On quasi-cyclic codes as a generalization of cyclic codes

Morgan Barbier
morgan.barbier@unicaen.fr

Joint work with:
Christophe Chabot
Guillaume Quintin

University of Caen – GREYC

Dinard, C2
October 9th 2012

GREYC
PROTECTION DE L'INFORMATION, CRYPTOGRAPHIE, CODES

Outline

Introduction

Definition

Let $\ell, m \in \mathbb{N}$. A code $\mathcal{C} \subset \mathbb{F}_q^{m\ell}$ is called *ℓ-quasi-cyclic* of length $m\ell$ iff

$$\forall c = (c_{11}, \ldots, c_{1\ell} | \ldots | c_{(m-1)1}, \ldots, c_{(m-1)\ell} | c_{m1}, \ldots, c_{m\ell}) \in \mathcal{C}$$

$$\Longrightarrow (c_{m1}, \ldots, c_{m\ell} | c_{11}, \ldots, c_{1\ell} | \ldots | c_{(m-1)1}, \ldots, c_{(m-1)\ell}) \in \mathcal{C}.$$

Introduction

Definition

Let $\ell, m \in \mathbb{N}$. A code $\mathcal{C} \subset \mathbb{F}_q^{m\ell}$ is called *ℓ-quasi-cyclic* of length $m\ell$ iff

$$\forall c = (c_{11}, \ldots, c_{1\ell} | \ldots | c_{(m-1)1}, \ldots, c_{(m-1)\ell} | c_{m1}, \ldots, c_{m\ell}) \in \mathcal{C}$$

$$\Longrightarrow (c_{m1}, \ldots, c_{m\ell} | c_{11}, \ldots, c_{1\ell} | \ldots | c_{(m-1)1}, \ldots, c_{(m-1)\ell}) \in \mathcal{C}.$$

$\Longrightarrow \mathcal{C} \subset (\mathbb{F}_{q^\ell})^m$ is cyclic

Introduction

Definition

Let $\ell, m \in \mathbb{N}$. A code $\mathcal{C} \subset \mathbb{F}_q^{m\ell}$ is called *ℓ-quasi-cyclic* of length $m\ell$ iff

$$\forall c = (c_{11}, \dots, c_{1\ell} | \dots | c_{(m-1)1}, \dots, c_{(m-1)\ell} | c_{m1}, \dots, c_{m\ell}) \in \mathcal{C}$$

$$\Longrightarrow (c_{m1}, \dots, c_{m\ell} | c_{11}, \dots, c_{1\ell} | \dots | c_{(m-1)1}, \dots, c_{(m-1)\ell}) \in \mathcal{C}.$$

$\Longrightarrow \mathcal{C} \subset (\mathbb{F}_{q^\ell})^m$ is cyclic but not necessary $\mathbb{F}_{q^\ell}$-linear.

Bijection

Theorem

There is a one-to-one correspondence between ℓ-quasi-cyclic codes over $\mathbb{F}_q$ of length $m\ell$ and left ideals of $M_\ell(\mathbb{F}_q)[X]/(X^m - 1)$.

Sketch of proof: There are one-to-one correspondence between:

1. ℓ-quasi-cyclic codes over $\mathbb{F}_q$ of length ℓm
2. submodule of $(\mathbb{F}_q[X]/(X^m - 1))^\ell$
3. left ideal of $M_\ell(\mathbb{F}_q[X]/(X^m - 1))$
4. left ideal of $M_\ell(\mathbb{F}_q)[X]/(X^m - 1)$.

2 to 3 is given by the Morita equivalence. $\square$

From theory to practice I

How to built a ℓ-quasi-cyclic code from a left ideal $M_\ell(\mathbb{F})[X]/(X^m - 1)$?

From theory to practice I

How to built a ℓ-quasi-cyclic code from a left ideal $M_\ell(\mathbb{F})[X]/(X^m - 1)$?

Proposition

Let $\mathcal{I} = \langle P_1(X), \ldots, P_r(X)\rangle$ be a left ideal of $M_\ell(\mathbb{F}_q)[X]/(X^m - 1)$. Then the $\mathbb{F}_q$-linear space spanned by

$$\left\{\mathrm{row}_k(X^i P_j(X)) : i = 0, \ldots, m-1,\ j = 1, \ldots, r,\ k = 1, \ldots, \ell\right\}$$

is a ℓ-quasi-cyclic code of length $m\ell$ over $\mathbb{F}_q$, where

$$\begin{array}{rcl} \mathrm{row}_k : M_\ell(\mathbb{F}_q)[X]/(X^m - 1) & \longrightarrow & \mathbb{F}_q^{m\ell} \\ P(X) = \sum_{j=0}^{m-1} P_j X^j & \longmapsto & (\mathrm{row}_k(P_0), \ldots, \mathrm{row}_k(P_{m-1})). \end{array}$$

From theory to practice II

How to built a left ideal from a ℓ-quasi-cyclic code?

Outline

Block rank

Proposition

Let $\mathcal{C}$ be an ℓ-quasi-cyclic code over $\mathbb{F}_q$ of dimension k and length $m\ell$. Then there exists an integer r such that $1 \leq r \leq k$ and for all generator matrix G of $\mathcal{C}$ and for all $i = 0, \ldots, m-1$, the rank of the $i+1, \ldots, i+\ell$ columns of G is r, and is called the block rank.

Proposition

There exist $g_1, \ldots, g_r$ linearly independent vectors of C such that $g_1, \ldots, g_r, T(g_1), \ldots, T(g_r), \ldots, T^{m-1}(g_1), \ldots, T^{m-1}(g_r)$ span C.

Generator polynomial

Definition (Generator polynomial)

Let

$$G_i = \begin{pmatrix} g_{1,i\ell+1} & \cdots & g_{1,(i+1)\ell} \\ \vdots & & \vdots \\ g_{r,i\ell+1} & \cdots & g_{r,(i+1)\ell} \\ & 0 & \end{pmatrix} \in M_\ell(\mathbb{F}_q),$$

and ν the smallest integer such that $G_\nu \neq 0$. We call

$$g(X) = \frac{1}{X^\nu} \sum_{i=0}^{m-1} G_i X^i \in M_\ell(\mathbb{F}_q)[X],$$

the *generator polynomial* of $\mathcal{C}$ and $\mathcal{C}$ corresponds to the left ideal spanned by $\langle g(X) \rangle$.

Property

Proposition

Let $\mathcal{C}$ be an ℓ-quasi-cyclic code of length $m\ell$ over $\mathbb{F}_q$. Let $P(X)$ be a generator polynomial of $\mathcal{C}$ and $Q(X)$ a generator polynomial of its dual. Then

$$P(X)\ {}^tQ^*(X) \equiv 0 \mod (X^m - 1)$$

where $Q^*(X) = X^{\deg Q} Q(1/X)$ denotes the reciprocal polynomial of Q and ${}^tQ$ the polynomial whose coefficients are the transposed matrices of the coefficients of Q.

Outline

Definition (Generalized Reed-Solomon codes)

Let $\mathcal{R}$ be a finite ring, $n \geq k \in \mathbb{N}$ be two integers, $(x_i)_{i=1,\ldots,n} \in \mathcal{R}^n$ be a subtractive set, and $v_i \in \mathcal{R}^n$ be n invertible elements of $\mathcal{R}$. We define

$$\mathrm{GRS}_{ll}(v, x, k) = \{(v_1\, \mathrm{ev}_l(P, x_1), \ldots, v_n\, \mathrm{ev}_l(P, x_n)) : P \in \mathcal{R}[X]_{<k}\}.$$

We can also define 3 other GRS codes.

Outline

From theory...

Remark (Thanks to Coste)

Let $\mathcal{R}$ be any finite ring, $n < m$ be two positive integers and $M \in M_{n\times m}(\mathcal{R})$. Then there exists a nonzero $x \in \mathcal{R}^m$ such that $Mx = 0$.

Proposition

Let $P \in \mathcal{R}[X]$ of degree at most n with at least $n+1$ roots contained in a commutative subtractive subset of A. Then $P = 0$.

...to practice

Algorithm 1: Welch-Berlekamp

Input : A received vector y of $\mathcal{R}^n$ with at most $t = \left\lfloor \frac{n-k}{2} \right\rfloor$ errors.
Output: The unique codeword within distance t of y.

début

$y' \leftarrow (v_1^{-1} y_1, \ldots, v_n^{-1} y_n)$,
compute $Q = Q_0(X) + Q_1(X)Y \in (\mathcal{R}[X])[Y]$

1. $Q(x_i, y_i') = 0$ for all $1 \leq i \leq n$,
2. $\deg Q_0 \leq n - t - 1$,
3. $\deg Q_1 \leq n - t - 1 - (k-1)$.
4. The leading coefficient of Q_1 is 1_A.

$P \leftarrow$ the unique root of Q in $\mathcal{R}[X]_{<k}$,
return $(v_1 \, \mathrm{ev}_I(P, x_1), \ldots, v_n \, \mathrm{ev}_I(P, x_n))$.

Outline

A primitive root of unity

Definition

Let q be a prime power. A matrix $A \in M_\ell(\mathbb{F}_{q^s})$ is called a *primitive m-th root of unity* if

- $A^m = I_\ell$,
- $A^i \neq I_\ell$ if $i < m$,
- $\det(A^i - A^j) \neq 0$, whenever $i \neq j$, that is power of A are a subtractive set.

Quasi-BCH codes

Definition (Left quasi-BCH codes)

Let A be a primitive m-th root of unity in $M_\ell(\mathbb{F}_{q^s})$ and $\delta \le m$. We define the *left ℓ-quasi-BCH code* of length $m\ell$, with respect to A, with designed minimum distance δ, over $\mathbb{F}_q$ by

$$\text{Q-BCH}_l(m,\ell,\delta,A) =$$
$$\left\{ (c_1,\dots,c_m) \in (\mathbb{F}_q^\ell)^m : \sum_{j=0}^{m-1} A^{ij} c_{j+1} = 0 \text{ for } i = 1,\dots,\delta-1 \right\}.$$

Similarly, we can define the *right ℓ-quasi-BCH codes*.

Outline

Q-BCH code as a cyclic RS code

Proposition

A study of the orthogonal codes gives

$$\begin{aligned}\text{Q-BCH}_l(m,\ell,\delta,A) &= \text{row}_1(\text{RS}_l((A^i)_{i=1,\ldots,m}, m-\delta+1))\\ \text{Q-BCH}_r(m,\ell,\delta,A) &= \text{row}_1(\text{RS}_r((A^i)_{i=1,\ldots,m}, m-\delta+1)).\end{aligned}$$

$\Longrightarrow$ Use the Welch-Berlekamp algorithm to decode the Q-BCH codes.

Conclusion I

New codes over $\mathbb{F}_4$			
$[171, 11, 109]_{\mathbb{F}_4}$	$[172, 11, 110]_{\mathbb{F}_4}$	$[173, 11, 110]_{\mathbb{F}_4}$	$[174, 11, 111]_{\mathbb{F}_4}$
$[175, 11, 112]_{\mathbb{F}_4}$	$[176, 11, 113]_{\mathbb{F}_4}$	$[177, 11, 114]_{\mathbb{F}_4}$	$[178, 11, 115]_{\mathbb{F}_4}$
$[179, 11, 115]_{\mathbb{F}_4}$	$[180, 11, 116]_{\mathbb{F}_4}$	$[181, 11, 117]_{\mathbb{F}_4}$	$[182, 11, 118]_{\mathbb{F}_4}$
$[183, 11, 119]_{\mathbb{F}_4}$	$[184, 10, 121]_{\mathbb{F}_4}$	$[184, 11, 120]_{\mathbb{F}_4}$	$[185, 10, 122]_{\mathbb{F}_4}$
$[185, 11, 121]_{\mathbb{F}_4}$	$[186, 10, 123]_{\mathbb{F}_4}$	$[186, 11, 122]_{\mathbb{F}_4}$	$[187, 10, 124]_{\mathbb{F}_4}$
$[187, 11, 123]_{\mathbb{F}_4}$	$[188, 10, 125]_{\mathbb{F}_4}$	$[188, 11, 124]_{\mathbb{F}_4}$	$[189, 10, 126]_{\mathbb{F}_4}$
$[189, 11, 125]_{\mathbb{F}_4}$	$[190, 10, 127]_{\mathbb{F}_4}$	$[190, 11, 126]_{\mathbb{F}_4}$	$[191, 10, 128]_{\mathbb{F}_4}$
$[191, 11, 127]_{\mathbb{F}_4}$	$[192, 11, 128]_{\mathbb{F}_4}$	$[193, 11, 128]_{\mathbb{F}_4}$	$[194, 11, 128]_{\mathbb{F}_4}$
$[195, 11, 128]_{\mathbb{F}_4}$	$[196, 11, 129]_{\mathbb{F}_4}$	$[197, 11, 130]_{\mathbb{F}_4}$	$[198, 11, 130]_{\mathbb{F}_4}$
$[199, 11, 131]_{\mathbb{F}_4}$	$[200, 11, 132]_{\mathbb{F}_4}$	$[201, 10, 133]_{\mathbb{F}_4}$	$[201, 11, 132]_{\mathbb{F}_4}$
$[202, 10, 134]_{\mathbb{F}_4}$	$[202, 11, 132]_{\mathbb{F}_4}$	$[203, 10, 135]_{\mathbb{F}_4}$	$[204, 10, 136]_{\mathbb{F}_4}$
$[204, 11, 133]_{\mathbb{F}_4}$	$[205, 11, 134]_{\mathbb{F}_4}$	$[210, 11, 137]_{\mathbb{F}_4}$	$[213, 11, 139]_{\mathbb{F}_4}$
$[214, 11, 140]_{\mathbb{F}_4}$			

Table: 49 new codes over $\mathbb{F}_4$ which have a larger minimum distance than the previously known ones.

Conclusion II

- 49 new best codes.

- Unique and list decoding algorithms faster on valuation rings (e.g. Galois rings) than finite fields.

- Generalization of well known results on cyclic codes over finite fields for cyclic codes over finite rings, with application to quasi-cyclic codes:
  - Correspondence between QC codes and some ideals.
  - Generator polynomials.
  - Two new classes of codes with decoding algorithm.
  - Orthogonality of these classes of codes.
  - Weight enumerator distribution.

On quasi-cyclic codes as a generalization of cyclic codes

Morgan Barbier
morgan.barbier@unicaen.fr

Joint work with:
Christophe Chabot
Guillaume Quintin

University of Caen – GREYC

Dinard, C2
October 9th 2012