Roos bound for skew cyclic codes in Hamming and rank metric

Alfarano, Gianira Nicoletta ; Lobillo, F J ; Neri, Alessandro

DOI: https://doi.org/10.1016/j.ffa.2020.101772

Finite Fields and Their Applications 69 (2021) 101772

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Roos bound for skew cyclic codes in Hamming and rank metric ☆

Gianira N. Alfarano [a,*], F.J. Lobillo [b], Alessandro Neri [c]

[a] *University of Zurich, Switzerland*
[b] *University of Granada, Spain*
[c] *Technical University of Munich, Germany*

ARTICLE INFO

Article history:
Received 6 February 2020
Received in revised form 11 August 2020
Accepted 9 October 2020
Available online 22 October 2020
Communicated by W. Cary Huffman

MSC:
11T71
94B65
16S36

Keywords:
Cyclic codes
Skew cyclic codes
Roos bound
Rank-metric codes
MRD codes

ABSTRACT

In this paper, a Roos like bound on the minimum distance for skew cyclic codes over a general field is provided. The result holds in the Hamming metric and in the rank metric. The proofs involve arithmetic properties of skew polynomials and an analysis of the rank of parity-check matrices. For the rank metric case, a way to arithmetically construct codes with a prescribed minimum rank distance, using the skew Roos bound, is also given. Moreover, some examples of MDS codes and MRD codes over finite fields are built, using the skew Roos bound.

☆ Research partially supported by grant PID2019-110525GB-I00 from Agencia Estatal de Investigación (AEI) and from Fondo Europeo de Desarrollo Regional (FEDER), and from Swiss National Science Foundation through grants no. 187711 and 188430.

* Corresponding author.
E-mail addresses: gianiranicoletta.alfarano@math.uzh.ch (G.N. Alfarano), jlobillo@ugr.es (F.J. Lobillo), alessandro.neri@tum.de (A. Neri).

https://doi.org/10.1016/j.ffa.2020.101772

1. Introduction

In the theory of error correcting codes, a crucial step was represented by the introduction of algebraic structures, which led to the branch called *algebraic coding theory*. More specifically, the basic idea that initiated the study of *linear codes* was to take a finite field F as alphabet, and then use the vector space structure F^n when dealing with codes and their codewords. Among the linear codes, one of the most studied families is the one of *cyclic codes*. Their importance is given by the ring structure underlying their polynomial representation. Formally, a cyclic block code $\mathcal{C}$ over F is defined as an ideal of $F[x]/(x^n - 1)$. It is well-known that the minimum Hamming distance of a cyclic code is lower bounded by the BCH bound, see [5,4,31]. Concretely, let $g(x)$ be the generator polynomial of $\mathcal{C}$, ω be a primitive n-th root of unity and b, δ be positive integers. If $g(\omega^{b+i}) = 0$ for $0 \leq i \leq \delta - 2$, i.e. g has $\delta - 1$ consecutive roots in an extension field of F, then the minimum Hamming distance of $\mathcal{C}$ is at least δ. The cyclicity property was further investigated in order to construct codes with prescribed Hamming distance. At a second step, Hartmann and Tzeng generalized the BCH bound deriving the well-known Hartmann-Tzeng (HT) bound [30]. Afterwards, Roos derived further generalizations which were shown to improve both the BCH and the HT bounds [45,44]. More precisely, the *Roos bound* that we will consider in this work states the following: if there are $b, s, \delta, k_0, \ldots, k_r \in \mathbb{N}$, such that $(s, n) = 1$, $k_{j-1} < k_j$ for $1 \leq j \leq r$ and $k_r - k_0 \leq \delta + r - 2$, and $g(\omega^{b+si+k_j}) = 0$, for $0 \leq i \leq \delta - 2$, $0 \leq j \leq r$, then the minimum Hamming distance of the cyclic code $\mathcal{C}$ generated by $g(x)$ is at least $\delta + r$.

Skew polynomial rings were introduced in 1930 by Ore in his seminal paper [41] and then they have been further studied by several authors, see for instance [34,35,37]. The research on linear codes in this setting led to new codes with better parameters than the old known linear codes. In 2007, Boucher, Geiselmann and Ulmer [7] extended the definition of cyclicity to codes defined over the skew polynomial ring (see also [8,9,14]). In these works, the authors derived bounds on the Hamming distance of skew cyclic codes, generalizing in some sense the BCH bound to skew cyclic codes. In [28], the authors gave a version of the Hartmann-Tzeng bound for skew cyclic codes and provided a construction of these codes with prescribed designed Hamming distance.

Skew polynomial rings played a crucial role also in the construction of codes endowed with the rank metric. These codes were first introduced independently by Delsarte [17], Gabidulin [20] and Roth [46], and have been shown to have many applications, such as network coding [49,48,18], distributed data storage [43,12,40] and post-quantum cryptography [21,42,22]. One of the most important constructions of rank-metric codes makes use of the ring of linearized polynomials. More specifically, these codes are known as *Gabidulin codes* and they are obtained by evaluating a particular set of linearized polynomials in a suitable set of points (see [17,20]). The connection with skew polynomials is due to the fact that there is a natural isomorphism between the ring of linearized polynomials over a finite field and the ring of skew polynomials. Generalizations of this construction were provided in [14], where a rank-metric version of the BCH bound was

proposed. Moreover the analogue of the Hartmann-Tzeng bound for skew-cyclic codes over finite field with respect to the rank metric was shown in [39].

In this paper we provide a generalization of the Roos bound for skew cyclic codes in the Hamming metric and in the rank metric. Our results generalize previous bounds on the minimum distance of skew cyclic codes in the Hamming metric [8,14,28], and in the rank metric [17,21,46,14,2,39]. However, our setting only requires a cyclic Galois extension of finite degree, without restricting to the case of finite fields.

The paper is structured as follows. In Section 2 we recall the basics of skew polynomial rings and the notion of skew cyclic codes, focusing on the family of skew Reed-Solomon codes. Section 3 is dedicated to the rank metric. We define the rank metric in the most general setting and describe the construction of Gabidulin codes over any cyclic Galois extension. In Section 4 we fix the mathematical setting for the whole paper, focusing on the defining sets for skew cyclic codes, and we prove the results that are crucial for the main proofs. Section 5 is devoted to the proof of the skew version of the Roos bound for the Hamming metric. We use the bound to construct some examples of (MDS) codes over finite fields. In Section 6 we provide the skew version of the Roos bound for the rank metric. We compare the construction of the codes in the Hamming metric with the one in the rank metric, which led to an interesting result, explaining that it could be possible to construct skew cyclic MRD codes, using the arithmetic properties of the defining sets. We conclude with some remarks and an open problem in Section 7.

2. Skew cyclic codes and skew Reed-Solomon codes

In this section we recall some basic notions on skew polynomial rings and skew cyclic codes. The interested reader is referred to the recent survey of Gluesing-Luerssen [23].

We will use the notation introduced in [28, §2] to recall the definition of skew cyclic codes and some important known results. Let F/K be a field extension of finite degree μ. We assume F/K is cyclic, i.e. its Galois group, $\mathrm{Gal}(F/K)$, is cyclic. Fix a generator σ of $\mathrm{Gal}(F/K)$, hence its order $|\sigma|$ is μ and $K = F^\sigma$ is its invariant subfield. Let $R = F[x;\sigma]$ be the skew polynomial ring induced by σ over F and n be a multiple of μ, namely $n = \nu\mu$ for some ν positive integer. Recall that the multiplication rule over the skew polynomial ring R is given by

$$xa = \sigma(a)x \text{ for all } a \in F.$$

In order to define skew cyclic codes over F it is enough to replace $F[x]/(x^n - 1)$ by $\mathcal{R} := R/R(x^n - 1)$, where $Rf(x)$ denotes the left ideal generated by the polynomial $f(x)$. Since σ has finite order μ, the center $Z(R)$ of R is given by the commutative polynomial ring $K[x^\mu]$, which follows directly from [32, Theorem 1.1.22]. Therefore, $x^n - 1$ belongs to $Z(R)$. Hence, $R(x^n - 1)$ is a twosided ideal and the quotient $\mathcal{R}$ is a K-algebra. The elements of $\mathcal{R}$ can be uniquely represented by polynomials of degree less than n and coefficients in F, hence there is a canonical isomorphism

$$\begin{aligned} F^n &\to \mathcal{R} \\ (a_0, \dots, a_{n-1}) &\mapsto a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \end{aligned} \tag{1}$$

of F-vector spaces, where the F-action on $\mathcal{R}$ is given by left multiplication.

An $[n,k]$-*linear code* $\mathcal{C}$ over F is defined as a subspace of F^n of dimension k. Hence, thanks to the above isomorphism, we can identify linear codes in F^n as vector subspaces of $\mathcal{R}$. We define the *Hamming distance* between two vectors in F^n as the number of components in which they differ. The *minimum (Hamming) distance* of a linear code $\mathcal{C}$ is defined as the minimum over all the distances between two distinct codewords in $\mathcal{C}$ and we denote it by $\mathrm{d}_H(\mathcal{C})$. Equivalently, $\mathrm{d}_H(\mathcal{C})$ is given by the minimum (Hamming) weight of the nonzero codewords in $\mathcal{C}$, where the *Hamming weight* of a vector $v \in F^n$ is defined as the number of its nonzero components and we denote it by $\mathrm{w}(v)$. When the minimum distance $d = \mathrm{d}_H(\mathcal{C})$ is known, we write that $\mathcal{C}$ is an $[n,k,d]$-linear code. The parameters n, k and d of a linear code $\mathcal{C}$ satisfy the following inequality, known as the Singleton bound [50]: $d \leq n - k + 1$. When the minimum distance of $\mathcal{C}$ reaches the bound, $\mathcal{C}$ is called *maximum distance separable (MDS) code*.

In the setting defined above, an $[n,k]$-linear code $\mathcal{C} \subseteq F^n$ is called *skew cyclic* if its image under the canonical isomorphism (1) is a left ideal of $\mathcal{R}$. We identify $\mathcal{C}$ without further mention with its image under the canonical isomorphism, hence we say that a skew cyclic code is a left ideal of $\mathcal{R}$.

As in the classical commutative case, the rich arithmetic structure of $R = F[x;\sigma]$ is the main tool which allows its use in different applications, including skew cyclic codes. This arithmetic structure has been studied by a lot of authors starting with the seminal paper [41]. In R, there is left (and right) Euclidean division, hence it is a left (and right) Euclidean domain. As a consequence, given $f, g \in R$ there exists the greatest common right divisor and least common left multiple of them and can be computed with the corresponding version of the extended Euclidean algorithm. We denote the least common left multiple of two polynomials $f, g \in R$ by $[f,g]_\ell$. A detailed computational treatment of skew polynomials, including left division and extended Euclidean algorithm can be found in [11, Sections 1.3 and 1.4].

Being R a left Euclidean domain, it is also a left PID, hence every left ideal of $\mathcal{R}$ is principal. In fact, by using the right greatest common right divisor, it is easy to prove that for each skew cyclic code $\mathcal{C}$, there exists a polynomial $g \in R$ which is a right divisor of $x^n - 1$, namely $g \mid_r x^n - 1$, such that $\deg(g) = n - k$ and g generates $\mathcal{C}$ as left ideal, i.e. $\mathcal{C} = \mathcal{R}g$.

Evaluation in skew polynomials makes use of truncated norms. For any $i \in \mathbb{N}_0$, the i-*th truncated norm on* F is defined as $N_i : F \to F$, with $N_0(a) = 1$ and $N_i(a) = \prod_{j=0}^{i-1} \sigma^j(a)$ for $i > 0$, for any $a \in F$. This is a special case of [35, (2.3)], where a deep discussion of evaluations can be found. Note that $N_1(a) = a$ and $N_{i+1}(a) = N_i(a)\sigma^i(a)$ for any $i > 0$. If $f(x) = \sum_{i=0}^{r} f_i x^i \in R$, it follows that the left division of $f(x)$ by $x - a$ is

$$f(x) = q(x)(x - a) + \sum_{i=0}^{r} f_i N_i(a)$$

as proved in [35, Lemma 2.4], hence $f(a) = \sum_{i=0}^{r} f_i N_i(a)$ is the correct notion of evaluation of skew polynomials.

The structure of a skew cyclic code is better understood if a full decomposition of its generator polynomial g as least common left multiple of linear polynomials can be provided. Let E/K be a cyclic field extension of degree n and $\theta \in \mathrm{Gal}(E/K)$ an automorphism of degree n, i.e. $K = E^{\theta}$. Let $S = E[x;\theta]$ and $\mathcal{S} := S/S(x^n - 1)$. Recall that $\mathcal{S} \cong K^{n\times n}$ is simple Artinian, see for instance [25, Theorem 1]. Hence all simple modules are isomorphic and given $g \in S$ of degree $n-k$ with $g \mid_r x^n - 1$, there exist $\beta_0, \beta_1, \ldots, \beta_{n-k-1} \in E$ such that g is the least common left multiple of $\{x - \beta_i \mid 0 \leq i \leq n-k-1\}$, that is

$$g = [x - \beta_0, \ldots, x - \beta_{n-k-1}]_{\ell}\,.$$

Recall that $x - \beta \mid_r x^n - 1$ if and only if $N_n(\beta) = 1$, and by Hilbert's Theorem 90 (see e.g. [36, Chapter VI, Theorem 6.1]) this happens if and only if $\beta = \theta(\alpha)\alpha^{-1}$ for some $\alpha \in E$. Hence, $\beta_i = \theta(\alpha_i)\alpha_i^{-1}$ for K-linear independent $\alpha_0, \ldots, \alpha_{n-k-1} \in E$, see [16, Theorem 5.3]. When these linear independent elements are part of a normal basis, a better knowledge of the parameters of the code is obtained. Concretely, we have the following result, that was first proved for the finite field case in [14, Proposition 1].

Proposition 1 *([27, Theorem 3.4]). Let $\alpha \in E$ such that $\{\alpha, \theta(\alpha), \ldots, \theta^{n-1}(\alpha)\}$ is a normal basis and $\beta = \theta(\alpha)\alpha^{-1}$. Let $1 \leq \delta \leq n$ and $g = \left[\{x - \theta^i(\beta) \mid 0 \leq i \leq \delta - 2\}\right]_{\ell}$. Then $\mathcal{S}g \subseteq \mathcal{S}$ is an MDS code of length n and minimum Hamming distance δ.*

These codes are usually called *skew Reed-Solomon codes* (see e.g. [38]), and denoted by

$$\mathrm{sRS}_{\beta}^{\theta}(n,\delta) = \mathcal{S}\left[\{x - \theta^i(\beta) \mid 0 \leq i \leq \delta - 2\}\right]_{\ell}\,.$$

Skew Reed-Solomon codes can be efficiently decoded. For instance, a skew version of the Peterson-Gorenstein-Zierler algorithm can be found in [24, Algorithm 1] for general Galois cyclic extensions of fields. There are also decoding algorithms for skew Reed-Solomon codes which are based on the skew version of the extended Euclidean algorithm. For finite fields, you can see [14, §5], and for rational functions over finite fields we refer to [26, Algorithm 1]. In fact, this last algorithm works for general Galois cyclic extensions, although it was presented for rational functions over finite fields. The same can be said of [26, Theorem 4], which is a version of Proposition 1 for the field of rational functions over finite field, but whose proof works over general Galois cyclic extensions.

The proof of Proposition 1 is based on the Circulant Lemma, which is a particular case of [35, Corollary 4.13]. We include the statement since it is going to be used to prove the main results of this paper.

Lemma 2 *(Circulant Lemma). Let $\{\alpha_0, \dots, \alpha_{n-1}\}$ be a K–basis of E. Then, for every positive integer $t \leq n$ and every subset $\{k_1, k_2, \dots, k_t\} \subseteq \{0, 1, \dots, n-1\}$,*

$$\begin{vmatrix} \alpha_{k_1} & \theta(\alpha_{k_1}) & \dots & \theta^{t-1}(\alpha_{k_1}) \\ \alpha_{k_2} & \theta(\alpha_{k_2}) & \dots & \theta^{t-1}(\alpha_{k_2}) \\ \vdots & \vdots & & \vdots \\ \alpha_{k_t} & \theta(\alpha_{k_t}) & \dots & \theta^{t-1}(\alpha_{k_t}) \end{vmatrix} \neq 0.$$

An elementary proof is available in [26].

3. Rank metric over any field extension

Although we will always consider cyclic extensions, here we discuss the rank metric in the most general case, in the spirit of the recent works of Augot, Loidreau and Robert [2,1,3]. A similar approach was first investigated by Roth in [47, Section 6].

Let K be a field and E be an extension field of degree n. Let $\theta \in \mathrm{Gal}(E/K)$ with order $|\theta| = \eta$, so η divides n. Let moreover $\mathcal{B} = \{b_1, \dots, b_n\}$ be an ordered K-basis of E. For a given vector $v = (v_1, \dots, v_N) \in E^N$, we consider the following two matrices:

$$M_{v,\theta} := \begin{pmatrix} v_1 & v_2 & \cdots & v_N \\ \theta(v_1) & \theta(v_2) & \cdots & \theta(v_N) \\ \vdots & \vdots & & \vdots \\ \theta^{\eta-1}(v_1) & \theta^{\eta-1}(v_2) & \cdots & \theta^{\eta-1}(v_N) \end{pmatrix},$$

$$M_{v,\mathcal{B}} := \begin{pmatrix} x_{1,1} & x_{2,1} & \cdots & x_{N,1} \\ x_{1,2} & x_{2,2} & \cdots & x_{N,2} \\ \vdots & \vdots & & \vdots \\ x_{1,n} & x_{2,n} & \cdots & x_{N,n} \end{pmatrix},$$

where $v_i = \sum_{j=1}^{n} x_{i,j} b_j$, for every $i = 1, \dots, N$.

Augot, Loidreau and Robert defined in [2] two different rank weights for a vector $v \in E^N$ as follows. Let E, K and θ be as above, and let $v \in E^N$. The quantities $\mathrm{w}_K(v)$ and $\mathrm{w}_E(v)$ are defined as

$$\begin{aligned} \mathrm{w}_K(v) &:= \mathrm{rk}_K(M_{v,\theta}) = \mathrm{rk}_K(M_{v,\mathcal{B}}), \\ \mathrm{w}_E(v) &:= \mathrm{rk}_E(M_{v,\theta}) = \deg(p_v), \end{aligned}$$

where $p_v = [x - v_1, \dots, x - v_N]_\ell \in E[x; \theta]$. It was shown by the same authors that these quantities are all equal in the following special case.

Proposition 3. *[2, Proposition 5] If $K = E^\theta$, then $\mathrm{w}_E(v) = \mathrm{w}_K(v)$, and they are both equal to*

$$\mathrm{w}_R(v) := \dim_K \langle v_1, \dots, v_N \rangle_K.$$

For the rest of this section we will only deal with the case $E^\theta = K$, i.e. $\mathrm{Gal}(E/K)$ is cyclic and the order of θ is n, therefore we will use the notation $\mathrm{w}_R(v)$ to denote the *rank weight* of a vector with respect to the cyclic extension E/K.

Definition 4. Let E/K be a cyclic field extension of finite degree, then the *rank distance* of two vectors $u, v \in E^N$ with respect to the extension E/K is defined as $\mathrm{d}_R(u,v) := \mathrm{w}_R(u-v)$.

With this metric, we can introduce the notion of rank-metric codes.

Definition 5. Let E/K be a cyclic finite extension field and let N, k, d be positive integers. An $[N,k,d]_{E/K}$ *rank-metric code* $\mathcal{C}$ is a k-dimensional E-subspace of E^N, endowed with the rank metric. The integer N is called the *length* of $\mathcal{C}$, k is the *dimension* of $\mathcal{C}$ and d is defined as

$$d = \mathrm{d}_R(\mathcal{C}) := \min\{\mathrm{d}_R(u,v) \mid u, v \in \mathcal{C}, u \neq v\}$$

and is called *minimum rank distance* of $\mathcal{C}$.

Definition 6. Let $k \leq N$ and $g \in E^N$ be a vector such that $\mathrm{w}_R(g) = N$, and τ be a generator of $\mathrm{Gal}(E/K)$. Then, the τ-*Gabidulin code* $\mathcal{G}_{k,\tau}(g)$ is the code

$$\mathcal{G}_{k,\tau}(g) = \left\langle g, \tau(g), \ldots, \tau^{k-1}(g) \right\rangle.$$

Observe that in the definition we are implicitly assuming that $n \geq N$, since for every $v \in E$ we have $\mathrm{w}_R(v) \leq [E:K] = n$.

Gabidulin codes were constructed independently by Delsarte [17] and Gabidulin [20] over finite fields, when τ is the Frobenius automorphism, and then generalized by Kshevetsky and Gabidulin in [33] to any generator of the Galois group. The general definitions for arbitrary fields were due to Roth in [47, Section 6] and to Augot, Loidreau and Robert in [2].

These codes are known to be *maximum rank distance (MRD)*, i.e. the minimum rank distance of a Gabidulin code is $N-k+1$, which is the maximum possible value according to the Singleton-like bound for the rank metric (see [17,20] for the finite field case, [2] for general fields). Moreover, it is well-known that Gabidulin codes are closed under duality. This means that for every $g \in E^N$ such that $\mathrm{w}_R(g) = N$, there exists $h \in E^N$ such that $\mathrm{w}_R(h) = N$ and $\mathcal{G}_{k,\tau}(g)^\perp = \mathcal{G}_{N-k,\tau}(h)$, where the dual is taken with respect to the standard inner product.

There is a way to characterize the minimum rank distance of an $[N,k,d]_{E/K}$ rank-metric code $\mathcal{C}$ in terms of the minimum Hamming distance of a family of linear block codes obtained from $\mathcal{C}$. This is explained by the next proposition, which directly follows from [20, Theorem 1] for the finite field case. For this purpose, we introduce the following

notation. For a given set $\mathcal{H} \subseteq E^N$, and a matrix $M \in K^{N\times N}$, we write $\mathcal{H} \cdot M := \{uM \mid u \in \mathcal{H}\}$.

Proposition 7. *Let $\mathcal{C}$ be an $[N, k, d]_{E/K}$ rank-metric code. Then*

$$\mathrm{d}_R(\mathcal{C}) = \min\{\mathrm{d}_H(\mathcal{C} \cdot M) \mid M \in \mathrm{GL}_N(K)\}.$$

Proof. Let $\delta := \min\{\mathrm{d}_H(\mathcal{C} \cdot M) \mid M \in \mathrm{GL}_N(K)\}$ and $d := \mathrm{d}_R(\mathcal{C})$. For every $c \in \mathcal{C}$, $M \in \mathrm{GL}_N(K)$, we have $\mathrm{w}_R(cM) = \mathrm{w}_R(c)$ and $\mathrm{w}_R(cM) \leq \mathrm{w}(cM)$. Hence, $\delta \geq d$. On the other hand, suppose that $c = (c_1, \ldots, c_N) \in \mathcal{C}$ is of minimal rank weight. Let $S := \langle c_1, \ldots, c_N\rangle_K$ that for hypothesis has dimension d over K, and choose a basis $v_1, \ldots, v_d$ of S. Hence, there exists a matrix $\bar{M} \in \mathrm{GL}_N(K)$ such that $c\bar{M} = (v_1, \ldots, v_d, 0, \ldots, 0)$. This implies that $\delta \leq \mathrm{d}_H(\mathcal{C} \cdot \bar{M}) \leq \mathrm{w}(c\bar{M}) = d$, which concludes the proof. □

4. Defining sets

For the rest of the paper, F/K will denote an arbitrary cyclic field extension and $\sigma \in \mathrm{Gal}(F/K)$ an automorphism of order $|\sigma| = \mu$ such that $K = F^\sigma$. We say that σ *has an extension θ of degree ν* if there exists a field extension E/F and $\theta \in \mathrm{Gal}(E/K)$ such that $|\theta| = n = \nu\mu$, $\theta_{|F} = \sigma$ and $E^\theta = F^\sigma = K$.

We fix such an extension E/F of degree ν.

$$\begin{array}{c} E \\ \nu \,\big|\, \\ F \\ \mu \,\big|\, \\ K \end{array} \Bigg) n$$

Recall that $R = F[x;\sigma]$, $\mathcal{R} = \frac{R}{R(x^n-1)}$, $S = E[x;\theta]$ and $\mathcal{S} = \frac{S}{S(x^n-1)}$. Since for any $f \in R$, we have $Sf \cap R = Rf$ (see [28, Lemma 2.3]), there is a natural inclusion $\mathcal{R} \subseteq \mathcal{S}$. As we have observed in Section 2, we get that $\mathcal{S} \cong K^{n\times n}$ as K-algebras.

Let $\mathcal{C} = \mathcal{R}g$ be an $[n, k]$ skew cyclic code with $g \,|_r\, x^n - 1$, and $\widehat{\mathcal{C}} = \mathcal{S}g$. It follows that $\mathcal{C}$ is a subfield subcode of $\widehat{\mathcal{C}}$. Moreover, there exist $\beta_0, \ldots, \beta_{n-k-1} \in E$ such that

$$g = [x - \beta_0, \ldots, x - \beta_{n-k-1}]_\ell,$$

as explained in Section 2.

Given $\{a_0, \ldots, a_{t-1}\} \subseteq E$, define the following $n \times t$ matrix (see also [34,35]):

$$N(a_0, \ldots, a_{t-1}) = \Big(N_i(a_j)\Big)_{\substack{0\leq i\leq n-1\\ 0\leq j\leq t-1}} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_0 & a_1 & \cdots & a_{t-1} \\ N_2(a_0) & N_2(a_1) & \cdots & N_2(a_{t-1}) \\ \vdots & \vdots & \ddots & \vdots \\ N_{n-1}(a_0) & N_{n-1}(a_1) & \cdots & N_{n-1}(a_{t-1}) \end{pmatrix}.$$

For any matrix M we denote by $\ker(M)$ its left kernel, i.e. $\ker(M) = \{v \mid vM = 0\}$.

Proposition 8. *Let $\widehat{\mathcal{C}} \subseteq \mathcal{S}$ be the $[n,k]$ skew cyclic code generated be $g = [x - \beta_0, \dots, x - \beta_{n-k-1}]_\ell$, with $\beta_0, \dots, \beta_{n-k-1} \in E$. Then, $\widehat{\mathcal{C}} = \ker\left(N(\beta_0, \dots, \beta_{n-k-1})\right)$, i.e. $N(\beta_0, \dots, \beta_{n-k-1})$ is a parity check matrix for $\mathcal{C}$ and $\widehat{\mathcal{C}}$.*

Proof. A polynomial $f = \sum_{i=0}^{n-1} f_i x^i$ is in $\widehat{\mathcal{C}}$ if and only if $x - \beta_j \mid_r f$ for all $0 \leq j \leq n-k-1$. Since $x - \beta_j \mid_r f$ if and only if $\sum_{i=0}^{n-1} f_i N_i(\beta_j) = 0$, the result follows. □

As we pointed out before, $x - \beta \mid_r x^n - 1$ if and only if $\beta = \theta(\alpha)\alpha^{-1}$, for some $\alpha \in E \setminus \{0\}$. For all $\alpha \in E$ we use the notation

$$\alpha^{[\theta]} = \left(\alpha, \theta(\alpha), \dots, \theta^{n-1}(\alpha)\right)^\top.$$

Proposition 9. *Assume $\beta_i = \theta(\alpha_i)\alpha_i^{-1}$ for each $0 \leq i \leq n-k-1$ and let $g = [x - \beta_0, \dots, x - \beta_{n-k-1}]_\ell$. Then*

$$\widehat{\mathcal{C}} = \mathcal{S}g = \ker\left(\alpha_0^{[\theta]} \middle| \alpha_1^{[\theta]} \middle| \cdots \middle| \alpha_{n-k-1}^{[\theta]}\right).$$

Proof. Since $N_i(\beta_j) = \theta^i(\alpha_j)\alpha_j^{-1}$, it follows that $(1, \beta_j, N_2(\beta_j), \cdots, N_{n-1}(\beta_j))^\top = \alpha_j^{[\theta]}\alpha_j^{-1}$, hence, by [35, Equation (4.12)],

$$N(\beta_0, \dots, \beta_{n-k-1}) = \left(\alpha_0^{[\theta]} \middle| \alpha_1^{[\theta]} \middle| \cdots \middle| \alpha_{n-k-1}^{[\theta]}\right) \begin{pmatrix} \alpha_0^{-1} & & & \\ & \alpha_1^{-1} & & \\ & & \ddots & \\ & & & \alpha_{n-k-1}^{-1} \end{pmatrix}$$

and

$$\ker\left(N(\beta_0, \dots, \beta_{n-k-1})\right) = \ker\left(\alpha_0^{[\theta]} \middle| \alpha_1^{[\theta]} \middle| \cdots \middle| \alpha_{n-k-1}^{[\theta]}\right)$$

as desired. □

From Proposition 9 it immediately follows the next result.

Corollary 10. *Let $\alpha \in E$ be such that $\{\alpha, \theta(\alpha), \dots, \theta^{n-1}(\alpha)\}$ is a normal basis and let $\beta = \theta(\alpha)\alpha^{-1}$. Let moreover δ be an integer such that $1 \leq \delta \leq n$. Then*

$$\mathrm{sRS}_\beta^\theta(n, \delta) = \mathcal{G}_{\delta-1,\theta}(\alpha^{[\theta]})^\perp.$$

In particular, skew Reed-Solomon codes are MRD codes of dimension $n - \delta + 1$ and minimum rank distance δ.

Note that Corollary 10 is a generalization of [10, Proposition 3.2], which deal with finite fields only.

Let $\alpha \in E$ such that $\{\alpha, \theta(\alpha), \dots, \theta^{n-1}(\alpha)\}$ is a K-basis. Let $\beta = \theta(\alpha)\alpha^{-1}$. It is well known that

$$x^n - 1 = \left[\{x - \theta^i(\beta) \mid 0 \le i \le n-1\}\right]_\ell,$$

see e.g. [16, Theorem 5.3]

Definition 11. Let $g \in R$ such that $g \mid_r x^n - 1$, $\mathcal{C} = \mathcal{R}g$ and $\widehat{\mathcal{C}} = \mathcal{S}g$. The *$\beta$-defining set of g* is

$$T_\beta(g) = \left\{0 \le i \le n-1 \;\middle|\; x - \theta^i(\beta) \mid_r g\right\}.$$

In particular, $\left[\{x - \theta^i(\beta) \mid i \in T_\beta(g)\}\right]_\ell \mid_r g$.

5. Skew Roos bound for the Hamming metric

In this section, we will keep the notation of Definition 11. Hence we will write $\mathcal{C}$ for the skew cyclic code $\mathcal{C} = \mathcal{R}g$, where $g \in R$ is such that $g \mid_r x^n - 1$, and $\widehat{\mathcal{C}} = \mathcal{S}g$.

Lemma 12. *Let $\alpha_1, \dots, \alpha_{t+r} \in E$ be linear independent elements over K. Let $\{k_0, \dots, k_r\} \subseteq \{0, \dots, n-1\}$ be such that $k_r - k_0 \le t + r - 1$ and $k_{j-1} < k_j$ for $1 \le j \le r$. Let*

$$A_0 = \begin{pmatrix} \theta^{k_0}(\alpha_1) & \theta^{k_1}(\alpha_1) & \cdots & \theta^{k_r}(\alpha_1) \\ \vdots & \vdots & \ddots & \vdots \\ \theta^{k_0}(\alpha_{t+r}) & \theta^{k_1}(\alpha_{t+r}) & \cdots & \theta^{k_r}(\alpha_{t+r}) \end{pmatrix}.$$

Let $s \in \{0, \dots, n-1\}$ such that $(s, n) = 1$ and

$$A_i = \left(A_0 \;\middle|\; \theta^s(A_0) \;\middle|\; \dots \;\middle|\; \theta^{si}(A_0) \right),$$

for $0 \le i \le r$. Then $\mathrm{rk}(A_{t-1}) = t + r$.

Proof. Let $\mathcal{A}_i \subseteq E^{t+r}$ be the column space of A_i, so $\dim(\mathcal{A}_i) = \mathrm{rk}(A_i)$. Observe that

$$\{k_0, \dots, k_r\} \subseteq \{k_0, k_0 + 1, \dots, k_0 + t + r - 1\},$$

hence A_0 is obtained from

$$A = \begin{pmatrix} \theta^{k_0}(\alpha_1) & \theta^{k_0+1}(\alpha_1) & \cdots & \theta^{k_0+t+r-1}(\alpha_1) \\ \vdots & \vdots & \ddots & \vdots \\ \theta^{k_0}(\alpha_{t+r}) & \theta^{k_0+1}(\alpha_{t+r}) & \cdots & \theta^{k_0+t+r-1}(\alpha_{t+r}) \end{pmatrix}$$

after deleting some columns. By the Circulant Lemma (Lemma 2), $\mathrm{rk}(A) = t + r$, hence $\dim(\mathcal{A}_0) = \mathrm{rk}(A_0) = r + 1$. Assume by contradiction that $\dim(\mathcal{A}_{t-1}) < t + r$. Since $\mathcal{A}_i \subseteq \mathcal{A}_{i+1}$ for $0 \leq i \leq t-2$, it follows that there exists $0 \leq j \leq t-2$ such that $\dim(\mathcal{A}_j) = \dim(\mathcal{A}_{j+1})$, i.e. $\mathcal{A}_j = \mathcal{A}_{j+1}$. Since $\mathcal{A}_{i+1} = \mathcal{A}_i + \theta^s(\mathcal{A}_i)$ for $0 \leq i \leq t-2$, it follows that $\mathcal{A}_j = \theta^s(\mathcal{A}_j)$, i.e. $\mathcal{A}_j$ is invariant under the action of θ^s. Hence $\mathcal{A}_j \supseteq \mathcal{A}_0 + \theta^s(\mathcal{A}_0) + \cdots + \theta^{s(t+r-1)}(\mathcal{A}_0)$. In particular $\mathcal{A}_j$ contains the columns of

$$A' = \begin{pmatrix} \theta^{k_0}(\alpha_1) & \theta^{k_0+s}(\alpha_1) & \cdots & \theta^{k_0+s(t+r-1)}(\alpha_1) \\ \vdots & \vdots & \ddots & \vdots \\ \theta^{k_0}(\alpha_{t+r}) & \theta^{k_0+s}(\alpha_{t+r}) & \cdots & \theta^{k_0+s(t+r-1)}(\alpha_{t+r}) \end{pmatrix}.$$

Since $(s, n) = 1$, $K = E^\theta = E^{\theta^s}$, so again by Lemma 2, $\det(A') \neq 0$, and therefore $\dim(\mathcal{A}_j) \geq t + r$. Finally $\mathcal{A}_{t-1} \supseteq \mathcal{A}_j$, so we get $t + r > \dim(\mathcal{A}_{t-1}) \geq t + r$, that is a contradiction. □

The following theorem is inspired by [28, Theorem 3.3].

Theorem 13 *(Skew Roos bound for the Hamming metric). Let $\mathcal{C}$ be the skew cyclic code $\mathcal{R}g$, where $g \in R$ and $\widehat{\mathcal{C}} = \mathcal{S}g$. Let $\alpha \in E$ such that $\{\alpha, \theta(\alpha), \ldots, \theta^{n-1}(\alpha)\}$ is a K-basis and let $\beta = \theta(\alpha)\alpha^{-1}$. Moreover, assume that there are $b, s, \delta, k_0, \ldots, k_r$ such that, $(s, n) = 1$, $k_j < k_{j+1}$ for $0 \leq j \leq r-1$, $k_r - k_0 \leq \delta + r - 2$, and $b + si + k_j \in T_\beta(g)$ for all $0 \leq i \leq \delta - 2$ and $0 \leq j \leq r$. Then $\mathrm{d}_H(\mathcal{C}) \geq \mathrm{d}_H(\widehat{\mathcal{C}}) \geq \delta + r$.*

Proof. The inequality $\mathrm{d}_H(\mathcal{C}) \geq \mathrm{d}_H(\widehat{\mathcal{C}})$ follows since $\mathcal{C}$ is a subfield subcode of $\widehat{\mathcal{C}}$. Let $w = \delta + r - 1$ and let $c \in \widehat{\mathcal{C}} = \mathcal{S}g$ such that $\mathrm{w}(c) \leq w$, i.e. $c = \sum_{h=1}^{w} c_h x^{l_h}$ for suitable $\{l_1, \ldots, l_w\} \subseteq \{0, \ldots, n-1\}$. For each $0 \leq i \leq \delta - 2$ and $0 \leq j \leq r$, $x - \theta^{b+si+k_j}(\beta) \mid_r c$, so

$$\begin{aligned} 0 &= \textstyle\sum_{h=1}^{w} c_h N_{l_h}(\theta^{b+si+k_j}(\beta)) \\ &= \theta^{b+si+k_j}(\alpha)^{-1} \textstyle\sum_{h=1}^{w} c_h \theta^{b+si+k_j+l_h}(\alpha). \end{aligned}$$

We get that $\bar{c} := (c_1, \ldots, c_w)$ is in the left kernel of the matrix $\theta^b(B)$ where

$$B = \left(A_0 \;\middle|\; \theta^s(A_0) \;\middle|\; \cdots \;\middle|\; \theta^{s(\delta-2)}(A_0) \right)$$

and

$$A_0 = \left(\theta^{k_j+l_h}(\alpha)\right)_{\substack{1 \leq h \leq w \\ 0 \leq j \leq r}}.$$

Applying Lemma 12 with $t = \delta - 1$, we get that $\mathrm{rk}(B) = w$. Hence, $\bar{c} = 0$ and, so, $c = 0$ is the only element in $\mathcal{S}g$ of weight at most $\delta + r - 1$. □

If $s = 1$ we obtain an nice relation with skew Reed-Solomon codes, as next proposition shows.

Proposition 14. *Let $\mathcal{C}$ be the skew cyclic code $\mathcal{R}g$, where $g \in R$ and $\widehat{\mathcal{C}} = \mathcal{S}g$. Let $\alpha \in E$ such that $\{\alpha, \theta(\alpha), \dots, \theta^{n-1}(\alpha)\}$ is a K-basis and let $\beta = \theta(\alpha)\alpha^{-1}$. Moreover, assume that there are $b, \delta, k_0, \dots, k_r$ such that $k_j < k_{j+1}$ for $0 \leq j \leq r-1$, $k_r - k_0 \leq \delta + r - 2$, and $b+i+k_j \in T_\beta(g)$ for all $0 \leq i \leq \delta-2$ and $0 \leq j \leq r$. Then $\mathrm{sRS}^{\theta}_{\theta^{b+k_0}(\beta)}(n, \delta+r) \supseteq \widehat{\mathcal{C}}$. In particular $\mathrm{d}_H(\mathcal{C}) \geq \delta + r$ and $\mathrm{d}_R(\mathcal{C}) \geq \delta + r$.*

Proof. Up to replacing β by $\theta^b(\beta)$, we may assume $b = 0$. Since $k_j < k_{j+1}$ for all j, it follows that $k_l \geq k_j + (l - j)$ for all $j \leq l$. Assume, for a contradiction, that $k_j + \delta - 1 < k_{j+1}$. Then

$$k_0 + j + \delta - 1 \leq k_j + \delta - 1 < k_{j+1} \leq k_r - (r - j - 1),$$

and consequently

$$\delta + r - 2 = (j + \delta - 1) + (r - j - 1) < k_r - k_0,$$

which is incompatible with the hypothesis $k_r - k_0 \leq \delta + r - 2$. Therefore $k_{j+1} \leq k_j + \delta - 1$ and

$$\bigcup_{j=0}^{r} \{k_j + i \mid 0 \leq i \leq \delta - 2\} = [k_0, k_r + \delta - 2] \cap \mathbb{Z}.$$

Since $k_r \geq k_0 + r$, it follows that

$$[k_0, k_0 + \delta + r - 2] \cap \mathbb{Z} \subseteq T_\beta(g),$$

so, if $f = \left[\{x - \theta^{k_0+i}(\beta) \mid 0 \leq i \leq \delta + r - 2\}\right]_\ell$, we have that

$$f \mid_r g.$$

This implies that $\mathcal{S}f \supseteq \mathcal{S}g$. Since $\mathcal{S}f = \mathrm{sRS}^{\theta}_{\theta^{k_0}(\beta)}(n, \delta + r)$ and $\mathcal{S}g = \widehat{\mathcal{C}} \supseteq \mathcal{C}$, the result follows using Proposition 1 and Corollary 10. □

Corollary 15. *Assume that there are $b, \delta, s, k_0, \dots, k_r$ such that $k_j < k_{j+1}$ for $0 \leq j \leq r-1$, $k_r - k_0 \leq \delta + r - 2$, $(s, n) = 1$, and $b + is + k_j s \in T_\beta(g)$ for all $0 \leq i \leq \delta - 2$ and $0 \leq j \leq r$. Then there exists b' such that $\mathrm{sRS}^{\theta^s}_{\theta^{b'+k_0 s}(\beta)}(n, \delta + r) \supseteq \widehat{\mathcal{C}}$. In particular $\mathrm{d}_H(\mathcal{C}) \geq \delta + r$ and $\mathrm{d}_R(\mathcal{C}) \geq \delta + r$.*

Proof. Apply Proposition 14 to θ^s and $b' = bu$ where $us + vn = 1$. □

Proposition 14 and its Corollary 15 say that $\{0,1,\dots,\delta+r-2\} \subseteq T_{\theta^{k_0(\beta)}}(g)$ and $\{0,1,\dots,\delta+r-2\} \subseteq T_{\theta^{b'+k_0 s(\beta)}}(g)$ respectively, so they are instances of the skew BCH bound as presented in [28, Corollary 3.4] in the general framework of Galois cyclic extensions. Moreover, as we have already remarked after Proposition 1, there are efficient decoding algorithms which can be applied for skew cyclic codes in the framework of Proposition 14 and Corollary 15.

Theorem 13 and Proposition 14 use the fact that the corresponding distances of $\mathcal{C}$ are bounded by the distances of $\widehat{\mathcal{C}}$. In these cases both distances are closely related as next results show.

Let $\pi = \theta^\mu$. Then $F = E^\pi$. The proof of next proposition is essentially [53, Theorem 9].

Proposition 16. *Let $A = \{\alpha_1,\dots,\alpha_k\} \subseteq E$ such that π induces a permutation on A, i.e., for all $1 \le j \le k$, there exists a unique $1 \le \pi(j) \le k$ such that $\pi(\alpha_j) = \alpha_{\pi(j)}$. Let $\widehat{\mathcal{C}} = \ker\left(\alpha_1^{[\theta]}\middle|\cdots\middle|\alpha_k^{[\theta]}\right) \subseteq E^n$ and $\mathcal{C} = \widehat{\mathcal{C}} \cap F^n$. Then $\mathrm{d}_H(\widehat{\mathcal{C}}) = \mathrm{d}_H(\mathcal{C})$.*

Proof. Since $\mathcal{C} \subseteq \widehat{\mathcal{C}}$, it follows that $\mathrm{d}_H(\mathcal{C}) \ge \mathrm{d}_H(\widehat{\mathcal{C}})$. Let $c = (c_0,\dots,c_{n-1}) \in \widehat{\mathcal{C}}$ such that $\mathrm{w}(c) = \mathrm{d}_H(\widehat{\mathcal{C}})$. The hypothesis $\pi(\alpha_j) = \alpha_{\pi(j)}$ implies that $\pi(\theta^i(\alpha_j)) = \theta^i(\alpha_{\pi(j)})$, so, for each $0 \le j \le s-1$, π^j induces a permutation on the columns of $\left(\alpha_1^{[\theta]}\middle|\cdots\middle|\alpha_k^{[\theta]}\right)$. Since $c \in \widehat{\mathcal{C}}$,

$$(c_0,\dots,c_{n-1})\left(\alpha_1^{[\theta]}\middle|\cdots\middle|\alpha_k^{[\theta]}\right) = 0,$$

so

$$(\pi^j(c_0),\dots,\pi^j(c_{n-1}))\left(\alpha_1^{[\theta]}\middle|\cdots\middle|\alpha_k^{[\theta]}\right) = 0$$

for each $0 \le j \le s-1$. It follows that

$$(\mathrm{Tr}_{E/F}(c_0),\dots,\mathrm{Tr}_{E/F}(c_{n-1}))\left(\alpha_1^{[\theta]}\middle|\cdots\middle|\alpha_k^{[\theta]}\right) = 0,$$

i.e. $(\mathrm{Tr}_{E/F}(c_0),\dots,\mathrm{Tr}_{E/F}(c_{n-1})) \in \widehat{\mathcal{C}}$. Up to replacing c with some scalar multiple, we can assume $0 \ne (\mathrm{Tr}_{E/F}(c_0),\dots,\mathrm{Tr}_{E/F}(c_{n-1})) \in F^n$, hence $(\mathrm{Tr}_{E/F}(c_0),\dots,\mathrm{Tr}_{E/F}(c_{n-1})) \in \mathcal{C} \setminus \{0\}$. Therefore

$$\mathrm{d}_H(\mathcal{C}) \le \mathrm{w}(\mathrm{Tr}_{E/F}(c_0),\dots,\mathrm{Tr}_{E/F}(c_{n-1})) \le \mathrm{w}(c) = \mathrm{d}_H(\widehat{\mathcal{C}}),$$

and then we have the equality. □

By using the notation of [28, p. 94], let $C_n = \{0,1,\dots,n-1\}$ be regarded as a cyclic group of order n and, since $n = \nu\mu$, $\mu C_n = \{0,\mu,\dots,(\nu-1)\mu\}$ is a subgroup of order ν of C_n. Moreover, let $C_n/\mu C_n$ be the quotient group. If $T = T^1 \cup \cdots \cup T^\ell \subseteq C_n$ such that $T^j \in C_n/\mu C_n$, it follows that $i \in T$ implies $i+\mu \in T$. A set with this property is

said to be *μ-closed*. The defining set of a polynomial $g \in R = F[x;\sigma]$ is μ-closed because $F = E^{\pi}$.

Proposition 17. *Let $g \in R$ such that $g \mid_r x^n - 1$. Let $\alpha \in E$ such that $\{\alpha, \theta(\alpha), \dots, \theta^{n-1}(\alpha)\}$ is a normal basis. Let $\beta = \theta(\alpha)\alpha^{-1}$ and let $T_\beta(g) = \{i \in C_n \ : \ x - \theta^i(\beta) \mid_r g\}$. Then π induces a permutation on $\{\theta^i(\alpha) \mid i \in T_\beta(g)\}$.*

Proof. By [28, Lemma 4.3], $T_\beta(g) = T^1 \cup \cdots \cup T^\ell$ for some cosets $T^j \in C_n/\mu C_n$. Let $A = \{\theta^i(\alpha) \mid i \in T_\beta(g)\}$. If $\theta^i(\alpha) \in A$,

$$\pi(\theta^i(\alpha)) = \theta^{i+\mu}(\alpha) \in A$$

because $i \in T_\beta(g)$ implies $i + \mu \in T_\beta(g)$. □

Example 18. Let $F = \mathbb{F}_{2^6}$ be the finite field with 2^6 elements, a be a primitive element satisfying $a^6 + a^4 + a^3 + a + 1$ and consider the automorphism $\sigma : F \to F$ given by $\sigma(a) = a^2$. The order of σ is 6.

Moreover, let $E = \mathbb{F}_{2^{12}}$ be an extension field of F. Let γ be a primitive element of E satisfying $\gamma^{12} + \gamma^7 + \gamma^6 + \gamma^5 + \gamma^3 + \gamma + 1$. The embedding $\varphi : F \to E$ is defined as $\varphi(a) = \gamma^9 + \gamma^5 + \gamma^4 + \gamma^2 + \gamma = \gamma^{65}$. Let $\theta : E \to E$ be the extension of the automorphism σ to the field E, that is the Frobenius automorphism of order 12.

Now, fix $\alpha := \gamma^5$ to be a normal element of E as a $\mathbb{F}_2$-vector space. Hence $\beta := \theta(\alpha)\alpha^{-1} = \gamma^5$. Choose the parameters of the Roos bound as $b = 0$, $\delta = 3$, $r = 1$, $k_0 = 9$ and $k_1 = 10$. It follows that the defining set we are looking for is $T_\beta(g) = \{2, 3, 4, 8, 9, 10\}$. Now we compute the least common left multiple $\left[x - \theta^i(\beta)\right]_\ell^{i=2,3,4,8,9,10} \in F[x;\sigma]$ which defines a skew cyclic code of dimension 6 and distance at least 4. In particular, the code has generator polynomial

$$g = x^6 + a^{31}x^5 + a^{26}x^4 + ax^3 + a^5x^2 + a^{43}x + a^{49}.$$

With the aid of the software Magma [6], we can then compute the exact distance of the code that turns to be 6. Therefore, the code $\mathcal{C} = \mathcal{R}g$ is a $[12, 6, 6]$ code over the field $F = \mathbb{F}_{2^6}$.

Example 19. Let $K = \mathbb{F}_2$, $F = \mathbb{F}_{2^7}$, a be a primitive element and $\sigma : F \to F$, given by $\sigma(a) = a^2$. Let $E = \mathbb{F}_{2^{14}}$ be the extension field of F of degree 2 and γ be a primitive element of E. By following Example 18, let $\alpha := \gamma^7$ be a normal element of E as K-vector space and fix $\beta := \theta(\alpha)\alpha^{-1} = \gamma^7$. Consider $b = 0, \delta = 3, r = 2, k_0 = 2, k_1 = 4, k_2 = 5$ as the parameters of the Roos bound. It follows that the defining set for the code we are constructing is $T_\beta(g) = \{2, 3, 4, 5, 6, 9, 10, 11, 12, 13\}$, and g is computed as the least common left multiple $\left[\{x - \theta^i(\beta) \mid i \in T_\beta(g)\}\right]_\ell \in F[x;\sigma]$. The code generated by g is a $[14, 4, 11]$ MDS linear code over $\mathbb{F}_{2^7}$.

Example 20. We are going to include an example concerning convolutional codes. Convolutional codes can be equivalently described as direct summands of $\mathbb{F}[z]^n$, where $\mathbb{F}$ is a finite field, or as a vector subspace of $\mathbb{F}(z)^n$, the field of rational functions over a finite field. This equivalence was firstly established in [19, Theorem 3], and a more recent refinement can also be found in [29, Proposition 1]. We can also provide a lower bound on the free distance of a convolutional code, since it is lower bounded by its minimum Hamming distance. For this example we follow an analogous construction to [28, Example 2.5]. Let $F = \mathbb{F}_{16}(z)$ and $\sigma : F \to F$ the automorphism defined by $\sigma(z) = \frac{b^9}{z+b^4}$, where $\mathbb{F}_{16} = \mathbb{F}_2[b]/(b^4+b+1)$. This is an automorphism of order $\mu = 15$ and, by Lüroth's Theorem [52, §10.2], the invariant subfield is $K = F^\sigma = \mathbb{F}_{16}(u)$ for some $u \in \mathbb{F}_{16}(z)$. Let $\mathbb{F}_{256} = \mathbb{F}_2[a]/(a^8 + a^4 + a^3 + a^2 + 1)$. It is straightforward to check that a canonical embedding $\epsilon : \mathbb{F}_{16} \to \mathbb{F}_{256}$ is defined by $\epsilon(b) = a^{17}$. Let $\pi : \mathbb{F}_{256} \to \mathbb{F}_{256}$ be the automorphism defined by $\pi(a) = a^{16}$, and let also denote by π the canonical extension to $E = \mathbb{F}_{256}(z)$, i.e.

$$\pi\left(\frac{a_0 + a_1 t + \cdots + a_m t^m}{b_0 + b_1 t + \cdots + b_{m'} t^{m'}}\right) = \frac{a_0^{16} + a_1^{16} t + \cdots + a_m^{16} t^m}{b_0^{16} + b_1^{16} t + \cdots + b_{m'}^{16} t^{m'}}.$$

We also use σ to denote its canonical extension to $\sigma : E \to E$, so $\sigma(z) = \frac{a^{153}}{z+a^{68}}$. Since $\mathbb{F}_{16} = \mathbb{F}_{256}^{\pi}$, it follows that $\sigma\pi = \pi\sigma$, so $\theta = \sigma\pi : E \to E$ is an extension of σ of degree $\nu = 2$. In order to build a skew cyclic convolutional code of a designed Hamming distance using the Roos bound, we need a normal basis of E over $K = E^\theta$. Such a basis can be obtained from $\alpha = az$, and the corresponding root is $\beta = \theta(\alpha)\alpha^{-1} = \frac{a^{168}}{z^2+a^{68}z}$. Let $T = \{0, 2, 3, 4, 7, 9, 10, 11, 15, 17, 18, 19, 22, 24, 25, 26\}$. Then T is μ-closed, and $g = \left[\{x - \theta^i(\beta) \mid i \in T\}\right]_\ell$ generates a skew cyclic convolutional code of rate 14/30. This polynomial has degree 16 and its coefficients are rational functions up to degree 11 which we have computed with the aid of [51]. Now, $T \supseteq \{0, 2, 3, 4, 7, 9, 10, 11\}$, which corresponds to the parameters $b = 0$, $\delta = 3$, $s = 7$ and $k_0, k_1, k_2, k_3 = 0, 2, 3, 4$. So, its Hamming distance is bounded from below by $\delta + r = 3 + 3 = 6$.

Remark 21. Observe that in the preceding examples the lower bounds obtained using a skew BCH bound and a skew Hartmann-Tzeng bound can be seen to be the same as the lower bound derived with the aid of Theorem 13. However, these examples are only to show how to construct skew cyclic codes with a prescribed minimum distance.

At this point a reader will be wondering whether it is possible to construct skew cyclic codes such that the best lower bound obtained via Theorem 13 improves the skew HT and the skew BCH bounds. The answer is yes. To see this, take any classical cyclic code of length n over a finite field such that the Roos bound provides a better estimate on the lower bound than the one obtained by the HT and BCH bounds. For examples, one can take [45, Examples 1 & 2]. This will result in a set of integers modulo n which we use as defining set $T_\beta(g)$ for a skew cyclic code in which $F = E$ and $[F : K] = n$.

Table 1
Skew cyclic codes constructed using the Roos bound. The rows in which appears a * indicate that the corresponding code is MDS.

K	F	$E = K(\gamma)$	α	b	δ	r	$T_\beta(g)$	$[n, k, d]$
$\mathbb{F}_2$	$\mathbb{F}_{2^6}$	$\mathbb{F}_{2^{12}}$	γ^5	0	3	1	$\{2, 3, 4, 8, 9, 10\}$	$[12, 6, 6]$
$\mathbb{F}_2$	$\mathbb{F}_{2^6}$	$\mathbb{F}_{2^{12}}$	γ^5	0	3	1	$\{1, 2, 3, 4, 7, 8, 9, 10\}$	$[12, 4, 8]$
$\mathbb{F}_2$	$\mathbb{F}_{2^5}$	$\mathbb{F}_{2^{20}}$	γ^{11}	0	3	1	$\{1, 2, 3, 6, 7, 8, 11, 12, 13, 16, 17, 18\}$	$[20, 8, 11]$
$\mathbb{F}_2$	$\mathbb{F}_{2^7}$	$\mathbb{F}_{2^{14}}$	γ^7	0	3	1	$\{0, 5, 6, 7, 12, 13\}$	$[14, 8, 7]^*$
$\mathbb{F}_2$	$\mathbb{F}_{2^7}$	$\mathbb{F}_{2^{14}}$	γ^7	0	3	2	$\{0, 1, 2, 3, 4, 7, 8, 9, 10, 11\}$	$[14, 4, 11]^*$
$\mathbb{F}_3$	$\mathbb{F}_{3^6}$	$\mathbb{F}_{3^{12}}$	γ^7	0	3	1	$\{2, 3, 4, 8, 9, 10\}$	$[12, 6, 7]^*$
$\mathbb{F}_3$	$\mathbb{F}_{3^5}$	$\mathbb{F}_{3^{15}}$	$2\gamma^{13} + \gamma^{11} + \gamma^{10} + 2$	0	3	1	$\{2, 3, 4, 7, 8, 9, 12, 13, 14\}$	$[15, 6, 10]^*$
$\mathbb{F}_5$	$\mathbb{F}_{5^5}$	$\mathbb{F}_{5^{10}}$	$\gamma^9 + \gamma^7 + \gamma^6 + 3\gamma^5 + 2\gamma^3 + \gamma + 3$	0	3	1	$\{0, 1, 2, 5, 6, 7\}$	$[10, 4, 7]^*$

We conclude this section by commenting on Table 1, which provides a list of skew cyclic codes, computed as in Example 18. Hence $F = K(a)$, where a is a primitive element of F and $E = K(\gamma)$, with γ primitive element of E. The generator polynomials of the skew cyclic codes in the table are computed by the aid of Magma [6] as least common left multiples (we omit to write it for brevity). Moreover, always with the aid of Magma, we computed the effective minimum distances of the constructed skew-cyclic codes. Observe that in some cases with this construction we obtain codes reaching the Singleton bound.

6. Skew Roos bound for the rank metric

In this section we provide the rank-metric version of the skew Roos bound, which improves the bound of Theorem 13. The proof uses all the tools developed in the previous sections, and in particular it relies on Theorem 13, Lemmas 2 and 12 and Proposition 7.

Also in this section we will use the notation introduced in Definition 11, writing $\mathcal{C} = \mathcal{R}g$, where $g \in R$ is such that $g \mid_r x^n - 1$, and $\widehat{\mathcal{C}} = \mathcal{S}g$.

The following result improves Corollary 15 and provides the real analogue of the Roos bound for skew cyclic code in the rank metric.

Theorem 22 *(Skew Roos bound for the rank metric). Assume that there are $b, s, \delta, k_0, \dots, k_r$ such that $(s, n) = 1$, $k_j < k_{j+1}$ for $0 \le j \le r-1$, $k_r - k_0 \le \delta + r - 2$, and $b + si + k_j \in T_\beta(g)$ for all $0 \le i \le \delta - 2$ and $0 \le j \le r$. Then $\mathrm{d}_R(\mathcal{C}) \ge \mathrm{d}_R(\widehat{\mathcal{C}}) \ge \delta + r$.*

Proof. As before $\mathrm{d}_R(\mathcal{C}) \ge \mathrm{d}_R(\widehat{\mathcal{C}})$ because $\mathcal{C}$ is a subfield subcode of $\widehat{\mathcal{C}}$. By Proposition 7, we need to prove that for every $M^{-1} \in \mathrm{GL}_n(K)$, we have $\mathrm{d}_H(\widehat{\mathcal{C}} \cdot M^{-1}) \ge \delta + r$. Take a generic $M \in \mathrm{GL}_n(K)$, define $w = \delta + r - 1$ and consider $c \in \widehat{\mathcal{C}} \cdot M^{-1}$ such that $\mathrm{w}(c) \le w$, i.e. $c = \sum_{h=1}^{w} c_h x^{l_h}$ for a suitable $S := \{l_1, \dots, l_w\} \subseteq \{0, \dots, n-1\}$. Denote by M_S the matrix obtained from M only selecting the rows indexed by the elements in S (here we assume the row indices to be $0, 1, \dots, n-1$). As in the proof of Theorem 13, we get that $\bar{c} := (c_1, \dots, c_w)$ belongs to the left kernel of the matrix $M_S \tilde{B}$, where

$$\tilde{B} = \left(A \;\middle|\; \theta^s(A) \;\middle|\; \cdots \;\middle|\; \theta^{s(\delta-2)}(A) \right),$$

and

$$A = \left(\theta^{k_j+h}(\alpha)\right)_{\substack{0\le h\le n-1\\ 0\le j\le r}}.$$

Now observe that

$$\begin{aligned} M_S\tilde{B} &= \left(M_SA \;\middle|\; M_S\theta^s(A) \;\middle|\; \cdots \;\middle|\; M_S\theta^{s(\delta-2)}(A) \right) \\ &= \left(M_SA \;\middle|\; \theta^s(M_SA) \;\middle|\; \cdots \;\middle|\; \theta^{s(\delta-2)}(M_SA) \right), \end{aligned}$$

where the last equality follows from the fact that the coefficients of M_S are in K, and hence are fixed by θ. We observe now that the matrix M_SA is of the form

$$M_SA = A_0 = \left(\theta^{k_j}(\beta_h)\right)_{\substack{1\le h\le w\\ 0\le j\le r}},$$

where the elements β_h's are given by $\beta_h = M_{\{l_h\}}\alpha^{[\theta]}$, and are linearly independent over K. Hence, by Lemma 2, A_0 has rank r. At this point, by applying Lemma 12 on the matrices $M_S\tilde{B}$ and $M_SA = A_0$, with $t = \delta - 1$ we get that $\mathrm{rk}(M_S\tilde{B}) = w$ and hence $\bar{c} = 0$, so $c = 0$ is the only element in $\widehat{\mathcal{C}} \cdot M^{-1}$ of weight at most $\delta + r - 1$. This proves that $\mathrm{d}_H(\widehat{\mathcal{C}} \cdot M^{-1}) \ge \delta + r$ and concludes the proof. □

In Section 3, we mentioned that Gabidulin codes are MRD codes, since their parameters attain a Singleton-like bound for the rank metric. Actually, there are two Singleton-like bounds for the rank metric, depending on how the length and the extension degree of the code are related. Formally, let $\mathcal{C}$ be an $[n, k, d]_{F/K}$ rank-metric code and let $\mu = [F : K]$, then

$$k \le n - d + 1 \tag{2}$$

$$k \le \frac{n}{\mu}(\mu - d + 1) \tag{3}$$

In particular, one considers inequality (2) when $n \le \mu$, and inequality (3) if μ divides n. In this setting, an $[n, k, d]_{F/K}$ rank-metric code is *maximum rank distance (MRD)* if its parameters meet with equality one of the two bounds above.

Since in the construction of rank-metric codes that we gave using the skew Roos bound of Theorem 22 we deal with $n = \mu\nu$, we should only consider inequality (3), that with our notation becomes

$$k \le \nu(\mu - d + 1). \tag{4}$$

Hence, a code $\mathcal{C}$ satisfying the hypotheses of Theorem 22 is an $[n, k, \ge \delta + r]_{F/K}$ rank-metric code, where $k = n - \deg g \le \nu(\mu - \delta - r + 1)$.

Example 23. Consider the code $\mathcal{C}$ constructed in Example 18 endowed with the rank metric. Putting together the Singleton-like bound in (4) and the skew Roos bound for

Table 2
Skew cyclic rank-metric codes constructed using the Roos bound. The rows in which appears a * indicate that the corresponding code is MRD.

K	F	E	δ	r	n	k	$\mu - \frac{\mu k}{n} + 1$	d_R
$\mathbb{F}_2$	$\mathbb{F}_{2^6}$	$\mathbb{F}_{2^{12}}$	3	1	12	6	4	4^*
$\mathbb{F}_2$	$\mathbb{F}_{2^6}$	$\mathbb{F}_{2^{12}}$	3	1	12	4	5	5^*
$\mathbb{F}_2$	$\mathbb{F}_{2^5}$	$\mathbb{F}_{2^{20}}$	3	1	20	8	4	4^*
$\mathbb{F}_2$	$\mathbb{F}_{2^7}$	$\mathbb{F}_{2^{14}}$	3	1	14	8	4	4^*
$\mathbb{F}_2$	$\mathbb{F}_{2^7}$	$\mathbb{F}_{2^{14}}$	3	2	14	4	6	6^*
$\mathbb{F}_3$	$\mathbb{F}_{3^6}$	$\mathbb{F}_{3^{12}}$	3	1	12	6	4	4^*
$\mathbb{F}_3$	$\mathbb{F}_{3^5}$	$\mathbb{F}_{3^{15}}$	3	1	15	6	5	$4 \leq \mathrm{d}_R \leq 5$
$\mathbb{F}_5$	$\mathbb{F}_{5^5}$	$\mathbb{F}_{5^{10}}$	3	1	10	4	4	4^*

the rank metric of Theorem 22, we get that $\mathcal{C}$ is a $[12, 6, \geq 4]_{F/K}$ rank-metric code, where $F = \mathbb{F}_{2^6}$ and $K = \mathbb{F}_2$, which satisfies the following chain of inequalities

$$4 = \delta + r \leq \mathrm{d}_R(\mathcal{C}) \leq \mu - \frac{\mu k}{n} + 1 = 4.$$

Therefore, the inequalities above are all equalities and $\mathcal{C}$ is an MRD code.

Example 24. Consider now the code $\mathcal{C}$ constructed in Example 19 equipped with the rank metric. In this case, combining the Singleton-like bound in (4) with the skew Roos bound for the rank metric of Theorem 22, we deduce that $\mathcal{C}$ is a $[14, 4]_{F/K}$ code with $F = \mathbb{F}_{2^7}$, $K = \mathbb{F}_2$ and whose minimum rank distance satisfies

$$5 = \delta + r \leq \mathrm{d}_R(\mathcal{C}) \leq \mu - \frac{\mu k}{n} + 1 = 6.$$

Hence, according to the two bounds, we have an MRD code or an almost MRD code (i.e. $\mathrm{d}_R(\mathcal{C}) = \mu - \frac{\mu k}{n}$), depending on the exact value of $\mathrm{d}_R(\mathcal{C})$. However, studying the set $T_\beta(g)$ more carefully, we can see that it also satisfy a skew Roos bound with $b = 0$, $s = 1$, $\delta' = 6$ and $r = 0$ (i.e. a skew BCH bound). Hence the code $\mathcal{C}$ is actually an MRD code.

Remark 25. It is very interesting to observe that the skew-cyclic code $\mathcal{C}$ considered in Examples 18 and 23 is not an MDS code, but an MRD code (with respect to the Singleton-like bound in (3)). This is quite surprising since for $[n, k]_{F/K}$ rank-metric codes such that $n \leq [F : K]$, i.e. when we need to consider the Singleton-like bound in (2), MRD codes are also MDS. In addition, we have by construction that $\mathcal{C} = \widehat{\mathcal{C}} \cap F^n$, i.e. $\mathcal{C}$ is a subfield subcode of a rank-metric code $\widehat{\mathcal{C}} \leq E^n$. It is possible to verify that $\widehat{\mathcal{C}}$ is not an MRD code (since it has codewords of rank weight equal to 6), even though $\mathcal{C}$ is MRD.

In Table 2, we analyze the same skew cyclic codes from Table 1, endowed with the rank metric. Observe that, in all the cases, we get almost MRD codes or MRD codes.

The behavior of the codes constructed with respect to the rank metric can be partially understood as follows. Let $T \subseteq C_n$ be a μ-closed set, i.e. such that $i \in T$ if and only if $i + \mu \in T$. This means that $T = T_\beta(g)$ for some $g \in \mathcal{R}$ and $T = T^1 \cup \cdots \cup T^\ell$, where $T^j \in C_n/\mu C_n$. Hence, we can just consider for each T^j a representative i_j belonging to $C_\mu = \{0, 1, \ldots, \mu - 1\}$. We denote this set by $T^F_\beta(g) := \{i_1, \ldots, i_\ell\}$.

Proposition 26. *Suppose that the defining set $T_\beta(g)$ satisfies a skew Roos bound as in Theorem 22 for some $\delta \geq 2$ and $r \geq 0$. Then the minimum rank distance of the code $\mathcal{C} = \mathcal{R}g$ satisfies $\delta + r \leq \mathrm{d}_R(\mathcal{C}) \leq |T^F_\beta(g)| + 1$. In particular, if $|T^F_\beta(g)| = \delta + r - 1$, then $\mathcal{C}$ is an MRD code.*

Proof. The first inequality is the skew Roos bound of Theorem 22. For the second inequality, we have that $T^F_\beta(g)$ is a system of representative for $T_\beta(g)$, which is its μ-closure. Therefore, $|T_\beta(g)| = \nu|T^F_\beta(g)|$ and $k = n - |T_\beta(g)| = \nu\mu - \nu|T^F_\beta(g)|$. Combining this equality with (4), we obtain

$$k = \nu\mu - \nu|T^F_\beta(g)| \leq \nu(\mu - d + 1),$$

from which we derive the desired inequality. The second statement follows directly. □

Remark 27. Proposition 26 translates the skew Roos bound and the Singleton-like bound in an arithmetic problem. Indeed, it essentially requires to find a defining set with a suitable cardinality and only working modulo n and μ to construct rank-metric codes whose minimum distance is upper and lower-bounded.

We can observe that in almost all the cases of Table 2 with $r = 1$, we get $|T^F_\beta(g)| = \delta + r - 1$, with the δ and the r provided. In the codes from the second and the fifth rows, we get $|T^F_\beta(g)| = \delta' + r' - 1$, with some different δ' and r' for which $T_\beta(g)$ satisfies the skew Roos bound.

Corollary 28. *Let $b, \delta', \mu, \nu, n, s$ be nonnegative integers such that $\mu, \nu \geq 1$, $2 \leq \delta' \leq \mu$, $n = \mu\nu$ and $(s, n) = 1$. Define $T := \{b, b + s, b + 2s, \ldots, b + (\delta' - 2)s\} \subseteq C_\mu$, where all the elements are taken modulo μ, and let $\bar{T}$ be its μ-closure in C_n. Then $\bar{T} = T_\beta(g)$ for some polynomial $g \in R = F[x; \sigma]$, such that the code $\mathcal{R}g$ is an $[n, n - \nu(\delta' - 1), \delta']_{F/K}$ MRD code.*

Proof. First, observe that $|T| = \delta' - 1$, i.e. all the elements $b + is \mod \mu$ are distinct, for $0 \leq i \leq \delta' - 2$. Indeed, if there are $0 \leq i \leq j \leq \delta' - 2$ such that $b + is \equiv b + js \mod \mu$, then we would have $(j - i)s \equiv 0 \mod \mu$. Since $(s, \mu) = 1$, this implies $(j - i) \equiv 0 \mod \mu$, which implies $i - j = 0$, due to the assumptions that $0 \leq j - i \leq \delta' - 2 \leq \mu - 2$. It is left to show that the μ-closure of T, that is $\bar{T}$, satisfies a skew Roos bound with $\delta = \delta'$ and $r = 0$. However, this is clear by construction, since for every $0 \leq i \leq \delta' - 2$ the equivalence class

of $b+is$ in $C_n/\mu C_n$ is contained in $\bar{T}$. In particular the set $\{b+is \mid 0 \leq i \leq \delta'-2\} \subseteq \bar{T}$ in C_n. We conclude the proof using Proposition 26. □

Example 29. Let us fix any triple of fields $K \subseteq F \subseteq E$ such that $[F:K] = \mu = 11$, and $[E:F] = \nu = 7$, and take the polynomial g such that $T_\beta^F(g) = \{0,1,2,3,5,6\}$. We can observe that the set $T_\beta(g)$ satisfies the skew Roos bound of Theorem 22 with $b=0$, $s=12$, $\delta=3$, $r=3$, $k_0=0$, $k_1=1$, $k_2=2$ and $k_3=5$. Hence, $\delta+r=6$ and $|T_\beta^F(g)|=6$, and by Proposition 26 the code $\mathcal{C}=\mathcal{R}g$ is a $[77,49,\mathrm{d}_R(\mathcal{C})]_{F/K}$ rank-metric code whose minimum distance satisfies $6 \leq \mathrm{d}_R(\mathcal{C}) \leq 7$.

At this point it is important to remark that in all the construction of MRD codes of Table 2, the codes satisfy also a skew Roos bound with $r=0$ and $\delta = |T_\beta^F(g)|+1$, that is they can be obtained using Corollary 28. Unfortunately, it does not seem trivial to construct MRD codes according to Proposition 26, different from the ones in Corollary 28. Indeed, this is not possible when μ is a prime number, as shown in the following result.

Proposition 30. *Let $s,b,\delta,k_0,\dots,k_r$ be integers such that $(s,n)=1$, $k_j < k_{j+1}$ for $0 \leq j \leq r-1$, $k_r - k_0 \leq \delta+r-2$, and $b+si+k_j \in T_\beta(g)$ for all $0 \leq i \leq \delta-2$ and $0 \leq j \leq r$. Moreover, assume that μ is a prime number. If $|T_\beta^F(g)| = \delta+r-1$, then $T_\beta(g)$ satisfies a BCH bound with $\delta' = \delta+r$.*

Proof. Up to replacing β with $\theta^b(\beta)$, it is enough to prove the statement when $b=0$. Let $A := \{k_0,\dots k_r\} \subseteq C_\mu$ and $B := \{0,s,\dots s(\delta-2)\} \subseteq C_\mu$. In this setting we have $T_\beta^F(g) \supseteq A+B$, where

$$A+B = \{a+b \mid a \in A, b \in B\}$$

and all the elements are taken modulo μ. First, we can suppose $\delta+r-1 < \mu$, otherwise we would get a trivial code. Moreover, we can also assume that $\delta > 2$ and $r \geq 1$, otherwise we have already a BCH bound. Combining the hypotheses and Cauchy-Davenport Theorem [13,15], we have the following equalities

$$|T_\beta^F(g)| = |A+B| = |A| + |B| - 1 = \delta + r - 1.$$

The pairs of sets (A,B) for which equality holds in the Cauchy-Davenport Theorem have been characterized by Vosper in [54]. Applying this result in our setting, i.e. when $|A| = \delta-1 > 1$, $|B| = r+1 > 1$ and $|A|+|B|-1 < \mu$, we get that $|A+B| = |A|+|B|-1$ if and only if A and B are representable as arithmetic progressions with the same common difference s' and clearly s' is coprime to μ. Hence also $A+B = T_\beta^F(g)$ is representable as an arithmetic progression with difference s', and this implies that $T_\beta(g)$ satisfies a BCH bound. □

7. Conclusions and open problems

In this paper, we provided a generalization of the Roos bound for skew cyclic codes in the Hamming and rank metric over a general field. The only requirement that we ask is to have a cyclic Galois extension of finite degree, but we do not require to work on finite fields. For the rank metric case, we also provide in Proposition 26 a way to arithmetically construct codes with a prescribed minimum rank distance, using the skew Roos bound of Theorem 22. Finally, we constructed some example of MDS codes and MRD codes over finite fields obtained using the skew Roos bounds of Theorems 13 and 22.

In the second part of Proposition 26, we suggest a way to construct MRD codes only using an arithmetic argument modulo μ and n. However, we could not come up with a general construction of MRD codes based on that, except for codes satisfying a skew Roos bound with parameters $\delta = |T^F_\beta(g)| + 1$ and $r = 0$. Hence we suggest the following open problem.

Problem 1. Is it possible to give a different systematic construction of MRD codes meeting (3) based on Proposition 26 that can not be obtained using Corollary 28, i.e. not satisfying any skew Roos bound with parameters $\delta = |T^F_\beta(g)| + 1$ and $r = 0$?

As shown in Proposition 30, the answer to this question is negative when μ is prime. However, the general case is still unclear.

References

[1] D. Augot, Generalization of Gabidulin codes over fields of rational functions, in: 21st International Symposium on Mathematical Theory of Networks and Systems (MTNS 2014), 2014.
[2] D. Augot, P. Loidreau, G. Robert, Rank metric and Gabidulin codes in characteristic zero, in: 2013 IEEE International Symposium on Information Theory, IEEE, 2013, pp. 509–513.
[3] D. Augot, P. Loidreau, G. Robert, Generalized Gabidulin codes over fields of any characteristic, Des. Codes Cryptogr. 86 (8) (2018) 1807–1848.
[4] R.C. Bose, D.K. Ray-Chaudhuri, Further results on error correcting binary group codes, Inf. Control 3 (3) (1960) 279–290.
[5] R.C. Bose, D.K. Ray-Chaudhuri, On a class of error correcting binary group codes, Inf. Control 3 (1) (1960) 68–79.
[6] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, in: Computational Algebra and Number Theory, London, 1993, J. Symb. Comput. 24 (3–4) (1997) 235–265.
[7] D. Boucher, W. Geiselmann, F. Ulmer, Skew-cyclic codes, Appl. Algebra Eng. Commun. Comput. 18 (4) (2007) 379–389.
[8] D. Boucher, F. Ulmer, Codes as modules over skew polynomial rings, in: IMA International Conference on Cryptography and Coding, Springer, 2009, pp. 38–55.
[9] D. Boucher, F. Ulmer, Coding with skew polynomial rings, J. Symb. Comput. 44 (12) (2009) 1644–1656.
[10] D. Boucher, F. Ulmer, Linear codes using skew polynomials with automorphisms and derivations, Des. Codes Cryptogr. 70 (3) (2014) 405–431.
[11] J. Bueso, J. Gómez-Torrecillas, A. Verschoren, Algorithmic Methods in Non-Commutative Algebra: Applications to Quantum Groups, Mathematical Modelling: Theory and Applications, Springer, 2003.
[12] G. Calis, O.O. Koyluoglu, A general construction for PMDS codes, IEEE Commun. Lett. 21 (3) (2017) 452–455.
[13] A.L.B. Cauchy, Recherches sur les nombres, J. Éc. Polytech. 9 (1813) 99–123.

[14] L. Chaussade, P. Loidreau, F. Ulmer, Skew codes of prescribed distance or rank, Des. Codes Cryptogr. 50 (3) (2009) 267–284.
[15] H. Davenport, On the addition of residue classes, J. Lond. Math. Soc. 10 (1935) 30–32.
[16] J. Delenclos, A. Leroy, Noncommutative symmetric functions and w-polynomials, J. Algebra Appl. 06 (05) (2007) 815–837.
[17] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, J. Comb. Theory, Ser. A 25 (3) (1978) 226–241.
[18] T. Etzion, A. Wachter-Zeh, Vector network coding based on subspace codes outperforms scalar linear network coding, IEEE Trans. Inf. Theory 64 (4) (2018) 2460–2473.
[19] G.D. Forney Jr., Convolutional codes I: algebraic structure, IEEE Trans. Inf. Theory 16 (6) (1970) 720–738.
[20] E.M. Gabidulin, Theory of codes with maximum rank distance, Probl. Pereda. Inf. 21 (1) (1985) 3–16.
[21] E.M. Gabidulin, A. Paramonov, O. Tretjakov, Ideals over a non-commutative ring and their application in cryptology, in: Advances in Cryptology – EUROCRYPT'91, Springer, 1991, pp. 482–489.
[22] P. Gaborit, G. Murat, O. Ruatta, G. Zémor, Low rank parity check codes and their application to cryptography, in: Workshop on Coding and Cryptography (WCC), 2013.
[23] H. Gluesing-Luerssen, Skew-polynomial rings and skew-cyclic codes, preprint, arXiv:1902.03516, 2019.
[24] J. Gómez-Torrecillas, F.J. Lobillo, G. Navaro, Computing free distances of idempotent convolutional codes, in: Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation, ISSAC '18, ACM, New York, NY, USA, 2018, pp. 175–182.
[25] J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, A new perspective of cyclicity in convolutional codes, IEEE Trans. Inf. Theory 62 (5) (2016) 2702–2706.
[26] J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, A Sugiyama-like decoding algorithm for convolutional codes, IEEE Trans. Inf. Theory 63 (10) (2017) 6216–6226.
[27] J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, Peterson–Gorenstein–Zierler algorithm for skew RS codes, Linear Multilinear Algebra 66 (3) (2018) 469–487.
[28] J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, A. Neri, Hartmann-Tzeng bound and skew cyclic codes of designed Hamming distance, Finite Fields Appl. 50 (2018) 84–112.
[29] J. Gómez-Torrecillas, F. Lobillo, G. Navarro, Cyclic distances of idempotent convolutional codes, J. Symb. Comput. (2019).
[30] C.R. Hartmann, K.K. Tzeng, Generalizations of the BCH bound, Inf. Control 20 (5) (1972) 489–498.
[31] A. Hocquenghem, Codes correcteurs d'erreurs, Chiffres 2 (2) (1959) 147–156.
[32] N. Jacobson, Finite-Dimensional Division Algebras over Fields, Springer, Berlin, 1996.
[33] A. Kshevetskiy, E.M. Gabidulin, The new construction of rank codes, in: Proceedings of the International Symposium on Information Theory (ISIT) 2005, Sept 2005, pp. 2105–2108.
[34] T.-Y. Lam, A General Theory of Vandermonde Matrices, Center for Pure and Applied Mathematics, University of California, Berkeley, 1985.
[35] T.-Y. Lam, A. Leroy, Vandermonde and Wronskian matrices over division rings, J. Algebra 119 (2) (1988) 308–336.
[36] S. Lang, Algebra, revised third edition, Graduate Texts in Mathematics, vol. 211, Springer, 2002.
[37] A. Leroy, Noncommutative polynomial maps, J. Algebra Appl. 11 (04) (2012) 1250076.
[38] S. Liu, F. Manganiello, F.R. Kschischang, Construction and decoding of generalized skew-evaluation codes, in: 2015 IEEE 14th Canadian Workshop on Information Theory (CWIT), IEEE, 2015, pp. 9–13.
[39] U. Martínez-Peñas, On the roots and minimum rank distance of skew cyclic codes, Des. Codes Cryptogr. 83 (3) (2017) 639–660.
[40] A. Neri, A.-L. Horlemann-Trautmann, Random construction of partial MDS codes, Des. Codes Cryptogr. 88 (4) (2020) 711–725.
[41] O. Ore, Theory of non-commutative polynomials, Ann. Math. 34 (3) (1933) 480–508.
[42] R. Overbeck, Structural attacks for public key cryptosystems based on Gabidulin codes, J. Cryptol. 21 (2) (2008) 280–301.
[43] A.S. Rawat, O.O. Koyluoglu, N. Silberstein, S. Vishwanath, Optimal locally repairable and secure codes for distributed storage systems, IEEE Trans. Inf. Theory 60 (1) (2013) 212–236.
[44] C. Roos, A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound, J. Comb. Theory, Ser. A 33 (2) (1982) 229–232.
[45] C. Roos, A new lower bound for the minimum distance of a cyclic code, IEEE Trans. Inf. Theory 29 (3) (1983) 330–332.

[46] R.M. Roth, Maximum-rank array codes and their application to crisscross error correction, IEEE Trans. Inf. Theory 37 (2) (mar 1991) 328–336.
[47] R.M. Roth, Tensor codes for the rank metric, IEEE Trans. Inf. Theory 42 (6) (1996) 2146–2157.
[48] D. Silva, F.R. Kschischang, Universal secure network coding via rank-metric codes, IEEE Trans. Inf. Theory 57 (2) (2011) 1124–1135.
[49] D. Silva, F.R. Kschischang, R. Koetter, A rank-metric approach to error control in random network coding, IEEE Trans. Inf. Theory 54 (9) (2008) 3951–3967.
[50] R. Singleton, Maximum distance q-nary codes, IEEE Trans. Inf. Theory 10 (2) (1964) 116–118.
[51] W. Stein, et al., Sage mathematics software (Version 8.9), The Sage Development Team, http://www.sagemath.org, 2019.
[52] B.L. van der Waerden, Modern Algebra, vol. I, Frederick Ungar Publishing Co., 1949.
[53] J.H. Van Lint, R.M. Wilson, On the minimum distance of cyclic codes, IEEE Trans. Inf. Theory 32 (1) (January 1986) 23–40.
[54] A.G. Vosper, The critical pairs of subsets of a group of prime order, J. Lond. Math. Soc. 1 (2) (1956) 200–205.