]. Gabidulin codes over Galois rings were introduced in [7], and later extended to finite principal ideal rings in [6]. Such families of Gabidulin codes over rings were proposed for Space-Time Coding in the case of a single fading block in [6, 7], and they were proposed for physical-layer singleshot Network Coding in [6].

In this work, we introduce MSRD codes and linearized Reed-Solomon codes over finite chain rings. In Section 2, we collect some preliminaries on finite chain rings. In Section 3, we define the sum-rank metric over finite chain rings, together with the corresponding Singleton bound and the definition of MSRD codes. Section 4 contains the technical tools regarding skew polynomials for linearized Reed-Solomon codes and their decoding. In Section 5, we define linearized Reed-Solomon codes over finite chain rings and prove that they are MSRD. In Section 6, we provide a sum-rank metric Welch-Berlekamp decoder for linearized Reed-Solomon codes over finite chain rings.

2 Preliminaries on Finite Chain Rings

For a general reference, see [18]. A *chain ring* is a (local) ring whose ideals form a chain with respect to set inclusion. Throughout this manuscript, we fix a finite chain ring R. We will denote by $\mathfrak{m}$ the maximal ideal of R. We will fix the prime power $q = |R/\mathfrak{m}|$, and we denote $\mathbb{F}_q = R/\mathfrak{m}$, the *finite field* with q elements.

Let $h \in R[x]$ be a monic polynomial of degree m whose image in $\mathbb{F}_q[x]$ is irreducible. Throughout this manuscript, we will fix $S = R/(h)$. The ring S is a free local Galois extension of R of rank m with maximal ideal $\mathfrak{M} = \mathfrak{m}S$. Furthermore, the Galois group of $R \subseteq S$ is cyclic of order m, and generated by a ring automorphism $\sigma : S \longrightarrow S$ such that $R = \{a \in S \mid \sigma(a) = a\}$ and $\sigma(c) = c^q$, for some primitive element $c \in S$. Moreover, it holds that $S/\mathfrak{M} = \mathbb{F}_{q^m}$ and $\rho(\sigma(a)) = \overline{\sigma}(\rho(a))$, for all $a \in S$, where $\rho : S \longrightarrow S/\mathfrak{M} = \mathbb{F}_{q^m}$ is the natural projection map, and $\overline{\sigma}(b) = b^q$, for all $b \in \mathbb{F}_{q^m}$. We will usually denote $\overline{a} = \rho(a)$, and therefore, $\overline{\sigma(a)} = \overline{\sigma}(\overline{a})$, for $a \in S$.

An important feature of local rings is that the group of units is formed by the elements outside of the maximal ideal. That is, $R^* = R \setminus \mathfrak{m}$ and $S^* = S \setminus \mathfrak{M}$. Finally, the following technical lemma will be useful for our purposes. Items 2 and 3 follow from Item 1, which is [18, p. 92, ex. V.14].

Lemma 1. *Let $\beta_1, \beta_2, \ldots, \beta_r \in S$ be R-linearly independent (thus $r \leq m$).*

1. *There are $\beta_{r+1}, \ldots, \beta_m \in S$ such that $\beta_1, \beta_2, \ldots, \beta_m$ are a basis of S over R.*
2. *The projections $\overline{\beta}_1, \overline{\beta}_2, \ldots, \overline{\beta}_r \in \mathbb{F}_{q^m}$ are $\mathbb{F}_q$-linearly independent.*
3. *$\beta_1, \beta_2, \ldots, \beta_r \in S^*$.*

3 MSRD Codes on Finite Chain Rings

The sum-rank metric over fields was first defined in [19] but was previously used in [14, Sec. III]. The rank metric was extended to finite principal ideal rings in [6]. In this section, we will introduce the sum-rank metric for finite chain rings.

Since R is a finite chain ring, then it is a principal ideal ring. Therefore, given $A \in R^{m \times n}$, there exist two invertible matrices $P \in R^{m \times m}$ and $Q \in R^{n \times n}$, and a diagonal matrix $D = \mathrm{Diag}(d_1, d_2, \ldots, d_r) \in R^{m \times n}$, with $r = \min\{m, n\}$, such that $A = PDQ$. The elements $d_1, d_2, \ldots, d_r \in R$ are unique up to multiplication by units and the diagonal matrix D is called the *Smith normal form* of A. Hence we may define ranks and free ranks as in [6, Def. 3.3].

Definition 1. *Given $A \in R^{m\times n}$ with Smith normal form $D = \mathrm{Diag}(d_1, \ldots, d_r) \in R^{m\times n}$, $r = \min\{m, n\}$, we define the rank and free rank of A, respectively, as*

$$\mathrm{rk}(A) = |\{i \in [r] \mid d_i \neq 0\}| \quad \textit{and} \quad \mathrm{frk}(A) = |\{i \in [r] \mid d_i \in R^*\}|.$$

We will work with linear codes in S^n. To that end, we will translate the rank metric from $R^{m\times n}$ to S^n as in [6, Sec. III-B]. For a positive integer t and an ordered basis $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in S^m$ of S over R, we define $M_{\boldsymbol{\alpha}} : S^t \longrightarrow R^{m\times t}$ by

$$M_{\boldsymbol{\alpha}}(\mathbf{c}) = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,t} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m,1} & c_{m,2} & \cdots & c_{m,t} \end{pmatrix} \in R^{m\times t}, \tag{1}$$

where $\mathbf{c} = \sum_{i=1}^{m} \alpha_i(c_{i,1}, c_{i,2}, \ldots, c_{i,t}) \in R^t$, for $i = 1, 2, \ldots, m$. We define $\mathrm{rk}(\mathbf{c}) = \mathrm{rk}\left(M_{\boldsymbol{\alpha}}(\mathbf{c})\right)$ and $\mathrm{frk}(\mathbf{c}) = \mathrm{frk}\left(M_{\boldsymbol{\alpha}}(\mathbf{c})\right)$, which is independent of $\boldsymbol{\alpha}$ [6].

We may now define the sum-rank metric for the ring extension $R \subseteq S$. This definition coincides with the classical one [14, 19] when R and S are fields. Over finite chain rings, this definition coincides with the Hamming metric when $n_1 = n_2 = \ldots = n_\ell = 1$ and with rank metric as above [6] when $\ell = 1$.

Definition 2 (Sum-rank metric). *Consider positive integers $n_1, n_2, \ldots, n_\ell$ and $n = n_1 + n_2 + \cdots + n_\ell$. We define the sum-rank weight of $\mathbf{c} \in S^n$ over R for the length partition $n = n_1 + n_2 + \cdots + n_\ell$ as*

$$\mathrm{wt}_{SR}(\mathbf{c}) = \sum_{i=1}^{\ell} \mathrm{rk}\left(\mathbf{c}^{(i)}\right),$$

where $\mathbf{c} = \left(\mathbf{c}^{(1)}, \mathbf{c}^{(2)}, \ldots, \mathbf{c}^{(\ell)}\right)$ and $\mathbf{c}^{(i)} \in S^{n_i}$, for $i = 1, 2, \ldots, \ell$. We define the sum-rank metric $\mathrm{d}_{SR} : S^{2n} \longrightarrow S^n$ over R for the length partition $n = n_1 + n_2 + \cdots + n_\ell$ by $\mathrm{d}_{SR}(\mathbf{c}, \mathbf{d}) = \mathrm{wt}_{SR}(\mathbf{c} - \mathbf{d})$, for $\mathbf{c}, \mathbf{d} \in S^n$. For an arbitrary code $\mathcal{C} \subseteq S^n$, we define $\mathrm{d}_{SR}(\mathcal{C}) = \min\{\mathrm{d}_{SR}(\mathbf{c}, \mathbf{d}) \mid \mathbf{c}, \mathbf{d} \in \mathcal{C}, \mathbf{c} \neq \mathbf{d}\}$.

The sum-rank metric is indeed a metric by [6, Th. 3.9]. The subring R and the length partition $n = n_1 + n_2 + \cdots + n_\ell$ will not be specified unless necessary.

The next lemma can be proven as [17, Th. 1] using the Smith normal form.

Lemma 2. *For $\mathbf{c} \in S^n$, $R \subseteq S$ and the length partition $n = n_1 + \cdots + n_\ell$,*

$$\mathrm{wt}_{SR}(\mathbf{c}) = \min\{\mathrm{wt}_H(\mathbf{c}\mathrm{Diag}(A_1, A_2, \ldots, A_\ell)) | A_i \in R^{n_i\times n_i} \textit{ invertible}, 1 \leq i \leq \ell\}.$$

Lemma 2 implies the Singleton bound for the sum-rank metric over $R \subseteq S$, which recovers [15, Prop. 34] for R and S fields, and [6, Prop. 3.20] when $\ell = 1$.

Proposition 1 (Singleton bound). *Given an arbitrary code $\mathcal{C} \subseteq S^n$ (linear or not), and setting $k = \log_{|S|} |\mathcal{C}|$, it holds that $\mathrm{d}_{SR}(\mathcal{C}) \leq n - k + 1$.*

We define MSRD codes as follows, which recovers MSRD codes [15, Th. 4] when R and S are fields, MDS codes over finite chain rings when $n_1 = n_2 = \ldots = n_\ell = 1$, and MRD codes over finite chain rings [6, Def. 3.21] when $\ell = 1$.

Definition 3 (MSRD codes). *We say that a code $\mathcal{C} \subseteq S^n$ is a maximum sum-rank distance (MSRD) code over R for the length partition $n = n_1 + n_2 + \cdots + n_\ell$ if $k = \log_{|S|} |\mathcal{C}|$ is a positive integer and $\mathrm{d}_{SR}(\mathcal{C}) = n - k + 1$.*

From Lemma 2, we deduce the following auxiliary lemma, which we will use in Section 5 to prove that linearized Reed-Solomon codes are MSRD.

Lemma 3. *Given an arbitrary code $\mathcal{C} \subseteq S^n$ (linear or not) such that $k = \log_{|S|} |\mathcal{C}|$ is a positive integer, it holds that $\mathcal{C}$ is MSRD for $R \subseteq S$ and the length partition $n = n_1 + n_2 + \cdots + n_\ell$ if, and only if, the code $\mathcal{C}\mathrm{Diag}(A_1, A_2, \ldots, A_\ell)$ is MDS for all invertible matrices $A_i \in R^{n_i \times n_i}$, for $i = 1, 2, \ldots, \ell$.*

4 Skew Polynomials on Finite Chain Rings

The ring of *skew polynomials* [20] over S with morphism σ is the set $S[x; \sigma]$ formed by elements $F = F_0 + F_1 x + F_2 x^2 + \cdots + F_d x^d$, for $F_0, F_1, \ldots, F_d \in S$ and $d \in \mathbb{N}$. If $F_d \neq 0$, we define the *degree* of F as $\deg(F) = d$, and we say that F is *monic* if $F_d = 1$. If $F = 0$, then we define $\deg(F) = -\infty$. Moreover, sums of skew polynomials and products with scalars on the left are defined as in the case of conventional polynomials. However, the product is given by the rules $xa = \sigma(a)x$ and $x^i x^j = x^{i+j}$, for $a \in S$ and $i, j \in \mathbb{N}$.

In order to define linearized Reed-Solomon codes for the extension $R \subseteq S$, we will need the following definitions. We start with the following operators, considered in [10, Def. 3.1] and [11, Eq. (2.7)] for division rings.

Definition 4 ([10, 11]). *Fix $a \in S$ and define the R-linear operator $\mathcal{D}_a^i : S \longrightarrow S$ by $\mathcal{D}_a^i(\beta) = \sigma^i(\beta)\sigma^{i-1}(a)\cdots\sigma(a)a$, for all $\beta \in S$, and all $i \in \mathbb{N}$. Given $F = \sum_{i=0}^d F_i x^i \in S[x; \sigma]$ and $(a, \beta) \in S^2$, where $d \in \mathbb{N}$, we define*

$$F_a(\beta) = \sum_{i=0}^{d} F_i \mathcal{D}_a^i(\beta) \in S.$$

We will also need the concept of *conjugacy* [8, 9].

Definition 5 (Conjugacy [8, 9]). *We say that $a, b \in S$ are conjugate in S with respect to σ if there exists $\beta \in S^*$ such that $b = a^\beta$, where $a^\beta = \sigma(\beta)a\beta^{-1}$.*

The following result follows by combining [8, Th. 23] and [9, Th. 4.5], and was presented in the following form in [12, Th. 2.1] for general division rings.

Lemma 4 ([8, 9]). *If $\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_\ell \in \mathbb{F}_{q^m}^*$ are pairwise non-conjugate (with respect to $\overline{\sigma}$) and $F \in \mathbb{F}_{q^m}[x; \overline{\sigma}]$ is not zero, then*

$$\sum_{i=1}^{\ell} \dim_{\mathbb{F}_q}(\ker(F_{\overline{a}_i})) \leq \deg(F).$$

We now extend this result to the finite chain rings $R \subseteq S$. To this end, we define the *free rank* of an R-module M as the maximum size of an R-linearly independent subset of M. We will denote it by $\mathrm{frk}_R(M)$.

Theorem 1. *Let $a_1, a_2, \ldots, a_\ell \in S^*$ be such that $a_i - a_j^\beta \in S^*$, for all $\beta \in S^*$, and for $1 \leq i < j \leq \ell$. For any non-zero monic $F \in S[x;\sigma]$, we have*

$$\sum_{i=1}^{\ell} \mathrm{frk}_R(F_{a_i}^{-1}(\mathfrak{M})) \leq \deg(F).$$

Proof. If $F = F_0 + F_1 x + \cdots + F_d x^d$, where $F_0, F_1, \ldots, F_d \in S$, denote $\overline{F} = \overline{F}_0 + \overline{F}_1 x + \cdots \overline{F}_d x^d \in \mathbb{F}_{q^m}[x;\overline{\sigma}]$. We have the following two facts:

1) We have that $\mathrm{frk}_R(F_a^{-1}(\mathfrak{M})) \leq \dim_{\mathbb{F}_q}(\ker(\overline{F}_{\overline{a}}))$. We now prove this claim. From Definition 4 and the fact that $\overline{\sigma(a)} = \overline{\sigma}(\overline{a})$, $\overline{F}_{\overline{a}}(\overline{\beta}) = \overline{F_a(\beta)}$, for all $a, \beta \in S$. This means that, if $F_a(\beta) \in \mathfrak{M}$, then $\overline{F}_{\overline{a}}(\overline{\beta}) = \overline{F_a(\beta)} = 0$. Therefore, $\overline{F_a^{-1}(\mathfrak{M})} \subseteq \ker(\overline{F}_{\overline{a}})$. By Item 2 in Lemma 1, $\mathrm{frk}_R(F_a^{-1}(\mathfrak{M})) \leq \dim_{\mathbb{F}_q}(\overline{F_a^{-1}(\mathfrak{M})})$. Thus we conclude that $\mathrm{frk}_R(F_a^{-1}(\mathfrak{M})) \leq \dim_{\mathbb{F}_q}(\overline{F_a^{-1}(\mathfrak{M})}) \leq \dim_{\mathbb{F}_q}(\ker(\overline{F}_{\overline{a}}))$.

2) $\overline{a}_i \neq \overline{a}_j^{\overline{\beta}}$ for $1 \leq i < j \leq \ell$ and $\overline{\beta} \in \mathbb{F}_{q^m}^*$, since $\beta \in S^*$ and $a_i - a_j^\beta \notin \mathfrak{M}$.

By 2), Lemma 4 applies and, using 1) and the fact that F is monic,

$$\sum_{i=1}^{\ell} \mathrm{frk}_R(F_{a_i}^{-1}(\mathfrak{M})) \leq \sum_{i=1}^{\ell} \dim_{\mathbb{F}_q}(\ker(\overline{F}_{\overline{a}_i})) \leq \deg(\overline{F}) = \deg(F). \qquad \square$$

We will also need the following alternative notion of evaluation [8, 9] based on right Euclidean division [20].

Definition 6 ([8, 9]). *Given a skew polynomial $F \in S[x;\sigma]$ and $a \in S$, we define the remainder evaluation of F at a, denoted by $F(a)$, as the only scalar $F(a) \in S$ such that there exist $Q \in S[x;\sigma]$ with $F = Q \cdot (x - a) + F(a)$.*

We also need the following lemma, which is [9, Th. 2.7] and [8, Lemma 1].

Lemma 5. *Let $F, G \in S[x;\sigma]$, $a \in S$ and $\beta \in S^*$.*

1. *If $G(a) = 0$ then $(FG)(a) = 0$. If $\beta = G(a) \in S^*$ then $(FG)(a) = F(a^\beta)G(a)$.*
2. *$F_a(\beta) = F(a^\beta)\beta$.*

We will show that annihilator skew polynomials and Lagrange interpolating skew polynomials exist for sequences of evaluation points as follows.

Definition 7. *Consider vectors $\mathbf{a} = (a_1, a_2, \ldots, a_\ell) \in (S^*)^\ell$ and $\boldsymbol{\beta}_i = (\beta_{i,1}, \beta_{i,2}, \ldots, \beta_{i,n_i}) \in S^{n_i}$, for $i = 1, 2, \ldots, \ell$. Set $\boldsymbol{\beta} = (\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_\ell)$. We say that $(\mathbf{a}, \boldsymbol{\beta})$ satisfies the MSRD property if the following conditions hold:*

1. *$a_i - a_j^\beta \in S^*$, for all $\beta \in S^*$ and for $1 \leq i < j \leq \ell$.*
2. *$\beta_{i,1}, \beta_{i,2}, \ldots, \beta_{i,n_i}$ are linearly independent over R, for $i = 1, 2, \ldots, \ell$ and, by Item 3 in Lemma 1, they lie in S^*.*

The next step is the existence of minimal annihilator skew polynomials.

Theorem 2. *Let $(\mathbf{a}, \boldsymbol{\beta})$ as in Definition 7, satisfying the MSRD property. There are $\gamma_{i,j} \in S^*$ and skew polynomials of degree $\deg(G_{i,j}) = \sum_{u=1}^{i-1} n_u + j$,*

$$G_{i,j} = \left(x - a_i^{\gamma_{i,j}}\right) \cdots \left(x - a_i^{\gamma_{i,1}}\right) \left(x - a_{i-1}^{\gamma_{i-1,n_{i-1}}}\right) \cdots \left(x - a_1^{\gamma_{1,1}}\right), \text{ such that}$$

$$\begin{cases} G_{i,j}(a_u^{\beta_{u,v}}) = 0, & \text{if } 1 \leq u \leq i-1, \text{ or if } u = i \text{ and } 1 \leq v \leq j, \\ G_{i,j}(a_u^{\beta_{u,v}}) \in S^*, & \text{if } i+1 \leq u \leq \ell, \text{ or if } u = i \text{ and } j+1 \leq v \leq n_i, \end{cases}$$

for $j = 1, 2, \ldots, n_i$ and $i = 1, 2, \ldots, \ell$.

Proof. We prove the proposition by induction in the pair (i, j). For the basis step, we only need to define $G_{1,1} = x - a_1^{\beta_{1,1}}$. We have $G_{1,1,a_1}(\beta_{1,1}) = 0$ by Item 2 in Lemma 5. On the other hand, since $\deg(G_{1,1}) = 1$ and it is non-zero and monic, then $G_{1,1,a_u}(\beta_{u,v}) \in S^*$, if $(u, v) \neq (1, 1)$, by Theorem 1.

Now, we have two cases for the inductive step. Either we go from $G_{i,j}$ to $G_{i,j+1}$, if $j < n_i$, or from G_{i,n_i} to $G_{i+1,1}$ if $i < \ell$. The process stops when $i = \ell$ and $j = n_\ell$. We will only develop the first case of induction step.

Assume that $G_{i,j}$ satisfies the proposition and $j < n_i$. In particular, $G_{i,j}(a_i^{\beta_{i,j+1}}) \in S^*$. Define $\gamma_{i,j+1} = G_{i,j}(a_i^{\beta_{i,j+1}})\beta_{i,j+1} \in S^*$ and $G_{i,j+1} = \left(x - a_i^{\gamma_{i,j+1}}\right) G_{i,j}$. By Lemma 5 and the assumptions on $G_{i,j}$, we have $G_{i,j+1}(a_u^{\beta_{u,v}}) = 0$, if $1 \leq u \leq i-1$, or if $u = i$ and $1 \leq v \leq j+1$. Since $G_{i,j+1}$ has such zeros, it is non-zero, monic and of degree $\sum_{u=1}^{i-1} n_u + j + 1$, then we deduce from Theorem 1 that $G_{i,j+1}(a_u^{\beta_{u,v}}) \in S^*$, if $i+1 \leq u \leq \ell$, or if $u = i$ and $j+2 \leq v \leq n_i$. □

We immediately deduce the following two consequences.

Corollary 1. *Let $(\mathbf{a}, \boldsymbol{\beta})$ be as in Definition 7, and satisfying the MSRD property. Then there exists a monic skew polynomial $F \in S[x;\sigma]$ such that $\deg(F) = n_1 + n_2 + \cdots + n_\ell$ and $F_{a_i}(\beta_{i,j}) = 0$, for $j = 1, 2, \ldots, n_i$ and $i = 1, 2, \ldots, \ell$.*

Corollary 2. *Let $(\mathbf{a}, \boldsymbol{\beta})$ be as in Definition 7, and satisfying the MSRD property. For $j = 1, 2, \ldots, n_i$ and $i = 1, 2, \ldots, \ell$, there is a monic skew polynomial $F_{i,j} \in S[x;\sigma]$ such that $\deg(F) = n_1 + n_2 + \cdots + n_\ell - 1$, $F_{i,j,a_i}(\beta_{i,j}) = 1$, and $F_{i,j,a_u}(\beta_{u,v}) = 0$, for all $v = 1, 2, \ldots, n_i$ and $u = 1, 2, \ldots, \ell$ with $u \neq i$ or $v \neq j$.*

We may also obtain the following generalization of [6, Prop. 3.15].

Corollary 3. *Let $a_1, a_2, \ldots, a_\ell \in S$ be such that $a_i - a_j^\beta \in S^*$, for all $\beta \in S^*$ and for $1 \leq i < j \leq \ell$. Let $\mathbf{u}_i \in S^{n_i}$ and let $t_i = \mathrm{rk}(\mathbf{u}_i)$, for $i = 1, 2, \ldots, \ell$. Set $t = t_1 + t_2 + \cdots + t_\ell$. Then there exists a monic skew polynomial $F \in S[x;\sigma]$ such that $\deg(F) = t$ and $F_{a_i}(u_{i,j}) = 0$, for $j = 1, 2, \ldots, n_i$ and for $i = 1, 2, \ldots, \ell$.*

Proof. From the Smith normal form, there are $\boldsymbol{\alpha}_i \in S^{t_i}$ and $B_i \in R^{t_i \times n_i}$ such that $\mathbf{u}_i = \boldsymbol{\alpha}_i B_i$, $\mathrm{frk}(\boldsymbol{\alpha}_i) = t_i$ and $\mathrm{rk}(B_i) = t_i$, for $i = 1, 2, \ldots, \ell$. In particular, $(\mathbf{a}, \boldsymbol{\alpha})$ satisfies the MSRD property (Definition 7), where $\mathbf{a} = (a_1, a_2, \ldots, a_\ell)$

and $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_\ell)$. By Corollary 1, there exists a monic skew polynomial $F \in S[x;\sigma]$ such that $\deg(F) = t$ and $F_{a_i}(\alpha_{i,j}) = 0$, for $j = 1, 2, \ldots, t_i$ and for $i = 1, 2, \ldots, \ell$. Since the map F_{a_i} is R-linear and $\mathbf{u}_i = \boldsymbol{\alpha}_i B_i$, we deduce that $F_{a_i}(u_{i,j}) = 0$, for $j = 1, 2, \ldots, n_i$ and for $i = 1, 2, \ldots, \ell$, and we are done. □

We now extend the matrices from [15, p. 604] to finite chain rings.

Definition 8. *Consider vectors* $\mathbf{a} = (a_1, a_2, \ldots, a_\ell) \in S^\ell$ *and* $\boldsymbol{\beta}_i = (\beta_{i,1}, \beta_{i,2}, \ldots, \beta_{i,n_i}) \in S^{n_i}$, *for* $i = 1, 2, \ldots, \ell$. *Set* $\boldsymbol{\beta} = (\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_\ell)$ *and* $n = n_1 + n_2 + \cdots + n_\ell$. *For* $k = 1, 2, \ldots, n$, *we define the extended Moore matrix*

$$M_k(\mathbf{a}, \boldsymbol{\beta}) = \left(\begin{array}{ccc|c|ccc} \beta_{1,1} & \ldots & \beta_{1,n_1} & \ldots & \beta_{\ell,1} & \ldots & \beta_{\ell,n_\ell} \\ \mathcal{D}_{a_1}(\beta_{1,1}) & \ldots & \mathcal{D}_{a_1}(\beta_{1,n_1}) & \ldots & \mathcal{D}_{a_\ell}(\beta_{\ell,1}) & \ldots & \mathcal{D}_{a_\ell}(\beta_{\ell,n_\ell}) \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \mathcal{D}_{a_1}^{k-1}(\beta_{1,1}) & \ldots & \mathcal{D}_{a_1}^{k-1}(\beta_{1,n_1}) & \ldots & \mathcal{D}_{a_\ell}^{k-1}(\beta_{\ell,1}) & \ldots & \mathcal{D}_{a_\ell}^{k-1}(\beta_{\ell,n_\ell}) \end{array} \right).$$

The following result follows from Corollary 2 as in the classical case.

Theorem 3. *Let* $(\mathbf{a}, \boldsymbol{\beta})$ *as in Definition 7, satisfying the MSRD property. Let* $n = n_1 + \cdots + n_\ell$. *Then* $M_n(\mathbf{a}, \boldsymbol{\beta})$ *is invertible. In particular, given* $c_{i,j} \in S$, *for* $j = 1, 2, \ldots, n_i$ *and* $i = 1, 2, \ldots, \ell$, *there exists a unique* $F \in S[x;\sigma]$ *such that* $\deg(F) \leq n - 1$, *and* $F_{a_i}(\beta_{i,j}) = c_{i,j}$, *for* $j = 1, 2, \ldots, n_i$ *and* $i = 1, 2, \ldots, \ell$.

5 Linearized Reed-Solomon Codes

In this section, we extend linearized Reed-Solomon codes [15] to finite chain rings, providing the first construction of MSRD codes over finite chain rings.

The following definition is [15, Def. 31] when R and S are fields. Over finite chain rings, it coincides with Gabidulin codes [6, Def. 3.22] when $\ell = 1$ and generalized Reed-Solomon codes [21, Def. 22] when $m = n_1 = \ldots = n_\ell = 1$.

Definition 9. *Let* $(\mathbf{a}, \boldsymbol{\beta})$ *as in Definition 7, satisfying the MSRD property. For* $k = 1, 2, \ldots, n$, *we define the* k*-dimensional linearized Reed-Solomon code as the linear code* $\mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta}) \subseteq S^n$ *with generator matrix* $M_k(\mathbf{a}, \boldsymbol{\beta})$ *(Definition 8).*

The main result of this section is the following. It coincides with [15, Th. 4] when R and S are fields, with [6, Th. 3.24] over finite chain rings when $\ell = 1$, and with [21, Prop. 23 & Cor. 24] over finite chain rings when $m = n_1 = \ldots = n_\ell = 1$.

Theorem 4. *Let* $(\mathbf{a}, \boldsymbol{\beta})$ *as in Definition 7, satisfying the MSRD property. For* $k = 1, 2, \ldots, n$, *the code* $\mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta}) \subseteq S^n$ *is a free* S*-module of rank* k *and an MSRD code over* R *for the length partition* $n = n_1 + \cdots + n_\ell$.

Proof. Let $A_i \in R^{n_i \times n_i}$ be invertible, for $i = 1, 2, \ldots, \ell$. By the R-linearity of σ, we have that $\mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta})\mathrm{Diag}(A_1, A_2, \ldots, A_\ell) = \mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta}\mathrm{Diag}(A_1, A_2, \ldots, A_\ell))$, which is also a linearized Reed-Solomon code, since $(\mathbf{a}, \boldsymbol{\beta}\mathrm{Diag}(A_1, A_2, \ldots, A_\ell))$ also satisfies the MSRD property since $A_1, A_2, \ldots, A_\ell$ are invertible. Therefore, from Lemma 3, we see that we only need to prove that $\mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta})$ is MDS and a free S-module of rank k. Both properties follow from the fact that any $k \times k$ square submatrix of $M_k(\mathbf{a}, \boldsymbol{\beta})$ is invertible by Theorem 3. □

Finally, we show how to explicitly construct sequences $(\mathbf{a}, \boldsymbol{\beta})$ satisfying the MSRD property. In this way, we have explicitly constructed linearized Reed-Solomon codes for the finite chain ring extension $R \subseteq S$. The R-linearly independent elements $\beta_{i,1}, \beta_{i,2}, \ldots, \beta_{i,n_i} \in S^*$ can be chosen as subsets of any basis of S over R, for $i = 1, 2, \ldots, \ell$. We now show how to choose $a_1, a_2, \ldots, a_\ell \in S$.

Proposition 2. *Let $1 \leq \ell \leq q-1$ and let $\gamma \in \mathbb{F}_{q^m}^*$ be a primitive element, that is, $\mathbb{F}_{q^m}^* = \{\gamma^0, \gamma^1, \ldots, \gamma^{q^m-2}\}$. Such an element always exists [13, Th. 2.8]. Take $a_1, a_2, \ldots, a_\ell \in S^*$ such that $\overline{a}_i = \gamma^{i-1}$, for $i = 1, 2, \ldots, \ell$. Then $a_1, a_2, \ldots, a_\ell \in S^*$ are such that $a_i - a_j^\beta \in S^*$, for all $\beta \in S^*$ and all $1 \leq i < j \leq \ell$.*

In particular, we have shown the existence of linear MSRD codes of any rank for the extension $R \subseteq S$ for the following parameters.

Corollary 4. *Let $1 \leq \ell \leq q-1$, $1 \leq n_i \leq m$ for $i = 1, 2, \ldots, \ell$, $1 \leq k \leq n$, and $n = n_1 + \cdots + n_\ell$. Then there exists a code $\mathcal{C} \subseteq S^n$ that is a free S-module of rank k and is MSRD over R for the length partition $n = n_1 + \cdots + n_\ell$.*

6 A Welch-Berlekamp Decoder

In this section, we present a cubic-complexity Welch-Berlekamp sum-rank error-correcting algorithm for the linearized Reed-Solomon codes from Definition 9. The decoder is based on the original one by Welch and Berlekamp [2]. Welch-Berlekamp decoders for the sum-rank metric in the case of fields were given in [3, 16, 1], listed in decreasing order of computational complexity.

Fix $(\mathbf{a}, \boldsymbol{\beta})$ as in Definition 7, satisfying the MSRD property. We will set $b_{i,j} = \sigma(\beta_{i,j}) a_i \beta_{i,j}^{-1}$, for $j = 1, 2, \ldots, n_i$ and for $i = 1, 2, \ldots, \ell$. Next fix a dimension k with $1 \leq k \leq n-1$, and consider the linearized Reed–Solomon code $\mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta}) \subseteq S^n$ (Definition 9). The number of sum-rank errors that it can correct is

$$t = \left\lfloor \frac{\mathrm{d}_{SR}(\mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta})) - 1}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor. \tag{2}$$

Let $\mathbf{c} \in \mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta})$ be any *codeword*, let $\mathbf{e} \in S^n$ be an *error vector* such that $\mathrm{wt}_{SR}(\mathbf{e}) \leq t$, and define the *received word* as

$$\mathbf{r} = \mathbf{c} + \mathbf{e} \in S^n. \tag{3}$$

Since $\mathrm{wt}_{SR}(\mathbf{e}) \leq t$ and $2t + 1 \leq \mathrm{d}_{SR}(\mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta}))$, there is a unique solution $\mathbf{c} \in \mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta})$ to the decoding problem. Define the auxiliary vectors $\mathbf{c}' = \mathbf{c} \cdot \mathrm{Diag}(\boldsymbol{\beta})^{-1}$, $\mathbf{e}' = \mathbf{e} \cdot \mathrm{Diag}(\boldsymbol{\beta})^{-1}$, and $\mathbf{r}' = \mathbf{r} \cdot \mathrm{Diag}(\boldsymbol{\beta})^{-1}$. By Lagrange interpolation (Theorem 3) and Lemma 5, there exist unique $F, G, R \in S[x; \sigma]$, all of degree less than n, such that $F(\mathbf{b}) = \mathbf{c}'$, $G(\mathbf{b}) = \mathbf{e}'$, and $R(\mathbf{b}) = \mathbf{r}'$, which denote componentwise remainder evaluation (Definition 6). Moreover, since $\mathbf{c} \in \mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta})$, then $\deg(F) < k$. Following the original Welch–Berlekamp decoder, we want to find a non-zero monic skew polynomial $L \in S[x; \sigma]$ with $\deg(L) \leq t$ and such that

$$(LR)(\mathbf{b}) = (LF)(\mathbf{b}). \tag{4}$$

However, since we do not know F, we look instead for non-zero $L, Q \in S[x;\sigma]$ such that L is monic, $\deg(L) \leq t$, $\deg(Q) \leq t+k-1$ and

$$(LR)(\mathbf{b}) = Q(\mathbf{b}). \tag{5}$$

In the following two lemmas, we show that (4) and (5) can be solved, and once L and Q are obtained, F may be obtained by left Euclidean division.

Lemma 6. *There exists a non-zero monic skew polynomial $L \in S[x;\sigma]$ with $\deg(L) \leq t$ satisfying (4). In particular, there exist non-zero $L, Q \in S[x;\sigma]$ such that L is monic, $\deg(L) \leq t$, $\deg(Q) \leq t+k-1$ and (5) holds.*

Proof. By Corollary 3, there exists a non-zero monic skew polynomial $L \in S[x;\sigma]$ such that $\deg(L) \leq t$ and $L_{a_i}(e_{i,j}) = 0$, for $j = 1, 2, \ldots, n_i$ and for $i = 1, 2, \ldots, \ell$. The reader may verify from the definitions and Lemma 5 that

$$(LG)(b_{i,j}) = L_{b_{i,j}}(G(b_{i,j})) = L_{b_{i,j}}(e'_{i,j}) = L_{a_i}(e_{i,j}) = 0,$$

for $j = 1, 2, \ldots, n_i$ and for $i = 1, 2, \ldots, \ell$. Since $R(\mathbf{b}) = F(\mathbf{b}) + G(\mathbf{b})$, we conclude that $(L(R-F))(\mathbf{b}) = (LG)(\mathbf{b}) = 0$ by Lemma 5. In other words, L satisfies (4). □

Lemma 7. *If $L, Q \in S[x;\sigma]$ are such that L is monic, $\deg(L) \leq t$, $\deg(Q) \leq t+k-1$ and (5) holds, then $Q = LF$.*

Proof. First, by (5) and the product rule (Item 1 in Lemma 5), if $(F-R)(b_{i,j}) = 0$, then $(LF-Q)(b_{i,j}) = 0$, for $j = 1, 2, \ldots, n_i$ and for $i = 1, 2, \ldots, \ell$. From this fact, and using Lemmas 2 and 5, the reader may deduce that

$$\mathrm{wt}_{SR}\left((LF-Q)(\mathbf{b}) \cdot \mathrm{Diag}(\boldsymbol{\beta})\right) \leq \mathrm{wt}_{SR}\left((F-R)(\mathbf{b}) \cdot \mathrm{Diag}(\boldsymbol{\beta})\right) \leq t.$$

Therefore, we may apply Lemma 6 to LF and Q, instead of F and R. Thus there exists a non-zero monic $L_0 \in S[x;\sigma]$ such that $\deg(L_0) \leq t$ and $(L_0(LF-Q))(\mathbf{b}) = \mathbf{0}$. Now observe that $\deg\left(L_0(LF-Q)\right) \leq 2t+k-1 < n$. By Lemma 5 and Theorem 3, we conclude that $L_0(LF-Q) = 0$. Since L_0 is non-zero and monic, we conclude that $LF = Q$ and we are done. □

Finally, once we find non-zero $L, Q \in S[x;\sigma]$ such that L is monic, $\deg(L) \leq t$, $\deg(Q) \leq t+k-1$ and (5) holds, then we may find F by left Euclidean division, since $Q = LF$ by Lemma 7 above. Left Euclidean division is possible in $S[x;\sigma]$ since σ is invertible. Finding L and Q using R and $\mathbf{b}$ (which are known) amounts to solving a system of linear equations derived from (5) using the Smith normal form, as in [6, Sec. III-D]. Using this method, the decoding algorithm has an overall complexity of $\mathcal{O}(n^3)$ operations over the ring S.

References

1. Bartz, H., Jerkovits, T., Puchinger, S., Rosenkilde, J.: Fast decoding of codes in the rank, subspace, and sum-rank metric. IEEE Trans. Info. Theory **67**(8), 5026–5050 (2021)

2. Berlekamp, E.R., Welch, L.: Error correction of algebraic block codes (1986), u.S. Patent No. 4,633,470
3. Boucher, D.: An algorithm for decoding skew Reed–Solomon codes with respect to the skew metric. Des., Codes, Crypto. **88**, 1991–2005 (2020)
4. Feng, C., Silva, D., Kschischang, F.R.: An algebraic approach to physical-layer network coding. IEEE Trans. Info. Theory **59**(11), 7576–7596 (2013)
5. Gabidulin, E.M.: Theory of codes with maximum rank distance. Problems Inform. Transmission **21**(1), 1–12 (1985)
6. Kamche, H.T., Mouaha, C.: Rank-metric codes over finite principal ideal rings and applications. IEEE Trans. Info. Theory **65**(12), 7718–7735 (2019)
7. Kiran, T., Rajan, B.: Optimal STBCs from codes over Galois rings. In: IEEE International Conference on Personal Wireless Communications. pp. 120–124 (2005)
8. Lam, T.Y.: A general theory of Vandermonde matrices. Expositiones Mathematicae **4**, 193–215 (1986)
9. Lam, T.Y., Leroy, A.: Vandermonde and Wronskian matrices over division rings. J. Algebra **119**(2), 308–336 (1988)
10. Lam, T.Y., Leroy, A.: Hilbert 90 theorems over divison rings. Transactions of the American Mathematical Society **345**(2), 595–622 (1994)
11. Leroy, A.: Pseudolinear transformations and evaluation in Ore extensions. Bulletin of the Belgian Mathematical Society **2**(3), 321–347 (1995)
12. Leroy, A.: Noncommutative polynomial maps. Journal of Algebra and its Applications **11**(04), 1250076 (2012)
13. Lidl, R., Niederreiter, H.: Finite Fields, Encyclopedia of Mathematics and its Applications, vol. 20. Addison-Wesley, Amsterdam (1983)
14. Lu, H.F., Kumar, P.V.: A unified construction of space-time codes with optimal rate-diversity tradeoff. IEEE Trans. Info. Theory **51**(5), 1709–1730 (May 2005)
15. Martínez-Peñas, U.: Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring. J. Algebra **504**, 587–612 (2018)
16. Martínez-Peñas, U., Kschischang, F.R.: Reliable and secure multishot network coding using linearized reed-solomon codes. IEEE Trans. Info. Theory **65**(8), 4785–4803 (2019)
17. Martínez-Peñas, U., Kschischang, F.R.: Universal and dynamic locally repairable codes with maximal recoverability via sum-rank codes. IEEE Trans. Info. Theory **65**(12), 7790–7805 (2019)
18. McDonald, B.: Finite rings with identity, vol. 28. Marcel Dekker Inc. (1974)
19. Nóbrega, R.W., Uchôa-Filho, B.F.: Multishot codes for network coding using rank-metric codes. In: Proc. 2010 Third IEEE Int. Workshop on Wireless Network Coding. pp. 1–6 (2010)
20. Ore, O.: Theory of non-commutative polynomials. Annals of Mathematics (2) **34**(3), 480–508 (1933)
21. Quintin, G., Barbier, M., Chabot, C.: On generalized Reed–Solomon codes over commutative and noncommutative rings. IEEE Trans. Info. Theory **59**(9), 5882–5897 (2013)
22. Reed, I.S., Solomon, G.: Polynomial codes over certain finite fields. J. Soc. Ind. and Appl. Math. **8**(2), 300–304 (1960)
23. Shehadeh, M., Kschischang, F.R.: Rate-diversity optimal multiblock space-time codes via sum-rank codes. In: Proc. IEEE Int. Symp. Info. Theory. pp. 3055–3060 (2020)