

# Spectral Analysis of Quasi-Cyclic Codes

## An Improved Lower Bound on the Minimum Distance

Alexander Zeh<sup>1</sup> San Ling<sup>2</sup>



<sup>1</sup> Department of Computer Science  
Technion—Israel Institute of Technology,  
Haifa



<sup>2</sup> Division of Mathematical Sciences  
School of Physical Mathematical Sciences,  
Nanyang Technological University, Singapore

CodingSeminar@Technion  
11th May 2014

## Cyclic Code $\mathcal{C}$

1957 Prange

1960 **BCH**:  $d \geq \delta$ ,  $\left\lfloor \frac{\delta-1}{2} \right\rfloor$  decoding

1965 Improved bounds & decoding  
-90 (**HT**, Roos, ...)

2003 Kötter–Vardy based on  
Guruswami–Sudan

List decoding via supercode:

$$(1 - 1/q) \left( n - \sqrt{n \left( n - \frac{\delta}{1-1/q} \right)} \right)$$

## Quasi-Cyclic Code $QC$

1969 Chen–Peterson–Weldon  
Asymptotically goodness

1970 Exhaustive computer search  
-90 Several best-known codes

2001 Lally–Fitzpatrick [**LF2001**]  
RGB/POT basis

2012 Semenov–Trifonov [**ST2012**]  
Spectral analysis

- 1 Definitions and RGB/POT [LF2001]
- 2 Spectral Analysis of Semenov–Trifonov [ST2012] & BCH-like Bound
- 3 HT-like Bound and Syndrome-Based Decoding [ZL2014]
- 4 Conclusion and Outlook

# Definition of Quasi-Cyclic Codes

## Definition

A linear  $[m \cdot \ell, k, d]_q$  code  $\mathcal{QC}$  is  $\ell$ -quasi-cyclic if

$$\begin{aligned} & (c_{0,0} \dots c_{\ell-1,0} \quad c_{0,1} \dots c_{\ell-1,1} \quad \dots \quad c_{0,m-1} \dots c_{\ell-1,m-1}) \in \mathcal{QC} \\ & \Rightarrow \\ & (c_{0,m-1} \dots c_{\ell-1,m-1} \quad c_{0,0} \dots c_{\ell-1,0} \quad \dots \quad c_{0,m-2} \dots c_{\ell-1,m-2}) \in \mathcal{QC}. \end{aligned}$$

If  $\ell = 1$ , then cyclic code.

**Recap:** Generator  $g(X) \mid (X^m - 1) = \prod_i (X - \alpha^i)$  of an  $[m \cdot 1, k, d]_q$  code:

$$\mathcal{C} = \left\{ c(X) = i(X)g(X) : \forall i(X) \text{ with } \deg i(X) < k \right\}.$$

Generator of  $\mathcal{QC}$ ?

# RGB in POT (i)

$$(c_{0,0} \dots c_{\ell-1,0} \quad c_{0,1} \dots c_{\ell-1,1} \quad \dots \quad c_{0,m-1} \dots c_{\ell-1,m-1}) \in \mathcal{QC}$$

Let  $\ell$  polynomials be

$$c_i(X) = c_{i,0} + c_{i,1}X + \dots + c_{i,m-1}X^{m-1}, \quad \forall i \in [\ell].$$

Then a basis of  $\mathcal{QC}$  is [LF2001]:

$$\mathbf{G}(X) = \begin{pmatrix} g_{0,0}(X) & g_{0,1}(X) & \dots & g_{0,\ell-1}(X) \\ & g_{1,1}(X) & \dots & g_{1,\ell-1}(X) \\ & & \ddots & \vdots \\ 0 & & & g_{\ell-1,\ell-1}(X) \end{pmatrix},$$

such that:

$$\mathcal{QC} = \left\{ (c_0(X) \dots c_{\ell-1}(X)) = (i_0(X) \dots i_{\ell-1}(X)) \mathbf{G}(X) \right\},$$

with  $\sum_{j \in [\ell]} (\deg i_j(X) + 1) \leq k$ .

$$\mathbf{G}(X) = \begin{pmatrix} g_{0,0}(X) & g_{0,1}(X) & \cdots & g_{0,\ell-1}(X) \\ & g_{1,1}(X) & \cdots & g_{1,\ell-1}(X) \\ & & \ddots & \vdots \\ & & & g_{\ell-1,\ell-1}(X) \end{pmatrix},$$

where:

- 1)  $g_{i,j}(X) = 0, \quad \forall 0 \leq j < i < \ell,$
- 2)  $g_{i,i}(X) | (X^m - 1), \quad \forall i \in [\ell],$
- 3)  $\deg g_{j,i}(X) < \deg g_{i,i}(X), \quad \forall j < i, i \in [\ell].$

# Spectral Analysis (i)

$$\mathbf{G}(X) = \begin{pmatrix} g_{0,0}(X) & g_{0,1}(X) & \cdots & g_{0,\ell-1}(X) \\ & g_{1,1}(X) & \cdots & g_{1,\ell-1}(X) \\ & & \ddots & \vdots \\ & 0 & & g_{\ell-1,\ell-1}(X) \end{pmatrix}$$

## Definition (Eigenvalue and Multiplicity)

An **eigenvalue**  $\lambda_i = \alpha^{ji}$  of  $QC$  is a root of

$$\det(\mathbf{G}(X)) = \prod_{i \in [\ell]} g_{i,i}(X)$$

with **algebraic multiplicity**  $u_i$  such that

$$(X - \lambda_i)^{u_i} \mid \det(\mathbf{G}(X)).$$

$$\mathbf{G}(X) = \begin{pmatrix} g_{0,0}(X) & g_{0,1}(X) & \cdots & g_{0,\ell-1}(X) \\ & g_{1,1}(X) & \cdots & g_{1,\ell-1}(X) \\ & & \ddots & \vdots \\ & & & g_{\ell-1,\ell-1}(X) \end{pmatrix}$$

### Definition (Eigenvector and Eigenspace)

The **eigenvectors**  $\mathbf{v}_i^{\langle 0 \rangle}, \mathbf{v}_i^{\langle 1 \rangle}, \dots, \mathbf{v}_i^{\langle u_i-1 \rangle}$  in  $\mathbb{F}_{q^r}^\ell$  of  $\mathcal{QC}$  are s.t.

$$\mathbf{G}(\lambda_i)\mathbf{v}_i^{\langle j \rangle} = \mathbf{0}, \quad \forall j \in [u_i],$$

and its solution space is called **eigenspace**  $\mathcal{V}_i$ .

[ST2012]: algebraic multiplicity = geometric multiplicity =  $u_i!$



## Definition (Eigencode)

Let  $\mathcal{V} \subseteq \mathbb{F}_{q^r}^\ell$  be an eigenspace. Define the  $[n^{ec} = \ell, k^{ec}, d^{ec}]_q$  **eigencode**:

$$\mathbb{C}(\mathcal{V}) \stackrel{\text{def}}{=} \left\{ (c_0 \dots c_{\ell-1}) \in \mathbb{F}_q^\ell \mid \forall (v_0 \dots v_{\ell-1}) \in \mathcal{V} \subseteq \mathbb{F}_{q^r}^\ell : \sum_{i=0}^{\ell-1} v_i c_i = 0 \right\}.$$

**Remark:** If  $\exists \mathbf{v} = (v_0 \ v_1 \ \dots \ v_{\ell-1}) \in \mathcal{V}$  s.t. the elements  $v_0, v_1, \dots, v_{\ell-1}$  are linearly independent over  $\mathbb{F}_q$ , then:

$$\mathbb{C}(\mathcal{V}) = \{(0 \ 0 \ \dots \ 0)\},$$

and  $d^{ec} = \infty$ .

# BCH-like Lower Bound on the Minimum Distance (i)

## Theorem ([Thm. 2, ST2012])

Let  $QC$  be an  $[m \cdot \ell, k, d]_q$   $\ell$ -quasi-cyclic code and let the set

$$D \stackrel{\text{def}}{=} \{f, f + z, \dots, f + (\delta - 2)z\}$$

for some integers  $f$ ,  $\delta > 2$  and  $z > 0$  with  $\gcd(m, z) = 1$  be s.t.

$$\alpha^i, \quad \forall i \in D$$

are eigenvalues of  $QC$ . Let the eigencode be  $\mathbb{C}(\bigcap_{i \in D} \mathcal{V}_i)$ . Then:

$$d \geq d^{ST} \stackrel{\text{def}}{=} \min(\delta, d^{ec}).$$

**Proof:** In [ST2012] by explicit parity-check matrix.

# BCH-like Lower Bound on the Minimum Distance (ii)

## Example (Binary 2-Quasi-Cyclic Code)

Let  $\mathcal{QC}$  be the binary  $[63 \cdot 2, 100, 6]_2$  2-quasi-cyclic code with

$$\mathbf{G}(X) = \begin{pmatrix} g_{0,0}(X) & g_{0,1}(X) \\ 0 & g_{1,1}(X) \end{pmatrix} \quad \begin{aligned} g_{0,0}(X) &= m_0(X)m_1(X)m_9(X), \\ g_{0,1}(X) &= g_{0,0}(X)a_{0,1}(X), \\ g_{1,1}(X) &= g_{0,0}(X)m_5(X) \end{aligned}$$

$\lambda_i = \alpha^i$	$\mathbf{G}(\lambda_i)$	$\mathbf{v}_i^{(0)}, \mathbf{v}_i^{(1)}$
$i \in \{0, 1, 2, 4, 8, 9, 16, 18, 32, 36\} = M_0 \cup M_1 \cup M_9$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	$\mathbf{v}_i^{(0)}, \mathbf{v}_i^{(1)} \in \mathbb{F}_2^{26}$
$i \in \{5, 10, 17, 20, 34, 40\} = M_5$	$\begin{pmatrix} g_{0,0}(\lambda_i) & g_{0,1}(\lambda_i) \\ 0 & 0 \end{pmatrix}$	$\mathbf{v}_i^{(0)} = \begin{pmatrix} 1 & -\frac{g_{0,0}(\lambda_i)}{g_{0,1}(\lambda_i)} \end{pmatrix}^T$

**Question?** a)  $D = \{0, 1, 2\}$ , b)  $D = \{0, 5, 10\}$ , c)  $D = \{1, 5, 9\}$

# HT-like Lower Bound on the Minimum Distance (i)

## Theorem ([Thm. 1, ZL2014])

Let  $QC$  be an  $[m \cdot \ell, k, d]_q$   $\ell$ -quasi-cyclic code and let the set

$$D \stackrel{\text{def}}{=} \left\{ \begin{aligned} &f, f + z, \dots, f + (\delta - 2)z, \\ &f + 1, f + 1 + z, \dots, f + 1 + (\delta - 2)z, \\ &\quad \ddots \quad \quad \quad \ddots \quad \quad \quad \dots \quad \quad \quad \ddots \\ &f + \nu, f + \nu + z, \dots, f + \nu + (\delta - 2)z \end{aligned} \right\},$$

for some integers  $f$ ,  $\delta > 2$  and  $z > 0$  with  $\gcd(m, z) = 1$  be s.t.

$$\alpha^i, \quad \forall i \in D$$

are eigenvalues of  $QC$ . Let the eigencode be  $\mathbb{C}(\bigcap_{i \in D} \mathcal{V}_i)$ . Then:

$$d \geq d^* \stackrel{\text{def}}{=} \min(\delta + \nu, d^{\text{ec}}).$$

# HT-like Lower Bound on the Minimum Distance (ii)

## Example (Binary 2-Quasi-Cyclic Code)

Let  $\mathcal{QC}$  be the binary  $[63 \cdot 2, 100, 6]_2$  2-quasi-cyclic code with

$$\mathbf{G}(X) = \begin{pmatrix} g_{0,0}(X) & g_{0,1}(X) \\ 0 & g_{1,1}(X) \end{pmatrix} \quad \begin{aligned} g_{0,0}(X) &= m_0(X)m_1(X)m_9(X), \\ g_{0,1}(X) &= g_{0,0}(X)a_{0,1}(X), \\ g_{1,1}(X) &= g_{0,0}(X)m_5(X) \end{aligned}$$

$\lambda_i = \alpha^i$	$\mathbf{G}(\lambda_i)$	$\mathbf{v}_i^{(0)}, \mathbf{v}_i^{(1)}$
$i \in \{0, 1, 2, 4, 8, 9, 16, 18, 32, 36\} = M_0 \cup M_1 \cup M_9$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	$\mathbf{v}_i^{(0)}, \mathbf{v}_i^{(1)} \in \mathbb{F}_2^6$
$i \in \{5, 10, 17, 20, 34, 40\} = M_5$	$\begin{pmatrix} g_{0,0}(\lambda_i) & g_{0,1}(\lambda_i) \\ 0 & 0 \end{pmatrix}$	$\mathbf{v}_i^{(0)} = \left(1 \quad -\frac{g_{0,0}(\lambda_i)}{g_{0,1}(\lambda_i)}\right)^T$

$$D = \{0, 4, 8, 1, 5, 9\}$$

$$\delta + \nu = 4 + 1 = 5$$

$$d^{ec} = \infty$$

# Syndrome-Based Decoding (i)

$$\mathbf{c}(X) = (c_0(X) \ c_1(X) \ \dots \ c_{\ell-1}(X))$$

From HT-like bound, we have:

$$\begin{array}{l} \mathbf{G}(\alpha^f), \mathbf{G}(\alpha^{f+z}), \dots, \mathbf{G}(\alpha^{f+(\delta-2)z}) \\ \vdots \quad \quad \quad \vdots \quad \quad \quad \dots \quad \quad \quad \vdots \\ \mathbf{G}(\alpha^{f+\nu}), \mathbf{G}(\alpha^{f+\nu+z}), \dots, \mathbf{G}(\alpha^{f+\nu+(\delta-2)z}) \end{array} = 0, 0, \dots, 0$$

with intersection of eigenspaces  $\mathcal{V}$ . Or:

$$\begin{array}{l} \mathbf{c}(\alpha^f) \circ \mathbf{v}, \mathbf{c}(\alpha^f) \circ \mathbf{v}, \dots, \mathbf{c}(\alpha^{f+(\delta-2)z}) \circ \mathbf{v} \\ \vdots \quad \quad \quad \vdots \quad \quad \quad \dots \quad \quad \quad \vdots \\ \mathbf{c}(\alpha^{f+\nu}) \circ \mathbf{v}, \mathbf{c}(\alpha^{f+\nu+z}) \circ \mathbf{v}, \dots, \mathbf{c}(\alpha^{f+\nu+(\delta-2)z}) \circ \mathbf{v} \end{array} = 0, 0, \dots, 0$$

$\forall \mathbf{c}(X) \in \mathcal{QC}$  and  $\mathbf{v} \in \mathcal{V}$ .

# Syndrome-Based Decoding (ii)

We have:

$$\mathbf{c}(\alpha^{f+j}) \circ \mathbf{v}, \mathbf{c}(\alpha^{f+j+z}) \circ \mathbf{v}, \dots, \mathbf{c}(\alpha^{f+j+(\delta-2)z}) \circ \mathbf{v} = 0, 0, \dots, 0$$

$\forall j \in [\nu + 1]$  and  $\forall \mathbf{c}(X) \in \mathcal{QC}$  and  $\mathbf{v} \in \mathcal{V}$ . Therefore for:

$$\mathbf{r}(X) = \mathbf{c}(X) + \mathbf{e}(X),$$

we define  $\nu + 1$  syndrome polynomials in  $\mathbb{F}_{q^r}[X]$  with

$$S^{(j)}(X) \stackrel{\text{def}}{=} \sum_{i=0}^{\delta-2} \mathbf{r}(\alpha^{f+j+iz}) \circ \mathbf{v} X^i = \sum_{i=0}^{\delta-2} \mathbf{e}(\alpha^{f+j+iz}) \circ \mathbf{v} X^i \quad \forall j \in [\nu + 1],$$

and with  $\Lambda(X) = \sum_{i \in E} (1 - X\alpha^{iz})$  we get  $\nu + 1$  **Key Equations**:

$$S^{(j)}(X)\Lambda(X) \equiv \Omega^{(j)}(X) \pmod{X^{\delta-1}} \quad \forall j \in [\nu + 1].$$

# Syndrome-Based Decoding (iii)

## Example

Suppose the all-zero codeword of the  $[63 \cdot 2, 100, 6]_2$  code was sent:

$$r_0(X) = e_0(X) = 1 + X^{32}, \quad r_1(X) = e_1(X) = X^{32}.$$

Let  $\mathbf{v}^{(5)} = (1 \ \alpha^4 + 1) \in \mathbb{F}_{2^6}^2$  in  $\cap_{i \in D} \mathcal{V}_i$ , where  $D = \{0, 4, 8, 1, 5, 9\}$ . The error-locator polynomial is

$$\sum_{i=0}^2 \Lambda_i X^i = 1 + \alpha^{49} X + \alpha^2 X^2 = (1 - X)(1 - X\alpha^{128}).$$

Error-evaluation gives two error values in  $\mathbb{F}_{2^6}$ :

$$E_0 = 1 \text{ and } E_{32} = \alpha^4.$$

We can reconstruct  $\tilde{\varepsilon} = 3$  error values

$$e_{0,0} = 1, \ e_{32,0} = 1 \text{ and } e_{32,1} = 1 \text{ in } \mathbb{F}_2.$$



# Summary and Outlook

## Summary for $[m \cdot \ell, k, d]_q$ $\ell$ -quasi-cyclic code $QC$

- 1 Recap of RGB/POT generator basis  $\mathbf{G}(X)$  of [LF2001] for  $QC$
- 2 Recap of spectral analysis of [ST2012] and BCH-like bound  $d \geq \delta$
- 3 [ZL2014]: HT-like bound and decoding up to  $\lfloor \frac{\delta + \nu - 1}{2} \rfloor$

## Outlook

- Generalization of other bounds for  $C$  to  $QC$
- Decoding and construction of interleaved  $QC$
- Quasi-cyclic product code:
  - 1  $\ell$ - $QC \otimes C = \ell$ - $QC$
  - 2  $\ell_a$ - $QC \otimes \ell_b$ - $QC = \ell_a \ell_b$ - $QC$
- List decoding via supercode

Thank you!