

CYCLIC AND NEGACYCLIC CODES OVER \mathbb{Z}_4 AND THEIR BINARY IMAGES

Jacques Wolfmann
IMATH (GRIM)
Université du Sud Toulon-Var
France

ANKARA, August 2008

Motivation

$$\text{Gray Map : } \mathbb{Z}_4^n \xrightarrow{\phi} \mathbb{F}_2^{2n}$$

$\Gamma = \text{Linear Cyclic Code over } \mathbb{Z}_4$



$K = \text{Kerdock Code (non linear code over } \mathbb{F}_2)$

Γ^\perp (dual of Γ)



$P = \text{Preparata Code (non linear code over } \mathbb{F}_2)$

K and P are formally dual.

Questions:

Codes C over \mathbb{Z}_4 such that $\phi(C)$ is linear ?

Cyclique ? linear Cyclique ?

Vectors and Polynomials over \mathbb{Z}_4

- $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = (\{0, 1\}, + \text{ mod } 2, \times \text{ mod } 2)$
 $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = (\{0, 1, 2, 3\}, + \text{ mod } 4, \times \text{ mod } 4)$
- Additions in $\mathbb{F}_2, \mathbb{F}_2^m, \mathbb{F}_2[x]$ denoted by \oplus ,
 - Additions in $\mathbb{Z}_4, \mathbb{Z}_4^m, \mathbb{Z}_4[x]$ denoted by $+$.

Binary decomposition, binary reduction

Define two maps \tilde{r} and \tilde{q} from \mathbb{Z}_4 into \mathbb{F}_2 :
 If $\lambda \in \mathbb{Z}_4$, then the 2-adic expansion of λ is :

$$\lambda = \tilde{r}(\lambda) + 2\tilde{q}(\lambda)$$

$$\tilde{r}(0) = 0, \tilde{q}(0) = 0, \quad \tilde{r}(1) = 1, \tilde{q}(1) = 0,$$

$$\tilde{r}(2) = 0, \tilde{q}(2) = 1, \quad \tilde{r}(3) = 1, \tilde{q}(3) = 1.$$

Extending \tilde{r} and \tilde{q} to \mathbb{Z}_4^n and $\mathbb{Z}_4[x]$:

If $\underline{z} = (z_1, \dots, z_i, \dots, z_n) \in \mathbb{Z}_4^n$ then :

$$\tilde{r}(\underline{z}) = (\tilde{r}(z_1), \dots, \tilde{r}(z_i), \dots, \tilde{r}(z_n))$$

$$\tilde{q}(\underline{z}) = (\tilde{q}(z_1), \dots, \tilde{q}(z_i), \dots, \tilde{q}(z_n))$$

$$\underline{z} = \tilde{r}(\underline{z}) + 2\tilde{q}(\underline{z}).$$

$\tilde{r}(\underline{z})$ is the binary reduction of \underline{z} .

If $u(x) \in \mathbb{Z}_4[x]$ then:

$$u(x) = \tilde{r}(x) + 2\tilde{q}(x)$$

with $\tilde{r}(x)$ and $\tilde{q}(x)$ in $\mathbb{F}_2[x]$.

$\tilde{r}(x)$ is the binary reduction of $u(x)$.

Examples:

$$\underline{z} = (1, 0, 3, 2, 3, 1):$$

$$\tilde{r}(\underline{z}) = (1, 0, 1, 0, 1, 1), \quad \tilde{q}(\underline{z}) = (0, 0, 1, 1, 1, 0).$$

$$u(x) = 1 + 3x^2 + 2x^3 + 3x^4 + x^5:$$

$$\tilde{r}(x) = 1 + x^2 + x^4 + x^5, \quad \tilde{q}(x) = x^2 + x^3 + x^4$$

Special properties :

Let $U = \tilde{A} + 2\tilde{B}$ be with :

$U \in \mathbb{Z}_4^n$ (or $\mathbb{Z}_4[x]$) and $\tilde{A}, \tilde{B} \in \mathbb{F}_2^n$ (or $\mathbb{F}_2[x]$).

- $2U = 2\tilde{A}$
- $3U = -U = \tilde{A} + 2(\tilde{A} \oplus \tilde{B})$
- $U^2 = (\tilde{A})^2$

If \tilde{X} and \tilde{Y} are in \mathbb{F}_2^n (or $\mathbb{F}_2[x]$) :

- $2(\tilde{X} + \tilde{Y}) = 2(\tilde{X} \oplus \tilde{Y})$
- $2\tilde{X} = 2\tilde{Y}(x) \implies \tilde{X} = \tilde{Y}$

Componentwise product:
(or Hadamard product)

$$(u_1, \dots, u_n) \star (v_1, \dots, v_n) = (u_1v_1, \dots, u_nv_n)$$

$$\left(\sum_{i=0}^{t-1} u_i x^i\right) \star \left(\sum_{i=0}^{t-1} v_i x^i\right) = \sum_{i=0}^{t-1} u_i v_i x^i.$$

$$U \star V = \{u \star v \mid u \in U, v \in V\}$$

$(\mathbb{F}_2^n, +, \otimes)$ is a commutative ring.

Notation:

$$R_d[x] = \{a_0 + a_1x + \dots + a_{d-1}x^{d-1} \mid a_i \in R\}$$

Polynomial representation of R^t :

$$\mathcal{P} : R^t \rightarrow R_t[x]$$

$$\mathcal{P}(a_0, a_1, \dots, a_i, \dots, a_{t-1}) = \sum_{i=0}^{t-1} a_i x^i.$$

Ring of Polynomials modulo $f(x)$:

If $f(x) \in R[x]$ with $\deg(f(x)) = d, d \geq 1$,
then :

$$R[x]/(f(x)) = (R_d[x], + \text{ mod } f(x), \times \text{ mod } f(x))$$

Factorization of polynomials

$\mathbb{Z}_4[x]$ is not a unique factorization domain :

$$\begin{aligned} x^2 &= (x - 2)(x - 2) \\ x^4 - 1 &= (x - 1)(x + 1)(x^2 + 1) \\ &= (x + 1)^2(x^2 + 2x + 3). \end{aligned}$$

Weights and distances in \mathbb{F}_2^t and \mathbb{Z}_4^t

$\underline{u} = (u_1, u_2, \dots, u_t)$, $\underline{v} = (v_1, v_2, \dots, v_t)$ in R^t .

Hamming weight :

$$w_H(\underline{u}) = \#\{i \mid u_i \neq 0\}$$

Hamming distance :

$$d_H(\underline{u}, \underline{v}) = \#\{i \mid u_i \neq v_i\} = w_H(v - u)$$

If $R = \mathbb{Z}_4$ define $w^{(j)}(\underline{u}) = \#\{i \mid u_i = j\}$
for $j = 0, 1, 2, 3$.

Lee weight :

$$w_L(\underline{u}) = w^{(1)}(u) + w^{(3)}(u) + 2w^{(2)}(u)$$

Lee distance :

$$d_L(\underline{u}, \underline{v}) = w_L(\underline{v} - \underline{u})$$

Example: $\underline{u} = (1, 2, 1, 0, 1)$, $\underline{v} = (2, 1, 3, 1, 2)$

$$v - u = (1, 3, 2, 1, 1) \text{ and}$$

$$d_L(\underline{u}, \underline{v}) = 3 + 1 + 2 = 6$$

Polynomial version:

If $u(x), v(x)$ are the polynomial representation of $\underline{u}, \underline{v}$ then:

$$d_H(u(x), v(x)) = d_H(\underline{u}, \underline{v}) \text{ and}$$

$$d_L(u(x), v(x)) = d_L(\underline{u}, \underline{v}).$$

Let E be a subset of R^t and let d be a distance in R^t .

For $u \in E$ and $j \in \{0, 1, \dots, t\}$, define :

$$D_j(u) = \#\{v \in E \mid d(u, v) = j\}$$

E is said distance invariant if, for every j in $\{0, 1, \dots, t\}$ the number $D_j(u)$ is independent of the choice of u in E .

If $0 \in E$, then for every u the number $D_j(u)$ is equal to the number A_j of elements of E of weight j .

Derivatives, Even part, Odd part in $\mathbb{F}_2[x]$

- $\frac{d}{dx}[x^{2i}] = 0, \frac{d}{dx}[x^{2i+1}] = x^{2i}$

If $\tilde{a}(x) = \sum_{i \in I} a_i x^i \in \mathbb{F}_2[x]$, define :

$$E_v(\tilde{a}(x)) = \sum_{i \text{ even}} a_i x^i \text{ (even part)}$$

$$O_d(\tilde{a}(x)) = \sum_{i \text{ odd}} a_i x^i \text{ (odd part)}$$

Then :

- $O_d(\tilde{a}(x)) = x \frac{d}{dx}[\tilde{a}(x)]$

- $E_v(\tilde{a}(x)) = \tilde{a}(x) \oplus x \frac{d}{dx}[\tilde{a}(x)]$

In $\mathbb{Z}_4[x]$:

- $\tilde{a}(-x) = \tilde{a}(x) + 2O_d(\tilde{a}(x))$
 $= \tilde{a}(x) + 2x \frac{d}{dx}[\tilde{a}(x)].$

Linear, Cyclic, Negacyclic

Definitions :

R : commutative ring, $t \in \mathbb{N}^*$.

A linear code of length t over R is a R -submodule of R^t .

Remark : A linear code over a ring is not necessarily a free module.

Let ω be an invertible element of R .

The ω -shift σ_ω of R^t is the permutation of R^t defined by :

$$\sigma_\omega(a_0, a_1, \dots, a_{t-1}) = (\omega a_{t-1}, a_0, \dots, a_{t-2}).$$

Constacyclic code : A subset C of R^t is a constacyclic code of length t over R if there exists an invertible element of R such that $\sigma(C) \subseteq C$.

cyclic code : if $\omega = 1$.

$\sigma_1 = \sigma$ is the shift

Negacyclic code : if $\omega = -1$.

σ_{-1} is the negashift

Warning : in classical theory for codes over finite field, cyclic means linear and shift invariant. In this talk, a cyclic code is shift invariant and not necessarily linear.

Proposition 1 *A subset C of R^t is a linear ω -constacyclic code of length t over R if and only if its polynomial representation is an ideal of $R[x]/(x^t - \omega)$.*

Notations

$$\mathcal{A}(t) = R[x]/(x^t - 1).$$

$\langle r(x) \rangle$: ideal of $\mathcal{A}(t)$ generated by $r(x)$.

Special notations :

$$\text{If } R = \mathbb{F}_2, t = n : \mathcal{A}_2(n), \langle r(x) \rangle_2^n, \mathcal{P}_2^n$$

$$\text{If } R = \mathbb{F}_2, t = 2n : \mathcal{A}_2(2n), \langle r(x) \rangle_2^{2n}, \mathcal{P}_2^{2n}$$

$$\text{If } R = \mathbb{Z}_4, t = n : \mathcal{A}_4(n), \langle r(x) \rangle_4^n, \mathcal{P}_4^n$$

Remark:

$$\text{If } u(x) \in \mathcal{A}_4(t) \text{ then } \langle 2u(x) \rangle_4^t = 2 \langle \tilde{u}(x) \rangle_2^t.$$

Gray map and Nechaev-Gray map

Definition 2

Identifying \mathbb{F}_2^{2n} as $\mathbb{F}_2^n \times \mathbb{F}_2^n$,
the **Gray map** ϕ from \mathbb{Z}_4^n into \mathbb{F}_2^{2n} is defined
by :

If $Z = \tilde{r}(Z) + 2\tilde{q}(Z)$ with $\tilde{r}(Z), \tilde{q}(Z)$ in $\mathbb{F}_2[x]$:

$$\phi(Z) = (\tilde{q}(Z), \tilde{r}(Z) \oplus \tilde{q}(Z))$$

Example :

If $Z = (1, 3, 0, 2, 3, 2)$ then :

$$\phi(Z) = (0, 1, 0, 1, 1, 1 \mid 1, 0, 0, 1, 0, 1)$$

Remark :

$$\phi(2Z) = (\tilde{r}(Z), \tilde{r}(Z))$$

$$\phi(X + 2Y) = \phi(X) \oplus \phi(2Y)$$

If $n = 1$:

$$\phi(0) = (0, 0), \quad \phi(1) = (0, 1)$$

$$\phi(2) = (1, 1), \quad \phi(3) = (1, 0)$$

Proposition 3

The gray map is an isometry for the Lee distance in \mathbb{Z}_4^n and the Hamming distance in \mathbb{F}_2^{2n} .

Polynomial Gray Map

Definition 4

\mathcal{P}_4^n : polynomial representation of \mathbb{Z}_4^n .

\mathcal{P}_2^{2n} : polynomial representation of \mathbb{F}_2^{2n} .

The polynomial Gray Map ϕ_P is:

$$\phi_P = \mathcal{P}_2^{2n} \phi (\mathcal{P}_4^n)^{-1}$$

If $a(x)$ is the polynomial representation of \underline{a} then $\phi_P(a(x))$ is the polynomial representation of $\phi(\underline{a})$.

$$\begin{array}{ccc} \underline{a} = (a_0, a_1, \dots, a_{n-1}) & \xrightarrow{\phi} & (\tilde{q}_0, \tilde{q}_1, \dots, \tilde{q}_{n-1} \mid \tilde{r}_0 \oplus \tilde{q}_0, \tilde{r}_1 \oplus \tilde{q}_1, \dots, \tilde{r}_{n-1} \oplus \tilde{q}_{n-1}) \\ \downarrow \mathcal{P}_4^n & & \downarrow \mathcal{P}_2^{2n} \\ a(x) = \tilde{r}(x) + 2\tilde{q}(x) & \xrightarrow{\phi_P} & \tilde{q}(x) \oplus x^n(\tilde{r}(x) \oplus \tilde{q}(x)) \end{array}$$

$$\phi_P(\tilde{r}(x) + 2\tilde{q}(x)) = \tilde{q}(x) \oplus x^n(\tilde{r}(x) \oplus \tilde{q}(x))$$

The Gray map of the negashift is the shift of the Gray map.

Theorem 5 $n \in \mathbb{N}^*$, n odd,
 ϕ : Gray, ν : negashift of \mathbb{Z}_4^n , $\tilde{\sigma}$: shift of \mathbb{F}_2^{2n} .

$$\boxed{\phi\nu = \tilde{\sigma}\phi}$$

With $a_i = \tilde{r}_i + 2\tilde{q}_i$:

$$\begin{array}{ccc} (a_0, a_1, \dots, a_{n-1}) & \xrightarrow{\phi} & (\tilde{q}_0, \tilde{q}_1, \dots, \tilde{q}_{n-1} \mid \tilde{r}_0 \oplus \tilde{q}_0, \tilde{r}_1 \oplus \tilde{q}_1, \dots, \tilde{r}_{n-1} \oplus \tilde{q}_{n-1}) \\ \downarrow \nu & & \downarrow \tilde{\sigma} \\ (-a_{n-1}, a_0, \dots, a_{n-2}) & \xrightarrow{\phi} & (\tilde{r}_{n-1} \oplus \tilde{q}_{n-1}, \tilde{q}_0, \dots, \mid \tilde{q}_{n-1}, \tilde{r}_0 \oplus \tilde{q}_0, \dots, \tilde{r}_{n-2} \oplus \tilde{q}_{n-2}) \end{array}$$

Corollary 6 n odd.

$$\boxed{\phi(\text{Linear negacyclic code}) = \text{dist.invariant cyclic code}}$$

$$\begin{array}{ccc} C & \xrightarrow{\phi} & \phi(C) \\ \downarrow \nu & & \downarrow \tilde{\sigma} \\ C & \xrightarrow{\phi} & \phi(C) \end{array}$$

Proof: C lin.negacyclic code. $\phi(\nu(C)) = \tilde{\sigma}(\phi(C))$.
 Since $\nu(C) = C$, then $\phi(C) = \tilde{\sigma}(\phi(C))$

C is Lee-distance invariant and ϕ isometry from Lee to Hamming.
 Then $\phi(C)$ is distance invariant.

Remarque: $\phi(C)$ is not necessarily a linear code.

Polynomial version

\mathcal{P}_4^n : polynomial representation of \mathbb{Z}_4^n .

p^+ : $\mathbb{Z}_4[x]/(x^n + 1) \rightarrow \mathbb{Z}_4[x]/(x^n + 1)$

$$a(x) \rightarrow xa(x).$$

$$p^+ \mathcal{P}_4^n = \mathcal{P}_4^n \nu$$

$$\underline{a} = (a_0, a_1, \dots, a_{n-1}) \xrightarrow{\mathcal{P}_4^n} a(x) = \sum_{i=0}^{n-1} a_i x^i$$

$$\downarrow \nu \qquad \qquad \qquad \downarrow p^+$$

$$(-a_{n-1}, a_0, \dots, a_{n-2}) \xrightarrow{\mathcal{P}_4^n} xa(x) \bmod (x^n + 1)$$

Equivalent transformations :

multiplication of $\mathcal{P}_4^n(\underline{a})$ by $x \bmod (x^n + 1)$

negashift of \underline{a} in \mathbb{Z}_4^n .

shift of $\phi(\underline{a})$ in \mathbb{F}_2^{2n} .

C : linear negacyclic code.

J : ideal in $\mathbb{Z}_4[x]/(x^n + 1)$, polynomial representation of C .

$$\begin{array}{ccccc}
 J & \xrightarrow{(\mathcal{P}_4^n)^{-1}} & C & \xrightarrow{\phi} & \phi(C) \\
 \downarrow p^+ & & \downarrow \nu & & \downarrow \tilde{\sigma} \\
 J & \xrightarrow{(\mathcal{P}_4^n)^{-1}} & C & \xrightarrow{\phi} & \phi(C)
 \end{array}$$

Definition 7

The Nechaev permutation $\tilde{\pi}$ of \mathbb{F}_2^{2n} defined by:

$$\tilde{\pi}(a_0, \dots, a_i, \dots, a_{2n-1}) = (a_{\tau(0)}, \dots, a_{\tau(i)}, \dots, a_{\tau(2n-1)})$$

where τ : permutation of $\{0, 1, \dots, i, \dots, 2n-1\}$:

$$(1, n+1)(3, n+3) \dots (2i+1, n+2i+1) \dots (n-2, 2n-2)$$

Proposition 8 Assume n odd.

\mathcal{P}_4^n : polynomial representation of \mathbb{Z}_4^n

$$\mu: \mathbb{Z}_4[x]/(x^n + 1) \rightarrow \mathbb{Z}_4[x]/(x^n + 1)$$

$$a(x) \rightarrow a(-x)$$

$\tilde{\mu}$: permutation of \mathbb{Z}_4^n

$$(a_0, a_1, \dots, a_i, \dots, a_{n-1}) \rightarrow (a_0, -a_1, a_2, \dots, (-1)^i a_i, \dots, a_{n-1}).$$

$\tilde{\pi}$: Nechaev permutation.

ϕ : Gray map

then :

$$\boxed{\begin{array}{l} \mu \mathcal{P}_4^n = \mathcal{P}_4^n \tilde{\mu} \\ \tilde{\pi} \phi = \phi \tilde{\mu} \end{array}}$$

$$\begin{array}{ccccc} \mathbb{Z}_4[x]/(x^n + 1) & \xrightarrow{(\mathcal{P}_4^n)^{-1}} & \mathbb{Z}_4^n & \xrightarrow{\phi} & \mathbb{F}_2^{2n} \\ \downarrow \mu & & \downarrow \tilde{\mu} & & \downarrow \tilde{\pi} \\ \mathbb{Z}_4[x]/(x^n + 1) & \xrightarrow{(\mathcal{P}_4^n)^{-1}} & \mathbb{Z}_4^n & \xrightarrow{\phi} & \mathbb{F}_2^{2n} \end{array}$$

By using $-a_i = \tilde{r}_i + 2(\tilde{r}_i \oplus \tilde{q}_i)$:

$$\begin{array}{ccc}
 a(x) = \tilde{r}(x) + 2\tilde{q}(x) & \xrightarrow{\mu} & a(-x) \\
 \downarrow (\mathcal{P}_4^n)^{-1} & & \downarrow (\mathcal{P}_4^n)^{-1} \\
 \underline{a} = (a_0, a_1, \dots, a_{n-1}) & \xrightarrow{\tilde{\mu}} & (a_0, \dots, (-1)^i a_i, \dots, a_{n-1}) \\
 \downarrow \phi & & \downarrow \phi \\
 (\dots \tilde{q}_i, \dots \mid \dots \tilde{r}_i \oplus \tilde{q}_i, \dots) & \xrightarrow{\tilde{\pi}} & (\tilde{q}_0, \tilde{r}_1 \oplus \tilde{q}_1, \tilde{q}_2 \dots \mid \tilde{r}_0 \oplus \tilde{q}_0, \tilde{q}_1, \tilde{r}_2 \oplus \tilde{q}_2 \dots)
 \end{array}$$

Equivalent transformations :

- substitution of x by $-x$ in $\mathbb{Z}_4[x]/(x^n + 1)$
- $\tilde{\mu}$ in \mathbb{Z}_4^n .
- Nechaev permutation in \mathbb{F}_2^{2n} .

Proposition 9

$\mu: u(x) \rightarrow u(-x)$.

If n is odd then μ is a ring isomorphism.

Corollary 10

If I is an ideal of $\mathcal{A}_4(n)$ then $\mu(I)$ is an ideal of $\mathbb{Z}_4[x]/(x^n + 1)$.

$$\begin{array}{ccccc}
 I & \xrightarrow{(\mathcal{P}_4^n)^{-1}} & \text{lin. cycl. code} & \xrightarrow{\phi} & \phi(\text{lin. cycl. code}) \\
 \downarrow \mu & & \downarrow \tilde{\mu} & & \downarrow \tilde{\pi} \\
 \mu(I) & \xrightarrow{(\mathcal{P}_4^n)^{-1}} & \text{lin. negacycl. code} & \xrightarrow{\phi} & \text{cycl. code}
 \end{array}$$

Definition 11

The Nechaev-Gray map is the map ψ from \mathbb{Z}_4^n into \mathbb{F}_2^{2n} defined by :

$$\psi = \tilde{\pi}\phi$$

$$\begin{array}{ccccc}
 I & \xrightarrow{(\mathcal{P}_4^n)^{-1}} & \text{lin. cycl. code} & \xrightarrow{\phi} & \phi(\text{lin. cycl. code}) \\
 \downarrow \mu & & \downarrow \tilde{\mu} & & \downarrow \tilde{\pi} \\
 \mu(I) & \xrightarrow{(\mathcal{P}_4^n)^{-1}} & \text{lin. negacycl. code} & \xrightarrow{\phi} & \text{cycl. code}
 \end{array}$$

Theorem 12 *If n odd :*

$$\psi(\text{linear cyclic code}) = \text{cyclic code.}$$

SUMMARY

Theorem 13

Let C be a linear code over \mathbb{Z}_4 . Let ϕ be the Gray map and let ψ be the Nechaev-Gray map.

1) $\phi(C)$ is a cyclic code if and only if C is a negacyclic code.

2) $\psi(C)$ is a cyclic code if and only if C is a cyclic code.

Polynomial version n odd.

Definition 14

The ϕ_P polynomial Gray map and the ψ_P polynomial Nechaev-Gray map are defined by:

If $a(x) : \text{polynomial representation of } \underline{a}$, then

$$\phi_P(a(x)) = \mathcal{P}_2^{2n}(\phi_P(\underline{a}))$$

$$\psi_P(a(x)) = \mathcal{P}_2^{2n}(\psi_P(\underline{a}))$$

(polynomial representation of $\phi(\underline{a})$ and $\psi(\underline{a})$)

If $a(x) = \tilde{r}(x) + 2\tilde{q}(x)$, then :

$$\phi_P(a(x)) = \tilde{q}(x) \oplus x^n(\tilde{q}(x) \oplus \tilde{r}(x))$$

Proposition 15 (Main property)

$\mu: u(x) \rightarrow u(-x)$.

$$\psi_P = \phi_P \mu$$

$$\psi_P(a(x)) = \phi_P(a(-x))$$

Proposition 16

$$\psi_P(a(x)) = (x^n + 1)\tilde{q}(x) \oplus x \frac{d}{dx} [(x^n + 1)\tilde{r}(x)]$$

Example:

$$\underline{a} = (1, 3, 0, 2, 3, 2, 0).$$

$$a(x) = 1 + 3x + 2x^3 + 3x^4 + 2x^5.$$

$$\begin{aligned} a(-x) &= 1 - 3x - 2x^3 + 3x^4 - 2x^5 \\ &= 1 + x + 2x^3 + 3x^4 + 2x^5 \\ &= 1 + x + x^4 + 2(x^3 + x^4 + x^5). \end{aligned}$$

$$\begin{aligned} \psi_P(a(x)) &= \phi_P(a(-x)) \\ &= x^3 + x^4 + x^5 + x^7((1 + x + x^4) \oplus (x^3 + x^4 + x^5)) \\ &= x^3 + x^4 + x^5 + x^7(1 + x + x^3 + x^5) \\ &= x^3 + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{12}. \end{aligned}$$

$$\psi(\underline{a}) = (0, 0, 0, 1, 1, 1, 0 \mid 1, 1, 0, 1, 0, 1, 0).$$

CYCLIC CODES OVER \mathbb{Z}_4

Lemma 17 (Hensel)

If $\tilde{d}(x)$ is a monic divisor of $x^n - 1$ over \mathbb{F}_2 with n odd, then there is a unique monic divisor $d(x)$ of $x^n - 1$ over \mathbb{Z}_4 such that the binary reduction of $d(x)$ is $\tilde{d}(x)$.

$d(x)$ is the **Hensel lift** of $\tilde{d}(x)$.

Construction :

$\epsilon d(x^2) = \tilde{d}(x)\tilde{d}(-x)$ calculated in $\mathbb{Z}_4[x]$ and with $\epsilon \in [-1, +1]$.

Example. In $\mathbb{F}_2[x]$:

$$x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

If $\tilde{d}(x) = x^3 + x + 1$ then :

$$\begin{aligned}\tilde{d}(x)\tilde{d}(-x) &= (x^3 + x + 1)(-x^3 - x + 1) \\ &= -x^6 - 2x^4 - x^2 + 1 \\ &= -(x^6 + 2x^4 + x^2 - 1)\end{aligned}$$

and finally : $d(x) = x^3 + 2x^2 + x + 3$.

Similarly we find in $\mathbb{Z}_4[x]$:

$$\begin{aligned}x^7 - 1 &= \\ (x - 1)(x^3 + 2x^2 + x + 3)(x^3 + 3x^2 + 2x + 3).\end{aligned}$$

Structure of \mathbb{Z}_4 -linear-cyclic codes of odd lengths

Theorem 18 (Several authors)

Let n be odd.

a) Every ideal in $\mathcal{A}_4(n)$ is a principal ideal .

b) If C is a linear cyclic code of length n over \mathbb{Z}_4 , then its polynomial representation I is a principal ideal generated by a constant polynomial or a polynomial of the form :

$$g(x) = a(x)[b(x) + 2]$$

where $x^n - 1 = a(x)b(x)c(x)$ in $\mathbb{Z}_4[x]$.

c) The cardinality of C is $4^{\deg c(x)} 2^{\deg b(x)}$.

Notation : $[n, a(x), b(x), c(x)]$ code.

Remark : A decomposition of $x^n - 1$ into irreducible factors in $\mathbb{Z}_4[x]$ can be deduced from the decomposition of $x^n - 1$ into irreducible factors in $\mathbb{F}_2[x]$ by using Hensel Lemma.

Proposition 19 *If $g(x) = a(x)[b(x) + 2]$ is the generator of a linear cyclic code over \mathbb{Z}_4 of odd length n , with $x^n - 1 = a(x)b(x)c(x)$ then :*

$$\mathcal{P}_4^n(C) = \langle a(x)b(x) \rangle_4^n + \langle 2a(x) \rangle_4^n$$

Proof

- $g(x) = a(x)[b(x) + 2]$
 $c(x)g(x) = a(x)b(x)c(x) + 2a(x)c(x) = 2a(x)c(x)$
 since $a(x)b(x)c(x) = x^n - 1$.
- $2g(x) = 2a(x)b(x)$
 From $u(x)b(x) + v(x)c(x) = 1$:
 $2u(x)a(x)b(x) + 2v(x)a(x)c(x) = 2a(x)$,
 $2u(x)g(x) + v(x)c(x)g(x) = 2a(x)$ hence
 $2a(x) \in \mathcal{P}_4^n(C)$.
- $a(x)b(x)$ and $2a(x)$ both belong to $\mathcal{P}_4^n(C)$.
 Therefore $\langle a(x)b(x) \rangle_4^n + \langle 2a(x) \rangle_4^n$ is
 included in $\mathcal{P}_4^n(C)$.
- Conversely, every member of \mathcal{P}_4^n is a
 multiple of $a(x)[b(x) + 2]$ and thus
 belongs to $\langle a(x)b(x) \rangle_4^n + \langle 2a(x) \rangle_4^n$.

Proposition 20

$$\mathcal{P}_4^n(C) \cap \langle 2 \rangle_4^n = \langle 2a(x) \rangle_4^n$$

Proof

If $u(x) \in \mathcal{P}_4^n(C) \cap \langle 2 \rangle_4^n$:

$$u(x) = m(x)a(x)[b(x) + 2] = 2s(x)$$

• Euclidean division in $\mathbb{Z}_4[x]$:

$$m(x) = c(x)q(x) + r(x) \text{ with } \deg r(x) < \deg c(x).$$

$$u(x) = (x^n - 1)q(x) + r(x)a(x)b(x) + 2a(x)[c(x)q(x) + r(x)]$$

• Modulo $(x^n - 1)$:

$$2s(x) = r(x)a(x)b(x) + 2a(x)[c(x)q(x) + r(x)]$$

• Binary reduction: $\tilde{r}(x)\tilde{a}(x)\tilde{b}(x) = 0$.

Since $a(x)b(x)$ is non-zero : $\tilde{r}(x) = 0$.

This means $r(x) = 2q_1(x)$

• Finally:

$$u(x) = 2a(x)b(x)q_1(x) + 2a(x)[c(x)q(x) + r(x)].$$

Therefore $u(x)$ belongs to $\langle 2a(x) \rangle_4^n$.

Conclusion:

$\mathcal{P}_4^n(C) \cap \langle 2 \rangle_4^n$ is included in $\langle 2a(x) \rangle_4^n$.

• Conversely, $\langle 2a(x) \rangle_4^n$ is obviously included in $\mathcal{P}_4^n(C) \cap \langle 2 \rangle_4^n$.

Negacyclic codes of odd lengths

Proposition 21

Define $\mu: \mathcal{A}_4(n) \rightarrow \mathbb{Z}_4[x]/(x^n + 1)$ such that:
 $\mu(a(x)) = a(-x)$.

If n is odd then μ is a ring isomorphism.

Corollary 22

If I is a subset of $\mathcal{A}_4(n)$ with n odd, then I is an ideal of $\mathcal{A}_4(n)$ if and only if $\mu(I)$ is an ideal of $\mathbb{Z}_4[x]/(x^n + 1)$.

Corollary 23

Let n be odd.

a) Every ideal in the ring $\mathbb{Z}_4[x]/(x^n + 1)$ is a principal ideal .

b) If C is a linear negacyclic code of length n , then its polynomial representation I is a principal ideal generated by a constant polynomial or a polynomial of the form : $g(x) = a(x)[b(x) + 2]$ where $x^n + 1 = a(x)b(x)c(x)$ in $\mathbb{Z}_4[x]$.

c) The cardinality of C is $4^{\deg c(x)} 2^{\deg b(x)}$.

Examples of Nechaev-Gray images.

C : linear cyclic code over \mathbb{Z}_4 .

Generator : $g(x) = a(x)[b(x) + 2]$.

$\tilde{C} = \psi(C)$.

Length of \tilde{C} : $\tilde{n} = 2n$.

Cardinality of $\tilde{C} = 2^k$

($k = 2 \deg c(x) + \deg b(x)$)

w : min.weight of \tilde{C} ,

$w_{lin.}$: largest min.weight for binary linear codes of length \tilde{n} and dimension k

$w_{cycl.}$: largest min. weight for binary (\tilde{n}, k) linear cyclic codes.

1) $\tilde{n} = 14$

$a(x) = (x - 1)(x^3 + 2x^2 + x + 3)$, $b(x) = 1$.

$k = 6$, $w = 6$, $w_{lin.} = 5$, $w_{cycl.} = 4$.

2) $\tilde{n} = 42$

$a(x) = (x - 1)(x^3 + 2x^2 + x + 3)$

$(x^6 + 2x^5 + 3x^4 + 3x^2 + x + 1)$

$(x^6 + x^5 + 3x^4 + 3x^2 + 2x + 1)$

$b(x) = x^2 + x + 1$.

$k = 8$, $w = 18$, $w_{lin.} = 18$, $w_{cycl.} = 14$.

\mathbb{Z}_4 -LINEAR CYCLIC CODES WHOSE
NECHAEV-GRAY IMAGES ARE
 \mathbb{F}_2 -LINEAR CYCLIC CODES

$C : [n, a(x), b(x), c(x)]$ linear cyclic code
over \mathbb{Z}_4 , n odd.

ϕ : Gray map, ψ : Nechaev-Gray map.

Question : we know that $\psi(C)$ is a cyclic code.

When $\psi(C)$ is a linear cyclic code ?

When $\phi(C)$ is a linear code ? a linear cyclic code ?

Proposition 24

C : lin.cyclic code over \mathbb{Z}_4 of odd length n .

$g(x) = a(x)[b(x) + 2]$: generator of C .

ϕ : Gray map.

$\phi(C)$ is a binary linear code if and only if :
 $\langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n \star \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n \subseteq \langle \tilde{a}(x) \rangle_2^n$

Proof:

From the definitions:

$$\phi(\underline{u}_1 + \underline{u}_2) = \phi(\underline{u}_1) + \phi(\underline{u}_2) + \phi(2(\tilde{u}_1 \star \tilde{u}_2)).$$

Consequence:

$\phi(C)$ is a binary linear code if and only if :

$$\forall \underline{u}_1 \in C, \forall \underline{u}_2 \in C, 2(\tilde{u}_1 \star \tilde{u}_2) \in C$$

Polynomial version:

$\phi(C)$ is a binary linear code if and only if :

$$\begin{aligned} & \forall m_1(x) \in \mathcal{A}_4(n), \forall m_2(x) \in \mathcal{A}_4(n) \\ (C) \quad & 2(\tilde{m}_1(x)\tilde{g}(x) \star \tilde{m}_2(x)\tilde{g}(x)) \in \mathcal{P}_4^n(C) \end{aligned}$$

Since $\tilde{g}(x) = \tilde{a}(x)\tilde{b}(x)$, then (C) is:

$$2(\tilde{m}_1(x)\tilde{a}(x)\tilde{b}(x) \star \tilde{m}_2(x)\tilde{a}(x)\tilde{b}(x)) \in \mathcal{P}_4^n(C)$$

From

- $\mathcal{P}_4^n(C) \cap (2\mathcal{A}_4(n)) = \langle 2a(x) \rangle_4^n$,
- $\langle 2a(x) \rangle_4^n = 2 \langle \tilde{a}(x) \rangle_2^n$,
- $2\tilde{v}(x) = 2\tilde{u}(x) \Rightarrow \tilde{v}(x) = \tilde{u}(x)$,

$2(\tilde{m}_1(x)\tilde{a}(x)\tilde{b}(x) \star \tilde{m}_2(x)\tilde{a}(x)\tilde{b}(x)) \in \mathcal{P}_4^n(C)$
is equivalent to:

$$\tilde{m}_1(x)\tilde{a}(x)\tilde{b}(x) \star \tilde{m}_2(x)\tilde{a}(x)\tilde{b}(x) \in \langle \tilde{a}(x) \rangle_2^n$$

which gives the expected result.

Theorem 25 (W. 2000)

C : lin.cyclic code over \mathbb{Z}_4 of odd length n .

1) $\psi(C)$ is a distance invariant cyclic code.

2) $\psi(C)$ is contained in the linear cyclic code of length $2n$ generated by $\tilde{a}(x)\tilde{b}(x)$.

3) If $\psi(C)$ is a linear code then $\psi(C)$ is the linear cyclic code of length $2n$ generated by $\tilde{a}(x)^2\tilde{b}(x)$.

Proof:

$\psi(C)$ distance invariant

Comes from:

$$\begin{aligned}\psi(C) &= \tilde{\pi}(\phi(C)), \\ \phi(C) &\text{ distance invariant,} \\ \tilde{\pi} &\text{ vector isomorphism.}\end{aligned}$$

$\psi(C)$ in the lin.cyc.code generated by $\tilde{a}(x)\tilde{b}(x)$.

If $u(x) \in \mathcal{P}_4^n(C)$ then $u(x) = m(x)g(x)$.

Euclidean division in $\mathbb{Z}_4[x]$:

$$m(x) = c(x)Q(x) + R(x), \quad \deg(R(x)) < \deg(c(x)).$$

In $\mathbb{Z}_4[x]$:

$$u(x) = a(x)b(x)c(x)Q(x) + R(x)a(x)b(x) \\ + 2a(x)[c(x)Q(x) + R(x)]$$

In $\mathcal{A}_4(n)$ (because $x^n - 1 = a(x)b(x)c(x)$):

$$u(x) = R(x)a(x)b(x) + 2a(x)[c(x)Q(x) + R(x)].$$

Remark: if $v(x) = u(-x)$ then $\tilde{v}(x) = \tilde{u}(x)$.

Hence $u(-x) = \tilde{R}(x)\tilde{a}(x)\tilde{b}(x) + 2\tilde{Q}_1(x)$.

$$\begin{aligned} \psi_P(u(x)) &= \phi_P(u(-x)) \\ &= \tilde{Q}_1(x) + x^n[\tilde{R}(x)\tilde{a}(x)\tilde{b}(x) + \tilde{Q}_1(x)] \\ &= x^n\tilde{R}(x)\tilde{a}(x)\tilde{b}(x) + (x^n + 1)\tilde{Q}_1(x). \end{aligned}$$

Since $x^n - 1 = \tilde{a}(x)\tilde{b}(x)\tilde{c}(x)$ then $\psi_P(u(x))$ is a multiple of $\tilde{a}(x)\tilde{b}(x)$ and therefore belongs to $\langle \tilde{a}(x)\tilde{b}(x) \rangle_2^{2n}$.

$\psi(C)$ lin. $\Rightarrow \psi(C) = \text{lin.cyc. gener. by } \tilde{a}(x)^2 \tilde{b}(x)$.

We know:

- (1) $\psi(C)$ is a linear cyclic code.
- (2) $\psi_P(C) \subseteq \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^{2n}$.
- (3) $\psi_P(C)$ is a vector subspace of $\mathcal{A}_2(2n)$.
- (4) $\mathcal{P}_4^n(C) \cap \langle 2 \rangle_4^n = \langle 2a(x) \rangle_4^n$

From (2): $\tilde{u}(x) \in \psi_P(C) \Rightarrow \tilde{u}(x) = \tilde{m}(x)\tilde{a}(x)\tilde{b}(x)$.

From (3): $\tilde{c}(x)\tilde{u}(x) \in \psi_P(C)$ and:

$$\begin{aligned} \tilde{c}(x)\tilde{u}(x) &= \tilde{m}(x)\tilde{a}(x)\tilde{b}(x)\tilde{c}(x) \\ &= \tilde{m}(x)(x^n - 1) = \tilde{m}(x) + x^n\tilde{m}(x). \\ &= \phi_P(2\tilde{m}(x)) = \psi_P(2\tilde{m}(x)). \end{aligned}$$

Then $\psi_P(2\tilde{m}(x)) \in \psi_P(C)$ and $2\tilde{m}(x) \in C$.

From (4): $\tilde{m}(x) \in \langle a(x) \rangle_4^n$
 $\tilde{m}(x) = \tilde{s}(x)\tilde{a}(x)$ in $\mathcal{A}_2(n)$.
 $\tilde{u}(x) = \tilde{s}(x)\tilde{a}(x)^2\tilde{b}(x)$
 $\psi_P(C) \subseteq \langle \tilde{a}(x)^2\tilde{b}(x) \rangle_2^{2n}$.

Cardinalities:

$$|\psi_P(C)| = |C| = 4^{\deg c(x)} 2^{\deg b(x)}$$

$x^{2n} - 1 = \tilde{a}(x)^2\tilde{b}(x)^2\tilde{c}(x)^2$ then:

$$|\langle \tilde{a}(x)^2\tilde{b}(x) \rangle_2^{2n}| = 4^{\deg c(x)} 2^{\deg b(x)}$$

Conclusion: $\psi_P(C) = \langle \tilde{a}(x)^2\tilde{b}(x) \rangle_2^{2n}$.

Special construction of divisors of $x^n - 1$.

Definition 26

Let $\tilde{u}(x)$ be a divisor of $x^n - 1$ in $\mathbb{F}_2[x]$ with n odd and let β be a primitive n -th root of unity over \mathbb{F}_2 .

- 1) If $\tilde{u}(x) = 1$ then $(\tilde{u} \circledast \tilde{u})(x) = 1$
- 2) If not, $(\tilde{u} \circledast \tilde{u})(x)$ is the divisor of $x^n - 1$ in $\mathbb{F}_2[x]$ whose roots are the $\beta^i \beta^j$ such that β^i and β^j are roots of $\tilde{u}(x)$.

EXAMPLE $n = 21$

(0)(1, 2, 4, 8, 16, 11)(3, 6, 12)(5, 10, 20, 19, 17, 13)
(7, 14)(9, 18, 15)

$$x^{21} - 1 = \tilde{m}_0(x) \tilde{m}_1(x) \tilde{m}_3(x) \tilde{m}_5(x) \tilde{m}_7(x) \tilde{m}_9(x)$$

$\tilde{m}_i(x)$: minimal polynomial of β^i over \mathbb{F}_2 .

$$\tilde{u}(x) = \tilde{m}_0(x) \tilde{m}_1(x)$$

Roots of $\tilde{u}(x)$: $\beta^0, \beta^1, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^{11}$.

Roots of $(\tilde{u} \circledast \tilde{u})(x)$:

$$\beta^0, \beta^1, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^{11}$$

$$\beta^3, \beta^6, \beta^{12}, \beta^5, \beta^{10}, \beta^{20}, \beta^{19}$$

$$\beta^{17}, \beta^{13}, \beta^9, \beta^{18}, \beta^{15}.$$

$$(\tilde{u} \circledast \tilde{u})(x) = \tilde{m}_0(x) \tilde{m}_1(x) \tilde{m}_3(x) \tilde{m}_5(x) \tilde{m}_9(x)$$

Theorem 27 (W. 2000) n odd.

C : linear cyclic code C over \mathbb{Z}_4 of length n .

$g(x) = a(x)[b(x) + 2]$: generator of C with

$x^n - 1 = a(x)b(x)c(x)$ in $\mathbb{Z}_4[x]$.

ϕ : Gray map, ψ : Nechaev-Gray map.

Let $\tilde{e}(x)$ be such that :

$x^n - 1 = (\tilde{c} \circledast \tilde{c})(x)\tilde{e}(x)$ in $\mathbb{F}_2[x]$.

I) The following properties are equivalent :

1) $\phi(C)$ is a binary linear code.

2) $\psi(C)$ is a binary linear cyclic code.

3) $(\tilde{c} \circledast \tilde{c})(x)$ divides $\tilde{b}(x)\tilde{c}(x)$ in $\mathbb{F}_2[x]$.

4) $\tilde{a}(x)$ divides $\tilde{e}(x)$ in $\mathbb{F}_2[x]$.

II) If one of the previous conditions holds then $\psi(C)$ is the binary linear cyclic code of length $2n$ generated by $\tilde{a}(x)^2\tilde{b}(x)$.

Main tool: Mattson-Solomon Transform

$n \in \mathbb{N}$, $n \geq 2$, p prime power, q a power of p
 n not a multiple of p .

K : the splitting field of $x^n - 1$ over \mathbb{F}_q .

ω : primitive root of $x^n - 1$ in K .

Definition 28 *The Mattson-Solomon Transform associated to ω is the map:*

$T_\omega: \mathcal{A}_q(n) \rightarrow \mathcal{A}_q(n)$ s.t. :

$$T_\omega(m(x)) = \sum_{i=0}^{n-1} m(\omega^{-i})x^i$$

Theorem 29 *T_ω is a bijective map and*

$$(T_\omega)^{-1} = n^{-1}T_{\omega^{-1}}$$

where n^{-1} inverse modulo p .

If $T_\omega(m(x)) = \bar{m}(x)$ then $m(x) = n^{-1} \sum_{j=0}^{n-1} \bar{m}(\omega^j)x^j$.

Hadamard product:

$$\left(\sum_{i=0}^{n-1} a_i x^i\right) \otimes \left(\sum_{i=0}^{n-1} b_i x^i\right) = \sum_{i=0}^{n-1} a_i b_i x^i$$

Theorem 30

T_ω is a ring isomorphism from
 $(\mathcal{A}_q(n), +, \times)$ into $(\mathcal{A}_q(n), +, \otimes)$.

$$T_\omega(a(x) + b(x)) = T_\omega(a(x)) + T_\omega(b(x))$$

$$T_\omega(a(x)b(x)) = T_\omega(a(x)) \otimes T_\omega(b(x))$$

$$T_\omega(x^0) = x^0$$

Sketch of the proof of the main Theorem:

Special case:

If $c(x) = 1$ then $x^n - 1 = \tilde{a}(x)\tilde{b}(x)$ and $g(x) = 2\tilde{a}(x)$.

Hence $\phi(C)$ is the linear cyclic code generated by $(x^n - 1)\tilde{a}(x) = \tilde{a}(x)^2\tilde{b}(x)$.

Furthermore, since $g(-x) = g(x)$ then $\psi(C) = \phi(C)$.

From now on, assume $c(x) \neq 1$.

Part II):

Direct consequence of a previous result.

$\phi(C)$ is linear $\Leftrightarrow \psi(C)$ is linear cyclic

The Nechaev permutation is a linear map and $\psi(C)$ is cyclic.

$$\frac{(\tilde{c} \otimes \tilde{c})(x) \text{ divides } \tilde{b}(x)\tilde{c}(x) \Leftrightarrow \tilde{a}(x) \text{ divides } \tilde{e}(x)}{x^n - 1 = \tilde{a}(x)\tilde{b}(x)\tilde{c}(x) = (\tilde{c} \otimes \tilde{c})(x)\tilde{e}(x)}$$

$\tilde{a}(x)$ divides $\tilde{e}(x) \Rightarrow \phi(C)$ is linear

Let $\tilde{s}(x) = \tilde{m}_1(x)\tilde{a}(x)\tilde{b}(x) \star \tilde{m}_2(x)\tilde{a}(x)\tilde{b}(x)$.

Using the inverse Mattson-Solomon transform with $\tilde{d}(x) = \tilde{a}(x)\tilde{b}(x)$ we obtain:

$$\begin{aligned} \sum_{k=0}^{n-1} s(\beta^k)x^k &= \left(\sum_{i=0}^{n-1} \tilde{m}_1(\beta^i)\tilde{d}(\beta^i)x^i \right) \left(\sum_{j=0}^{n-1} \tilde{m}_2(\beta^j)\tilde{d}(\beta^j)x^j \right) \\ &= \sum_{(\tilde{c} \otimes \tilde{c})(\beta^k)=0, i+j=k} \tilde{m}_1(\beta^i)\tilde{d}(\beta^i)\tilde{m}_2(\beta^j)\tilde{d}(\beta^j)x^k \end{aligned}$$

$$\begin{aligned} \tilde{s}(\beta^k) \neq 0 &\Rightarrow (\tilde{c} \otimes \tilde{c})(\beta^k) = 0 \\ (1) \quad (\tilde{c} \otimes \tilde{c})(\beta^k) \neq 0 &\Rightarrow \tilde{s}(\beta^k) = 0 \end{aligned}$$

Since $x^n - 1 = (\tilde{c} \otimes \tilde{c})(x)\tilde{e}(x)$ and n odd, $\tilde{c} \otimes \tilde{c}(x)$ and $\tilde{e}(x)$ have no common root.

Thus:

$$(2) \quad (\tilde{c} \otimes \tilde{c})(\beta^k) \neq 0 \Leftrightarrow \tilde{e}(\beta^k) = 0.$$

From (1) and (2):

$$\tilde{e}(\beta^k) = 0 \Rightarrow \tilde{s}(\beta^k) = 0.$$

$\tilde{e}(x)$ divides $\tilde{s}(x)$ hence $\tilde{s}(x) \in \langle \tilde{e}(x) \rangle_2^n$.

$\tilde{s}(x) \in \langle \tilde{e}(x) \rangle_2^n$ and if $\tilde{a}(x)$ divides $\tilde{e}(x)$ then:

$$\langle \tilde{e}(x) \rangle_2^n \subseteq \langle \tilde{a}(x) \rangle_2^n,$$

$$\tilde{s}(x) = \tilde{m}_1(x)\tilde{a}(x)\tilde{b}(x) \star \tilde{m}_2(x)\tilde{a}(x)\tilde{b}(x) \in \langle \tilde{a}(x) \rangle_2^n$$

$$\langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n \star \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n \subseteq \langle \tilde{a}(x) \rangle_2^n$$

which proves that $\phi(C)$ is linear.

$\phi(C)$ is linear $\Rightarrow \tilde{a}(x)$ divides $\tilde{e}(x)$

Assume $\phi(C)$ linear code.

1) $\tilde{a}(x) = 1$: obviously $\tilde{a}(x)$ divides $\tilde{e}(x)$.

2) $\tilde{a}(x) \neq 1$.

Notation:

$$K = \{k \mid 0 \leq k \leq n-1, (\tilde{c} \otimes \tilde{c})(\beta^k) = 0\}$$

$$J(k) = \{j \mid 0 \leq j \leq n-1, \tilde{c}(\beta^j) = 0, \tilde{c}(\beta^{k-j}) = 0\}.$$

$$A_j(k) = \tilde{d}(\beta^j)\tilde{d}(\beta^{k-j}) \text{ with } \tilde{d}(x) = \tilde{a}(x)\tilde{b}(x).$$

$$S_k(X) = \sum_{j \in J(k)} A_j(k)X^j.$$

Since $\phi(C)$ linear code, if $0 \leq t \leq n - 1$
 $\exists \tilde{\lambda}_t(x) : \tilde{a}(x)\tilde{b}(x) \star x^t\tilde{a}(x)\tilde{b}(x) = \tilde{\lambda}_t(x)\tilde{a}(x)$
Inverse Mattson-Solomon transform :

$$\sum_{k \in K} S_k(\beta^t)x^k = \sum_{k \in K} \tilde{\lambda}_t(\beta^k)\tilde{a}(\beta^k)x^k$$

$$K = \{k \mid 0 \leq k \leq n - 1, (\tilde{c} \otimes \tilde{c})(\beta^k) = 0\}$$

$$S_k(X) = \sum_{j \in J(k)} A_j(k)X^j$$

From the definitions: $\forall k \in K : A_j(k) \neq 0$
then $S_k(X)$ is not the zero-polynomial.

$$1 \leq \deg(S_k(X)) \leq n - 1$$

\Downarrow

Not all the n roots of $x^n - 1$ are roots of $S_k(X)$.

\Downarrow

$$\exists t, 0 \leq t \leq n - 1 : S_k(\beta^t) \neq 0.$$

\Downarrow

$$\tilde{\lambda}_t(\beta^k)\tilde{a}(\beta^k) \neq 0.$$

\Downarrow

$$\tilde{a}(\beta^k) \neq 0.$$

We deduce:

$$(\tilde{c} \otimes \tilde{c})(\beta^k) = 0 \Rightarrow \tilde{a}(\beta^k) \neq 0.$$

$$\tilde{a}(\beta^k) = 0 \Rightarrow (\tilde{c} \otimes \tilde{c})(\beta^k) \neq 0.$$

$$\tilde{a}(\beta^k) = 0 \Rightarrow \tilde{e}(\beta^k) = 0.$$

which means that $\tilde{a}(x)$ divides $\tilde{e}(x)$.

EXAMPLE

$$n = 21$$

$$\mathbb{F}_{64} = \mathbb{F}(\alpha), \beta = \alpha^3$$

$\tilde{m}_i(x)$: minimal polynomial of β^i over \mathbb{F}_2 .

$$x^{21} - 1 = \tilde{m}_0(x)\tilde{m}_1(x)\tilde{m}_3(x)\tilde{m}_5(x)\tilde{m}_7(x)\tilde{m}_9(x)$$

$$\tilde{a}(x) = \tilde{m}_7(x)$$

$$\tilde{b}(x) = \tilde{m}_3(x)\tilde{m}_5(x)\tilde{m}_9(x)$$

$$\tilde{c}(x) = \tilde{m}_0(x)\tilde{m}_1(x)$$

$$(\tilde{c} \circledast \tilde{c})(x) = \tilde{m}_0(x)\tilde{m}_1(x)\tilde{m}_3(x)\tilde{m}_5(x)\tilde{m}_9(x)$$

$$\tilde{e}(x) = \tilde{m}_7(x)$$

$a(x), b(x), c(x)$ Hensel lifts of $\tilde{a}(x), \tilde{b}(x), \tilde{c}(x)$.

C : linear cyclic code C over \mathbb{Z}_4 of length 21 generated by $g(x) = a(x)[b(x) + 2]$.

$\psi(C)$ is the binary linear cyclic code of length 42 generated by $\tilde{a}(x)^2 \tilde{b}(x)$.

Finding, for a given odd n , all linear cyclic codes C over \mathbb{Z}_4 of length n whose Nechaev-Gray images are binary linear cyclic codes.

For each divisor $\tilde{c}(x)$ of $x^n - 1$ over \mathbb{F}_2 :

1) Calculate $(\tilde{c} \circledast \tilde{c})(x)$.

2) Determine $\tilde{e}(x)$ such that :

$$x^n - 1 = (\tilde{c} \circledast \tilde{c})(x)\tilde{e}(x) \text{ over } \mathbb{F}_2.$$

3) For each divisor $\tilde{a}(x)$ of $\tilde{e}(x)$ over \mathbb{F}_2 :

(i) Determine $\tilde{b}(x)$ such that :

$$x^n - 1 = \tilde{a}(x)\tilde{b}(x)\tilde{c}(x) \text{ over } \mathbb{F}_2.$$

(ii) Calculate the Hensel lifts $a(x)$, $b(x)$, $c(x)$ of $\tilde{a}(x)$, $\tilde{b}(x)$, $\tilde{c}(x)$.

(iii) Calculate the generator of C :

$$g(x) = a(x)[b(x) + 2] \text{ of } C.$$

C : \mathbb{Z}_4 -linear cyclic code of odd length n ,
 $g(x)$: generator of C .

Question :

We know when $\psi(C)$ is a linear cyclic code (equivalent to : $\phi(C)$ linear code).

When $\phi(C)$ is a linear cyclic code ?

Theorem 31 (W. 2000) n odd.

A) The following properties are equivalent :

- 1) $\phi(C)$ is a binary linear cyclic code.*
- 2) C is a negacyclic code.*
- 3) $g(x) = 2d(x)$ or $g(x) = d(x) + 2$
where $d(x)$ is a divisor of $x^n - 1$ in $\mathbb{Z}_4[x]$.*

B) If $g(x) = 2d(x)$ then $\phi(C)$ is the binary linear cyclic code of length $2n$ generated by $\tilde{d}(x)(x^n - 1)$.

If $g(x) = d(x) + 2$ then $\phi(C)$ is the binary linear cyclic code of length $2n$ generated by $\tilde{d}(x)$.

Summary

n odd,

ϕ : Gray , ψ : Nechaev-Gray .

C : linear cyclic code over \mathbb{Z}_4 of length n .

$g(x)$: generator of C .

$\phi(C)$ linear code

\Updownarrow

$\psi(C)$ linear cyclic code

$\phi(C)$ linear cyclic code

\Updownarrow

$$\left\{ \begin{array}{l} g(x) = 2d(x) \text{ or } g(x) = d(x) + 2 \\ \text{(with } d(x) \text{ divisor of } x^n - 1) \end{array} \right.$$

Nechaev-Gray map better than Gray-map

Examples

Theorem 32

n odd.

$C : [n, a(x), b(x), c(x)]$ code.

$\psi : \text{Nechaev-Gray map.}$

If $c(x) = x^s - 1$ where s is a divisor of n , then:

$\psi(C)$ is a linear cyclic code of length $2n$.

Special case : $n = 2^t - 1, c(x) = x - 1$.

Proof

{roots of $\tilde{c}(x)$ } = mult.sub-group of order s .

Hence $(\tilde{c} \circledast \tilde{c})(x) = \tilde{c}(x)$.

$$x^n - 1 = \tilde{a}(x)\tilde{b}(x)\tilde{c}(x) = \tilde{e}(x)(\tilde{c} \circledast \tilde{c})(x)$$

and $\tilde{a}(x)$ divides $\tilde{e}(x)$.

Special divisors of $x^n - 1$ over \mathbb{F}_2 :

Binary weight: if $i = \sum_{j=0}^{r-1} \epsilon_j 2^j \in \mathbb{N}$ then
 $w_2(i) = \text{weight of } (\epsilon_0, \epsilon_1, \dots, \epsilon_j, \dots, \epsilon_{r-1})$

α : primitive root of $\mathbb{F}_{2^{2t-1}}$

- $\tilde{m}_i(x)$: minimal polynomial of α^i over \mathbb{F}_2 .
- $\tilde{\pi}_j(x)$: product, without repetition, of the $\tilde{m}_i(x)$ such that $w_2(i) = j$.
- $\tilde{M}_u(x) = \prod_{1 \leq w_2(j) \leq u} \tilde{\pi}_j(x) \quad (u \geq 1)$
- $\tilde{M}_0(x) = 1$

Example: $t = 3, n = 31$.

$$\begin{aligned} x^{31} - 1 = & \\ & \tilde{m}_0(x)\tilde{m}_1(x)\tilde{m}_3(x)\tilde{m}_5(x)\tilde{m}_7(x)\tilde{m}_{11}(x)\tilde{m}_{15}(x) = \\ & (x-1)(x^5+x^2+1)(x^5+x^4+x^3+x^2+1)(x^5+x^4+x^2+x+1) \\ & (x^5+x^3+x^2+x+1)(x^5+x^4+x^3+x+1)(x^5+x^3+1) \end{aligned}$$

$$\begin{aligned} w_2(i) = 1 : i = 1, \quad w_2(i) = 2 : i = 3, 5 \\ w_2(i) = 3 : i = 7, 11, \quad w_2(i) = 4 : i = 15. \end{aligned}$$

$$\tilde{\pi}_1(x) = \tilde{m}_1(x) = (x^5 + x^2 + 1)$$

$$\begin{aligned} \tilde{\pi}_2(x) &= \tilde{m}_3(x)\tilde{m}_5(x) \\ &= (x^5 + x^4 + x^3 + x^2 + 1)(x^5 + x^4 + x^2 + x + 1). \end{aligned}$$

$$\begin{aligned} \tilde{\pi}_3(x) &= \tilde{m}_7(x)\tilde{m}_{11}(x) \\ &= (x^5 + x^3 + x^2 + x + 1)(x^5 + x^4 + x^3 + x + 1) \end{aligned}$$

$$\tilde{\pi}_4(x) = \tilde{m}_{15}(x) = (x^5 + x^3 + 1).$$

$$\tilde{M}_1(x) = \tilde{\pi}_1(x) = \tilde{m}_1(x),$$

$$\tilde{M}_2(x) = \tilde{\pi}_1(x)\tilde{\pi}_2(x) = \tilde{m}_1(x)\tilde{m}_3(x)\tilde{m}_5(x).$$

$$\tilde{M}_3(x) = \tilde{\pi}_1(x)\tilde{\pi}_2(x)\tilde{\pi}_3(x) = \tilde{m}_1(x)\tilde{m}_3(x)\tilde{m}_5(x)\tilde{m}_7(x)\tilde{m}_{11}(x).$$

Theorem 33 $n = 2^t - 1$.

α : primitive root of \mathbb{F}_{2^t} .

$\tilde{m}_1(x)$: minimal polynomial of α over \mathbb{F}_2 .

$m_1(x), \pi_2(x)$: Hensel lifts of $\tilde{m}_i(x), \tilde{\pi}_2(x)$.

ψ : Nechaev-Gray map.

C : $[n, a(x), b(x), c(x)]$ code.

If

- 1) $c(x) = m_1(x)$ or $c(x) = (x-1)m_1(x)$,
- 2) $\pi_2(x)$ divides $b(x)$,

then $\psi(C)$ is a linear cyclic code.

Proof

$$\{\text{roots of } \tilde{c}(x)\} = \Gamma(\alpha) = \{\alpha, \alpha^2, \dots, \alpha^{2^i}, \dots, \alpha^{2^t-1}\}$$
$$\text{or} = \{1\} \cup \Gamma(\alpha).$$

$$(\tilde{c} \circledast \tilde{c})(x) = \tilde{\pi}_2(x)$$

$$\text{or} = \tilde{c}(x)\tilde{\pi}_2(x)$$

$$x^n - 1 = \tilde{a}(x)\tilde{b}(x)\tilde{c}(x) = \tilde{e}(x)(\tilde{c} \circledast \tilde{c})(x)$$

$$= \tilde{e}(x)\tilde{\pi}_2(x)$$

$$\text{or} = \tilde{e}(x)\tilde{c}(x)\tilde{\pi}_2(x).$$

If $\pi_2(x)$ divides $b(x)$ then $\tilde{a}(x)$ divides $\tilde{e}(x)$.

Reed-Muller code of order one as doubly extended Nechaev-Gray image

Theorem 34

$$n = 2^t - 1.$$

α : primitive root of \mathbb{F}_{2^t} .

$\tilde{m}_\alpha(x)$: minimal polynomial of α over \mathbb{F}_2 .

$$x^n - 1 = (x - 1)\tilde{m}_\alpha(x)\tilde{h}(x) \text{ over } \mathbb{F}_2.$$

$m_\alpha(x)$: Hensel lift of $\tilde{m}_\alpha(x)$.

$h(x)$: Hensel lift of $\tilde{h}(x)$.

ψ : Nechaev-Gray map.

C : linear cyclic code over \mathbb{Z}_4 of length n generated by $h(x)(m_\alpha(x) + 2)$.

1) $\psi(C)$ is the binary linear cyclic code of length $2n$ generated by $\tilde{h}(x)^2 \tilde{m}_\alpha(x)$.

2) If C^+ is the extended code of C then $\psi(C^+)$ is the Reed-Muller code of order one of length 2^{t+1} .

Remark :

$\psi(C^+) = \psi(C)^{++}$ doubly extended binary linear cyclic code.

Tools for a proof

$\psi(C)$ linear cyclic code.

$$\begin{aligned} \tilde{c}(x) &= x - 1, \quad (\tilde{c} \circledast \tilde{c})(x) = \tilde{c}(x), \\ \tilde{e}(x) &= \tilde{a}(x)\tilde{b}(x) \text{ thus } \tilde{a}(x) \text{ divides } \tilde{e}(x). \end{aligned}$$

$\psi(C^+)$ Reed-Muller code.

Generator of the simplex code of length $2^t - 1$ defined by α :

$$\tilde{s}(x) = (x - 1)\tilde{h}(x) = \sum_{i=0}^{n-t} \tilde{s}_i x^i.$$

Generator matrix of the simplex code:

$$S_t = \begin{pmatrix} \tilde{s}_0 & \tilde{s}_1 & \dots & \tilde{s}_{n-t} & 0 & \dots & \dots & 0 \\ 0 & \tilde{s}_0 & \tilde{s}_1 & \dots & \tilde{s}_{n-t} & 0 & \dots & 0 \\ 0 & 0 & \tilde{s}_0 & \tilde{s}_1 & \dots & \tilde{s}_{n-t} & 0 & \dots \\ \vdots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & 0 & \tilde{s}_0 & \tilde{s}_1 & \dots & \tilde{s}_{n-t} \end{pmatrix}$$

Generator matrix of the Reed-Muller code of order one and length 2^{t+1} :

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 & 1 & 1 & 1 & 1 & \dots & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 1 & 1 & 1 & \dots & 1 & 1 \\ & & & & & & 0 & & & & & & & 0 \\ & & & & & & \vdots & & & & & & & \vdots \\ & & & & & & 0 & & & & & & & 0 \\ & & & & & & 0 & & & & & & & 0 \\ & & & & & & & & & & & & & \vdots \end{pmatrix} \begin{matrix} \rho_0 \\ \rho_1 \\ \vdots \\ \rho_i \\ \vdots \\ \vdots \\ \vdots \end{matrix}$$

$$\begin{aligned} \mathcal{P}_4^n(C) &= \langle a(x)b(x) \rangle_4^n + \langle 2a(x) \rangle_4^n \\ &= \langle h(x)m_\alpha(x) \rangle_4^n + \langle 2h(x) \rangle_4^n \\ &= \langle \sum_{i=0}^{n-1} x^i \rangle_4^n + \langle 2h(x) \rangle_4^n. \end{aligned}$$

ρ_0 : Gray image of $2 \sum_{i=0}^{n-1} x^i$ extended.

ρ_1 : Gray image of $\sum_{i=0}^{n-1} x^i$ extended.

ρ_i : Gray image of $x^{i-2}\tilde{s}(x) = x^{i-2}(x - 1)\tilde{h}(x)$ extended.

$\dim(C^+) = \dim \phi(C^+) = \dim(\text{Reed-Muller of order one})$.

Conclusion: $\phi(C^+) = \text{Reed-Muller of order one}$.

$\psi(C^+)$ equivalent to $\phi(C^+)$ since Nechaev permutation permutes words components of $\phi(C)$.

Reed-Muller code of order two as doubly extended Nechaev-Gray image

Theorem 35 $n = 2^t - 1$.

α : primitive root of \mathbb{F}_{2^t} .

$\tilde{m}_\alpha(x)$: minimal polynomial of α over \mathbb{F}_2 .

$m_\alpha(x), \pi_2(x)$: Hensel lifts of $\tilde{m}_\alpha(x), \tilde{\pi}_2(x)$.

ψ : Nechaev-Gray map.

C : linear cyclic code over \mathbb{Z}_4 of length n

generated by $a(x)(b(x) + 2)$ with

$x^n - 1 = a(x)b(x)c(x)$ and

$c(x) = (x - 1)m_\alpha(x), b(x) = \pi_2(x)$

C^+ : extended code.

then

$\psi(C^+)$ is the reed- Muller code of order two of length 2^{t+1} .

Remark :

$\psi(C^+) = \psi(C)^{++}$ doubly extended binary linear cyclic code.

TWO KIND OF \mathbb{Z}_4 CYCLIC CODES

Two kind of \mathbb{Z}_4 -Cyclic Codes

$x^n - 1 = \tilde{a}(x)\tilde{b}(x)\tilde{c}(x)$ in $\mathbb{F}_2[x]$, n odd,
 $a(x), b(x), c(x)$: Hensel lifts of $\tilde{a}(x), \tilde{b}(x), \tilde{c}(x)$,

Polynomial representation:

$$\text{(Type A)} : \langle a(x)b(x) + 2a(x) \rangle_4^n$$

$$\text{(Type B)} : \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n + 2 \langle \tilde{a}(x) \rangle_2^n$$

Fact 1

Let \tilde{C}_1 and \tilde{C}_2 be two \mathbb{F}_2 -**linear** codes of odd length n .

$C = \tilde{C}_1 + 2\tilde{C}_2$ is a \mathbb{Z}_4 -**linear** code if and only if :

$$(*) \quad \tilde{C}_1 * \tilde{C}_1 \subseteq \tilde{C}_2$$

Remarks:

1) If \tilde{C}_1 and \tilde{C}_2 binary **linear cyclic** then C is a type (B) code.

2) **Condition (*) is not trivial to check and we need a more practical one.**

The two following facts are previous results.

Fact 2

Every \mathbb{Z}_4 -linear cyclic code C of odd length n is of type (A).

Fact 3 (Main Theorem) Let n be odd.

If C is a type (A) code and if $\tilde{e}(x)$ is such that $x^n - 1 = (\tilde{c} \circledast \tilde{c})(x)\tilde{e}(x)$ in $\mathbb{F}_2[x]$, then :

(I) The following properties are equivalent :

$$(*) \quad \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n * \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n \subseteq \langle \tilde{a}(x) \rangle_2^n.$$

(**) $\psi(C)$ is a binary linear cyclic code.

(***) $\tilde{a}(x)$ divides $\tilde{e}(x)$ in $\mathbb{F}_2[x]$.

(II) If one of these conditions is satisfied then

$$\psi(C) = \langle \tilde{a}(x)^2 \tilde{b}(x) \rangle_2^{2n}$$

.

Open problems

(Type A) : $\langle a(x)b(x) + 2a(x) \rangle_4^n$

(Type B) : $\langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n + 2 \langle \tilde{a}(x) \rangle_2^n$

P_1 : When type (B) codes are \mathbb{Z}_4 -linear ?
(find a better condition than (*))

P_2 : When is $\langle a(x)b(x) + 2a(x) \rangle_4^n$ equal to
 $\langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n + 2 \langle \tilde{a}(x) \rangle_2^n$?

P_3 : What are the Nechaev-Gray images of
type (B) codes ?

n odd.

ψ_P : Polynomial Nechaev-Gray map.

Recall that if $f(x) = \tilde{r}(x) + 2\tilde{q}(x) \in \mathcal{A}_4(n)$ with $\tilde{r}(x)$ and $\tilde{q}(x)$ in $\mathcal{A}_2(n)$. then :

$$\psi_P(f(x)) = (x^n + 1)\tilde{q}(x) \oplus x \frac{d}{dx} [(x^n + 1)\tilde{r}(x)]$$

Theorem 36

If C is a type (B) code of odd length n and ψ is the Nechaev-Gray map, then $\psi(C)$ is a binary linear cyclic code of length $2n$.

More precisely,

if $\mathcal{P}_4^n(C) = \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^{+2} + 2 \langle \tilde{a}(x) \rangle_2^n$, then $\psi(C)$ is generated by $\tilde{a}(x)^2\tilde{b}(x)$.

Corollary 37

The set of binary linear cyclic codes of length $2n$, n odd, is the set of Nechaev-Gray images of the type (B) codes of length n .

Proof:

$$x^n - 1 = \tilde{a}(x)\tilde{b}(x)\tilde{c}(x) \text{ in } \mathbb{F}_2[x].$$

- $\psi_P(C) \subseteq \langle \tilde{a}(x)^2\tilde{b}(x) \rangle_2^{2n}$.

Typical word of $\mathcal{P}_4^n(C)$:

$$f(x) = \tilde{\lambda}(x)\tilde{a}(x)\tilde{b}(x) + 2\tilde{\mu}(x)\tilde{a}(x).$$

Lemma and $\frac{d}{dx}[\tilde{a}(x)^2\tilde{b}(x)^2] = 0$ give:

$$\psi_P(f(x)) =$$

$$\tilde{\mu}(x)\tilde{a}(x)^2\tilde{b}(x)\tilde{c}(x) \oplus x\tilde{a}(x)^2\tilde{b}(x)^2 \frac{d}{dx}[\tilde{\lambda}(x)\tilde{c}(x)]$$

thus $\psi_P(f(x))$ belongs to $\langle \tilde{a}(x)^2\tilde{b}(x) \rangle_2^{2n}$.

- Cardinality of $\psi_P(C)$:

$$I_1 = \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n, I_2 = \langle \tilde{a}(x) \rangle_2^n$$

$I_1 + 2I_1$ is a direct sum (easy).

$$|C| = |I_1| \parallel |I_2| = 4^{\deg \tilde{c}(x)} 2^{\deg \tilde{b}(x)}$$

$$= |\langle \tilde{a}(x)^2\tilde{b}(x) \rangle_2^{2n}|.$$

ψ_P bijective map, then $|\psi_P(C)| = |\langle \tilde{a}(x)^2\tilde{b}(x) \rangle_2^{2n}|$.

- Conclusion:

$$\psi_P(C) = \langle \tilde{a}(x)^2\tilde{b}(x) \rangle_2^{2n}$$

\mathbb{Z}_4 -linearity of type (B) codes

Theorem 38 (*n odd*)

Let $\tilde{e}(x)$ be such that $x^n - 1 = (\tilde{c} \circledast \tilde{c})(x)\tilde{e}(x)$ in $\mathbb{F}_2[x]$.

The conditions below are equivalent :

- 1) $\langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n + 2 \langle \tilde{a}(x) \rangle_2^n$
is a linear code.
- 2) $\tilde{a}(x)$ divides $\tilde{e}(x)$ in $\mathbb{F}_2[x]$.
- 3) $\langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n + 2 \langle \tilde{a}(x) \rangle_2^n$
 $= \langle a(x)(b(x) + 2) \rangle_4^n$.

Remarks :

a) If one of the conditions of the Theorem is true, then :

$$\psi(\langle a(x)b(x) + 2a(x) \rangle_4^n) = \langle \tilde{a}(x)^2\tilde{b}(x) \rangle_2^{2n}.$$

b) In order to solve P_1 , condition 2) above is better than condition (*) of Fact 3, which is uneasy to check.

A family of \mathbb{Z}_4 -self-dual linear cyclic codes

Question :

$C = \tilde{C}_1 + 2\tilde{C}_2$, where \tilde{C}_1 and \tilde{C}_2 are binary linear cyclic linear codes.

When C is a \mathbb{Z}_4 -self-dual linear code ?

Definition 39

Let \tilde{C} be a binary code and let s be any integer, $s \geq 1$.

The code \tilde{C} is said to be s -divisible if the weight of every word of \tilde{C} is divisible by s .

Lemma 40 (From Mc Eliece)

\tilde{C} : \mathbb{F}_2 -linear cyclic code of odd length n with generator $\tilde{g}(x)$ such that $x^n - 1 = \tilde{g}(x)\tilde{h}(x)$ in $\mathbb{F}_2[x]$.

R : the set of roots of $\tilde{h}(x)$ in the splitting field of $x^n - 1$ over $\mathbb{F}_2[x]$.

If t is the smallest integer such that $\beta_1\beta_2 \cdots \beta_t = 1$ where $\beta_1, \beta_2, \dots, \beta_t$ are in R , then :

\tilde{C} is 2^{t-1} -divisible and is not 2^t -divisible.

As a consequence of the previous lemma we have the next corollary :

Corollary 41

With the above notations, let $\tilde{h}^(x)$ be the reciprocal polynomial of $\tilde{h}(x)$.*

The code \tilde{C} is 2^s -divisible with $s \geq 3$ if and only if $((\tilde{h} \circledast \tilde{h})(x), \tilde{h}^(x)) = 1$.*

Theorem 42

Let \tilde{C}_1 and \tilde{C}_2 be two binary linear cyclic codes of odd length n .

Then the code $C = \tilde{C}_1 + 2\tilde{C}_2$ is a \mathbb{Z}_4 -self-dual linear code if and only if

$$\tilde{C}_2 = \tilde{C}_1^\perp \text{ and } \tilde{C}_1 \text{ is 8-divisible.}$$

Starting point of the proof:

$C = \tilde{C}_1 + 2\tilde{C}_2$ is a \mathbb{Z}_4 -linear code then

$\tilde{C}_1 * \tilde{C}_1 \subseteq \tilde{C}_2$ which implies $\tilde{C}_1 \subseteq \tilde{C}_2$.

Then there exist $\tilde{a}(x)$ and $\tilde{b}(x)$ such that

$\tilde{a}(x)\tilde{b}(x)$ divides $x^n - 1$ in $\mathbb{F}_2[x]$ and

$\tilde{C}_1 = \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n$, $\tilde{C}_2 = \langle \tilde{a}(x) \rangle_2^n$.

In other words, C is a \mathbb{Z}_4 -linear type (B) code.

Hence $C = \langle a(x)b(x) + 2a(x) \rangle_4^n$

with $a(x)$, $b(x)$, $c(x)$ Hensel lifts.

The sequel of the proof use the description of C^\perp and Corollary 41.

(see reference [8] for details).

Corollary 43

Let \tilde{C}_1 and \tilde{C}_2 be two binary linear cyclic codes of odd length n and minimum distances d_1 and d_2 respectively.

If $C = \tilde{C}_1 + 2\tilde{C}_2$ is a \mathbb{Z}_4 -self-dual linear code of odd length n then :

$\psi(C)$ is a \mathbb{F}_2 -self-dual linear cyclic code of length $2n$ and minimum distance $\min(d_1, 2d_2)$.

Corollary 44 (Example)

If \tilde{C} is the dual code of the 2-correcting BCH binary code of length $2^m - 1$ with $m \geq 5$ if m is odd and $m \geq 8$ if m is even, then $\tilde{C} + 2\tilde{C}^\perp$ is a \mathbb{Z}_4 -self-dual linear code.

REFERENCES

- [1] A. R. Calderbank and N. J. A. Sloane, "Modular and p -adic Cyclic Codes" *Designs, Codes and Cryptography*, vol. 6, no. 1, pp. 21–35, 1995.
- [2] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The \mathbb{Z}_4 -linearity of Kerdock, Preparata, Goethals, and related codes" *IEEE Trans. Inform. Theory*, vol. 40, pp. 301-319, 1994.
- [3] P. Kanwar and S. R. López-Permouth, "Cyclic Codes Over the Integers Modulo p^m " *Finite Fields and Their Applications*, vol. 3, pp. 334–352, 1997.
- [4] V. S. Pless, Z. Qian, "Cyclic Codes and Quadratic Residue Codes Over \mathbb{Z}_4 " *IEEE Trans. Inform. Theory*, vol. 42, pp. 1594-1600, 1996.
- [5] V. S. Pless, W. C. Huffman, *Handbook of Coding Theory* Elsevier, Amsterdam, 1998.
- [6] V. S. Pless, P. Solé, Z. Qian, "Cyclic Self-Dual \mathbb{Z}_4 -Codes" *Finite Fields and Their Applications*, vol. 3, pp. 48-69, 1997.
- [7] H. Tapia-Recillas, G. Vega, "Some Constacyclic Codes over \mathbb{Z}_{2^k} and Binary Quasi-cyclic Codes", *Discrete Applied Mathematics*, vol. 128(1), pp.305-316, 2003.
- [8] G. Vega, J. Wolfmann, "Some families of \mathbb{Z}_4 -cyclic codes", *Finite Field and Their Applications*, vol. 10, pp 530-539, 2004.
- [9] J. Wolfmann, "Negacyclic and Cyclic Codes Over \mathbb{Z}_4 " *IEEE Trans. Inform. Theory*, vol. 45, pp. 2527-2532, 1999.
- [10] J. Wolfmann, "Binary Images of Cyclic Codes Over \mathbb{Z}_4 " *IEEE Trans. Inform. Theory*, vol. 47, pp. 1773-1779, 2001.