

About the n th-root codes: a Gröbner bases approach to the weight computation

Marta Giorgetti

Department of Mathematics, University of Milan, Italy
mail: giorgetti@mat.unimi.it

Linz, May 2006

Special semester in Gröbner basis, Cryptography,
Coding theory and Algebraic Combinatorics.

This is work in progress contained in my Ph.D. thesis,
supervised by F. Dalla Volta and M. Sala.

Definition 1 (nth-root codes). Let

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

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

$$H = \begin{pmatrix} g_1(L) \\ g_2(L) \\ \vdots \\ g_r(L) \end{pmatrix}$$

is its parity-check matrix, where $g_t(L) = (g_t(l_1), \dots, g_t(l_N))$.

Definition 2. Being $C = \Omega(q, n, q^m, L, \mathcal{P})$ an n th-root code, we say that C is **zerofree** if $0 \notin L$.

Definition 3. Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an n th-root code, $\omega \in \mathbb{N}$ such that $1 \leq \omega \leq N = |L|$, $\bar{L} = R_n \setminus \{L \cup \{0\}\}$. Then we define the following two ideals:

- $\mathbf{J}_w = J_w(C) = J_w(q, n, q^m, L, \mathcal{P}) \subset \mathbb{F}_{q^n}[z_1, \dots, z_w, y_1, \dots, y_w]$,

$$J_w(C) = \left\langle \sum_{k=1}^w y_k g_t(z_k), y_j^{q-1} - 1, p_{ij}(z_i, z_j), \frac{z_j^n - 1}{\prod_{l \in \bar{L}}(z_j - \alpha^l)} \right\rangle;$$

- $\hat{\mathbf{J}}_w = \hat{J}_w(C) = \hat{J}_w(q, n, q^m, L, \mathcal{P}) \subset \mathbb{F}_{q^n}[z_1, \dots, z_w, y_1, \dots, y_w, \mu]$,

$$\hat{J}_w(C) = \left\langle \sum_{k=1}^w y_k g_t(z_k) + \mu g_t(0), y_j^{q-1} - 1, \mu^{q-1} - 1, p_{ij}(z_i, z_j), \frac{z_j^n - 1}{\prod_{l \in \bar{L}}(z_j - \alpha^l)} \right\rangle$$

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 polynomials in $\mathbb{F}_q[z_i, z_j]$, $i, j = 1, \dots, w$ and $t = 1, \dots, r$.

Moreover $\eta(J_w)$ and $\hat{\eta}(\hat{J}_w)$ are the number of solutions of J_w and \hat{J}_w , respectively.

Theorem 1. Let $C = \Omega(q, n, q^m, L, \mathcal{P})$ be an n th-root code, then the number of codewords of weight w are exactly

$$A_w(C) = \frac{\eta(J_w)}{w!}$$

in the zerofree case and

$$A_w(C) = \frac{\hat{\eta}(\hat{J}_{w-1})}{(w-1)!} + \frac{\eta(J_w)}{w!}$$

in the non-zerofree case.

Example 1. Classical Goppa code.

- $g(x) = x^2 + x + 1$ the Goppa polynomial irreducible over \mathbb{F}_{2^3}
- L a set of elements which are not roots of $g(x)$, e.g.

$$L = \mathbb{F}_{2^3} = \{\alpha_i, i = 1, \dots, 8\}.$$

Hence $\Gamma = \Gamma(L, g)$ is the binary classical Goppa code generated by $g(x)$ having the following parity check matrix

$$H = \begin{pmatrix} \frac{1}{g(\alpha_1)} & \frac{1}{g(\alpha_2)} & \frac{1}{g(\alpha_3)} & \frac{1}{g(\alpha_4)} & \frac{1}{g(\alpha_5)} & \frac{1}{g(\alpha_6)} & \frac{1}{g(\alpha_7)} & \frac{1}{g(\alpha_8)} \\ \frac{\alpha_1}{g(\alpha_1)} & \frac{\alpha_2}{g(\alpha_2)} & \frac{\alpha_3}{g(\alpha_3)} & \frac{\alpha_4}{g(\alpha_4)} & \frac{\alpha_5}{g(\alpha_5)} & \frac{\alpha_6}{g(\alpha_6)} & \frac{\alpha_7}{g(\alpha_7)} & \frac{\alpha_8}{g(\alpha_8)} \end{pmatrix}$$

Since $q = 2$, $m = 3$, $n = q^m - 1 = 7$, $L = \mathbb{F}_{2^3}$ and $\mathcal{P} = \left\{ \frac{1}{g(x)}, \frac{x}{g(x)} \right\}$, therefore Γ is an n th-root code, i.e.

$$\Gamma = \Omega \left(2, 7, 2^3, \mathbb{F}_8, \left\{ \frac{1}{g(x)}, \frac{x}{g(x)} \right\} \right).$$

We obtain with Singular that

w	Gröbner basis for $J_w(\Gamma)$	Gröbner basis for $\hat{J}_{w-1}(\Gamma)$
1,2,3,4	{1}	{1}
5	{1}	$\mathcal{G}(\hat{J}_4) \neq \{1\}$

Since $\mathcal{G}(J_5) = \{1\}$ every 5-weight word in this Goppa code has the first component equal to zero. The ideal \hat{J}_4 is

$$\hat{J}_4 = \begin{cases} g(z_2)g(z_3)g(z_4)g(0) + g(z_1)g(z_3)g(z_4)g(0) + \\ g(z_1)g(z_2)g(z_4)g(0) + g(z_1)g(z_2)g(z_3)g(0) + \\ g(z_1)g(z_2)g(z_3)g(z_4), \\ z_1g(z_2)g(z_3)g(z_4)g(0) + z_2g(z_1)g(z_3)g(z_4)g(0) + \\ z_3g(z_1)g(z_2)g(z_4)g(0) + z_4g(z_1)g(z_2)g(z_3)g(0), \\ z_i^7 + 1, i = 1, 2, 3, 4 \\ p_{1,2}(z_1, z_2), p_{1,3}(z_1, z_3), p_{1,4}(z_1, z_4), \\ p_{2,3}(z_2, z_3), p_{2,4}(z_2, z_4), p_{3,4}(z_3, z_4). \end{cases}$$

There are no polynomials $y_j^{q-1} - 1, \mu^{q-1} - 1$, because the code is binary, i.e. $y_j, \mu \in \{0, 1\}$.

The leading terms of $\mathcal{G}(\hat{J}_4)$ are:

$$\begin{aligned} \text{lt}(\hat{J}_4[1]) &= z_1 z_2, & \text{lt}(\hat{J}_4[2]) &= z_1^2, & \text{lt}(\hat{J}_4[3]) &= z_1 z_3^2, \\ \text{lt}(\hat{J}_4[4]) &= z_2^3, & \text{lt}(\hat{J}_4[5]) &= z_1 z_4^3, & \text{lt}(\hat{J}_4[6]) &= z_3^4, \\ \text{lt}(\hat{J}_4[7]) &= z_2^2 z_3^2, & \text{lt}(\hat{J}_4[8]) &= z_4^5, & \text{lt}(\hat{J}_4[9]) &= z_2^2 z_4^3, \\ \text{lt}(\hat{J}_4[10]) &= z_3^3 z_4^3. \end{aligned}$$

From the leading terms of $\mathcal{G}(\hat{J}_4)$ we compute the number $\hat{\eta}_4$ of system solutions and then, by Theorem 1, the number of 5-weight words:

$$A_5 = \frac{\eta_5}{5!} + \frac{\hat{\eta}_4}{4!}.$$

Being $\eta_5 = 0$ and $\hat{\eta}_4 = 48$ the number of 5-weight words in Γ is $\frac{48}{4!} = 2$.