On cellular codes and their cryptographic applications

Pierre Loidreau

DGA MI and IRMAR, Université de Rennes 1

ACCT-2014, September 9th, 2014

Motivations

- Quasi-cyclic codes are everywhere
  - Cryptography: Reduce public-key Size
    - Codes: MDPC, QC-McEliece, LRPC
    - Lattices: Ring-LWE, NTRU
  - Coding theory: Reduce complexity, good properties
    - QC-LDPC constructions in standards
- $\Rightarrow$ Goal:
  1. Use the algebraic structure to improve efficiency
  2. Give a framework to study the security

Position of the problem

- Doubly circulant code $[2n, n]$ over $\mathbb{F}_q$

$$\mathcal{C} = < (\mathbf{I}_n \mid \mathbf{A}) >, \ \ \mathbf{A} \text{ circulant}$$

- Related cryptographic problems
  - Decoding in $\mathcal{C}$, Hamming (rank) t errors
  - Finding low-weight (rank) codewords in $\mathcal{C}$

Actual gain in efficiency

- Without structure
  - Hamming, ISD: $2n^3\binom{2n}{n}/\binom{2n-t}{n}$
  - Rank: Let $q = p^v$

$C_1 = t^3 n^3 p^{\lceil \frac{t(n+1)-n)}{t} \rceil}$	$C_2 = n^3 v^3 \min(p^{t\lfloor \frac{v}{2} \rfloor}, p^{(t-1)\lfloor \frac{(n+1)v}{n} \rfloor})$
$C_3 = (n+t)^3 t^3 p^{(n+1)(t-1)}$	$C_4 = (n+t)^3 p^{(t-1)(v-t)+2}$

- Using the structure
  - Hamming: Gain of $\sqrt{n}$ in decoding and n in finding low-weight codewords
  - Rank: ?

Outline of the talk

- Cellular codes
- Projected cellular codes
- Hamming metric case
- Rank metric case

Cellular codes

Definition - (I)

- $g(x) = \sum_{i=0}^{m-1} g_i x^i \in K[x]$ of degree m, and $\mathcal{R}_g = K[x]/(g)$
- $\psi_g : \; a(x) \in \mathcal{R}_g \longmapsto \mathbf{a} = (a_0, \ldots, a_{m-1}) \in K^m$
- Morphism of *commutative algebras*

$$\Phi_g \;:\; a(x) \in \mathcal{R}_g \;\mapsto\; \underbrace{\mathbf{A}}_{a\ cell} = \begin{pmatrix} \psi_g(a(x)) \\ \psi_g(xa(x)) \\ \vdots \\ \psi_g(x^{m-1}a(x)) \end{pmatrix} \in K^{m \times m}$$

Definition - (II)

Definition

Let

$$\mathbf{G}_{\mathcal{M}} = \begin{pmatrix} a_{1,1}(x) & \cdots & a_{1,\ell}(x) \\ \vdots & \ddots & \vdots \\ a_{s,1}(x) & \cdots & a_{s,\ell}(x) \end{pmatrix} \to \mathbf{G} = \begin{pmatrix} \mathbf{A}_{1,1} & \cdots & \mathbf{A}_{1,\ell} \\ \vdots & \ddots & \vdots \\ \mathbf{A}_{s,1} & \cdots & \mathbf{A}_{s,\ell} \end{pmatrix}$$

Then $\mathcal{C}_g =< \mathbf{G} >_K$ *is a* g*-cellular code of index* ℓ

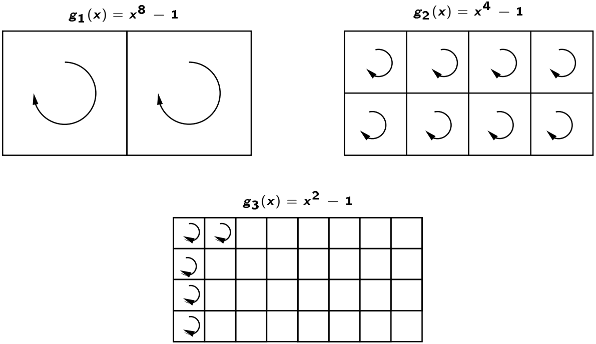


Figure: Different ways of considering a doubly circulant code as a cellular code

Some properties and lack of properties

- $\mathcal{C}_g$ is an $[n = \ell m, k \leq ms]_K$ code
- $\mathbf{A}_{i,j}$ in the commutative subalgebra of $\mathcal{M}_{m\times m}(K)$ generated by

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots & \\ g_0 & g_1 & g_2 & \cdots & g_{m-1} \end{pmatrix}$$

- Generalisation of quasi-cyclic codes
- Generally trivial automorphism group
- No particular structure of the dual code

Projected cellular codes

Projection operation

- Let $f(x) \in L[x]$, $L \hookleftarrow K$ of degree δ such that $f(x)|g(x)$.

$$\begin{array}{rrcl} \Pi \ : & \mathcal{R}_g & \longrightarrow & \mathcal{R}_f = L[x]/f \cdot L[x], \\ & a(x) \bmod g(x) & \mapsto & a'(x) = a(x) \bmod f(x) \end{array}$$

- Let $\mathcal{C}_g =< (\mathbf{A}_{i,j}) >_K$ a cellular code, $\mathcal{C}_f =< (\mathbf{A}'_{i,j}) >_L$, where

$$< (\mathbf{A}_{i,j}) >_K \stackrel{\Phi_g^{-1}}{\rightarrow} < (a_{i,j}(x)) >_{\mathcal{R}_g} \stackrel{\Pi}{\rightarrow} < (a'_{i,j}(x)) >_{\mathcal{R}_f} \stackrel{\Phi_f}{\rightarrow} < (\mathbf{A}'_{i,j}) >_L$$

Projected code

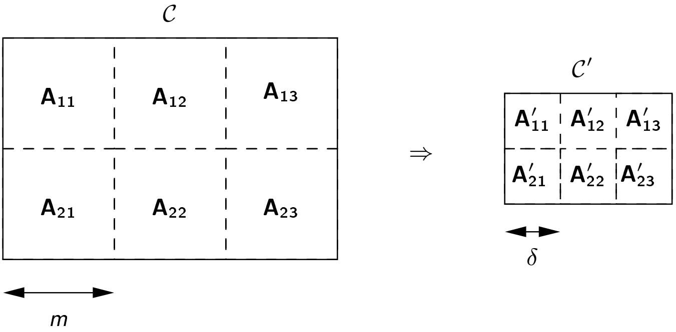


Figure: Projected code with $\ell = 3$

Proposition

$\mathcal{C}_f$ is an f-cellular code over L of length $\ell\delta$ and dimension $\leq s \times \delta$

Example

- Parameters: $K = \mathbb{F}_2$, $g(x) = x^6 - 1$

$$\mathbf{G} = \begin{array}{cr} \begin{pmatrix} c_0 & c_1 & c_2 & c_3 & c_4 & c_5 \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_0 \\ c_2 & c_3 & c_4 & c_5 & c_0 & c_1 \\ c_3 & c_4 & c_5 & c_0 & c_1 & c_2 \\ c_4 & c_5 & c_0 & c_1 & c_2 & c_3 \\ c_5 & c_6 & c_1 & c_2 & c_3 & c_4 \end{pmatrix} & \begin{array}{r} c(x) \\ xc(x) \\ x^2c(x) \\ x^3c(x) \\ x^4c(x) \\ x^5c(x) \end{array} \end{array}$$

- $g(x) = (x^3 - 1)(x^3 + 1) = (x^2 - 1)(x^4 + x^2 + 1)$.

Example

1. $f(x) = x^3 - 1$, then let
   $a_0 = c_0 + c_3,\ a_1 = c_1 + c_4, a_3 = c_2 + c_5$
   $$\mathcal{C}_f = < \begin{pmatrix} a_0 & a_1 & a_2 \\ a_1 & a_0 & a_2 \\ a_2 & a_1 & a_0 \end{pmatrix} >$$
2. $f(x) = x^2 - 1$, and $b_0 = c_0 + c_2 + c_4,\ b_1 = c_1 + c_3 + c_5$
   $$\mathcal{C}_f = < \begin{pmatrix} b_0 & b_1 \\ b_1 & b_0 \end{pmatrix} >$$

Quasi-cyclic particuliarity

- If $g(x) = x^m - 1$, then $\mathbf{b} = (\mathbf{b}_1, \ldots, \mathbf{b}_\ell) \in K^{m\ell}$ is in $\mathcal{C}_g^\perp$, iff

$$\forall i = 1, \ldots, s \quad \sum_{k=1}^{\ell} a_{i,k}(x) b_k(x) = 0$$

$$\Rightarrow \quad \mathcal{C}_g^\perp = <(\mathbf{B}_{i,j})_{i=1,j=1}^{\ell-s,\ell}>_K$$

Proposition

Let $g(x) = x^{m=uv} - 1$, and $f(x) = x^u - 1$ then

$$(\mathcal{C}_f)^\perp = (\mathcal{C}^\perp)_f = <(\mathbf{B}'_{i,j})_{i=1,j=1}^{\ell-s,\ell}>_K$$

General principle of decoding

- Input: $\mathbf{y} = \mathbf{c} + \mathbf{e}$, $\mathbf{c} \in \mathcal{C}_g$
- Procedure:
  1. $\overset{\psi_g^{-1}(\mathbf{y})}{\Rightarrow} \quad (y_1(x), \ldots, y_\ell(x)) = (c_1(x) + e_1(x), \ldots, c_\ell(x) + e_\ell(x))$
  2. Let $f(x) \in L[x]$ dividing $g(x)$:

     $$\mathbf{y}'(x) = (y'_1(x), \ldots, y'_\ell(x)) = (c'_1(x) + e'_1(x), \ldots, c'_\ell(x) + e'_\ell(x))$$

  3. $\overset{\psi_f(\mathbf{y}'(x))}{\Rightarrow} \mathbf{y}' = \mathbf{c}' + \mathbf{e}'$, $\mathbf{c} \in \mathcal{C}_f$
  4. Decode in $\mathcal{C}_f$
- Improves the decoding of $\mathcal{C}_g$??

Hamming metric case

Projection in Hamming metric

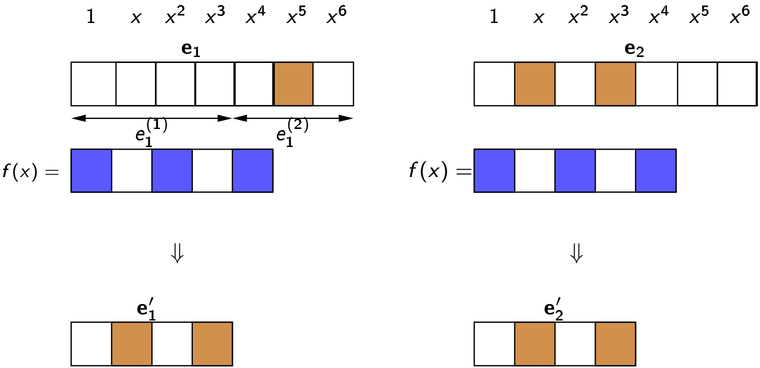
Proposition

Let $\mathbf{e} = (\mathbf{e}_1, \ldots, \mathbf{e}_\ell) \in K^{m\ell}$ *of weight* t*. If* $e_i(x) = e_i^{(1)}(x) + x^{\deg(f)} e_i^{(2)}(x)$ *and* $u_i^{(2)} = wt(e_i^{(2)}(x))$ *then:*

$$wt(\mathbf{e}') \leq t + \sum_{i=1}^{\ell} (wt(f) - 2) u_i^{(2)} \leq t(wt(f) - 1)$$

- Consequence :
  - If $f(x) = x^\delta + a$, $a \in L \hookleftarrow K$ then $wt(\mathbf{e}') \leq t$

Example



1 x x^2 x^3 x^4 x^5 x^6
$\mathbf{e}_1$
$e_1^{(1)}$
$e_1^{(2)}$
$f(x) =$
$\Downarrow$
$\mathbf{e}_1'$
1 x x^2 x^3 x^4 x^5 x^6
$\mathbf{e}_2$
$f(x) =$
$\Downarrow$
$\mathbf{e}_2'$

Decoding via projection - (I)

- Let $n' = \deg(f)\ell$
- Let $k' = \deg(f)s$
- Choice of $\mathcal{C}_f$: choose $f(x)|g(x)$ such that

$$t' = t(wt(f) - 1) \leq d_{GV} = n'H^{-1}(1 - k'/n')$$

$$\Rightarrow \ \mathbf{e}' \text{ uniquely decoded with complexity } k'^2 n' \frac{\binom{n'}{k'}}{\binom{n'-t'}{k'}}$$

- Use this information to finish the decoding...

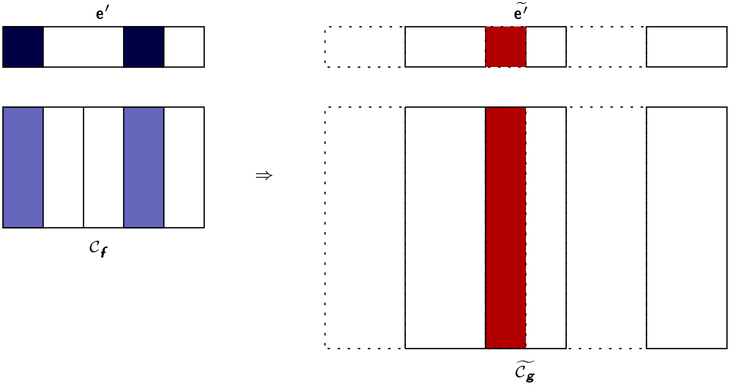
Decoding via projection - (II)

- Conditions on the parameters: since $k'/n' = k/n$

$$\frac{t(wt(f)-1)}{\deg(f)} \leq \ell H^{-1}(1-k/n)$$

- Complexity: $k'^2 n' \frac{\binom{n'}{k'}}{\binom{n'-t'}{k'}}$
- Finishing the decoding:
  1. Puncture $\mathcal{C}_g$ on mt' positions $\Rightarrow \widetilde{\mathcal{C}_g}$, $[\widetilde{n} = n - mt', k]$
  2. Decode weight $\max(t-t', 0)$ errors in $\widetilde{\mathcal{C}_g}$ with complexity

$$\approx k^2(n-mt')\frac{\binom{n-mt'}{k}}{\binom{n-\max(t-t',0)}{k}}$$



$\mathbf{e}'$
$\mathcal{C}_{\boldsymbol{f}}$
$\Rightarrow$
$\widetilde{\mathbf{e}'}$
$\widetilde{\mathcal{C}_{\boldsymbol{g}}}$

Case of divisible quasi-cyclic codes

- Let $g(x) = x^{m=uv} - 1$, then $f(x) = (x^v - 1)|g(x)$:
  - $\mathcal{C}_f$ quasi-cyclic
  - $wt(\mathbf{e}') \leq wt(\mathbf{e})$
  - Complexity gain $\approx (k/u)^3/\sqrt{v}$, provided GV satisfied

Application to MDPC cryptosystem

- *Original parameters :* $g(x) = x^{4800} - 1,\ t = 84, \ell = 2$

$$\underbrace{(\mathbf{I} \mid \mathbf{a})}_{9600}$$

- $d_{GV} = 0.11 \times 9600 = 1050 >> t$
- Choice of $f(x)$: $x^{400} - 1$,
  - $d_{gv} = 88$ for unique decoding in $\mathcal{C}_f$
  - Recovering $\mathbf{e}'$ of weight 84 : gain of $12^3/4 \approx 2^8$
  - $\widetilde{\mathcal{C}_f}$ of dimension 4800 and length $9600 - 84 * 12 = 9596$

Rank metric case

Action on the metric

Proposition

Let $\mathbf{e} \in K^{m\ell}$ *of rank* t*. Then if* $f(x) \in L[x]$ *and if* $[L : K] = u$

$$Rk(\mathbf{e}') \leq u \times Rk(\mathbf{e})$$

- Importance of the smallest field in which $g(x)$ non-prime

Decoding in rank metric

- Let $n' = \deg(f)\ell$
- Let $k' = \deg(f)s$
- Choose $f(x) \in L[x] \mid g(x)$ such that

$$t' = ut \leq d_{GV} = (n' + um)/2 - \sqrt{(um - n')^2/4 + umk'}$$

$\Rightarrow$ $\mathbf{e}'$ uniquely decoded

- Usually sufficient to recover $\mathbf{e}$

Application to LRPC Cryptosystem

- *Original parameters :* $g(x) = x^{47} - 1$, code over $\mathbb{F}_{2^{47}}$, $t = 4$
  - $g(x) = (x-1)f(x)f^*(x)$ in $\mathbb{F}_2[X] \Rightarrow u = 1$
  - $\mathcal{C}_f$ $[n' = 46, k' = 23]$ over $\mathbb{F}_{2^{47}}$
  - $d_{GV} = 13$
- Complexity comparisons

	$Log_2(C_1)$	$Log_2(C_2)$	$Log_2(C_3)$	$Log_2(C_4)$
$\mathcal{C}_g$	129	218	216	187
$\mathcal{C}_f$	126	120	117	184

Perspectives

- Cancellation of errors by projection $\Rightarrow$ improvement of complexity
- Factorizable QC-codes: Improvement in the search for small weight codewords
- Decoding via trellis of projection
- For cryptography: Take into account factorization of polynomials $x^m - 1$