On the binary quasi-cyclic codes

Stefka Bouyuklieva and Iliya Bouyukliev
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences

Outline

- Irreducible Cyclic Codes.
- Quasi-Cyclic Codes - a Module Description.
- Irreducible Quasi-Cyclic Codes - a Trace Description.
- Circulants.
- Quasi-Cyclic Codes - equivalences.

Irreducible Cyclic Codes

Definition 1 *Let $f(x)$ be an irreducible divisor of $x^n - 1$ over $\mathbb{F}_q$, $(q,n) = 1$. The cyclic code of length n over $\mathbb{F}_q$ generated by $g(x) = (x^n - 1)/f(x)$ is called an irreducible (or a minimal) cyclic code.*

Definition 2 *Let n be a divisor of $q^s - 1$ and let γ be a primitive n-th root of unity in $\mathbb{F}_{q^s}$. Then*

$$C(q,s,m) = C_\gamma = \{(\mathrm{Tr}_s(\xi), \mathrm{Tr}_s(\xi\gamma), \ldots, \mathrm{Tr}_s(\xi\gamma^{n-1})) | \xi \in \mathbb{F}_{q^s}\}$$

is called an irreducible cyclic code over $\mathbb{F}_q$ ($m = (q^s - 1)/n$).

$$C(q,s,m) = C_\gamma = C(\langle\gamma\rangle)$$

Irreducible Cyclic Codes

Theorem 1 *The irreducible cyclic* $[n,k]$ *code is isomorphic to the field* $GF(q^k)$.

Example: $n = 7$, $q = 2$, $k = 3$, $h(x) = x^3 + x + 1$

$e(x) = x^6 + x^5 + x^3 + 1$ is the generating idempotent of C, and

$$C = \{0, e(x), xe(x), x^2e(x), \ldots, x^6e(x)\}$$

This is the binary [7,3,4] simplex code with the only nonzero weight 4.

Irreducible Cyclic Codes

Example: $n = 7, q = 2, k = 3, h(x) = x^3 + x + 1, \gamma = x$

$$C \setminus \{0\} \rightarrow \begin{pmatrix} Tr(1) & Tr(\gamma) & \cdots & Tr(\gamma^6) \\ Tr(\gamma) & Tr(\gamma^2) & \cdots & Tr(1) \\ & & \vdots & \\ Tr(\gamma^6) & Tr(1) & \cdots & Tr(\gamma) \end{pmatrix}$$

If $\gamma = x$ then $1 \mapsto (100), \gamma \mapsto (010), \gamma^2 \mapsto (001)$

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} = (1\ \gamma\ \gamma^2\ \cdots\ \gamma^6)$$

Quasi-Cyclic Codes

Let T be the cyclic shift operator on $\mathbb{F}_q^n$. A *quasi-cyclic* (QC) code is a linear subspace of $\mathbb{F}_q^n$ invariant under T^s for some integer s.

A code is said to be quasi-cyclic if every cyclic shift of a codeword by s positions results in another codeword.

$\Rightarrow\ s \mid n\ \Rightarrow\ n = sm.$

The smallest such positive integer r is called the *index* of the code.

QC codes - a Module Description

Seguin, Drolet:

T - the cyclic shift operator on $\mathbb{F}_q^n$;
C - a QC code over $\mathbb{F}_q$ with index r (invariant under T^r)
$\Rightarrow C$ - A-module ($A = \mathbb{F}_q[x]$) via the multiplication
$a(x)v = a(T^r)v,\ v \in C,\ a(x) \in A$

C is an irreducible QC code if it is nontrivial and irreducible as an A-module

$ann(C) = \{a(x) \in A \mid a(x)v = 0,\ \forall v \in C\} \triangleleft A$
$\Rightarrow\ ann(C) = \langle \pi(x) \rangle$, $\pi(x)$ - order of C

QC codes - a Module Description

$ann(C) = \langle \pi(x) \rangle$, $\pi(x)$ - order of C

C is irreducible QC code $\Longleftrightarrow$ $C = Av$ for some $v \in C$ and the order $\pi(x)$ of C is irreducible.

$k = \dim(C) = \deg \pi(x)$

If $r = 1$ then $\pi(x)$ is the parity check polynomial of C

Let the order of u for $u \in \mathbb{F}_q^n$ be the order of the submodule $Au = \{a(x)u \mid a(x) \in A\}$

QC codes - a Module Description

$$e_i = (0,\ldots,0,1,0,\ldots,0) \Rightarrow \mathbb{F}_q^n = Ae_0 \oplus Ae_1 \oplus \cdots \oplus Ae_{r-1}$$

The order of e_i is $x^{n/r} - 1$

$$u \in \mathbb{F}_q^n \Rightarrow u = \sum_{i=0}^{r-1} a_i(x)e_i,\ ord(u) = lcm\{\frac{x^{n/r}-1}{(a_i(x), x^{n/r}-1)}\}$$

$ord(u)$ is irreducible $\iff$ $\frac{x^{n/r}-1}{(a_i(x),x^{n/r}-1)} = h(x)$ or 1

$\iff$ $(a_i(x), x^{n/r}-1) = \frac{x^{n/r}-1}{h(x)} = g(x)$ or $x^{n/r}-1$

$\iff$ $a_i(x) \pmod{x^{n/r}-1} \in \langle g(x) \rangle$, where $\langle g(x) \rangle$ is a cyclic code of length n/r, and $h(x)$ is irreducible

QC codes - a Trace Description

$$\Psi(\sum_{i=0}^{r-1} a_i(x)e_i) = (\overline{a_0(x)}, \overline{a_1(x)}, \ldots, \overline{a_{r-1}(x)})$$

where $\overline{a_i(x)} = a_i(x) \mod x^{n/r} - 1$.
Since $\langle g(x) \rangle$ is irreducible cyclic code, then

$$\langle g(x) \rangle = \{(\mathrm{Tr}(\alpha\beta^j))_0^{n/r-1} | \alpha \in \mathbb{F}_{q^k}\}$$

where $h(\beta^{-1}) = 0$.

$$\Rightarrow \Psi(Av) = \{(((\mathrm{Tr}(\alpha\gamma_0\beta^j))_0^{n/r-1}, \ldots, (\mathrm{Tr}(\alpha\gamma_{r-1}\beta^j))_0^{n/r-1}))\}$$

$$= C(\gamma_0, \gamma_1, \ldots, \gamma_{r-1})$$

QC codes - a Trace Description

Theorem 2 *Let C be a q-ary QC code of length n and index r. Then C is irreducible $\iff$ it is generated by a single element whose order is an irreducible polynomial $h(x)$, $h(x) \mid x^{n/r} - 1$. The dimension of C is $\deg h(x)$, and $\Psi(C) = C(\gamma_0, \gamma_1, \ldots, \gamma_{r-1})$. Conversely $C(\gamma_0, \gamma_1, \ldots, \gamma_{r-1})$ is an irreducible QC code whose index is a divisor of r.*

Quasi-Cyclic Codes and circulants

Circulants are basic components in a generator matrix for a QC code C.

A 1-generator QC code is generated by a matrix in the following form:

$$G = [G_0\ G_1\ \ldots\ G_{r-1}]$$

where G_i are circulants of order m.

If $g_0(x), g_1(x), \ldots, g_{r-1}(x)$ are the corresponding defining polynomials, then

$$k = \dim(C) = m - \deg(\gcd(g_0(x), g_1(x), \ldots, g_{r-1}(x)))$$

Piret's Construction

The main idea - combining irreducible cyclic codes.

$e(x)$ - the idempotent of an irreducible cyclic $[n,k]$ code,
$k = ord_n(2)$, $m = (2^k - 1)/n$,
γ - a primitive element of $GF(2^k)$, $\alpha = \gamma^m$.

$$\begin{aligned} \text{codeword} &\leftrightarrow \text{element of } GF(2^k) \\ e(x) &\leftrightarrow 1 \\ xe(x) &\leftrightarrow \alpha \\ \beta(x)e(x) &\leftrightarrow \gamma \\ \beta(x)^j e(x) &\leftrightarrow \gamma^j. \end{aligned}$$

Irreducible Cyclic Codes - our idea

Let $K = \mathbb{F}_{2^k}$, α - a primitive element,

$$\mathbb{F}_{2^k} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^k-2}\},$$

$2^k - 1 = mr$, $(m, r) = 1$, $\beta = \alpha^r$.
For $0 \leq a \leq r-1$ we define

$$C_a[i, j] = Tr(\alpha^{r(i+j)+ma}) = Tr(\alpha^{ma}\beta^{i+j})$$

$$D_a[i, j] = Tr(\alpha^{r(j-i)+a}) = Tr(\alpha^{a}\beta^{j-i})$$

Irreducible Cyclic Codes

The code whose nonzero codewords are the rows of the matrix

$$(C_0 \;\; C_1 \;\; \ldots \;\; C_{r-1})^T$$

is an irreducible cyclic code of length m and dimension $ord_m(q)$.

$$C_a = \begin{pmatrix} Tr(\alpha^{ma}) & Tr(\alpha^{ma}\beta) & \cdots & Tr(\alpha^{ma}\beta^{m-1}) \\ Tr(\alpha^{ma}\beta) & Tr(\alpha^{ma}\beta^2) & \cdots & Tr(\alpha^{ma}) \\ & & \ddots & \\ Tr(\alpha^{ma}\beta^{m-1}) & Tr(\alpha^{ma}) & \cdots & Tr(\alpha^{ma}\beta^{m-2}) \end{pmatrix}$$

QC codes - a trace description

The code whose nonzero weights are the rows of the matrix

$$\begin{pmatrix} C_0 & C_1 & \dots & C_{r-1} \\ C_1 & C_2 & \dots & C_0 \\ & & \vdots & \\ C_{r-1} & C_0 & \dots & C_{r-2} \end{pmatrix}$$

is the simplex $[2^k - 1 = mr, k]$ code.

QC codes - a trace description

Let $0 \leq a_1 < a_2 < \cdots < a_t \leq r-1$. The code whose nonzero weights are the rows of the matrix

$$C(a_1, a_2, \ldots, a_t) \longrightarrow \begin{pmatrix} C_{a_1} & C_{a_2} & \cdots & C_{a_t} \\ C_{a_1+1} & C_{a_2+1} & \cdots & C_{a_t+1} \\ & & \vdots & \\ C_{a_1+r-1} & C_{a_2+r-1} & \cdots & C_{a_t+r-1} \end{pmatrix}$$

is a QC code of length mt.

$$C(a_1, a_2, \ldots, a_t) = C(a_1+l, a_2+l, \ldots, a_t+l),\ 0 \leq l \leq r-1$$

$$C(2a_1, 2a_2, \ldots, 2a_t) \approx C(a_1, a_2, \ldots, a_t)$$

QC codes - equivalences

Theorem 3 *The following transformations send the code* $C(a_1, a_2, \ldots, a_t)$ *to an equivalent one:*

(i) *a permutation of the column-circulants:*
$C(a_1, a_2, \ldots, a_t) \approx C(a_{1\sigma}, a_{2\sigma}, \ldots, a_{t\sigma}), \sigma \in S_t$;

(ii) *a cyclic shift with* l *positions to each circulant:*
$C(a_1, a_2, \ldots, a_t) = C(a_1 + l, a_2 + l, \ldots, a_t + l)$,
$0 \leq l \leq r - 1$;

(iii) *a substitution* $x \longrightarrow x^2$ *(Frobenius isomorphism):*
$C(2a_1, 2a_2, \ldots, 2a_t) \approx C(a_1, a_2, \ldots, a_t)$.

QC codes - a trace description

$$k = 6,\ 2^6 - 1 = 63 = 7 \cdot 9,\ m = 9,\ r = 7$$

$$C(0,1) \approx C(0,2) \approx C(0,4) \approx C(0,3) \approx C(0,6) \approx C(0,5)$$

$\Rightarrow$ a unique code for $t = 2$ ([18,6,6] code)

$$C(0,1,3) \approx C(0,2,6) \approx C(0,4,5)$$
$$C(0,1,5) \approx C(0,4,6) \approx C(0,2,3)$$
$$C(0,1,2) \approx C(0,2,4) \approx C(0,1,4) \approx \cdots$$

3 inequivalent codes for $t = 3$ ($n = 27, k = 6$):

$1 + 9y^{10} + 9y^{12} + 27y^{14} + 18y^{16}, |Aut(C)| = 18$

$1 + 36y^{12} + 27y^{16}, |Aut(C)| = 51840$

$1 + 27y^{12} + 27y^{14} + 9y^{18}, |Aut(C)| = 1296$

QC codes - a trace description

$$k = 8,\ 2^8 - 1 = 255 = 15 \cdot 17\ m = 17,\ r = 15$$

t	2	3	4	5	6	7
inequivalent codes	3	10	27	56	91	115
optimal codes	1	1	1	1	3	-
d	14	24	32	40	48	57
two-wight codes	-	1	1	1	2	1

$$C(1),\ C(3),\ C(5),\ C(7)$$

$$C(0,1) \approx C(0,14) \approx C(0,7),\ C(0,3),\ C(0,5)$$

QC codes - open problems

- A sequence of the transformations from Theorem 6 is a sufficient condition for equivalence of two binary QC codes? When the products of these three transformations give a necessary condition for equivalence?
- What is going on when $m < k$?
- Is the theory for $q > 2$ the same?
- Are there BWD quasi-cyclic codes?
- What about two-weight quasi-cyclic codes?