About Skew Reed-Solomon Codes

NonCommutative Rings and their Applications, VII

Delphine Boucher

Univ Rennes 1, IRMAR, France

6th July 2021

Reed-Solomon Codes

- Linear code C of length n and dimension k over $\mathbb{F}_q$: subspace of $\mathbb{F}_q^n$ of dimension k.

- Hamming weight of $c \in \mathbb{F}_q^n$:

$$w_H(c) = \#\{i \in \{1, \ldots, n\} \mid c_i \neq 0\}.$$

- Minimum distance for the Hamming metric :

$$d = \min_{c \in C, c \neq 0} w_H(c).$$

- Singleton bound : $d \leq n - k + 1$.
- MDS codes : $d = n - k + 1$.

Definition

Consider $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ pairwise distinct. The Reed-Solomon code of length n and dimension k is

$$C = \{(f(\alpha_1), \ldots, f(\alpha_n)) \mid f \in \mathbb{F}_q[X], \deg(f) < k\}.$$

MDS Theorem

The Reed-Solomon code C is MDS ($d = n - k + 1$).

A classical proof

As $f \neq 0 \in \mathbb{F}_q[X]_{<k}$ has at most $k-1$ roots and as $\alpha_1, \ldots, \alpha_n$ are pairwise distinct, the number of zero coordinates of $c = (f(\alpha_1), \ldots, f(\alpha_n))$ is less than k and the weight of c is greater than $n - k$.

Another proof using the two facts :

- $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ pairwise distinct : $\deg(\underbrace{\operatorname{lcm}_{1 \le i \le n}(X - \alpha_i)}_{P}) = n$;
- for $c \in \mathbb{F}_q^n$, $w_H(c) = \deg(\underbrace{\operatorname{lcm}_{c_i \neq 0}(X - \alpha_i)}_{W})$.

Consider $c = (f(\alpha_1), \ldots, f(\alpha_n))$ $\quad f \neq 0 \in \mathbb{F}_q[X]_{<k}$

$\forall i$, $(W.f)(\alpha_i) = \underbrace{W(\alpha_i)}_{0 \text{ if } c_i \neq 0} \times \underbrace{f(\alpha_i)}_{0 \text{ if } c_i = 0} = 0$

Therefore $\underbrace{P}_{n} \mid W.\underbrace{f}_{<k}$ and $\deg(W) > n-k$.

Skew Reed-Solomon codes

- A : a division ring,
  θ : an automorphism of A,
  δ : a derivation of A,
  $R = A[X;\theta,\delta]$, ring of skew polynomials (Ore, 1933) :

$$\forall a \in A, X \cdot a = \theta(a)X + \delta(a).$$

- R euclidean on the right : $\mathrm{r\_rem}$, lclm, gcrd exist ;
  R euclidean on the left.

- Evaluation of $f \in R$ at $\alpha \in A$ (Lam & Leroy, 1988)

$$f(\alpha) = \mathrm{r\_rem}(f, X - \alpha).$$

- Product formula (Lam & Leroy, 1988) : consider $f, g \in R, \alpha \in A$

$$\boxed{(f \cdot g)(\alpha) = \begin{cases} f(\alpha^{g(\alpha)}) \times g(\alpha) & \text{if } g(\alpha) \neq 0 \\ 0 & \text{if } g(\alpha) = 0 \end{cases}}$$

where for $\alpha \in A$ and $y \in A^*$,

$$\alpha^y := \theta(y)\alpha y^{-1} + \delta(y) y^{-1} \text{ (conjugation)}.$$

- P-independance (Lam & Leroy, 1988) : consider $\alpha_1, \ldots, \alpha_n \in A$, $\alpha_1, \ldots, \alpha_n$ P-independant : $\deg(\underbrace{\mathrm{lclm}_{1 \leq i \leq n}(X - \alpha_i)}_{P}) = n$.
- Skew polynomial weight of c (Martinez-Penas, 2018 ; B., 2020) : consider $\alpha_1, \ldots, \alpha_n \in A$, P-independant,

$$w_\alpha(c) \quad = \quad \deg(\underbrace{\mathrm{lclm}_{c_i \neq 0}(X - \alpha_i^{c_i})}_{W})$$

$\rightarrow$ Maximum Skew Distance (MSD) code (M.P. 2018) :

$$d = \min_{c \in C, c \neq 0} w_\alpha(c) = n - k + 1.$$

Definition (B. & Ulmer, 2014 ; Martinez-Penaz, 2018)

Consider $\alpha_1, \ldots, \alpha_n \in A$, P-independant. The skew Reed-Solomon code of length n and dimension k is

$$C = \{(f(\alpha_1), \ldots, f(\alpha_n)) \mid f \in A[X;\theta,\delta], \deg(f) < k\}.$$

MSD Theorem (Martinez-Penas 2018 ; B., 2020)

The skew Reed-Solomon code C is MSD.

A proof using the two facts :

- $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ P-independant : $\deg(\underbrace{\mathrm{lclm}_{1 \le i \le n}(X - \alpha_i)}_{P}) = n$;
- for $c \in \mathbb{F}_q^n$, $w_\alpha(c) = \deg(\underbrace{\mathrm{lclm}_{c_i \neq 0}(X - \alpha_i^{c_i})}_{W})$.

Consider $c = (f(\alpha_1) \ldots f(\alpha_n))$ $\quad f \in R_{<k}$, $f \neq 0$

$$\forall i, \ (W.f)(\alpha_i) \underset{\text{LL88}}{=} \begin{cases} \underbrace{W(\alpha_i^{f(\alpha_i)})}_{=0} \times f(\alpha_i) & \text{if } f(\alpha_i) \neq 0 \\ 0 & \text{if } f(\alpha_i) = 0 \end{cases}$$

$= 0$

$P \mid_r W.f \qquad \deg(W) > n - k.$

Decoding algorithms : an overview

Decoding Reed-Solomon codes (Berlekamp-Welch).

require : $r = (r_1, \ldots, r_n) = c + e$ with $c = (f(\alpha_1), \ldots, f(\alpha_n))$, $f \in \mathbb{F}_q[X]_{<k}$,

$$\mathrm{w_H}(e) \le t = \lfloor (n-k)/2 \rfloor.$$

ensure : f.

1 : Compute nonzero $Q_0, Q_1 \in \mathbb{F}_q[X]$ such that

$$\begin{aligned} &\forall i \in \{1, \ldots, n\}, Q_0(\alpha_i) + r_i \times Q_1(\alpha_i) = 0, \\ &\deg(Q_0) \le n - 1 - t, \\ &\deg(Q_1) \le n - 1 - t - (k-1). \end{aligned}$$

2 : $f \leftarrow -Q_0/Q_1$.

3 : **return** f.

Decoding Reed-Solomon codes.

require : $r = (r_1, \ldots, r_n) = c + e$ with $c = (f(\alpha_1), \ldots, f(\alpha_n))$, $f \in \mathbb{F}_q[X]_{<k}$, $\mathrm{w_H}(e) \leq t$.

ensure : f.

0 : $g \leftarrow \mathrm{interpol}((\alpha_i), (r_i))$.

1 : Compute nonzero $Q_0, Q_1 \in \mathbb{F}_q[X]$ such that

$$\begin{array}{l} \forall i \in \{1, \ldots, n\}, Q_0(\alpha_i) + r_i \times Q_1(\alpha_i) = 0, \\ \deg(Q_0) \leq n - 1 - t, \\ \deg(Q_1) \leq n - 1 - t - (k - 1). \end{array}$$

2 : $f \leftarrow -Q_0/Q_1$.

3 : **return** f.

Decoding Reed-Solomon codes.

require : $r = (r_1, \ldots, r_n) = c + e$ with $c = (f(\alpha_1), \ldots, f(\alpha_n))$, $f \in \mathbb{F}_q[X]_{<k}$,

$$\mathrm{w_H}(\underbrace{\epsilon(\alpha_1), \ldots, \epsilon(\alpha_n)}_{e}) \leq t,$$

$\epsilon = g - f$ and $g = \mathrm{interpol}((\alpha_i), (r_i))$.

ensure : f.

0 : $g \leftarrow \mathrm{interpol}((\alpha_i), (r_i))$.

1 : Compute nonzero $Q_0, Q_1 \in \mathbb{F}_q[X]$ such that

$$\forall i \in \{1, \ldots, n\}, (Q_0 + Q_1 \cdot g)(\alpha_i) = 0,$$
$$\deg(Q_0) \leq n - 1 - t,$$
$$\deg(Q_1) \leq n - 1 - t - (k - 1).$$

2 : $f \leftarrow$ quotient in the division of Q_0 by $-Q_1$ in $\mathbb{F}_q[X]$.

3 : **return** f.

Decoding skew Reed-Solomon codes with the skew polynomial metric (B. 20).

require : $r = (r_1, \ldots, r_n) = c + e$ with $c = (f(\alpha_1), \ldots, f(\alpha_n))$, $f \in R_{<k}$,

$$\mathrm{w}_\alpha(\underbrace{\epsilon(\alpha_1), \ldots, \epsilon(\alpha_n)}_{e}) \leq t.$$

$\epsilon = g - f$ and $g = \mathrm{r\_interpol}((\alpha_i), (r_i))$.

ensure : f.

0 : $g \leftarrow \mathrm{r\_interpol}((\alpha_i), (r_i))$.

1 : Compute nonzero $Q_0, Q_1 \in R$ such that

$$\begin{array}{l} \forall i \in \{1, \ldots, n\}, (Q_0 + Q_1 \cdot g)(\alpha_i) = 0, \\ \deg(Q_0) \leq n - 1 - t, \\ \deg(Q_1) \leq n - 1 - t - (k - 1). \end{array}$$

2 : $f \leftarrow$ quotient in the left division of Q_0 by $-Q_1$ in R.

3 : **return** f.

Proof :

Consider $\underbrace{Z = Q_0 + Q_1 \cdot f}_{\deg < n-t}$ and $E = \mathrm{lclm}_{Z(\alpha_i) \neq 0}(X - \alpha_i^{Z(\alpha_i)})$.

Proof :

Consider $\underbrace{Z = Q_0 + Q_1 \cdot f}_{\deg < n-t}$ and $E = \mathrm{lclm}_{Z(\alpha_i) \neq 0}(X - \alpha_i^{Z(\alpha_i)})$.

For i in $\{1, \ldots, n\}$,

1. $(E \cdot Z)(\alpha_i) = 0 \rightarrow P|_r E \cdot Z$.

Proof :

Consider $\underbrace{Z = Q_0 + Q_1 \cdot f}_{\deg < n-t}$ and $E = \mathrm{lclm}_{Z(\alpha_i) \neq 0}(X - \alpha_i^{Z(\alpha_i)})$.

For i in $\{1, \ldots, n\}$,

1. $(E \cdot Z)(\alpha_i) = 0 \rightarrow P|_r E \cdot Z$.
2. $Z(\alpha_i) = (Q_0 + Q_1 \cdot f)(\alpha_i) - \underbrace{(Q_0 + Q_1 \cdot g)(\alpha_i)}_{0} = (-Q_1 \cdot (g - f))(\alpha_i)$

Lemma

Consider $a, b \in R$.
If $b|_r a$ then $w_\alpha(a(\alpha_1), \ldots, a(\alpha_n)) \leq w_\alpha(b(\alpha_1), \ldots, b(\alpha_n))$.

Proof :

Consider $\underbrace{Z = Q_0 + Q_1 \cdot f}_{\deg < n-t}$ and $\underbrace{E = \mathrm{lclm}_{Z(\alpha_i)\neq 0}(X - \alpha_i^{Z(\alpha_i)})}_{\deg \leq t}$.

For i in $\{1, \ldots, n\}$,

1. $(E \cdot Z)(\alpha_i) = 0 \rightarrow P|_r E \cdot Z$.
2. $Z(\alpha_i) = (Q_0 + Q_1 \cdot f)(\alpha_i) - \underbrace{(Q_0 + Q_1 \cdot g)(\alpha_i)}_{0} = (-Q_1 \cdot (g - f))(\alpha_i)$

Lemma

Consider $a, b \in R$.
If $b|_r a$ then $w_\alpha(a(\alpha_1), \ldots, a(\alpha_n)) \leq w_\alpha(b(\alpha_1), \ldots, b(\alpha_n))$.

$\rightarrow \deg(E) \leq w_\alpha(e) \leq t$.

Proof :

Consider $\underbrace{Z = Q_0 + Q_1 \cdot f}_{\deg < n-t}$ and $\underbrace{E = \mathrm{lclm}_{Z(\alpha_i)\neq 0}(X - \alpha_i^{Z(\alpha_i)})}_{\deg \leq t}$.

For i in $\{1, \ldots, n\}$,

1. $(E \cdot Z)(\alpha_i) = 0 \rightarrow P|_r E \cdot Z$.
2. $Z(\alpha_i) = (Q_0 + Q_1 \cdot f)(\alpha_i) - \underbrace{(Q_0 + Q_1 \cdot g)(\alpha_i)}_{0} = (-Q_1 \cdot (g - f))(\alpha_i)$

Lemma

Consider $a, b \in R$.
If $b|_r a$ then $w_\alpha(a(\alpha_1), \ldots, a(\alpha_n)) \leq w_\alpha(b(\alpha_1), \ldots, b(\alpha_n))$.

$\rightarrow \deg(E) \leq w_\alpha(e) \leq t$.

We get that $E \cdot Z = 0$ and $Z = 0$.

List decoding of Reed-Solomon codes (Sudan).

require : $r = (r_1, \ldots, r_n) = c + e$ with $c = (f(\alpha_1), \ldots, f(\alpha_n))$, $f \in \mathbb{F}_q[X]_{<k}$,

$$\mathrm{w_H}(\underbrace{\epsilon(\alpha_1), \ldots, \epsilon(\alpha_n)}_{e}) \leq \tau,$$

$\epsilon = g - f = \gcd(g - f, \ldots, g^\ell - f^\ell)$ and $g = \mathrm{interpol}((\alpha_i), (r_i))$.

ensure : $\mathcal{L}$, list containing f.

0 : $g \leftarrow \mathrm{interpol}((\alpha_i), (r_i))$.

1 : Compute $Q_0, Q_1, \ldots, Q_\ell$ nonzero in $\mathbb{F}_q[X]$ such that

$$\forall i \in \{1, \ldots, n\}, (Q_0 + Q_1 \cdot g + \cdots + Q_\ell \cdot g^\ell)(\alpha_i) = 0,$$
$$\deg(Q_j) \leq n - 1 - \tau - j(k-1).$$

2 : $\mathcal{L} \leftarrow \{\tilde{f} \in \mathbb{F}_q[X]_{<k} \mid Q_0 + Q_1 \cdot \tilde{f} + \cdots + Q_\ell \cdot \tilde{f}^\ell = 0\}$.

3 : **return** $\mathcal{L}$.

List decoding of skew R.-S. codes with the skew polynomial metric (B. 20).

require : $r = (r_1, \ldots, r_n) = c + e$ with $c = (f(\alpha_1), \ldots, f(\alpha_n))$, $f \in R_{<k}$,

$$\mathrm{w}_\alpha(\underbrace{\epsilon(\alpha_1), \ldots, \epsilon(\alpha_n)}_{\neq e}) \leq \tau,$$

$\epsilon = \mathrm{gcrd}(g - f, \ldots, g^\ell - f^\ell) \neq g - f$ and $g = \mathrm{r\_interpol}((\alpha_i), (r_i))$.

ensure : $\mathcal{L}$, list containing f.

0 : $g \leftarrow \mathrm{r\_interpol}((\alpha_i), (r_i))$.

1 : Compute $Q_0, Q_1, \ldots, Q_\ell$ nonzero in R such that

$$\forall i \in \{1, \ldots, n\}, (Q_0 + Q_1 \cdot g + \cdots + Q_\ell \cdot g^\ell)(\alpha_i) = 0,$$
$$\deg(Q_j) \leq n - 1 - \tau - j(k-1).$$

2 : $\mathcal{L} \leftarrow \{\tilde{f} \in R_{<k} \mid Q_0 + Q_1 \cdot \tilde{f} + \cdots + Q_\ell \cdot \tilde{f}^\ell = 0\}$.

3 : **return** $\mathcal{L}$.

Thank you for your attention !