Multidimensional Quasi-Cyclic and Convolutional Codes

Buket Özkaya

joint work with Cem Güneri

7 May 2015

For m, ℓ integers with $(m, q) = 1$, a QC code of length $m\ell$ and index ℓ over $\mathbb{F}_q$ is a linear code $\mathcal{C} \subseteq \mathbb{F}_q^{m\ell}$, if it is invariant under shift of codewords by ℓ positions.

For m, ℓ integers with $(m, q) = 1$, a QC code of length $m\ell$ and index ℓ over $\mathbb{F}_q$ is a linear code $\mathcal{C} \subseteq \mathbb{F}_q^{m\ell}$, if it is invariant under shift of codewords by ℓ positions.

$$c = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix} \in \mathbb{F}_q^{m\times\ell} \simeq \mathbb{F}_q^{m\ell}$$

Invariance under shift by ℓ units is equivalent to being closed under row shift. In particular, a QC code of index $\ell = 1$ is a cyclic code.

For m, ℓ integers with $(m, q) = 1$, a QC code of length $m\ell$ and index ℓ over $\mathbb{F}_q$ is a linear code $\mathcal{C} \subseteq \mathbb{F}_q^{m\ell}$, if it is invariant under shift of codewords by ℓ positions.

$$c = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix} \in \mathbb{F}_q^{m \times \ell} \simeq \mathbb{F}_q^{m\ell}$$

Invariance under shift by ℓ units is equivalent to being closed under row shift. In particular, a QC code of index $\ell = 1$ is a cyclic code.

If $\mathcal{C}$ is also closed under column shift, then it's called a 2D cyclic code.

Algebraic Structure

The codewords of a cyclic code can be viewed as polynomials via the identification:

$$\begin{array}{ccc} \mathbb{F}_q^m & \longrightarrow & \mathbb{F}_q[x]/\langle x^m - 1\rangle = R \\ \begin{pmatrix} c_0 \\ \vdots \\ c_{m-1} \end{pmatrix} & \mapsto & c(x) = \displaystyle\sum_{i=0}^{m-1} c_i x^i \end{array}$$

The shift by 1 unit corresponds to $x.c(x) \Rightarrow$ a cyclic code is an ideal in R.

Algebraic Structure

Similarly one can define a QC code in R^ℓ:

$$\begin{array}{ccc} \mathbb{F}_q^{m\times \ell} & \longrightarrow & R^\ell \\ \begin{pmatrix} c_{00} & c_{01} & \cdots & c_{0,\ell-1} \\ \vdots & \vdots & & \vdots \\ c_{m-1,0} & c_{m-1,1} & \cdots & c_{m-1,\ell-1} \end{pmatrix} & \mapsto & \vec{c}(x) = (c_0(x), \ldots, c_{\ell-1}(x)) \end{array}$$

where $c_j(x) = \displaystyle\sum_{i=0}^{m-1} c_{ij}x^i$, $\forall\ 0 \le j \le \ell - 1$.

Algebraic Structure

Similarly one can define a QC code in R^ℓ:

$$\begin{array}{ccc} \mathbb{F}_q^{m\times\ell} & \longrightarrow & R^\ell \\ \begin{pmatrix} c_{00} & c_{01} & \cdots & c_{0,\ell-1} \\ \vdots & \vdots & & \vdots \\ c_{m-1,0} & c_{m-1,1} & \cdots & c_{m-1,\ell-1} \end{pmatrix} & \mapsto & \vec{c}(x) = (c_0(x), \ldots, c_{\ell-1}(x)) \end{array}$$

where $c_j(x) = \sum_{i=0}^{m-1} c_{ij}x^i$, $\forall\ 0 \le j \le \ell - 1$.

Row shift in $\mathbb{F}_q^{m\times\ell}$ corresponds to coordinatewise multiplication by x in R^ℓ.

Algebraic Structure

Similarly one can define a QC code in R^ℓ:

$$\begin{array}{ccc} \mathbb{F}_q^{m\times\ell} & \longrightarrow & R^\ell \\ \begin{pmatrix} c_{00} & c_{01} & \cdots & c_{0,\ell-1} \\ \vdots & \vdots & & \vdots \\ c_{m-1,0} & c_{m-1,1} & \cdots & c_{m-1,\ell-1} \end{pmatrix} & \mapsto & \vec{c}(x) = (c_0(x), \ldots, c_{\ell-1}(x)) \end{array}$$

where $c_j(x) = \sum_{i=0}^{m-1} c_{ij}x^i$, $\forall\ 0 \le j \le \ell - 1$.

Row shift in $\mathbb{F}_q^{m\times\ell}$ corresponds to coordinatewise multiplication by x in R^ℓ.
$\Rightarrow \mathcal{C} \subseteq R^\ell$ is an R-submodule.

Algebraic Structure

Let $S := \mathbb{F}_q[x, y]/\langle x^m - 1, y^\ell - 1\rangle$ and view a codeword $c = (c_{ij}) \in \mathcal{C}$ as a 2-variate polynomial in S:

$$c(x, y) = \sum_{i=0}^{m-1} \sum_{j=0}^{\ell-1} c_{ij} x^i y^j$$

Algebraic Structure

Let $S := \mathbb{F}_q[x,y]/\langle x^m - 1, y^\ell - 1\rangle$ and view a codeword $c = (c_{ij}) \in \mathcal{C}$ as a 2-variate polynomial in S:

$$c(x,y) = \sum_{i=0}^{m-1} \sum_{j=0}^{\ell-1} c_{ij} x^i y^j$$

Then

$$\mathcal{C} \text{ is QC} \Leftrightarrow \mathcal{C} \text{ is an } R\text{-submodule in } S.$$
$$\mathcal{C} \text{ is 2D-cyclic} \Leftrightarrow \mathcal{C} \text{ is an ideal in } S.$$

Constituents (Ling-Solé, 2001)

Consider the factorization of $x^m - 1$ into irreducibles in $\mathbb{F}_q[x]$:

$$x^m - 1 = f_1(x) \ldots f_s(x)$$

Constituents (Ling-Solé, 2001)

Consider the factorization of $x^m - 1$ into irreducibles in $\mathbb{F}_q[x]$:

$$x^m - 1 = f_1(x) \dots f_s(x)$$

Since $(m, q) = 1$, there are no repeating factors. By CRT we have:

$$R = \mathbb{F}_q[x]/\langle x^m - 1\rangle \simeq \mathbb{F}_q[x]/\langle f_1(x)\rangle \oplus \dots \oplus \mathbb{F}_q[x]/\langle f_s(x)\rangle$$

Constituents (Ling-Solé, 2001)

Consider the factorization of $x^m - 1$ into irreducibles in $\mathbb{F}_q[x]$:

$$x^m - 1 = f_1(x) \dots f_s(x)$$

Since $(m, q) = 1$, there are no repeating factors. By CRT we have:

$$R = \mathbb{F}_q[x]/\langle x^m - 1\rangle \simeq \mathbb{F}_q[x]/\langle f_1(x)\rangle \oplus \dots \oplus \mathbb{F}_q[x]/\langle f_s(x)\rangle$$

$$R \simeq \mathbb{E}_1 \oplus \dots \oplus \mathbb{E}_s \;\Rightarrow\; R^\ell \simeq \bigoplus_{i=1}^{s} \mathbb{E}_i^\ell$$

Constituents (Ling-Solé, 2001)

Consider the factorization of $x^m - 1$ into irreducibles in $\mathbb{F}_q[x]$:

$$x^m - 1 = f_1(x) \ldots f_s(x)$$

Since $(m, q) = 1$, there are no repeating factors. By CRT we have:

$$R = \mathbb{F}_q[x]/\langle x^m - 1 \rangle \simeq \mathbb{F}_q[x]/\langle f_1(x) \rangle \oplus \ldots \oplus \mathbb{F}_q[x]/\langle f_s(x) \rangle$$

$$R \simeq \mathbb{E}_1 \oplus \ldots \oplus \mathbb{E}_s \;\Rightarrow\; R^\ell \simeq \bigoplus_{i=1}^{s} \mathbb{E}_i^\ell$$

Hence, $\mathcal{C} = \bigoplus_{i=1}^{s} \mathcal{C}_i$ where $\mathcal{C}_i \subseteq \mathbb{E}_i^\ell$ is a length ℓ code over $\mathbb{E}_i$ for each $1 \leq i \leq s$. $\mathcal{C}_i$'s are said to be the *constituents* of $\mathcal{C}$.

Concatenated Form

Let $\langle\theta_i\rangle$ be the minimal cyclic code of length m over $\mathbb{F}_q$ with the check polynomial $f_i(x)$ and the primitive idempotent generator θ_i. Note that $\langle\theta_i\rangle$ is isomorphic to $\mathbb{E}_i = \mathbb{F}_{q^{\deg f_i}}$.

Concatenated Form

Let $\langle\theta_i\rangle$ be the minimal cyclic code of length m over $\mathbb{F}_q$ with the check polynomial $f_i(x)$ and the primitive idempotent generator θ_i. Note that $\langle\theta_i\rangle$ is isomorphic to $\mathbb{E}_i = \mathbb{F}_{q^{\deg f_i}}$.

Theorem (Jensen, 1985)

Let C be a QC code. For some subset $\mathcal{I}$ of $\{1,\ldots,s\}$, we have

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

where $\mathfrak{C}_i$ is a linear code over $\mathbb{E}_i$ of length ℓ. Converse also holds.

Concatenated Form

Let $\langle \theta_i \rangle$ be the minimal cyclic code of length m over $\mathbb{F}_q$ with the check polynomial $f_i(x)$ and the primitive idempotent generator θ_i. Note that $\langle \theta_i \rangle$ is isomorphic to $\mathbb{E}_i = \mathbb{F}_{q^{\deg f_i}}$.

Theorem (Jensen, 1985)

Let C be a QC code. For some subset $\mathcal{I}$ of $\{1, \ldots, s\}$, we have

$$C = \bigoplus_{i \in \mathcal{I}} (\langle \theta_i \rangle \Box \mathfrak{C}_i),$$

where $\mathfrak{C}_i$ is a linear code over $\mathbb{E}_i$ of length ℓ. Converse also holds.

Theorem (Güneri-Özbudak, 2013)

$\mathfrak{C}_i = \mathcal{C}_i$ for each i.

Convolutional Codes

An (ℓ, k) convolutional code C over $\mathbb{F}_q$ is defined as a k-dimensional $\mathbb{F}_q(x)$-subspace of $\mathbb{F}_q(x)^\ell$.

Convolutional Codes

An (ℓ, k) convolutional code C over $\mathbb{F}_q$ is defined as a k-dimensional $\mathbb{F}_q(x)$-subspace of $\mathbb{F}_q(x)^\ell$.

A generator matrix of C is a $k \times \ell$ matrix over $\mathbb{F}_q(x)$. By clearing off the denominators of all the entries in any generating matrix, we can obtain a PGM for C such that

$$C = \left\{ (u_0(x), \ldots, u_{k-1}(x))\, G : \ (u_0(x), \ldots, u_{k-1}(x)) \in \mathbb{F}_q(x)^k \right\}.$$

Convolutional Codes

An (ℓ, k) convolutional code C over $\mathbb{F}_q$ is defined as a k-dimensional $\mathbb{F}_q(x)$-subspace of $\mathbb{F}_q(x)^\ell$.

A generator matrix of C is a $k \times \ell$ matrix over $\mathbb{F}_q(x)$. By clearing off the denominators of all the entries in any generating matrix, we can obtain a PGM for C such that

$$C = \left\{ (u_0(x), \ldots, u_{k-1}(x))\, G : \ (u_0(x), \ldots, u_{k-1}(x)) \in \mathbb{F}_q(x)^k \right\}.$$

Moreover, it is usually assumed that G is noncatastrophic in the sense that finite weight outputs come from finite weight inputs:

i. G is noncatastrophic if and only if the g.c.d. of all $k \times k$ minors of G is x^b for some nonnegative integer b.
ii. G is basic if and only if the g.c.d. of all $k \times k$ minors of G is 1.

Convolutional Codes vs. QC Codes

If C is given with a basic PGM, which exists for any convolutional code (McEliece), then all polynomial codewords come from polynomial information words. Moreover, a basic PGM has a polynomial right inverse.

Convolutional Codes vs. QC Codes

If C is given with a basic PGM, which exists for any convolutional code (McEliece), then all polynomial codewords come from polynomial information words. Moreover, a basic PGM has a polynomial right inverse.

An (ℓ, k) convolutional code over $\mathbb{F}_q$ can be viewed as an $\mathbb{F}_q[x]$-submodule of $\mathbb{F}_q[x]^\ell$.

Convolutional Codes vs. QC Codes

If C is given with a basic PGM, which exists for any convolutional code (McEliece), then all polynomial codewords come from polynomial information words. Moreover, a basic PGM has a polynomial right inverse.

An (ℓ, k) convolutional code over $\mathbb{F}_q$ can be viewed as an $\mathbb{F}_q[x]$-submodule of $\mathbb{F}_q[x]^\ell$.

(Tanner, Solomon-van Tilborg, Levy-Costello, Lally)
For $\mathcal{C} \subseteq \mathbb{F}_q[x]^\ell$ a convolutional code, define an associated QC code as $\bar{\mathcal{C}} = \mathcal{C}/\langle x^m - 1\rangle \subseteq (\mathbb{F}_q[x]/\langle x^m - 1\rangle)^\ell$.

Convolutional Codes vs. QC Codes

If C is given with a basic PGM, which exists for any convolutional code (McEliece), then all polynomial codewords come from polynomial information words. Moreover, a basic PGM has a polynomial right inverse.

An (ℓ, k) convolutional code over $\mathbb{F}_q$ can be viewed as an $\mathbb{F}_q[x]$-submodule of $\mathbb{F}_q[x]^\ell$.

(Tanner, Solomon-van Tilborg, Levy-Costello, Lally)
For $\mathcal{C} \subseteq \mathbb{F}_q[x]^\ell$ a convolutional code, define an associated QC code as $\bar{\mathcal{C}} = \mathcal{C}/\langle x^m - 1\rangle \subseteq (\mathbb{F}_q[x]/\langle x^m - 1\rangle)^\ell$.

Theorem (Lally)

$d_f(\mathcal{C}) \geq d(\bar{\mathcal{C}})$

Convolutional Codes vs. QC Codes

Idea: $\vec{c'}(x) = \vec{c}(x) \mod (x^m - 1)$

Convolutional Codes vs. QC Codes

Idea: $\vec{c'}(x) = \vec{c}(x) \mod (x^m - 1)$

Case 1: $\vec{c'}(x) \neq 0 \Rightarrow wt(\vec{c}(x)) \geq wt(\vec{c'}(x))$.

Convolutional Codes vs. QC Codes

Idea: $\vec{c'}(x) = \vec{c}(x) \mod (x^m - 1)$

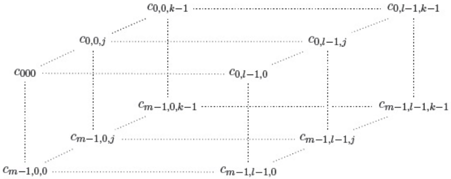
Case 1: $\vec{c'}(x) \neq 0 \Rightarrow wt(\vec{c}(x)) \geq wt(\vec{c'}(x))$.

Case 2: $\vec{c'}(x) = 0 \Rightarrow \vec{c}(x) = (x^m - 1)^\gamma \cdot \vec{y}(x)$
Then consider $\vec{y}(x) \in C$ and $\vec{y'}(x) = \vec{y}(x) \mod (x^m - 1)$

$\Rightarrow \vec{y'}(x) \in C'$ and $wt(\vec{c}(x)) \geq wt(\vec{y'}(x))$ (Massey, Costello, Justesen).

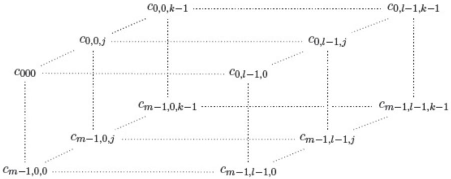
3D codes

For m, ℓ, k integers with $(m, q) = 1$, consider a $\mathbb{F}_q$-linear code whose codewords are viewed as cubes in $\mathbb{F}_q^{m\times\ell\times k}$:

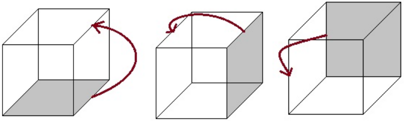


3D codes

For m, ℓ, k integers with $(m, q) = 1$, consider a $\mathbb{F}_q$-linear code whose codewords are viewed as cubes in $\mathbb{F}_q^{m \times \ell \times k}$:

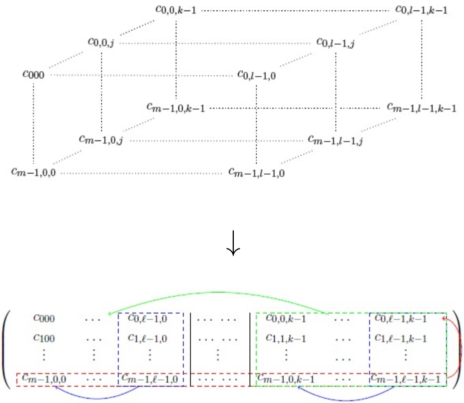


We call C a 3D cyclic code if it is closed under bottom-to-top, right-to-left and back-to-front face shifts of its codewords.

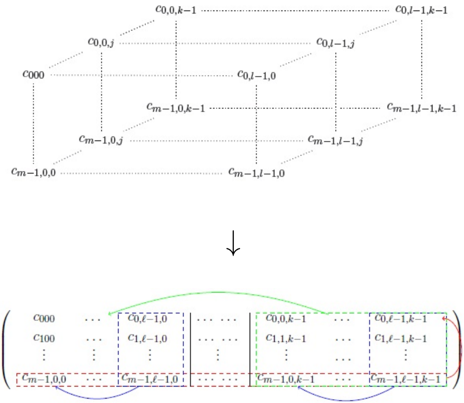


A 3D cyclic code can be viewed as an index ℓk QC code, if we put its codewords into a 2D form:

A 3D cyclic code can be viewed as an index ℓk QC code, if we put its codewords into a 2D form:



A 3D cyclic code can be viewed as an index ℓk QC code, if we put its codewords into a 2D form:

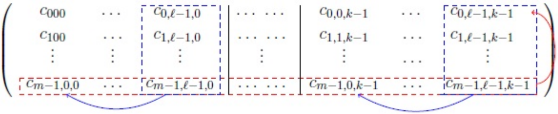


The face shifts in the 3D representation correspond to row shift, column shift in each $m \times \ell$ subarrays and $m \times \ell$ block shift, respectively.

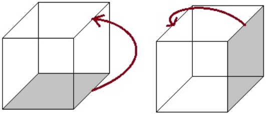
$C \subset \mathbb{F}_q^{m\times \ell k}$ is called a quasi 2D cyclic (Q2DC) code if its codewords are closed under row shift and column shifts in each $m \times \ell$ subarrays.

$$\left(\begin{array}{ccc|cc|ccc}
c_{000} & \cdots & c_{0,\ell-1,0} & \cdots & \cdots & c_{0,0,k-1} & \cdots & c_{0,\ell-1,k-1} \\
c_{100} & \cdots & c_{1,\ell-1,0} & \cdots & \cdots & c_{1,1,k-1} & \cdots & c_{1,\ell-1,k-1} \\
\vdots & \vdots & \vdots & \vdots & & \vdots & \cdots & \vdots \\
c_{m-1,0,0} & \cdots & c_{m-1,\ell-1,0} & \cdots & \cdots & c_{m-1,0,k-1} & \cdots & c_{m-1,\ell-1,k-1}
\end{array}\right)$$

$C \subset \mathbb{F}_q^{m\times \ell k}$ is called a quasi 2D cyclic (Q2DC) code if its codewords are closed under row shift and column shifts in each $m \times \ell$ subarrays.



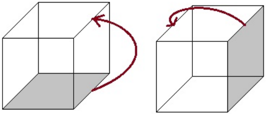
In other words, the codewords of a Q2DC code $C \subset \mathbb{F}_q^{m\times \ell \times k}$ are closed under bottom-to-top, right-to-left shifts.



$C \subset \mathbb{F}_q^{m \times \ell k}$ is called a quasi 2D cyclic (Q2DC) code if its codewords are closed under row shift and column shifts in each $m \times \ell$ subarrays.

$$\left(\begin{array}{ccc|cc|ccc} c_{000} & \cdots & c_{0,\ell-1,0} & \cdots & \cdots & c_{0,0,k-1} & \cdots & c_{0,\ell-1,k-1} \\ c_{100} & \cdots & c_{1,\ell-1,0} & \cdots & \cdots & c_{1,1,k-1} & \cdots & c_{1,\ell-1,k-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \cdots & \vdots \\ c_{m-1,0,0} & \cdots & c_{m-1,\ell-1,0} & \cdots & \cdots & c_{m-1,0,k-1} & \cdots & c_{m-1,\ell-1,k-1} \end{array}\right)$$

In other words, the codewords of a Q2DC code $C \subset \mathbb{F}_q^{m \times \ell \times k}$ are closed under bottom-to-top, right-to-left shifts.



Observe that for $k = 1$ we get a 2D cyclic code.

Algebraic Structure

Q2DC codes are S-submodules in S^k, where the codewords can be written as

$$\vec{c}(x, y) = (c_0(x, y), \ldots, c_{k-1}(x, y))$$

such that $c_t(x, y) = \sum_{i=1}^{m-1} \sum_{j=1}^{\ell-1} c_{ijt} x^i y^j \in S$, $0 \leq t \leq k-1$.

Algebraic Structure

Q2DC codes are S-submodules in S^k, where the codewords can be written as

$$\vec{c}(x,y) = (c_0(x,y), \ldots, c_{k-1}(x,y))$$

such that $c_t(x,y) = \sum_{i=1}^{m-1} \sum_{j=1}^{\ell-1} c_{ijt} x^i y^j \in S$, $0 \le t \le k-1$.

Equivalently, view them as elements of $T = \mathbb{F}_q[x,y,z]/\langle x^m - 1, y^\ell - 1, z^k - 1 \rangle$ such that

$$c(x,y,z) = \sum_{i=1}^{m-1} \sum_{j=1}^{\ell-1} \sum_{t=1}^{k-1} c_{ijt} x^i y^j z^t$$

.

Algebraic Structure

Q2DC codes are S-submodules in S^k, where the codewords can be written as

$$\vec{c}(x,y) = (c_0(x,y), \ldots, c_{k-1}(x,y))$$

such that $c_t(x,y) = \sum_{i=1}^{m-1} \sum_{j=1}^{\ell-1} c_{ijt} x^i y^j \in S$, $0 \leq t \leq k-1$.
Equivalently, view them as elements of $T = \mathbb{F}_q[x,y,z]/\langle x^m - 1, y^\ell - 1, z^k - 1 \rangle$ such that

$$c(x,y,z) = \sum_{i=1}^{m-1} \sum_{j=1}^{\ell-1} \sum_{t=1}^{k-1} c_{ijt} x^i y^j z^t$$

.

Invariance under face shifts in $\mathcal{C}$ amounts to being closed under multiplication by x, y and z in T.

Algebraic Structure

Q2DC codes are S-submodules in S^k, where the codewords can be written as

$$\vec{c}(x,y) = (c_0(x,y), \ldots, c_{k-1}(x,y))$$

such that $c_t(x,y) = \sum_{i=1}^{m-1} \sum_{j=1}^{\ell-1} c_{ijt} x^i y^j \in S$, $0 \le t \le k-1$.

Equivalently, view them as elements of $T = \mathbb{F}_q[x,y,z]/\langle x^m - 1, y^\ell - 1, z^k - 1\rangle$ such that

$$c(x,y,z) = \sum_{i=1}^{m-1} \sum_{j=1}^{\ell-1} \sum_{t=1}^{k-1} c_{ijt} x^i y^j z^t$$

.

Invariance under face shifts in $\mathcal{C}$ amounts to being closed under multiplication by x, y and z in T.

$\mathcal{C}$ is Q2DC $\Leftrightarrow$ $\mathcal{C}$ is an S-submodule of T
$\mathcal{C}$ is 3D-cyclic $\Leftrightarrow$ $\mathcal{C}$ is an ideal in T

Quasi-nD-Cyclic Code

$$
\begin{aligned}
R_1 &= \mathbb{F}_q[x_1]/\langle x_1^{m_1}-1\rangle \\
R_2 &= \mathbb{F}_q[x_1,x_2]/\langle x_1^{m_1}-1, x_2^{m_2}-1\rangle \\
&\vdots \\
R_n &= \mathbb{F}_q[x_1,x_2,\ldots,x_n]/\langle x_1^{m_1}-1,\ldots,x_n^{m_n}-1\rangle \\
R_{n+1} &= \mathbb{F}_q[x_1,\ldots,x_n,x_{n+1}]/\langle x_1^{m_1}-1,\ldots,x_{n+1}^{m_{n+1}}-1\rangle
\end{aligned}
$$

Quasi-nD-Cyclic Code

$$
\begin{aligned}
R_1 &= \mathbb{F}_q[x_1]/\langle x_1^{m_1} - 1 \rangle \\
R_2 &= \mathbb{F}_q[x_1, x_2]/\langle x_1^{m_1} - 1, x_2^{m_2} - 1 \rangle \\
&\vdots \\
R_n &= \mathbb{F}_q[x_1, x_2, \dots, x_n]/\langle x_1^{m_1} - 1, \dots, x_n^{m_n} - 1 \rangle \\
R_{n+1} &= \mathbb{F}_q[x_1, \dots, x_n, x_{n+1}]/\langle x_1^{m_1} - 1, \dots, x_{n+1}^{m_{n+1}} - 1 \rangle
\end{aligned}
$$

Then a QnDC code of length $m_1 m_2 \dots m_n m_{n+1}$ is an R_n-submodule of R_{n+1}, whereas an $(n+1)$D cyclic code in an ideal in R_{n+1}.

Quasi-nD-Cyclic Code

$$
\begin{aligned}
R_1 &= \mathbb{F}_q[x_1]/\langle x_1^{m_1} - 1 \rangle \\
R_2 &= \mathbb{F}_q[x_1, x_2]/\langle x_1^{m_1} - 1, x_2^{m_2} - 1 \rangle \\
&\vdots \\
R_n &= \mathbb{F}_q[x_1, x_2, \ldots, x_n]/\langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1 \rangle \\
R_{n+1} &= \mathbb{F}_q[x_1, \ldots, x_n, x_{n+1}]/\langle x_1^{m_1} - 1, \ldots, x_{n+1}^{m_{n+1}} - 1 \rangle
\end{aligned}
$$

Then a QnDC code of length $m_1 m_2 \ldots m_n m_{n+1}$ is an R_n-submodule of R_{n+1}, whereas an $(n+1)$D cyclic code in an ideal in R_{n+1}.

Note that such a code can be viewed as a QC code of index $m_2 m_3 \ldots m_n m_{n+1}$

Concatenated Form and Asymptotics

Theorem

Constituents (outer codes) of a QnDC code are $Q(n-1)DC$ codes. Converse also holds.

Concatenated Form and Asymptotics

Theorem

Constituents (outer codes) of a QnDC code are $Q(n-1)DC$ codes. Converse also holds.

Theorem

QnDC codes are asymptotically good.

Concatenated Form and Asymptotics

Theorem

Constituents (outer codes) of a QnDC code are $Q(n-1)DC$ codes. Converse also holds.

Theorem

QnDC codes are asymptotically good.

Idea for $n = 2$:
QC codes are known to be asymptotically good, take one such sequence $\{\mathcal{C}_j\}$ with $d(\mathcal{C}_j) = d_j$ over $\mathbb{E}_i$ and consider $\widetilde{\mathcal{C}_j} = \langle\theta_i\rangle\Box\mathcal{C}_j$.
Then $\{\widetilde{\mathcal{C}_j}\}$ is also an asymptotically good sequence of Q2DC codes with minimum distance at least $d(\theta_i)d_j$.

nD-convolutional codes

Suppose that G is an $k \times \ell$ full rank polynomial matrix G with entries from $\mathbb{F}_q[x_1, \ldots, x_n]$. An n-dimensional (nD) convolutional code over $\mathbb{F}_q$ of length ℓ is defined in general as an $\mathbb{F}_q[[x_1, \ldots, x_n]]$-module in $\mathbb{F}_q[[x_1, \ldots, x_n]]^\ell$ generated by the rows of G (Fornasini-Valcher, Weiner), i.e.

nD-convolutional codes

Suppose that G is an $k \times \ell$ full rank polynomial matrix G with entries from $\mathbb{F}_q[x_1, \ldots, x_n]$. An n-dimensional (nD) convolutional code over $\mathbb{F}_q$ of length ℓ is defined in general as an $\mathbb{F}_q[[x_1, \ldots, x_n]]$-module in $\mathbb{F}_q[[x_1, \ldots, x_n]]^\ell$ generated by the rows of G (Fornasini-Valcher, Weiner), i.e.

$$C = \left\{ (u_0, \ldots, u_{k-1})\, G : \ u_i \in \mathbb{F}_q[[x_1, \ldots, x_n]] \ \forall i \right\}.$$

nD-convolutional codes

Suppose that G is an $k \times \ell$ full rank polynomial matrix G with entries from $\mathbb{F}_q[x_1, \ldots, x_n]$. An n-dimensional (nD) convolutional code over $\mathbb{F}_q$ of length ℓ is defined in general as an $\mathbb{F}_q[[x_1, \ldots, x_n]]$-module in $\mathbb{F}_q[[x_1, \ldots, x_n]]^\ell$ generated by the rows of G (Fornasini-Valcher, Weiner), i.e.

$$C = \{(u_0, \ldots, u_{k-1})\, G : \; u_i \in \mathbb{F}_q[[x_1, \ldots, x_n]] \; \forall i\}\,.$$

We assume that C is encoded by a is a noncatastrophic PGM G: all the full size ($k \times k$) minors of G has no common divisors in $\mathbb{F}_q[x_1, \ldots, x_n]$ with nonzero constant term.

Finite weight power series are clearly polynomials. Therefore, we will consider

$$C = \{(u_0, \ldots, u_{k-1})\, G : \; u_i \in \mathbb{F}_q[x_1, \ldots, x_n] \; \forall i\}$$

and such a code will be referred to as (ℓ, k) nD convolutional code, which is an $\mathbb{F}_q[x_1, \ldots, x_n]$-module in $\mathbb{F}_q[x_1, \ldots, x_n]^{\ell}$.

Finite weight power series are clearly polynomials. Therefore, we will consider

$$C = \{(u_0, \ldots, u_{k-1})\, G : \ u_i \in \mathbb{F}_q[x_1, \ldots, x_n] \ \forall i\}$$

and such a code will be referred to as (ℓ, k) nD convolutional code, which is an $\mathbb{F}_q[x_1, \ldots, x_n]$-module in $\mathbb{F}_q[x_1, \ldots, x_n]^\ell$.

Unlike the classical case ($n = 1$), not every such module is necessarily free when $n \geq 2$, although only free nD convolutional codes are studied in some articles.

Note that if we reduce an n-dimensional convolutional code C modulo the ideal $I_n = \langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1 \rangle$ then the resulting linear block code $\bar{C} = C/I_n \subseteq R_n^\ell = (\mathbb{F}_q[x_1, x_2, \ldots, x_n]/I_n)^\ell$ is nothing but a Q-nD-C code.

Note that if we reduce an n-dimensional convolutional code C modulo the ideal $I_n = \langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1 \rangle$ then the resulting linear block code $\bar{C} = C/I_n \subseteq R_n^\ell = (\mathbb{F}_q[x_1, x_2, \ldots, x_n]/I_n)^\ell$ is nothing but a Q-nD-C code.

Question: How to generalize the distance relation?

Note that if we reduce an n-dimensional convolutional code C modulo the ideal $I_n = \langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1 \rangle$ then the resulting linear block code $\bar{C} = C/I_n \subseteq R_n^\ell = (\mathbb{F}_q[x_1, x_2, \ldots, x_n]/I_n)^\ell$ is nothing but a Q-nD-C code.

Question: How to generalize the distance relation?

Problems:

1. The existence of a basic PGM for any nD convolutional code is unknown.
2. The weight preserving property is proven for 1D case only.

For nonzero polynomials $g_1, \ldots, g_\ell \in \mathbb{F}_q[x_1, \ldots, x_n]$, consider the set

$$J_{m_1,\ldots,m_n} = \{u(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]; ug_i \in I_n, \forall i = 1, \ldots, \ell\}.$$

For nonzero polynomials $g_1, \ldots, g_\ell \in \mathbb{F}_q[x_1, \ldots, x_n]$, consider the set

$$J_{m_1,\ldots,m_n} = \{u(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]; ug_i \in I_n, \forall i = 1, \ldots, \ell\}.$$

Note that $J_{m_1,\ldots,m_n}$ is clearly an ideal of $\mathbb{F}_q[x_1, \ldots, x_n]$. Moreover,

$$I_n = \langle x_1^{m_n} - 1, \ldots, x_n^{m_n} - 1\rangle \subseteq J_{m_1,\ldots,m_n}$$

holds in general.

For nonzero polynomials $g_1, \ldots, g_\ell \in \mathbb{F}_q[x_1, \ldots, x_n]$, consider the set

$$J_{m_1,\ldots,m_n} = \{u(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]; ug_i \in I_n, \forall i = 1, \ldots, \ell\}.$$

Note that $J_{m_1,\ldots,m_n}$ is clearly an ideal of $\mathbb{F}_q[x_1, \ldots, x_n]$. Moreover,

$$I_n = \langle x_1^{m_n} - 1, \ldots, x_n^{m_n} - 1\rangle \subseteq J_{m_1,\ldots,m_n}$$

holds in general.

For 1-generator 1D convolutional codes, we have the following equivalence to noncatastrophicity.

Lemma

Let $g_0(x), \ldots, g_{\ell-1}(x)$ be nonzero polynomials in $\mathbb{F}_q[x]$. Let

$$J_m = \{h(x) \in \mathbb{F}_q[x] : h(x)g_i(x) \in \langle x^m - 1\rangle \forall i = 0, \ldots, \ell - 1\}.$$

Then, the encoder $G = \big(g_0(x), \ldots, g_{\ell-1}(x)\big)$ is noncatastrophic for the convolutional code C that it generates iff $J_m = \langle x^m - 1\rangle$ for all $m \geq 1$.

We will consider 1-generator 2D convolutional codes given with a PGM $G = \big(g_1(x,y), \ldots, g_\ell(x,y)\big)$ which satisfies

$$J_{m_1,m_2} = \langle x^{m_1} - 1, y^{m_2} - 1 \rangle, \tag{1}$$

for all $m_1, m_2 \geq 1$.

We will consider 1-generator 2D convolutional codes given with a PGM $G = \big(g_1(x,y), \ldots, g_\ell(x,y)\big)$ which satisfies

$$J_{m_1,m_2} = \langle x^{m_1} - 1, y^{m_2} - 1 \rangle, \tag{1}$$

for all $m_1, m_2 \geq 1$.

Theorem

Let C be a 1-generator (ℓ, k) 2D convolutional code given with a PGM $G = (g_1(x,y), \ldots, g_\ell(x,y))$ satisfying (1) for some $m_1, m_2 \geq 1$. Let C' be the associated Q2DC code in $\left(\mathbb{F}_q[x,y]/\langle x^{m_1} - 1, y^{m_2} - 1 \rangle\right)^\ell$. Then $d_f(C) \geq d(C')$.