On the decoding of quasi-BCH codes

Morgan Barbier[1] Clément Pernet[2] Guillaume Quintin[3]

[1]University of Caen GREYC, France.

[2]University Joseph Fourier, INRIA/LIG-MOAIS, France.

[3]École polytechnique, INRIA Grace/LIX CRYPTO, France.

WCC 2013, April 16th

Quasi-cyclic codes

Definition

*Let $n = m\ell$, we say that $\mathcal{C} \subseteq \mathbb{F}_q^n$ is ℓ-**quasi-cyclic** if*

$$(x_1, \ldots, x_\ell, \ldots, x_{\ell+1}, \ldots, x_{2\ell}, x_{n-\ell+1}, \ldots, x_n) \in \mathcal{C} \Rightarrow (x_{n-\ell+1}, \ldots, x_n, x_1, \ldots, x_\ell, \ldots, x_{\ell+1}, \ldots, x_{2\ell}) \in \mathcal{C}.$$

- They have been studied:
  - Lally and Fitzpatrick [LF01],
  - Ling and Solé [LS01] and
  - Cayrel, Chabot and Necer [CCN10].
- Application to the McEliece cryptosystem:
  - Berger, Cayrel, Gaborit and Otmani [BCGO09].

Before defining quasi-BCH codes

Definition

Let $\Gamma \in M_{\ell\times\ell}(\mathbb{F}_q)$*. We say that* Γ *is a primitive m-th root of unity if*

- $\Gamma^m = Id_\ell,$
- $\forall 0 < i < m, \quad \Gamma^i \neq Id_\ell$ *and*
- $\forall 0 \leq i \neq j < m, \quad \det(\Gamma^i - \Gamma^j) \neq 0.$

Definition

Let A *be a any ring, we let* $A^\times$ *be the group of units of* A*. In fact,* $\gamma \in A$ *is primitive m-th root of unity if* $\gamma^i - 1$ *is a unit of* A *for* $i = 1, \ldots, m-1$ *and* $\gamma^m = 1$*.*

Proposition

There exists, at least, one primitive $(q^{s\ell} - 1)$*-th root of unity in* $M_{\ell\times\ell}(\mathbb{F}_{q^s})$*.*

Quasi-cyclic codes

Definition

Let $\Gamma \in M_{\ell\times\ell}(\mathbb{F}_{q^s})$ *be a primitive m-th root of unity and* $\delta > 0$*.*
The **quasi-BCH** *with respect to* Γ *of designed distance* δ *is*

$$\text{Q-BCH}(\Gamma,\delta) := \left\{ (c_1,\ldots,c_m) \in \left(\mathbb{F}_q^\ell\right)^m : \sum_{j=0}^{m-1} (\Gamma^i)^j c_{j+1} = 0 \textit{ pour } i = 1,\ldots,\delta-1 \right\}.$$

Generalized Reed-Solomon code over rings (1)

Definition

- *Let* $0 < k \leq m$ *be two integers.*
- *Let* $\vec{x} = (x_1, \ldots, x_m) \in A^m$ *and* $\vec{v} = (v_1, \ldots, v_m) \in (A^\times)^m$ *such that*
  - $x_i - x_j \in A^\times$ *and*
  - $x_i x_j = x_j x_i$

  for all $i \neq j$.

The **left** *submodule of* A^m *generated by the vectors*

$$(f(x_1) \cdot v_1, \ldots, f(x_m) \cdot v_m) \in A^m \text{ with } f \in A[X]_{<k}$$

is called a **left generalized Reed-Solomon code (LGRS) over** A **with parameters** $[\vec{v}, \vec{x}, k]_A$ *or* $[n, k]$ *or* $[\vec{x}, k]_A$ *if there is no confusion.*

Generalized Reed-Solomon code over rings (2)

One can also define **right generalized Reed-Solomon (RGRS)** codes.

Definition

Let $f = \sum_{i=0}^{d} f_i X^i \in A[X]$ *and* $a \in A$. *We call* **left evaluation of** f **at** a *the quantity*

$$f(a) := \sum_{i=0}^{d} f_i a^i \in A \qquad \longrightarrow \textit{for left GRS}$$

and **right evaluation of** f **at** a *the quantity*

$$(a)f := \sum_{i=0}^{d} a^i f_i \in A. \qquad \longrightarrow \textit{for right GRS}$$

Why Reed-Solomon codes over rings?

1. In [BCQ12] M. Barbier, C. Chabot and G. Quintin found "good" $\mathbb{F}_4$ linear codes using **Reed-Solomon codes over**

$$\mathbb{F}_4\left[\begin{pmatrix} 0 & \omega & 0 \\ \omega & \omega^2 & \omega^2 \\ 1 & \omega^2 & 1 \end{pmatrix}\right] \text{ with } \omega \in F_4 \text{ and } \mathbb{F}_2[\omega] = \mathbb{F}_4.$$

   - "Good" means that, over a fixed alphabet A, given n and k, the minimum distance of our $[n, k, \cdot]_A$-code is greater than the minimum distance of all the other **known** $[n, k, \cdot]_A$-codes.
   - Thanks to Markus Grassl.

2. M. Barbier, C. Chabot and G. Quintin tried to find other good codes using **Reed-Solomon codes over** $M_{\ell\times\ell}(\mathbb{F}_q)$. These codes are bad.

3. We can solve our current problem with them.

Duality

Definition

Let $\vec{x} = (x_1, \ldots, x_m)$ and $\vec{y} = (y_1, \ldots, y_m)$ be two vectors of A^m. The **inner product** is defined as

$$\langle \vec{x}, \vec{y} \rangle := \sum_{i=0}^{m} x_i y_i .$$

Definition

Let S be a subset of A^m. Then the set $\{\vec{x} \in A^m : \forall \vec{s} \in S, \langle \vec{s}, \vec{x} \rangle = 0\}$ denoted by $S^\perp$ is called the **right dual of** *S and is a right submodule of A^m.*
We define similarly the **left dual of** *S which we will denote by ${}^\perp S$.*

Duality for Reed-Solomon codes

Proposition

- *Let* $\gamma \in A$ *be a primitive* m*-th root of unity.*
- *Let* $\vec{x} = (1, \gamma, \gamma^2, \ldots, \gamma^{m-1}) \in A^m$*.*

Then the right (resp. left) dual of the LGRS (resp. RGRS) code with parameters $[\vec{x}, \vec{x}, k]_A$ *is the RRS (resp. LRS) code with parameters* $[\vec{x}, m-k]_A$*.*

Proposition

- *Let* $\Gamma \in M_{\ell \times \ell}(\mathbb{F}_{q^s})$ *be a primitive*
- m*-th root of unity and* $\mathcal{C} = \text{Q-BCH}_q(m, \ell, \delta, \Gamma)$*.*

Then there exists a RRS code $\mathcal{R}$ *over the ring* $M_{\ell \times \ell}(\mathbb{F}_{q^s})$ *with parameters* $[m, m-\delta+1, \delta]_{M_{\ell \times \ell}(\mathbb{F}_{q^s})}$ *and an* $\mathbb{F}_q$*-linear,* $\mathbb{F}_q$*-isometric embedding* $\psi : \mathcal{C} \to \mathcal{R}$*.*

ψ is explicit

ψ is a linear embedding

$$\psi : \mathcal{C} \longrightarrow \left(M_{\ell\times\ell}(\mathbb{F}_{q^s})\right)^m$$

defined by

$$(c_{11}, \ldots, c_{1\ell}, \ldots, c_{m1}, \ldots, c_{m\ell}) \longmapsto \left[\begin{pmatrix} c_{11} & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ c_{1\ell} & 0 & \ldots & 0 \end{pmatrix}, \ldots, \begin{pmatrix} c_{m1} & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ c_{m\ell} & 0 & \ldots & 0 \end{pmatrix}\right]$$

So we can apply the Welch-Berlekamp algorithm

Algorithm 1 Welch-Berlekamp for quasi-BCH codes

Require: a received vector $\vec{y} \in \mathbb{F}_q^{m\ell}$ with at most $\tau \leq \left\lfloor \frac{\delta-1}{2} \right\rfloor$ errors.
Ensure: the unique codeword within distance τ of $\vec{y}$.

1: $(Z_1, \ldots, Z_m) \leftarrow \psi(\vec{y})$.
2: Find $Q = Q_0(X) + Q_1(X)Y \in (M_{\ell\times\ell}(\mathbb{F}_{q^s})[X])[Y]$ of degree 1 such that
   1. $(\Gamma^{i-1}, Z_i)Q = 0$ for all $i = 1, \ldots, m$,
   2. $\deg Q_0 \leq m - \tau - 1$,
   3. $\deg Q_1 \leq m - \tau - 1 - (k-1)$.
3: $f \leftarrow$ the unique root of Q in $(M_{\ell\times\ell}(\mathbb{F}_{q^s}))[X]_{<k}$ such that $d\left((Z_1, \ldots, Z_m), ((I_\ell)f, \ldots, (\Gamma^{m-1})f)\right) \leq \tau$.
4: **return** $\psi^{-1}\left((I_\ell)f, (\Gamma)f, \ldots, (\Gamma^{m-1})f\right)$.

Advantages and drawbacks

Until now, we have

- **generalized the known relation** between Reed-Solomon codes and BCH codes,
- which allowed us to give an explicit **decoding algorithm** for quasi-BCH codes.

But

- the complexity analysis shows that the **decoding algorithm** is **not polynomial**.
- We have to find a way to make it polynomial.
- We **cannot** apply list-decoding **Guruswami-Sudan** algorithms.
- We have to **implement it**.
- We have to find **another approach**.

The block distance

Definition

*Let $n = m\ell$. We define the ℓ-**block weight** of $x = (x_{11}, \dots, x_{1\ell}, \dots, x_{m1}, \dots, x_{m\ell}) \in \mathbb{F}_q^n$ to be*

$$\text{Block-w}_\ell(x) := |\{i : (x_{i1}, \dots, x_{i\ell}) \neq 0\}|$$

*and the ℓ-**block distance** between x and $y \in \mathbb{F}_q^n$ to be $\text{Block-w}_\ell(x - y)$.*

Interleaved codes

Definition

Let $\mathcal{C}_1, \ldots, \mathcal{C}_\ell$ be error correcting codes of length m over $\mathbb{F}_q$.
The **interleaved code $\mathcal{C}$ with respect to $\mathcal{C}_1, \ldots, \mathcal{C}_\ell$** is a subset of

- $M_{\ell \times m}(\mathbb{F}_q)$, equipped with the ℓ-block distance with respect to the columns, such that $\vec{c} \in \mathcal{C}$ if and only if the i-th row of $\vec{c}$ is a codeword of $\mathcal{C}_i$ for $i = 1, \ldots, \ell$,

or (recall that $n = m\ell$)

- $\mathbb{F}_q^n$, equipped with the ℓ-block distance such that $x = (x_{11}, \ldots, x_{1\ell}, \ldots, x_{m1}, \ldots, x_{m\ell}) \in \mathcal{C}$ if and only if $(x_{1i}, x_{2i}, \ldots, x_{mi}) \in \mathcal{C}_i$ for all i.

We let $\mathrm{In}(\mathcal{C}_1, \ldots, \mathcal{C}_\ell) := \mathcal{C}$.

$$(c_{11}, \ldots, c_{1\ell}, \ldots, c_{m1}, \ldots, c_{m\ell}) \leftrightarrow \begin{array}{|c|c|c|} \hline c_{11} & \ldots & c_{m1} \\ \hline \vdots & & \vdots \\ \hline c_{1\ell} & \ldots & c_{m\ell} \\ \hline \end{array} \begin{array}{l} \in \mathcal{C}_1 \\ \\ \in \mathcal{C}_\ell \end{array}$$

Quasi-BCH codes and interleaved codes

Proposition

The quasi-BCH code $\mathcal{C}$ over $\mathbb{F}_q$ is an interleaved code of ℓ subcodes of Reed-Solomon codes over $\mathbb{F}_{q^{s'}}$ in the following sense:

there exist ℓ Reed-Solomon codes $\mathcal{C}_1, \ldots, \mathcal{C}_\ell$ over $\mathbb{F}_q$ and an isometric isomorphism from $\mathcal{C}$, equipped with the ℓ-block distance, to a subcode of the interleaved code with respect to $\mathcal{C}_1, \ldots, \mathcal{C}_\ell$.

Again the embedding is explicit

There exists $s' \in \mathbb{N}$ and $P \in \mathrm{GL}(\mathbb{F}_{q^{s'}})$ such that the embedding σ of the previous slide is given by

$$\sigma : \mathcal{C} \longrightarrow \mathrm{In}(\mathcal{C}_1, \ldots, C_\ell)$$

$$\begin{pmatrix} v_{11} \\ \vdots \\ v_{1\ell} \\ \vdots \\ v_{m1} \\ \vdots \\ v_{m\ell} \end{pmatrix} = \begin{pmatrix} P^{-1} & & \\ & \ddots & \\ & & P^{-1} \end{pmatrix} \begin{pmatrix} c_{11} \\ \vdots \\ c_{1\ell} \\ \vdots \\ c_{m1} \\ \vdots \\ c_{m\ell} \end{pmatrix}$$

Advantages and drawbacks

- We can decode quasi-BCH codes in **polynomial time**.
  - We can use any known **unique decoding** algorithm for Reed-Solomon codes.
  - We can use the **Guruswami-Sudan list decoding** algorithm.
  - We can also use the **Bleichenbacher, Kiayias and Yung** algorithm [BKY07] but only if $\mathcal{C}_1 = \mathcal{C}_2 = \cdots = \mathcal{C}_\ell$.
- We must **implement this algorithm**.
- What about the other quasi-cyclic codes? Are they interleaved codes?

References I

T. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani.
Reducing Key Length of the McEliece Cryptosystem.
In *Proceedings of the 2nd International Conference on Cryptology in Africa: Progress in Cryptology*, AFRICACRYPT '09, pages 77–97, Berlin, Heidelberg, 2009. Springer-Verlag.

M. Barbier, C. Chabot, and G. Quintin.
On quasi-cyclic codes as a generalization of cyclic codes.
Finite Fields and Their Applications, 18(5):904–919, 2012.

D. Bleichenbacher, A Kiayias, and M. Yung.
Decoding interleaved Reed-Solomon codes over noisy channels.

Theoretical Computer Science, 379(3):348–360, 2007.
Automata, Languages and Programming.

P.-L. Cayrel, C. Chabot, and A. Necer.
Quasi-cyclic codes as codes over rings of matrices.
Finite Fields and Their Applications, 16(2):100–115, 2010.

K. Lally and P. Fitzpatrick.
Algebraic structure of quasicyclic codes.
Discrete Applied Mathematics, 111(1–2):157–175, 2001.

S. Ling and P. Solé.
On the algebraic structure of quasi-cyclic codes .I. Finite fields.
IEEE Trans. Inform. Theory, 47(7):2751–2760, nov 2001.