Code-Based Cryptography

Error-Correcting Codes and Cryptography

I. Márquez-Corbella

informatiques mathématiques

1. Error-Correcting Codes and Cryptography

1. Introduction I - Cryptography
2. Introduction II - Coding Theory
3. Encoding (Linear Transformation)
4. Parity Checking
5. Error Correcting Capacity
6. Decoding (A Difficult Problem)
7. Reed-Solomon Codes
8. **Goppa Codes**
9. McEliece Cryptosystem

New codes from the GRS codes

1. **Main disadvantage of GRS codes:**

Consider $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ of length n, then $n \leq q$

New codes from the GRS codes

1. **Main disadvantage of GRS codes:**

   Consider $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ of length n, then $n \leq q$

2. **New codes from GRS:** How to construct codes over small alphabets with the same features as GRS codes?

New codes from the GRS codes

1. **Main disadvantage of GRS codes:**

   Consider $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ of length n, then $n \leq q$

2. **New codes from GRS:** How to construct codes over small alphabets with the same features as GRS codes?
   - Construct a GRS over a large extension of $\mathbb{F}$

New codes from the GRS codes

1. **Main disadvantage of GRS codes:**

   Consider $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ of length n, then $n \leq q$

2. **New codes from GRS:** How to construct codes over small alphabets with the same features as GRS codes?
   - Construct a GRS over a large extension of $\mathbb{F}$
   - $\mathcal{C}_{\mathrm{NEW}} = \mathrm{GRS} \cap \mathbb{F}$

Alternant codes

- $a = (a_1, \ldots, a_n) \in \mathbb{F}_{q^m}^n$ with $a_i \neq a_j$ for all $i \neq j$
- $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_{q^m}^n$ with $b_i \neq 0$ for all i.

Alternant codes

$$\mathrm{Alt}_r(\mathbf{a}, \mathbf{b}) = (\mathrm{GRS}_r(\mathbf{a}, \mathbf{b}))^{\perp} \cap \mathbb{F}_q$$

Alternant codes

- $a = (a_1, \ldots, a_n) \in \mathbb{F}_{q^m}^n$ with $a_i \neq a_j$ for all $i \neq j$ $\Longrightarrow$ support
- $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_{q^m}^n$ with $b_i \neq 0$ for all i. $\Longrightarrow$ **column multipliers**

Alternant codes

$$\mathrm{Alt}_r(\mathbf{a}, \mathbf{b}) = (\mathrm{GRS}_r(\mathbf{a}, \mathbf{b}))^{\perp} \cap \mathbb{F}_q$$

Alternant codes - Parameters

Proposition

$\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})$ is an $[n, k, d]_q$ code with

$$k \geq n - mr \quad \text{and} \quad d \geq r + 1$$

Proof:

Recall that

$$\mathrm{GRS}_r(\mathbf{a}, \mathbf{b})^{\perp} = \underbrace{\mathrm{GRS}_{n-k}(\mathbf{a}, \mathbf{c})}_{[n, n-r, r+1]_{q^m} \text{ code}}$$

Hence, $\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})$ can be defined by:

$$\left.\begin{array}{l} r \text{ parity check equations over } \mathbb{F}_{q^m} \\ mr \text{ parity check equations over } \mathbb{F}_q \end{array}\right\} \Longrightarrow \dim\left(\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})\right) \geq n - mr$$

Moreover, the minimum distance of $\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})$ is at least the minimum distance of $\mathrm{GRS}_{n-k}(\mathbf{a}, \mathbf{c})$ since $\mathrm{Alt}_r(\mathbf{a}, \mathbf{b}) \subseteq \mathrm{GRS}_{n-k}(\mathbf{a}, \mathbf{c})$

Decoding Alternant codes

$$\mathrm{Alt}_r(\mathbf{a}, \mathbf{b}) \subseteq \mathrm{GRS}_{n-r}(\mathbf{a}, \mathbf{c})$$

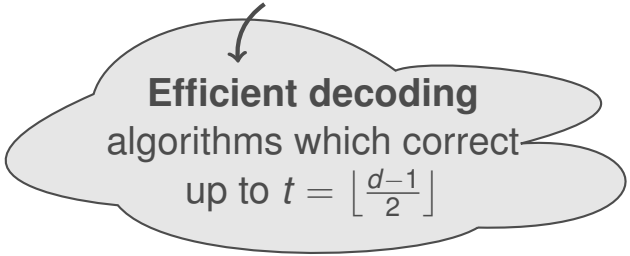
Decoding Alternant codes

$$\mathrm{Alt}_r(\mathbf{a}, \mathbf{b}) \subseteq \mathrm{GRS}_{n-r}(\mathbf{a}, \mathbf{c})$$

Efficient decoding algorithms which correct up to $t = \left\lfloor \frac{d-1}{2} \right\rfloor$

Decoding Alternant codes

$$\mathrm{Alt}_r(\mathbf{a}, \mathbf{b}) \subseteq \mathrm{GRS}_{n-r}(\mathbf{a}, \mathbf{c})$$



We have an efficient decoding algorithm for $\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})$ which corrects up to $\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{r}{2} \right\rfloor$

Goppa Codes

- $L = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}$ with $\alpha_i \neq \alpha_j$ for all $i \neq j$
- $g(X) \in \mathbb{F}_{q^m}[X]$ monic polynomial with

$$\deg(g) = t \quad \text{and} \quad g(\alpha_i) \neq 0 \ , \forall i$$

Goppa Codes

- $L = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}$ with $\alpha_i \neq \alpha_j$ for all $i \neq j$ $\Longrightarrow$ support
- $g(X) \in \mathbb{F}_{q^m}[X]$ monic polynomial with

$$\deg(g) = t \quad \text{and} \quad g(\alpha_i) \neq 0 \ , \forall i \qquad \Longrightarrow \text{ generator polynomial}$$

Goppa Codes

- $L = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}$ with $\alpha_i \neq \alpha_j$ for all $i \neq j$ $\Longrightarrow$ support
- $g(X) \in \mathbb{F}_{q^m}[X]$ monic polynomial with

$$\deg(g) = t \quad \text{and} \quad g(\alpha_i) \neq 0\ , \forall i \qquad \Longrightarrow \text{ generator polynomial}$$

Goppa Code

$$\Gamma\left(L, g\right) = \mathrm{Alt}_t(\mathbf{a}, \mathbf{b}) = \left(\mathrm{GRS}_t(\mathbf{a}, \mathbf{b})\right)^{\perp} \cap \mathbb{F}_q$$

with $\mathbf{a} = L$ and $b_i = \frac{1}{g(a_i)}$

Goppa Codes

- $L = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}$ with $\alpha_i \neq \alpha_j$ for all $i \neq j$ $\Longrightarrow$ support
- $g(X) \in \mathbb{F}_{q^m}[X]$ monic polynomial with

$$\deg(g) = t \quad \text{and} \quad g(\alpha_i) \neq 0\ , \forall i \qquad \Longrightarrow \text{ generator polynomial}$$

Goppa Code

$$\Gamma\left(L, g\right) = \mathrm{Alt}_t(\mathbf{a}, \mathbf{b}) = \left(\mathrm{GRS}_t(\mathbf{a}, \mathbf{b})\right)^{\perp} \cap \mathbb{F}_q$$

with $\mathbf{a} = L$ and $b_i = \frac{1}{g(a_i)}$

Proposition: Alternative definition of Goppa codes

$$\mathbf{c} \in \Gamma\left(L, g\right) \iff R_{\mathbf{c}}(X) = \sum_{j=1}^{n} \frac{c_j}{X - \alpha_j} \equiv 0 \mod g(X)$$

Alternative Definition of Goppa Codes

$$\mathbf{c} \in \Gamma(L, g) \iff \sum_{i=1}^{n} c_i p_{i,j} = 0 \quad \text{for } j = 1, \ldots, t-1$$

with $p_{i,j}$ such that $p_i(X) = p_{i,0} + p_{i,1}X + \ldots + p_{i,t-1}X^{t-1} \equiv \dfrac{1}{X - \alpha_i} \mod g(X)$

Alternative Definition of Goppa Codes

$$\mathbf{c} \in \Gamma(L, g) \iff \sum_{i=1}^{n} c_i p_{i,j} = 0 \quad \text{for } j = 1, \ldots, t-1$$

with $p_{i,j}$ such that $p_i(X) = p_{i,0} + p_{i,1}X + \ldots + p_{i,t-1}X^{t-1} \equiv \dfrac{1}{X - \alpha_i} \mod g(X)$

Thus

$$H = \begin{pmatrix} p_{1,0} & \cdots & p_{n,0} \\ \vdots & \ddots & \vdots \\ p_{1,t-1} & \cdots & p_{n,t-1} \end{pmatrix} \in \mathbb{F}_q^{t \times n}$$ is a **parity-check matrix** for $\Gamma(L, g)$

Alternative Definition of Goppa Codes

$$\mathbf{c} \in \Gamma(L, g) \iff \sum_{i=1}^{n} c_i p_{i,j} = 0 \quad \text{for } j = 1, \ldots, t-1$$

We claim that

$$p_i(X) \equiv -\frac{g(X) - g(\alpha_i)}{X - \alpha_i} g(\alpha_i)^{-1} \mod g(X)$$

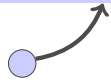
1. $g(X) - g(\alpha_j)$ has α_j as zero. So $g(X) - g(\alpha_j)$ is divisible by $X - \alpha_j$
2. $p_i(X)(X - \alpha_j) = -\left(g(X) - g(\alpha_j)\right) g(\alpha_j)^{-1} = 1 - g(X)g(\alpha_j)^{-1} \equiv 1 \mod g(X)$

Alternative Definition of Goppa Codes

Let $g(X) = g_0 + g_1 X + \ldots + g_t X^t$

$$p_i(X) \equiv -\frac{g(X) - g(\alpha_i)}{X - \alpha_i} g(\alpha_i)^{-1} \mod g(X)$$

Result from the previous slide



Alternative Definition of Goppa Codes

Let $g(X) = g_0 + g_1 X + \ldots + g_t X^t$

$$p_i(X) \equiv \sum_{j=1}^{t} -g_j \sum_{l=0}^{j-1} X^l \alpha_i^{j-1-l} g(\alpha_i)^{-1} \mod g(X)$$

$$X^j - \alpha_i^j \;\big|\; X - \alpha_i$$

$$X^{j-1} + \alpha_i X^{j-2} + \ldots + \alpha_i^{j-1}$$

Alternative Definition of Goppa Codes

Let $g(X) = g_0 + g_1 X + \ldots + g_t X^t$

$$p_i(X) \equiv \sum_{l=0}^{t-1} \left(\sum_{j=l+1}^{t} -g_j \alpha_i^{j-1-l} g(\alpha_i)^{-1} \right) X^l \mod g(X)$$

Rearrange the terms

Alternative Definition of Goppa Codes

Let $g(X) = g_0 + g_1 X + \ldots + g_t X^t$

$$p_i(X) \equiv \sum_{l=0}^{t-1} \left(\sum_{j=l+1}^{t} -g_j \alpha_i^{j-1-l} g(\alpha_i)^{-1} \right) X^l \mod g(X)$$

Thus we have the following expressions for $p_{i,j}$:

$$\begin{cases} p_{i,0} &= -(g_1 + g_2\alpha_i + \ldots + g_t\alpha_i^{t-1})g(\alpha_i)^{-}1 \\ p_{i,1} &= -(g_2 + g_3\alpha_i + \ldots + g_t\alpha_i^{t-2})g(\alpha_i)^{-}1 \\ \vdots &\vdots \quad \vdots \\ p_{i,t-1} &= -g_t g(\alpha_i)^{-1} \end{cases}$$

Alternative Definition of Goppa Codes

Let $g(X) = g_0 + g_1 X + \ldots + g_t X^t$

$$p_i(X) \equiv \sum_{l=0}^{t-1} \left(\sum_{j=l+1}^{t} -g_j \alpha_i^{j-1-l} g(\alpha_i)^{-1} \right) X^l \mod g(X)$$

We find that $H = CAB$ with

$$C = \begin{pmatrix} 0 & 0 & 0 & \cdots & -g_t \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & -g_t & \cdots & -g_3 \\ 0 & -g_t & -g_{t-1} & \cdots & -g_2 \\ -g_t & -g_{t-1} & -g_{t-2} & \cdots & -g_1 \end{pmatrix},$$

$$A = \begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & \ddots & \vdots \\ \alpha_1^{t-1} & \cdots & \alpha_n^{t-1} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} g(\alpha_1)^{-1} & & 0 \\ & \ddots & \\ 0 & & g(\alpha_n)^{-1} \end{pmatrix}$$

Alternative Definition of Goppa Codes

Since C is invertible

$$H = A \cdot B = \begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & \ddots & \vdots \\ \alpha_1^{t-1} & \cdots & \alpha_n^{t-1} \end{pmatrix} \begin{pmatrix} g(\alpha_1)^{-1} & & 0 \\ & \ddots & \\ 0 & & g(\alpha_n)^{-1} \end{pmatrix}$$

is another parity check matrix for $\Gamma(L, g)$

Binary Goppa Codes

- $L = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{2^m}$ with $\alpha_i \neq \alpha_j$ for all $i \neq j$
- $g(X) \in \mathbb{F}_{2^m}[X]$ monic **separable** polynomial with

$$\deg(g) = t \quad \text{and} \quad g(\alpha_i) \neq 0 \ , \forall i$$

Separable $=$ All its roots are distinct $=$ Square Free polynomial

Binary Goppa Codes

- $L = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{2^m}$ with $\alpha_i \neq \alpha_j$ for all $i \neq j$ $\Longrightarrow$ support
- $g(X) \in \mathbb{F}_{2^m}[X]$ monic **separable** polynomial with

$$\deg(g) = t \quad \text{and} \quad g(\alpha_i) \neq 0\ , \forall i \qquad \Longrightarrow \text{ generator polynomial}$$

$$\text{Separable} \quad = \quad \text{All its roots are distinct} \quad = \quad \text{Square Free polynomial}$$

Binary Goppa Codes

- $L = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{2^m}$ with $\alpha_i \neq \alpha_j$ for all $i \neq j$ $\Longrightarrow$ support
- $g(X) \in \mathbb{F}_{2^m}[X]$ monic **separable** polynomial with

$$\deg(g) = t \quad \text{and} \quad g(\alpha_i) \neq 0 \ , \forall i \qquad \Longrightarrow \text{ generator polynomial}$$

Proposition

The binary Goppa code $\Gamma(L, g)$ has minimum distance d with $d \geq 2t + 1$

Binary Goppa Codes

Proposition

Let g be a **square free Goppa** polynomial with coefficients in $\mathbb{F}_{2^m}$. Then,

$$\Gamma(L, g) = \Gamma(L, g^2)$$

Proof:

1. Since $g(X)$ divides $g^2(X)$ we have that $\Gamma(L, g^2) \subseteq \Gamma(L, g)$

2. Let $\mathbf{c} \in \Gamma(L, g)$ and define $f(X) = \prod_{i=1}^{n} (X - \alpha_i)^{c_i}$

   It is easy to check that $\dfrac{f'(X)}{f(X)} = \sum_{j=1}^{n} \dfrac{c_j}{X - \alpha_j} \equiv 0 \mod g(X)$

   Since $f(X)$ and $g(X)$ has no common factors then $g(X)$ divides $f'(X)$.
   Moreover, in $\mathbb{F}_{2^m}$ every derivative only have terms with binary exponents, i.e.

$$\begin{aligned} f'(X) &= f_0 + f_2 X^2 + \cdots + f_{2u} X^{2u} \\ &= (h_0 + h_1 X + h_u X^u)^2 \\ &= (h(X))^2 \text{ with } h_i^2 = f_i \text{ and } 2u \leq \deg(f'(X)) \end{aligned}$$

   Thus $g(X)$ divides $(h(X))^2$, but since $g(X)$ is square free, we have that $g(X)$ divides $h(X)$ or, equivalently, $g^2(X)$ divides $f'(X)$.
   And we can conclude that $\mathbf{c} \in \Gamma(L, g^2)$.

Binary Goppa Codes

Proposition

Let g be a **square free Goppa** polynomial with coefficients in $\mathbb{F}_{2^m}$. Then,

$$\mathrm{Alt}_r(L, \frac{1}{g(\alpha_i)}) = \Gamma(L, g) = \Gamma(L, g^2) = \mathrm{Alt}_{2r}(L, \frac{1}{g^2(\alpha_i)})$$

Proof:

1. Since $g(X)$ divides $g^2(X)$ we have that $\Gamma(L, g^2) \subseteq \Gamma(L, g)$

2. Let $\mathbf{c} \in \Gamma(L, g)$ and define $f(X) = \prod_{i=1}^{n} (X - \alpha_i)^{c_i}$

   It is easy to check that $\frac{f'(X)}{f(X)} = \sum_{j=1}^{n} \frac{c_j}{X - \alpha_j} \equiv 0 \mod g(X)$

   Since $f(X)$ and $g(X)$ has no common factors then $g(X)$ divides $f'(X)$.
   Moreover, in $\mathbb{F}_{2^m}$ every derivative only have terms with binary exponents, i.e.

$$\begin{aligned} f'(X) &= f_0 + f_2 X^2 + \cdots + f_{2u} X^{2u} \\ &= (h_0 + h_1 X + h_u X^u)^2 \\ &= (h(X))^2 \text{ with } h_i^2 = f_i \text{ and } 2u \leq \deg(f'(X)) \end{aligned}$$

   Thus $g(X)$ divides $(h(X))^2$, but since $g(X)$ is square free, we have that $g(X)$ divides $h(X)$ or, equivalently, $g^2(X)$ divides $f'(X)$.
   And we can conclude that $\mathbf{c} \in \Gamma(L, g^2)$.

Binary Goppa Codes

Proposition

Let g be a **square free Goppa** polynomial with coefficients in $\mathbb{F}_{2^m}$.
Then, the binary Goppa code $\Gamma(L, g)$ has minimum distance d with $d \geq 2t + 1$

Proof:
This Proposition is a consequence of the previous result:

$$\Gamma(L, g) = \Gamma(L, g^2)$$

- The lower bound on the dimension uses that $g(X)$ has degree r
- The lower bound on the minimum distance uses that $g^2(X)$ has degree $2r$

1. Error-Correcting Codes and Cryptography

1. Introduction I - Cryptography
2. Introduction II - Coding Theory
3. Encoding (Linear Transformation)
4. Parity Checking
5. Error Correcting Capacity
6. Decoding (A Difficult Problem)
7. Reed-Solomon Codes
8. Goppa Codes
9. **McEliece Cryptosystem**