Goppa Code in Classic McEliece

Elena Kirshanova

Seminar at RUB
September 20, 2021

Outline

I. Goppa Code: definition, encoding, decoding

II. Goppa Code in Classic McEliece

Part I

Goppa Code

Goppa Code: definition

Fix the following parameters:

- $m \geq 1$, prime $q \geq 2$ define $\mathbb{F}_{q^m}$
- $L = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_{q^m}$, α_i are distinct, $n \leq q^m$
- $g(x) \in \mathbb{F}_{q^m}[x]$, $\deg g(x) \leq t$ s.t. $g(\alpha_i) \neq 0 \; \forall i$.

Goppa Code: definition

Fix the following parameters:

- $m \geq 1$, prime $q \geq 2$ define $\mathbb{F}_{q^m}$
- $L = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_{q^m}$, α_i are distinct, $n \leq q^m$
- $g(x) \in \mathbb{F}_{q^m}[x]$, $\deg g(x) \leq t$ s.t. $g(\alpha_i) \neq 0 \; \forall i$.

Goppa Code C of length n is

$$C = \Gamma(L, g) = \left\{ c \in \mathbb{F}_q^n \; : \; \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} = 0 \bmod g(x) \right\}$$

Easy to check: $\frac{1}{x-\alpha_i} = -\frac{g(x)-g(\alpha_i)}{x-\alpha_i} g^{-1}(\alpha_i) \bmod g(x)$.

Goppa Code: definition

Fix the following parameters:

- $m \geq 1$, prime $q \geq 2$ define $\mathbb{F}_{q^m}$
- $L = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_{q^m}$, α_i are distinct, $n \leq q^m$
- $g(x) \in \mathbb{F}_{q^m}[x]$, $\deg g(x) \leq t$ s.t. $g(\alpha_i) \neq 0 \; \forall i$.

Goppa Code C of length n is

$$C = \Gamma(L, g) = \left\{ c \in \mathbb{F}_q^n \; : \; \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} = 0 \bmod g(x) \right\}$$

Easy to check: $\frac{1}{x-\alpha_i} = -\frac{g(x)-g(\alpha_i)}{x-\alpha_i} g^{-1}(\alpha_i) \bmod g(x)$.

In Classic McEliece, $q = 2$ and $g(x)$ is monic, irreducible.

Goppa Code: parity-check matrix

Write $g(x) = \sum_{i=0}^{t} g_i x^i$, $g_i \in \mathbb{F}_{q^m}$, look at $\frac{g(x)-g(\alpha_i)}{x-\alpha_i} =$

Goppa Code: parity-check matrix

Write $g(x) = \sum_{i=0}^{t} g_i x^i$, $g_i \in \mathbb{F}_{q^m}$, look at $\frac{g(x)-g(\alpha_i)}{x-\alpha_i} =$

$$\frac{g_t(x^t - \alpha_i^t) + \ldots + g_1(x - \alpha_i) + g_0 \cdot 0}{x - \alpha_i} =$$

Goppa Code: parity-check matrix

Write $g(x) = \sum_{i=0}^{t} g_i x^i$, $g_i \in \mathbb{F}_{q^m}$, look at $\frac{g(x)-g(\alpha_i)}{x-\alpha_i} =$

$$\frac{g_t(x^t - \alpha_i^t) + \ldots + g_1(x - \alpha_i) + g_0 \cdot 0}{x - \alpha_i} =$$

$$g_t \cdot (x^{t-1} + \alpha_i x^{t-2} + \ldots + \alpha_i^{t-1}) + \ldots + g_2 \cdot (x + \alpha_i) + g_1.$$

Look at the coeffs of a codeword $\sum c_i \frac{g(x)-g(\alpha_i)}{x-\alpha_i} g^{-1}(\alpha_i)$.

Goppa Code: parity-check matrix

Write $g(x) = \sum_{i=0}^{t} g_i x^i$, $g_i \in \mathbb{F}_{q^m}$, look at $\frac{g(x)-g(\alpha_i)}{x-\alpha_i} =$

$$\frac{g_t(x^t - \alpha_i^t) + \ldots + g_1(x - \alpha_i) + g_0 \cdot 0}{x - \alpha_i} =$$

$$g_t \cdot (x^{t-1} + \alpha_i x^{t-2} + \ldots + \alpha_i^{t-1}) + \ldots + g_2 \cdot (x + \alpha_i) + g_1.$$

Look at the coeffs of a codeword $\sum c_i \frac{g(x)-g(\alpha_i)}{x-\alpha_i} g^{-1}(\alpha_i)$.

x^{t-1} : $\quad g_t \cdot g^{-1}(\alpha_1)c_1 + \ldots + g_t \cdot g^{-1}(\alpha_n)c_n$

Goppa Code: parity-check matrix

Write $g(x) = \sum_{i=0}^{t} g_i x^i$, $g_i \in \mathbb{F}_{q^m}$, look at $\frac{g(x)-g(\alpha_i)}{x-\alpha_i} =$

$$\frac{g_t(x^t - \alpha_i^t) + \ldots + g_1(x-\alpha_i) + g_0 \cdot 0}{x-\alpha_i} =$$

$$g_t \cdot (x^{t-1} + \alpha_i x^{t-2} + \ldots + \alpha_i^{t-1}) + \ldots + g_2 \cdot (x + \alpha_i) + g_1.$$

Look at the coeffs of a codeword $\sum c_i \frac{g(x)-g(\alpha_i)}{x-\alpha_i} g^{-1}(\alpha_i)$.

$$\begin{aligned}
x^{t-1}: &\quad g_t \cdot g^{-1}(\alpha_1)c_1 + \ldots + g_t \cdot g^{-1}(\alpha_n)c_n \\
x^{t-2}: &\quad (g_{t-1} + \alpha_1 g_t) \cdot g^{-1}(\alpha_1)c_1 + \ldots + (g_{t-1} + \alpha_1 g_t) \cdot g^{-1}(\alpha_n)c_n \\
&\quad \vdots \\
x^0: &\quad (g_1 + \ldots + g_t\alpha^{t-1})g^{-1}(\alpha_1)c_1 + \ldots + (g_1 + \ldots + g_t\alpha^{t-1})g^{-1}(\alpha_n)c_n
\end{aligned}$$

Goppa Code: parity-check matrix

$c \in \Gamma(L, g) \iff$ all coeffs of x^j are $0 \iff \overline{H}c = 0$ for $\overline{H} \in \mathbb{F}_{q^m}^{t \times n}$

$$\overline{H} = \begin{pmatrix} g_t \cdot g^{-1}(\alpha_1) & \dots & g_t \cdot g^{-1}(\alpha_n) \\ (g_{t-1} + \alpha_1 g_t) \cdot g^{-1} & \dots & (g_{t-1} + \alpha_1 g_t) \cdot g^{-1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ (g_1 + \ldots + g_t \alpha^{t-1}) g^{-1}(\alpha_1) & \dots & (g_1 + \ldots + g_t \alpha^{t-1}) g^{-1}(\alpha_1) \end{pmatrix} =$$

Goppa Code: parity-check matrix

$c \in \Gamma(L, g) \iff$ all coeffs of x^j are $0 \iff \overline{H}c = 0$ for $\overline{H} \in \mathbb{F}_{q^m}^{t \times n}$

$$\overline{H} = \begin{pmatrix} g_t \cdot g^{-1}(\alpha_1) & \dots & g_t \cdot g^{-1}(\alpha_n) \\ (g_{t-1} + \alpha_1 g_t) \cdot g^{-1} & \dots & (g_{t-1} + \alpha_1 g_t) \cdot g^{-1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ (g_1 + \ldots + g_t \alpha^{t-1}) g^{-1}(\alpha_1) & \dots & (g_1 + \ldots + g_t \alpha^{t-1}) g^{-1}(\alpha_1) \end{pmatrix} =$$

$$\underbrace{\begin{pmatrix} g_t & 0 & \dots & 0 \\ g_{t-1} & g_t & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & \dots & g_t \end{pmatrix}}_{G} \cdot \underbrace{\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{t-1} & \alpha_2^{t-1} & \dots & \alpha_n^{t-1} \end{pmatrix}}_{X} \cdot \underbrace{\begin{pmatrix} g^{-1}(\alpha_1) & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & g^{-1}(\alpha_n) \end{pmatrix}}_{Y}$$

Goppa Code: parity-check matrix

$c \in \Gamma(L, g) \iff$ all coeffs of x^j are $0 \iff \overline{H}c = 0$ for $\overline{H} \in \mathbb{F}_{q^m}^{t \times n}$

$$\overline{H} = \begin{pmatrix} g_t \cdot g^{-1}(\alpha_1) & \dots & g_t \cdot g^{-1}(\alpha_n) \\ (g_{t-1} + \alpha_1 g_t) \cdot g^{-1} & \dots & (g_{t-1} + \alpha_1 g_t) \cdot g^{-1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ (g_1 + \ldots + g_t \alpha^{t-1}) g^{-1}(\alpha_1) & \dots & (g_1 + \ldots + g_t \alpha^{t-1}) g^{-1}(\alpha_1) \end{pmatrix} =$$

$$\underbrace{\begin{pmatrix} g_t & 0 & \dots & 0 \\ g_{t-1} & g_t & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & \dots & g_t \end{pmatrix}}_{G} \cdot \underbrace{\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{t-1} & \alpha_2^{t-1} & \dots & \alpha_n^{t-1} \end{pmatrix}}_{X} \cdot \underbrace{\begin{pmatrix} g^{-1}(\alpha_1) & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & g^{-1}(\alpha_n) \end{pmatrix}}_{Y}$$

G is invertible, $H = G^{-1}\overline{H} = \begin{pmatrix} g^{-1}(\alpha_1) & \dots & g^{-1}(\alpha_n) \\ \alpha_1 g^{-1}(\alpha_1) & \dots & \alpha_n g^{-1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ \alpha_1^{t-1} g^{-1}(\alpha_1) & \dots & \alpha_n^{t-1} g^{-1}(\alpha_n) \end{pmatrix}$

Goppa Code: parity-check matrix

$$H = \begin{pmatrix} g^{-1}(\alpha_1) & \dots & g^{-1}(\alpha_n) \\ \alpha_1 g^{-1}(\alpha_1) & \dots & \alpha_n g^{-1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ \alpha_1^{t-1} g^{-1}(\alpha_1) & \dots & \alpha_n^{t-1} g^{-1}(\alpha_n) \end{pmatrix} \in \mathbb{F}_{q^m}^{t \times n}$$

Obtain a matrix over $\mathbb{F}_q^{tm \times n}$ by considering a natural bijection $\mathbb{F}_{q^m}^{t \times n} \to \mathbb{F}_q^{tm \times n}$ using a fixed basis.

Example

- $q = 2$, $m = 3$, $\mathbb{F}_{q^m} = \mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3 + x + 1)$.
- $g(x) = x^2 + x + 1$ - irred. in $\mathbb{F}_2$, has roots in $GF(2^2), GF(2^4)$ but not in $GF(2^3)$.
- Take $L = \mathbb{F}_{2^3} = \{0, 1, \alpha, \alpha^2, \alpha+1, \alpha^2+\alpha, \alpha^2+\alpha+1, \alpha^2+1\}$, where $\alpha^3 + \alpha + 1 = 0$.

Example

- $q = 2$, $m = 3$, $\mathbb{F}_{q^m} = \mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3 + x + 1)$.
- $g(x) = x^2 + x + 1$ - irred. in $\mathbb{F}_2$, has roots in $GF(2^2), GF(2^4)$ but not in $GF(2^3)$.
- Take $L = \mathbb{F}_{2^3} = \{0, 1, \alpha, \alpha^2, \alpha+1, \alpha^2+\alpha, \alpha^2+\alpha+1, \alpha^2+1\}$, where $\alpha^3 + \alpha + 1 = 0$.

$$\overline{H} = \begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^2 \end{pmatrix} \quad \text{over } \mathbb{F}_{2^3}$$

$$H = \left(\begin{array}{cccccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ \hline & & & & & & & \\ & & & & & & & \\ & & & & & & & \end{array}\right.$$

Example

- $q = 2$, $m = 3$, $\mathbb{F}_{q^m} = \mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3 + x + 1)$.
- $g(x) = x^2 + x + 1$ - irred. in $\mathbb{F}_2$, has roots in $GF(2^2), GF(2^4)$ but not in $GF(2^3)$.
- Take $L = \mathbb{F}_{2^3} = \{0, 1, \alpha, \alpha^2, \alpha+1, \alpha^2+\alpha, \alpha^2+\alpha+1, \alpha^2+1\}$, where $\alpha^3 + \alpha + 1 = 0$.

$$\overline{H} = \begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^2 \end{pmatrix} \quad \text{over } \mathbb{F}_{2^3}$$

$$H = \left(\begin{array}{cccccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right) \quad \text{over } \mathbb{F}_2$$

Decoding Goppa codes

- Minimal distance of $\Gamma(L, g)$ is $d \geq t + 1$.

  For $q = 2$ and g – separable, $d \geq 2t + 1$ (exercise)

- $y = (y_1, \ldots, y_n) = (c_1, \ldots c_n) + (e_1, \ldots, e_n)$ – received word, $\omega(e) \leq \lfloor \frac{d-1}{2} \rfloor$.

  $\mathcal{B} = \{i \mid e_i \neq 0\}$ – error-positions, $|\mathcal{B}| = \omega(e)$

Decoding Goppa codes

- $s(x) = \sum_i \frac{y_i}{x-\alpha_i} = \sum_i \frac{e_i}{x-\alpha_i} \bmod g(x)$ – syndrome of y.
- Two helping polynomials:

$$\sigma(x) = \prod_{i \in \mathcal{B}} (x - \alpha_i) - \text{ error locator polynomial}$$

$$w(x) = \sum_{i \in \mathcal{B}} e_i \prod_{j \in \mathcal{B}, j \neq i} (x - \alpha_j)$$

- Facts:

$$(1) \quad e_k = \frac{w(\alpha_k)}{\sigma'(\alpha_k)} \; \forall \, k \in \mathcal{B}$$

$$(2) \quad \sigma(x)s(x) = w(x) \bmod g(x)$$

- $\deg \sigma(x) = |\mathcal{B}| = \omega(e)$, $\deg w(x) = \omega(e) - 1$
- We have $\deg g = t$ equations, $2\omega(e) - 1$ unknowns.
  Since $\omega(e) < (t-1)/2$, we can determine e_k's.

Part II

Goppa Code in Classic McEliece

according to the 3rd round submission
`https://classic.mceliece.org/nist/mceliece-20201010.pdf`

Keys in Classic McEliece

- sk $= g, (\alpha_1, \ldots, \alpha_n)$ – a compact description of Goppa code
- pk $= (\mathbf{I}_{tm}|T) \in \mathbb{F}_2^{tm \times n}$ – systematic form of H– a parity-check matrix of the code
- there are parameter sets which use a 'semi-systematic' form of H

Assumption: pk is indistinguishable from a random binary matrix.

Also implicitely: pk is useless in making decoding efficient

Key recovery attacks

- Attack: "Support splitting algorithm"[1]
- the attack is based on finding permutation equivalent code
- main idea: enumerate (almost) all irred. g, asymptotic cost $\approx 2^{mt}$. This is much more costly than ISD

[1] N. Sendrier. Finding the permutation between equivalent codes: the support splitting algorithm, 2020
P. Loidreau, N. Sendrier Weak keys in the McEliece public-key cryptosystem

Other security considerations[3]

- McEliece/Niederreiter key pair is often described as

$$\text{sk} = H \text{ (structured)} \qquad \text{pk} = M \cdot H \cdot P,$$

  P -permutation matrix, M - random non-singular.

- As described in Classic McEliece, $P = \mathbf{I}_n$.

---

[2] V. M. Sidelnikov, S. O. Shestakov, On insecurity of cryptosystems based on generalized Reed-Solomon codes

[3] based on D. Engelbert, R. Overbeck, and A. Schmidt. A Summary of McEliece-Type Cryptosystems and their Security

Other security considerations[3]

- McEliece/Niederreiter key pair is often described as

$$\text{sk} = H \text{ (structured)} \quad \text{pk} = M \cdot H \cdot P,$$

  P -permutation matrix, M - random non-singular.

- As described in Classic McEliece, $P = \mathbf{I}_n$.
- There is an attack that given $\{\alpha_i\}_i$, and P, recovers g. (Use decoding equation for several codewords: for c s.t. $HP^{-1}c = 0$, $s_c(x) = 0 \bmod g(x)$
- There is an attack that given $\{\alpha_i\}_i$, and M, recovers g. Interpret $M^{-1}pk$ as a matrix over $\mathbb{F}_{q^m}$, apply Sidelnikov-Shestakov.[2]
- In Classic McEliece $\{\alpha_i\}_i$ are secret.

---

[2] V. M. Sidelnikov, S. O. Shestakov, On insecurity of cryptosystems based on generalized Reed-Solomon codes

[3] based on D. Engelbert, R. Overbeck, and A. Schmidt. A Summary of McEliece-Type Cryptosystems and their Security