Quasi-Twisted Codes as Contractions of Quasi-Cyclic Codes

Ferruh Özbudak and Buket Özkaya

Middle East Technical University, Ankara

ALCOCRYPT
20-24 February 2023

Constacyclic codes

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a prime power. Let m be a positive integer with $\gcd(m, q) = 1$. For $\lambda \in \mathbb{F}_q^*$, a linear code $C \subseteq \mathbb{F}_q^m$ is called a λ-*constacyclic* code if it is invariant under the λ-constashift of codewords: $(c_0, \ldots, c_{m-1}) \in C \Longrightarrow (\lambda c_{m-1}, c_0, \ldots, c_{m-2}) \in C$. In particular, if $\lambda = 1$ or $q = 2$, then C is a cyclic code.

Constacyclic codes

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a prime power. Let m be a positive integer with $\gcd(m, q) = 1$. For $\lambda \in \mathbb{F}_q^*$, a linear code $C \subseteq \mathbb{F}_q^m$ is called a λ-*constacyclic* code if it is invariant under the λ-constashift of codewords: $(c_0, \ldots, c_{m-1}) \in C \Longrightarrow (\lambda c_{m-1}, c_0, \ldots, c_{m-2}) \in C$. In particular, if $\lambda = 1$ or $q = 2$, then C is a cyclic code.

Consider $I = \langle x^m - \lambda \rangle$ of $\mathbb{F}_q[x]$ and define $R := \mathbb{F}_q[x]/I$. For an element $\mathbf{a} \in \mathbb{F}_q^m$, we associate an element of R via the following $\mathbb{F}_q$-module isomorphism:

$$\begin{array}{rcl} \phi : \ \mathbb{F}_q^m & \longrightarrow & R \\ \mathbf{a} = (a_0, \ldots, a_{m-1}) & \longmapsto & a(x) := a_0 + \cdots + a_{m-1}x^{m-1}. \end{array}$$

Observe that the λ-constashift in $\mathbb{F}_q^m$ corresponds to multiplication by x in R. Therefore, a λ-constacyclic code $C \subseteq \mathbb{F}_q^m$ can be viewed as an ideal of R.

Constacyclic codes

Since every ideal in R is principal, there exists a unique monic polynomial $g(x) \in R$ such that $C = \langle g(x) \rangle$, *i.e.*, each codeword $c(x) \in C$ is of the form $c(x) = a(x)g(x)$, for some $a(x) \in R$. The polynomial $g(x)$, which is a divisor of $x^m - \lambda$, is called the *generator polynomial* of C.

Constacyclic codes

Since every ideal in R is principal, there exists a unique monic polynomial $g(x) \in R$ such that $C = \langle g(x) \rangle$, *i.e.*, each codeword $c(x) \in C$ is of the form $c(x) = a(x)g(x)$, for some $a(x) \in R$. The polynomial $g(x)$, which is a divisor of $x^m - \lambda$, is called the *generator polynomial* of C.

Let $\mathrm{wt}(c)$ denote the number of nonzero coefficients in $c(x) \in C$. Recall that the minimum distance of C is defined as

$$d(C) := \min\{\mathrm{wt}(c) : 0 \neq c(x) \in C\}$$

when C is not the trivial zero code. We have $C = \{\mathbf{0}_m\}$ if and only if $g(x) = x^m - \lambda$. In this case, we assume throughout that $d(C) = \infty$.

Constacyclic codes

Let r be the smallest divisor of $q-1$ with $\lambda^r = 1$ and let α be a primitive rm^{th} root of unity such that $\alpha^m = \lambda$. Then, $\xi := \alpha^r$ is a primitive m^{th} root of unity and the roots of $x^m - \lambda$ are of the form $\alpha, \alpha\xi, \ldots, \alpha\xi^{m-1}$. Henceforth, let

$$\Omega := \{\alpha\xi^k : 0 \leq k \leq m-1\} = \{\alpha^{1+kr} : 0 \leq k \leq m-1\}$$

be the set of all m^{th} roots of λ and let $\mathbb{F}$ be the smallest extension of $\mathbb{F}_q$ that contains Ω (equivalently, $\mathbb{F}$ is the splitting field of $x^m - \lambda$).

Constacyclic codes

Let r be the smallest divisor of $q-1$ with $\lambda^r = 1$ and let α be a primitive rm^{th} root of unity such that $\alpha^m = \lambda$. Then, $\xi := \alpha^r$ is a primitive m^{th} root of unity and the roots of $x^m - \lambda$ are of the form $\alpha, \alpha\xi, \ldots, \alpha\xi^{m-1}$. Henceforth, let

$$\Omega := \{\alpha\xi^k : 0 \leq k \leq m-1\} = \{\alpha^{1+kr} : 0 \leq k \leq m-1\}$$

be the set of all m^{th} roots of λ and let $\mathbb{F}$ be the smallest extension of $\mathbb{F}_q$ that contains Ω (equivalently, $\mathbb{F}$ is the splitting field of $x^m - \lambda$).

Given the λ-constacyclic code $C = \langle g(x) \rangle$, the set of roots of its generator polynomial, say

$$L := \{\alpha\xi^k \ : \ g(\alpha\xi^k) = 0\} \subseteq \Omega,$$

is called the *zero set* of C. The power set $\mathcal{P}(L)$ of L is called the *defining set* of C. Clearly, $L = \emptyset$ if and only if $C = \langle 1 \rangle = \mathbb{F}_q^m$.

Constacyclic codes

A nonempty subset $E \subseteq \Omega$ is said to be *consecutive* if there exist integers e, n and δ with $e \geq 0, \delta \geq 2, n > 0$ and $\gcd(m, n) = 1$ such that

$$E := \{\alpha\xi^{e+zn} \ : \ 0 \leq z \leq \delta - 2\} \subseteq \Omega.$$

Constacyclic codes

A nonempty subset $E \subseteq \Omega$ is said to be *consecutive* if there exist integers e, n and δ with $e \geq 0, \delta \geq 2, n > 0$ and $\gcd(m, n) = 1$ such that

$$E := \{\alpha\xi^{e+zn} \ : \ 0 \leq z \leq \delta - 2\} \subseteq \Omega.$$

Let $\mathcal{P}(\Omega)$ denote the power set of Ω. Observe that any $P \in \mathcal{P}(\Omega)$ is the zero set of some λ-constacyclic code $D_P \subseteq \mathbb{F}^m$ since $x^m - \lambda$ splits into linear factors over $\mathbb{F}$.

Constacyclic codes

A nonempty subset $E \subseteq \Omega$ is said to be *consecutive* if there exist integers e, n and δ with $e \geq 0, \delta \geq 2, n > 0$ and $\gcd(m, n) = 1$ such that

$$E := \{\alpha\xi^{e+zn} \ : \ 0 \leq z \leq \delta - 2\} \subseteq \Omega.$$

Let $\mathcal{P}(\Omega)$ denote the power set of Ω. Observe that any $P \in \mathcal{P}(\Omega)$ is the zero set of some λ-constacyclic code $D_P \subseteq \mathbb{F}^m$ since $x^m - \lambda$ splits into linear factors over $\mathbb{F}$.

Let C be a nontrivial λ-constacyclic code of length m over some subfield of $\mathbb{F}$ with zero set $L \subseteq \Omega$. Then, for any $P \subseteq L$, C is contained in D_P and therefore we have $d(C) \geq d(D_P)$.

Defining set bounds

We define a *defining set bound* to be a member of a chosen family

$$\mathcal{B}(C) := \{(P, d_P)\} \subseteq \mathcal{P}(\Omega) \times (\mathbb{N} \cup \{\infty\})$$

such that, for any $(P, d_P) \in \mathcal{B}(C)$, $P \subseteq L$ implies $d(C) \geq d(D_P) \geq d_P$

Defining set bounds

We define a *defining set bound* to be a member of a chosen family

$$\mathcal{B}(C) := \{(P, d_P)\} \subseteq \mathcal{P}(\Omega) \times (\mathbb{N} \cup \{\infty\})$$

such that, for any $(P, d_P) \in \mathcal{B}(C)$, $P \subseteq L$ implies $d(C) \geq d(D_P) \geq d_P$

We set

$$\mathcal{B}_1(C) := \{(P, d(D_P)) : D_P \subseteq \mathbb{F}^m \text{ has zero set } P, \text{ for all } P \subseteq L\}.$$

In particular, following the notation given above in the case when $P = L = \Omega$, we have $D_\Omega = \{\mathbf{0}_m\}$ over $\mathbb{F}$ with $d(D_\Omega) = \infty$ and consequently, we include (Ω, ∞) in every collection $\mathcal{B}(C)$ as a convention when $L = \Omega$.

Defining set bounds

If we choose

$$\mathcal{B}_2(C) := \{(E, |E| + 1) : E \subseteq L \text{ is consecutive}\},$$

then we obtain the BCH bound.

Defining set bounds

If we choose

$$\mathcal{B}_2(C) := \{(E, |E| + 1) : E \subseteq L \text{ is consecutive}\},$$

then we obtain the BCH bound.

Similarly, we formulate the HT bound as

$$\mathcal{B}_3(C) := \{(D, \delta + s) : D = \{\alpha\xi^{e+zn_1+yn_2} : 0 \leq z \leq \delta - 2, 0 \leq y \leq s\} \subseteq L\},$$

for integers $e \geq 0$, $\delta \geq 2$ and positive integers s, n_1 and n_2 such that $\gcd(m, n_1) = 1$ and $\gcd(m, n_2) < \delta$.

Defining set bounds

If we choose

$$\mathcal{B}_2(C) := \{(E, |E| + 1) : E \subseteq L \text{ is consecutive}\},$$

then we obtain the BCH bound.

Similarly, we formulate the HT bound as

$$\mathcal{B}_3(C) := \{(D, \delta + s) : D = \{\alpha\xi^{e+zn_1+yn_2} : 0 \leq z \leq \delta - 2, 0 \leq y \leq s\} \subseteq L\},$$

for integers $e \geq 0$, $\delta \geq 2$ and positive integers s, n_1 and n_2 such that $\gcd(m, n_1) = 1$ and $\gcd(m, n_2) < \delta$.

Finally, the Roos bound corresponds to the choice

$$\mathcal{B}_4(C) := \{(MN, |M| + d_N - 1) : \text{there exists a consecutive set } M' \subseteq \Omega \text{ such that } M' \supseteq M \text{ with } |M'| \leq |M| + d_N - 2\},$$

for any $\emptyset \neq MN \subseteq L$ with $MN = \frac{1}{\alpha} \bigcup_{\varepsilon \in M} \varepsilon N$.

Contraction

Theorem (Bierbrauer,2002)

If C is a λ-constacyclic code of length m and dimension k over $\mathbb{F}_q$ such that $\gcd(m, q) = 1$ *and* $\lambda^r = 1$*, then there exists a q-ary cyclic code D of length rm, dimension k and minimum distance $r \cdot d(C)$ with codewords of the form* $(\mathbf{c}, \lambda^{-1} \cdot \mathbf{c}, \ldots, \lambda^{-(r-1)} \cdot \mathbf{c})$*, where* $\mathbf{c} \in C$*.*
Conversely, let D be a q-ary cyclic code of length rm such that $\gcd(m, q) = 1$ *and* $r \mid q - 1$ *with* $\lambda^r = 1$*, for some nonzero element* $\lambda \in \mathbb{F}_q$*, and with zeros* $\{\alpha^{-v_1}, \ldots, \alpha^{-v_t}\}$ *such that* $-v_1 \equiv -v_2 \equiv \cdots \equiv -v_t \mod r$*. Then, the codewords of D are of the form* $(\lambda^{r-1} \cdot \mathbf{c}, \lambda^{r-2} \cdot \mathbf{c}, \ldots, \lambda \cdot \mathbf{c}, \mathbf{c})$*, where* $\mathbf{c}$ *is a codeword of a q-ary λ-constacyclic code C of length m and minimum distance* $\frac{d(D)}{r}$*. Moreover, C and D have the same dimensions over* $\mathbb{F}_q$*.*

Quasi-twisted codes

Let m and ℓ be positive integer with $\gcd(m, q) = 1$. A linear code $C \subseteq \mathbb{F}_q^{m\ell}$ is called a λ-quasi-twisted (λ-QT) code of index ℓ if it is invariant under the λ-constashift of codewords by ℓ positions and ℓ is the least positive integer with this property. In particular, if $\ell = 1$, then C is a λ-constacyclic code, and if $\lambda = 1$ or $q = 2$, then C is a QC code of index ℓ.

Quasi-twisted codes

Let m and ℓ be positive integer with $\gcd(m, q) = 1$. A linear code $C \subseteq \mathbb{F}_q^{m\ell}$ is called a λ-quasi-twisted (λ-QT) code of index ℓ if it is invariant under the λ-constashift of codewords by ℓ positions and ℓ is the least positive integer with this property. In particular, if $\ell = 1$, then C is a λ-constacyclic code, and if $\lambda = 1$ or $q = 2$, then C is a QC code of index ℓ.

If we view a codeword $\mathbf{c} \in C$ as an $m \times \ell$ array

$$\mathbf{c} = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix},$$

then being invariant under λ-constashift by ℓ positions in $\mathbb{F}_q^{m\ell}$ corresponds to being closed under row λ-constashift in $\mathbb{F}_q^{m\times\ell}$.

Quasi-twisted codes

$$\Phi : \quad \mathbb{F}_q^{m\ell} \quad \longrightarrow \quad R^{\ell}$$

$$\mathbf{c} = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix} \quad \longmapsto \quad \mathbf{c}(x)$$

$$\mathbf{c}(x) = (c_0(x), \ldots, c_{\ell-1}(x))$$

$$\begin{matrix} \downarrow & & \downarrow \\ c_0(x) & \cdots & c_{\ell-1}(x) \end{matrix}$$

Quasi-twisted codes

$$\Phi : \quad \mathbb{F}_q^{m\ell} \quad \longrightarrow \quad R^\ell$$

$$\mathbf{c} = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix} \quad \longmapsto \quad \mathbf{c}(x) = (c_0(x), \ldots, c_{\ell-1}(x))$$

$$\downarrow \qquad \downarrow$$

$$c_0(x) \quad \ldots \quad c_{\ell-1}(x)$$

Observe that the row λ-constashift invariance in $\mathbb{F}_q^{m\times\ell}$ corresponds to being closed under componentwise multiplication by x in R^ℓ. Therefore, the map Φ above yields an R-module isomorphism and any λ-QT code $C \subseteq \mathbb{F}_q^{m\ell} \simeq \mathbb{F}_q^{m\times\ell}$ of index ℓ can be viewed as an R-submodule of R^ℓ.

CRT Decomposition

We assume that $x^m - \lambda$ factors into irreducible polynomials in $\mathbb{F}_q[x]$ as

$$x^m - \lambda = f_1(x) f_2(x) \cdots f_s(x).$$

CRT Decomposition

We assume that $x^m - \lambda$ factors into irreducible polynomials in $\mathbb{F}_q[x]$ as

$$x^m - \lambda = f_1(x) f_2(x) \cdots f_s(x).$$

Since $\gcd(m, q) = 1$, there are no repeating factors. By the Chinese Remainder Theorem (CRT), we have

$$R \cong \bigoplus_{i=1}^{s} \mathbb{F}_q[x]/\langle f_i(x) \rangle.$$

CRT Decomposition

We assume that $x^m - \lambda$ factors into irreducible polynomials in $\mathbb{F}_q[x]$ as

$$x^m - \lambda = f_1(x) f_2(x) \cdots f_s(x).$$

Since $\gcd(m, q) = 1$, there are no repeating factors. By the Chinese Remainder Theorem (CRT), we have

$$R \cong \bigoplus_{i=1}^{s} \mathbb{F}_q[x]/\langle f_i(x) \rangle.$$

For each $i \in \{1, 2, \ldots, s\}$, let u_i be the smallest nonnegative integer such that $f_i(\alpha \xi^{u_i}) = 0$. Since the $f_i(x)$'s are irreducible, the direct summands can be viewed as field extensions of $\mathbb{F}_q$, obtained by adjoining the element $\alpha \xi^{u_i}$. If we set $\mathbb{E}_i := \mathbb{F}_q(\alpha \xi^{u_i}) \cong \mathbb{F}_q[x]/\langle f_i(x) \rangle$, for each $1 \leq i \leq s$, then $\mathbb{E}_i$ is an intermediate field between $\mathbb{F}$ and $\mathbb{F}_q$ such that $\left[\mathbb{E}_i : \mathbb{F}_q\right] = \deg(f_i)$.

CRT Decomposition

We have

$$\begin{array}{rcl} R & \simeq & \mathbb{E}_1 \oplus \cdots \oplus \mathbb{E}_s \\ a(x) & \mapsto & \left(a(\alpha\xi^{u_1}), \ldots, a(\alpha\xi^{u_s})\right). \end{array}$$

CRT Decomposition

We have

$$\begin{aligned} R &\simeq \mathbb{E}_1 \oplus \cdots \oplus \mathbb{E}_s \\ a(x) &\mapsto \left(a(\alpha\xi^{u_1}), \ldots, a(\alpha\xi^{u_s})\right). \end{aligned}$$

This implies that

$$\begin{aligned} R^\ell &\simeq \mathbb{E}_1^\ell \oplus \cdots \oplus \mathbb{E}_s^\ell \\ \mathbf{a}(x) &\mapsto \left(\mathbf{a}(\alpha\xi^{u_1}), \ldots, \mathbf{a}(\alpha\xi^{u_s})\right), \end{aligned}$$

where $\mathbf{a}(\delta)$ denotes the componentwise evaluation at $\delta \in \mathbb{F}$, for any $\mathbf{a}(x) = \big(a_0(x), \ldots, a_{\ell-1}(x)\big) \in R^\ell$.

Constituents

Hence, a λ-QT code $C \subseteq R^\ell$ decomposes as

$$C \simeq C_1 \oplus \cdots \oplus C_s,$$

where C_i is a linear code in $\mathbb{E}_i^\ell$, for each i. These linear codes over various extensions of $\mathbb{F}_q$ are called the *constituents* of C.

Constituents

Hence, a λ-QT code $C \subseteq R^\ell$ decomposes as

$$C \simeq C_1 \oplus \cdots \oplus C_s,$$

where C_i is a linear code in $\mathbb{E}_i^\ell$, for each i. These linear codes over various extensions of $\mathbb{F}_q$ are called the *constituents* of C.

Let $C \subseteq R^\ell$ be generated as an R-module by

$$\left\{ \left(a_{1,0}(x), \ldots, a_{1,\ell-1}(x)\right), \ldots, \left(a_{r,0}(x), \ldots, a_{r,\ell-1}(x)\right) \right\}.$$

Then, for $1 \leq i \leq s$, we have

$$C_i = \mathrm{Span}_{\mathbb{E}_i}\left\{ \left(a_{b,0}(\alpha\xi^{u_i}), \ldots, a_{b,\ell-1}(\alpha\xi^{u_i})\right) : 1 \leq b \leq r \right\}.$$

Constituents

Note that each field $\mathbb{E}_i$ is isomorphic to a minimal λ-constacyclic code of length m over $\mathbb{F}_q$; namely, the λ-constacyclic code in $\mathbb{F}_q^m$ with the irreducible check polynomial $f_i(x)$. If we denote by θ_i the generating primitive idempotent for the minimal λ-constacyclic code $\langle \theta_i \rangle$ in consideration, then the isomorphism is given by the maps

Constituents

Note that each field $\mathbb{E}_i$ is isomorphic to a minimal λ-constacyclic code of length m over $\mathbb{F}_q$; namely, the λ-constacyclic code in $\mathbb{F}_q^m$ with the irreducible check polynomial $f_i(x)$. If we denote by θ_i the generating primitive idempotent for the minimal λ-constacyclic code $\langle\theta_i\rangle$ in consideration, then the isomorphism is given by the maps

$$\begin{array}{rcl} \varphi_i : \langle\theta_i\rangle & \longrightarrow & \mathbb{E}_i \\ a(x) & \longmapsto & a(\alpha\xi^{u_i}) \end{array} \qquad \begin{array}{rcl} \psi_i : \mathbb{E}_i & \longrightarrow & \langle\theta_i\rangle \\ \delta & \longmapsto & \sum_{k=0}^{m-1} a_k x^k, \end{array}$$

where

$$a_k = \frac{1}{m}\mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_q}(\delta\alpha^{-k}\xi^{-ku_i}).$$

Trace Representation

$$\mathbf{c} = \frac{1}{m} \begin{pmatrix} \left(\sum_{i=1}^{s} \mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_q} \left(\kappa_{i,t} \alpha^{-0} \xi^{-0 u_i} \right) \right)_{0 \le t \le \ell-1} \\ \left(\sum_{i=1}^{s} \mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_q} \left(\kappa_{i,t} \alpha^{-1} \xi^{-u_i} \right) \right)_{0 \le t \le \ell-1} \\ \vdots \\ \left(\sum_{i=1}^{s} \mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_q} \left(\kappa_{i,t} \alpha^{-(m-1)} \xi^{-(m-1) u_i} \right) \right)_{0 \le t \le \ell-1} \end{pmatrix}, \qquad (1)$$

where $\kappa_i = (\kappa_{i,0}, \ldots, \kappa_{i,\ell-1}) \in C_i$, for all i. Since $mC = C$, every codeword in C can still be written in the form above with the constant $\frac{1}{m}$ removed.

Concatenation

Theorem

i. *Let C be an R-submodule of R^ℓ (i.e., a q-ary λ-QT code). Then, for some subset $\mathcal{I}$ of $\{1, \ldots, s\}$, there exist linear codes $\mathfrak{C}_i \subseteq \mathbb{E}_i^\ell$ such that*

$$C = \bigoplus_{i \in \mathcal{I}} \langle \theta_i \rangle \square \mathfrak{C}_i.$$

ii. *Conversely, let $\mathfrak{C}_i$ be a linear code over $\mathbb{E}_i$ of length ℓ, for each $i \in \mathcal{I} \subseteq \{1, \ldots, s\}$. Then,*

$$C = \bigoplus_{i \in \mathcal{I}} \langle \theta_i \rangle \square \mathfrak{C}_i$$

is a q-ary λ-QT code of length $m\ell$ and index ℓ.

Concatenation

Theorem

i. *Let C be an R-submodule of R^ℓ (i.e., a q-ary λ-QT code). Then, for some subset $\mathcal{I}$ of $\{1, \ldots, s\}$, there exist linear codes $\mathfrak{C}_i \subseteq \mathbb{E}_i^\ell$ such that*

$$C = \bigoplus_{i \in \mathcal{I}} \langle \theta_i \rangle \square \mathfrak{C}_i.$$

ii. *Conversely, let $\mathfrak{C}_i$ be a linear code over $\mathbb{E}_i$ of length ℓ, for each $i \in \mathcal{I} \subseteq \{1, \ldots, s\}$. Then,*

$$C = \bigoplus_{i \in \mathcal{I}} \langle \theta_i \rangle \square \mathfrak{C}_i$$

is a q-ary λ-QT code of length $m\ell$ and index ℓ.

Moreover, each constituent C_i is equal to the outer code $\mathfrak{C}_i$ in the concatenated structure, for each i.

The Jensen bound

Theorem

Let $C \subseteq R^\ell$ be a λ-QT code with the concatenated structure

$$C = \bigoplus_{i \in \mathcal{I}} \langle \theta_i \rangle \square C_i,$$

for some $\mathcal{I} \subseteq \{1, \ldots, s\}$. Let $C_{i_1}, \ldots, C_{i_t}$ be the nonzero constituents of C, for $\{i_1, \ldots, i_t\} \subseteq \mathcal{I}$, such that $d(C_{i_1}) \leq d(C_{i_2}) \leq \cdots \leq d(C_{i_t})$. Then

$$d(C) \geq \min_{1 \leq r \leq t} \left\{ d(C_{i_r}) d(\langle \theta_{i_1} \rangle \oplus \cdots \oplus \langle \theta_{i_r} \rangle) \right\}. \tag{2}$$

Spectral Theory

Consider the ring homomorphism:

$$\begin{array}{rcl} \Psi \ : \ \mathbb{F}_q[x]^\ell & \longrightarrow & R^\ell \\ (\widetilde{f}_0(x), \ldots, \widetilde{f}_{\ell-1}(x)) & \longmapsto & (f_0(x), \ldots, f_{\ell-1}(x)). \end{array}$$

Spectral Theory

Consider the ring homomorphism:

$$\begin{array}{rcl} \Psi \ : \ \mathbb{F}_q[x]^\ell & \longrightarrow & R^\ell \\ (\widetilde{f}_0(x), \ldots, \widetilde{f}_{\ell-1}(x)) & \longmapsto & (f_0(x), \ldots, f_{\ell-1}(x)). \end{array}$$

Given a λ-QT code $C \subseteq R^\ell$, it follows that the preimage $\widetilde{C}$ of C in $\mathbb{F}_q[x]^\ell$ is an $\mathbb{F}_q[x]$-submodule containing $\widetilde{K} = \{(x^m - \lambda)\mathbf{e}_j : 0 \leq j \leq \ell - 1\}$, where each $\mathbf{e}_j$ denotes the standard basis vector of length ℓ with 1 at the j^{th} coordinate and 0 elsewhere.

Spectral Theory

Consider the ring homomorphism:

$$\begin{array}{rcl} \Psi \ : \ \mathbb{F}_q[x]^\ell & \longrightarrow & R^\ell \\ (\widetilde{f}_0(x), \ldots, \widetilde{f}_{\ell-1}(x)) & \longmapsto & (f_0(x), \ldots, f_{\ell-1}(x)). \end{array}$$

Given a λ-QT code $C \subseteq R^\ell$, it follows that the preimage $\widetilde{C}$ of C in $\mathbb{F}_q[x]^\ell$ is an $\mathbb{F}_q[x]$-submodule containing $\widetilde{K} = \{(x^m - \lambda)\mathbf{e}_j : 0 \leq j \leq \ell - 1\}$, where each $\mathbf{e}_j$ denotes the standard basis vector of length ℓ with 1 at the j^{th} coordinate and 0 elsewhere.

Since $\widetilde{C}$ is a submodule of $\mathbb{F}_q[x]^\ell$ and contains $\widetilde{K}$, it has a generating set of the form

$$\{\mathbf{u}_1, \ldots, \mathbf{u}_p, (x^m - \lambda)\mathbf{e}_0, \ldots, (x^m - \lambda)\mathbf{e}_{\ell-1}\},$$

where $p \geq 0$, $\mathbf{u}_b = (u_{b,0}(x), \ldots, u_{b,\ell-1}(x)) \in \mathbb{F}_q[x]^\ell$, for each $b \in \{1, \ldots, p\}$.

Spectral Theory

Hence, the rows of

$$\mathcal{G} = \begin{pmatrix} u_{1,0}(x) & \dots & u_{1,\ell-1}(x) \\ \vdots & & \vdots \\ u_{p,0}(x) & \dots & u_{p,\ell-1}(x) \\ x^m - \lambda & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & x^m - \lambda \end{pmatrix}$$

generate $\widetilde{C}$. By using elementary row operations, we triangularise $\mathcal{G}$ so that another equivalent generating set is obtained from the rows of an upper-triangular $\ell \times \ell$ matrix over $\mathbb{F}_q[x]$ as:

Spectral Theory

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

where

1. $g_{i,j}(x) = 0$, for all $0 \leq j < i \leq \ell - 1$.
2. $\deg(g_{i,j}(x)) < \deg(g_{j,j}(x))$, for all $i < j$.
3. $g_{i,i}(x) \mid (x^m - \lambda)$, for all $0 \leq i \leq \ell - 1$.
4. If $g_{i,i}(x) = (x^m - \lambda)$, then $g_{i,j}(x) = 0$, for all $i \neq j$.

Spectral Theory

The *determinant* of $\widetilde{G}(x)$ is defined as

$$\det(\widetilde{G}(x)) := \prod_{j=0}^{\ell-1} g_{j,j}(x).$$

Spectral Theory

The *determinant* of $\widetilde{G}(x)$ is defined as

$$\det(\widetilde{G}(x)) := \prod_{j=0}^{\ell-1} g_{j,j}(x).$$

An *eigenvalue* β of C is a root of $\det(\widetilde{G}(x))$. Note that all eigenvalues are elements of Ω, since $g_{j,j}(x) \mid (x^m - \lambda)$, for each $0 \leq j \leq \ell - 1$.

Spectral Theory

The *determinant* of $\widetilde{G}(x)$ is defined as

$$\det(\widetilde{G}(x)) := \prod_{j=0}^{\ell-1} g_{j,j}(x).$$

An *eigenvalue* β of C is a root of $\det(\widetilde{G}(x))$. Note that all eigenvalues are elements of Ω, since $g_{j,j}(x) \mid (x^m - \lambda)$, for each $0 \leq j \leq \ell - 1$.

The null space of $\widetilde{G}(\beta)$ is called the *eigenspace* of β, denoted by $\mathcal{V}_\beta$, such that

$$\mathcal{V}_\beta := \{\mathbf{v} \in \mathbb{F}^\ell : \widetilde{G}(\beta)\mathbf{v}^\top = \mathbf{0}_\ell^\top\},$$

where $\mathbb{F}$ is the splitting field of $x^m - \lambda$ as before.

Spectral Theory

The *determinant* of $\widetilde{G}(x)$ is defined as

$$\det(\widetilde{G}(x)) := \prod_{j=0}^{\ell-1} g_{j,j}(x).$$

An *eigenvalue* β of C is a root of $\det(\widetilde{G}(x))$. Note that all eigenvalues are elements of Ω, since $g_{j,j}(x) \mid (x^m - \lambda)$, for each $0 \leq j \leq \ell - 1$.

The null space of $\widetilde{G}(\beta)$ is called the *eigenspace* of β, denoted by $\mathcal{V}_\beta$, such that

$$\mathcal{V}_\beta := \{\mathbf{v} \in \mathbb{F}^\ell : \widetilde{G}(\beta)\mathbf{v}^\top = \mathbf{0}_\ell^\top\},$$

where $\mathbb{F}$ is the splitting field of $x^m - \lambda$ as before.

Let $\overline{\Omega} \subseteq \Omega$ denote the set of all eigenvalues of C. Note that $\overline{\Omega} = \emptyset$ iff each $g_{j,j}(x)$ in $\widetilde{G}(x)$ is constant and C is the trivial full space code. From this point on, we exclude the full space code and we assume that $|\overline{\Omega}| = t > 0$.

Spectral Theory

Choose an arbitrary eigenvalue $\beta_i \in \overline{\Omega}$, for some $i \in \{1, \ldots, t\}$. Let $\{\mathbf{v}_{i,0}, \ldots, \mathbf{v}_{i,n_i-1}\}$ be a basis for the corresponding eigenspace $\mathcal{V}_i$.

Spectral Theory

Choose an arbitrary eigenvalue $\beta_i \in \overline{\Omega}$, for some $i \in \{1, \ldots, t\}$. Let $\{\mathbf{v}_{i,0}, \ldots, \mathbf{v}_{i,n_i-1}\}$ be a basis for the corresponding eigenspace $\mathcal{V}_i$.

$$V_i := \begin{pmatrix} \mathbf{v}_{i,0} \\ \vdots \\ \mathbf{v}_{i,n_i-1} \end{pmatrix} = \begin{pmatrix} v_{i,0,0} & \cdots & v_{i,0,\ell-1} \\ \vdots & \vdots & \vdots \\ v_{i,n_i-1,0} & \cdots & v_{i,n_i-1,\ell-1} \end{pmatrix},$$

Spectral Theory

Choose an arbitrary eigenvalue $\beta_i \in \overline{\Omega}$, for some $i \in \{1, \ldots, t\}$. Let $\{\mathbf{v}_{i,0}, \ldots, \mathbf{v}_{i,n_i-1}\}$ be a basis for the corresponding eigenspace $\mathcal{V}_i$.

$$V_i := \begin{pmatrix} \mathbf{v}_{i,0} \\ \vdots \\ \mathbf{v}_{i,n_i-1} \end{pmatrix} = \begin{pmatrix} v_{i,0,0} & \cdots & v_{i,0,\ell-1} \\ \vdots & \vdots & \vdots \\ v_{i,n_i-1,0} & \cdots & v_{i,n_i-1,\ell-1} \end{pmatrix},$$

We let

$$H_i := (1, \beta_i, \ldots, \beta_i^{m-1}) \otimes V_i$$

and define

$$H := \begin{pmatrix} H_1 \\ \vdots \\ H_t \end{pmatrix} = \begin{pmatrix} V_1 & \beta_1 V_1 & \ldots & \beta_1^{m-1} V_1 \\ \vdots & \vdots & & \vdots \\ V_t & \beta_t V_t & \ldots & \beta_t^{m-1} V_t \end{pmatrix}.$$

Spectral Theory

Choose an arbitrary eigenvalue $\beta_i \in \overline{\Omega}$, for some $i \in \{1, \ldots, t\}$. Let $\{\mathbf{v}_{i,0}, \ldots, \mathbf{v}_{i,n_i-1}\}$ be a basis for the corresponding eigenspace $\mathcal{V}_i$.

$$V_i := \begin{pmatrix} \mathbf{v}_{i,0} \\ \vdots \\ \mathbf{v}_{i,n_i-1} \end{pmatrix} = \begin{pmatrix} v_{i,0,0} & \cdots & v_{i,0,\ell-1} \\ \vdots & \vdots & \vdots \\ v_{i,n_i-1,0} & \cdots & v_{i,n_i-1,\ell-1} \end{pmatrix},$$

We let

$$H_i := (1, \beta_i, \ldots, \beta_i^{m-1}) \otimes V_i$$

and define

$$H := \begin{pmatrix} H_1 \\ \vdots \\ H_t \end{pmatrix} = \begin{pmatrix} V_1 & \beta_1 V_1 & \ldots & \beta_1^{m-1} V_1 \\ \vdots & \vdots & & \vdots \\ V_t & \beta_t V_t & \ldots & \beta_t^{m-1} V_t \end{pmatrix}.$$

Proposition

The matrix H is a parity-check matrix for C.

Spectral bound

Definition

We define the *eigencode* corresponding to an eigenspace $\mathcal{V} \subseteq \mathbb{F}^{\ell}$ by

$$\mathbb{C}(\mathcal{V}) = \mathbb{C} := \left\{ \mathbf{u} \in \mathbb{F}_q^{\ell} \ : \ \sum_{j=0}^{\ell-1} v_j u_j = 0, \forall \mathbf{v} \in \mathcal{V} \right\}.$$

In case we have $\mathbb{C} = \{\mathbf{0}_{\ell}\}$, then it is assumed that $d(\mathbb{C}) = \infty$.

Spectral bound

Definition

We define the *eigencode* corresponding to an eigenspace $\mathcal{V} \subseteq \mathbb{F}^\ell$ by

$$\mathbb{C}(\mathcal{V}) = \mathbb{C} := \left\{ \mathbf{u} \in \mathbb{F}_q^\ell \ : \ \sum_{j=0}^{\ell-1} v_j u_j = 0, \forall \mathbf{v} \in \mathcal{V} \right\}.$$

In case we have $\mathbb{C} = \{\mathbf{0}_\ell\}$, then it is assumed that $d(\mathbb{C}) = \infty$.

Theorem

Let C be a λ-QT code of index ℓ with eigenvalue set $\emptyset \neq \overline{\Omega} \subseteq \Omega$, let $D_{\overline{\Omega}}$ be the λ-constacyclic code of length m over $\mathbb{F}$ with zero set $\overline{\Omega}$ and let $\mathcal{B}(D_{\overline{\Omega}}) \subseteq \mathcal{P}(\Omega) \times (\mathbb{N} \cup \{\infty\})$ be an arbitrary family of defining set bounds for $D_{\overline{\Omega}}$. For any $\emptyset \neq P \subseteq \overline{\Omega}$ such that $(P, d_P) \in \mathcal{B}(D_{\overline{\Omega}})$, we define $\mathcal{V}_P := \bigcap_{\beta \in P} \mathcal{V}_\beta$ as the common eigenspace of the eigenvalues in P and let $\mathbb{C}_P$ denote the corresponding eigencode. Then,

$$d(C) \geq \min\{d_P, d(\mathbb{C}_P)\}.$$

Contraction Idea

Let $\gcd(m, q) = 1$ and $r \mid q - 1$ with $\lambda^r = 1$, for some nonzero element $\lambda \in \mathbb{F}_q$.

Contraction Idea

Let $\gcd(m, q) = 1$ and $r \mid q - 1$ with $\lambda^r = 1$, for some nonzero element $\lambda \in \mathbb{F}_q$.

- $[m\ell, k, d]_q$ λ-QT code $\Longrightarrow$ $[rm\ell, k, rd]_q$ QC code

Contraction Idea

Let $\gcd(m, q) = 1$ and $r \mid q - 1$ with $\lambda^r = 1$, for some nonzero element $\lambda \in \mathbb{F}_q$.

- $[m\ell, k, d]_q$ λ-QT code $\Longrightarrow$ $[rm\ell, k, rd]_q$ QC code
- $[rm\ell, k, d]_q$ QC code $\Longrightarrow$ $[m\ell, k, d/r]_q$ λ-QT code

Contraction Idea

Recall that $\gcd(m, q) = 1$ and $r \mid q - 1$ with $\lambda^r = 1$, for some nonzero element $\lambda \in \mathbb{F}_q$.

Contraction Idea

Recall that $\gcd(m, q) = 1$ and $r \mid q - 1$ with $\lambda^r = 1$, for some nonzero element $\lambda \in \mathbb{F}_q$.

- We obtain analogous conditons to have a contraction
  $[rm\ell, k, d]_q$ QC code $\Longrightarrow$ $[m\ell, k, d/r]_q$ λ-QT code

Contraction Idea

Recall that $\gcd(m, q) = 1$ and $r \mid q - 1$ with $\lambda^r = 1$, for some nonzero element $\lambda \in \mathbb{F}_q$.

- We obtain analogous conditons to have a contraction
  $[rm\ell, k, d]_q$ QC code $\Longrightarrow$ $[m\ell, k, d/r]_q$ λ-QT code

- Note that k does not change.

Contraction Idea

Recall that $\gcd(m, q) = 1$ and $r \mid q - 1$ with $\lambda^r = 1$, for some nonzero element $\lambda \in \mathbb{F}_q$.

- We obtain analogous conditons to have a contraction
  $[rm\ell, k, d]_q$ QC code $\Longrightarrow$ $[m\ell, k, d/r]_q$ λ-QT code
- Note that k does not change.
- Then we also have new lower bounds of λ-QT codes considered as contractions.

Thanks for your attention!