Some Facts about Binary Goppa Codes

Indocrypt 2009 tutorial

Nicolas Sendrier

INRIA

December 13, 2009, New Delhi, India

Irreducible Binary Goppa Codes

Parameters: m, t and $n \leq 2^m$

$$\text{Let} \begin{cases} L = (\alpha_1, \ldots, \alpha_n) \text{ distinct in } \mathbf{F}_{2^m} \\ g(z) \in \mathbf{F}_{2^m}[z] \text{ monic irreducible of degree } t \end{cases}$$

The binary irreducible Goppa code $\Gamma(L, g)$ of *support* L and *generator* $g(z)$ is defined as the following subspace of $\{0, 1\}^n$

$$a = (a_1, \ldots, a_n) \in \Gamma(L, g) \Leftrightarrow R_a(z) = \sum_{j=1}^{n} \frac{a_i}{z - \alpha_j} = 0 \bmod g(z)$$

- the dimension of $\Gamma(L, g)$ is $k \geq n - tm$
- the minimum distance of $\Gamma(L, g)$ is $d \geq 2t + 1$
- there exists a t-bounded polynomial time decoder for $\Gamma(L, g)$

Alternative Definition of Binary Goppa Codes

We have

$$\Gamma(L,g) = \{a \in \{0,1\}^n \mid aH^T = 0\}$$

where

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

Properties of Binary Goppa Codes

For all $b = (b_1, \ldots, b_n) \in \{0, 1\}^n$, its locator polynomial is defined as

$$\sigma_b(z) = \prod_{j=1}^{n} (z - \alpha_j)^{b_j}$$

(we denote $\sigma'_b(z)$ its derivative) and its syndrome is defined as

$$R_b(z) = \sum_{j=1}^{n} \frac{b_j}{z - \alpha_j}$$

Proposition 1 For all $b \in \{0, 1\}^n$, we have $R_b(z)\sigma_b(z) = \sigma'_b(z)$

Proposition 2 $a \in \Gamma(L, g) \Leftrightarrow g(z) \mid \sigma'_a(z)$

Proof: $a \in \Gamma(L, g) \Leftrightarrow R_a(z) = 0 \bmod g(z) \Leftrightarrow \sigma'_a(z) = 0 \bmod g(z) \Leftrightarrow g(z) \mid \sigma'_a(z)$

Main Parameters of Goppa Codes

Dimension: $k \geq n - mt$

there are t parity check equations with coefficients in $\mathbf{F}_{2^m}$, thus at most mt independent parity check equations with binary coefficients $\rightarrow$ the codimension is at most mt

Minimum distance: $\mathrm{dmin}(\Gamma(L,g)) \geq 2t+1$

$\Gamma(L,g)$ is an alternant code of designed distance $t+1$

$$a \in \Gamma(L,g) \Leftrightarrow g(z) \mid \sigma_a'(z) \Leftrightarrow g(z)^2 \mid \sigma_a'(z) \Leftrightarrow a \in \Gamma(L,g^2)$$

because in charateristic 2 the derivative $\sigma_a'(z)$ is a square

This implies that $\Gamma(L,g) = \Gamma(L,g^2)$ is an alternant code of designed distance $2t+1$. Its minimum distance is thus $\geq 2t+1$

Decoding Binary Goppa Codes

Let $b = a + e \in \{0, 1\}^n$ be the received word with $a \in \Gamma(L, g)$ and $\mathrm{wt}(e) \leq t$

We have $R_b(z) = R_a(z) + R_e(z) = R_e(z) \bmod g(z)^2$ and thus

$$R_e(z)\sigma_e(z) = \sigma_e'(z) \bmod g(z)^2$$

This key equation can be solved with the extended Euclidean algorithm and provides the locator polynomial $\sigma_e(z)$ of the error

After computing the roots of $\sigma_e(z)$ we obtain the error e and the codeword a

Decoding Complexity

Counting the operations in the field $\mathbf{F}_{2^m}$, we get

1. Computing the syndrome $R_b(z)$ $\rightarrow O(nt)$
2. Solving the key equation $\rightarrow O(t^2)$
3. Computing the roots of the locator polynomial $\rightarrow O(mt^2)$

Step 3 uses the Berlekamp trace algorithm

In practice, for sizes used in cryptosystems, the Step 3 is the most expensive

Berlekamp Trace Algorithm

Problem: Find the roots of $\sigma(z) \in \mathbf{F}_{2^m}[z]$ assuming $\sigma(z) \mid z + z^{2^m}$

Trace polynomial ($\mathrm{Tr}(\cdot)$ is the trace in $\mathbf{F}_{2^m}$ over $\mathbf{F}_2$):

$$T(z) = z + z^2 + z^4 + \cdots + z^{2^{m-1}} = \prod_{\mathrm{Tr}(\gamma)=0} (z - \gamma)$$

$$1 + T(z) = \prod_{\mathrm{Tr}(\gamma)=1} (z - \gamma) \text{ and } T(z)(T(z) + 1) = z + z^{2^m}$$

We compute $\begin{cases} \sigma_0(z) = \mathrm{gcd}(\sigma(z), T(z)) \\ \sigma_1(z) = \mathrm{gcd}(\sigma(z), T(z) + 1) = \sigma(z)/\sigma_0(z) \end{cases}$

We can repeat this recursively with $T(\beta z)$ instead of $T(z)$ with some $\beta \in \mathbf{F}_{2^m}$, hopefully splitting the polynomials again

Doing this with $T(\beta z)$ when $\beta \in \{\beta_0, \ldots, \beta_{m-1}\}$ runs through a basis of $\mathbf{F}_{2^m}$ over $\mathbf{F}_2$ will separate all the roots of (z)

and here lives the dragons. . .