Decoding Reed-Solomon Skew-Differential Codes

J. Gómez-Torrecillas

Department of Algebra, University of Granada

Quadratic Forms, Rings and Codes
Université d'Artois
July 8th, 2021

Based on a joint work with **G. Navarro** and **P. Sánchez-Hernández.**

The general idea

The human framework: In Granada, the *Algebra and Information Theory group*[1] likes to design new algebraic decoding algorithms for nice classes of codes.

[1] https://www.ugr.es/local/ait/index_en.html

[2] That is, it satisfies that $\phi(a+b) = \phi(a) + \phi(b)$ for all $a, b \in K$.

The general idea

The human framework: In Granada, the *Algebra and Information Theory group*[1] likes to design new algebraic decoding algorithms for nice classes of codes.

A simple mathematical framework:

[1] https://www.ugr.es/local/ait/index_en.html

[2] That is, it satisfies that $\phi(a+b) = \phi(a) + \phi(b)$ for all $a, b \in K$.

The general idea

The human framework: In Granada, the *Algebra and Information Theory group*[1] likes to design new algebraic decoding algorithms for nice classes of codes.

A simple mathematical framework:

- Let K be a field.

[1] https://www.ugr.es/local/ait/index_en.html

[2] That is, it satisfies that $\phi(a+b) = \phi(a) + \phi(b)$ for all $a, b \in K$.

The general idea

The human framework: In Granada, the *Algebra and Information Theory group*[1] likes to design new algebraic decoding algorithms for nice classes of codes.

A simple mathematical framework:

- Let K be a field.
- For any additive map[2] $\phi : K \to K$, set

$$K^{\phi} = \{b \in K : \phi(ab) = \phi(a)b \text{ for all } a \in K\}.$$

[1] https://www.ugr.es/local/ait/index_en.html
[2] That is, it satisfies that $\phi(a+b) = \phi(a) + \phi(b)$ for all $a, b \in K$.

The general idea

The human framework: In Granada, the *Algebra and Information Theory group*[1] likes to design new algebraic decoding algorithms for nice classes of codes.

A simple mathematical framework:

- Let K be a field.
- For any additive map[2] $\phi : K \to K$, set

$$K^{\phi} = \{b \in K : \phi(ab) = \phi(a)b \text{ for all } a \in K\}.$$

- A straightforward argument shows that K^{ϕ} is a subfield of K and, obviously, ϕ becomes a K^{ϕ}–linear map.

[1] https://www.ugr.es/local/ait/index_en.html

[2] That is, it satisfies that $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in K$.

The general idea

The human framework: In Granada, the *Algebra and Information Theory group*[1] likes to design new algebraic decoding algorithms for nice classes of codes.

A simple mathematical framework:

- Let K be a field.
- For any additive map[2] $\phi : K \to K$, set

$$K^{\phi} = \{b \in K : \phi(ab) = \phi(a)b \text{ for all } a \in K\}.$$

- A straightforward argument shows that K^{ϕ} is a subfield of K and, obviously, ϕ becomes a K^{ϕ}–linear map.
- A tempting idea is to use good enough field extensions K/K^{ϕ} to design K–linear error corrector codes with efficient algebraic decoding algorithms.

[1] https://www.ugr.es/local/ait/index_en.html

[2] That is, it satisfies that $\phi(a+b) = \phi(a) + \phi(b)$ for all $a, b \in K$.

The concrete framework

- In this talk, we consider additive maps on K stemming from skew derivations.

The concrete framework

- In this talk, we consider additive maps on K stemming from skew derivations.
- As algebraic objects, our codes can be seen as a special case of module (σ, δ)–code in the sense of
  [BU] D. Boucher, F. Ulmer. Linear codes using skew polynomials with automorphisms and derivations. Des. Codes Cryptogr. 70 (2014) 405–431.
  in a similar way as Reed-Solomon codes may be interpreted as examples of cyclic codes.

The concrete framework

- In this talk, we consider additive maps on K stemming from skew derivations.
- As algebraic objects, our codes can be seen as a special case of module (σ, δ)–code in the sense of **[BU] D. Boucher, F. Ulmer. Linear codes using skew polynomials with automorphisms and derivations. Des. Codes Cryptogr. 70 (2014) 405–431.**
  in a similar way as Reed-Solomon codes may be interpreted as examples of cyclic codes.
- Our aim in the first part: To construct a class of codes, from a skew derivation, endowed with an algebraic decoding algorithm inspired by Peterson-Gorenstein-Zierler's one. **We only require Linear Algebra.**

The concrete framework

- In this talk, we consider additive maps on K stemming from skew derivations.
- As algebraic objects, our codes can be seen as a special case of module (σ, δ)–code in the sense of **[BU] D. Boucher, F. Ulmer. Linear codes using skew polynomials with automorphisms and derivations. Des. Codes Cryptogr. 70 (2014) 405–431.** in a similar way as Reed-Solomon codes may be interpreted as examples of cyclic codes.
- Our aim in the first part: To construct a class of codes, from a skew derivation, endowed with an algebraic decoding algorithm inspired by Peterson-Gorenstein-Zierler's one. **We only require Linear Algebra.**
- Objective of the second part: show why the first part works. **Requirement: some basic facts on (non-commutative) rings.**

The concrete framework

A *skew derivation* on K is a pair (σ, δ), where σ is a field automorphism of K, and $\delta : K \to K$ is an additive map subject to the condition

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b, \qquad (1)$$

for all $a, b \in K$.

The concrete framework

A *skew derivation* on K is a pair (σ, δ), where σ is a field automorphism of K, and $\delta : K \to K$ is an additive map subject to the condition

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b, \tag{1}$$

for all $a, b \in K$.

Given $u \in K$, let $\varphi_u : K \to K$ be defined by

$$\varphi_u(a) = \sigma(a)u + \delta(a), \tag{2}$$

for all $a \in K$.

It is an additive map.

The code builder

Proposition 1

Assume that the dimension of K as a K^{φ_u}–vector space is $m < \infty$. The minimal polynomial of the K^{φ_u}–linear map φ_u has degree m and, henceforth, it has at least[a] a cyclic vector[b]. Moreover $\alpha \in K$ is such a cyclic vector if and only if the matrix

$$A = \begin{pmatrix} \alpha & \varphi_u(\alpha) & \cdots & \varphi_u^{m-1}(\alpha) \\ \varphi_u(\alpha) & \varphi_u^2(\alpha) & \cdots & \varphi_u^m(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_u^{m-1}(\alpha) & \varphi_u^m(\alpha) & \cdots & \varphi_u^{2m-2}(\alpha) \end{pmatrix}$$

is invertible.

[a] If there is one, then **most** of the elements in K become cyclic vectors.

[b] That is, $\{\alpha, \varphi_u(\alpha), \ldots, \varphi_u^{m-1}(\alpha)\}$ is a K^{φ_u}–basis of K

The definition

Definition 2

Given $2 \leq d \leq m$, define the K–linear code $C_{(\varphi_u,\alpha,d)} \subseteq K^m$ of dimension $m-d+1$ as the left kernel of the matrix

$$H = \begin{pmatrix} \alpha & \varphi_u(\alpha) & \cdots & \varphi_u^{d-2}(\alpha) \\ \varphi_u(\alpha) & \varphi_u^2(\alpha) & \cdots & \varphi_u^{d-1}(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_u^{m-1}(\alpha) & \varphi_u^{m}(\alpha) & \cdots & \varphi_u^{m+d-3}(\alpha) \end{pmatrix},$$

that is, $C_{(\varphi_u,\alpha,d)} = \{w \in K^m : wH = 0\}$. It is endowed with the Hamming metric.

The definition

Definition 2

Given $2 \leq d \leq m$, define the K–linear code $C_{(\varphi_u,\alpha,d)} \subseteq K^m$ of dimension $m-d+1$ as the left kernel of the matrix

$$H = \begin{pmatrix} \alpha & \varphi_u(\alpha) & \cdots & \varphi_u^{d-2}(\alpha) \\ \varphi_u(\alpha) & \varphi_u^2(\alpha) & \cdots & \varphi_u^{d-1}(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_u^{m-1}(\alpha) & \varphi_u^m(\alpha) & \cdots & \varphi_u^{m+d-3}(\alpha) \end{pmatrix},$$

that is, $C_{(\varphi_u,\alpha,d)} = \{w \in K^m : wH = 0\}$. It is endowed with the Hamming metric.

Remark: The matrix H is transpose to the generating matrix of some instances of linearized Reed-Solomon codes in the sense of

U. Martínez-Peñas, Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring. J. Algebra 504 (2018) 587-612.

So our RS skew-differential codes are dual to some of them. In particular, it comes out that $C_{(\varphi_u,\alpha,d)}$ is an MDS code.

Decoding, I

Next, let us describe the decoding algorithm for $C_{(\varphi_u,\alpha,d)}$, that corrects up to $\tau = \lfloor \frac{d-1}{2} \rfloor$ errors ($d \geq 3$).

Suppose that we receive a word

$$y = (y_0, \dots, y_{m-1}) \in K^m$$

with $y = c + e \in K^m$, where c is a codeword, and

$$e = (e_0, \dots, e_{m-1})$$

is an error vector, which is assumed to be nonzero in the discussion below.

Decoding, I

Next, let us describe the decoding algorithm for $C_{(\varphi_u,\alpha,d)}$, that corrects up to $\tau = \lfloor \frac{d-1}{2} \rfloor$ errors ($d \geq 3$).

Suppose that we receive a word

$$y = (y_0, \dots, y_{m-1}) \in K^m$$

with $y = c + e \in K^m$, where c is a codeword, and

$$e = (e_0, \dots, e_{m-1})$$

is an error vector, which is assumed to be nonzero in the discussion below.

Suppose that the nonzero components $e_{k_1}, \dots, e_{k_v} \in K$ of e occur at the positions $0 \leq k_1 < \cdots < k_v \leq m-1$. We assume that $v \leq \tau$.

Decoding,II

- We start by computing, for $i = 0, \ldots, d-2$, the *syndromes*

$$S_{i,0} = \sum_{j=0}^{m-1} y_j \varphi_u^{i+j}(\alpha), \tag{3}$$

which are the components of the vector yH.

Decoding,II

- We start by computing, for $i = 0, \ldots, d-2$, the *syndromes*

$$S_{i,0} = \sum_{j=0}^{m-1} y_j \varphi_u^{i+j}(\alpha), \tag{3}$$

which are the components of the vector yH.

- For every pair i, k of nonnegative integers such that $i + k \leq 2\tau - 1$ we may compute $S_{i,k} \in K$ recursively from (3) according to the rule

$$S_{i,k+1} = \sigma^{-1}(\delta(S_{i,k}) - S_{i+1,k}). \tag{4}$$

Decoding,II

- We start by computing, for $i = 0, \dots, d-2$, the *syndromes*

$$S_{i,0} = \sum_{j=0}^{m-1} y_j \varphi_u^{i+j}(\alpha), \tag{3}$$

which are the components of the vector yH.

- For every pair i, k of nonnegative integers such that $i + k \leq 2\tau - 1$ we may compute $S_{i,k} \in K$ recursively from (3) according to the rule

$$S_{i,k+1} = \sigma^{-1}(\delta(S_{i,k}) - S_{i+1,k}). \tag{4}$$

- We may thus form *syndrome matrix*

$$S = \begin{pmatrix} S_{0,0} & S_{0,1} & \cdots & S_{0,\tau-1} \\ S_{1,0} & S_{1,1} & \cdots & S_{1,\tau-1} \\ \vdots & \vdots & \ddots & \vdots \\ S_{\tau,0} & S_{\tau,1} & \cdots & S_{\tau,\tau-1} \end{pmatrix}.$$

Decoding, III

Next, for $1 \leq r \leq \tau$, let S_r denote the matrix formed by the r first columns of S and compute

$$\theta = \max\{r : rank\, S_r = r\}.$$

Proposition 3

The left kernel of the matrix

$$B = \begin{pmatrix} S_{0,0} & S_{0,1} & \cdots & S_{0,\theta-1} \\ S_{1,0} & S_{1,1} & \cdots & S_{1,\theta-1} \\ \vdots & \vdots & \ddots & \vdots \\ S_{\theta,0} & S_{\theta,1} & \cdots & S_{\theta,\theta-1} \end{pmatrix}$$

is a one dimensional vector subspace of $K^{\theta+1}$ spanned by a vector $\rho = (\rho_0, \dots, \rho_\theta)$ with $\rho_\theta \neq 0$.

Decoding, IV

The localization of the positions $k_1, \dots, k_v \in \{0, \dots, m-1\}$ at which the error values $e_{k_1}, \dots, e_{k_v}$ appear will be done with the help of a locator matrix built from $\rho = (\rho_0, \dots, \rho_\theta)$ as follows.

Decoding, IV

The localization of the positions $k_1, \dots, k_v \in \{0, \dots, m-1\}$ at which the error values $e_{k_1}, \dots, e_{k_v}$ appear will be done with the help of a locator matrix built from $\rho = (\rho_0, \dots, \rho_\theta)$ as follows.

- For $j = 0, \dots, m-1$ and $i = 0, \dots m - \theta - 1$, set

$$l_{0,j} = \begin{cases} \rho_j & \text{if } j = 0, \dots, \theta \\ 0 & \text{if } j = \theta + 1, \dots, m-1 \end{cases}, \qquad l_{i,-1} = 0. \tag{5}$$

Decoding, IV

The localization of the positions $k_1, \ldots, k_v \in \{0, \ldots, m-1\}$ at which the error values $e_{k_1}, \ldots, e_{k_v}$ appear will be done with the help of a locator matrix built from $\rho = (\rho_0, \ldots, \rho_\theta)$ as follows.

- For $j = 0, \ldots, m-1$ and $i = 0, \ldots m-\theta-1$, set

$$l_{0,j} = \begin{cases} \rho_j & \text{if } j = 0, \ldots, \theta \\ 0 & \text{if } j = \theta+1, \ldots, m-1 \end{cases}, \qquad l_{i,-1} = 0. \tag{5}$$

- We may then construct a matrix

$$L = \begin{pmatrix} l_{0,0} & l_{0,1} & \cdots & l_{0,m-1} \\ l_{1,0} & l_{1,1} & \cdots & l_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ l_{m-\theta-1,0} & l_{m-\theta-1,1} & \cdots & l_{m-\theta-1,m-1} \end{pmatrix} \tag{6}$$

  by defining its entries recursively as

$$l_{i+1,j} = \sigma(l_{i,j-1}) + \delta(l_{i,j}). \tag{7}$$

Decoding, V

For $i = 0, \ldots, m-1$ let ϵ_i denote the vector of K^m whose i–th component equal to 1, and every other component is 0. By $Row(LA)$ we denote the row space of the matrix LA.

Theorem 4

The error positions $k_1, \ldots, k_v$ are, precisely, those

$$k \in \{0, \ldots, m-1\}$$

such that $\epsilon_k \notin Row(LA)$. The error values $e_{k_1}, \ldots, e_{k_v} \in K$ are the unique solution of the linear system

$$S_{i,0} = \sum_{j=1}^{v} e_{k_j} \varphi_u^{i+k_j}(\alpha), \qquad (0 \leq i \leq v-1).$$

RS skew-differential codes over finite fields.

Let us assume here that $K = \mathbb{F}$ is the finite field with p^r elements for some prime p, so our codes become linear block codes over the alphabet $\mathbb{F}$.

[3] Setting $K^{\varphi_u} = \mathbb{F}_q$, and $n_1, \dots, n_t$ the degrees of the distinct irreducible factors appearing in the canonical factorization of the minimal polynomial $\mu \in \mathbb{F}_q[X]$, we obtain that the probability for a given $\alpha \in K$ to be a cyclic vector is

$$(1 - q^{-n_1}) \cdots (1 - q^{-n_t}).$$

RS skew-differential codes over finite fields.

Let us assume here that $K = \mathbb{F}$ is the finite field with p^r elements for some prime p, so our codes become linear block codes over the alphabet $\mathbb{F}$. Let τ be the Frobenius automorphism of $\mathbb{F}$.

[3] Setting $K^{\varphi_u} = \mathbb{F}_q$, and $n_1, \ldots, n_t$ the degrees of the distinct irreducible factors appearing in the canonical factorization of the minimal polynomial $\mu \in \mathbb{F}_q[X]$, we obtain that the probability for a given $\alpha \in K$ to be a cyclic vector is

$$(1 - q^{-n_1}) \cdots (1 - q^{-n_t}).$$

RS skew-differential codes over finite fields.

Let us assume here that $K = \mathbb{F}$ is the finite field with p^r elements for some prime p, so our codes become linear block codes over the alphabet $\mathbb{F}$. Let τ be the Frobenius automorphism of $\mathbb{F}$.
The steps of the design method of an RS skew-differential block code may be then enumerated as follows:

[3] Setting $K^{\varphi_u} = \mathbb{F}_q$, and $n_1, \dots, n_t$ the degrees of the distinct irreducible factors appearing in the canonical factorization of the minimal polynomial $\mu \in \mathbb{F}_q[X]$, we obtain that the probability for a given $\alpha \in K$ to be a cyclic vector is

$$(1 - q^{-n_1}) \cdots (1 - q^{-n_t}).$$

RS skew-differential codes over finite fields.

Let us assume here that $K = \mathbb{F}$ is the finite field with p^r elements for some prime p, so our codes become linear block codes over the alphabet $\mathbb{F}$. Let τ be the Frobenius automorphism of $\mathbb{F}$.
The steps of the design method of an RS skew-differential block code may be then enumerated as follows:

1. Choose a natural $0 < h < r$, and set $\sigma = \tau^h$ and $m = \frac{r}{(r,h)}$, the order of σ, which will also become the length of the code.

---

[3] Setting $K^{\varphi_u} = \mathbb{F}_q$, and $n_1, \dots, n_t$ the degrees of the distinct irreducible factors appearing in the canonical factorization of the minimal polynomial $\mu \in \mathbb{F}_q[X]$, we obtain that the probability for a given $\alpha \in K$ to be a cyclic vector is

$$(1 - q^{-n_1}) \cdots (1 - q^{-n_t}).$$

RS skew-differential codes over finite fields.

Let us assume here that $K = \mathbb{F}$ is the finite field with p^r elements for some prime p, so our codes become linear block codes over the alphabet $\mathbb{F}$. Let τ be the Frobenius automorphism of $\mathbb{F}$.
The steps of the design method of an RS skew-differential block code may be then enumerated as follows:

1. Choose a natural $0 < h < r$, and set $\sigma = \tau^h$ and $m = \frac{r}{(r,h)}$, the order of σ, which will also become the length of the code.
2. Choose v and u in $\mathbb{F}$, with $u + v \neq 0$, in order to set the σ-derivation $\delta : \mathbb{F} \to \mathbb{F}$ as $\delta(c) = v(\sigma(c) - c)$ and the additive map φ_u as $\varphi_u(c) = \sigma(c)u + \delta(c)$ for every $c \in \mathbb{F}$.

---

[3] Setting $K^{\varphi_u} = \mathbb{F}_q$, and $n_1, \dots, n_t$ the degrees of the distinct irreducible factors appearing in the canonical factorization of the minimal polynomial $\mu \in \mathbb{F}_q[X]$, we obtain that the probability for a given $\alpha \in K$ to be a cyclic vector is

$$(1 - q^{-n_1}) \cdots (1 - q^{-n_t}).$$

RS skew-differential codes over finite fields.

Let us assume here that $K = \mathbb{F}$ is the finite field with p^r elements for some prime p, so our codes become linear block codes over the alphabet $\mathbb{F}$. Let τ be the Frobenius automorphism of $\mathbb{F}$.
The steps of the design method of an RS skew-differential block code may be then enumerated as follows:

1. Choose a natural $0 < h < r$, and set $\sigma = \tau^h$ and $m = \frac{r}{(r,h)}$, the order of σ, which will also become the length of the code.
2. Choose v and u in $\mathbb{F}$, with $u + v \neq 0$, in order to set the σ-derivation $\delta : \mathbb{F} \to \mathbb{F}$ as $\delta(c) = v(\sigma(c) - c)$ and the additive map φ_u as $\varphi_u(c) = \sigma(c)u + \delta(c)$ for every $c \in \mathbb{F}$.
3. By a random[3] search, find a cyclic vector α.

[3] Setting $K^{\varphi_u} = \mathbb{F}_q$, and $n_1, \dots, n_t$ the degrees of the distinct irreducible factors appearing in the canonical factorization of the minimal polynomial $\mu \in \mathbb{F}_q[X]$, we obtain that the probability for a given $\alpha \in K$ to be a cyclic vector is

$$(1 - q^{-n_1}) \cdots (1 - q^{-n_t}).$$

RS skew-differential codes over finite fields.

Let us assume here that $K = \mathbb{F}$ is the finite field with p^r elements for some prime p, so our codes become linear block codes over the alphabet $\mathbb{F}$. Let τ be the Frobenius automorphism of $\mathbb{F}$.

The steps of the design method of an RS skew-differential block code may be then enumerated as follows:

1. Choose a natural $0 < h < r$, and set $\sigma = \tau^h$ and $m = \frac{r}{(r,h)}$, the order of σ, which will also become the length of the code.
2. Choose v and u in $\mathbb{F}$, with $u + v \neq 0$, in order to set the σ-derivation $\delta : \mathbb{F} \to \mathbb{F}$ as $\delta(c) = v(\sigma(c) - c)$ and the additive map φ_u as $\varphi_u(c) = \sigma(c)u + \delta(c)$ for every $c \in \mathbb{F}$.
3. By a random[3] search, find a cyclic vector α.
4. Finally, choose a designed distance $3 \leq d \leq m$, and set the parity check matrix H as in Definition 2.

[3] Setting $K^{\varphi_u} = \mathbb{F}_q$, and $n_{\mathbf{1}}, \dots, n_t$ the degrees of the distinct irreducible factors appearing in the canonical factorization of the minimal polynomial $\mu \in \mathbb{F}_q[X]$, we obtain that the probability for a given $\alpha \in K$ to be a cyclic vector is

$$(1 - q^{-n_{\mathbf{1}}}) \cdots (1 - q^{-n_t}).$$

Example

- Consider $\mathbb{F} = \mathbb{F}_2(a)$ the field with $256 = 2^8$ elements, where $a^8 + a^4 + a^3 + a^2 + 1 = 0$.

Example

- Consider $\mathbb{F} = \mathbb{F}_2(a)$ the field with $256 = 2^8$ elements, where $a^8 + a^4 + a^3 + a^2 + 1 = 0$.
- Let σ be the Frobenius automorphism of $\mathbb{F}$, that is, $\sigma(c) = c^2$ for any $c \in \mathbb{F}$, which has order $m = 8$. Then our code is of length 8.

Example

- Consider $\mathbb{F} = \mathbb{F}_2(a)$ the field with $256 = 2^8$ elements, where $a^8 + a^4 + a^3 + a^2 + 1 = 0$.
- Let σ be the Frobenius automorphism of $\mathbb{F}$, that is, $\sigma(c) = c^2$ for any $c \in \mathbb{F}$, which has order $m = 8$. Then our code is of length 8.
- We set $v = a$, yielding the σ-derivation given by $\delta(c) = ac^2 + ac$ for every $c \in \mathbb{F}$, and $u = a^2$, so $\varphi_u(c) = a^{26}c^2 + ac$ for every $c \in \mathbb{F}$.

Example

- Consider $\mathbb{F} = \mathbb{F}_2(a)$ the field with $256 = 2^8$ elements, where $a^8 + a^4 + a^3 + a^2 + 1 = 0$.
- Let σ be the Frobenius automorphism of $\mathbb{F}$, that is, $\sigma(c) = c^2$ for any $c \in \mathbb{F}$, which has order $m = 8$. Then our code is of length 8.
- We set $v = a$, yielding the σ-derivation given by $\delta(c) = ac^2 + ac$ for every $c \in \mathbb{F}$, and $u = a^2$, so $\varphi_u(c) = a^{26}c^2 + ac$ for every $c \in \mathbb{F}$.
- We now choose $\alpha = a^9$. The matrix A from Proposition 1 takes now the form

$$A = \begin{pmatrix} a^9 & a^{146} & a^{103} & a^{244} & a^{214} & a^{89} & a & a^{200} \\ a^{146} & a^{103} & a^{244} & a^{214} & a^{89} & a & a^{200} & a^{237} \\ a^{103} & a^{244} & a^{214} & a^{89} & a & a^{200} & a^{237} & a^{95} \\ a^{244} & a^{214} & a^{89} & a & a^{200} & a^{237} & a^{95} & a^{105} \\ a^{214} & a^{89} & a & a^{200} & a^{237} & a^{95} & a^{105} & a^{175} \\ a^{89} & a & a^{200} & a^{237} & a^{95} & a^{105} & a^{175} & a^{184} \\ a & a^{200} & a^{237} & a^{95} & a^{105} & a^{175} & a^{184} & a^{21} \\ a^{200} & a^{237} & a^{95} & a^{105} & a^{175} & a^{184} & a^{21} & a^{159} \end{pmatrix}.$$

Example

- Consider $\mathbb{F} = \mathbb{F}_2(a)$ the field with $256 = 2^8$ elements, where $a^8 + a^4 + a^3 + a^2 + 1 = 0$.
- Let σ be the Frobenius automorphism of $\mathbb{F}$, that is, $\sigma(c) = c^2$ for any $c \in \mathbb{F}$, which has order $m = 8$. Then our code is of length 8.
- We set $v = a$, yielding the σ-derivation given by $\delta(c) = ac^2 + ac$ for every $c \in \mathbb{F}$, and $u = a^2$, so $\varphi_u(c) = a^{26}c^2 + ac$ for every $c \in \mathbb{F}$.
- We now choose $\alpha = a^9$. The matrix A from Proposition 1 takes now the form

$$A = \begin{pmatrix} a^9 & a^{146} & a^{103} & a^{244} & a^{214} & a^{89} & a & a^{200} \\ a^{146} & a^{103} & a^{244} & a^{214} & a^{89} & a & a^{200} & a^{237} \\ a^{103} & a^{244} & a^{214} & a^{89} & a & a^{200} & a^{237} & a^{95} \\ a^{244} & a^{214} & a^{89} & a & a^{200} & a^{237} & a^{95} & a^{105} \\ a^{214} & a^{89} & a & a^{200} & a^{237} & a^{95} & a^{105} & a^{175} \\ a^{89} & a & a^{200} & a^{237} & a^{95} & a^{105} & a^{175} & a^{184} \\ a & a^{200} & a^{237} & a^{95} & a^{105} & a^{175} & a^{184} & a^{21} \\ a^{200} & a^{237} & a^{95} & a^{105} & a^{175} & a^{184} & a^{21} & a^{159} \end{pmatrix}.$$

- The determinant of A equals a^{47}, so that α is a cyclic vector. Finally, we set a designed distance $d = 5$.

Example

Let then $C = C_{(\varphi_u, a^9, 5)} \subseteq \mathbb{F}^8$ be the $[8,4,5]_{256}$-linear code defined as the left kernel of the matrix H below.

From H, by standard methods, we have also computed a generating matrix G.

$$H = \begin{pmatrix} a^9 & a^{146} & a^{103} & a^{244} \\ a^{146} & a^{103} & a^{244} & a^{214} \\ a^{103} & a^{244} & a^{214} & a^{89} \\ a^{244} & a^{214} & a^{89} & a \\ a^{214} & a^{89} & a & a^{200} \\ a^{89} & a & a^{200} & a^{237} \\ a & a^{200} & a^{237} & a^{95} \\ a^{200} & a^{237} & a^{95} & a^{105} \end{pmatrix} \text{ and } G = \begin{pmatrix} 1 & 0 & 0 & 0 & a^{105} & a^{69} & a^{221} & a^{41} \\ 0 & 1 & 0 & 0 & a^{109} & a^{25} & a^{232} & a^{166} \\ 0 & 0 & 1 & 0 & a^{145} & a^{54} & a^{104} & a^{36} \\ 0 & 0 & 0 & 1 & a^{251} & a^{141} & a^{42} & a^{60} \end{pmatrix}.$$

Example

Let us exemplify the encoding-decoding process. The error-correcting capacity of C is $\tau = 2$.

Example

Let us exemplify the encoding-decoding process. The error-correcting capacity of C is $\tau = 2$.

Suppose we want to transmit the message

$$M = \left(a^{61}, a^{102}, a^{182}, a^{250}\right),$$

so that we encode it to a codeword

$$c = MG = \left(a^{61}, a^{102}, a^{182}, a^{250}, a^{33}, a^{126}, a^{121}, a^{226}\right) \in C.$$

Example

Let us exemplify the encoding-decoding process. The error-correcting capacity of C is $\tau = 2$.

Suppose we want to transmit the message

$$M = \left(a^{61}, a^{102}, a^{182}, a^{250}\right),$$

so that we encode it to a codeword

$$c = MG = \left(a^{61}, a^{102}, a^{182}, a^{250}, a^{33}, a^{126}, a^{121}, a^{226}\right) \in C.$$

During the transmission, c is corrupted by adding the error vector

$$e = \left(0, a^{2}, 0, a^{2}, 0, 0, 0, 0\right),$$

yielding then the received word

$$y = c + e = \left(a^{61}, a^{6}, a^{182}, a^{107}, a^{33}, a^{126}, a^{121}, a^{226}\right).$$

Example

Now, we run our decoding algorithm.

- We first calculate the syndromes

$$yH = \left(a^{32}, a^{96}, a^{250}, a^{236}\right) \neq 0,$$

  so it is detected some error.

Example

Now, we run our decoding algorithm.

- We first calculate the syndromes

$$yH = \left(a^{32}, a^{96}, a^{250}, a^{236}\right) \neq 0,$$

  so it is detected some error.

- The syndrome matrix computed according to (4) is then

$$S = \begin{pmatrix} a^{32} & a^{3} \\ a^{96} & a^{67} \\ a^{250} & a^{221} \end{pmatrix}.$$

Example

Now, we run our decoding algorithm.

- We first calculate the syndromes

$$yH = \left(a^{32}, a^{96}, a^{250}, a^{236}\right) \neq 0,$$

  so it is detected some error.

- The syndrome matrix computed according to (4) is then

$$S = \begin{pmatrix} a^{32} & a^{3} \\ a^{96} & a^{67} \\ a^{250} & a^{221} \end{pmatrix}.$$

- The first column of S is a multiple of its second column, so that S has rank 1 and, henceforth, $\theta = 1$.

Example

Now, we run our decoding algorithm.

- We first calculate the syndromes
$$yH = \left(a^{32}, a^{96}, a^{250}, a^{236}\right) \neq 0,$$
so it is detected some error.
- The syndrome matrix computed according to (4) is then
$$S = \begin{pmatrix} a^{32} & a^{3} \\ a^{96} & a^{67} \\ a^{250} & a^{221} \end{pmatrix}.$$
- The first column of S is a multiple of its second column, so that S has rank 1 and, henceforth, $\theta = 1$.
- Therefore, the matrix B in Proposition 3 takes the form
$$B = \begin{pmatrix} a^{32} \\ a^{96} \end{pmatrix}.$$
and a basis of its left kernel is provided by the vector
$$\rho = \left(a, a^{192}\right).$$

Example

- The matrix L defined in (6) becomes

$$L = \begin{pmatrix} a & a^{192} & 0 & 0 & 0 & 0 & 0 & 0 \\ a^{27} & a^{125} & a^{129} & 0 & 0 & 0 & 0 & 0 \\ a^{132} & a^{44} & a^{148} & a^{3} & 0 & 0 & 0 & 0 \\ a^{193} & a^{105} & a^{215} & a^{102} & a^{6} & 0 & 0 & 0 \\ a^{222} & a^{134} & a^{212} & a^{108} & a^{134} & a^{12} & 0 & 0 \\ a^{205} & a^{117} & a^{209} & a^{216} & a^{212} & a^{25} & a^{24} & 0 \\ a^{158} & a^{70} & a^{195} & a^{206} & a^{88} & a^{245} & a^{222} & a^{48} \end{pmatrix},$$

Example

- The matrix L defined in (6) becomes

$$L = \begin{pmatrix} a & a^{192} & 0 & 0 & 0 & 0 & 0 & 0 \\ a^{27} & a^{125} & a^{129} & 0 & 0 & 0 & 0 & 0 \\ a^{132} & a^{44} & a^{148} & a^{3} & 0 & 0 & 0 & 0 \\ a^{193} & a^{105} & a^{215} & a^{102} & a^{6} & 0 & 0 & 0 \\ a^{222} & a^{134} & a^{212} & a^{108} & a^{134} & a^{12} & 0 & 0 \\ a^{205} & a^{117} & a^{209} & a^{216} & a^{212} & a^{25} & a^{24} & 0 \\ a^{158} & a^{70} & a^{195} & a^{206} & a^{88} & a^{245} & a^{222} & a^{48} \end{pmatrix},$$

- and LA results

$$LA = \begin{pmatrix} a^{246} & a^{98} & a^{77} & a^{98} & a^{245} & a^{164} & a^{146} & a^{23} \\ a^{137} & a^{27} & a^{44} & a^{27} & a^{24} & a^{129} & a^{103} & a^{22} \\ a^{203} & a^{169} & a^{175} & a^{169} & a^{222} & a^{76} & a^{244} & a^{124} \\ a^{26} & a^{40} & a^{184} & a^{40} & a^{160} & a^{124} & a^{214} & a^{58} \\ a^{10} & a^{203} & a^{21} & a^{203} & a^{155} & a^{58} & a^{89} & a^{116} \\ a^{43} & a^{26} & a^{159} & a^{26} & a^{25} & a^{116} & a & a^{169} \\ a^{61} & a^{10} & a^{198} & a^{10} & a^{28} & a^{169} & a^{200} & a^{40} \end{pmatrix}.$$

Example

- The identification of the positions $k \in \{0, 1 \dots, 7\}$ such that $\epsilon_k \notin \mathrm{Row}(LA)$ can be easily done if we compute the row reduced echelon form of LA,

$$LA_{rref} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example

- The identification of the positions $k \in \{0, 1 \dots, 7\}$ such that $\epsilon_k \notin \mathrm{Row}(LA)$ can be easily done if we compute the row reduced echelon form of LA,

$$LA_{rref} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- It is clear that ϵ_1 and ϵ_3 do not belong to $\mathrm{Row}(LA)$. Therefore, there are errors at positions 1 and 3.

Example

- The identification of the positions $k \in \{0, 1 \ldots, 7\}$ such that $\epsilon_k \notin \mathrm{Row}(LA)$ can be easily done if we compute the row reduced echelon form of LA,

$$LA_{rref} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- It is clear that ϵ_1 and ϵ_3 do not belong to $\mathrm{Row}(LA)$. Therefore, there are errors at positions 1 and 3.
- We finally need to solve a linear system in order to recover the error values. Indeed, the error values are the solution of the system

$$\begin{pmatrix} a^{146} & a^{103} \\ a^{244} & a^{214} \end{pmatrix} \begin{pmatrix} e_1 \\ e_3 \end{pmatrix} = \begin{pmatrix} a^{32} & a^{96} \end{pmatrix}.$$

Example

- The identification of the positions $k \in \{0, 1 \ldots, 7\}$ such that $\epsilon_k \notin \mathrm{Row}(LA)$ can be easily done if we compute the row reduced echelon form of LA,

$$LA_{rref} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- It is clear that ϵ_1 and ϵ_3 do not belong to $\mathrm{Row}(LA)$. Therefore, there are errors at positions 1 and 3.
- We finally need to solve a linear system in order to recover the error values. Indeed, the error values are the solution of the system

$$\begin{pmatrix} a^{146} & a^{103} \\ a^{244} & a^{214} \end{pmatrix} \begin{pmatrix} e_1 \\ e_3 \end{pmatrix} = \begin{pmatrix} a^{32} & a^{96} \end{pmatrix}.$$

- The solution is, as expected, $e_1 = a^2$ and $e_3 = a^2$.

Mathematical setup and proofs

The aim of this part is to prove the mathematical results that ground our decoding algorithm.

Mathematical setup and proofs

The aim of this part is to prove the mathematical results that ground our decoding algorithm.

So, let (σ, δ) be a skew-derivation on a field K. Recall that, for each $u \in K$, we define

$$\varphi_u(a) = \sigma(a)u + \delta(a), \tag{8}$$

for all $a \in K$, thus obtaining a map $\varphi_u : K \to K$.

Mathematical setup and proofs

The aim of this part is to prove the mathematical results that ground our decoding algorithm.

So, let (σ, δ) be a skew-derivation on a field K. Recall that, for each $u \in K$, we define

$$\varphi_u(a) = \sigma(a)u + \delta(a), \tag{8}$$

for all $a \in K$, thus obtaining a map $\varphi_u : K \to K$. This additive map becomes right K^{φ_u}–linear, where

$$K^{\varphi_u} = \{b \in K : \varphi_u(ab) = \varphi_u(a)b \text{ for all } a \in K\}$$

is the φ_u–invariant subfield of K.

Mathematical setup and proofs

The aim of this part is to prove the mathematical results that ground our decoding algorithm.

So, let (σ, δ) be a skew-derivation on a field K. Recall that, for each $u \in K$, we define

$$\varphi_u(a) = \sigma(a)u + \delta(a), \tag{8}$$

for all $a \in K$, thus obtaining a map $\varphi_u : K \to K$. This additive map becomes right K^{φ_u}–linear, where

$$K^{\varphi_u} = \{b \in K : \varphi_u(ab) = \varphi_u(a)b \text{ for all } a \in K\}$$

is the φ_u–invariant subfield of K.

Set

- $\mathrm{End}(K)$ the ring of endomorphisms of K as an additive group.
- $\mathcal{R}$ the subring of $\mathrm{End}(K)$ generated by K and φ_u.
- Here, K is seen as a subring of $\mathrm{End}(K)$ by considering each element a of K as the additive endomorphism given by multiplication by a.

Mathematical setup and proofs

Proposition 5

If the dimension of K as a K^{φ_u}–vector space is $m < \infty$, then the minimal polynomial of φ_u as a K^{φ_u}–linear map has degree m. Consequently, φ_u has at least a cyclic vector $\alpha \in K$. Moreover,

$$\mathcal{R} = K \oplus K\varphi_u \oplus \cdots \oplus K\varphi_u^{m-1}. \qquad (9)$$

Proposition 5

If the dimension of K as a K^{φ_u}–vector space is $m < \infty$, then the minimal polynomial of φ_u as a K^{φ_u}–linear map has degree m. Consequently, φ_u has at least a cyclic vector $\alpha \in K$. Moreover,

$$\mathcal{R} = K \oplus K\varphi_u \oplus \cdots \oplus K\varphi_u^{m-1}. \tag{9}$$

Proof.

It easily follows from (1) that, in $\mathrm{End}(K)$,

$$\varphi_u a = \sigma(a)\varphi_u + \delta(a), \tag{10}$$

for all $a \in K$. This implies that $\mathcal{R} = K + K\varphi_u + K\varphi_u^2 + \cdots$.

Mathematical setup and proofs

Proposition 5

If the dimension of K as a K^{φ_u}–vector space is $m < \infty$, then the minimal polynomial of φ_u as a K^{φ_u}–linear map has degree m. Consequently, φ_u has at least a cyclic vector $\alpha \in K$. Moreover,

$$\mathcal{R} = K \oplus K\varphi_u \oplus \cdots \oplus K\varphi_u^{m-1}. \tag{9}$$

Proof.

It easily follows from (1) that, in $\mathrm{End}(K)$,

$$\varphi_u a = \sigma(a)\varphi_u + \delta(a), \tag{10}$$

for all $a \in K$. This implies that $\mathcal{R} = K + K\varphi_u + K\varphi_u^2 + \cdots$.

Now, since $\dim_{K^{\varphi_u}} K = m$, the minimal polynomial of φ_u as a K^{φ_u}–linear map has degree $n \leq m$. This in particular implies that $\mathcal{R} = K + K\varphi_u + \cdots + K\varphi_u^{n-1}$.

Mathematical setup and proofs

Proposition 5

If the dimension of K as a K^{φ_u}–vector space is $m < \infty$, then the minimal polynomial of φ_u as a K^{φ_u}–linear map has degree m. Consequently, φ_u has at least a cyclic vector $\alpha \in K$. Moreover,

$$\mathcal{R} = K \oplus K\varphi_u \oplus \cdots \oplus K\varphi_u^{m-1}. \tag{9}$$

Proof.

It easily follows from (1) that, in $\mathrm{End}(K)$,

$$\varphi_u a = \sigma(a)\varphi_u + \delta(a), \tag{10}$$

for all $a \in K$. This implies that $\mathcal{R} = K + K\varphi_u + K\varphi_u^2 + \cdots$.

Now, since $\dim_{K^{\varphi_u}} K = m$, the minimal polynomial of φ_u as a K^{φ_u}–linear map has degree $n \leq m$. This in particular implies that $\mathcal{R} = K + K\varphi_u + \cdots + K\varphi_u^{n-1}$.

On the other hand, by Jacobson-Bourbaki's correspondence, $m = \dim_K \mathcal{R}$. We thus derive that $n = m$ and (9). □

Mathematical setup

From now on, we assume that $\dim_{K^{\varphi_u}} K = m < \infty$. According to Proposition 5, the minimal equation of φ_u over K^{φ_u} has degree m, that is, is of the form

$$0 = \varphi_u^m + \mu_{m-1}\varphi_u^{m-1} + \cdots + \mu_1\varphi_u + \mu_0 \tag{11}$$

with $\mu_i \in K^{\varphi_u}$ for $i = 0, \ldots, m-1$.

Let $\alpha \in K$. For any subset $\{t_1, \dots, t_n\} \subseteq \{0, \dots, m-1\}$, define, as in

[DL] J. Delenclos and A. Leroy. *Noncommutative symmetric functions and W-polynomials.* Journal of Algebra and Its Applications, 6 (2007), 815–837,

the matrix

$$W(\varphi_u^{t_1}(\alpha), \dots, \varphi_u^{t_n}(\alpha)) = \begin{pmatrix} \varphi_u^{t_1}(\alpha) & \varphi_u^{t_2}(\alpha) & \cdots & \varphi_u^{t_n}(\alpha) \\ \varphi_u^{t_1+1}(\alpha) & \varphi_u^{t_2+1}(\alpha) & \cdots & \varphi_u^{t_n+1}(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_u^{t_1+n-1}(\alpha) & \varphi_u^{t_2+n-1}(\alpha) & \cdots & \varphi_u^{t_n+n-1}(\alpha) \end{pmatrix}.$$

Lemma 6 (DL, Theorem 5.3)

Given $\alpha \in K$, the following conditions are equivalent.

1. α *is a cyclic vector for the* K^{φ_u}*–linear map* φ_u.
2. $W(\alpha, \varphi_u(\alpha), \dots, \varphi_u^{m-1}(\alpha))$ *is an invertible matrix.*
3. $W(\varphi_u^{t_1}(\alpha), \dots, \varphi_u^{t_n}(\alpha))$ *is an invertible matrix for every subset* $\{t_1, \dots, t_n\} \subseteq \{0, \dots, m-1\}$.

Lemma 6 (DL, Theorem 5.3)

Given $\alpha \in K$, the following conditions are equivalent.

1. α *is a cyclic vector for the* K^{φ_u}*–linear map* φ_u.
2. $W(\alpha, \varphi_u(\alpha), \ldots, \varphi_u^{m-1}(\alpha))$ *is an invertible matrix.*
3. $W(\varphi_u^{t_1}(\alpha), \ldots, \varphi_u^{t_n}(\alpha))$ *is an invertible matrix for every subset* $\{t_1, \ldots, t_n\} \subseteq \{0, \ldots, m-1\}$.

Proof.

For every nonzero $c \in K$, consider the conjugate of u by c:

$$ {}^{c}u = \sigma(c)uc^{-1} + \delta(c)c^{-1}. $$

Lemma 6 (DL, Theorem 5.3)

Given $\alpha \in K$, the following conditions are equivalent.

1. α *is a cyclic vector for the* K^{φ_u}*–linear map* φ_u.
2. $W(\alpha, \varphi_u(\alpha), \dots, \varphi_u^{m-1}(\alpha))$ *is an invertible matrix.*
3. $W(\varphi_u^{t_1}(\alpha), \dots, \varphi_u^{t_n}(\alpha))$ *is an invertible matrix for every subset* $\{t_1, \dots, t_n\} \subseteq \{0, \dots, m-1\}$.

Proof.

For every nonzero $c \in K$, consider the conjugate of u by c:

$$ {}^{c}u = \sigma(c)uc^{-1} + \delta(c)c^{-1}. $$

We get

$$ K^{\varphi_u} = \{c \in K \setminus \{0\} \mid {}^{c}u = u\} \cup \{0\}; $$

the latter being the $(\sigma - \delta)$–centralizer of u in the terminology of [DL].

Lemma 6 (DL, Theorem 5.3)

Given $\alpha \in K$, the following conditions are equivalent.

1. α *is a cyclic vector for the* K^{φ_u}*–linear map* φ_u.
2. $W(\alpha, \varphi_u(\alpha), \ldots, \varphi_u^{m-1}(\alpha))$ *is an invertible matrix.*
3. $W(\varphi_u^{t_1}(\alpha), \ldots, \varphi_u^{t_n}(\alpha))$ *is an invertible matrix for every subset* $\{t_1, \ldots, t_n\} \subseteq \{0, \ldots, m-1\}$.

Proof.

For every nonzero $c \in K$, consider the conjugate of u by c:

$$ {}^{c}u = \sigma(c)uc^{-1} + \delta(c)c^{-1}. $$

We get

$$ K^{\varphi_u} = \{c \in K \setminus \{0\} \mid {}^{c}u = u\} \cup \{0\}; $$

the latter being the $(\sigma - \delta)$–centralizer of u in the terminology of [DL]. Since α is a cyclic vector for φ_u precisely when $\{\alpha, \varphi_u(\alpha), \ldots, \varphi_u^{m-1}(\alpha)\}$ is a K^{φ_u}–basis of K, we may apply [DL, Theorem 5.3] to deduce that the three conditions are equivalent. □

Fix a cyclic vector $\alpha \in K$ of φ_u. From Lemma 6 we get

Theorem 7

For $2 \leq d \leq m$, let $C_{(\varphi_u,\alpha,d)} \subseteq K^m$ be the left kernel of the matrix

$$H = \begin{pmatrix} \alpha & \varphi_u(\alpha) & \cdots & \varphi_u^{d-2}(\alpha) \\ \varphi_u(\alpha) & \varphi_u^2(\alpha) & \cdots & \varphi_u^{d-1}(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_u^{m-1}(\alpha) & \varphi_u^{m}(\alpha) & \cdots & \varphi_u^{m+d-3}(\alpha) \end{pmatrix}, \tag{12}$$

that is, $C_{(\varphi_u,\alpha,d)} = \{c \in K^m : cH = 0\}$. Then $C_{(\varphi_u,\alpha,d)}$ is a K–linear code of dimension $m-d+1$ and minimum Hamming distance d.

Skew polynomial rings

The skew derivation (σ, δ) leads to the construction of a non commutative polynomial ring $R = K[x; \sigma, \delta]$, often called a skew polynomial ring. The elements of R are polynomials in an indeterminate x with coefficients from K written on the left (that is, the monomials $1, x, x^2, \dots$ form a basis of R as a left vector space over K). The multiplication of R is subject to the following rule:

$$xa = \sigma(a)x + \delta(a), \tag{13}$$

for all $a \in K$.

Skew polynomial rings

The skew derivation (σ, δ) leads to the construction of a non commutative polynomial ring $R = K[x; \sigma, \delta]$, often called a skew polynomial ring. The elements of R are polynomials in an indeterminate x with coefficients from K written on the left (that is, the monomials $1, x, x^2, \dots$ form a basis of R as a left vector space over K). The multiplication of R is subject to the following rule:

$$xa = \sigma(a)x + \delta(a), \tag{13}$$

for all $a \in K$.

Proposition 8

The map $\pi : R \to \mathcal{R}$ that sends $\sum_i f_i x^i$ onto $\sum_i f_i \varphi_u^i$ is a surjective ring homomorphism whose kernel is $R\mu = \mu R$, where

$$\mu = x^m + \sum_{i=0}^{m-1} \mu_i x^i$$

is a polynomial in R built from the coefficients of the minimal equation of φ_u, see (11). Hence, there is a left K–linear isomorphism of rings $R/R\mu \cong \mathcal{R}$.

Skew polynomial rings

We may thus identify $\mathcal{R}$ with $R/R\mu$, and, therefore, its elements with polynomials in R with degree smaller than m (this identification makes correspond φ_u with x). This view makes some concepts more natural, like the degree of an element of $\mathcal{R}$.

Skew polynomial rings

We may thus identify $\mathcal{R}$ with $R/R\mu$, and, therefore, its elements with polynomials in R with degree smaller than m (this identification makes correspond φ_u with x). This view makes some concepts more natural, like the degree of an element of $\mathcal{R}$.

The coordinate isomorphism of left K–vector spaces

$$\mathfrak{v} : \mathcal{R} \to K^m, \qquad (\sum_{i=0}^{m-1} f_i x^i \mapsto (f_0, f_1, \ldots, f_{m-1}))$$

allows the transfer of elements and vector subspaces between both K–vector spaces.

Decoding Algorithm's mathematical foundations

Let $c \in C_{(\varphi_u,\alpha,d)}$ be a codeword that is transmitted through a noisy channel, and let

$$y = (y_0, y_1, \ldots, y_{m-1}) \in K^m$$

be the received word.

Decoding Algorithm's mathematical foundations

Let $c \in C_{(\varphi_u,\alpha,d)}$ be a codeword that is transmitted through a noisy channel, and let

$$y = (y_0, y_1, \ldots, y_{m-1}) \in K^m$$

be the received word. We may decompose $y = c + e$, where

$$e = (e_0, e_1, \ldots, e_{m-1}) \in K^m$$

is the error vector.

Decoding Algorithm's mathematical foundations

Let $c \in C_{(\varphi_u,\alpha,d)}$ be a codeword that is transmitted through a noisy channel, and let

$$y = (y_0, y_1, \ldots, y_{m-1}) \in K^m$$

be the received word. We may decompose $y = c + e$, where

$$e = (e_0, e_1, \ldots, e_{m-1}) \in K^m$$

is the error vector. By $k_1, \ldots, k_v \in \{0, 1, \ldots, m-1\}$ we denote the positions where the nonzero error values $e_{k_1}, \ldots, e_{k_v} \in K$ occur.

Decoding Algorithm's mathematical foundations

Let $c \in C_{(\varphi_u,\alpha,d)}$ be a codeword that is transmitted through a noisy channel, and let

$$y = (y_0, y_1, \dots, y_{m-1}) \in K^m$$

be the received word. We may decompose $y = c + e$, where

$$e = (e_0, e_1, \dots, e_{m-1}) \in K^m$$

is the error vector. By $k_1, \dots, k_v \in \{0, 1, \dots, m-1\}$ we denote the positions where the nonzero error values $e_{k_1}, \dots, e_{k_v} \in K$ occur. We prove first that the latter can be computed from y once the positions are known.

Proposition 9

If $0 \leq i \leq d-2$, then

$$\sum_{j=0}^{m-1} y_j \varphi_u^{i+j}(\alpha) = \sum_{j=1}^{v} e_{k_j} \varphi_u^{i+k_j}(\alpha). \qquad (14)$$

Therefore, if $v \leq d-1$, then $(e_{k_1}, \dots, e_{k_v})$ is the unique solution of the linear system of equations

$$\sum_{j=0}^{m-1} y_j \varphi_u^{i+j}(\alpha) = \sum_{j=1}^{v} e_{k_j} \varphi_u^{i+k_j}(\alpha), \qquad (0 \leq i \leq v-1). \qquad (15)$$

Proof.

The equations (14) hold because $C_{(\varphi_u,\alpha,d)}$ is the left kernel of the matrix H defined in (12). The linear system (15) has a unique solution since the matrix

$$\begin{pmatrix} \varphi_u^{k_1}(\alpha) & \varphi_u^{k_1+1}(\alpha) & \cdots & \varphi_u^{k_1+v-1}(\alpha) \\ \varphi_u^{k_2}(\alpha) & \varphi_u^{k_2+1}(\alpha) & \cdots & \varphi_u^{k_2+v-1}(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_u^{k_v}(\alpha) & \varphi_u^{k_v+1}(\alpha) & \cdots & \varphi_u^{k_v+v-1}(\alpha) \end{pmatrix} = W(\varphi_u^{k_1}(\alpha), \dots, \varphi_u^{k_v}(\alpha))^t$$

is invertible by Lemma 6.

□

For every pair (i, k) of non-negative integers, set

$$S_{i,k} = \sum_{j=1}^{v} \varphi_u^{i+k_j}(\alpha)\psi^k(e_{k_j}), \tag{16}$$

where, for all $a \in K$,

$$\psi(a) = \sigma^{-1}(\delta(a) - ua). \tag{17}$$

For every pair (i, k) of non-negative integers, set

$$S_{i,k} = \sum_{j=1}^{v} \varphi_u^{i+k_j}(\alpha)\psi^k(e_{k_j}), \tag{16}$$

where, for all $a \in K$,

$$\psi(a) = \sigma^{-1}(\delta(a) - ua). \tag{17}$$

Lemma 10

For all pairs (i, k) of non-negative integers, we have

$$\sigma(S_{i,k+1}) = \delta(S_{i,k}) - S_{i+1,k} \tag{18}$$

Moreover,

$$S_{i,0} = \sum_{j=0}^{m-1} y_j \varphi_u^{i+j}(\alpha), \tag{19}$$

for every $i = 0, \dots, d-2$, and the values $S_{i,k}$ can be computed recursively by means of (18) from the received word y whenever $i + k \leq d - 2$.

Proof.

Observe that

$$\sigma(a\psi(b)) = \delta(ab) - \varphi_u(a)b, \tag{20}$$

for all $a, b \in K$.

Proof.

Observe that

$$\sigma(a\psi(b)) = \delta(ab) - \varphi_u(a)b, \tag{20}$$

for all $a, b \in K$.Indeed,

$$\begin{aligned} \sigma(a\psi(b)) &\overset{(17)}{=} \sigma(a)(\delta(b) - ub) \\ &\overset{(1)}{=} \delta(ab) - \delta(a)b - \sigma(a)ub \\ &\overset{(8)}{=} \delta(ab) - \varphi_u(a)b. \end{aligned}$$

Proof.

Observe that

$$\sigma(a\psi(b)) = \delta(ab) - \varphi_u(a)b, \tag{20}$$

for all $a, b \in K$.Indeed,

$$\begin{aligned}\sigma(a\psi(b)) &\overset{(17)}{=} \sigma(a)(\delta(b) - ub) \\ &\overset{(1)}{=} \delta(ab) - \delta(a)b - \sigma(a)ub \\ &\overset{(8)}{=} \delta(ab) - \varphi_u(a)b.\end{aligned}$$

For every pair (i, k),

$$\begin{aligned}\sigma(S_{i,k+1}) &\overset{(16)}{=} \textstyle\sum_{j=1}^{v} \sigma(\varphi_u^{i+k_j}(\alpha)\psi^{k+1}(e_{k_j})) \\ &\overset{(20)}{=} \textstyle\sum_{j=1}^{v} \delta(\varphi_u^{i+k_j}(\alpha)\psi^{k}(e_{k_j})) - \sum_{j=1}^{v} \varphi_u^{i+k_j+1}(\alpha)\psi^{k}(e_{k_j}) \\ &\overset{(16)}{=} \delta(S_{i,k}) - S_{i+1,k}.\end{aligned}$$

Proof.

Observe that

$$\sigma(a\psi(b)) = \delta(ab) - \varphi_u(a)b, \qquad (20)$$

for all $a, b \in K$.Indeed,

$$\begin{aligned} \sigma(a\psi(b)) &\overset{(17)}{=} \sigma(a)(\delta(b) - ub) \\ &\overset{(1)}{=} \delta(ab) - \delta(a)b - \sigma(a)ub \\ &\overset{(8)}{=} \delta(ab) - \varphi_u(a)b. \end{aligned}$$

For every pair (i, k),

$$\begin{aligned} \sigma(S_{i,k+1}) &\overset{(16)}{=} \textstyle\sum_{j=1}^{v} \sigma(\varphi_u^{i+k_j}(\alpha)\psi^{k+1}(e_{k_j})) \\ &\overset{(20)}{=} \textstyle\sum_{j=1}^{v} \delta(\varphi_u^{i+k_j}(\alpha)\psi^{k}(e_{k_j})) - \sum_{j=1}^{v} \varphi_u^{i+k_j+1}(\alpha)\psi^{k}(e_{k_j}) \\ &\overset{(16)}{=} \delta(S_{i,k}) - S_{i+1,k}. \end{aligned}$$

Finally, (19) follows from (14). □

Set $T = \{k_1, \ldots, k_v\}$, and let A_T be the submatrix of $A = W(\alpha, \varphi_u(\alpha), \ldots, \varphi_u^{m-1}(\alpha))$ formed by the columns at positions $k_1, \ldots, k_v$, that is

$$A_T = \begin{pmatrix} \varphi_u^{k_1}(\alpha) & \varphi_u^{k_2}(\alpha) & \cdots & \varphi_u^{k_v}(\alpha) \\ \varphi_u^{k_1+1}(\alpha) & \varphi_u^{k_2+1}(\alpha) & \cdots & \varphi_u^{k_v+1}(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_u^{k_1+m-1}(\alpha) & \varphi_u^{k_2+m-1}(\alpha) & \cdots & \varphi_u^{k_v+m-1}(\alpha) \end{pmatrix}.$$

The locator polynomial

Proposition 11

Define, for every $1 \leq r$*, the matrix*

$$E_r = \begin{pmatrix} e_{k_1} & \psi(e_{k_1}) & \cdots & \psi^{r-1}(e_{k_1}) \\ e_{k_2} & \psi(e_{k_2}) & \cdots & \psi^{r-1}(e_{k_2}) \\ \vdots & \vdots & \ddots & \vdots \\ e_{k_v} & \psi(e_{k_v}) & \cdots & \psi^{r-1}(e_{k_v}) \end{pmatrix}.$$

and set

$$\theta = \max\{r : rank\, E_r = r\}.$$

1. *If* $V \subseteq K^m$ *is the left kernel of the matrix* $A_T E_\theta$*, then* $\mathfrak{v}^{-1}(V) = \mathcal{R}\rho$ *for some* $\rho \in \mathcal{R}$ *of degree* θ*.*
2. *If* B *is the matrix formed by the first* $\theta + 1$ *rows of* $A_T E_\theta$*, then we may choose* $\rho = \rho_0 + \rho_1 x + \cdots + \rho_\theta x^\theta$*, for any nonzero vector* $(\rho_0, \rho_1, \ldots, \rho_\theta)$ *in the left kernel of* B*.*

The locator polynomial

(1) We will prove that the K–vector subspace $I = \mathfrak{v}^{-1}(V)$ of $\mathcal{R}$ is a left ideal.

The locator polynomial

(1) We will prove that the K–vector subspace $I = \mathfrak{v}^{-1}(V)$ of $\mathcal{R}$ is a left ideal. To do this, we need just to check that $xI \subseteq I$.

The locator polynomial

(1) We will prove that the K–vector subspace $I = \mathfrak{v}^{-1}(V)$ of $\mathcal{R}$ is a left ideal. To do this, we need just to check that $xI \subseteq I$. Given $\sum_{i=0}^{m-1} a_i x^i \in \mathcal{R}$ we get from (13), since $\mu = 0$ in $\mathcal{R}$, that

$$x\left(\sum_{i=0}^{m-1} a_i x^i\right) = \sum_{i=0}^{m-1} (\sigma(a_{i-1}) + \delta(a_i) - \sigma(a_{m-1})\mu_i)x^i, \tag{21}$$

where we set $a_{-1} = 0$.

The locator polynomial

(1) We will prove that the K–vector subspace $I = \mathfrak{v}^{-1}(V)$ of $\mathcal{R}$ is a left ideal. To do this, we need just to check that $xI \subseteq I$. Given $\sum_{i=0}^{m-1} a_i x^i \in \mathcal{R}$ we get from (13), since $\mu = 0$ in $\mathcal{R}$, that

$$x(\sum_{i=0}^{m-1} a_i x^i) = \sum_{i=0}^{m-1} (\sigma(a_{i-1}) + \delta(a_i) - \sigma(a_{m-1})\mu_i)x^i, \tag{21}$$

where we set $a_{-1} = 0$.

Suppose that $(a_0, \dots, a_{m-2}, a_{m-1})A_T E_\theta = 0$.

The locator polynomial

(1) We will prove that the K–vector subspace $I = \mathfrak{v}^{-1}(V)$ of $\mathcal{R}$ is a left ideal. To do this, we need just to check that $xI \subseteq I$. Given $\sum_{i=0}^{m-1} a_i x^i \in \mathcal{R}$ we get from (13), since $\mu = 0$ in $\mathcal{R}$, that

$$x(\sum_{i=0}^{m-1} a_i x^i) = \sum_{i=0}^{m-1} (\sigma(a_{i-1}) + \delta(a_i) - \sigma(a_{m-1})\mu_i) x^i, \tag{21}$$

where we set $a_{-1} = 0$.

Suppose that $(a_0, \ldots, a_{m-2}, a_{m-1}) A_T E_\theta = 0$. The maximality of θ ensures that the last column of $E_{\theta+1}$ is a linear combination of the former θ columns.

The locator polynomial

(1) We will prove that the K–vector subspace $I = \mathfrak{v}^{-1}(V)$ of $\mathcal{R}$ is a left ideal. To do this, we need just to check that $xI \subseteq I$. Given $\sum_{i=0}^{m-1} a_i x^i \in \mathcal{R}$ we get from (13), since $\mu = 0$ in $\mathcal{R}$, that

$$x(\sum_{i=0}^{m-1} a_i x^i) = \sum_{i=0}^{m-1} (\sigma(a_{i-1}) + \delta(a_i) - \sigma(a_{m-1})\mu_i)x^i, \tag{21}$$

where we set $a_{-1} = 0$.

Suppose that $(a_0, \dots, a_{m-2}, a_{m-1})A_T E_\theta = 0$. The maximality of θ ensures that the last column of $E_{\theta+1}$ is a linear combination of the former θ columns. Hence,

$$(a_0, \dots, a_{m-2}, a_{m-1})A_T E_{\theta+1} = 0.$$

The locator polynomial

(1) We will prove that the K–vector subspace $I = \mathfrak{v}^{-1}(V)$ of $\mathcal{R}$ is a left ideal. To do this, we need just to check that $xI \subseteq I$. Given $\sum_{i=0}^{m-1} a_i x^i \in \mathcal{R}$ we get from (13), since $\mu = 0$ in $\mathcal{R}$, that

$$x\left(\sum_{i=0}^{m-1} a_i x^i\right) = \sum_{i=0}^{m-1} (\sigma(a_{i-1}) + \delta(a_i) - \sigma(a_{m-1})\mu_i) x^i, \qquad (21)$$

where we set $a_{-1} = 0$.

Suppose that $(a_0, \ldots, a_{m-2}, a_{m-1}) A_T E_\theta = 0$. The maximality of θ ensures that the last column of $E_{\theta+1}$ is a linear combination of the former θ columns. Hence,

$$(a_0, \ldots, a_{m-2}, a_{m-1}) A_T E_{\theta+1} = 0.$$

Observe that

$$A_T E_{\theta+1} = \begin{pmatrix} S_{0,0} & S_{0,1} & \cdots & S_{0,\theta} \\ S_{1,0} & S_{1,1} & \cdots & S_{1,\theta} \\ \vdots & \vdots & \ddots & \vdots \\ S_{m-1,0} & S_{m-1,1} & \cdots & S_{m-1,\theta} \end{pmatrix}.$$

The locator polynomial

Therefore,

$$\sum_{i=0}^{m-1} a_i S_{i,k} = 0, \qquad \text{for all } 0 \leq k \leq \theta. \tag{22}$$

The locator polynomial

Therefore,

$$\sum_{i=0}^{m-1} a_i S_{i,k} = 0, \qquad \text{for all } 0 \leq k \leq \theta. \tag{22}$$

For $0 \leq k \leq \theta - 1$ we have

$$\begin{aligned}
\textstyle\sum_{i=0}^{m-1}(\sigma(a_{i-1}) + \delta(a_i))S_{i,k} &\overset{(1)}{=} \textstyle\sum_{i=0}^{m-1}\{\sigma(a_{i-1})S_{i,k} + \delta(a_i S_{i,k}) - \sigma(a_i)\delta(S_{i,k})\} \\
&\overset{(22)}{=} \textstyle\sum_{i=0}^{m-1} \sigma(a_{i-1})S_{i,k} - \sum_{i=0}^{m-1} \sigma(a_i)\delta(S_{i,k}) \\
&\overset{(18)}{=} \textstyle\sum_{i=0}^{m-1} \sigma(a_{i-1})S_{i,k} \\
&\quad \textstyle - \sum_{i=0}^{m-1} \sigma(a_i)[\sigma(S_{i,k+1}) + S_{i+1,k}] \\
&= \textstyle\sum_{i=0}^{m-1} \sigma(a_{i-1})S_{i,k} - \sigma(\sum_{i=0}^{m-1} a_i S_{i,k+1}) \\
&\quad \textstyle - \sum_{i=0}^{m-1} \sigma(a_i)S_{i+1,k} \\
&\overset{(22)}{=} \textstyle\sum_{i=0}^{m-1} \sigma(a_{i-1})S_{i,k} - \sum_{i=0}^{m-1} \sigma(a_i)S_{i+1,k} \\
&= -\sigma(a_{m-1})S_{m,k}.
\end{aligned}$$

The locator polynomial

Since, by (11), $\varphi_u^m + \sum_{i=0}^{m-1} \mu_i \varphi_u^i = 0$, we get

$$\begin{aligned} S_{m,k} &= \sum_{j=1}^{v} \varphi_u^{m+k_j}(\alpha)\psi^k(e_{k_j}) \\ &= \sum_{j=1}^{v}[-\sum_{i=0}^{m-1} \mu_i \varphi_u^{k_j+i}(\alpha)]\psi^k(e_{k_j}) \\ &= -\sum_{i=0}^{m-1} \mu_i \sum_{j=1}^{v} \varphi_u^{k_j+i}(\alpha)\psi^k(e_{k_j}) \\ &= -\sum_{i=0}^{m-1} \mu_i S_{i,k}. \end{aligned}$$

Then $\sum_{i=0}^{m-1}(\sigma(a_{i-1}) + \delta(a_i))S_{i,k} = \sum_{i=0}^{m-1} \sigma(a_{m-1})\mu_i S_{i,k}$ and, therefore,

$$(b_0, b_1, \dots, b_{m-1})A_T E_\theta = 0,$$

where $b_i = \sigma(a_{i-1}) + \delta(a_i) - \sigma(a_{m-1})\mu_i$ for $i = 0, \dots, m-1$.

The locator polynomial

We thus deduce from (21) that $x(\sum_{i=0}^{m-1} a_i x^i) \in I$ whenever $\sum_{i=0}^{m-1} a_i x^i \in I$.

Hence, I is a left ideal of $\mathcal{R}$ and $I = \mathcal{R}\rho$ for some nonzero polynomial ρ. As for its degree concerns, we have

$$\deg \rho = \dim_K \frac{\mathcal{R}}{\mathcal{R}\rho} = \dim_K \frac{K^m}{V} = \theta,$$

since $A_T E_\theta$ is full rank.

The locator polynomial

We thus deduce from (21) that $x(\sum_{i=0}^{m-1} a_i x^i) \in I$ whenever $\sum_{i=0}^{m-1} a_i x^i \in I$.

Hence, I is a left ideal of $\mathcal{R}$ and $I = \mathcal{R}\rho$ for some nonzero polynomial ρ. As for its degree concerns, we have

$$\deg \rho = \dim_K \frac{\mathcal{R}}{\mathcal{R}\rho} = \dim_K \frac{K^m}{V} = \theta,$$

since $A_T E_\theta$ is full rank.

(2) Write $\rho = \rho_0 + \cdots + \rho_\theta x^\theta$. Then the vector $(\rho_0, \ldots, \rho_\theta, 0, \ldots, 0) \in K^m$ belongs to the left kernel of $A_T E_\theta$, and, hence, to the left kernel of B.

The locator polynomial

We thus deduce from (21) that $x(\sum_{i=0}^{m-1} a_i x^i) \in I$ whenever $\sum_{i=0}^{m-1} a_i x^i \in I$.

Hence, I is a left ideal of $\mathcal{R}$ and $I = \mathcal{R}\rho$ for some nonzero polynomial ρ. As for its degree concerns, we have

$$\deg \rho = \dim_K \frac{\mathcal{R}}{\mathcal{R}\rho} = \dim_K \frac{K^m}{V} = \theta,$$

since $A_T E_\theta$ is full rank.

(2) Write $\rho = \rho_0 + \cdots + \rho_\theta x^\theta$. Then the vector $(\rho_0, \ldots, \rho_\theta, 0, \ldots, 0) \in K^m$ belongs to the left kernel of $A_T E_\theta$, and, hence, to the left kernel of B. But every nonzero vector in the left kernel of B gives the coefficients of a polynomial in $\mathcal{R}\rho$, so, since ρ is of minimal degree, such a vector must be a multiple of $(\rho_0, \ldots, \rho_\theta)$.

The error locator matrix

Next, we will construct the error-locator matrix from the polynomial ρ given in Proposition 11.

For $j = 0, \ldots, m-1$ and $i = 0, \ldots m - \theta - 1$, set

$$l_{0,j} = \begin{cases} \rho_j & \text{if } j = 0, \ldots, \theta \\ 0 & \text{if } j = \theta + 1, \ldots, m-1 \end{cases}, \qquad l_{i,-1} = 0.$$

We may then construct a matrix

$$L = \begin{pmatrix} l_{0,0} & l_{0,1} & \cdots & l_{0,m-1} \\ l_{1,0} & l_{1,1} & \cdots & l_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ l_{m-\theta-1,0} & l_{m-\theta-1,1} & \cdots & l_{m-\theta-1,m-1} \end{pmatrix} \tag{23}$$

by defining its entries recursively as

$$l_{i+1,j} = \sigma(l_{i,j-1}) + \delta(l_{i,j}).$$

The error locator matrix

For $i = 0, \ldots, m-1$, let ϵ_i denote the vector of K^m whose i–th component is equal to 1, and every other component is 0. By $Row(LA)$ we denote the row space of the matrix LA.

Theorem 12

If $T = \{k_1, \ldots, k_v\}$ is the set of error positions, then

$$T = \{k \in \{0, \ldots, m-1\} : \epsilon_k \notin Row(LA)\}.$$

The error locator matrix

For $i = 0, \dots, m-1$, let ϵ_i denote the vector of K^m whose i–th component is equal to 1, and every other component is 0. By $Row(LA)$ we denote the row space of the matrix LA.

Theorem 12

If $T = \{k_1, \dots, k_v\}$ is the set of error positions, then

$$T = \{k \in \{0, \dots, m-1\} : \epsilon_k \notin Row(LA)\}.$$

Proof.

According to Proposition 11, $\mathfrak{v}(\mathcal{R}\rho) = \ker(\cdot A_T E_\theta)$. A K–basis of $\mathcal{R}\rho$ is $\{\rho, x\rho, \dots, x^{m-1-\theta}\rho\}$. Hence, the rows of

$$M_\rho = \begin{pmatrix} \mathfrak{v}(\rho) \\ \mathfrak{v}(x\rho) \\ \vdots \\ \mathfrak{v}(x^{m-1-\theta}\rho) \end{pmatrix}$$

give a basis of $\mathfrak{v}(\mathcal{R}\rho)$. A straightforward computation based on (1) leads to $L = M_\rho$.

The error locator matrix

Let I be denote the identity matrix of size $m \times m$, and denote by I_T the submatrix of I formed by the columns at positions $k_1, \dots, k_v$. Note that $A_T = AI_T$.

The error locator matrix

Let I be denote the identity matrix of size $m \times m$, and denote by I_T the submatrix of I formed by the columns at positions $k_1, \dots, k_v$. Note that $A_T = AI_T$.

We have proved that $Row(L) = \ker(\cdot A_T E_\theta)$, so that

$$x \in Row(LA) \Leftrightarrow xA^{-1} \in Row(L) \Leftrightarrow xA^{-1} \in \ker(\cdot A_T E_\theta) \Leftrightarrow x \in \ker(\cdot I_T E_\theta).$$

The error locator matrix

Let I be denote the identity matrix of size $m \times m$, and denote by I_T the submatrix of I formed by the columns at positions $k_1, \dots, k_v$. Note that $A_T = AI_T$.

We have proved that $Row(L) = \ker(\cdot A_T E_\theta)$, so that

$$x \in Row(LA) \Leftrightarrow xA^{-1} \in Row(L) \Leftrightarrow xA^{-1} \in \ker(\cdot A_T E_\theta) \Leftrightarrow x \in \ker(\cdot I_T E_\theta).$$

This implies that $Row(LA) = \ker(\cdot I_T E_\theta)$.

The error locator matrix

Let I be denote the identity matrix of size $m \times m$, and denote by I_T the submatrix of I formed by the columns at positions $k_1, \dots, k_v$. Note that $A_T = AI_T$.

We have proved that $Row(L) = \ker(\cdot A_T E_\theta)$, so that

$$x \in Row(LA) \Leftrightarrow xA^{-1} \in Row(L) \Leftrightarrow xA^{-1} \in \ker(\cdot A_T E_\theta) \Leftrightarrow x \in \ker(\cdot I_T E_\theta).$$

This implies that $Row(LA) = \ker(\cdot I_T E_\theta)$.

Finally, let $i \in \{0, \dots, m-1\}$.
If $i \in T$, then $\epsilon_i I_T E_\theta$ is the i–th row of E_θ, while if $i \notin T$, then $\epsilon_i I_T E_\theta = 0$.

The error locator matrix

Let I be denote the identity matrix of size $m \times m$, and denote by I_T the submatrix of I formed by the columns at positions $k_1, \ldots, k_v$. Note that $A_T = AI_T$.

We have proved that $Row(L) = \ker(\cdot A_T E_\theta)$, so that

$$x \in Row(LA) \Leftrightarrow xA^{-1} \in Row(L) \Leftrightarrow xA^{-1} \in \ker(\cdot A_T E_\theta) \Leftrightarrow x \in \ker(\cdot I_T E_\theta).$$

This implies that $Row(LA) = \ker(\cdot I_T E_\theta)$.

Finally, let $i \in \{0, \ldots, m-1\}$.
If $i \in T$, then $\epsilon_i I_T E_\theta$ is the i–th row of E_θ, while if $i \notin T$, then $\epsilon_i I_T E_\theta = 0$.
Since every row of E_θ is non zero, we get that $\epsilon_i \in Row(LA)$ if and only if $i \notin T$.

So, everything will work whenever we were able to compute

$$\theta = \max\{r : rank\ E_r = r\}.$$

So, everything will work whenever we were able to compute

$$\theta = \max\{r : rank\ E_r = r\}.$$

Lemma 13

For every $r \geq 1$, define the matrix

$$S_r = \begin{pmatrix} S_{0,0} & S_{0,1} & \cdots & S_{0,r-1} \\ S_{1,0} & S_{1,1} & \cdots & S_{1,r-1} \\ \vdots & \vdots & \ddots & \vdots \\ S_{\tau,0} & S_{\tau,1} & \cdots & S_{\tau,r-1} \end{pmatrix}.$$

If $v \leq \tau$, then $\theta = \max\{r : rank\ S_r = r\}$.

Proof.

Observe that $S_r = ME_r$, where

$$M = \begin{pmatrix} \varphi_u^{k_1}(\alpha) & \varphi_u^{k_2}(\alpha) & \cdots & \varphi_u^{k_v}(\alpha) \\ \varphi_u^{k_1+1}(\alpha) & \varphi_u^{k_2+1}(\alpha) & \cdots & \varphi_u^{k_v+1}(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_u^{k_1+\tau}(\alpha) & \varphi_u^{k_2+\tau}(\alpha) & \cdots & \varphi_u^{k_v+\tau}(\alpha) \end{pmatrix}.$$

Since $v \leq \tau$, the rank of M is v due to Lemma 6. We thus get that $rk\, S_r = rk\, E_r$ for all $r \geq 1$, which gives the desired determination of θ. □

Module theoretical locus.

- Set $R = K[x;\sigma,\delta]$ and $0 \neq f \in R$.

Module theoretical locus.

- Set $R = K[x;\sigma,\delta]$ and $0 \neq f \in R$.
- Recall the following general definition [BU]: A *module* (σ,δ)*–code* is an R–submodule of R/Rf.

Module theoretical locus.

- Set $R = K[x;\sigma,\delta]$ and $0 \neq f \in R$.
- Recall the following general definition [BU]: A *module* (σ,δ)*–code* is an R–submodule of R/Rf.
- Our aim here: precisely locate $C_{(\varphi_u,\alpha,d)}$ within the class of module (σ,δ)–codes.

Module theoretical locus.

- Set $R = K[x; \sigma, \delta]$ and $0 \neq f \in R$.
- Recall the following general definition [BU]: A *module* (σ, δ)*–code* is an R–submodule of R/Rf.
- Our aim here: precisely locate $C_{(\varphi_\mu, \alpha, d)}$ within the class of module (σ, δ)–codes.
- Recall that $\mathcal{R} \cong R/R\mu$, and fix the coordinate K–isomorphism $\mathfrak{v} : R/R\mu \to K^m$.

Module theoretical locus.

- Set $R = K[x;\sigma,\delta]$ and $0 \neq f \in R$.
- Recall the following general definition [BU]: A *module* (σ,δ)*–code* is an R–submodule of R/Rf.
- Our aim here: precisely locate $C_{(\varphi_\mu,\alpha,d)}$ within the class of module (σ,δ)–codes.
- Recall that $\mathcal{R} \cong R/R\mu$, and fix the coordinate K–isomorphism $\mathfrak{v} : R/R\mu \to K^m$.
- We identify elements of $\mathcal{R}$ with those in $R/R\mu$, and the latter with polynomials in R of degree at most $m-1$.

Module theoretical locus.

- Set $R = K[x;\sigma,\delta]$ and $0 \neq f \in R$.
- Recall the following general definition [BU]: A *module* (σ,δ)*–code* is an R–submodule of R/Rf.
- Our aim here: precisely locate $C_{(\varphi_u,\alpha,d)}$ within the class of module (σ,δ)–codes.
- Recall that $\mathcal{R} \cong R/R\mu$, and fix the coordinate K–isomorphism $\mathfrak{v} : R/R\mu \to K^m$.
- We identify elements of $\mathcal{R}$ with those in $R/R\mu$, and the latter with polynomials in R of degree at most $m-1$.

Proposition 14

Let $C \subseteq K^m$ a K–vector subspace. Then C is a module (σ,δ)–code in $R/R\mu$ if and only if $C = \mathfrak{v}(\mathcal{R}g)$, where

$$g = [x - {}^{c_1}u, \dots, x - {}^{c_k}u]_\ell, \tag{24}$$

the least common left multiple in R of $x - {}^{c_1}u, \dots, x - {}^{c_k}u$, for some $c_1, \dots, c_k \in K^*$.

Module theoretical locus.

Proof.

- Since $\mathcal{R} \subseteq \mathrm{End}(K)$, we get that K is a left $\mathcal{R}$–module.

Module theoretical locus.

Proof.

- Since $\mathcal{R} \subseteq \mathrm{End}(K)$, we get that K is a left $\mathcal{R}$–module.
- Indeed, it is isomorphic to $R/R(x-u)$.

Module theoretical locus.

Proof.

- Since $\mathcal{R} \subseteq \mathrm{End}(K)$, we get that K is a left $\mathcal{R}$–module.
- Indeed, it is isomorphic to $R/R(x-u)$.
- Now, $\mathcal{R} = \mathrm{End}({}_{K^{\varphi_u}}K)$ (use, for instance, Jacobson-Bourbaki's Theorem).

Module theoretical locus.

Proof.

- Since $\mathcal{R} \subseteq \mathrm{End}(K)$, we get that K is a left $\mathcal{R}$–module.
- Indeed, it is isomorphic to $R/R(x-u)$.
- Now, $\mathcal{R} = \mathrm{End}({}_{K^{\varphi_u}}K)$ (use, for instance, Jacobson-Bourbaki's Theorem).
- So, all simple left $\mathcal{R}$–modules are isomorphic to $R/R(x-u)$.

Module theoretical locus.

Proof.

- Since $\mathcal{R} \subseteq \mathrm{End}(K)$, we get that K is a left $\mathcal{R}$–module.
- Indeed, it is isomorphic to $R/R(x-u)$.
- Now, $\mathcal{R} = \mathrm{End}({}_{K^{\varphi_u}}K)$ (use, for instance, Jacobson-Bourbaki's Theorem).
- So, all simple left $\mathcal{R}$–modules are isomorphic to $R/R(x-u)$.
- Hence, every maximal left ideal of $\mathcal{R}$ is of the form $\mathcal{R}(x - {}^{c}u)$, for some $c \in K$.

Module theoretical locus.

Proof.

- Since $\mathcal{R} \subseteq \mathrm{End}(K)$, we get that K is a left $\mathcal{R}$–module.
- Indeed, it is isomorphic to $R/R(x-u)$.
- Now, $\mathcal{R} = \mathrm{End}({}_{K^{\varphi_u}}K)$ (use, for instance, Jacobson-Bourbaki's Theorem).
- So, all simple left $\mathcal{R}$–modules are isomorphic to $R/R(x-u)$.
- Hence, every maximal left ideal of $\mathcal{R}$ is of the form $\mathcal{R}(x - {}^c u)$, for some $c \in K$.
- Since every left ideal of $\mathcal{R}$ is intersection of finitely many of them, we get the description (24) for their generators.

□

Module theoretical locus.

As a consequence of the results in [DL], we get

Proposition 15

Let $\{c_1, \dots, c_k\} \subseteq K^*$ *be a linearly independent set over* K^{φ_u}*, with* $k \leq m-1$*, and set*

$$g = [x - {}^{c_1}u, \dots, x - {}^{c_k}u]_\ell.$$

Then $deg(g) = k$*,* g *is a right divisor of* μ*, and* $\mathfrak{v}(\mathcal{R}g)$ *is the left kernel of the Wronskian matrix*

$$W_m^u(c_1, \dots, c_k) = \begin{pmatrix} c_1 & c_2 & \cdots & c_k \\ \varphi_u(c_1) & \varphi_u(c_2) & \cdots & \varphi_u(c_k) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_u^{m-1}(c_1) & \varphi_u^{m-1}(c_2) & \cdots & \varphi_u^{m-1}(c_k) \end{pmatrix}$$

Module theoretical locus.

Corollary 16

The code $C_{(\varphi_u,\alpha,d)}$ *is a module* (σ,δ)*–code, endowed with the Hamming metric, given by* $C_{(\varphi_u,\alpha,d)} = \mathfrak{v}(\mathcal{R}g)$*, where*

$$g = [x - {}^{\alpha}u, x - {}^{\varphi_u(\alpha)}u, \dots, x - {}^{\varphi_u^{d-2}(\alpha)}u].$$