An algorithm for decoding skew Reed-Solomon codes with respect to the skew metric.

Delphine Boucher

Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France
delphine.boucher@univ-rennes1.fr

Abstract. After giving a new interpretation of the skew metric defined in [4], we show that the decoding algorithm of [2] for skew Reed-Solomon codes remains valid with respect to this metric.

1 Introduction

Skew Reed-Solomon codes are a generalization of Reed-Solomon codes and Gabidulin codes. These codes are MDS codes for the Hamming metric and a decoding algorithm inspired from Welch-Berlekamp algorithm was designed in [2] over finite fields. In [4], the author defines a new metric, called skew-metric, which is optimal for skew Reed-Solomon codes defined over any division ring (Maximum Skew Distance codes, Theorem 1 of [4]).

The aim of this note is to give a new interpretation of the skew metric defined in [4] and prove that the decoding Algorithm 1 page 22 of [2] can be adapted from the Hamming metric to the skew metric.

In Section 2, we recall the material for defining skew Reed-Solomon codes and the skew metric. In Section 3 we give a new interpretation of the skew metric using a least common left multiple of linear skew polynomials. In Section 4, we prove that Algorithm 1 page 22 of [2] can be adapted from the Hamming metric to the skew metric.

2 Generalities on skew Reed-Solomon codes

Consider a division ring A, θ be an automorphism over A, δ be a θ-derivation which is a map $\delta : A \to A$ such that for all a and b in A:

$$\begin{aligned} \delta(a+b) &= \delta(a) + \delta(b) \\ \delta(ab) &= \delta(a)b + \theta(a)\delta(b), \end{aligned}$$

The ring $R = A[X; \theta, \delta]$ is defined on the set $\{\sum_{i=0}^{n} a_i X^i | n \in \mathbb{N}, a_i \in A\}$ where the addition is the usual addition of polynomials and the multiplication is defined by the rule : for a in A

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

The ring R is called a skew polynomial ring or Ore ring (cf. [6]) 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 of skew polynomials and greatest common right multiples of skew polynomials are necessarily *monic* skew polynomials.

Definition 1. *([3] p. 310) Let A be a division ring, θ be an automorphism over A and δ be a θ-derivation. Consider the ring $R = A[X;\theta,\delta]$. 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.*

The following definition ([3] p. 310) generalizes the classical notion of the norm of a field element : for a in A, for $i \in \mathbb{N}$, $N_i^{\theta,\delta}(a)$ is recursively defined as

$$\begin{aligned} N_0^{\theta,\delta}(a) &= 1 \\ N_{i+1}^{\theta,\delta}(a) &= \theta(N_i^{\theta,\delta}(a))\, a + \delta(N_i^{\theta,\delta}(a)). \end{aligned}$$

If $f = \sum_i f_i X^i \in R$ and $a \in A$ then $f(a) = \sum_i f_i N_i^{\theta,\delta}(a)$ (see Lemma 1 of [2] or Proposition 2.9 of [3]).

Definition 2. *([3], page 321) Let A be a division ring, θ be an automorphism over A, δ be a θ-derivation and $n \in \mathbb{N}^*$. Let $\alpha_1, \ldots, \alpha_n$ in A. The (θ,δ)-* **Vandermonde matrix** *of $\alpha = (\alpha_1, \ldots, \alpha_n)$ is defined by*

$$V_n^{\theta,\delta}(\alpha) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ N_1^{\theta,\delta}(\alpha_1) & N_1^{\theta,\delta}(\alpha_2) & \cdots & N_1^{\theta,\delta}(\alpha_n) \\ \vdots & \vdots & \cdots & \vdots \\ N_{n-1}^{\theta,\delta}(\alpha_1) & N_{n-1}^{\theta,\delta}(\alpha_2) & \cdots & N_{n-1}^{\theta,\delta}(\alpha_n) \end{pmatrix}.$$

Remark 1. If A is a finite field ($A = \mathbb{F}_{p^m}$, with p prime number), θ is the Frobenius automorphism ($\theta : a \mapsto a^p$ and $\delta = 0$), then one gets the classical notion of the norm of a field element : $N_i(a) = \theta^{i-1}(a) \cdots \theta(a) a = a^{\frac{p^i-1}{p-1}}$.

Later, we will define the skew Reed-Solomon codes by evaluating some skew polynomials at points $\alpha_1, \ldots, \alpha_n$ of A such that $\mathrm{rank}(V_n^{\theta,\delta}(\alpha)) = n$. We will say that these points are P-independent. The following theorem establishes a link between the rank of the Vandermonde matrix mentioned above and the degree of the least common left multiple of linear skew polynomials.

Theorem 1 (Theorem 8, [3] page 326). *Let A be a division ring, θ be an automorphism of A and δ be a θ-derivation. Consider the ring $R = A[X;\theta,\delta]$. Let $\alpha_1, \ldots, \alpha_n \in A$ and $g = \mathrm{lclm}_{1 \le i \le n}(X - \alpha_i) \in R$ be the least common left multiple of $X - \alpha_i, i = 1, \ldots, n$, then $\deg(g) = \mathrm{rank}\left(\mathrm{V}_{\mathrm{n}}^{\theta,\delta}(\alpha_1, \ldots, \alpha_{\mathrm{n}})\right)$. If $\deg(g) = n$ then $\alpha_1, \ldots, \alpha_n$ are* **P-independent**.

Consider a subset Ω of A, the **rank** of Ω is $Rank(\Omega) := \deg \mathrm{lclm}_{u\in\Omega}(X-u)$. Assume that $\alpha_1,\ldots,\alpha_n$ are P-independent. If Ω is a subset of A such that $\mathrm{lclm}_{1\leq i\leq n}(X-\alpha_i) = \mathrm{lclm}_{u\in\Omega}(X-u)$, then $(\alpha_1,\ldots,\alpha_n)$ is a P**-basis** of Ω.

Definition 3 (Definition 7 of [2], Definition 19 of [4]). *Let A be a division ring, θ be an automorphism of A and δ be a θ-derivation. Let $n \in \mathbb{N}^*$, $k \in \{1\ldots,n\}$. Consider the ring $R = A[X;\theta,\delta]$ and $\alpha_1,\ldots,\alpha_n$ on A P-independent in A. The* **skew Reed-Solomon code** *of length n, dimension k and support $\alpha = (\alpha_1,\ldots,\alpha_n)$ is defined as*

$$\mathcal{R}_{k,n}^{\theta,\delta}(\alpha) = \{(f(\alpha_1),\ldots,f(\alpha_n)) \mid f \in R, \deg(f) < k\}.$$

Skew Reed-Solomon codes are MDS codes for the Hamming metric ([2]) and MSD (Maximum Skew Distance) for the skew metric (see Definition 9 and Theorem 1 of [4] or Theorem 3 at the end of Section 3). In what follows we recall the definition of the skew metric and give a new interpretation of this metric by using the least common left multiple of linear skew polynomials.

3 Skew metric

Recall that for $y = (y_1,\ldots,y_n)$ in A^n, the **Hamming weight** of y is the number of non-zero coordinates of y :

$$w_H(y) := \#\{i \in \{1,\ldots,n\} \mid y_i \neq 0\}.$$

Consider a division subring K of A, the **rank weight** of y is the dimension of the space generated by its coordinates over K:

$$w_R(y) := \dim(< y_1,\ldots,y_n >_K).$$

Reed-Solomon codes are optimal for the Hamming metric (Maximum Separable Distance codes), while Gabidulin codes are optimal for the rank metric (Maximum Rank Distance codes).

Definition 4 (Definition 9 of [4]). *Let A be a division ring, θ be an automorphism of A and δ be a θ-derivation. Let $n \in \mathbb{N}^*$, $k \in \{1\ldots,n\}$. Consider the ring $R = A[X;\theta,\delta]$ and $\alpha = (\alpha_1,\ldots,\alpha_n)$ in A^n such that $\alpha_1,\ldots,\alpha_n$ are P-independent. Consider $P = \mathrm{lclm}_{1\leq i\leq n}(X-\alpha_i)$ in R. The* **skew weight** *of $y = (y_1,\ldots,y_n) \in A^n$ is*

$$w_\alpha(y) = n - Rank(Z_\alpha(F))$$

where $F \in R$ is the skew interpolation polynomial of degree $< n$ at the n points (α_i, y_i) and $Z_\alpha(F) = \{u \in A \mid F(u) = P(u) = 0\}$.

Note that the skew interpolation polynomial F at the points (α_i, y_i) in the above definition exists because the n points $\alpha_1,\ldots,\alpha_n$ are P-independent (see also [3] page 326).

Example 1. Consider $\mathbb{F}_{2^6} = \mathbb{F}_2(a)$ where $a^6 + a^4 + a^3 + a + 1 = 0$ and θ the automorphism Frobenius over $\mathbb{F}_{2^6}$. Consider $\alpha = (a, a^2, a^3, a^4, a^5, a^6)$. Using Magma, one computes $\mathrm{lclm}_{1\leq i\leq 6}(X - a^i) = X^6 - 1$ in $\mathbb{F}_{2^6}[X;\theta]$, therefore $a, a^2, a^3, a^4, a^5, a^6$ are P-independent (and α is a P-basis of $\mathbb{F}_{2^6}^*$). Consider $e = (0, 0, 0, 0, a^{56}, a^{55})$, its skew weight is $w_\alpha(e) = 6 - Rank(Z_\alpha(F))$ where $F = aX^5 + a^{31}X^4 + a^{46}X^3 + a^{22}X^2 + a^{10}X + a^4$ is the skew interpolation polynomial at the points $(a^i, e_i)_{1\leq i\leq 6}$. The set of roots of F in $\mathbb{F}_{2^6}^*$ is $Z_\alpha(F) = \{a, a^2, a^3, a^4, a^8, a^9, a^{10}, a^{11}, a^{12}, a^{14}, a^{21}, a^{22}, a^{24}, a^{26}, a^{28}, a^{29}, a^{30}, a^{33}, a^{34}, a^{39}, a^{43}, a^{45}, a^{48}, a^{50}, a^{51}, a^{54}, a^{57}, a^{58}, a^{59}, a^{61}, a^{62}\}$ and its rank is $Rank(Z_\alpha(F)) = \deg \mathrm{lclm}_{u\in Z_\alpha(F)}(X - u) = \deg(X^5 + a^{30}X^4 + a^{45}X^3 + a^{21}X^2 + a^9X + a^3) = 5$. Therefore the skew weight of e is $6 - 5 = 1$. Notice here that the Hamming weight of e is 2 and the rank weight of e is $\dim(< a^{56}, a^{55} >_{\mathbb{F}_2}) = 2$.

In what follows, a new interpretation of the skew metric is given (Proposition 1). First two intermediate Lemmas (Lemma 1 and Lemma 2) will be useful.

Lemma 1. *Let A be a division ring, θ be an automorphism of A and δ be a θ-derivation. Consider $\alpha = (\alpha_1, \ldots, \alpha_n)$ in A^n such that $\alpha_1, \ldots, \alpha_n$ are P-independentd $y = (y_1, \ldots, y_n)$ in A^n. Consider the ring $R = A[X;\theta,\delta]$, $P = \mathrm{lclm}_{1\leq i\leq n}(X - \alpha_i)$ in R and $F \in R$ the skew interpolation polynomial of degree $< n$ at the n points (α_i, y_i). Then*

$$w_\alpha(y) = \deg(P) - \deg(\mathrm{gcrd}(P, F)) = \deg(\mathrm{lclm}(P, F)) - \deg(F).$$

Proof. According to Definition 4, $w_\alpha(y) = \deg(P) - \deg(\mathrm{lclm}_{u\in U}(X - u))$ where $U = \{u \in A \mid F(u) = P(u) = 0\}$. Let us prove that $\mathrm{lclm}_{u\in U}(X - u)$ is equal to $\mathrm{gcrd}(F, P)$. For all u in U, $X - u$ divides F and P on the right, therefore $\mathrm{lclm}_{u\in U}(X - u)$ divides $\mathrm{gcrd}(F, P)$ on the right.

Consider a common right factor H of F and P. According to Theorem 4 of [6], as P is a least common left multiple of irreducible skew polynomials, H is also the least common left multiple of irreducible skew polynomials. Furthermore, all the degrees of these factors are necessarily equal to 1. Consider $V \subset A$ such that $H = \mathrm{lclm}_{v\in V}(X - v)$. Consider v in V; as H divides P and F on the right, $X - v$ divides P and F on the right, therefore $v \in U$ and H divides $\mathrm{lclm}_{u\in U}(X - u)$. One can conclude that $\mathrm{lclm}_{u\in U}(X - u)$ is equal to $\mathrm{gcrd}(\mathrm{F}, \mathrm{P})$ and $w_\alpha(y) = \deg(P) - \deg(\mathrm{gcrd}(P, F)) = \deg(\mathrm{lclm}(P, F)) - \deg(F)$.

■

Example 2. Consider $A = \mathbb{F}_3(z)$ and $\theta \in Aut(A)$ defined by $\theta(z) = \frac{z-1}{z+1}$. Its inverse automorphism is defined by $\theta^{-1}(z) = \frac{1+z}{1-z}$. Consider $\alpha = (z, z^2, z^3, z^4)$. The least common left multiple of $X - z, X - z^2, X - z^3$ and $X - z^4$ in $A[X;\theta]$ is $P = X^4 + 2$ therefore z, z^2, z^3 and z^4 are P-independent over A. Consider $e = (0, 0, z^2 + z, z^3 + z) \in A^4$ and F the skew interpolation polynomial at the points $(z^i, e_i)_{1\leq i\leq 4}$. One has $F = (z^5 + z^4 + z^2 + z)/(z^4 + 2z^2 + z + 2)X^3 + (2z^4 + 2z^3 + 2z + 2)/(z^5 + 2z^4 + z^3 + 2z)X^2 + (2z^2 + z + 2)/(z^3 + 2z^2 + 2z)X + (z^3 + 2z^2 + z)/(z^2 + z + 2)$ and F divides P on the right, therefore the skew weight of e is $w_\alpha(e) = 4 - \deg(\mathrm{gcrd}(F, P)) = 1$.

Definition 5. *([3]) Let A be a division ring, θ be an automorphism over A and δ be a θ-derivation. The* $(\theta,\delta)-$**conjugacy class** *of an element $a \in A$ is the set of all its* **conjugates**

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

where c is taken over A^*.

The following property will be useful next (product formulae) :

Theorem 2 (Product theorem 2.7 of [3]). *Let A be a division ring, θ be an automorphism over A, δ be a θ-derivation and $R = A[X;\theta,\delta]$. Let f, g in R and $a \in A$. If $g(a) = 0$, then $(f \cdot g)(a) = 0$. If $g(a) \neq 0$, then $(f \cdot g)(a) = f(a^{g(a)})g(a)$.*

Lemma 2. *Let A be a division ring, θ be an automorphism over A, δ be a θ-derivation and $R = A[X;\theta,\delta]$. Consider $\alpha_1, \ldots, \alpha_n$ in A, P-independent, consider $F \in R \setminus \{0\}$ and $P = \mathrm{lclm}_{1\leq i\leq N}(X - \alpha_i) \in R$. Consider the monic skew polynomial $E = \mathrm{lclm}_{F(\alpha_i)\neq 0}(X - \alpha_i^{F(\alpha_i)})$, then $E \cdot F = \lambda \cdot \mathrm{lclm}(P, F)$ where λ is a non zero constant.*

Proof.

Consider $\tilde{E}$ such that $\tilde{E} \cdot F = \mathrm{lclm}(P, F)$. Let us first prove that $\tilde{E}$ divides E on the right. This amounts to show that $\tilde{E} \cdot F$ divides $E \cdot F$ on the right. As F divides $E \cdot F$ on the right and $\tilde{E} \cdot F = \mathrm{lclm}(P, F)$, it remains to prove that P divides $E \cdot F$ on the right. Consider i in $\{1, \ldots, N\}$. If $F(\alpha_i) \neq 0$, then according to the definition of E, $E(\alpha_i^{F(\alpha_i)}) = 0$. According to product formulae (Theorem 2), $(E \cdot F)(\alpha_i) = E(\alpha_i^{F(\alpha_i)}) \times F(\alpha_i)$, therefore one has

$$(E \cdot F)(\alpha_i) = 0. \tag{2}$$

If $F(\alpha_i) = 0$ then the previous equality (2) still holds (according to Theorem 2). One concludes that P divides $E \cdot F$ on the right. Therefore $\mathrm{lclm}(P, F) = \tilde{E} \cdot F$ divides $E \cdot F$ on the right and $\tilde{E}$ divides E on the right. To prove that E divides $\tilde{E}$ on the right, it suffices to prove that $\tilde{E}$ cancels at $\alpha_i^{F(\alpha_i)}$ for all i in $\{1, \ldots, N\}$ such that $F(\alpha_i) \neq 0$. Consider i in $\{1, \ldots, N\}$ such that $F(\alpha_i) \neq 0$. As P divides $\tilde{E} \cdot F$ on the right, its right roots are also right roots of $\tilde{E} \cdot F$, therefore $\tilde{E} \cdot F$ cancels at α_i. Furthermore $F(\alpha_i) \neq 0$, therefore, according to the product formulae, $\tilde{E}(\alpha_i^{F(\alpha_i)}) = 0$.

To conclude, there exists λ in $A \setminus \{0\}$ such that $E = \lambda\tilde{E}$.

■

From Lemma 1 and Lemma 2, one deduces a new interpretation of the skew weight. :

Proposition 1. *Let A be a division ring, θ be an automorphism over A, δ be a θ-derivation and $R = A[X;\theta,\delta]$. Consider $\alpha = (\alpha_1, \ldots, \alpha_n)$ in A^n such that $\alpha_1, \ldots, \alpha_n$ are P-independent. Consider $y = (y_1, \ldots, y_n)$ in A^n. The skew weight of y satisfies :*

$$w_\alpha(y) = \deg \mathrm{lclm}_{y_i\neq 0}(X - \alpha_i^{y_i}). \tag{3}$$

PROOF. Consider $P = \mathrm{lclm}_{1\leq i\leq n}(X-\alpha_i)$ and F the interpolation skew polynomial with degree $< n$ such that $F(\alpha_i) = y_i$ for all i in $\{1,\ldots,n\}$. According to Lemma 1, $w_\alpha(y) = \deg(\mathrm{lclm}(P,F)) - \deg(F)$. According to Lemma 2, $\mathrm{lclm}(P,F) = E\cdot F$ where $E = \mathrm{lclm}_{y_i\neq 0}(X-\alpha_i^{y_i})$, therefore $w_\alpha(y) = \deg(E)$.

■

Example 3. (see Example 1) Consider $\mathbb{F}_{2^6} = \mathbb{F}_2(a)$ where $a^6+a^4+a^3+a+1 = 0$ and $\theta : x \mapsto x^2$. Consider $\alpha = (a, a^2, a^3, a^4, a^5, a^6)$ and $e = (0,0,0,0,a^{56}, a^{55})$. The skew weight of e is equal to the degree of the lclm of $X - a^{56}\times\theta(a^5)/a^5 = X - a^{61}$ and $X - a^{55}\times\theta(a^6)/a^6 = X - a^{61}$, therefore it is equal to 1.

Example 4. (see Example 2) Consider $A = \mathbb{F}_3(z)$ and θ the automorphism of A defined by $\theta(z) = (z-1)/(z+1)$. Consider $\alpha = (z, z^2, z^3, z^4)$ and $e = (0,0,z^2+z, z^3+z)$. The skew weight of e is equal to the degree of the lclm of $X - z^3\times\theta(z^2+z)/(z^2+z) = X - z^3(2z^2+z)/((z^2+2z+1)(z^2+z)) = X - (2z^4+z^3)/(z^3+1)$ and $X - z^4\times\theta(z^3+z)/(z^3+z) = X - z^4(2z^3+z^2+2z+1)/((z^3+1)(z^3+z)) = X - (2z^4+z^3)/(z^3+1)$, therefore $w_\alpha(e)$ is equal to 1.

Remark 2. Consider the notations of Proposition 1. If $\theta = id$ and $\delta = 0$ then $\mathrm{lclm}_{y_i\neq 0}(X-\alpha_i^{y_i}) = \mathrm{lcm}_{y_i\neq 0}(X-\alpha_i) = \prod_{y_i\neq 0}(X-\alpha_i)$ therefore the skew weight of y is equal to its Hamming weight : $w_\alpha(y) = w_H(y)$ (see also Example 36 of [4]).

Remark 3. Consider the notations of Proposition 1. If all the α_i are conjugate, consider $\xi\in A$, $a_i\in A^*$ such that $\alpha_i = \xi^{a_i}$, then if $y_i\neq 0$, $\alpha_i^{y_i} = \xi^{a_i y_i}$ and the skew weight of y is the rank of the Vandermonde matrix of $(\xi^{a_i y_i})$. According to Theorem 4.5 of [3], this is the rank weight of $(a_i y_i)$:$w_\alpha(e) = w_R((a_i y_i)_{y_i\neq 0}) = w_R((a_i y_i)_{1\leq i\leq n})$.

Example 5. We give here some computations of skew weights and rank weights over $\mathbb{F}_4^2$ and $\mathbb{F}_9^2$ where θ is the Frobenius automorphism.

Consider $A = \mathbb{F}_4 = \mathbb{F}_2(a)$, $\theta : x\mapsto x^2$ and $\delta = 0$. There are 6 vectors e of $\mathbb{F}_4^2$ of Hamming weight $w_H(e) = 1$ and 9 of Hamming weight $w_H(e) = 2$. There are 9 vectors e of rank weight $w_R(e) = 1$ and 6 of rank weight $w_R(e) = 2$. There are 6 P-independent couples $\alpha = (\alpha_1, \alpha_2)$. For each such α, there are 9 vectors e of skew weight $w_\alpha(e) = 1$ and 6 vectors e of skew weight $w_\alpha(e) = 2$. The details are given in Table 5.

Consider $A = \mathbb{F}_9 = \mathbb{F}_3(a)$ with $a^2 - a - 1 = 0$, $\theta : x\mapsto x^2$ and $\delta = 0$. There are 16 vectors of $\mathbb{F}_9^2$ of Hamming weight 1 and 64 of Hamming weight 2; 32 vectors of rank weight 1 and 48 vectors of rank weight 2. There are 72 P-independent couples (α_1,α_2). For 48 P-independent α, there are 16 vectors e of $\mathbb{F}_9^2$ with skew weight $w_\alpha(e) = 1$ and 64 with skew weight $w_\alpha(e) = 2$. For the other 24 P-independent α, there are 32 vectors e with skew weight $w_\alpha(e) = 1$ and 48 vectors e with skew weight $w_\alpha(e) = 2$.

Here is a proof of Theorem 1 of [4] using formulation (3).

$e \in \mathbb{F}_4^2$	$1,0$	$a,0$	$a^2,0$	$0,1$	$1,1$	$a,1$	$a^2,1$	$0,a$	$1,a$	a,a	a^2,a	$0,a^2$	$1,a^2$	a,a^2	a^2,a^2
$w_H(e)$	1	1	1	1	2	2	2	1	2	2	2	1	2	2	2
$w_R(e)$	1	1	1	1	1	2	2	1	2	1	2	1	2	2	1
$w_{(a,1)}(e)$	1	1	1	1	2	2	1	1	1	2	2	1	2	1	2
$w_{(1,a)}(e)$	1	1	1	1	2	1	2	1	2	2	1	1	1	2	2
$w_{(a^2,a)}(e)$	1	1	1	1	2	2	1	1	1	2	2	1	2	1	2

Table 1. Hamming weight, rank weight, skew weights of vectors of $\mathbb{F}_4^2$

Theorem 3 (Theorem 1 of [4]). *Let A be a division ring, θ be an automorphism of A and δ be a θ-derivation. Let $n \in \mathbb{N}^*$, $k \in \{1 \dots, n\}$. Consider $\alpha_1, \dots, \alpha_n$ on A P-independent in A. The skew Reed-Solomon code $\mathcal{R}_{k,n}^{\theta,\delta}(\alpha)$ is MDS for the skew metric (Maximum Skew Distance).*

Proof. Consider a codeword $c = (f(\alpha_1), \dots, f(\alpha_n))$ of skew weight $w < n - k + 1$ where $f \in R$ is of degree $< k$. Consider $E(X) = \mathrm{lclm}_{c_i \neq 0}(X - \alpha_i^{c_i})$, then according to Product Theorem 2, for all i in $\{1, \dots, n\}$, $(E \cdot f)(\alpha_i) = 0$. Furthermore, according to (3), the degree of the skew polynomial E is equal to the skew weight of c, therefore the degree of $E \cdot f$ is less than or equal to $(n-k)+(k-1) = n-1$. As $E \cdot f$ cancels at n P-independent points, it cancels. As E is nonzero, $f = 0$ and $c = 0$. ∎

4 Decoding algorithm

We prove here that the decoding algorithm 1 on page 22 of [2] with respect to the Hamming distance still works with respect to the skew metric. We first need a small technical lemma.

Lemma 3. *Let A be a division ring, θ be an automorphism over A, δ be a θ-derivation and $R = A[X; \theta, \delta]$. Consider $\alpha = (\alpha_1, \dots, \alpha_n)$ in A^n such that $\alpha_1, \dots, \alpha_n$ are P-independent. Consider g and Q in R then*
$w_\alpha((Q \cdot g)(\alpha_1), \dots, (Q \cdot g)(\alpha_n)) \leq w_\alpha(g(\alpha_1), \dots, g(\alpha_n))$.

Proof. Consider $P = \mathrm{lclm}_{1 \leq i \leq n}(X - \alpha_i)$. According to Lemma 1,
$\begin{cases} w_\alpha(g(\alpha_1), \dots, g(\alpha_n)) = \deg(P) - \deg(\mathrm{gcrd}(g, P)) \\ w_\alpha((Q \cdot g)(\alpha_1), \dots, (Q \cdot g)(\alpha_n)) = \deg(P) - \deg(\mathrm{gcrd}(Q \cdot g, P)) \end{cases}$,
therefore, $w_\alpha((Q \cdot g)(\alpha_1), \dots, (Q \cdot g)(\alpha_n)) = w_\alpha(g(\alpha_1), \dots, g(\alpha_n)) + \deg(\mathrm{gcrd}(g, P)) - \deg(\mathrm{gcrd}(Q \cdot g, P)) \leq w_\alpha(g(\alpha_1), \dots, g(\alpha_n))$. ∎

Proposition 2. *Decoding algorithm 1 is correct.*

Proof. The n equations of point 1. of the algorithm are linear in the $d_0 + d_1 + 2 \geq n+1$ unknowns $q_{0,0}, \dots, q_{0,d_0}, q_{1,0}, \dots, q_{1,d_1}$, therefore there is a nonzero solution (Q_0, Q_1) satisfying point 1. of the algorithm.

Consider $Z(X) = Q_0(X) + Q_1(X) \cdot f(X) \in R$ and $E(X) = \mathrm{lclm}_{Z(\alpha_i) \neq 0}(X - \alpha_i^{Z(\alpha_i)})$. According to Product Theorem 2, the skew polynomial $E \cdot Z$ cancels at

Algorithm 1 Skew weight Decoding algorithm of skew Reed-Solomon code

Require: A a division ring, $\theta \in \mathrm{Aut}(A)$, δ a θ-derivation, $R = A[X;\theta,\delta]$, $\alpha = (\alpha_1,\ldots,\alpha_n)$ P-independent over A, $r \in A^n$ such that $r = c + e$ with $\mathrm{w}_\alpha(e) \leq t := \lfloor (n-k)/2 \rfloor$, $c = (f(\alpha_1),\ldots,f(\alpha_n))$, $f \in R$ and $\deg(f) < k$.

Ensure: f

1: Computation of Q_0 and Q_1 in R such that $\deg(Q_0) \leq d_0 := n-1-t$, $\deg(Q_1) \leq d_1 := d_0 - (k-1)$ and $(Q_0 + Q_1 \cdot r_i)(\alpha_i) = 0$ for all i in $\{1,\ldots,n\}$:
Solve the linear system with unknowns $q_{0,0},\ldots,q_{0,d_0},q_{1,0},\ldots,q_{1,d_1}$:

$$\begin{cases} \text{if } r_i = 0 : \displaystyle\sum_{j=0}^{d_0} q_{0,j}\, N_j^{\theta,\delta}(\alpha_i) = 0 \\ \text{if } r_i \neq 0 : \displaystyle\sum_{j=0}^{d_0} q_{0,j}\, N_j^{\theta,\delta}(\alpha_i) + \sum_{j=0}^{d_1} q_{1,j}\, N_j^{\theta,\delta}\left(\alpha_i^{r_i}\right) r_i = 0 \end{cases}$$

$$Q_0(X) \leftarrow \sum_{j=0}^{d_0} q_{0,j} X^j$$

$$Q_1(X) \leftarrow \sum_{j=0}^{d_1} q_{1,j} X^j$$

2: Computation of the quotient f in the left division of $Q_0(X)$ by $-Q_1(X)$ in R

3: **return** f

α_i for all i in $\{1,\ldots,n\}$. Furthermore, for i in $\{1,\ldots,n\}$, $(Q_0 + Q_1 \cdot r_i)(\alpha_i) = 0$ therefore, $Z(\alpha_i) = (Q_1 \cdot f)(\alpha_i) - (Q_1 \cdot r_i)(\alpha_i) = (Q_1 \cdot (f - r_i))(\alpha_i)$. Consider g in R of degree $< n$ such that for all i in $\{1,\ldots,n\}$, $g(\alpha_i) = r_i$. Consider i in $\{1,\ldots,n\}$, one has

$$Z(\alpha_i) = (Q_1 \cdot (f - r_i))(\alpha_i) = (Q_1 \cdot (f-g))(\alpha_i) + (Q_1 \cdot (g - r_i))(\alpha_i).$$

As $(g - r_i)(\alpha_i) = 0$, one gets $Z(\alpha_i) = (Q_1 \cdot (f-g))(\alpha_i)$. According to Lemma 3, as $w_\alpha((f-g)(\alpha_1),\ldots,(f-g)(\alpha_n)) := w_\alpha((f-r_1)(\alpha_1),\ldots,(f-r_n)(\alpha_n)) \leq t$, one gets $w_\alpha((Q_1 \cdot (f-g))(\alpha_1),\ldots,(Q_1 \cdot (f-g))(\alpha_n)) \leq t$, therefore

$$w_\alpha(Z(\alpha_1),\ldots,Z(\alpha_n)) \leq t.$$

According to (3), the degree of E is equal to $w_\alpha(Z(\alpha_1),\ldots,Z(\alpha_n))$, therefore, it is less than or equal to t. As the degree of Z is less than or equal to $n-t-1$, the degree of $E \cdot Z$ is $\leq n-t-1+t < n$. The skew polynomial $E \cdot Z$ cancels at n P-independent points, therefore it is equal to 0. To conclude, the skew polynomial Z is equal to 0. As $(Q_0, Q_1) \neq (0,0)$, f is the quotient in the left division of $-Q_0$ by Q_1.

■

Example 6. (see Examples 1 and 3) Consider $\mathbb{F}_{2^6} = \mathbb{F}_2(a)$ where $a^6 + a^4 + a^3 + a + 1 = 0$ and θ the Frobenius automorphism over $\mathbb{F}_{2^6}$. Consider the skew Reed-Solomon code with support $\alpha = (a, a^2, a^3, a^4, a^5, a^6)$ and dimension 3, $f = a$

and $e = (0, 0, 0, 0, a^{56}, a^{55})$. The skew weight of e is equal to 1 (see Example 1). Consider $r = (a, a, a, a, a, a) + e = (a, a, a, a, 1, a^{19})$. Then the unknown skew polynomials Q_0 and Q_1 have degrees at most 4 and 2 and a non zero solution to the linear system satisfied by their coefficients is $(1, 0, a^9, 0, 0, a^{62}, 0, a^5)$. Therefore $Q_0 = 1 + a^9X^2 = (a^{62} + a^5X^2) \cdot a$, $Q_1 = a^{62} + a^5X^2$ and the quotient in the left division of Q_0 by $-Q_1$ is equal to a.

Example 7. (see Examples 2 and 4) Consider $A = \mathbb{F}_3(z)$ with $\theta(z) = (z - 1)/(z+1)$ and $R = A[X; \theta]$. Consider the skew Reed-Solomon code with support $\alpha = (z, z^2, z^3, z^4)$ and dimension 2. Consider $f = X + 1/z$ and $e = (0, 0, z^2 + z, z^3 + z)$. The skew weight of e is equal to 1 (see Example 2). The received word is $r = (z + 1/z, z^2 + 1/z, z^3 + 1/z, z^4 + 1/z) + e = ((z^2 + 1)/z, (z^3 + 1)/z, (z^4 + z^3 + z^2 + 1)/z, (z^5 + z^4 + z^2 + 1)/z)$. Then the unknown skew polynomials Q_0 and Q_1 have degrees at most 2 and 1 and a non zero solution to the linear system satisfied by their coefficients is $(1, (z^5 + 2z^4 + 2z^3 + z + 1)/(z^4 + z^3 + z^2), (z^3 + 1)/(z^3 + 2z^2), 2z, (2z^3 + 2)/(z^3 + 2z^2))$. Therefore $Q_0 = (z^3 + 1)/(z^3 + 2z^2)X^2 + (z^5 + 2z^4 + 2z^3 + z + 1)/(z^4 + z^3 + z^2)X + 1$, $Q_1 = (2z^3 + 2)/(z^3 + 2z^2)X + 2z$ and the quotient in the left division of Q_0 by $-Q_1$ in R is equal to $X + 1/z$.

Lastly one can notice that the ring $R = A[X; \theta, \delta]$ can be considered in a more general setting, when θ is an endomorphism of A (and not necessarily an automorphism). In this setting (see [3]), the ring R is right Euclidean; divisions on the right, greatest common right divisors and least common left multiples of skew polynomials still exist, therefore the skew metric and the skew Reed-Solomon codes are still defined. For the decoding algorithm, we still have the relation $Q_0 + Q_1 \cdot f = 0$, but f cannot be uniquely determined as the quotient in the *left* division of Q_0 by $-Q_1$, because the division on the left requires θ to be invertible. However, one can recover f by considering the skew reciprocal polynomial of $Q_0 + Q_1 \cdot f$. Namely, one gets that $Q_0^* + \Theta^{\deg(Q_1)}(f^*) \cdot Q_1^* = 0$ where $\Theta : \sum a_i X^i \mapsto \sum \theta(a_i) X^i$ and for $a(X) = \sum a_i X^i$ with degree d, $a^*(X) := \sum X^{d-i} \cdot a_i$. Therefore $\Theta^{\deg(Q_1)}(f^*)$ is the quotient in the *right* division of $-Q_0^*$ by Q_1^*. As θ is an endomorphism over the division ring A, θ is injective, therefore one can recover f^* from $\Theta^{\deg(Q_1)}(f^*)$. As we know the degree of f and its valuation (given by the degrees and the valuations of Q_0 and Q_1), one can recover f from f^*. The following example illustrates a situation where θ is an endomorphism which is not bijective.

Example 8. Consider $A = \mathbb{F}_3(z)$, θ the endomorphism of A defined by $\theta(z) = z^2$ and $R = A[X; \theta]$. Consider $\alpha = (z, z^2, \ldots, z^6)$. The degree of $\mathrm{lclm}(X - z^i, i = 1, \ldots, 6)$ is equal to 6, therefore $z, z^2, \ldots z^6$ are P-independent. Consider the skew Reed-Solomon code with support α and dimension 2. Its minimum distance is 5.

Consider $e = (0, 0, z, 2, 0, 2z/(z + 2))$, one can verify that the skew weight $w_\alpha(e)$ of e is equal to 2.

Consider $f = zX - 1/z$. The codeword associated to f is

$c = (z^2 - 1/z, z^3 - 1/z, z^4 - 1/z, z^5 - 1/z, z^6 - 1/z, z^7 - 1/z)$.

Consider the received word $r = c + e$. The unknown skew polynomials Q_0 and Q_1 have degrees at most 3 and 2. Solving the linear system given by point

1. of the algorithm yields : $Q_0 = (2z^5+z^2+z+1)/(z^{16}+2z^{12}+2z^{10})X^3+(z^{23}+2z^{17}+2z^{16}+2z^{15}+2z^{14}+z^5+2z^2+2z+2)/(z^{24}+2z^{20}+2z^{18})X^2+(2z^{16}+z^{12}+z^{10}+2z^9+z^3+z^2+z+1)/(z^{14}+2z^{10}+2z^8)X+1$ and $Q_1 = (z^5+2z^2+2z+2)/(z^{20}+2z^{16}+2z^{14})X^2+(2z^9+z^3+z^2+z+1)/(z^{12}+2z^8+2z^6)X+z$.

Performing the right division of $-Q_0^* = -(X^3+(2z^{64}+z^{48}+z^{40}+2z^{36}+z^{12}+z^8+z^4+1)/(z^{56}+2z^{40}+2z^{32})X^2+(z^{46}+2z^{34}+2z^{32}+2z^{30}+2z^{28}+z^{10}+2z^4+2z^2+2)/(z^{48}+2z^{40}+2z^{36})X+(2z^5+z^2+z+1)/(z^{16}+2z^{12}+2z^{10}))$ by $Q_1^* = z^4X^2+(2z^{18}+z^6+z^4+z^2+1)/(z^{24}+2z^{16}+2z^{12})X+(z^5+2z^2+2z+2)/(z^{20}+2z^{16}+2z^{14})$ yields $2/z^8X+z^4$. As $\deg(Q_1)=2$, one gets $f^* = 2/z^2X+z$ and $f = zX+2/z$.

5 Conclusion

In this paper, a new interpretation of the skew metric defined in [4] is given and the decoding algorithm of [2] is adapted to the skew metric for skew Reed-Solomon codes. This algorithm was improved recently by the authors of [5] who obtained an algorithm with a quadratic complexity. This algorithm handles a more general setting (linearized Reed-Solomon codes with the skew metric).

Acknowledgement. I thank the referees for their fruitful comments and suggestions.

This work was supported by the French government "Investissements d'Avenir" program ANR-11-LABX-0020-01.

References

1. D. Augot, P. Loidreau, G. Robert, *Generalized Gabidulin codes over fields of any characteristic*, Designs, Codes and Cryptography, Springer Verlag, 2017, 10.1007/s10623-017-0425-6
2. D. Boucher and F. Ulmer, *Linear codes using skew polynomials with automorphisms and derivations*. Designs, Codes and Cryptography, Springer Verlag, 2014, 70 (3), pp.405-431.
3. T.Y. Lam and A. Leroy, *Vandermonde and Wronskian Matrices over Division Rings*, Journal of Algebra, 119, 308-336 (1988)
4. U. Martínez-Peñas, *Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring*, Journal of Algebra, 504, 587-612 (2018)
5. U. Martínez-Peñas, F.R. Kschischang, *Reliable and Secure Multishot Network Coding using Linearized Reed-Solomon Codes* arXiv:1805.03789
6. O. Ore, *Theory of Non-Commutative Polynomials*, The Annals of Mathematics, 2nd Ser, 34(3), 480-508 (1933)