On some algebraic interpretation of classical codes

Marta Giorgetti

Department of Physic and Mathematics,
Università dell'Insubria, Como

Soria Summer School on Computational Mathematics
2-11 July 2008

Generalize good properties of cyclic codes

Cyclic codes

- have a rich algebraic structure
    - fast sharp estimates on their most important parameters and
    - exact determination of parameters via commutative algebra techniques;
- posses decoding algorithm which is extremely efficient.

Our goal is to extend algebraic structure of cyclic codes;

Generalize good properties of cyclic codes

Cyclic codes

- have a rich algebraic structure
  - fast sharp estimates on their most important parameters and
  - exact determination of parameters via commutative algebra techniques;
- posses decoding algorithm which is extremely efficient.

Our goal is to extend algebraic structure of cyclic codes;

Generalize good properties of cyclic codes

Cyclic codes

- have a rich algebraic structure
  - fast sharp estimates on their most important parameters and
  - exact determination of parameters via commutative algebra techniques;
- posses decoding algorithm which is extremely efficient.

Our goal is to extend algebraic structure of cyclic codes;

Generalize good properties of cyclic codes

Cyclic codes

- have a rich algebraic structure
  - fast sharp estimates on their most important parameters and
  - exact determination of parameters via commutative algebra techniques;
- posses decoding algorithm which is extremely efficient.

Our goal is to extend algebraic structure of cyclic codes;

Generalize good properties of cyclic codes

Cyclic codes

- have a rich algebraic structure
    - fast sharp estimates on their most important parameters and
    - exact determination of parameters via commutative algebra techniques;
- posses decoding algorithm which is extremely efficient.

  Our goal is to extend algebraic structure of cyclic codes;

Definition

Let

- **q** be a power of prime, $\mathbb{F}_q$ is the finite field of q elements,
- **n** $\in \mathbb{N}, n \geq 1$ such that $(n, q) = 1$,
- $\mathbf{R_n} = \{\bar{z} \in \bar{\mathbb{F}}_q | \bar{z}^n = 1\}$,
- **m** $\in \mathbb{N}, m \geq 1$ such that $R_n \subseteq \mathbb{F}_{q^m}$, not necessary the smallest,
- **L** $\subset R_n \cup \{0\}$, $L = \{l_1, \ldots, l_N\}$,
- $\mathcal{P} = \{g_1(x), g_2(x), \ldots, g_r(x)\} \subset \mathbb{F}_{q^m}[x]$ such that $\forall i = 1, \ldots, N$ exists at least $j = 1, \ldots, r$ such that $g_j(l_i) \neq 0$.

Definition

Let

- **q** be a power of prime, $\mathbb{F}_q$ is the finite field of q elements,
- **n** $\in \mathbb{N}, n \geq 1$ such that $(n, q) = 1$,
- $\mathbf{R_n} = \{\bar{z} \in \bar{\mathbb{F}}_q | \bar{z}^n = 1\}$,
- **m** $\in \mathbb{N}, m \geq 1$ such that $R_n \subseteq \mathbb{F}_{q^m}$, not necessary the smallest,
- **L** $\subset R_n \cup \{0\}$, $L = \{l_1, \dots, l_N\}$,
- $\mathcal{P} = \{g_1(x), g_2(x), \dots, g_r(x)\} \subset \mathbb{F}_{q^m}[x]$ such that $\forall i = 1, \dots, N$ exists at least $j = 1, \dots, r$ such that $g_j(l_i) \neq 0$.

Definition

Let

- **q** be a power of prime, $\mathbb{F}_q$ is the finite field of q elements,
- **n** $\in \mathbb{N}, n \geq 1$ such that $(n, q) = 1$,
- $\mathbf{R_n} = \{\bar{z} \in \bar{\mathbb{F}}_q | \bar{z}^n = 1\}$,
- **m** $\in \mathbb{N}, m \geq 1$ such that $R_n \subseteq \mathbb{F}_{q^m}$, not necessary the smallest,
- **L** $\subset R_n \cup \{0\}$, $L = \{l_1, \ldots, l_N\}$,
- $\mathcal{P} = \{g_1(x), g_2(x), \ldots, g_r(x)\} \subset \mathbb{F}_{q^m}[x]$ such that $\forall i = 1, \ldots, N$ exists at least $j = 1, \ldots, r$ such that $g_j(l_i) \neq 0$.

Definition

Let

- **q** be a power of prime, $\mathbb{F}_q$ is the finite field of q elements,
- **n** $\in \mathbb{N}, n \geq 1$ such that $(n, q) = 1$,
- $\mathbf{R_n} = \{\bar{z} \in \bar{\mathbb{F}}_q | \bar{z}^n = 1\}$,
- **m** $\in \mathbb{N}, m \geq 1$ such that $R_n \subseteq \mathbb{F}_{q^m}$, not necessary the smallest,
- **L** $\subset R_n \cup \{0\}$, $L = \{l_1, \ldots, l_N\}$,
- $\mathcal{P} = \{g_1(x), g_2(x), \ldots, g_r(x)\} \subset \mathbb{F}_{q^m}[x]$ such that $\forall i = 1, \ldots, N$ exists at least $j = 1, \ldots, r$ such that $g_j(l_i) \neq 0$.

Definition

Let

- **q** be a power of prime, $\mathbb{F}_q$ is the finite field of q elements,
- **n** $\in \mathbb{N}, n \geq 1$ such that $(n, q) = 1$,
- $\mathbf{R_n} = \{\bar{z} \in \bar{\mathbb{F}}_q | \bar{z}^n = 1\}$,
- **m** $\in \mathbb{N}, m \geq 1$ such that $R_n \subseteq \mathbb{F}_{q^m}$, not necessary the smallest,
- **L** $\subset R_n \cup \{0\}$, $L = \{l_1, \ldots, l_N\}$,
- $\mathcal{P} = \{g_1(x), g_2(x), \ldots, g_r(x)\} \subset \mathbb{F}_{q^m}[x]$ such that $\forall i = 1, \ldots, N$ exists at least $j = 1, \ldots, r$ such that $g_j(l_i) \neq 0$.

Definition

Let

- **q** be a power of prime, $\mathbb{F}_q$ is the finite field of q elements,
- **n** $\in \mathbb{N}, n \geq 1$ such that $(n, q) = 1$,
- $\mathbf{R_n} = \{\bar{z} \in \bar{\mathbb{F}}_q | \bar{z}^n = 1\}$,
- **m** $\in \mathbb{N}, m \geq 1$ such that $R_n \subseteq \mathbb{F}_{q^m}$, not necessary the smallest,
- **L** $\subset R_n \cup \{0\}$, $L = \{l_1, \ldots, l_N\}$,
- $\mathcal{P} = \{g_1(x), g_2(x), \ldots, g_r(x)\} \subset \mathbb{F}_{q^m}[x]$ such that
  $\forall i = 1, \ldots, N$ exists at least $j = 1, \ldots, r$ such that $g_j(l_i) \neq 0$.

Definition

Then $C = \Omega(q, n, q^m, L, \mathcal{P})$ is the **nth-root code** defined over $\mathbb{F}_q$ such that

$$H = \begin{pmatrix} g_1(l_1), & \ldots, & g_1(l_N) \\ g_2(l_1), & \ldots, & g_2(l_N) \\ \vdots & & \vdots \\ g_r(l_1), & \ldots, & g_r(l_N) \end{pmatrix} = \begin{pmatrix} g_1(L) \\ g_2(L) \\ \vdots \\ g_r(L) \end{pmatrix}$$

is its **parity-check matrix**.

Definition

Remark

$C = (q, n, q^m, L, \mathcal{P})$ is linear over $\mathbb{F}_q$, its length is $N = |L|$ and its distance d is greater than or equal to 2, because there are no columns in H composed only of zeros.

Remark

Since any function from $\mathbb{F}_{q^m}$ to itself can be expressed as a polynomial, we can accept in $\mathcal{P}$ also rational functions of type f/g, $f, g \in \mathbb{F}_{q^m}$, such that $g(\bar{x}) \neq 0$ for any $\bar{x} \in \mathbb{F}_{q^m}$.

Definition

Remark

$C = (q, n, q^m, L, \mathcal{P})$ is linear over $\mathbb{F}_q$, its length is $N = |L|$ and its distance d is greater than or equal to 2, because there are no columns in H composed only of zeros.

Remark

Since any function from $\mathbb{F}_{q^m}$ to itself can be expressed as a polynomial, we can accept in $\mathcal{P}$ also rational functions of type f/g, $f, g \in \mathbb{F}_{q^m}$, such that $g(\bar{x}) \neq 0$ for any $\bar{x} \in \mathbb{F}_{q^m}$.

Properties

Definition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an nth-root code and $v \in (\mathbb{F}_q)^N$.

- If $\bar{L} = \emptyset$, we say that C is **maximal**.
- If $\mathcal{P} \subset \mathbb{F}_q[x]$, we say that C is **proper**.
- If $0 \notin L$, we say that C is **zerofree**, non-zerofree otherwise.

Properties

Definition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an nth-root code and $v \in (\mathbb{F}_q)^N$.

- If $\bar{L} = \emptyset$, we say that C is **maximal**.
- If $\mathcal{P} \subset \mathbb{F}_q[x]$, we say that C is **proper**.
- If $0 \notin L$, we say that C is **zerofree**, non-zerofree otherwise.

Properties

Definition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an nth-root code and $v \in (\mathbb{F}_q)^N$.

- If $\bar{L} = \emptyset$, we say that C is **maximal**.
- If $\mathcal{P} \subset \mathbb{F}_q[x]$, we say that C is **proper**.
- If $0 \notin L$, we say that C is **zerofree**, non-zerofree otherwise.

Properties

Definition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an nth-root code and $v \in (\mathbb{F}_q)^N$.

- If $\bar{L} = \emptyset$, we say that C is **maximal**.
- If $\mathcal{P} \subset \mathbb{F}_q[x]$, we say that C is **proper**.
- If $0 \notin L$, we say that C is **zerofree**, non-zerofree otherwise.

Proposition

Let C be a linear code over $\mathbb{F}_q$ of length N and $d \geq 2$. Then C is an nth-root code for any $n \geq N-1$, $(n,q)=1$. In particular:

1. *if $n = N$, then C can be maximal zerofree,*
2. *if $n = N-1$, then C is maximal non-zerofree.*

Proof

Corollary

Let C be a linear code. C is an nth-root code if and only if $d \geq 2$.

Proposition

Let C be a linear code over $\mathbb{F}_q$ of length N and $d \geq 2$. Then C is an nth-root code for any $n \geq N-1$, $(n,q)=1$. In particular:

1. *if $n = N$, then C can be maximal zerofree,*
2. *if $n = N-1$, then C is maximal non-zerofree.*

▸ Proof

Corollary

Let C be a linear code. C is an nth-root code if and only if $d \geq 2$.

▸▸ Skip proofs

Let C be a linear code over $\mathbb{F}_q$ of length N, dimension k and $d \geq 2$, with parity-check matrix $H = (h_{i,j}) \in (\mathbb{F}_q)^{(N-k)\times N}$. Since $d \geq 2$ there is no $j = 1, \ldots, N$ such that $h_{i,j} = 0, \forall i = 1, \ldots N-k$. Let n be a natural number such that $n \geq N-1$ and $(n,q) = 1$. Let $R_n = \{\alpha_1, \ldots, \alpha_n\}$ be the set of nth-roots of unity over $\mathbb{F}_q$.

- Suppose that $n \geq N$. Let L be a subset of R_n, $|L| = N$, and $r = N-k$. Thanks to the Lagrange interpolation theorem we can find r polynomials $g_i(x) \in \mathbb{F}_{q^m}[x]$ such that $g_i(\alpha_j) = h_{i,j} \, \forall \, \alpha_j \in L$, $i = 1, \ldots, r$, $j = 1, \ldots, N$, viewing any $h_{i,j}$ as an element of $\mathbb{F}_{q^m}$. We collect polynomials $g_i(x)$ in set $\mathcal{P} = \{g_i\}_{1 \leq i \leq r}$. Polynomials $g_i(x)$ are such that for any $i = 1, \cdots, r$ there is at least one $1 \leq j \leq r$ such that $g_j(\alpha_i) \neq 0$. Then it is obvious that code C can be seen as the zerofree nth-root code $\Omega(q, n, q^m, L, \mathcal{P})$.
- With the above construction, if $n = N$ code C is maximal, since $L = R_n$.
- Let L be a set composed of 0 and $N-1$ elements of R_n. With the above argument it is easy to proof that C is a non-zerofree nth-root code. If $n = N-1$, code C is maximal non-zerofree, since $L = R_n \cup \{0\}$.

Back

Let

- $\mathbf{q = 2, n = 7, q^m = 8, L = \mathbb{F}_{2^3}}$,
  $\mathcal{P} = \{\mathbf{g_1(x) = \frac{1}{x^2+x+1}, g_2(x) = \frac{x}{x^2+x+1}}\}$
- $C = \Omega(2, 7, 8, \mathbb{F}_8, \{g_1, g_2\})$ is
  - **non-zerofree** $(0 \in L)$,
  - **maximal** $(\bar{L} = R_n \setminus L = \emptyset)$,
  - **proper** $(g_1(x), g_2(x) \in \mathbb{F}_2(x))$
  - parity-check matrix is the following:

$$H = \begin{pmatrix} g_1(1) & g_1(\beta) & g_1(\beta^2) & g_1(\beta^3) & g_1(\beta^4) & g_1(\beta^5) & g_1(\beta^6) & g_1(0) \\ g_2(1) & g_2(\beta) & g_2(\beta^2) & g_2(\beta^3) & g_2(\beta^4) & g_2(\beta^5) & g_2(\beta^6) & g_2(0) \end{pmatrix},$$

i.e.

$$H = \begin{pmatrix} 1 & \beta^2 & \beta^4 & \beta^2 & \beta & \beta & \beta^4 & 1 \\ 1 & \beta^3 & \beta^6 & \beta^5 & \beta^5 & \beta^6 & \beta^3 & 0 \end{pmatrix}.$$

Let

- $\mathbf{q = 2, n = 7, q^m = 8, L = \mathbb{F}_{2^3}}$,
  $\mathcal{P} = \{\mathbf{g_1(x) = \frac{1}{x^2+x+1}, g_2(x) = \frac{x}{x^2+x+1}}\}$
- $C = \Omega(2, 7, 8, \mathbb{F}_8, \{g_1, g_2\})$ is
  - **non-zerofree** $(0 \in L)$,
  - **maximal** $(\bar{L} = R_n \setminus L = \emptyset)$,
  - **proper** $(g_1(x), g_2(x) \in \mathbb{F}_2(x))$
  - parity-check matrix is the following:

$$H = \begin{pmatrix} g_1(1) & g_1(\beta) & g_1(\beta^2) & g_1(\beta^3) & g_1(\beta^4) & g_1(\beta^5) & g_1(\beta^6) & g_1(0) \\ g_2(1) & g_2(\beta) & g_2(\beta^2) & g_2(\beta^3) & g_2(\beta^4) & g_2(\beta^5) & g_2(\beta^6) & g_2(0) \end{pmatrix},$$

i.e.

$$H = \begin{pmatrix} 1 & \beta^2 & \beta^4 & \beta^2 & \beta & \beta & \beta^4 & 1 \\ 1 & \beta^3 & \beta^6 & \beta^5 & \beta^5 & \beta^6 & \beta^3 & 0 \end{pmatrix}.$$

Let

- $\mathbf{q = 2, n = 7, q^m = 8, L = \mathbb{F}_{2^3}}$,
  $\mathcal{P} = \{\mathbf{g_1(x) = \frac{1}{x^2+x+1}, g_2(x) = \frac{x}{x^2+x+1}}\}$
- $C = \Omega(2, 7, 8, \mathbb{F}_8, \{g_1, g_2\})$ is
  - **non-zerofree** $(0 \in L)$,
  - **maximal** $(\bar{L} = R_n \setminus L = \emptyset)$,
  - **proper** $(g_1(x), g_2(x) \in \mathbb{F}_2(x))$
  - parity-check matrix is the following:

$$H = \begin{pmatrix} g_1(1) & g_1(\beta) & g_1(\beta^2) & g_1(\beta^3) & g_1(\beta^4) & g_1(\beta^5) & g_1(\beta^6) & g_1(0) \\ g_2(1) & g_2(\beta) & g_2(\beta^2) & g_2(\beta^3) & g_2(\beta^4) & g_2(\beta^5) & g_2(\beta^6) & g_2(0) \end{pmatrix},$$

i.e.

$$H = \begin{pmatrix} 1 & \beta^2 & \beta^4 & \beta^2 & \beta & \beta & \beta^4 & 1 \\ 1 & \beta^3 & \beta^6 & \beta^5 & \beta^5 & \beta^6 & \beta^3 & 0 \end{pmatrix}.$$

Let

- $\mathbf{q = 2, n = 7, q^m = 8, L = \mathbb{F}_{2^3}}$,
  $\mathcal{P} = \{\mathbf{g_1(x) = \frac{1}{x^2+x+1}, g_2(x) = \frac{x}{x^2+x+1}}\}$
- $C = \Omega(2, 7, 8, \mathbb{F}_8, \{g_1, g_2\})$ is
  - **non-zerofree** $(0 \in L)$,
  - **maximal** $(\bar{L} = R_n \setminus L = \emptyset)$,
  - **proper** $(g_1(x), g_2(x) \in \mathbb{F}_2(x))$
  - parity-check matrix is the following:

$$H = \begin{pmatrix} g_1(1) & g_1(\beta) & g_1(\beta^2) & g_1(\beta^3) & g_1(\beta^4) & g_1(\beta^5) & g_1(\beta^6) & g_1(0) \\ g_2(1) & g_2(\beta) & g_2(\beta^2) & g_2(\beta^3) & g_2(\beta^4) & g_2(\beta^5) & g_2(\beta^6) & g_2(0) \end{pmatrix},$$

i.e.

$$H = \begin{pmatrix} 1 & \beta^2 & \beta^4 & \beta^2 & \beta & \beta & \beta^4 & 1 \\ 1 & \beta^3 & \beta^6 & \beta^5 & \beta^5 & \beta^6 & \beta^3 & 0 \end{pmatrix}.$$

Let

- $\mathbf{q = 2, n = 7, q^m = 8, L = \mathbb{F}_{2^3}}$,
  $\mathcal{P} = \{\mathbf{g_1(x)} = \frac{\mathbf{1}}{\mathbf{x^2+x+1}}, \mathbf{g_2(x)} = \frac{\mathbf{x}}{\mathbf{x^2+x+1}}\}$
- $C = \Omega(2, 7, 8, \mathbb{F}_8, \{g_1, g_2\})$ is
  - **non-zerofree** $(0 \in L)$,
  - **maximal** $(\bar{L} = R_n \setminus L = \emptyset)$,
  - **proper** $(g_1(x), g_2(x) \in \mathbb{F}_2(x))$
  - parity-check matrix is the following:

$$H = \begin{pmatrix} g_1(1) & g_1(\beta) & g_1(\beta^2) & g_1(\beta^3) & g_1(\beta^4) & g_1(\beta^5) & g_1(\beta^6) & g_1(0) \\ g_2(1) & g_2(\beta) & g_2(\beta^2) & g_2(\beta^3) & g_2(\beta^4) & g_2(\beta^5) & g_2(\beta^6) & g_2(0) \end{pmatrix},$$

i.e.

$$H = \begin{pmatrix} 1 & \beta^2 & \beta^4 & \beta^2 & \beta & \beta & \beta^4 & 1 \\ 1 & \beta^3 & \beta^6 & \beta^5 & \beta^5 & \beta^6 & \beta^3 & 0 \end{pmatrix}.$$

Let

- $\mathbf{q = 2, n = 7, q^m = 8, L} = \mathbb{F}_{2^3}$,
  $\mathcal{P} = \{\mathbf{g_1(x)} = \frac{\mathbf{1}}{\mathbf{x^2+x+1}}, \mathbf{g_2(x)} = \frac{\mathbf{x}}{\mathbf{x^2+x+1}}\}$
- $C = \Omega(2, 7, 8, \mathbb{F}_8, \{g_1, g_2\})$ is
  - **non-zerofree** $(0 \in L)$,
  - **maximal** $(\bar{L} = R_n \setminus L = \emptyset)$,
  - **proper** $(g_1(x), g_2(x) \in \mathbb{F}_2(x))$
  - parity-check matrix is the following:

$$H = \begin{pmatrix} g_1(1) & g_1(\beta) & g_1(\beta^2) & g_1(\beta^3) & g_1(\beta^4) & g_1(\beta^5) & g_1(\beta^6) & g_1(0) \\ g_2(1) & g_2(\beta) & g_2(\beta^2) & g_2(\beta^3) & g_2(\beta^4) & g_2(\beta^5) & g_2(\beta^6) & g_2(0) \end{pmatrix},$$

i.e.

$$H = \begin{pmatrix} 1 & \beta^2 & \beta^4 & \beta^2 & \beta & \beta & \beta^4 & 1 \\ 1 & \beta^3 & \beta^6 & \beta^5 & \beta^5 & \beta^6 & \beta^3 & 0 \end{pmatrix}.$$

It is easy to see that C is an $[8, 2, 5]$ code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

and weight distribution

$$A_0 = 1,\ A_1 = A_2 = A_3 = A_4 = 0,\ A_5 = 2,\ A_6 = 1$$

Let $\mathbf{q} = \mathbf{2}$, $\mathbf{n} = \mathbf{5}$, $\mathbf{q^m} = \mathbf{2^4}$, $\mathbf{L} = \mathbf{R_5}$ and $\mathcal{P} = \{\mathbf{g}\}$, where $g = \gamma^{12}x^4 + \gamma^{11}x^3 + x^2 + \gamma^{14}x + \gamma^3$ and γ is a primitive element of $\mathbb{F}_{16}$ with minimal polynomial $x^4 + x + 1$.
Let $\mathbf{C} = \mathbf{\Omega}(\mathbf{2}, \mathbf{5}, \mathbf{2^4}, \mathbf{R_5}, \mathcal{P})$. Code C is **maximal** ($\bar{L} = \emptyset$) and **zerofree** ($0 \notin L$) and its parity-check matrix is the following:

$$H = \left(g(\gamma^3), g(\gamma^6), g(\gamma^9), g(\gamma^{12}), g(\gamma^{15})\right) = \left(\gamma^6, \gamma^2, \gamma^3, \gamma^{14}, \gamma^{15}\right).$$

It is easy to see that C is an [5,2,3] code with generator matrix

$$G = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{pmatrix}.$$

By contradiction: if C is proper maximal
then $C = \Omega(2,5,2^4,R_5,\mathcal{P}')$, where $\mathcal{P}' = \{g_1',\dots,g_r'\} \subset \mathbb{F}_2[x]$.
Its parity-check matrix is then

$$H' = \begin{pmatrix} g_1'(\gamma^3), & g_1'(\gamma^6), & g_1'(\gamma^9), & g_1'(\gamma^{12}), & g_1'(\gamma^{15}) \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ g_i'(\gamma^3), & g_i'(\gamma^6), & g_i'(\gamma^9), & g_i'(\gamma^{12}), & g_i'(\gamma^{15}) \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ g_r'(\gamma^3), & g_r'(\gamma^6), & g_r'(\gamma^9), & g_r'(\gamma^{12}), & g_r'(\gamma^{15}) \end{pmatrix}.$$

Let

$$\mathbf{e_1} = \mathbf{g_i'}(\gamma^{\mathbf{3}}),\ \mathbf{e_2} = \mathbf{g_i'}(\gamma^{\mathbf{6}}),\ \mathbf{e_3} = \mathbf{g_i'}(\gamma^{\mathbf{9}}),\ \mathbf{e_4} = \mathbf{g_i'}(\gamma^{\mathbf{12}}),\ \mathbf{e_5} = \mathbf{g_i'}(\gamma^{\mathbf{15}}),$$

for some $i = 1,\dots,r$ and
they must satisfy $\mathbf{e_1}+\mathbf{e_2}+\mathbf{e_3} = \mathbf{0}$ and $\mathbf{e_3}+\mathbf{e_4}+\mathbf{e_5} = \mathbf{0}$.

$$\mathbf{J} \subset \mathbb{F}_{\mathbf{16}}[\mathbf{b_0}, \ldots, \mathbf{b_{15}}, \mathbf{e_1}, \ldots, \mathbf{e_5}]$$

has at least a solution $\varepsilon = (\bar{\mathbf{b}}_\mathbf{0}, \ldots, \bar{\mathbf{b}}_\mathbf{15}, \bar{\mathbf{e}}_\mathbf{1}, \ldots, \bar{\mathbf{e}}_\mathbf{5})$ in $\mathcal{V}(J)$ such that $(\bar{e}_1, \bar{e}_2, \bar{e}_3, \bar{e}_4, \bar{e}_5) \neq (0,0,0,0,0)$.

$$\begin{array}{llll} J =< & e_1 + e_2 + e_3, & e_3 + e_4 + e_5, & \left\{b_i^2 + b_i\right\}_{0 \le i \le 15}, \\ & \left\{e_i^{16} + e_i\right\}_{1 \le i \le 5}, & g'(\gamma^3) - e_1, & g'(\gamma^6) - e_2, \\ & g'(\gamma^9) - e_3 & g'(\gamma^{12}) - e_4, & g'(\gamma^{15}) - e_5 >, \end{array}$$

A computer computation shows that a **Gröbner basis** of J contains $\{\mathbf{e_1}, \ldots, \mathbf{e_5}\}$ and so $\mathcal{V}(J)$ does not contain ε, hence g' does not exist. This means that **no polynomial in $\mathcal{P}$ can have coefficients in $\mathbb{F}_2$**, which proves our claim.

Remark

In order to define the same nth-root code it is possible to use different n. For example to define a linear code with length $N = 5$, we can use the five 5th roots of unity or five elements chosen from the set of the seven 7th roots of unity.

Let C be a linear binary code, having parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Remark

In order to define the same nth-root code it is possible to use different n. For example to define a linear code with length $N = 5$, we can use the five 5th roots of unity or five elements chosen from the set of the seven 7th roots of unity.

Let C be a linear binary code, having parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

First case: maximal, zerofree nth-root code

$\Omega(2,5,2^4,L_1,\mathcal{P}_1)$, where

$$L_1 = R_5 = \{\gamma^3,\gamma^6,\gamma^9,\gamma^{12},\gamma^{15}\} \subset \mathbb{F}_{16} =<\gamma> \cup \{0\},$$

$$\mathcal{P}_1 \subset \mathbb{F}_{16}[x] \text{ is } \mathcal{P}_1 = \{g_1, g_2\}, \text{ with}$$

$$g_1 = \gamma^7 x^4 + \gamma^{14} x^3 + \gamma^{11} x^2 + \gamma^{13} x + 1,$$

$$g_2 = \gamma^2 x^4 + \gamma^4 x^3 + \gamma x^2 + \gamma^8 x + 1\ .$$

Second case: non-maximal, zerofree nth-root code

$C = \Omega(2,7,2^3,L_2,\mathcal{P}_2)$, where

$$L_2 \subset R_7 = \mathbb{F}_8^* =< \beta >, L_2 = \{\beta,\beta^2,\beta^3,\beta^4,\beta^5\},$$

$$\mathcal{P}_2 \subset \mathbb{F}_{2^3}[t] \text{ is } \mathcal{P}_2 = \{p_1,p_2\}, \text{ with}$$

$$p_1 = t^4 + t^2 + t + 1,$$

$$p_2 = \beta^4 t^4 + \beta^6 t^3 + t + \beta^2 .$$

Third case: non-maximal, non-zerofree nth-root code

$C = \Omega(2, 7, 2^3, L_3, \mathcal{P}_3)$, where

$$L_3 \subset \mathbb{F}_8, L_3 = \{\beta, \beta^2, \beta^3, \beta^4, 0\},$$

$$\mathcal{P}_3 \subset \mathbb{F}_8[z] \text{ is } \mathcal{P}_3 = \{h_1, h_2\}, \text{ with}$$

$$h_1 = \beta^5 z^4 + z^3 + \beta^5 z^2 + \beta^4 z,$$

$$h_2 = \beta^6 z^4 + \beta^3 z^2 + \beta^5 z + 1 \ .$$

First case: maximal, zerofree nth-root code

Second case: non-maximal, zerofree nth-root code

Third case: non-maximal, non-zerofree nth-root code

Observation

Note however that code C cannot be seen as a maximal non-zerofree code.

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an nth-root code, w and $\hat{w}$ be natural numbers such that $2 \leq w \leq N = |L|$, $1 \leq \hat{w} \leq N - 1$.

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an nth-root code, w and $\hat{w}$ be natural numbers such that $2 \leq w \leq N = |L|$, $1 \leq \hat{w} \leq N - 1$. We denote by $J_w(C)$ and $\hat{J}_{\hat{w}}(C)$ the following two ideals:

$$\begin{aligned} J_w = \quad & J_w(C) = \quad J_w(q, n, q^m, L, \mathcal{P}) \subset \quad \mathbb{F}_{q^m}[z_1, \ldots, z_w, y_1, \ldots, y_w], \\ \hat{J}_{\hat{w}} = \quad & \hat{J}_{\hat{w}}(C) = \quad \hat{J}_{\hat{w}}(q, n, q^m, L, \mathcal{P}) \subset \quad \mathbb{F}_{q^m}[z_1, \ldots, z_{\hat{w}}, y_1, \ldots, y_{\hat{w}}, \nu], \end{aligned}$$

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an nth-root code, w and $\hat{w}$ be natural numbers such that $2 \leq w \leq N = |L|$, $1 \leq \hat{w} \leq N-1$. We denote by $J_w(C)$ and $\hat{J}_{\hat{w}}(C)$ the following two ideals:

$$\begin{array}{llll} J_w = & J_w(C) = & J_w(q, n, q^m, L, \mathcal{P}) \subset & \mathbb{F}_{q^m}[z_1, \ldots, z_w, y_1, \ldots, y_w], \\ \hat{J}_{\hat{w}} = & \hat{J}_{\hat{w}}(C) = & \hat{J}_{\hat{w}}(q, n, q^m, L, \mathcal{P}) \subset & \mathbb{F}_{q^m}[z_1, \ldots, z_{\hat{w}}, y_1, \ldots, y_{\hat{w}}, \nu], \end{array}$$

$$J_w = \Big\langle \quad \begin{array}{l} \{\sum_{h=1}^{w} y_h g_s(z_h)\}_{1\leq s\leq r}, \left\{y_j^{q-1} - 1\right\}_{1\leq j\leq w}, \\ \{p_{ij}(z_i, z_j)\}_{1\leq i<j\leq w}, \left\{\frac{z_j^n - 1}{\prod_{l\in\bar{L}}(z_j - l)}\right\}_{1\leq j\leq w} \end{array} \Big\rangle \tag{1}$$

$$\hat{J}_{\hat{w}} = \Big\langle \quad \begin{array}{l} \left\{\sum_{h=1}^{\hat{w}} y_h g_s(z_h) + \nu g_s(0)\right\}_{1\leq s\leq r}, \left\{y_j^{q-1} - 1\right\}_{1\leq j\leq \hat{w}} \\ \nu^{q-1} - 1, \{p_{ij}(z_i, z_j)\}_{1\leq i<j\leq \hat{w}}, \left\{\frac{z_j^n - 1}{\prod_{l\in\bar{L}}(z_j - l)}\right\}_{1\leq j\leq \hat{w}} \end{array} \Big\rangle \tag{2}$$

where $p_{ij} = \sum_{h=0}^{n-1} z_i^h z_j^{n-1-h} = \frac{z_i^n - z_j^n}{z_i - z_j}$ are in $\mathbb{F}_q[z_i, z_j]$.

We denote by $\eta(\mathbf{J_w})$ and $\hat{\eta}(\hat{\mathbf{J}}_{\hat{\mathbf{w}}})$ the integers $\eta(J_w) = |\mathcal{V}(J_w)|$, $\hat{\eta}(\hat{J}_{\hat{w}}) = |\mathcal{V}(\hat{J}_{\hat{w}})|$.

Remark

Ideals J_w and $\hat{J}_{\hat{w}}$ are **radical**, *since they contain polynomials $y_j^q - y_j$ and $z_j^{n+1} - z_j$.*

If we are in the **binary** case ($q = 2$), variables y_j, $j = 1, \ldots, w$, and ν are 1, and so we can omit them and the ideals become:

$$\begin{aligned} J_w = J_w(C) &= J_w(2, n, 2^m, L, \mathcal{P}) \subset \mathbb{F}_{2^m}[z_1, \ldots, z_w], \\ \hat{J}_{\hat{w}} = \hat{J}_{\hat{w}}(C) &= \hat{J}_{\hat{w}}(2, n, 2^m, L, \mathcal{P}) \subset \mathbb{F}_{2^m}[z_1, \ldots, z_{\hat{w}}], \end{aligned}$$

$$\begin{aligned} J_w &= \langle \left\{ \sum_{h=1}^{w} g_s(z_h) \right\}_{1 \le s \le r}, \{p_{ij}(z_i, z_j)\}_{1 \le i < j \le w} \left\{ \frac{z_j^n - 1}{\prod_{l \in \bar{L}}(z_j - l)} \right\}_{1 \le j \le w} \rangle; \\ \hat{J}_{\hat{w}} &= \langle \left\{ \sum_{h=1}^{\hat{w}} g_s(z_h) + g_s(0) \right\}_{1 \le s \le r}, \{p_{ij}(z_i, z_j)\}_{1 \le i < j \le \hat{w}}, \left\{ \frac{z_j^n - 1}{\prod_{l \in \bar{L}}(z_j - l)} \right\}_{1 \le j \le \hat{w}} \rangle \end{aligned} \tag{3}$$

Proposition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an nth-root code.

In the **zerofree case**, *there is at least one* **codeword of weight w** *in C if and only if there exists at least* **one solution of $\mathbf{J_w(C)}$**.

In the **non-zerofree case**, *there is at least one* **codeword of weight w** *in C if and only if there exists at least* **one solution of $\mathbf{J_w(C)}$ or of $\mathbf{\hat{J}_{w-1}(C)}$**.

Moreover the number of codewords of weight w is

$$A_w = \frac{\eta(J_w)}{w!} \quad \text{in the zerofree case and}$$

$$A_w = \frac{\eta(J_w)}{w!} + \frac{\hat{\eta}(\hat{J}_{w-1})}{(w-1)!} \quad \text{in the non-zerofree case}$$

Proposition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an nth-root code.
In the **zerofree case**, *there is at least one* **codeword of weight w** *in C if and only if there exists at least* **one solution of $\mathbf{J_w(C)}$**.
In the **non-zerofree case**, *there is at least one* **codeword of weight w** *in C if and only if there exists at least* **one solution of $\mathbf{J_w(C)}$ or of $\mathbf{\hat{J}_{w-1}(C)}$**.
Moreover the number of codewords of weight w is

$$A_w = \frac{\eta(J_w)}{w!} \quad \text{in the zerofree case and}$$

$$A_w = \frac{\eta(J_w)}{w!} + \frac{\hat{\eta}(\hat{J}_{w-1})}{(w-1)!} \quad \text{in the non-zerofree case}$$

Proposition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an nth-root code.
In the **zerofree case**, *there is at least one* **codeword of weight w** *in C if and only if there exists at least* **one solution of $\mathbf{J_w(C)}$**.
In the **non-zerofree case**, *there is at least one* **codeword of weight w** *in C if and only if there exists at least* **one solution of $\mathbf{J_w(C)}$ or of $\mathbf{\hat{J}_{w-1}(C)}$**.
Moreover the number of codewords of weight w is

$$\mathbf{A_w} = \frac{\eta(\mathbf{J_w})}{\mathbf{w}!} \qquad \textit{in the zerofree case and}$$

$$\mathbf{A_w} = \frac{\eta(\mathbf{J_w})}{\mathbf{w}!} + \frac{\hat{\eta}(\mathbf{\hat{J}_{w-1}})}{(\mathbf{w-1})!} \qquad \textit{in the non-zerofree case}$$

Proposition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an nth-root code.
In the **zerofree case**, *there is at least one* **codeword of weight w** *in C if and only if there exists at least* **one solution of $\mathbf{J_w(C)}$**.
In the **non-zerofree case**, *there is at least one* **codeword of weight w** *in C if and only if there exists at least* **one solution of $\mathbf{J_w(C)}$ or of $\mathbf{\hat{J}_{w-1}(C)}$**.
Moreover the number of codewords of weight w is

$$\mathbf{A_w} = \frac{\eta(\mathbf{J_w})}{\mathbf{w}!} \qquad \textit{in the zerofree case and}$$

$$\mathbf{A_w} = \frac{\eta(\mathbf{J_w})}{\mathbf{w}!} + \frac{\eta(\mathbf{\hat{J}_{w-1}})}{(\mathbf{w-1})!} \qquad \textit{in the non-zerofree case}$$

Proposition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ *be an nth-root code.*
In the **zerofree case**, *there is at least one* **codeword of weight w** *in* C *if and only if there exists at least* **one solution of** $\mathbf{J_w(C)}$.
In the **non-zerofree case**, *there is at least one* **codeword of weight w** *in* C *if and only if there exists at least* **one solution of** $\mathbf{J_w(C)}$ **or of** $\mathbf{\hat{J}_{w-1}(C)}$.
Moreover the number of codewords of weight w *is*

$$\mathbf{A_w} = \frac{\eta(\mathbf{J_w})}{\mathbf{w!}} \qquad \textit{in the zerofree case and}$$

$$\mathbf{A_w} = \frac{\eta(\mathbf{J_w})}{\mathbf{w!}} + \frac{\hat{\eta}(\mathbf{\hat{J}_{w-1}})}{(\mathbf{w-1})!} \qquad \textit{in the non-zerofree case}$$

Proposition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an nth-root code.
In the **zerofree case**, *there is at least one* **codeword of weight w** *in C if and only if there exists at least* **one solution of $\mathbf{J_w(C)}$**.
In the **non-zerofree case**, *there is at least one* **codeword of weight w** *in C if and only if there exists at least* **one solution of $\mathbf{J_w(C)}$ or of $\mathbf{\hat{J}_{w-1}(C)}$**.
Moreover the number of codewords of weight w is

$$\mathbf{A_w} = \frac{\eta(\mathbf{J_w})}{\mathbf{w}!} \qquad \textit{in the zerofree case and}$$
$$\mathbf{A_w} = \frac{\eta(\mathbf{J_w})}{\mathbf{w}!} + \frac{\hat{\eta}(\mathbf{\hat{J}_{w-1}})}{(\mathbf{w-1})!} \qquad \textit{in the non-zerofree case}$$

INPUT:	a **zerofree nth-root code** $\mathbf{C} = \Omega(\mathbf{q}, \mathbf{n}, \mathbf{q^m}, \mathbf{L}, \mathcal{P})$,
	an integer $2 \leq \mathbf{w} \leq \lvert L \rvert$
OUTPUT:	the element $\mathbf{A_w}$ of the weight distribution of C
STEP 1:	construct ideal $\mathbf{J_w} = \mathbf{J_w}(\mathbf{C})$
STEP 2:	compute a Gröbner basis $\mathcal{G}_\mathbf{w}$ of J_w
STEP 3:	use $\mathcal{G}_w$ to get the number $\eta(\mathbf{J_w})$ of points in $\mathcal{V}(J_w)$
STEP 4:	return $\frac{\eta(\mathbf{J_w})}{\mathbf{w}!}$

INPUT:	a **zerofree nth-root code** $\mathbf{C} = \Omega(\mathbf{q}, \mathbf{n}, \mathbf{q}^{\mathbf{m}}, \mathbf{L}, \mathcal{P})$, an integer $2 \leq \mathbf{w} \leq \lvert L \rvert$
OUTPUT:	the element $\mathbf{A_w}$ of the weight distribution of C
STEP 1:	construct ideal $\mathbf{J_w} = \mathbf{J_w}(\mathbf{C})$
STEP 2:	compute a Gröbner basis $\mathcal{G}_\mathbf{w}$ of J_w
STEP 3:	use $\mathcal{G}_w$ to get the number $\eta(\mathbf{J_w})$ of points in $\mathcal{V}(J_w)$
STEP 4:	return $\frac{\eta(\mathbf{J_w})}{\mathbf{w}!}$

INPUT:	a **zerofree nth-root code** $\mathbf{C} = \mathbf{\Omega}(\mathbf{q}, \mathbf{n}, \mathbf{q}^{\mathbf{m}}, \mathbf{L}, \mathcal{P})$, an integer $2 \leq \mathbf{w} \leq \lvert L \rvert$
OUTPUT:	the element $\mathbf{A}_{\mathbf{w}}$ of the weight distribution of C
STEP 1:	construct ideal $\mathbf{J}_{\mathbf{w}} = \mathbf{J}_{\mathbf{w}}(\mathbf{C})$
STEP 2:	compute a Gröbner basis $\mathcal{G}_{\mathbf{w}}$ of J_w
STEP 3:	use $\mathcal{G}_w$ to get the number $\eta(\mathbf{J}_{\mathbf{w}})$ of points in $\mathcal{V}(J_w)$
STEP 4:	return $\frac{\eta(\mathbf{J}_{\mathbf{w}})}{\mathbf{w}!}$

INPUT:	a **zerofree nth-root code** $\mathbf{C} = \Omega(\mathbf{q}, \mathbf{n}, \mathbf{q}^{\mathbf{m}}, \mathbf{L}, \mathcal{P})$, an integer $2 \leq \mathbf{w} \leq \lvert L \rvert$
OUTPUT:	the element $\mathbf{A_w}$ of the weight distribution of C
STEP 1:	construct ideal $\mathbf{J_w} = \mathbf{J_w}(\mathbf{C})$
STEP 2:	compute a Gröbner basis $\mathcal{G}_{\mathbf{w}}$ of J_w
STEP 3:	use $\mathcal{G}_w$ to get the number $\eta(\mathbf{J_w})$ of points in $\mathcal{V}(J_w)$
STEP 4:	return $\frac{\eta(\mathbf{J_w})}{\mathbf{w}!}$

INPUT:	a **zerofree nth-root code** $\mathbf{C} = \mathbf{\Omega(q, n, q^m, L, \mathcal{P})}$, an integer $2 \leq \mathbf{w} \leq \lvert L \rvert$
OUTPUT:	the element $\mathbf{A_w}$ of the weight distribution of C
STEP 1:	construct ideal $\mathbf{J_w} = \mathbf{J_w(C)}$
STEP 2:	compute a Gröbner basis $\mathcal{G}_\mathbf{w}$ of J_w
STEP 3:	use $\mathcal{G}_w$ to get the number $\eta(\mathbf{J_w})$ of points in $\mathcal{V}(J_w)$
STEP 4:	return $\frac{\eta(\mathbf{J_w})}{\mathbf{w}!}$

INPUT:	a **zerofree nth-root code** $\mathbf{C} = \mathbf{\Omega}(\mathbf{q}, \mathbf{n}, \mathbf{q^m}, \mathbf{L}, \mathcal{P})$, an integer $2 \leq \mathbf{w} \leq \lvert L \rvert$
OUTPUT:	the element $\mathbf{A_w}$ of the weight distribution of C
STEP 1:	construct ideal $\mathbf{J_w} = \mathbf{J_w}(\mathbf{C})$
STEP 2:	compute a Gröbner basis $\mathcal{G}_\mathbf{w}$ of J_w
STEP 3:	use $\mathcal{G}_w$ to get the number $\eta(\mathbf{J_w})$ of points in $\mathcal{V}(J_w)$
STEP 4:	return $\frac{\eta(\mathbf{J_w})}{\mathbf{w}!}$

INPUT:	a **zerofree nth-root code** $\mathbf{C} = \mathbf{\Omega}(\mathbf{q}, \mathbf{n}, \mathbf{q}^{\mathbf{m}}, \mathbf{L}, \mathcal{P})$,
	an integer $2 \leq \mathbf{w} \leq \|L\|$
OUTPUT:	the element $\mathbf{A}_{\mathbf{w}}$ of the weight distribution of C
STEP 1:	construct ideal $\mathbf{J}_{\mathbf{w}} = \mathbf{J}_{\mathbf{w}}(\mathbf{C})$
STEP 2:	compute a Gröbner basis $\mathcal{G}_{\mathbf{w}}$ of J_w
STEP 3:	use $\mathcal{G}_w$ to get the number $\eta(\mathbf{J}_{\mathbf{w}})$ of points in $\mathcal{V}(J_w)$
STEP 4:	return $\frac{\eta(\mathbf{J}_{\mathbf{w}})}{\mathbf{w}!}$

INPUT:	a **non-zerofree nth-root code** $C = \Omega(q, n, q^m, L, \mathcal{P})$, an integer $2 \leq w \leq \lvert L \rvert$
OUTPUT:	the element A_w of the weight distribution of C
STEP 1:	construct ideals $J_w = J_w(C)$ and $\hat{J}_{w-1} = \hat{J}_{w-1}(C)$
STEP 2:	compute a Gröbner basis $\mathcal{G}_w$ of J_w and compute aGröbner basis $\hat{G}_{w-1}$ of $\hat{J}_{w-1}$
STEP 3:	use $\mathcal{G}_w$ to get the number $\eta(J_w)$ of points in $\mathcal{V}(J_w)$ and use $\hat{G}_{w-1}$ to get the number $\hat{\eta}(\hat{J}_{w-1})$ of points in $\mathcal{V}(\hat{J}_{w-1})$
STEP 4:	return $\frac{\eta(J_w)}{w!} + \frac{\hat{\eta}(\hat{J}_{w-1})}{(w-1)!}$

Let C as in the first Example:

$$C = \Omega(2, 7, 8, \mathbb{F}_8, \{g_1, g_2\}), g_1(x) = \frac{1}{x^2 + x + 1}, g_2(x) = \frac{x}{x^2 + x + 1}.$$

- $w = 2$, $J_2(C) \subseteq \mathbb{F}_2[z_1, z_2]$ and $\hat{J}_1(C) \subseteq \mathbb{F}_2[z_1]$:

$$J_2(C) = \langle g_1(z_1) + g_1(z_2), g_2(z_1) + g_2(z_2), z_1^7 - 1, z_2^7 - 1, p_{1,2}(z_1, z_2) \rangle$$

$$\hat{J}_1(C) = \langle g_1(z_1) + g_1(0), g_2(z_1) + g_2(0), z_1^7 - 1 \rangle$$

$\mathcal{G}_2$ and $\hat{\mathcal{G}}_1$ are trivial and hence there are no words of weight 2. The same for $w = 3, 4$.

Let C as in the first Example:

$$C = \Omega(2,7,8,\mathbb{F}_8,\{g_1,g_2\}), g_1(x) = \frac{1}{x^2+x+1}, g_2(x) = \frac{x}{x^2+x+1}.$$

- $w = 2$, $J_2(C) \subseteq \mathbb{F}_2[z_1,z_2]$ and $\hat{J}_1(C) \subseteq \mathbb{F}_2[z_1]$:

  $$J_2(C) = \langle g_1(z_1)+g_1(z_2), g_2(z_1)+g_2(z_2), z_1^7-1, z_2^7-1, p_{1,2}(z_1,z_2)\rangle$$

  $$\hat{J}_1(C) = \langle g_1(z_1)+g_1(0), g_2(z_1)+g_2(0), z_1^7-1\rangle$$

  $\mathcal{G}_2$ and $\hat{\mathcal{G}}_1$ are trivial and hence there are no words of weight 2. The same for $w = 3,4$.

- $w = 5$, construct J_5 and $\hat{J}_4$: $\mathcal{G}_5$ is trivial, but basis $\hat{\mathcal{G}}_4$ has the following leading terms

$$\left\{z_1 z_2,\ z_1^2,\ z_1 z_3^2,\ z_2^3,\ z_1 z_4^3,\ z_3^4,\ z_2^2 z_3^2,\ z_4^5,\ z_2^2 z_4^3,\ z_3^3 z_4^3\right\}.$$

  These monomials permit us to compute the number $\hat{\eta}(\hat{J}_4) = 48$. So that $A_5 = \frac{\eta(J_5)}{5!} + \frac{\hat{\eta}(\hat{J}_4)}{4!} = \frac{48}{4!} = 2$. Note that the 2 words of weight 5 in C have the last component non zero.

- Computing $\mathcal{G}_6$ we have a non trivial result, $\eta(J_6) = 720$, and for $\hat{J}_5$ we get an empty variety. The words of weight 6 are then $A_6 = \frac{\eta(J_6)}{6!} + \frac{\hat{\eta}(\hat{J}_5)}{5!} = \frac{720}{6!} = 1$.

- $w = 5$, construct J_5 and $\hat{J}_4$: $\mathcal{G}_5$ is trivial, but basis $\hat{\mathcal{G}}_4$ has the following leading terms

$$\left\{z_1 z_2,\ z_1^2,\ z_1 z_3^2,\ z_2^3,\ z_1 z_4^3,\ z_3^4,\ z_2^2 z_3^2,\ z_4^5,\ z_2^2 z_4^3,\ z_3^3 z_4^3\right\}.$$

  These monomials permit us to compute the number $\hat{\eta}(\hat{J}_4) = 48$. So that $A_5 = \frac{\eta(J_5)}{5!} + \frac{\hat{\eta}(\hat{J}_4)}{4!} = \frac{48}{4!} = 2$. Note that the 2 words of weight 5 in C have the last component non zero.
- Computing $\mathcal{G}_6$ we have a non trivial result, $\eta(J_6) = 720$, and for $\hat{J}_5$ we get an empty variety. The words of weight 6 are then $A_6 = \frac{\eta(J_6)}{6!} + \frac{\hat{\eta}(\hat{J}_5)}{5!} = \frac{720}{6!} = 1$.

w	$\mathcal{G}(J_w)$	$\hat{\mathcal{G}}(\hat{J}_{w-1})$	$\eta(J_w)$	$\hat{\eta}(\hat{J}_{w-1})$	A_w
2,3,4,7	$\{1\}$	$\{1\}$	0	0	0
5	$\{1\}$	not trivial	0	48	2
6	not trivial	$\{1\}$	720	0	1
8	–	$\{1\}$	–	0	0

Definition

The elements in $(\mathbb{F}_q^m)^{n-k}$, $\sigma = \mathbf{Hx}$ are called **syndromes**. We say that σ is the syndrome corresponding to x.

Definition

Let $C \subseteq (\mathbb{F}_q)^N$ be an (N, k) code. For any vector $a \in (\mathbb{F}_q)^n$ the set

$$a + C = \{a + x : x \in C\}$$

in called a **coset** (or translate) of C.

Definition

The elements in $(\mathbb{F}_q^m)^{n-k}$, $\sigma = \mathbf{H}\mathbf{x}$ are called **syndromes**. We say that σ is the syndrome corresponding to x.

Definition

Let $C \subseteq (\mathbb{F}_q)^N$ be an (N, k) code. For any vector $a \in (\mathbb{F}_q)^n$ the set

$$a + C = \{a + x : x \in C\}$$

in called a **coset** (or translate) of C.

We give as in the code case

- **ideals** for the zerofree case and in the non-zerofree case;
- **proposition** for A_w in the the zerofree case and in the non-zerofree case;
- **algorithms** the zerofree case and in the non-zerofree case.

Skip coset

We give as in the code case

- **ideals** for the zerofree case and in the non-zerofree case;
- **proposition** for A_w in the the zerofree case and in the non-zerofree case;
- **algorithms** the zerofree case and in the non-zerofree case.

Skip coset

We give as in the code case

- **ideals** for the zerofree case and in the non-zerofree case;
- **proposition** for A_w in the the zerofree case and in the non-zerofree case;
- **algorithms** the zerofree case and in the non-zerofree case.

Skip coset

$$J_w(a+C) \subset \mathbb{F}_{q^m}[z_1,\dots,z_w,y_1,\dots,y_w],$$
$$\hat{J}_{\hat{w}}(a+C) \subset \mathbb{F}_{q^m}[z_1,\dots,z_{\hat{w}},y_1,\dots,y_{\hat{w}},\nu],$$

$$J_w(a+C) = \langle \quad \left\{\sum_{h=1}^{w} y_h g_s(z_h) - \sigma(\mathbf{a})_s\right\}_{1\le s\le r}, \left\{y_j^{q-1}-1\right\}_{1\le j\le w}, \left\{p_{ij}(z_i,z_j)\right\}_{1\le i<j\le w}, \left\{\frac{z_j^n-1}{\prod_{l\in\bar{L}}(z_j-l)}\right\}_{1\le j\le w} \rangle; \tag{4}$$

$$\hat{J}_{\hat{w}}(a+C) = \langle \quad \left\{\sum_{h=1}^{\hat{w}} y_h g_s(z_h) + \nu g_s(0) - \sigma(a)_s\right\}_{1\le s\le r}, \left\{y_j^{q-1}-1\right\}_{1\le j\le \hat{w}} \nu^{q-1}-1, \left\{p_{ij}(z_i,z_j)\right\}_{1\le i<j\le \hat{w}}, \left\{\frac{z_j^n-1}{\prod_{l\in\bar{L}}(z_j-l)}\right\}_{1\le j\le \hat{w}} \rangle. \tag{5}$$

$$\eta(J_w(a+C)) = |\mathcal{V}(J_w(a+C))|, \quad \hat{\eta}(\hat{J}_{\hat{w}}(a+C)) = |\mathcal{V}(\hat{J}_{\hat{w}}(a+C))|.$$

$$J_w(a+C) \subset \mathbb{F}_{q^m}[z_1,\dots,z_w,y_1,\dots,y_w],$$
$$\hat{J}_{\hat{w}}(a+C) \subset \mathbb{F}_{q^m}[z_1,\dots,z_{\hat{w}},y_1,\dots,y_{\hat{w}},\nu],$$

$$J_w(a+C) = \langle \quad \left\{\sum_{h=1}^{w} y_h g_s(z_h) - \sigma(\mathbf{a})_s\right\}_{1\le s\le r}, \left\{y_j^{q-1}-1\right\}_{1\le j\le w}, \left\{p_{ij}(z_i,z_j)\right\}_{1\le i<j\le w}, \left\{\frac{z_j^n-1}{\prod_{l\in\bar{L}}(z_j-l)}\right\}_{1\le j\le w} \quad \rangle; \tag{4}$$

$$\hat{J}_{\hat{w}}(a+C) = \langle \quad \left\{\sum_{h=1}^{\hat{w}} y_h g_s(z_h) + \nu g_s(0) - \sigma(a)_s\right\}_{1\le s\le r}, \left\{y_j^{q-1}-1\right\}_{1\le j\le \hat{w}}, \nu^{q-1}-1, \left\{p_{ij}(z_i,z_j)\right\}_{1\le i<j\le \hat{w}}, \left\{\frac{z_j^n-1}{\prod_{l\in\bar{L}}(z_j-l)}\right\}_{1\le j\le \hat{w}} \rangle. \tag{5}$$

$$\eta(J_w(a+C)) = |\mathcal{V}(J_w(a+C))|, \quad \hat{\eta}(\hat{J}_{\hat{w}}(a+C)) = |\mathcal{V}(\hat{J}_{\hat{w}}(a+C))|.$$

Proposition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$, $a \in (\mathbb{F}_q)^N \setminus C$, and $a + C$ a coset of code C. In the zerofree case, there is at least one vector of weight w in coset $a + C$ if and only if there is at least one solution of $J_w(a + C)$. In the non-zerofree case, there is at least one vector of weight w in $a + C$ if and only if there is at least one solution of $J_w(a + C)$ or of $\hat{J}_{w-1}(a + C)$. Furthermore, the number of vectors of weight w in $a + C$ is

$$A_w(a) = \frac{\eta(J_w(a+C))}{w!} \quad \text{in the zerofree case and}$$

$$A_w(a) = \frac{\eta(J_w(a+C))}{w!} + \frac{\hat{\eta}(\hat{J}_{w-1}(a+C))}{(w-1)!} \quad \text{in the non-zerofree case}$$

Definition

$\diamondsuit$ Let $\mathcal{L}_C$ be a polynomial in $\mathbb{F}_q[X, z]$, where $X = (x_1, \ldots, x_r)$. Then $\mathcal{L}_C$ is a **general error locator polynomial** of C if

1. $\mathcal{L}_C(X, z) = z^t + a_{t-1}z^{t-1} + \cdots + a_0$, with $a_j \in \mathbb{F}_q[X]$, $0 \leq j \leq t-1$, that is, $\mathcal{L}_C$ is a monic polynomial with degree t with respect to the variable z and its coefficients are in $\mathbb{F}_q[X]$;

2. given a syndrome $\mathbf{s} = (\bar{s}_1, \ldots \bar{s}_r) \in (\mathbb{F}_{q^m})^{N-k}$, corresponding to a vector error of weight $\mu \leq t$ and error locations $\{k_1, \ldots, k_\mu\}$, if we evaluate the X variables in $\mathbf{s}$, then the roots of $\mathcal{L}_C(\mathbf{s}, z)$ are $\{\alpha^{k_1}, \ldots, \alpha^{k_\mu}, \underbrace{0, \ldots, 0}_{t-\mu}\}$.

Definition

Let $\mathcal{L}$ be a polynomial in $\mathbb{F}_q[X, W, z]$, $X = (x_1, \ldots, x_r)$ and $W = (w_\nu, \ldots, w_1)$, where $\nu \geq 1$ is the number of erasures that occurred. Then $\mathcal{L}$ is a **general error locator polynomial of type** ν of C if

1. $\mathcal{L}(X, W, z) = z^\tau + a_{\tau-1} z^{\tau-1} + \cdots + a_0$, with $a_j \in \mathbb{F}_q[X, W]$, for any $0 \leq j \leq \tau - 1$, that is, $\mathcal{L}$ is a monic polynomial with degree τ in the variable z and coefficients in $\mathbb{F}_q[X, W]$;
2. for any syndrome $\mathbf{s} = (\bar{s}_1, \ldots, \bar{s}_r)$ and any erasure location vector $\mathbf{w} = (\overline{w}_1, \ldots, \overline{w}_\nu)$, corresponding to an error of weight $\mu \leq \tau$ and error locations $\{k_1, \ldots, k_\mu\}$, if we evaluate the X variables in $\mathbf{s}$ and the W variables in $\mathbf{w}$, then the roots of $\mathcal{L}(\mathbf{s}, \mathbf{w}, z)$ are $\{\alpha^{k_1}, \ldots, \alpha^{k_\mu}, \underbrace{0, \ldots, 0}_{\tau-\mu}\}$.

Definition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be a zerofree maximal nth-root code, with correction capability t. We denote by $\mathbf{J^{C,t}}$ the ideal $J^{C,t} \subset \mathbb{F}_{q^m}[x_1, \ldots, x_r, z_t, \ldots, z_1, y_1, \ldots, y_t]$,

$$J^{C,t} = \langle \quad \left\{\sum_{h=1}^{t} y_h g_s(z_h) - x_s\right\}_{1\le s\le r}, \left\{y_j^{q-1} - 1\right\}_{1\le j\le t}, \\ \left\{z_i z_j p(z_i, z_j)\right\}_{i\neq j, 1\le i,j\le t}, \left\{z_j^{n+1} - z_j\right\}_{1\le j\le t} \quad \rangle \tag{6}$$

where $p(x, y) = \sum_{h=0}^{n-1} x^h y^{n-1-h}$. We denote by $\mathcal{G}^{C,t}$ the totaly reduced Gröbner basis of $J^{C,t}$ w.r.t. $>$.

- $x_1, \ldots, x_r$ represent correctable syndromes,
- $z_1, \ldots, z_t$ error locations and
- $y_1, \ldots, y_t$ error values.

Definition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be a zerofree maximal nth-root code, with correction capability t. We denote by $\mathbf{J^{C,t}}$ the ideal $J^{C,t} \subset \mathbb{F}_{q^m}[x_1, \ldots, x_r, z_t, \ldots, z_1, y_1, \ldots, y_t]$,

$$J^{C,t} = \langle \quad \left\{\sum_{h=1}^{t} y_h g_s(z_h) - x_s\right\}_{1 \le s \le r}, \left\{y_j^{q-1} - 1\right\}_{1 \le j \le t}, \left\{z_i z_j p(z_i, z_j)\right\}_{i \ne j, 1 \le i,j \le t}, \left\{z_j^{n+1} - z_j\right\}_{1 \le j \le t} \quad \rangle \tag{6}$$

where $p(x, y) = \sum_{h=0}^{n-1} x^h y^{n-1-h}$. We denote by $\mathcal{G}^{C,t}$ the totaly reduced Gröbner basis of $J^{C,t}$ w.r.t. $>$.

- $x_1, \ldots, x_r$ represent correctable syndromes,
- $z_1, \ldots, z_t$ error locations and
- $y_1, \ldots, y_t$ error values.

Definition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be a zerofree maximal nth-root code, with correction capability t. We denote by $\mathbf{J^{C,t}}$ the ideal $J^{C,t} \subset \mathbb{F}_{q^m}[x_1, \ldots, x_r, z_t, \ldots, z_1, y_1, \ldots, y_t]$,

$$J^{C,t} = \langle \quad \left\{\sum_{h=1}^{t} y_h g_s(z_h) - x_s\right\}_{1\le s\le r}, \left\{y_j^{q-1} - 1\right\}_{1\le j\le t}, \left\{z_i z_j p(z_i, z_j)\right\}_{i\ne j,\, 1\le i,j\le t}, \left\{z_j^{n+1} - z_j\right\}_{1\le j\le t} \quad \rangle \tag{6}$$

where $p(x, y) = \sum_{h=0}^{n-1} x^h y^{n-1-h}$. We denote by $\mathcal{G}^{C,t}$ the totaly reduced Gröbner basis of $J^{C,t}$ w.r.t. $>$.

- $x_1, \ldots, x_r$ represent correctable syndromes,
- $z_1, \ldots, z_t$ error locations and
- $y_1, \ldots, y_t$ error values.

Definition

Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be a zerofree maximal nth-root code, with correction capability t. We denote by $\mathbf{J^{C,t}}$ the ideal $J^{C,t} \subset \mathbb{F}_{q^m}[x_1, \ldots, x_r, z_t, \ldots, z_1, y_1, \ldots, y_t]$,

$$J^{C,t} = \langle \quad \left\{\sum_{h=1}^{t} y_h g_s(z_h) - x_s\right\}_{1\leq s\leq r}, \left\{y_j^{q-1} - 1\right\}_{1\leq j\leq t}, \left\{z_i z_j p(z_i, z_j)\right\}_{i\neq j,\, 1\leq i,j\leq t}, \left\{z_j^{n+1} - z_j\right\}_{1\leq j\leq t} \quad \rangle \tag{6}$$

where $p(x, y) = \sum_{h=0}^{n-1} x^h y^{n-1-h}$. We denote by $\mathcal{G}^{C,t}$ the totaly reduced Gröbner basis of $J^{C,t}$ w.r.t. $>$.

- $x_1, \ldots, x_r$ represent correctable syndromes,
- $z_1, \ldots, z_t$ error locations and
- $y_1, \ldots, y_t$ error values.

Lemma

Ideal $J^{C,t}$ is radical and stratified.

Proposition (♣)

In Gröbner basis $\mathcal{G}^{C,t}$ there exists a unique polynomial of type

$$g = z_t^t + a_{t-1} z_t^{t-1} + \ldots + a_0, a_i \in \mathbb{F}_q[X].$$

Lemma

Ideal $J^{C,t}$ is radical and stratified.

Proposition (♣)

In Gröbner basis $\mathcal{G}^{C,t}$ there exists a unique polynomial of type

$$g = z_t^t + a_{t-1} z_t^{t-1} + \ldots + a_0, a_i \in \mathbb{F}_q[X].$$

Theorem

If code C is a proper maximal zerofree nth-root code with correction capability t, then C possesses a general error locator polynomial.

Theorem

If code C is a proper maximal zerofree nth-root code with correction capability t, then C possesses a general error locator polynomial. Skip proof

Proof.

- A polynomial of type $g = z_t^t + a_{t-1} z_t^{t-1} + \ldots + a_0$, with $a_i \in \mathbb{F}_{q^m}[X]$, exists in $J^{C,t}$ (Proposition ♣).
- Since C is proper, all polynomials in ideal $J^{C,t}$ have coefficients in $\mathbb{F}_q$ and so g must be in $\mathbb{F}_q[X, z_t]$. Polynomial $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ satisfies:
  - condition (1) in Definition (♢);
  - condition (2) in Definition (♢), because correctable syndromes are in $\mathcal{V}(J^{C,t} \cap \mathbb{F}_q[X])$ and
  - g is in $J^{C,t}$.
- So $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ is a general error locator polynomial for C.

□

Proof.

- A polynomial of type $g = z_t^t + \mathrm{a}_{t-1} z_t^{t-1} + \ldots + \mathrm{a}_0$, with $\mathrm{a}_i \in \mathbb{F}_{q^m}[X]$, exists in $J^{C,t}$ (Proposition ♣).
- Since C is proper, all polynomials in ideal $J^{C,t}$ have coefficients in $\mathbb{F}_q$ and so g must be in $\mathbb{F}_q[X, z_t]$. Polynomial $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ satisfies:
  - condition (1) in Definition (♢);
  - condition (2) in Definition (♢), because correctable syndromes are in $\mathcal{V}(J^{C,t} \cap \mathbb{F}_q[X])$ and
  - g is in $J^{C,t}$.
- So $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ is a general error locator polynomial for C.

□

Proof.

- A polynomial of type $g = z_t^t + \mathrm{a}_{t-1} z_t^{t-1} + \ldots + \mathrm{a}_0$, with $\mathrm{a}_i \in \mathbb{F}_{q^m}[X]$, exists in $J^{C,t}$ (Proposition ♣).
- Since C is proper, all polynomials in ideal $J^{C,t}$ have coefficients in $\mathbb{F}_q$ and so g must be in $\mathbb{F}_q[X, z_t]$. Polynomial $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ satisfies:
  - condition (1) in Definition (♢);
  - condition (2) in Definition (♢), because correctable syndromes are in $\mathcal{V}(J^{C,t} \cap \mathbb{F}_q[X])$ and
  - g is in $J^{C,t}$.
- So $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ is a general error locator polynomial for C.

□

Proof.

- A polynomial of type $g = z_t^t + \mathrm{a}_{t-1} z_t^{t-1} + \ldots + \mathrm{a}_0$, with $\mathrm{a}_i \in \mathbb{F}_{q^m}[X]$, exists in $J^{C,t}$ (Proposition ♣).
- Since C is proper, all polynomials in ideal $J^{C,t}$ have coefficients in $\mathbb{F}_q$ and so g must be in $\mathbb{F}_q[X, z_t]$. Polynomial $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ satisfies:
  - condition (1) in Definition (♢);
  - condition (2) in Definition (♢), because correctable syndromes are in $\mathcal{V}(J^{C,t} \cap \mathbb{F}_q[X])$ and
  - g is in $J^{C,t}$.
- So $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ is a general error locator polynomial for C.

□

Proof.

- A polynomial of type $g = z_t^t + a_{t-1}z_t^{t-1} + \ldots + a_0$, with $a_i \in \mathbb{F}_{q^m}[X]$, exists in $J^{C,t}$ (Proposition ♣).
- Since C is proper, all polynomials in ideal $J^{C,t}$ have coefficients in $\mathbb{F}_q$ and so g must be in $\mathbb{F}_q[X, z_t]$. Polynomial $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ satisfies:
  - condition (1) in Definition (♢);
  - condition (2) in Definition (♢), because correctable syndromes are in $\mathcal{V}(J^{C,t} \cap \mathbb{F}_q[X])$ and
  - g is in $J^{C,t}$.
- So $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ is a general error locator polynomial for C.

□

Proof.

- A polynomial of type $g = z_t^t + \mathrm{a}_{t-1} z_t^{t-1} + \ldots + \mathrm{a}_0$, with $\mathrm{a}_i \in \mathbb{F}_{q^m}[X]$, exists in $J^{C,t}$ (Proposition ♣).
- Since C is proper, all polynomials in ideal $J^{C,t}$ have coefficients in $\mathbb{F}_q$ and so g must be in $\mathbb{F}_q[X, z_t]$. Polynomial $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ satisfies:
  - condition (1) in Definition (♢);
  - condition (2) in Definition (♢), because correctable syndromes are in $\mathcal{V}(J^{C,t} \cap \mathbb{F}_q[X])$ and
  - g is in $J^{C,t}$.
- So $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ is a general error locator polynomial for C.

$\square$

Proof.

- A polynomial of type $g = z_t^t + \mathrm{a}_{t-1} z_t^{t-1} + \ldots + \mathrm{a}_0$, with $\mathrm{a}_i \in \mathbb{F}_{q^m}[X]$, exists in $J^{C,t}$ (Proposition ♣).
- Since C is proper, all polynomials in ideal $J^{C,t}$ have coefficients in $\mathbb{F}_q$ and so g must be in $\mathbb{F}_q[X, z_t]$. Polynomial $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ satisfies:
  - condition (1) in Definition ($\diamondsuit$);
  - condition (2) in Definition ($\diamondsuit$), because correctable syndromes are in $\mathcal{V}(J^{C,t} \cap \mathbb{F}_q[X])$ and
  - g is in $J^{C,t}$.
- So $\mathcal{L} = g(X, z_t) \in \mathbb{F}_q[X, z_t]$ is a general error locator polynomial for C.

$\square$

Cyclic codes are proper maximal zerofree nth-root codes $\Longrightarrow$ cyclic codes have general error locator polynomials.

Example: first method

Let

- C be the $[5, 2, 3]$ linear code over $\mathbb{F}_2$;
- generator matrix $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$;
- $t = 1$;
- γ be a primitive element of $\mathbb{F}_{16}$ (minimal polynomial $z^4 + z + 1$);

Example: first method

Let

- C be the $[5, 2, 3]$ linear code over $\mathbb{F}_2$;
- generator matrix $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$;
- $t = 1$;
- γ be a primitive element of $\mathbb{F}_{16}$ (minimal polynomial $z^4 + z + 1$);

Example: first method

Let

- C be the $[5,2,3]$ linear code over $\mathbb{F}_2$;
- generator matrix $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$;
- $t = 1$;
- γ be a primitive element of $\mathbb{F}_{16}$ (minimal polynomial $z^4 + z + 1$);

Example: first method

Let

- C be the $[5, 2, 3]$ linear code over $\mathbb{F}_2$;
- generator matrix $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$;
- $t = 1$;
- γ be a primitive element of $\mathbb{F}_{16}$ (minimal polynomial $z^4 + z + 1$);

Example: first method

Let

- C be the $[5, 2, 3]$ linear code over $\mathbb{F}_2$;
- generator matrix $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$;
- $t = 1$;
- γ be a primitive element of $\mathbb{F}_{16}$ (minimal polynomial $z^4 + z + 1$);

Example: first method

- parity-check matrix $H = (\gamma^6, \gamma^2, \gamma^3, \gamma^{14}, 1)$
- $\mathbf{C} = \mathbf{\Omega}(\mathbf{2}, \mathbf{5}, \mathbf{2^4}, \mathbf{R_5}, \mathcal{P}')$, where
$$\mathcal{P}' = \{\gamma^{12}x^4 + \gamma^{11}x^3 + x^2 + \gamma^{14}x + \gamma^3\}.$$
- the Gröbner basis $\mathcal{G}'$ w.r.t. the lexicographical order induced by $x_1 < z_1$, its elements are:
$$\mathcal{G}'_{x_1} = x_1^5 + (\gamma^3)x_1^4 + (\gamma^3 + \gamma)x_1^2 + \gamma^2 x_1 + (\gamma^2 + \gamma + 1)$$
$$\mathcal{G}'_{x_1,z_1} = \mathbf{z_1} + x_1^3.$$

There is only one polynomial in z_1 of degree 1, as we expected, and it is another general error locator polynomial for C.

Example: first method

- parity-check matrix $H = (\gamma^6, \gamma^2, \gamma^3, \gamma^{14}, 1)$
- $\mathbf{C} = \mathbf{\Omega}(\mathbf{2}, \mathbf{5}, \mathbf{2^4}, \mathbf{R_5}, \mathcal{P}')$, where
$$\mathcal{P}' = \{\gamma^{12}x^4 + \gamma^{11}x^3 + x^2 + \gamma^{14}x + \gamma^3\}.$$
- the Gröbner basis $\mathcal{G}'$ w.r.t. the lexicographical order induced by $x_1 < z_1$, its elements are:
$$\mathcal{G}'_{x_1} = x_1^5 + (\gamma^3)x_1^4 + (\gamma^3 + \gamma)x_1^2 + \gamma^2 x_1 + (\gamma^2 + \gamma + 1)$$
$$\mathcal{G}'_{x_1,z_1} = \mathbf{z_1} + x_1^3.$$

There is only one polynomial in z_1 of degree 1, as we expected, and it is another general error locator polynomial for C.

Example: first method

- parity-check matrix $H = (\gamma^6, \gamma^2, \gamma^3, \gamma^{14}, 1)$
- $\mathbf{C} = \boldsymbol{\Omega}(\mathbf{2}, \mathbf{5}, \mathbf{2^4}, \mathbf{R_5}, \mathcal{P}')$, where
$$\mathcal{P}' = \{\gamma^{12}x^4 + \gamma^{11}x^3 + x^2 + \gamma^{14}x + \gamma^3\}\,.$$
- the Gröbner basis $\mathcal{G}'$ w.r.t. the lexicographical order induced by $x_1 < z_1$, its elements are:

$$\mathcal{G}'_{x_1} = x_1^5 + (\gamma^3)x_1^4 + (\gamma^3 + \gamma)x_1^2 + \gamma^2 x_1 + (\gamma^2 + \gamma + 1)$$

$$\mathcal{G}'_{x_1,z_1} = \mathbf{z_1} + x_1^3.$$

There is only one polynomial in z_1 of degree 1, as we expected, and it is another general error locator polynomial for C.

Example: first method

- parity-check matrix $H = (\gamma^6, \gamma^2, \gamma^3, \gamma^{14}, 1)$
- $\mathbf{C} = \mathbf{\Omega}(\mathbf{2}, \mathbf{5}, \mathbf{2^4}, \mathbf{R_5}, \mathcal{P}')$, where
  $$\mathcal{P}' = \{\gamma^{12}x^4 + \gamma^{11}x^3 + x^2 + \gamma^{14}x + \gamma^3\}\,.$$
- the Gröbner basis $\mathcal{G}'$ w.r.t. the lexicographical order induced by $x_1 < z_1$, its elements are:

$$\mathcal{G}'_{x_1} = x_1^5 + (\gamma^3)x_1^4 + (\gamma^3 + \gamma)x_1^2 + \gamma^2 x_1 + (\gamma^2 + \gamma + 1)$$

$$\mathcal{G}'_{x_1,z_1} = \mathbf{z_1} + x_1^3.$$

There is only one polynomial in z_1 of degree 1, as we expected, and it is another general error locator polynomial for C.

Example: first method

- parity-check matrix $H = (\gamma^6, \gamma^2, \gamma^3, \gamma^{14}, 1)$
- $\mathbf{C} = \mathbf{\Omega}(\mathbf{2}, \mathbf{5}, \mathbf{2^4}, \mathbf{R_5}, \mathcal{P}')$, where
$$\mathcal{P}' = \{\gamma^{12}x^4 + \gamma^{11}x^3 + x^2 + \gamma^{14}x + \gamma^3\}\,.$$
- the Gröbner basis $\mathcal{G}'$ w.r.t. the lexicographical order induced by $x_1 < z_1$, its elements are:

$$\mathcal{G}'_{x_1} = x_1^5 + (\gamma^3)x_1^4 + (\gamma^3 + \gamma)x_1^2 + \gamma^2 x_1 + (\gamma^2 + \gamma + 1)$$

$$\mathcal{G}'_{x_1,z_1} = \mathbf{z_1} + x_1^3.$$

There is only one polynomial in z_1 of degree 1, as we expected, and it is another general error locator polynomial for C.

Example: second method

We suppose that error general locator polynomial exist. Let

- C be the code studied in the previous examples;
- parity-check matrix is a row, $H = (e_1, e_2, e_3, e_4, e_5)$;
- an general error locator polynomial $z + f(x)$ (the degree t of z is 1) must satisfy the following conditions:
  - $f(e_i) = \alpha^i\,, \quad \forall 1 \leq i \leq 5, \qquad \text{and } f(0) = 0\,.$
  - $f(x)$ has degree at most 5
  - coefficients $b_i \in \mathbb{F}_2$,

$$\Downarrow$$

$$f(x) = b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x \; (f(0) = 0 \Rightarrow b_0 = 0).$$

Example: second method

We suppose that error general locator polynomial exist. Let

- C be the code studied in the previous examples;
- parity-check matrix is a row, $H = (e_1, e_2, e_3, e_4, e_5)$;
- an general error locator polynomial $z + f(x)$ (the degree t of z is 1) must satisfy the following conditions:
  - $f(e_i) = \alpha^i, \quad \forall 1 \le i \le 5, \qquad \text{and } f(0) = 0$.
  - $f(x)$ has degree at most 5
  - coefficients $b_i \in \mathbb{F}_2$,

$$\Downarrow$$

$$f(x) = b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x \; (f(0) = 0 \Rightarrow b_0 = 0).$$

Example: second method

We suppose that error general locator polynomial exist. Let

- C be the code studied in the previous examples;
- parity-check matrix is a row, $H = (e_1, e_2, e_3, e_4, e_5)$;
- an general error locator polynomial $z + f(x)$ (the degree t of z is 1) must satisfy the following conditions:
  - $f(e_i) = \alpha^i\,, \quad \forall 1 \leq i \leq 5, \qquad$ and $f(0) = 0\,.$
  - $f(x)$ has degree at most 5
  - coefficients $b_i \in \mathbb{F}_2$,

$$\Downarrow$$

$$f(x) = b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x \; (f(0) = 0 \Rightarrow b_0 = 0).$$

Example: second method

We suppose that error general locator polynomial exist. Let

- C be the code studied in the previous examples;
- parity-check matrix is a row, $H = (e_1, e_2, e_3, e_4, e_5)$;
- an general error locator polynomial $z + f(x)$ (the degree t of z is 1) must satisfy the following conditions:
  - $f(e_i) = \alpha^i$, $\forall 1 \leq i \leq 5,$ and $f(0) = 0$.
  - $f(x)$ has degree at most 5
  - coefficients $b_i \in \mathbb{F}_2$,

$$\Downarrow$$

$$f(x) = b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x \ (f(0) = 0 \Rightarrow b_0 = 0).$$

Example: second method

We suppose that error general locator polynomial exist. Let

- C be the code studied in the previous examples;
- parity-check matrix is a row, $H = (e_1, e_2, e_3, e_4, e_5)$;
- an general error locator polynomial $z + f(x)$ (the degree t of z is 1) must satisfy the following conditions:
  - $f(e_i) = \alpha^i\,, \quad \forall 1 \le i \le 5, \qquad$ and $f(0) = 0\,.$
  - $f(x)$ has degree at most 5
  - coefficients $b_i \in \mathbb{F}_2$,

$$\Downarrow$$

$$f(x) = b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x \;(f(0) = 0 \Rightarrow b_0 = 0).$$

Example: second method

We suppose that error general locator polynomial exist. Let

- C be the code studied in the previous examples;
- parity-check matrix is a row, $H = (e_1, e_2, e_3, e_4, e_5)$;
- an general error locator polynomial $z + f(x)$ (the degree t of z is 1) must satisfy the following conditions:
  - $f(e_i) = \alpha^i, \quad \forall 1 \leq i \leq 5, \qquad$ and $f(0) = 0$.
  - $f(x)$ has degree at most 5
  - coefficients $b_i \in \mathbb{F}_2$,

$$\Downarrow$$

$$f(x) = b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x \; (f(0) = 0 \Rightarrow b_0 = 0).$$

Example: second method

We suppose that error general locator polynomial exist. Let

- C be the code studied in the previous examples;
- parity-check matrix is a row, $H = (e_1, e_2, e_3, e_4, e_5)$;
- an general error locator polynomial $z + f(x)$ (the degree t of z is 1) must satisfy the following conditions:
  - $f(e_i) = \alpha^i\,, \quad \forall 1 \leq i \leq 5, \qquad \text{and } f(0) = 0\,.$
  - $f(x)$ has degree at most 5
  - coefficients $b_i \in \mathbb{F}_2$,

$$\Downarrow$$

$$f(x) = b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x \ (f(0) = 0 \Rightarrow b_0 = 0).$$

Example: second method

- The Gröbner basis of ideal $J \subset \mathbb{F}_{16}[b_1, b_2, b_3, b_4, b_5, e_1, e_2, e_3, e_4, e_5]$ given by

$$J = \langle \quad e_1 + e_2 + e_3,\ e_3 + e_4 + e_5,\ \{e_i^{15} + 1\}_{1 \le i \le 5},\ \{b_i^2 + b_i\}_{1 \le i \le 5}, \\ f(e_1) + \gamma^3,\ f(e_2) + \gamma^6,\ f(e_3) + \gamma^9,\ f(e_4) + \gamma^{12},\ f(e_5) + \gamma^{15} \rangle$$

where relations $e_1 = e_2 + e_3$, $e_4 = e_3 + e_5$ follow from matrix G.

We obtain:

$$e_1 = \gamma^6,\ e_2 = \gamma^2,\ e_3 = \gamma^3,\ e_4 = \gamma^{14},\ e_5 = 1$$

$$\Downarrow$$

- $H = (\gamma^6, \gamma^2, \gamma^3, \gamma^{14}, 1)$ and the general error locator polynomial is $f(x) = x^3$, as in the first method, part B.

Example: second method

- The Gröbner basis of ideal $J \subset \mathbb{F}_{16}[b_1, b_2, b_3, b_4, b_5, e_1, e_2, e_3, e_4, e_5]$ given by

$$J = \langle \quad e_1 + e_2 + e_3,\ e_3 + e_4 + e_5,\ \{e_i^{15} + 1\}_{1 \le i \le 5},\ \{b_i^2 + b_i\}_{1 \le i \le 5}, \\ f(e_1) + \gamma^3,\ f(e_2) + \gamma^6,\ f(e_3) + \gamma^9,\ f(e_4) + \gamma^{12},\ f(e_5) + \gamma^{15} \rangle$$

  where relations $e_1 = e_2 + e_3$, $e_4 = e_3 + e_5$ follow from matrix G.

We obtain:

$$e_1 = \gamma^6,\ e_2 = \gamma^2,\ e_3 = \gamma^3,\ e_4 = \gamma^{14},\ e_5 = 1$$

$$\Downarrow$$

- $H = (\gamma^6, \gamma^2, \gamma^3, \gamma^{14}, 1)$ and the general error locator polynomial is $f(x) = x^3$, as in the first method, part B.

Example: second method

- The Gröbner basis of ideal $J \subset \mathbb{F}_{16}[b_1, b_2, b_3, b_4, b_5, e_1, e_2, e_3, e_4, e_5]$ given by

$$J = \langle \quad e_1 + e_2 + e_3,\ e_3 + e_4 + e_5,\ \{e_i^{15} + 1\}_{1 \le i \le 5},\ \{b_i^2 + b_i\}_{1 \le i \le 5}, \\ f(e_1) + \gamma^3,\ f(e_2) + \gamma^6,\ f(e_3) + \gamma^9,\ f(e_4) + \gamma^{12},\ f(e_5) + \gamma^{15} \rangle$$

  where relations $e_1 = e_2 + e_3$, $e_4 = e_3 + e_5$ follow from matrix G.

  We obtain:

$$e_1 = \gamma^6,\ e_2 = \gamma^2,\ e_3 = \gamma^3,\ e_4 = \gamma^{14},\ e_5 = 1$$

$$\Downarrow$$

- $H = (\gamma^6, \gamma^2, \gamma^3, \gamma^{14}, 1)$ and the general error locator polynomial is $f(x) = x^3$, as in the first method, part B.

Example: second method

- The Gröbner basis of ideal $J \subset \mathbb{F}_{16}[b_1, b_2, b_3, b_4, b_5, e_1, e_2, e_3, e_4, e_5]$ given by

$$J = \langle \quad e_1 + e_2 + e_3,\ e_3 + e_4 + e_5,\ \{e_i^{15} + 1\}_{1 \le i \le 5},\ \{b_i^2 + b_i\}_{1 \le i \le 5},\ f(e_1) + \gamma^3,\ f(e_2) + \gamma^6,\ f(e_3) + \gamma^9,\ f(e_4) + \gamma^{12},\ f(e_5) + \gamma^{15} \rangle$$

  where relations $e_1 = e_2 + e_3$, $e_4 = e_3 + e_5$ follow from matrix G.

  We obtain:

$$e_1 = \gamma^6,\ e_2 = \gamma^2,\ e_3 = \gamma^3,\ e_4 = \gamma^{14},\ e_5 = 1$$

$$\Downarrow$$

- $H = (\gamma^6, \gamma^2, \gamma^3, \gamma^{14}, 1)$ and the general error locator polynomial is $f(x) = x^3$, as in the first method, part B.

Let

- τ be a natural number corresponding to the number of errors,
- μ be a natural number corresponding to the number of erasures and such that $2\tau + \mu < d$.

  We have to find solutions of equations of type:

$$\bar{s}_j + \sum_{l=1}^{\tau} a_l g_j(\alpha^{k_l}) + \sum_{\bar{l}=1}^{\nu} \bar{c}_{\bar{l}} g_j(\alpha^{h_{\bar{l}}}), \quad j = 1, \ldots, r \tag{7}$$

  where
  - $\{k_l\}$, $\{a_l\}$ and $\{c_{\bar{l}}\}$ are unknown
  - $\{\bar{s}_j\}$, $\{h_{\bar{l}}\}$ are known.

Skip erasures

Let

- τ be a natural number corresponding to the number of errors,
- μ be a natural number corresponding to the number of erasures and such that $2\tau + \mu < d$.

We have to find solutions of equations of type:

$$\bar{s}_j + \sum_{l=1}^{\tau} a_l g_j(\alpha^{k_l}) + \sum_{\bar{l}=1}^{\nu} \bar{c}_{\bar{l}} g_j(\alpha^{h_{\bar{l}}}), \quad j = 1, \ldots, r \qquad (7)$$

where

- $\{k_l\}$, $\{a_l\}$ and $\{c_{\bar{l}}\}$ are unknown
- $\{\bar{s}_j\}$, $\{h_{\bar{l}}\}$ are known.

Skip erasures

Let

- τ be a natural number corresponding to the number of errors,
- μ be a natural number corresponding to the number of erasures and such that $2\tau + \mu < d$.

  We have to find solutions of equations of type:

$$\bar{s}_j + \sum_{l=1}^{\tau} a_l g_j(\alpha^{k_l}) + \sum_{\bar{l}=1}^{\nu} \bar{c}_{\bar{l}} g_j(\alpha^{h_{\bar{l}}}), \quad j = 1, \ldots, r \tag{7}$$

where

- $\{k_l\}, \{a_l\}$ and $\{c_{\bar{l}}\}$ are unknown
- $\{\bar{s}_j\}, \{h_{\bar{l}}\}$ are known.

Skip erasures

Let

- τ be a natural number corresponding to the number of errors,
- μ be a natural number corresponding to the number of erasures and such that $2\tau + \mu < d$.

  We have to find solutions of equations of type:

$$\bar{s}_j + \sum_{l=1}^{\tau} a_l g_j(\alpha^{k_l}) + \sum_{\bar{l}=1}^{\nu} \bar{c}_{\bar{l}} g_j(\alpha^{h_{\bar{l}}}), \quad j = 1, \ldots, r \qquad (7)$$

  where

  - $\{k_l\}, \{a_l\}$ and $\{c_{\bar{l}}\}$ are unknown
  - $\{\bar{s}_j\}, \{h_{\bar{l}}\}$ are known.

Skip erasures

Let

- τ be a natural number corresponding to the number of errors,
- μ be a natural number corresponding to the number of erasures and such that $2\tau + \mu < d$.

  We have to find solutions of equations of type:

$$\bar{s}_j + \sum_{l=1}^{\tau} a_l g_j(\alpha^{k_l}) + \sum_{\bar{l}=1}^{\nu} \bar{c}_{\bar{l}} g_j(\alpha^{h_{\bar{l}}}), \quad j = 1, \ldots, r \qquad (7)$$

where

- $\{k_l\}, \{a_l\}$ and $\{c_{\bar{l}}\}$ are unknown
- $\{\bar{s}_j\}, \{h_{\bar{l}}\}$ are known.

Skip erasures

We introduce

- variables $W = (w_\nu, \dots, w_1)$, where $\{w_{\mathrm{h}}\}$ stand for erasure locations $(\alpha^{h_{\bar{l}}})$;
- $U = (u_1, \dots, u_\nu)$, where $\{u_{\mathrm{h}}\}$ stand for erasure values $\bar{c}_{\bar{l}}$ $(\mathrm{h} = 1, \dots, \nu)$.

When the word $v(x)$ is received, the number ν of erasures and their positions $\{w_{\mathrm{h}}\}$ are known.

$\{x_j\}$ stand for the syndromes $(j = 1, \dots, r)$, as:

We introduce

- variables $W = (w_\nu, \ldots, w_1)$, where $\{w_\mathrm{h}\}$ stand for erasure locations $(\alpha^{h_{\bar{l}}})$;
- $U = (u_1, \ldots, u_\nu)$, where $\{u_\mathrm{h}\}$ stand for erasure values $\bar{c}_{\bar{l}}$ $(\mathrm{h} = 1, \ldots, \nu)$.

When the word $v(x)$ is received, the number ν of erasures and their positions $\{w_\mathrm{h}\}$ are known.

$\{x_j\}$ stand for the syndromes $(j = 1, \ldots, r)$, as:

We introduce

- variables $W = (w_\nu, \dots, w_1)$, where $\{w_\mathrm{h}\}$ stand for erasure locations $(\alpha^{h_{\bar{l}}})$;
- $U = (u_1, \dots, u_\nu)$, where $\{u_\mathrm{h}\}$ stand for erasure values $\bar{c}_{\bar{l}}$ $(\mathrm{h} = 1, \dots, \nu)$.

When the word $v(x)$ is received, the number ν of erasures and their positions $\{w_\mathrm{h}\}$ are known.

$\{x_j\}$ stand for the syndromes $(j = 1, \dots, r)$, as:

We introduce

- variables $W = (w_\nu, \ldots, w_1)$, where $\{w_\mathrm{h}\}$ stand for erasure locations $(\alpha^{\bar{h}_l})$;
- $U = (u_1, \ldots, u_\nu)$, where $\{u_\mathrm{h}\}$ stand for erasure values $\bar{c}_{\bar{l}}$ $(\mathrm{h} = 1, \ldots, \nu)$.

When the word $v(x)$ is received, the number ν of erasures and their positions $\{w_\mathrm{h}\}$ are known.

$\{x_j\}$ stand for the syndromes $(j = 1, \ldots, r)$, as:

We introduce

- variables $W = (w_\nu, \dots, w_1)$, where $\{w_\mathrm{h}\}$ stand for erasure locations (α^{h_l});
- $U = (u_1, \dots, u_\nu)$, where $\{u_\mathrm{h}\}$ stand for erasure values $\bar{c}_l$ $(\mathrm{h} = 1, \dots, \nu)$.

When the word $v(x)$ is received, the number ν of erasures and their positions $\{w_\mathrm{h}\}$ are known.

$\{x_j\}$ stand for the syndromes $(j = 1, \dots, r)$, as:

Skip description for the erasure ideal

$$
\begin{array}{lll}
J^{C,\tau,\nu} = \langle & \{\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j\}_{j=1,\dots,r}, & \\
& \{z_i^{n+1} - z_i\}_{i=1,\dots,\tau}, & \{y_i^{q-1} - 1\}_{i=1,\dots,\tau}, \\
& \{u_h^q - u_h\}_{h=1,\dots,\nu}, & \{w_h^n - 1\}_{h=1,\dots,\nu}, \\
& \{x_j^{q^m} - x_j\}_{j=1,\dots,r}, & \{p(w_h, w_k)\}_{h\neq k, h,k=1,\dots,\nu}, \\
& \{z_i p(z_i, w_h)\}_{i=1,\dots,\tau, h=1,\dots,\nu}, & \{z_i z_j p(z_i, z_j)\}_{i\neq j, i,j=1,\dots,\tau}\rangle.
\end{array}
$$

We observe that polynomials:

- $\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j$ characterize the nth-root code;
- $z_i^{n+1} - z_i$ ensure that z_i are nth-roots of unity or 0;
- $y_i^{q-1} - 1$, $w_h^n - 1$, $u_h^q - u_h$ ensure that $y_i, w_h \in \mathbb{F}_q^*$ and $u_h \in \mathbb{F}_q$;
- $z_i p(z_i, w_h)$ ensure that an error cannot occur in a position corresponding to an erasure;
- $p(w_h, w_k)$ ensure that any two erasure locations are distinct;
- $z_i z_j p(z_i, z_j)$ ensure that any two error locations are distinct.

Ideal $J^{C,\tau,\nu}$ depends only on code C and on ν.

$$J^{C,\tau,\nu} = \langle \begin{array}{ll} \{\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j\}_{j=1,\dots,r}, & \\ \{z_i^{n+1} - z_i\}_{i=1,\dots,\tau}, & \{y_i^{q-1} - 1\}_{i=1,\dots,\tau}, \\ \{u_h^q - u_h\}_{h=1,\dots,\nu}, & \{w_h^n - 1\}_{h=1,\dots,\nu}, \\ \{x_j^{q^m} - x_j\}_{j=1,\dots,r}, & \{p(w_h, w_k)\}_{h\neq k, h,k=1,\dots,\nu}, \\ \{z_i p(z_i, w_h)\}_{i=1,\dots,\tau, h=1,\dots,\nu}, & \{z_i z_j p(z_i, z_j)\}_{i\neq j, i,j=1,\dots,\tau} \rangle. \end{array}$$

We observe that polynomials:

- $\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j$ characterize the nth-root code;
- $z_i^{n+1} - z_i$ ensure that z_i are nth-roots of unity or 0;
- $y_i^{q-1} - 1$, $w_h^n - 1$, $u_h^q - u_h$ ensure that $y_i, w_h \in \mathbb{F}_q^*$ and $u_h \in \mathbb{F}_q$;
- $z_i p(z_i, w_h)$ ensure that an error cannot occur in a position corresponding to an erasure;
- $p(w_h, w_k)$ ensure that any two erasure locations are distinct;
- $z_i z_j p(z_i, z_j)$ ensure that any two error locations are distinct.

Ideal $J^{C,\tau,\nu}$ depends only on code C and on ν.

$$
\begin{array}{lll}
J^{C,\tau,\nu} = \langle & \{\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j\}_{j=1,\dots,r}, & \\
& \{z_i^{n+1} - z_i\}_{i=1,\dots,\tau}, & \{y_i^{q-1} - 1\}_{i=1,\dots,\tau}, \\
& \{u_h^q - u_h\}_{h=1,\dots,\nu}, & \{w_h^n - 1\}_{h=1,\dots,\nu}, \\
& \{x_j^{q^m} - x_j\}_{j=1,\dots,r}, & \{p(w_h, w_k)\}_{h \neq k, h,k=1,\dots,\nu}, \\
& \{z_i p(z_i, w_h)\}_{i=1,\dots,\tau, h=1,\dots,\nu}, & \{z_i z_j p(z_i, z_j)\}_{i \neq j, i,j=1,\dots,\tau}\rangle.
\end{array}
$$

We observe that polynomials:

- $\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j$ characterize the nth-root code;
- $z_i^{n+1} - z_i$ ensure that z_i are nth-roots of unity or 0;
- $y_i^{q-1} - 1$, $w_h^n - 1$, $u_h^q - u_h$ ensure that $y_i, w_h \in \mathbb{F}_q^*$ and $u_h \in \mathbb{F}_q$;
- $z_i p(z_i, w_h)$ ensure that an error cannot occur in a position corresponding to an erasure;
- $p(w_h, w_k)$ ensure that any two erasure locations are distinct;
- $z_i z_j p(z_i, z_j)$ ensure that any two error locations are distinct.

Ideal $J^{C,\tau,\nu}$ depends only on code C and on ν.

$$
\begin{array}{lll}
J^{C,\tau,\nu} = \langle & \{\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j\}_{j=1,\dots,r}, & \\
& \{z_i^{n+1} - z_i\}_{i=1,\dots,\tau}, & \{y_i^{q-1} - 1\}_{i=1,\dots,\tau}, \\
& \{u_h^q - u_h\}_{h=1,\dots,\nu}, & \{w_h^n - 1\}_{h=1,\dots,\nu}, \\
& \{x_j^{q^m} - x_j\}_{j=1,\dots,r}, & \{p(w_h, w_k)\}_{h\neq k, h,k=1,\dots,\nu}, \\
& \{z_i p(z_i, w_h)\}_{i=1,\dots,\tau, h=1,\dots,\nu}, & \{z_i z_j p(z_i, z_j)\}_{i\neq j, i,j=1,\dots,\tau}\rangle.
\end{array}
$$

We observe that polynomials:

- $\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j$ characterize the nth-root code;
- $z_i^{n+1} - z_i$ ensure that z_i are nth-roots of unity or 0;
- $y_i^{q-1} - 1$, $w_h^n - 1$, $u_h^q - u_h$ ensure that $y_i, w_h \in \mathbb{F}_q^*$ and $u_h \in \mathbb{F}_q$;
- $z_i p(z_i, w_h)$ ensure that an error cannot occur in a position corresponding to an erasure;
- $p(w_h, w_k)$ ensure that any two erasure locations are distinct;
- $z_i z_j p(z_i, z_j)$ ensure that any two error locations are distinct.

Ideal $J^{C,\tau,\nu}$ depends only on code C and on ν.

$$
\begin{array}{lll}
J^{C,\tau,\nu} = \langle & \{\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j\}_{j=1,\dots,r}, & \\
& \{z_i^{n+1} - z_i\}_{i=1,\dots,\tau}, & \{y_i^{q-1} - 1\}_{i=1,\dots,\tau}, \\
& \{u_h^q - u_h\}_{h=1,\dots,\nu}, & \{w_h^n - 1\}_{h=1,\dots,\nu}, \\
& \{x_j^{q^m} - x_j\}_{j=1,\dots,r}, & \{p(w_h, w_k)\}_{h\neq k, h,k=1,\dots,\nu}, \\
& \{z_i p(z_i, w_h)\}_{i=1,\dots,\tau, h=1,\dots,\nu}, & \{z_i z_j p(z_i, z_j)\}_{i\neq j, i,j=1,\dots,\tau}\rangle.
\end{array}
$$

We observe that polynomials:

- $\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j$ characterize the nth-root code;
- $z_i^{n+1} - z_i$ ensure that z_i are nth-roots of unity or 0;
- $y_i^{q-1} - 1$, $w_h^n - 1$, $u_h^q - u_h$ ensure that $y_i, w_h \in \mathbb{F}_q^*$ and $u_h \in \mathbb{F}_q$;
- $z_i p(z_i, w_h)$ ensure that an error cannot occur in a position corresponding to an erasure;
- $p(w_h, w_k)$ ensure that any two erasure locations are distinct;
- $z_i z_j p(z_i, z_j)$ ensure that any two error locations are distinct.

Ideal $J^{C,\tau,\nu}$ depends only on code C and on ν.

$$
\begin{aligned}
J^{C,\tau,\nu} = \langle \quad & \{\textstyle\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j\}_{j=1,\dots,r}, \\
& \{z_i^{n+1} - z_i\}_{i=1,\dots,\tau}, \qquad \{y_i^{q-1} - 1\}_{i=1,\dots,\tau}, \\
& \{u_h^q - u_h\}_{h=1,\dots,\nu}, \qquad \{w_h^n - 1\}_{h=1,\dots,\nu}, \\
& \{x_j^{q^m} - x_j\}_{j=1,\dots,r}, \qquad \{p(w_h, w_k)\}_{h\neq k, h,k=1,\dots,\nu}, \\
& \{z_i p(z_i, w_h)\}_{i=1,\dots,\tau, h=1,\dots,\nu}, \qquad \{z_i z_j p(z_i, z_j)\}_{i\neq j, i,j=1,\dots,\tau}\rangle.
\end{aligned}
$$

We observe that polynomials:

- $\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j$ characterize the nth-root code;
- $z_i^{n+1} - z_i$ ensure that z_i are nth-roots of unity or 0;
- $y_i^{q-1} - 1$, $w_h^n - 1$, $u_h^q - u_h$ ensure that $y_i, w_h \in \mathbb{F}_q^*$ and $u_h \in \mathbb{F}_q$;
- $z_i p(z_i, w_h)$ ensure that an error cannot occur in a position corresponding to an erasure;
- $p(w_h, w_k)$ ensure that any two erasure locations are distinct;
- $z_i z_j p(z_i, z_j)$ ensure that any two error locations are distinct.

Ideal $J^{C,\tau,\nu}$ depends only on code C and on ν.

$$
\begin{array}{lll}
J^{C,\tau,\nu} = \langle & \{\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j\}_{j=1,\ldots,r}, & \\
& \{z_i^{n+1} - z_i\}_{i=1,\ldots,\tau}, & \{y_i^{q-1} - 1\}_{i=1,\ldots,\tau}, \\
& \{u_h^q - u_h\}_{h=1,\ldots,\nu}, & \{w_h^n - 1\}_{h=1,\ldots,\nu}, \\
& \{x_j^{q^m} - x_j\}_{j=1,\ldots,r}, & \{p(w_h, w_k)\}_{h\neq k, h,k=1,\ldots,\nu}, \\
& \{z_i p(z_i, w_h)\}_{i=1,\ldots,\tau, h=1,\ldots,\nu}, & \{z_i z_j p(z_i, z_j)\}_{i\neq j, i,j=1,\ldots,\tau}\rangle.
\end{array}
$$

We observe that polynomials:

- $\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j$ characterize the nth-root code;
- $z_i^{n+1} - z_i$ ensure that z_i are nth-roots of unity or 0;
- $y_i^{q-1} - 1$, $w_h^n - 1$, $u_h^q - u_h$ ensure that $y_i, w_h \in \mathbb{F}_q^*$ and $u_h \in \mathbb{F}_q$;
- $z_i p(z_i, w_h)$ ensure that an error cannot occur in a position corresponding to an erasure;
- $p(w_h, w_k)$ ensure that any two erasure locations are distinct;
- $z_i z_j p(z_i, z_j)$ ensure that any two error locations are distinct.

Ideal $J^{C,\tau,\nu}$ depends only on code C and on ν.

$$
\begin{array}{lll}
J^{C,\tau,\nu} = \langle & \{\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j\}_{j=1,\dots,r}, & \\
& \{z_i^{n+1} - z_i\}_{i=1,\dots,\tau}, & \{y_i^{q-1} - 1\}_{i=1,\dots,\tau}, \\
& \{u_h^q - u_h\}_{h=1,\dots,\nu}, & \{w_h^n - 1\}_{h=1,\dots,\nu}, \\
& \{x_j^{q^m} - x_j\}_{j=1,\dots,r}, & \{p(w_h, w_k)\}_{h\neq k, h,k=1,\dots,\nu}, \\
& \{z_i p(z_i, w_h)\}_{i=1,\dots,\tau, h=1,\dots,\nu}, & \{z_i z_j p(z_i, z_j)\}_{i\neq j, i,j=1,\dots,\tau}\rangle.
\end{array}
$$

We observe that polynomials:

- $\sum_{l=1}^{\tau} y_l g_j(z_l) + \sum_{\bar{l}}^{\nu} u_{\bar{l}} g_j(w_{\bar{l}}) - x_j$ characterize the nth-root code;
- $z_i^{n+1} - z_i$ ensure that z_i are nth-roots of unity or 0;
- $y_i^{q-1} - 1$, $w_h^n - 1$, $u_h^q - u_h$ ensure that $y_i, w_h \in \mathbb{F}_q^*$ and $u_h \in \mathbb{F}_q$;
- $z_i p(z_i, w_h)$ ensure that an error cannot occur in a position corresponding to an erasure;
- $p(w_h, w_k)$ ensure that any two erasure locations are distinct;
- $z_i z_j p(z_i, z_j)$ ensure that any two error locations are distinct.

Ideal $J^{C,\tau,\nu}$ depends only on code C and on ν.

Proposition

In Gröbner basis $\mathcal{G}^{C,\tau,\nu}$ there is a unique polynomial of type

$$g = z_\tau^\tau + a_{\tau-1} z^{\tau-1} + \ldots + a_0,\ a_i \in \mathbb{F}_{q^m}[X, W].$$

Theorem

If code C is a proper maximal zerofree nth-root code, then C possesses general error locator polynomials of type ν, for any $\nu \geq 0$.

Proposition

In Gröbner basis $\mathcal{G}^{C,\tau,\nu}$ there is a unique polynomial of type

$$g = z_\tau^\tau + a_{\tau-1} z^{\tau-1} + \ldots + a_0,\ a_i \in \mathbb{F}_{q^m}[X, W].$$

Theorem

If code C is a proper maximal zerofree nth-root code, then C possesses general error locator polynomials of type ν, for any $\nu \geq 0$.

Example III

Let C' be the shortened code obtained from code C presented in Example I. Code C' is a $[7, 1, 6]$ linear code, so that τ (errors) and μ (erasures) satisfy relation $\tau + \mu < 6$. If $\tau = 1, \mu = 2$, the syndrome ideal is

$$\begin{aligned} J = \quad & \{g_1(z_1) + u_1 g_1(w_1) + u_2 g(w_2) + x_1, g_2(z_1) + u_1 g_2(w_1) + u_2 g_2(w_2) + x_2, \\ & z_1^8 - z_1, w_1^7 - 1, w_2^7 - 1, x_1^8 - x_1, x_2^8 + x_2, u_1^2 + u_1, u_2^2 + u_2, \\ & z_1 p(z_1, w_1), z_1 p(z_1, w_2), p(w_1, w_2)\} \end{aligned}$$

and in the reduced Gröbner basis there is only one polynomial having z_1 as leading term (see Appendix of [4]).

Definition

Let g be a divisor of $x^n - 1$ over $\mathbb{F}_q$. We define S_C as the set $S_C = \{i_1, \dots, i_{n-k} | g(\alpha^{i_j}) = 0, 1 \leq i_j \leq n\}$ of all powers of α that are roots of g. Let H be the following matrix:

$$H = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \dots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \dots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_{n-k}} & \alpha^{2i_{n-k}} & \dots & \alpha^{(n-1)i_{n-k}} \end{pmatrix}.$$

The **cyclic** code C generated by g is the linear code C over $\mathbb{F}_q$ such that H is a parity-check matrix for C.

- $L = R_n$, i.e. $L = \{\alpha, \alpha^2, \dots, \alpha^n\}$
- $\mathcal{P} = \{x^{i_j} \mid i_j \in S_C\}$
- C as the nth-root code $\Omega(q, n, q^m, R_n, \{x^{i_j} \mid i_j \in S_C\})$

Proposition

Any cyclic code is a proper maximal zerofree nth-root code. As a consequence, it possesses a general error locator polynomial.

Definition

Let g be a divisor of $x^n - 1$ over $\mathbb{F}_q$. We define S_C as the set $S_C = \{i_1, \dots, i_{n-k} | g(\alpha^{i_j}) = 0, 1 \leq i_j \leq n\}$ of all powers of α that are roots of g. Let H be the following matrix:

$$H = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \dots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \dots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_{n-k}} & \alpha^{2i_{n-k}} & \dots & \alpha^{(n-1)i_{n-k}} \end{pmatrix}.$$

The **cyclic** code C generated by g is the linear code C over $\mathbb{F}_q$ such that H is a parity-check matrix for C.

- $L = R_n$, i.e. $L = \{\alpha, \alpha^2, \dots, \alpha^n\}$
- $\mathcal{P} = \{x^{i_j} \mid i_j \in S_C\}$
- C as the nth-root code $\Omega(q, n, q^m, R_n, \{x^{i_j} \mid i_j \in S_C\})$

Proposition

Any cyclic code is a proper maximal zerofree nth-root code. As a consequence, it possesses a general error locator polynomial.

Definition

Let g be a divisor of $x^n - 1$ over $\mathbb{F}_q$. We define S_C as the set $S_C = \{i_1, \ldots, i_{n-k} | g(\alpha^{i_j}) = 0, 1 \leq i_j \leq n\}$ of all powers of α that are roots of g. Let H be the following matrix:

$$H = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \ldots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \ldots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_{n-k}} & \alpha^{2i_{n-k}} & \ldots & \alpha^{(n-1)i_{n-k}} \end{pmatrix}.$$

The **cyclic** code C generated by g is the linear code C over $\mathbb{F}_q$ such that H is a parity-check matrix for C.

- $L = R_n$, i.e. $L = \{\alpha, \alpha^2, \ldots, \alpha^n\}$
- $\mathcal{P} = \{x^{i_j} \mid i_j \in S_C\}$
- C as the nth-root code $\Omega(q, n, q^m, R_n, \{x^{i_j} \mid i_j \in S_C\})$

Proposition

Any cyclic code is a proper maximal zerofree nth-root code. As a consequence, it possesses a general error locator polynomial.

Definition

Let g be a divisor of $x^n - 1$ over $\mathbb{F}_q$. We define S_C as the set $S_C = \{i_1, \ldots, i_{n-k} | g(\alpha^{i_j}) = 0, 1 \leq i_j \leq n\}$ of all powers of α that are roots of g. Let H be the following matrix:

$$H = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \ldots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \ldots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_{n-k}} & \alpha^{2i_{n-k}} & \ldots & \alpha^{(n-1)i_{n-k}} \end{pmatrix}.$$

The **cyclic** code C generated by g is the linear code C over $\mathbb{F}_q$ such that H is a parity-check matrix for C.

- $L = R_n$, i.e. $L = \{\alpha, \alpha^2, \ldots, \alpha^n\}$
- $\mathcal{P} = \{x^{i_j} \mid i_j \in S_C\}$
- C as the nth-root code $\Omega(q, n, q^m, R_n, \{x^{i_j} \mid i_j \in S_C\})$

Proposition

Any cyclic code is a proper maximal zerofree nth-root code. As a consequence, it possesses a general error locator polynomial.

Definition

Let g be a divisor of $x^n - 1$ over $\mathbb{F}_q$. We define S_C as the set $S_C = \{i_1, \dots, i_{n-k} | g(\alpha^{i_j}) = 0, 1 \leq i_j \leq n\}$ of all powers of α that are roots of g. Let H be the following matrix:

$$H = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \dots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \dots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_{n-k}} & \alpha^{2i_{n-k}} & \dots & \alpha^{(n-1)i_{n-k}} \end{pmatrix}.$$

The **cyclic** code C generated by g is the linear code C over $\mathbb{F}_q$ such that H is a parity-check matrix for C.

- $L = R_n$, i.e. $L = \{\alpha, \alpha^2, \dots, \alpha^n\}$
- $\mathcal{P} = \{x^{i_j} \mid i_j \in S_C\}$
- C as the nth-root code $\Omega(q, n, q^m, R_n, \{x^{i_j} \mid i_j \in S_C\})$

Proposition

Any cyclic code is a proper maximal zerofree nth-root code. As a consequence, it possesses a general error locator polynomial.

Shortened cyclic codes

Shortened cyclic codes can be seen as nth-root codes: if D is a subset of positions where cyclic code C is shortened, then code $C(D)$ is an nth-root code $\Omega(q, n, q^m, L, \mathcal{P})$, where q, n and $\mathcal{P}$ are as above and $L = \{\alpha^j \mid 1 \leq j \leq n, j \notin D\}$.

Reed Solomon code

A RS code is a cyclic code with generator polynomial $g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \ldots (x - \alpha^{b-\delta-2})$, where α is the primitive element of $\mathbb{F}_{q^m}$. A RS code can be treated as an nth-root code $\Omega(q, n, q^m, \mathbb{F}^*_{q^m}, \{x^i \mid i = b, b+1, \ldots, b+\delta-2\})$.

Shortened cyclic codes

Shortened cyclic codes can be seen as nth-root codes: if D is a subset of positions where cyclic code C is shortened, then code $C(D)$ is an nth-root code $\Omega(q, n, q^m, L, \mathcal{P})$, where q, n and $\mathcal{P}$ are as above and $L = \{\alpha^j \mid 1 \leq j \leq n, j \notin D\}$.

Reed Solomon code

A RS code is a cyclic code with generator polynomial $g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \ldots (x - \alpha^{b-\delta-2})$, where α is the primitive element of $\mathbb{F}_{q^m}$. A RS code can be treated as an nth-root code $\Omega(q, n, q^m, \mathbb{F}^*_{q^m}, \{x^i \mid i = b, b+1, \ldots, b+\delta-2\})$.

Definition

Let $g(z) \in \mathbb{F}_{q^m}[z]$, $\deg(g) = r \geq 2$, and let $L = \{\alpha_1, \ldots, \alpha_N\}$ denote a subset of elements of $\mathbb{F}_{q^m}$ which are not roots of $g(z)$. Then the **Goppa code** $\Gamma(L, g)$ is defined as the set of all vectors $c = (c_1, \ldots, c_N)$ with components in $\mathbb{F}_q$ that satisfy the condition:

$$\sum_{i=1}^{N} \frac{c_i}{z - \alpha_i} \equiv 0 \mod g(z) \, .$$

A parity-check matrix for $\Gamma(L, g)$ can be written as:

$$H = \begin{pmatrix} \frac{1}{g(\alpha_1)} & \frac{1}{g(\alpha_2)} & \cdots & \frac{1}{g(\alpha_N)} \\ \frac{\alpha_1}{g(\alpha_1)} & \frac{\alpha_2}{g(\alpha_2)} & \cdots & \frac{\alpha_N}{g(\alpha_N)} \\ \frac{\alpha_1^2}{g(\alpha_1)} & \frac{\alpha_2^2}{g(\alpha_2)} & \cdots & \frac{\alpha_N^2}{g(\alpha_N)} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_1^{r-1}}{g(\alpha_1)} & \frac{\alpha_2^{r-1}}{g(\alpha_2)} & \cdots & \frac{\alpha_N^{r-1}}{g(\alpha_N)} \end{pmatrix} .$$

- Setting q, m and L as in definition, $n = q^m - 1$, $\mathcal{P} = \{\frac{x^i}{g(x)}, \forall i = 0, \ldots, r-1\}$
- It follows that classical Goppa code $\Gamma(L, g)$ over $\mathbb{F}_q$ is the nth-root code

$$\Gamma = \Omega\left(q, q^m - 1, q^m, L, \left\{\frac{x^i}{g(x)} | i = 0, \ldots, r-1\right\}\right).$$

Proposition

If the Goppa polynomial g is in $\mathbb{F}_q[x]$, then $\Gamma(L, g)$ is a proper nth-root code. In particular, if $L = \mathbb{F}_{q^m} \setminus \{0\}$, code $\Gamma(L, g)$ is proper and maximal.

Theorem

Any classical Goppa code $\Gamma(L, g)$ such that $g \in \mathbb{F}_q[x]$ and $L = \mathbb{F}^*_{q^m}$ admits a general error locator polynomial.

- Setting q, m and L as in definition, $n = q^m - 1$, $\mathcal{P} = \{\frac{x^i}{g(x)}, \forall i = 0, \ldots, r-1\}$
- It follows that classical Goppa code $\Gamma(L, g)$ over $\mathbb{F}_q$ is the nth-root code

$$\Gamma = \Omega\left(q, q^m - 1, q^m, L, \left\{\frac{x^i}{g(x)} | i = 0, \ldots, r-1\right\}\right).$$

Proposition

If the Goppa polynomial g is in $\mathbb{F}_q[x]$, then $\Gamma(L, g)$ is a proper nth-root code. In particular, if $L = \mathbb{F}_{q^m} \setminus \{0\}$, code $\Gamma(L, g)$ is proper and maximal.

Theorem

Any classical Goppa code $\Gamma(L, g)$ such that $g \in \mathbb{F}_q[x]$ and $L = \mathbb{F}_{q^m}^*$ admits a general error locator polynomial.

- Setting q, m and L as in definition, $n = q^m - 1$, $\mathcal{P} = \{\frac{x^i}{g(x)}, \forall i = 0, \dots, r-1\}$
- It follows that classical Goppa code $\Gamma(L, g)$ over $\mathbb{F}_q$ is the nth-root code

$$\Gamma = \Omega\left(q, q^m - 1, q^m, L, \left\{\frac{x^i}{g(x)} | i = 0, \dots, r-1\right\}\right).$$

Proposition

If the Goppa polynomial g is in $\mathbb{F}_q[x]$, then $\Gamma(L, g)$ is a proper nth-root code. In particular, if $L = \mathbb{F}_{q^m} \setminus \{0\}$, code $\Gamma(L, g)$ is proper and maximal.

Theorem

Any classical Goppa code $\Gamma(L, g)$ such that $g \in \mathbb{F}_q[x]$ and $L = \mathbb{F}_{q^m}^*$ admits a general error locator polynomial.

- Setting q, m and L as in definition, $n = q^m - 1$, $\mathcal{P} = \{\frac{x^i}{g(x)}, \forall i = 0, \ldots, r-1\}$
- It follows that classical Goppa code $\Gamma(L, g)$ over $\mathbb{F}_q$ is the nth-root code

$$\Gamma = \Omega\left(q, q^m - 1, q^m, L, \left\{\frac{x^i}{g(x)} | i = 0, \ldots, r-1\right\}\right) .$$

Proposition

If the Goppa polynomial g is in $\mathbb{F}_q[x]$, then $\Gamma(L, g)$ is a proper nth-root code. In particular, if $L = \mathbb{F}_{q^m} \setminus \{0\}$, code $\Gamma(L, g)$ is proper and maximal.

Theorem

Any classical Goppa code $\Gamma(L, g)$ such that $g \in \mathbb{F}_q[x]$ and $L = \mathbb{F}_{q^m}^*$ admits a general error locator polynomial.

Consider the nth-root code of the first Example, shortened in position 0. It is a classical Goppa code with $g(x) = x^2 + x + 1$ and $L = \mathbb{F}_8^*$.
A general error locator polynomial for this code is

$$
\begin{aligned}
\mathcal{L} = & \mathbf{z_2^2} + \\
& z_2(x_1^5x_2^2 + x_1^5 + x_1^3x_2^2 + x_1^3 + x_1^2x_2^2 + \\
& x_1^2x_2 + x_1x_2^5 + x_1x_2^4 + x_1x_2^3 + x_1x_2^2 + \\
& x_1x_2 + x_1 + x_2^7 + x_2^4 + x_2^3 + x_2^2 + 1) + \\
& x_1^5x_2^2 + x_1^5x_2 + x_1^5 + x_1^4x_2^2 + \\
& x_1^3x_2^3 + x_1^2x_2 + x_1^2 + x_1x_2^6 + \\
& x_1x_2 + x_1 + x_2^7 + x_2^6 .
\end{aligned}
$$

Consider irreducible Goppa codes, $\Gamma(L, g)$ such that $L = \mathbb{F}_{q^m}$. These codes admit also the following parity-check matrix H:

$$H = \left(\frac{1}{\gamma-\zeta_0}, \quad \frac{1}{\gamma-\zeta_1}, \quad \cdots, \quad \frac{1}{\gamma-\zeta_{q^m-1}} \right),$$

where $\gamma \in \mathbb{F}_{q^{mr}}$ is any root of $g(x)$ and $\mathbb{F}_{q^m} = \{\zeta_i \mid 0 \leq i \leq q^m - 1\}$. We can extend the definition of nth-root codes to **generalized nth-root codes**, by allowing also $\mathcal{P} \subset \mathbb{F}_Q[X]$ with $\mathbb{F}_{q^m} \subset \mathbb{F}_Q$. In this sense, an irreducible Goppa code $\Gamma(L, g)$ can be considered as a generalized nth-root code $\Omega(q, q^m - 1, q^{mr}, \mathbb{F}_{q^{mr}}, \mathcal{P})$, where $\mathcal{P} = \{g(x)\} = \{\frac{1}{\gamma - x}\}$

Other families of codes

- Reed-Muller codes
- Hermitian codes

Other families of codes

- Reed-Muller codes
- Hermitian codes

We can investigate on

- general error locator polynomial for nth-root non proper;
- which other class of codes are nth-root;
- which representation of nth-root permits to find a sparse general error locator polynomial.

We can investigate on

- general error locator polynomial for nth-root non proper;
- which other class of codes are nth-root;
- which representation of nth-root permits to find a sparse general error locator polynomial.

We can investigate on

- general error locator polynomial for nth-root non proper;
- which other class of codes are nth-root;
- which representation of nth-root permits to find a sparse general error locator polynomial.

Bibliography

Fitzpatrick, P., On the key equation, IEEE Trans. Inform. Theory, 1995, volume = 41, 1290–1302, 5.

M. Giorgetti, "*About the nth-root codes: a Groebner basis approach to the weight computation*", poster presented at Workshop D1: Groebner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics, Linz, Austria, 1-6 may 2006.

M. Giorgetti, "*A Gröbner basis approach to the weight computation of some new codes*", Workshop on Coding and Cryptography, 22-23 may 2006, BCRI, UCC Cork, Ireland.

M. Giorgetti, M. Sala, *A commutative algebra approach to linear codes*, University College Cork, 2006, BCRI preprint, `www.bcri.ucc.ie`, number 58, Boole Centre BCRI, UCC Cork, Ireland.

M. Giorgetti, M. Sala "*General error locator polynomials for nth-root codes*", Workshop on Coding and Cryptography, 16-20 April 2007, INRIA, Paris, France.

T. Mora, E. Orsini, M. Sala, *General error locator polynomials for binary cyclic codes with* $t <= 2$ *and* $n < 63$, University College Cork, 2006, BCRI preprint, `www.bcri.ucc.ie`, number 43, Boole Centre BCRI, UCC Cork, Ireland.

E. Orsini, M. Sala, *General error locator polynomials for binary cyclic codes with* $t <= 2$ *and* $n < 63$, IEEE Trans. Inform. Theory, 2007, vol. 53, pag. 1095–1107.

E. Orsini, M. Sala, *Correcting errors and erasures via the syndrome variety*, J. Pure Appl. Algebra, 2005, vol. 200 pages 191–226, number 1-2.

M. Caboara, T. Mora, *The Chen-Reed-Helleseth-Truong decoding algorithm and the Gianni-Kalkbrenner Groebner shape theorem*, Applicable Algebra in Engineering, Communication and Computing 2002, vol. 13, p. 209–232