A Decoding Algorithm for Skew Cyclic Generalized Skew Reed Solomon Codes

Delphine Boucher, Kayodé Epiphane Nouetowa

A Decoding Algorithm for Skew Cyclic Generalized Skew Reed Solomon Codes

Delphine Boucher et Kayodé Epiphane Nouetowa *

January 15, 2025

Abstract

In this note we propose a decoding algorithm in the skew metric for a family of skew cyclic generalized skew Reed-Solomon codes which we prove to be MDS for the skew metric.

1 Introduction

Cyclic Reed-Solomon codes over finite fields are a family of well known codes which are cyclic evaluation codes, MDS for the Hamming metric. Their decoding in the Hamming metric has been widely studied (see [5] for an overview). By adding an automorphism θ to the ground field, cyclic codes can be generalized to θ-cyclic or skew cyclic codes while (generalized) Reed-Solomon codes can be extended to (generalized) skew Reed-Solomon codes. In this setting the Hamming metric can also be generalized to the skew metric, and decoding algorithms for (generalized) skew Reed-Solomon codes in the skew metric can be adapted ([4, 11]). Furthermore, recently, an iterative decoding algorithm has been settled for skew cyclic codes in the Hamming metric ([12]), but to our knowledge, there was no decoding algorithm in the skew metric for skew cyclic codes up to now.

In what follows we consider a new family of codes that we call skew cyclic generalized skew Reed-Solomon codes and we propose a decoding algorithm in the skew metric which is inspired by [5]. When θ is the identity we recover cyclic Reed-Solomon codes and their decoding algorithm in the Hamming metric.

In Section 2 we recall basic facts on skew polynomials, skew cyclic codes, the skew metric and generalized skew Reed-Solomon codes. In Section 3 we define the family of skew cyclic generalized skew Reed-Solomon codes and prove that they are MDS for the skew metric. In Section 4 we are concerned with a generalized multi-evaluation map whose inverse is a generalized multi-evaluation map and which can be computed efficiently. In Section 5 we derive a decoding algorithm for our family in the skew metric.

2 Generalities

Consider a power of a prime number q, an integer m, a finite field $\mathbb{F}_{q^m}$ and an automorphism θ over $\mathbb{F}_{q^m}$. The ring $R = \mathbb{F}_{q^m}[X;\theta]$ is defined on the set $\{\sum_{i=0}^{n} a_i X^i | n \in \mathbb{N}, a_i \in \mathbb{F}_{q^m}\}$

*Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France

where the addition is the usual addition of polynomials and the multiplication is defined by the rule : for a in $\mathbb{F}_{q^m}$

$$X \cdot a = \theta(a)\, X. \tag{1}$$

The ring R is called a skew polynomial ring or Ore ring and its elements are skew polynomials. When θ is not the identity, the ring R is not commutative, it is a left and right Euclidean ring whose left and right ideals are principal. Left and right gcd and lcm exist in R and can be computed using the left and right Euclidean algorithms. In what follows we will assume that least common left multiples (lclm) of skew polynomials are necessarily *monic* skew polynomials.

Skew cyclic codes were first introduced in [2] as codes which generalize cyclic codes. Skew-Reed Solomon codes were introduced later in [3] and [10] while generalized skew Reed-Solomon codes were introduced in [9].

Definition 1 *A* θ**-cyclic** *(or skew cyclic) code of length n in $\mathbb{N}^*$ is a left $R-$submodule $Rg/R(X^n-1) \subset R/R(X^n-1)$ where g is a monic right divisor of X^n-1. The skew polynomial g is called* **skew generator** *of the code and the code is denoted $(g)_n^\theta$.*

Definition 2 *([7, page 310]) For f in R and a in A, the* **(right) remainder evaluation** *of f at a is denoted $f(a)$ and is defined as the remainder of the right division of f by $X-a$. If $f(a)=0$, then a is a* **right root** *of f.*

If $f = \sum_i f_i X^i \in R$ and $a \in \mathbb{F}_{q^m}$ then $f(a) = \sum_i f_i N_i^\theta(a)$ (see [3, Lemma 1] or [7, Proposition 2.9]) where $N_i^\theta(a) = a\theta(a)\dots\theta^{i-1}(a)$.

Consider for $n \in \mathbb{N}^*$, $\boldsymbol{\alpha} = (\alpha_0, \dots, \alpha_{n-1})$ in $\mathbb{F}_{q^m}^n$. The **Vandermonde matrix** of $\boldsymbol{\alpha}$ is defined as $V_n^\theta(\boldsymbol{\alpha}) = (N_i^\theta(\alpha_j))_{0\le i,j\le n-1}$.

Theorem 1 *([7, page 326]) Consider $n \in \mathbb{N}^*$, $\boldsymbol{\alpha} = (\alpha_0, \dots, \alpha_{n-1}) \in \mathbb{F}_{q^m}^n$ and*

$g = \mathrm{lclm}_{0\le i\le n-1}(X-\alpha_i)$ in R. The degree of g is $\deg(g) = \mathrm{rank}\left(\mathrm{V}_\mathrm{n}^\theta(\boldsymbol{\alpha})\right)$. *If $\deg(g) = n$ then we say that $\boldsymbol{\alpha}$ is* P^θ**-independent** *or P-independent.*

For k in $\mathbb{N}$, we denote $R_{<k}$ the set of skew polynomials of degree less than k.

Definition 3 *([4, Lemma 1, Proposition 1]) Consider $n \in \mathbb{N}^*$, $k \in \{0\dots, n-1\}$, $\boldsymbol{\xi} = (\xi_0, \dots, \xi_{n-1})$ in $\mathbb{F}_{q^m}^n$ such that $\boldsymbol{\xi}$ is P^θ-independent and $\boldsymbol{v} = (v_0, \dots, v_{n-1})$ in $(\mathbb{F}_{q^m}^*)^n$. The* **generalized skew Reed-Solomon code** *of length n, dimension k, support $\boldsymbol{\xi}$ and multiplicator $\boldsymbol{v}$ is defined as*

$$\mathcal{GSRS}_{n,k}^\theta(\boldsymbol{\xi}, \boldsymbol{v}) = \{(f(\xi_0)v_0, \dots, f(\xi_{n-1})v_{n-1}) \mid f \in R_{<k}\}.$$

If $v_0 = \dots = v_{n-1} = 1$, then the code is a **skew Reed-Solomon code** *and denoted as*

$$\mathcal{SRS}_{n,k}^\theta(\boldsymbol{\xi}) = \{(f(\xi_0), \dots, f(\xi_{n-1})) \mid f \in R_{<k}\}.$$

We now recall the definition of the skew metric.

Definition 4 *([7]) The* $\theta-$**conjugacy class** *of an element $a \in \mathbb{F}_{q^m}$ is the set of all its* **conjugates**

$$a^c := \theta(c)ac^{-1}$$

where c is taken over $\mathbb{F}_{q^m}^*$.

Definition 5 *([10, 4]) Consider $n \in \mathbb{N}^*$, $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_{n-1})$ in $\mathbb{F}_{q^m}^n$ such that $\boldsymbol{\alpha}$ is P^θ-independent. Consider $\boldsymbol{v} = (v_0, \ldots, v_{n-1})$ in $\mathbb{F}_{q^m}^n$. The* **skew weight** *of $\boldsymbol{v}$ associated to $(\theta, \boldsymbol{\alpha})$ is defined by :*

$$\begin{array}{rcl} w_{\boldsymbol{\alpha}}^\theta(\boldsymbol{v}) & = & \deg \operatorname{lclm}_{v_i \neq 0}(X - \alpha_i^{v_i}) \\ & = & n - \deg(\operatorname{gcrd}(P, F)) \end{array} \tag{2}$$

where $P = \operatorname{lclm}_{0 \leq i \leq n-1}(X - \alpha_i)$ and F in $R_{<n}$ is such that $\forall i \in \{0, \ldots, n-1\}, F(\alpha_i) = v_i$.

The following theorem is a consequence of [10, Theorem 1], Theorem 1 or [4].

Theorem 2 *Consider $n \in \mathbb{N}^*$, $k \in \{0 \ldots, n-1\}$, $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_{n-1})$ in $\mathbb{F}_{q^m}^n$ such that $\boldsymbol{\alpha}$ is P^θ-independent and $\boldsymbol{v} = (v_0, \ldots, v_{n-1})$ in $(\mathbb{F}_{q^m}^*)^n$. Consider for i in $\{0, \ldots, n-1\}$, $\xi_i = \alpha_i^{v_i}$ and assume that $\boldsymbol{\xi} = (\xi_0, \ldots, \xi_{n-1})$ is P^θ-independent. The generalized skew Reed-Solomon code $\mathcal{GSRS}_{n,k}^\theta(\boldsymbol{\xi}, \boldsymbol{v})$ is MDS for the skew metric associated to $(\theta, \boldsymbol{\alpha})$.*

Proof. According to Theorem 1 of [10], the skew Reed-Solomon code $\mathcal{SRS}_{n,k}^\theta(\boldsymbol{\xi})$ is MDS for the skew metric associated to $(\theta, \boldsymbol{\xi})$. Consider c non-zero in $\mathcal{GSRS}_{n,k}^\theta(\boldsymbol{\xi}, \boldsymbol{v})$, then $\tilde{c} = (c_0/v_0, \ldots, c_{n-1}/v_{n-1})$ belongs to $\mathcal{SRS}_{n,k}^\theta(\boldsymbol{\xi})$. We have $w_{\boldsymbol{\alpha}}^\theta(c) = \deg \operatorname{lclm}_{c_i \neq 0}(X - \alpha_i^{c_i}) = \deg \operatorname{lclm}_{c_i \neq 0}(X - \xi_i^{c_i/v_i}) = w_{\boldsymbol{\xi}}^\theta(\tilde{c}) \geq n - k + 1$. ∎

3 Skew cyclic generalized skew Reed-Solomon codes

We know consider a new family of codes which are MDS for the skew metric associated to (θ, α) and which belong to a family of codes which are MDS for the Hamming metric (see [3, Theorem 4, Hamming condition 2]).

Consider n in $\mathbb{N}^*$. We define the set $\mathcal{A}_n$ as the set of elements α of $\mathbb{F}_{q^m}$ such that $\operatorname{lclm}_{0 \leq i \leq n-1}(X - N_i^\theta(\alpha))$ and $\operatorname{lclm}_{0 \leq i \leq n-1}(X - N_i^\theta(\frac{1}{\alpha}))$ are equal to $X^n - 1$.

In what follows, we assume that the automorphism θ is defined by $\theta : a \mapsto a^q$ and that n is a non-zero multiple of the order m of the automorphism θ. It belongs necessarily to $\{m, 2m, 3m, \ldots, (q-1)m\}$.

Lemma 1 *Consider α in $\mathcal{A}_n$, for i in $\{0, \ldots, n-1\}$, $\alpha_i = N_i^\theta(\alpha)$, $\xi_i = \alpha_i^{v_i}$ where $v = \operatorname{lclm}_{1 \leq i \leq n-1}(X - \frac{1}{\alpha_i}) = \sum_{\ell=0}^{n-1} v_\ell X^\ell$. Then $\boldsymbol{\xi} = (\xi_0, \ldots, \xi_{n-1})$ is P^θ-independent.*

Proof. We first notice that $\boldsymbol{\alpha}$ is P^θ-independent because $\operatorname{lclm}_{0 \leq i \leq n-1}(X - \alpha_i)$ is equal to $X^n - 1$ and has degree n (see Theorem 1). Furthermore, as $\operatorname{lclm}_{0 \leq i \leq n-1}(X - N_i^\theta(1/\alpha)) = X^n - 1$ is also of degree n, the rank of the square $n \times n$ matrix $(N_i^\theta(N_j^\theta(1/\alpha)))$ is equal to n. Using the fact that $N_n^\theta(\alpha) = 1$, we have $N_i^\theta(N_j^\theta(1/\alpha)) = N_{n-j}^{\theta^{-1}}(\theta^{-1}(N_i^\theta(\alpha)))$ and we get that $\theta^{-1}(\boldsymbol{\alpha})$ is $P^{\theta^{-1}}$-independent. As for i in $\{0, \ldots, n-2\}$, $v(N_{i+1}^\theta(1/\alpha)) = 0 = \sum_{j=0}^{n-1} N_j^\theta(N_{i+1}^\theta(\frac{1}{\alpha}))v_j = \sum_{j=0}^{n-1} \theta^{-1}(\alpha_j) N_{n-i-2}^{\theta^{-1}}(\theta^{-2}(\alpha_j))v_j$, we get that $\boldsymbol{v}$ belongs to the dual of $C = \mathcal{GSRS}_{n,n-1}^{\theta^{-1}}(\theta^{-2}(\boldsymbol{\alpha}), \theta^{-1}(\boldsymbol{\alpha}))$. Furthermore for i in $\{0, \ldots, n-1\}$, we have $\theta^{-2}(\alpha_i) = \theta^{-1}(\alpha_i)\frac{\theta^{-1}(\theta^{-1}(\alpha_i))}{\theta^{-1}(\alpha_i)}$. Therefore we can apply Theorem 2, and get that the code C is MDS for the skew metric associated to $(\theta^{-1}, \theta^{-1}(\boldsymbol{\alpha}))$. Following the same idea as in the first part of the proof of [11, Theorem 4], we get that the dual of C is a 1-dimensional code

MDS for the skew metric associated to $(\theta, \boldsymbol{\alpha})$, which proves that $w^{\theta}_{\boldsymbol{\alpha}}(\boldsymbol{v}) = n$. As $w^{\theta}_{\boldsymbol{\alpha}}(\boldsymbol{v}) = \deg \operatorname{lclm}_{0\le i\le n-1}(X-\xi_i)$, we get that $\boldsymbol{\xi}$ is P^{θ}-independent. ∎

Theorem 3 *Consider α in $\mathcal{A}_n$, for i in $\{0,\ldots,n-1\}$, $\alpha_i = N_i^{\theta}(\alpha)$, $\xi_i = \alpha_i^{v_i}$ where $v = \operatorname{lclm}_{1\le i\le n-1}(X-\frac{1}{\alpha_i}) = \sum_{\ell=0}^{n-1} v_\ell X^\ell$ and $g = \operatorname{lclm}_{1\le i\le 2t}\left(X-\frac{1}{\alpha_{n-i}}\right)$. The skew cyclic code $\mathcal{C}$ of length n and skew generator polynomial g is equal to the generalized skew Reed-Solomon code with length n, dimension $n-2t$, support $\boldsymbol{\xi}$ and multiplicator $\boldsymbol{v}$:*

$$\mathcal{C} = (g)^{\theta}_n = \mathcal{GSRS}^{\theta}_{n,n-2t}(\boldsymbol{\xi}, \boldsymbol{v}).$$

Furthermore $\mathcal{C}$ is MDS for the skew metric associated to $(\theta, \boldsymbol{\alpha})$.

Proof.

- As α belongs to $\mathcal{A}_n$, $\left(\frac{1}{\alpha_{n-2t}},\ldots,\frac{1}{\alpha_{n-1}}\right)$ is P^{θ}-independent. Therefore, $\dim(\mathcal{C}) = n - \deg(g) = n-2t$. A parity-check matrix of $\mathcal{C}$ is

  $$H = (N_j^{\theta}(\beta_{i+1}))_{0\le i\le 2t-1, 0\le j\le n-1}$$

  where for i in $\{0,\ldots,n-1\}$, $\beta_i = \frac{1}{\alpha_{n-i}}$.

- According to Lemma 1, $\boldsymbol{\xi} = (\xi_0,\ldots,\xi_{n-1})$ is P^{θ}-independent. Therefore, the code $\mathcal{GSRS}^{\theta}_{n,n-2t}(\boldsymbol{\xi}, \boldsymbol{v})$ is MDS for the skew metric associated to $(\theta, \boldsymbol{\alpha})$ according to Theorem 2. A generator matrix of $\mathcal{GSRS}^{\theta}_{n,n-2t}(\boldsymbol{\xi}, \boldsymbol{v})$ is

  $$G = (N_i^{\theta}(\xi_j)v_j)_{0\le i\le k-1, 0\le j\le n-1}.$$

  We have, for $i \in \{0,\ldots,2t-1\}$ and $j \in \{0,\ldots,k-1\}$,

  $$\begin{aligned}
  &\sum_{\ell=0}^{n-1} N_\ell^{\theta}(\beta_{i+1}) N_j^{\theta}(\xi_\ell) v_\ell = \sum_{\ell=0}^{n-1} N_\ell^{\theta}(\beta_{i+1}) N_j^{\theta}(\alpha_\ell)\theta^j(v_\ell)\\
  &= \sum_{\ell=0}^{n-1} N_\ell^{\theta}(\beta_{i+1}) N_\ell^{\theta}(\alpha_j)\theta^j(v_\ell)\\
  &= \sum_{\ell=0}^{n-1} N_\ell^{\theta}(\beta_{i+1})\theta^j(N_\ell^{\theta}(\beta_j)v_\ell)\\
  &= \theta^j\left(\sum_{\ell=0}^{n-1} N_\ell^{\theta}(\theta^{-j}(\beta_{i+1})\beta_j)v_\ell\right)\\
  &= \theta^j\left(\sum_{\ell=0}^{n-1} N_\ell^{\theta}(\theta^{-j}(\beta_{i+1})\beta_j)v_\ell\right)\\
  &= \theta^j\left(\sum_{\ell=0}^{n-1} N_\ell^{\theta}(\beta_{i+j+1})v_\ell\right) = 0
  \end{aligned}$$

  because $1 \le i+j+1 \le n-1$ and $v(\beta_{i+j+1}) = 0$. Therefore $H \times^t G = 0$ and $\mathcal{C} = \mathcal{GSRS}^{\theta}_{n,n-2t}(\boldsymbol{\xi}, \boldsymbol{v})$.

■

Remark 1 *If $\theta = id$, then the elements of $\mathcal{A}_n$ are the n-th roots of unity, $v = \prod_{i=1}^{n-1}\left(X - \frac{1}{\alpha^i}\right) = \sum_{i=0}^{n-1} X^i$ and $\xi_i = \alpha_i = \alpha^i$. Therefore $\mathcal{C}$ is the cyclic Reed-Solomon code $\{(f(1), f(\alpha)\ldots, f(\alpha^{n-1})) \mid f \in R_{<k}\}$ with generator polynomial $g = \prod_{i=1}^{2t}\left(X - \frac{1}{\alpha^{n-i}}\right)$.*

4 Interpolation and multi-evaluation.

We consider for $\boldsymbol{\xi}$ in $\mathbb{F}_{q^m}^n$ P^θ-independent and $\boldsymbol{v}$ in $(\mathbb{F}_{q^m}^*)^n$ the following generalized multi-evaluation map:

$$\mathcal{F}_{\boldsymbol{\xi},\boldsymbol{v}} : \left\{ \begin{array}{ccc} \mathbb{F}_{q^m}^n & \to & \mathbb{F}_{q^m}^n \\ (a_0, \ldots, a_{n-1}) & \mapsto & (f(\xi_0)v_0, \ldots, f(\xi_{n-1})v_{n-1}) \end{array} \right.$$

where $f = \sum_{i=0}^{n-1} a_i X^i \in R$. Computing the inverse of $\mathcal{F}_{\boldsymbol{\xi},\mathbf{1}}$ amounts to computing an interpolation polynomial (see [11, Appendix B], [13] or [1]). In what follows we prove that for special values of $\boldsymbol{\xi}$ and $\boldsymbol{v}$, the inverse map of $\mathcal{F}_{\boldsymbol{\xi},\boldsymbol{v}}$ is also a generalized multi-evaluation map.

4.1 Inverse map in a particular case.

Theorem 4 *Consider α in $\mathcal{A}_n$, for i in $\{0, \ldots, n-1\}$, $\alpha_i = N_i^\theta(\alpha)$, $\zeta_i = \frac{1}{\alpha_i}$, $\xi_i = \alpha_i^{v_i}$, $w_i = 1/\theta^i(v(1))$ where $v = \mathrm{lclm}_{1\le i\le n-1}(X - \frac{1}{\alpha_i}) = \sum_{\ell=0}^{n-1} v_\ell X^\ell$. The application $\mathcal{F}_{\boldsymbol{\xi},\boldsymbol{v}}$ is invertible and its inverse is the application $\mathcal{F}_{\boldsymbol{\zeta},\boldsymbol{w}}$.*

Proof. As $(1/\alpha_0, \ldots, 1/\alpha_{n-1})$ is P^θ-independent, $X - 1/\alpha_0 = X - 1$ does not divide $\mathrm{lclm}_{1\le i\le n-1}(X - \frac{1}{\alpha_i}) = v$ and $v(1)$ is non-zero. The applications $\mathcal{F}_{\boldsymbol{\xi},\boldsymbol{v}}$ and $\mathcal{F}_{\boldsymbol{\zeta},\boldsymbol{w}}$ are linear with respective matrices $(N_i^\theta(\xi_j)v_j)_{0\le i,j\le n-1}$ and $(N_i^\theta(\zeta_j)w_j)_{0\le i,j\le n-1}$ whose product is the identity matrix.

Namely consider $i,j \in \{0,\ldots,n-1\}$, we have $\sum_{\ell=0}^{n-1} N_i^\theta(\xi_\ell) v_\ell N_\ell^\theta(\zeta_j) w_j =$

$$\begin{aligned}
&= \sum_{\ell=0}^{n-1} N_i^\theta(N_\ell^\theta(\alpha))\theta^i(v_\ell) N_j^\theta(N_\ell^\theta(1/\alpha)) w_j \\
&= \sum_{\ell=0}^{n-1} N_\ell^\theta(N_i^\theta(\alpha) N_j^\theta(1/\alpha))\theta^i(v_\ell) w_j \\
&= \theta^i\left(\sum_{\ell=0}^{n-1} v_\ell N_\ell^\theta(\theta^{-i}(N_i^\theta(\alpha)/N_j^\theta(\alpha)))\right) w_j \\
&= \begin{cases} \theta^i(v(\frac{1}{\alpha_{j-i}}))w_j & \text{if } j \geq i \\ \theta^i(v(\frac{1}{\alpha_{n+j-i}}))w_j & \text{if } j < i \end{cases} \\
&= \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}.
\end{aligned}$$

We conclude that $\mathcal{F}_{\boldsymbol{\xi},\boldsymbol{v}}^{-1} = \mathcal{F}_{\boldsymbol{\zeta},\boldsymbol{w}}$. ∎

Remark 2 *If θ is the identity, then $v(1) = n$ and for $i \in \{0,\ldots,n-1\}$, $\zeta_i = \alpha^{-i}$, $w_i = \frac{1}{n}$. We get the classical Fourier transform and its inverse.*

4.2 Fast multi-evaluation.

We now adapt classical techniques to the skew polynomial setting (see [13, 14, 8, 1]) to compute $(f(\gamma_0),\ldots,f(\gamma_{n-1}))$ for $(\gamma_0,\ldots,\gamma_{n-1})$ in $\mathbb{F}_{q^m}^n$ P^θ-independent and n a power of 2 (see Algorithms 1 and 2). Consider for $0 \leq i \leq \kappa = \log_2(n)$ and $0 \leq j < 2^{\kappa-i}$, the skew polynomial $M_{i,j} = \mathrm{lclm}_{0\leq\ell<2^i}(X - \gamma_{j\times 2^i+\ell})$. We have

$$M_{i+1,j} = \mathrm{lclm}(M_{i,2j}, M_{i,2j+1}). \tag{3}$$

From the subproducts $M_{i,j}$, we compute $f(\gamma_0),\ldots,f(\gamma_{n-1})$ recursively by noticing that for i in $\{0,\ldots,n/2-1\}$, $f(\gamma_i) = (f \bmod_{\mathrm{r}} M_{\kappa-1,0})(\gamma_i)$ and $f(\gamma_{i+n/2}) = (f \bmod_{\mathrm{r}} M_{\kappa-1,1})(\gamma_{i+n/2})$ where $\bmod_{\mathrm{r}}$ means remainder in the division on the right. Now, in (3), the lclm computation can be replaced by a product. Namely, according to [8, Theorem 3.6 (2)], the expression given in (3) can be computed thanks to the following product

$$M_{i+1,j} = \tilde{M}_{i,2j} \cdot M_{i,2j+1}$$

where

$$\tilde{M}_{i,2j} = \mathrm{lclm}_{0\leq\ell<2^i}(X - \tilde{\gamma}_{2j\times 2^i+\ell})$$

with

$$\tilde{\gamma}_{2j\times 2^i+\ell} = \gamma_{2j\times 2^i+\ell} \times \theta(M_{i,2j+1}(\gamma_{2j\times 2^i+\ell}))/M_{i,2j+1}(\gamma_{2j\times 2^i+\ell}).$$

Algorithm 1: `FastLCLM`

Input: $\boldsymbol{\gamma} = (\gamma_0, \ldots, \gamma_{n-1}) \in \mathbb{F}_{q^m}^n$, P^θ-independent
Output: $\mathrm{lclm}_{0 \le i \le n-1}(X - \gamma_i)$.

1 **if** $n = 1$ **then**
2 return $X - \gamma_0$
3 $g = \texttt{FastLCLM}((\gamma_{n/2}, \ldots, \gamma_{n-1}))$
4 $\eta = \texttt{FastME}(g, (\gamma_0, \ldots, \gamma_{n/2-1}))$
5 $\tilde{\gamma} = (\gamma_i \times \theta(\eta_i)/\eta_i)_{i=0,\ldots,n/2-1}$
6 $f = \texttt{FastLCLM}((\tilde{\gamma_0}, \ldots, \tilde{\gamma}_{n/2-1}))$
7 return $f \cdot g$

Algorithm 2: `FastME`

Input: $\boldsymbol{\gamma} = (\gamma_0, \ldots, \gamma_{n-1}) \in \mathbb{F}_{q^m}^n$, P^θ-independent and $f \in R$.
Output: $(f(\gamma_0), \ldots, f(\gamma_{n-1}))$.

1 **if** $n = 1$ **then**
2 return $[f(\gamma_0)]$
3 $g_1 \leftarrow \texttt{FastLCLM}((\gamma_0, \ldots, \gamma_{n/2-1}))$
4 $g_2 \leftarrow \texttt{FastLCLM}((\gamma_{n/2}, \ldots, \gamma_{n-1}))$
5 $r_1 \leftarrow f \bmod_{\mathrm{r}} g_1$
6 $r_2 \leftarrow f \bmod_{\mathrm{r}} g_2$
7 $R_1 \leftarrow \texttt{FastME}(r_1, (\gamma_0, \ldots, \gamma_{n/2-1}))$
8 $R_2 \leftarrow \texttt{FastME}(r_2, (\gamma_{n/2}, \ldots, \gamma_{n-1}))$
9 return $R_1 + R_2$

5 A decoding algorithm in the skew metric.

Consider α in $\mathcal{A}_n$, for i in $\{0, \ldots, n-1\}$, $\alpha_i = N_i^\theta(\alpha)$, $\xi_i = \alpha_i^{v_i}$ where $v = \mathrm{lclm}_{1 \le i \le n-1}\left(X - \frac{1}{\alpha_i}\right) = \sum_{\ell=0}^{n-1} v_\ell X^\ell$.

Consider the skew cyclic code $\mathcal{C} = (g)_n^\theta$ of length n and skew generator polynomial

$$g = \mathrm{lclm}_{1 \le i \le 2t}\left(X - \frac{1}{\alpha_{n-i}}\right).$$

According to Theorem 3, the code $\mathcal{C}$ is also a generalized skew Reed-Solomon code:

$$\mathcal{C} = \mathcal{GSRS}_{n,n-2t}^\theta(\boldsymbol{\xi}, \boldsymbol{v})$$

which is MDS for the skew metric associated to $(\theta, \boldsymbol{\alpha})$.

The aim of this section is to design a decoding algorithm for the code $\mathcal{C}$ in the skew metric associated to $(\theta, \boldsymbol{\alpha})$. A first solution consists in decoding in $\mathcal{SRS}_{n,n-2t}^\theta(\boldsymbol{\xi})$ with the skew metric associated to $(\theta, \boldsymbol{\xi})$ (see Theorem 2) by using [4] or [11]. In what follows we design a new decoding algorithm which exploits the θ-cyclicity of the code. Consider

$$\boldsymbol{u} = \boldsymbol{c} + \boldsymbol{e} \tag{4}$$

where $\boldsymbol{c}$ belongs to $\mathcal{C} = (g)_n^\theta = \mathcal{GSRS}^\theta_{n,n-2t}(\boldsymbol{\xi}, \boldsymbol{v})$ and $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ satisfies $w^\theta_{\boldsymbol{\alpha}}(\boldsymbol{e}) = s \leq t$.

Consider the evaluation polynomial f in $R_{<k}$ such that

$$\forall i = 0, \ldots, n-1, f(\xi_i)v_i = c_i.$$

We want to recover the evaluation polynomial f from $\boldsymbol{u}$. We define the skew polynomial f_u in $R_{<n}$ such that $f_u(\xi_i)v_i = u_i$, for $i = 0, \ldots, n-1$ and the skew polynomial E in $R_{<n}$ such that $v_i E(\xi_i) = e_i$ for $i = 0, \ldots, n-1$. We have

$$f_u = f + E.$$

The skew localisator polynomial σ is defined as

$$\sigma = \mathrm{lclm}_{i \in I}(X - \alpha_i^{e_i})$$

where $I = \{i \in \{0, \ldots, n-1\} \mid e_i \neq 0\}$. We recall that its degree is equal to $s = w^\theta_{\boldsymbol{\alpha}}(\boldsymbol{e})$.

5.1 The reciprocal of the skew localisator polynomial

Recall that the **reciprocal of a skew polynomial** h non-zero in R is

$$h^* = \sum_{i=0}^{\deg(h)} \theta^{\deg(h)-i}(h_i)X^i.$$

We also recall (see [12, Lemma 1]) that if the constant term of h is non-zero then $(h^*)^* = \theta^{\deg(h)}(h)$ and if $f \in R$, then $(h \cdot f)^* = \theta^{\deg(h)}(f^*) \cdot h^*$.

Lemma 2 *Consider $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^n$ P^θ-independent, $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ and $\sigma = \mathrm{lclm}_{e_i \neq 0}(X - \alpha_i^{e_i})$ with degree s. We have $\deg(\sigma^*) = \deg(\sigma) = s$ and $\sigma = (\theta^{-s}(\sigma^*))^*$.*

Proof.

By definition of $s = w^\theta_{\boldsymbol{\alpha}}(\boldsymbol{e})$, the degree of σ is equal to s. To prove that the degree of σ^* is s, it suffices to prove that the constant term of σ does not cancel, i.e. that X does not divide σ. Denote w the Hamming weight of $\boldsymbol{e}$ and $0 \leq i_0 < \cdots < i_{w-1} \leq n-1$ such that $e_{i_0}, \ldots, e_{i_{w-1}} \neq 0$. Consider $\rho_w = 0$ and for $j \in \{0, \ldots, w-1\}$, $\rho_j = \alpha_{i_j}^{e_{i_j}}$. Assume that $X = X - \rho_w$ divides σ, then $\sigma = \mathrm{lclm}_{0 \leq j \leq w}(X - \rho_j) = \mathrm{lclm}_{0 \leq j \leq w-1}(X - \rho_j)$. As the degree of σ is equal to s, according to [7], the rank of the matrices $V = (N_i^\theta(\rho_j)))_{0 \leq i,j \leq w}$ and $\tilde{V} = (N_i^\theta(\rho_j)))_{0 \leq i,j \leq w-1}$ are equal to s. We have $V = M \times D$ where $M = \begin{pmatrix} 1/\rho_0 & \ldots & 1/\rho_{w-1} & 1 \\ 1 & \ldots & 1 & 0 \\ \theta(\rho_0) & \cdots & \theta(\rho_{w-1}) & 0 \\ \vdots & & & \\ \theta(N_{w-1}(\rho_0)) & \ldots & \theta(N_{w-1}(\rho_{w-1})) & 0 \end{pmatrix}$ and D is the square diagonal matrix with diagonal $(\rho_0, \rho_1, \ldots, \rho_{w-1}, 1)$. As the rank of the matrix $\theta(\tilde{M}) = (\theta(N_i^\theta(\rho_j))))_{0 \leq i,j \leq w-1}$ is equal to s, and as the first line $(1/\rho_0, \ldots, 1/\rho_{w-1}, 1)$ of the matrix M is linearly independent of the next ones, we get that the rank of the matrix M is equal to $s+1$. Therefore the rank of the matrix $V = M \times D$ is equal to $s+1$, a contradiction. To conclude, X does not divide σ and $\deg(\sigma^*) = \deg(\sigma)$. Therefore we get $(\theta^{-s}(\sigma^*))^* = \theta^s(\theta^{-s}(\sigma)) = \sigma$. ∎

5.2 Key equation.

We exploit here the fact that the code is θ-cyclic to recover $\theta^{-s}(\sigma^*)$ thanks to a "key equation" which is inspired from the classical key equation in the commutative setting.

Proposition 1 *Consider α in $\mathcal{A}_n$, for i in $\{0,\dots,n-1\}$, $\alpha_i = N_i^\theta(\alpha)$, $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ and $I = \{i \in \{0,\dots,n-1\} \mid e_i \neq 0\}$. Consider $\sigma = \mathrm{lclm}_{i\in I}(X-\alpha_i^{e_i})$ with degree s, $S = \sum_{j=0}^{2t-1} X^j \cdot e\left(\frac{1}{\alpha_{n-j-1}}\right)$ and $w = \sum_{i\in I} \theta^{-1}(\alpha_i)F_i$, where for i in I, F_i is defined by $\sigma \cdot e_i = \theta(F_i^*)\cdot(X-\alpha_i)$. We have*

$$S \cdot \theta^{-s}(\sigma^*) \equiv w \pmod{X^{2t}}. \tag{5}$$

Proof. Consider i in I. As $X-\alpha_i^{e_i}$ divides σ on the right, $X-\alpha_i$ divides $\sigma\cdot e_i$ on the right. Consider for $i\in I$, $G_i \in R$ such that $\sigma\cdot e_i = G_i\cdot(X-\alpha_i)$ and F_i in R such that $\theta(F_i^*) = G_i$. We have, for all i in I,

$$e_i \cdot \theta^{-s}(\sigma^*) = (1-\alpha_i X)\cdot F_i.$$

We get

$$\begin{aligned}
S\cdot\theta^{-s}(\sigma^*) &= \sum_{j=0}^{2t-1} X^j \cdot e\left(\frac{1}{\alpha_{n-j-1}}\right)\theta^{-s}(\sigma^*)\\
&= \sum_{j=0}^{2t-1} X^j \cdot \sum_{i\in I} e_i N_i^\theta\left(\frac{1}{\alpha_{n-j-1}}\right)\theta^{-s}(\sigma^*)\\
&= \sum_{j=0}^{2t-1}\sum_{i\in I} N_i^\theta(\theta^{-1}(\alpha\theta(\alpha_j)))X^j\cdot(e_i\theta^{-s}(\sigma^*))\\
&= \sum_{i\in I}\theta^{-1}(\alpha_i)\sum_{j=0}^{2t-1} N_j^\theta(\alpha_i)X^j\cdot(1-\alpha_i X)\cdot F_i\\
&= \sum_{i\in I}\theta^{-1}(\alpha_i)\left(\sum_{j=0}^{2t-1}(\alpha_i X)^j\cdot(1-\alpha_i X)\right)\cdot F_i.
\end{aligned}$$

Therefore $S\cdot\theta^{-s}(\sigma^*) \equiv \sum_{i\in I}\theta^{-1}(\alpha_i)F_i \pmod{X^{2t}}$.

■

Using the partial extended left Euclidean algorithm applied to X^{2t} and S, we can recover $P = \theta^{-s}(\sigma^*)$ and deduce σ from P thanks to Lemma 2.

5.3 Recovering the evaluation polynomial.

We now exploit the fact that the code is a generalized skew Reed-Solomon code. This part is highly inspired from [5].

Recall that we have $f_u = f+E$ and that we want to recover now the evaluation polynomial f from f_u and σ. Furthermore we have $\sigma = \mathrm{lclm}_{i\in I}(X-\alpha_i^{e_i}) = \mathrm{lclm}_{i\in I}(X-\xi_i^{e_i/v_i})$ where $I = \{i\in\{0,\dots,n-1\} \mid e_i\neq 0\}$. Therefore, according to the product formula ([7, Theorem

2.7]), $\sigma \cdot E$ cancels at ξ_i for all i in $\{0, \ldots, n-1\}$. Furthermore, for i in $\{0, \ldots, n-1\}$, $N_n^\theta(\xi_i) = N_n^\theta(\alpha_i)\frac{\theta^n(v_i)}{v_i} = \frac{\theta^n(v_i)}{v_i} = 1$ because n is a multiple of the order of θ. Therefore $\mathrm{lclm}_{0\le i\le n-1}(X - \xi_i) = X^n - 1$ and $X^n - 1$ divides $\sigma \cdot E$. Consider μ in R such that

$$\mu \cdot (X^n - 1) = \sigma \cdot E. \tag{6}$$

Consider $g_u = f_u \bmod_{\mathrm{r}} X^k$ and $h_u = f_u - g_u$. We have $E = h_u + (g_u - f)$ and $\mu X^n - \mu = \sigma \cdot h_u + \sigma \cdot (g_u - f) = \sigma \cdot h_u - (\sigma \cdot h_u \bmod_{\mathrm{r}} X^n) + (\sigma \cdot h_u \bmod_{\mathrm{r}} X^n) + \sigma \cdot (g_u - f)$.

As $\deg(\mu) < n$ and $\deg(\sigma \cdot (g_u - f)) \le t + k - 1 < n$, we have

$$\mu X^n = \sigma \cdot h_u - (\sigma \cdot h_u \bmod_{\mathrm{r}} X^n)$$

and

$$\mu = (\sigma \cdot h_u - (\sigma \cdot h_u \bmod_{\mathrm{r}} X^n))/X^n. \tag{7}$$

From (6), we recover E as the quotient in the left division of $\mu X^n - \mu$ by σ, and we get $f = f_u - E$.

5.4 Decoding algorithm.

We are now designing a decoding algorithm whose main steps rely on the generalized multi-evaluation map (Section 4), the computation of a skew localisator polynomial thanks to the application of a (partial) left Euclidean algorithm (subsection 5.2) and the recovering of the evaluation polynomial thanks to a multiplication and a left division (subsection 5.3).

Algorithm 3: Decoding Algorithm

Input: Received word $u \in \mathbb{F}_{q^m}^n$ given by (4), $\alpha \in \mathcal{A}_n$ and $\lambda = 1/v(1)$ where $v = \mathrm{lclm}_{1\le i\le n-1}(X - N_i^\theta(1/\alpha))$.

Output: Evaluation polynomial f in $R_{<k}$.

1 $\tilde{\boldsymbol{u}} = \texttt{FastME}(u, (N_i^\theta(1/\alpha))_{0\le i\le n-1})$.

2 $S = \sum_{i=0}^{2t-1} \theta^i(\tilde{u}_{n-i-1})X^i$.

3 $f_u = \sum_{i=0}^{n-1} \theta^i(\lambda)\tilde{u}_i X^i$.

4 $\sigma = P^*$ where (P, w) satisfies $S \cdot P \equiv w \pmod{X^{2t}}$ with $\deg(P) \le t$ and $\deg(w) < t$.

5 $\mu = (\sigma \cdot h_u - (\sigma \cdot h_u \bmod_{\mathrm{r}} X^n))/X^n$ where $h_u = f_u - (f_u \bmod_{\mathrm{r}} X^k)$.

6 $E =$ quotient in the left division of $\mu X^n - \mu$ by σ.

7 $f = f_u - E$.

Theorem 5 *Algorithm 3 is correct.*

Proof. We have $S = \sum_{i=0}^{2t-1} \theta^i(\tilde{u}_{n-i-1})X^i = \sum_{i=0}^{2t-1} X^i \cdot u\left(\frac{1}{\alpha_{n-i}}\right) = \sum_{i=0}^{2t-1} X^i \cdot e\left(\frac{1}{\alpha_{n-i}}\right)$ because for j in $\{0, \ldots, 2t-1\}$, $u\left(\frac{1}{\alpha_{n-j-1}}\right) = e\left(\frac{1}{\alpha_{n-j-1}}\right)$. According to Theorem 4, we have

$f_u = \sum_{i=0}^{n-1} \theta^i(\lambda) u \left(\frac{1}{\alpha_i}\right) X^i$. The computations of σ, μ and E are deduced from relations (5), (7) and (6).

■

5.5 Example.

We finish the section with an example illustrating our Decoding Algorithm (Algorithm 3). Consider $q = 3$, $m = 4$, $n = 8$, $k = 2$, $t = 3$ and $\alpha = a$, where $a^4 + 2a^3 + 2 = 0$. Then $v = X^7 + a^{14}X^6 + a^{72}X^5 + a^{38}X^4 + X^3 + a^{14}X^2 + a^{72}X + a^{38}$, and $\lambda = 1/v(1) = a^{59}$. Assume that the received word is $\boldsymbol{u} = (a^{56}, a^3, a^{64}, a^{73}, a^{67}, a^{47}, a^{69}, a^{45}) = \boldsymbol{c} + \boldsymbol{e}$ where $\boldsymbol{c} = (a^{19}, a^3, a^{26}, a^{74}, a^{57}, a^{60}, a^{52}, a^{64})$ is a code word and $\boldsymbol{e} = (a^{60}, 0, a^{42}, a^{30}, a^{47}, a^{56}, a^5, a^{50})$ is an error vector such that $w^{\theta}_{\boldsymbol{\alpha}}(\boldsymbol{e}) = 3$. We detail below the steps of Algorithm 3:

1 $\tilde{\boldsymbol{u}} = (a^{33}, a^{46}, a^{43}, a^{45}, a^{73}, a^{46}, a^{30}, a^{72})$.

2 $S = a^{49}X^5 + a^{45}X^4 + a^{51}X^3 + a^{14}X^2 + a^{10}X + a^{72}$

3 $f_u = a^{65}X^7 + aX^6 + a^{63}X^5 + a^{52}X^4 + a^{38}X^3 + a^{14}X^2 + a^{63}X + a^{12}$

4 $\sigma = X^3 + a^8X^2 + a^{42}X + a^{63}$

5 $\mu = a^{75}X^2 + a^{41}X + a^{56}$

6 $E = a^{65}X^7 + aX^6 + a^{63}X^5 + a^{52}X^4 + a^{38}X^3 + a^{14}X^2 + a^8X + a^{33}$

7 $f = f_u - E = aX + a^{44}$

6 Conclusion

We have designed a decoding algorithm in the skew metric for a family of skew cyclic codes that are generalized skew Reed-Solomon codes. This algorithm is inspired from [5] and requires an interpolation step that we have replaced with a fast multi-evaluation relying on multiplications and divisions on the right in the skew polynomial ring R. The other steps are performed thanks to an extended left Euclidean algorithm, a multiplication and a left division in R (see [6, 13] for the cost analysis of all these operations). Lastly, in future work, the algorithm could be improved by taking greater advantage of the particular structure of the points chosen for the support.

Acknowledgment

This work was conducted within the France 2030 program, Centre Henri Lebesgue ANR-11-LABX-0020-01 .

References

[1] Bartz, Hannes and Jerkovits, Thomas and Rosenkilde, Johan, *Fast Kötter-Nielsen-Høholdt interpolation over skew polynomial rings and its application in coding theory*, Des. Codes Cryptogr., 92, 2024, 2, 435–465

[2] D. Boucher, W. Geiselmann and F. Ulmer, *Skew-cyclic codes*, Applicable Algebra in Engineering, Communication and Computing, 18, 2007, 4, 379–389

[3] D. Boucher and F. Ulmer, *Linear codes using skew polynomials with automorphisms and derivations*, Des. Codes Cryptogr., 70, 2014, 3, 405–431

[4] D. Boucher *An algorithm for decoding skew Reed-Solomon codes with respect to the skew metric.* Des. Codes Cryptogr. 88, 1991-2005 (2020).

[5] M. Bras-Amorós, *A decoding approach to Reed-Solomon codes from their definition*, American Mathematical Monthly, 125, 2018, 4, 320–338

[6] X. Caruso and J. Le Borgne *A new faster algorithm for factoring skew polynomials over finite fields.* Journal of Symbolic Computation, 79, 411-443, 2017

[7] T.Y. Lam and A. Leroy, *Vandermonde and Wronskian Matrices over Division Rings*, Journal of Algebra, 119, 308–336 (1988).

[8] T.Y. Lam, A. Leroy and A. Ozturk, *Wedderburn polynomials over division rings. II*, Contemp. Math., 456, 73–98, Amer. Math. Soc., Providence, RI, 2008

[9] S. Liu, F. Manganiello and F. R. Kschischang, *Construction and decoding of generalized skew-evaluation codes*, 2015 IEEE 14th Canadian Workshop on Information Theory (CWIT), St. John's, NL, Canada, 2015, pp. 9-13

[10] U. Martìnez-Peñas, *Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring*, Journal of Algebra, 504, 2018, 587-612,

[11] U. Martínez-Peñas and F.R. Kschischang, *Reliable and secure multishot network coding using linearized Reed-Solomon codes*, IEEE Trans. Inform. Theory, 65, 2019, 8, 4785–4803

[12] K.E. Nouetowa and I. Pogildialov *Iterative decoding of skew constacyclic codes* WCC 2024: The Thirteenth International Workshop on Coding and Cryptography

[13] S. Puchinger and A. Wachter-Zeh, *Fast operations on linearized polynomials and their applications in coding theory*, J. Symbolic Comput., 89, 2018, 194–215

[14] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, Cambridge, 2013, xiv+795,