Sobre bases de Gröbner e códigos quasi-cíclicos

Marcelo Miranda

EnCoRI 2023

16 de junho de 2023

Contents

Introduction

In this presentation, we explore the Gröbner basis theory for modules with the primary intention of presenting some results and conjectures involving quasi-cyclic codes.

Introduction

In this presentation, we explore the Gröbner basis theory for modules with the primary intention of presenting some results and conjectures involving quasi-cyclic codes.

After that, we introduce QC-LDPC codes, giving a possible way to connect general Gröbner basis theory for modules to such class of codes.

Introduction

In this presentation, we explore the Gröbner basis theory for modules with the primary intention of presenting some results and conjectures involving quasi-cyclic codes.

After that, we introduce QC-LDPC codes, giving a possible way to connect general Gröbner basis theory for modules to such class of codes.

Finally, as perspectives of study for the current work, we establish another possible relations comprehending Gröbner basis theory, coding/decoding and lattices from codes.

Contents

Gröbner bases for modules

Set $R = \mathbb{K}[x_1, \cdots, x_n]$, a polynomial ring.

Gröbner bases for modules

Set $R = \mathbb{K}[x_1, \cdots, x_n]$, a polynomial ring.

Definition 2.1

Let $M \subseteq R^m$ be a submodule, let $\geq$ be a monomial order and let $\langle LT(M)\rangle \subseteq R$ be the monomial submodule generated by the leading terms of all $\mathbf{f} \in M$ with respect to $\geq$. A finite set $G = \{\mathbf{g}_1, \cdots, \mathbf{g}_s\} \subseteq M$ is a **Gröbner basis** of M if we have $\langle LT(M)\rangle = \langle LT(\mathbf{g}_1), \cdots, LT(\mathbf{g}_s)\rangle$.

Set $R = \mathbb{K}[x_1, \cdots, x_n]$, a polynomial ring.

Definition 2.1

Let $M \subseteq R^m$ be a submodule, let $\geq$ be a monomial order and let $\langle LT(M) \rangle \subseteq R$ be the monomial submodule generated by the leading terms of all $\mathbf{f} \in M$ with respect to $\geq$. A finite set $G = \{\mathbf{g}_1, \cdots, \mathbf{g}_s\} \subseteq M$ is a **Gröbner basis** of M if we have $\langle LT(M) \rangle = \langle LT(\mathbf{g}_1), \cdots, LT(\mathbf{g}_s) \rangle$.

Gröbner bases for modules

One important reference for the verification if a module basis is a Gröbner basis is the S-**element**.

Gröbner bases for modules

One important reference for the verification if a module basis is a Gröbner basis is the S-**element**.

Definition 2.2

Let $\geq$ be a monomial order in R^m, $\mathbf{f}, \mathbf{g} \in R^m$ and $\mathbf{m} = MMC(LT(\mathbf{f}), LT(\mathbf{g}))$. Then, the S-element of $\mathbf{f}$ and $\mathbf{g}$, denoted by $S(\mathbf{f}, \mathbf{g})$, is given by

$$S(\mathbf{f}, \mathbf{g}) = \frac{\mathbf{m}}{LT(\mathbf{f})}\mathbf{f} - \frac{\mathbf{m}}{LT(\mathbf{g})}\mathbf{g}.$$

Gröbner bases for modules

One important reference for the verification if a module basis is a Gröbner basis is the S-**element**.

Definition 2.2

Let $\geq$ be a monomial order in R^m, $\mathbf{f}, \mathbf{g} \in R^m$ and $\mathbf{m} = MMC(LT(\mathbf{f}), LT(\mathbf{g}))$. Then, the S-element of $\mathbf{f}$ and $\mathbf{g}$, denoted by $S(\mathbf{f}, \mathbf{g})$, is given by

$$S(\mathbf{f}, \mathbf{g}) = \frac{\mathbf{m}}{LT(\mathbf{f})}\mathbf{f} - \frac{\mathbf{m}}{LT(\mathbf{g})}\mathbf{g}.$$

Theorem 2.1 (Buchberger's Criterion for submodules [4])

Let $G = \{\mathbf{g}_1, \cdots, \mathbf{g}_s\} \subseteq R^m$ and $M = \langle \mathbf{g}_1, \cdots, \mathbf{g}_s \rangle$. Then, G is a Gröbner basis if, and only if, the remainder of the division of $S(\mathbf{g}_i, \mathbf{g}_j)$ by G is $\mathbf{0}$ for all i, j.

Gröbner bases for modules

One important reference for the verification if a module basis is a Gröbner basis is the S-**element**.

Definition 2.2

Let $\geq$ be a monomial order in R^m, $\mathbf{f}, \mathbf{g} \in R^m$ and $\mathbf{m} = MMC(LT(\mathbf{f}), LT(\mathbf{g}))$. Then, the S-element of $\mathbf{f}$ and $\mathbf{g}$, denoted by $S(\mathbf{f}, \mathbf{g})$, is given by

$$S(\mathbf{f}, \mathbf{g}) = \frac{\mathbf{m}}{LT(\mathbf{f})}\mathbf{f} - \frac{\mathbf{m}}{LT(\mathbf{g})}\mathbf{g}.$$

Theorem 2.1 (Buchberger's Criterion for submodules [4])

Let $G = \{\mathbf{g}_1, \cdots, \mathbf{g}_s\} \subseteq R^m$ and $M = \langle \mathbf{g}_1, \cdots, \mathbf{g}_s \rangle$. Then, G is a Gröbner basis if, and only if, the remainder of the division of $S(\mathbf{g}_i, \mathbf{g}_j)$ by G is $\mathbf{0}$ for all i, j.

By the Buchberger's Criterion, we can establish an algorithm that allows us to build, starting from a submodule basis, a Gröbner basis for the same submodule in R^m - the Buchberger's Algorithm for submodules.

Gröbner bases for modules

Definition 2.3

Let $G \subseteq R^m$ be a Gröbner basis of a submodule $M \subseteq R^m$. G is **minimal** if

- $LC(\mathbf{g}) = 1 \; \forall \; \mathbf{g} \in G$;
- $\forall \; \mathbf{g} \in G, LT(\mathbf{g}) \notin \langle LT(G - \{\mathbf{g}\})\rangle$.

Gröbner bases for modules

Definition 2.3

Let $G \subseteq R^m$ be a Gröbner basis of a submodule $M \subseteq R^m$. G is **minimal** if

- $LC(\mathbf{g}) = 1 \ \forall \ \mathbf{g} \in G$;
- $\forall \ \mathbf{g} \in G, LT(\mathbf{g}) \notin \langle LT(G - \{\mathbf{g}\})\rangle$.

Moreover, if

- $LM(\mathbf{g})$ divides no monomial of any element of $G - \{\mathbf{g}\}$,

then G is a **reduced** Gröbner basis of M.

Contents

Quasi-cyclic codes

Introduction and relation to modules

Quasi-cyclic codes can be seen as generalizations of cyclic codes in the sense they can be associated to submodules of R_m^l, with $R_m := \frac{\mathbb{F}_q[x]}{\langle x^m - 1 \rangle}$.

Quasi-cyclic codes can be seen as generalizations of cyclic codes in the sense they can be associated to submodules of R_m^l, with $R_m := \dfrac{\mathbb{F}_q[x]}{\langle x^m - 1\rangle}$.

Definition 3.1 (Classic)

A linear code C of length $n = ml$ in $\mathbb{F}_q$ is named **quasi-cyclic** of index l if, for each $c \in C$,

$$c = (c_0, \cdots, c_{n-1}) \in C \Longrightarrow c' = (c_{n-l}, \cdots, c_0, \cdots, c_{n-l-1}) \in C.$$

Quasi-cyclic codes

Introduction and relation to modules

If

$$c = (a_{11}a_{12}\cdots a_{1l}\ a_{21}a_{22}\cdots a_{2l}\ \cdots\ a_{m1}a_{m2}\cdots a_{ml}) \in \mathbb{F}_q^n$$

is a generating vector for a quasi-cyclic code C of index l, then, taking all possible vectors after shifting l coordinates, we obtain a generator matrix

If

$$c = (a_{11}\, a_{12} \cdots a_{1l}\ a_{21}\, a_{22} \cdots a_{2l}\ \cdots\ a_{m1}\, a_{m2} \cdots a_{ml}) \in \mathbb{F}_q^n$$

is a generating vector for a quasi-cyclic code C of index l, then, taking all possible vectors after shifting l coordinates, we obtain a generator matrix

$$G = \begin{bmatrix} a_{11}\, a_{12} \cdots a_{1l} & a_{21}\, a_{22} \cdots a_{2l} & \cdots & a_{m1}\, a_{m2} \cdots a_{ml} \\ a_{m1}\, a_{m2} \cdots a_{ml} & a_{11}\, a_{12} \cdots a_{1l} & \cdots & a_{(m-1)1}\, a_{(m-1)2} \cdots a_{(m-1)l} \\ \vdots & \vdots & \ddots & \vdots \\ a_{21}\, a_{22} \cdots a_{2l} & a_{31}\, a_{32} \cdots a_{3l} & \cdots & a_{11}\, a_{12} \cdots a_{1l} \end{bmatrix} \in M_{m \times lm}(\mathbb{F}_q)$$

for C.

Quasi-cyclic codes

Introduction and relation to modules

If

$$c = (a_{11}a_{12}\cdots a_{1l}\; a_{21}a_{22}\cdots a_{2l}\; \cdots\; a_{m1}a_{m2}\cdots a_{ml}) \in \mathbb{F}_q^n$$

is a generating vector for a quasi-cyclic code C of index l, then, taking all possible vectors after shifting l coordinates, we obtain a generator matrix

$$G = \begin{bmatrix} a_{11}a_{12}\cdots a_{1l} & a_{21}a_{22}\cdots a_{2l} & \cdots & a_{m1}a_{m2}\cdots a_{ml} \\ a_{m1}a_{m2}\cdots a_{ml} & a_{11}a_{12}\cdots a_{1l} & \cdots & a_{(m-1)1}a_{(m-1)2}\cdots a_{(m-1)l} \\ \vdots & \vdots & \ddots & \vdots \\ a_{21}a_{22}\cdots a_{2l} & a_{31}a_{32}\cdots a_{3l} & \cdots & a_{11}a_{12}\cdots a_{1l} \end{bmatrix} \in M_{m\times lm}(\mathbb{F}_q)$$

for C.

It is always possible to permutate the columns of C in order to find a generator matrix G_1, of an equivalent code to C, formed by l circulant blocks:

Quasi-cyclic codes

Introduction and relation to modules

If

$$c = (a_{11}\, a_{12} \cdots a_{1l}\;\, a_{21}\, a_{22} \cdots a_{2l}\;\, \cdots\;\, a_{m1}\, a_{m2} \cdots a_{ml}) \in \mathbb{F}_q^n$$

is a generating vector for a quasi-cyclic code C of index l, then, taking all possible vectors after shifting l coordinates, we obtain a generator matrix

$$G = \begin{bmatrix} a_{11}\, a_{12} \cdots a_{1l} & a_{21}\, a_{22} \cdots a_{2l} & \cdots & a_{m1}\, a_{m2} \cdots a_{ml} \\ a_{m1}\, a_{m2} \cdots a_{ml} & a_{11}\, a_{12} \cdots a_{1l} & \cdots & a_{(m-1)1}\, a_{(m-1)2} \cdots a_{(m-1)l} \\ \vdots & \vdots & \ddots & \vdots \\ a_{21}\, a_{22} \cdots a_{2l} & a_{31}\, a_{32} \cdots a_{3l} & \cdots & a_{11}\, a_{12} \cdots a_{1l} \end{bmatrix} \in M_{m \times lm}(\mathbb{F}_q)$$

for C.

It is always possible to permutate the columns of C in order to find a generator matrix G_1, of an equivalent code to C, formed by l circulant blocks:

$$G_1 = \begin{bmatrix} C_1 & C_2 & \cdots & C_l \end{bmatrix},$$

such that each $C_i \in M_m(\mathbb{F}_q)$, $1 \leq i \leq l$, is a circulant matrix obtained by the vector $(a_{0i}\; a_{1i}\; \cdots\; a_{(m-1)i}) \in \mathbb{F}_q^m$.

Quasi-cyclic codes

Introduction and relation to modules

Therefore, if a quasi-cyclic code has k generators, we can exhibit a generator matrix for an equivalent code (after a l-shift in its columns) in the form

$$G_2 = \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1l} \\ C_{21} & C_{22} & \cdots & C_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ C_{k1} & C_{k2} & \cdots & C_{kl} \end{bmatrix} \in M_{ml \times mk}(\mathbb{F}_q). \quad (1)$$

Quasi-cyclic codes

Introduction and relation to modules

Therefore, if a quasi-cyclic code has k generators, we can exhibit a generator matrix for an equivalent code (after a l-shift in its columns) in the form

$$G_2 = \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1l} \\ C_{21} & C_{22} & \cdots & C_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ C_{k1} & C_{k2} & \cdots & C_{kl} \end{bmatrix} \in M_{ml \times mk}(\mathbb{F}_q). \tag{1}$$

Remark 3.1

It is not guaranteed that G_2 has $n = ml$ linearly independent rows.

Therefore, if a quasi-cyclic code has k generators, we can exhibit a generator matrix for an equivalent code (after a l-shift in its columns) in the form

$$G_2 = \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1l} \\ C_{21} & C_{22} & \cdots & C_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ C_{k1} & C_{k2} & \cdots & C_{kl} \end{bmatrix} \in M_{ml \times mk}(\mathbb{F}_q). \tag{1}$$

Remark 3.1

It is not guaranteed that G_2 has $n = ml$ linearly independent rows.

Definition 3.2 (Equivalent)

A linear code having an equivalent code with generator matrix as in (1) is called **quasi-cyclic** code.

Therefore, if a quasi-cyclic code has k generators, we can exhibit a generator matrix for an equivalent code (after a l-shift in its columns) in the form

$$G_2 = \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1l} \\ C_{21} & C_{22} & \cdots & C_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ C_{k1} & C_{k2} & \cdots & C_{kl} \end{bmatrix} \in M_{ml \times mk}(\mathbb{F}_q). \tag{1}$$

Remark 3.1

It is not guaranteed that G_2 has $n = ml$ linearly independent rows.

Definition 3.2 (Equivalent)

A linear code having an equivalent code with generator matrix as in (1) is called **quasi-cyclic** code.

Since each C_{ij} is generated by a polynomial $a_{ij}(x) = a_{0ij} + a_{1ij}x + \cdots + a_{(m-1)ij}x^{m-1}$, then C_{ij} is isomorphic to an ideal of R_m; this gives

$$\mathbb{F}_q^{lm} \simeq R_m^l \Longrightarrow C \text{ is a } R_m\text{-submodule of the module } R_m^l.$$

Quasi-cyclic codes

Introduction and relation to modules

Let

$$\begin{array}{cccc} \phi: & (\mathbb{F}_q[x])^l & \to & R_m^l \\ & (p_1(x), \cdots, p_l(x)) & \mapsto & ([p_1(x)], \cdots, [p_l(x)]) \end{array}$$

Quasi-cyclic codes

Introduction and relation to modules

Let

$$\begin{array}{rccc} \phi: & (\mathbb{F}_q[x])^l & \rightarrow & R_m^l \\ & (p_1(x), \cdots, p_l(x)) & \mapsto & ([p_1(x)], \cdots, [p_l(x)]) \end{array}$$

be a map which has kernel $\widetilde{K} = \langle (x^m - 1)\mathbf{e}_i, 1 \leq i \leq l \rangle$ ($\{\mathbf{e}_i / 1 \leq i \leq l\}$ canonical basis of $(\mathbb{F}_q[x])^l$).

Let

$$\begin{array}{rccc} \phi: & (\mathbb{F}_q[x])^l & \to & R_m^l \\ & (p_1(x), \cdots, p_l(x)) & \mapsto & ([p_1(x)], \cdots, [p_l(x)]) \end{array}$$

be a map which has kernel $\widetilde{K} = \langle (x^m - 1)\mathbf{e}_i, 1 \leq i \leq l \rangle$ ($\{\mathbf{e}_i / 1 \leq i \leq l\}$ canonical basis of $(\mathbb{F}_q[x])^l$).

Let

$$\begin{array}{cccc} \phi : & (\mathbb{F}_q[x])^l & \to & R_m^l \\ & (p_1(x), \cdots, p_l(x)) & \mapsto & ([p_1(x)], \cdots, [p_l(x)]) \end{array}$$

be a map which has kernel $\widetilde{K} = \langle (x^m - 1)\mathbf{e}_i, 1 \leq i \leq l \rangle$ ($\{\mathbf{e}_i / 1 \leq i \leq l\}$ canonical basis of $(\mathbb{F}_q[x])^l$).

By the First Isomorphism Theorem, there exists the correspondence

$$C \Longleftrightarrow \widetilde{C} \text{ (preimages of } (\mathbb{F}_q[x])^l \text{ containing } \widetilde{K}).$$

Quasi-cyclic codes

Introduction and relation to modules

Consider a k-generator (linear) quasi-cyclic code $C = \langle \mathbf{r}_1, \cdots, \mathbf{r}_k \rangle$, in $\mathbb{F}_q$, q **prime**, with $\mathbf{r}_i = (r_{i1}, \cdots, r_{il})$.

Quasi-cyclic codes

Introduction and relation to modules

Consider a k-generator (linear) quasi-cyclic code $C = \langle \mathbf{r}_1, \cdots, \mathbf{r}_k \rangle$, in $\mathbb{F}_q$, q **prime**, with $\mathbf{r}_i = (r_{i1}, \cdots, r_{il})$. Then,

$$\widetilde{C} = \langle \mathbf{r}_1, \cdots, \mathbf{r}_k, (x^m - 1)e_j \rangle$$

is a module which has a minimal Gröbner basis $\widetilde{G}$ with respect to an order.

Consider a k-generator (linear) quasi-cyclic code $C = \langle \mathbf{r}_1, \cdots, \mathbf{r}_k \rangle$, in $\mathbb{F}_q$, q **prime**, with $\mathbf{r}_i = (r_{i1}, \cdots, r_{il})$. Then,

$$\widetilde{C} = \langle \mathbf{r}_1, \cdots, \mathbf{r}_k, (x^m - 1)e_j \rangle$$

is a module which has a minimal Gröbner basis $\widetilde{G}$ with respect to an order.

Also, there will exist a reduced Gröbner basis $\widetilde{G_1}$, obtained from $\widetilde{G}$, that is unique - its structure is given by the following Theorem:

Theorem 3.1 ([7])

Let $\widetilde{C}$ be a submodule of $(\mathbb{F}_q[x])^l$ containing $\widetilde{K} = \langle (x^m - 1)\mathbf{e}_i, 1 \leq i \leq l \rangle$. Then, $\widetilde{C}$ has a reduced Gröbner basis with respect to $\geq_{POT}$ and presented in the form

$$\widetilde{G} = \begin{bmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_l \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1l} \\ 0 & g_{22} & \cdots & g_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_{ll} \end{bmatrix}, \qquad (2)$$

$g_{ii} \neq 0 \ \forall\, i \in \{1, \cdots, l\}$ and

1. $g_{ii} | x^m - 1$ and if $\mathbf{f} \in \widetilde{C}$ has leading monomial in the i-th position, then $g_{ii}\mathbf{e}_i$ divides $LM(\mathbf{f})$;
2. $\deg(g_{ji}) < \deg(g_{ii}) \leq m \ \forall\, j < i$;
3. If $g_{ii} = x^m - 1$, then $\mathbf{g}_i = (x^m - 1)\mathbf{e}_i$;
4. The dimension of $\dfrac{(\mathbb{F}_q[x])^l}{\widetilde{C}}$ in $\mathbb{F}_q$ is $\sum_{i=1}^{l} \deg(g_{ii})$.

Theorem 3.1 ([7])

Let $\widetilde{C}$ be a submodule of $(\mathbb{F}_q[x])^l$ containing $\widetilde{K} = \langle (x^m - 1)\mathbf{e}_i, 1 \leq i \leq l \rangle$. Then, $\widetilde{C}$ has a reduced Gröbner basis with respect to $\geq_{POT}$ and presented in the form

$$\widetilde{G} = \begin{bmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_l \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1l} \\ 0 & g_{22} & \cdots & g_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_{ll} \end{bmatrix}, \quad (2)$$

$g_{ii} \neq 0 \;\forall\, i \in \{1, \cdots, l\}$ and

1. $g_{ii} | x^m - 1$ and if $\mathbf{f} \in \widetilde{C}$ has leading monomial in the i-th position, then $g_{ii}\mathbf{e}_i$ divides $LM(\mathbf{f})$;
2. $\deg(g_{ji}) < \deg(g_{ii}) \leq m \;\forall\, j < i$;
3. If $g_{ii} = x^m - 1$, then $\mathbf{g}_i = (x^m - 1)\mathbf{e}_i$;
4. The dimension of $\dfrac{(\mathbb{F}_q[x])^l}{\widetilde{C}}$ in $\mathbb{F}_q$ is $\sum_{i=1}^{l} \deg(g_{ii})$.

Proposition 3.1 ([7])

The dimension t of C, which has preimage $\widetilde{C}$ by ϕ with Gröbner basis as in (2), is

$$t = lm - \sum_{i=1}^{l} \deg(g_{ii}).$$

Quasi-cyclic codes

Finding sparse generator matrices

We recall the correspondence

$$C \text{ quasi-cyclic code}$$

Quasi-cyclic codes

Finding sparse generator matrices

We recall the correspondence

$$C \text{ quasi-cyclic code}$$

$$\Updownarrow$$

$$\widetilde{C} \text{ module}$$

Quasi-cyclic codes
Finding sparse generator matrices

We recall the correspondence

$$C \text{ quasi-cyclic code}$$

$$\Updownarrow$$

$$\widetilde{C} \text{ module}$$

$$\Updownarrow$$

$$\widetilde{G} \text{ Reduced Gröbner basis wrt the order } \geq_{POT} \text{ and presented as in (2).}$$

We recall the correspondence

$$C \text{ quasi-cyclic code}$$
$$\Updownarrow$$
$$\widetilde{C} \text{ module}$$
$$\Updownarrow$$
$$\widetilde{G} \text{ Reduced Gröbner basis wrt the order } \geq_{POT} \text{ and presented as in (2).}$$

This helps to prove the following Proposition:

Proposition 3.2

Let C be a k-generator quasi-cyclic code with matrix generator G and an equivalent code given by the generator matrix G_2 as in (1). Let $\widetilde{C}$ be its associated module with reduced Gröbner basis $\widetilde{G}$ as in (2) which, in turn, has a matrix representation with entries $g_{ij} = a_{0ij} + a_{1ij}x + \cdots + a_{(m-1)ij}x^{m-1} \pmod{(x^m - 1)}$, $1 \leq i, j \leq l$. Let G_B be the block matrix formed by the circulant blocks $G_{ij} \in M_m(\mathbb{F}_q)$ corresponding to the generator polynomials g_{ij} (as of cyclic codes) and finally define G_S as the matrix obtained from G_B after applying in its columns the inverse permutation of the one applied in the columns of G to get G_2. Then, G_S is a generator matrix for C.

Proposition 3.2

Let C be a k-generator quasi-cyclic code with matrix generator G and an equivalent code given by the generator matrix G_2 as in (1). Let $\widetilde{C}$ be its associated module with reduced Gröbner basis $\widetilde{G}$ as in (2) which, in turn, has a matrix representation with entries $g_{ij} = a_{0ij} + a_{1ij}x + \cdots + a_{(m-1)ij}x^{m-1} \pmod{(x^m - 1)}$, $1 \leq i, j \leq l$. Let G_B be the block matrix formed by the circulant blocks $G_{ij} \in M_m(\mathbb{F}_q)$ corresponding to the generator polynomials g_{ij} (as of cyclic codes) and finally define G_S as the matrix obtained from G_B after applying in its columns the inverse permutation of the one applied in the columns of G to get G_2. Then, G_S is a generator matrix for C.

By Proposition 3.2, we find k "new" generators for the quasi-cyclic code C. We conjecturate that those generators are the vectors with the lowest Hamming weight generating C; thus, G_S is the "sparsiest" generator matrix for such code.

Conjecture 3.1

Let C be a 1-generator quasi-cyclic code generated by a vector $v \in \mathbb{F}_2^n$ with Hamming weight m such that $n > m \geq \left\lceil \frac{n}{2} \right\rceil$. Then, there exists a vector $\overline{v} \in \mathbb{F}_2^n$, having Hamming weight $\min\{m, n-m\}$, that generates C.

Conjecture 3.1

Let C be a 1-generator quasi-cyclic code generated by a vector $v \in \mathbb{F}_2^n$ with Hamming weight m such that $n > m \geq \left\lceil \frac{n}{2} \right\rceil$. Then, there exists a vector $\overline{v} \in \mathbb{F}_2^n$, having Hamming weight $\min\{m, n-m\}$, that generates C.

Contents

QC-LDPC codes

Low-Density Parity Check codes are usually defined via parity-check matrices H which, in turn, are usually associated with Tanner graphs. In general, a linear code is an LDPC code if it is given by a sparse parity-check matrix $H \in M_{m\times n}(\mathbb{F}_q)$.

QC-LDPC codes

Low-Density Parity Check codes are usually defined via parity-check matrices H which, in turn, are usually associated with Tanner graphs. In general, a linear code is an LDPC code if it is given by a sparse parity-check matrix $H \in M_{m \times n}(\mathbb{F}_q)$. We use a characterization in order to define QC-LDPC (quasi-cyclic LDPC) codes ([3]):

QC-LDPC codes

Low-Density Parity Check codes are usually defined via parity-check matrices H which, in turn, are usually associated with Tanner graphs. In general, a linear code is an LDPC code if it is given by a sparse parity-check matrix $H \in M_{m\times n}(\mathbb{F}_q)$. We use a characterization in order to define QC-LDPC (quasi-cyclic LDPC) codes ([3]):

Definition 4.1

A linear code C is a QC-LDPC code of circulant size z if it is defined by a parity-check matrix H constituted by square blocks $z \times z$ which are or circulant permutation matrices (CPM) or the null matrix.

QC-LDPC codes

Low-Density Parity Check codes are usually defined via parity-check matrices H which, in turn, are usually associated with Tanner graphs. In general, a linear code is an LDPC code if it is given by a sparse parity-check matrix $H \in M_{m\times n}(\mathbb{F}_q)$. We use a characterization in order to define QC-LDPC (quasi-cyclic LDPC) codes ([3]):

Definition 4.1

A linear code C is a QC-LDPC code of circulant size z if it is defined by a parity-check matrix H constituted by square blocks $z \times z$ which are or circulant permutation matrices (CPM) or the null matrix.

In such case, if $H \in M_{m\times n}(\mathbb{F}_q)$ (usually $q = 2$), then we have length $n = zn_b$ and redudancy $m = zm_b$. It gives

$$H = \begin{bmatrix} P_{b(0,0)} & P_{b(0,1)} & \cdots & P_{b(0,n_b-1)} \\ P_{b(1,0)} & P_{b(1,1)} & \cdots & P_{b(1,n_b-1)} \\ \vdots & \vdots & \ddots & \vdots \\ P_{b(m_b-1,0)} & P_{b(m_b-1,1)} & \cdots & P_{b(m_b-1,n_b-1)} \end{bmatrix},$$

in which each block $P_{b(i,j)}$ is either a $z \times z$ CPM or the null matrix.

QC-LDPC codes

Example 4.1

Let C be the "minimal" QC code of index $l = 2$ in $\mathbb{F}_2^8$ generated by (11111100).

QC-LDPC codes

Example 4.1

Let C be the "minimal" QC code of index $l = 2$ in $\mathbb{F}_2^8$ generated by (11111100).

First, we find a generator matrix for C given by

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

QC-LDPC codes

Example 4.1

Let C be the "minimal" QC code of index $l = 2$ in $\mathbb{F}_2^8$ generated by (11111100).

First, we find a generator matrix for C given by

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Permutating the columns of G conveniently, one obtains the matrix

$$G_2 = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{array} \right] := \left[\begin{array}{c|c} C_{11} & C_{12} \end{array} \right],$$

in which each C_{ij} are circulant matrices with generating polynomials given by $c_{11}(x) = c_{12}(x) = 1 + x + x^2$, respectively.

QC-LDPC codes

Therefore, the associated module $\widetilde{C}$ is given by

$$\widetilde{C} = \left\langle \begin{bmatrix} 1+x+x^2 \\ 1+x+x^2 \end{bmatrix}, \begin{bmatrix} x^4-1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ x^4-1 \end{bmatrix} \right\rangle.$$

QC-LDPC codes

Therefore, the associated module $\widetilde{C}$ is given by

$$\widetilde{C} = \left\langle \begin{bmatrix} 1+x+x^2 \\ 1+x+x^2 \end{bmatrix}, \begin{bmatrix} x^4-1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ x^4-1 \end{bmatrix} \right\rangle.$$

Via Buchberger's Algorithm, one finds the Gröbner basis

$$\widetilde{G} = \left\{ \begin{bmatrix} 1+x+x^2 \\ 1+x+x^2 \end{bmatrix}, \begin{bmatrix} x^4-1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ x^4-1 \end{bmatrix}, \begin{bmatrix} 1+x \\ x+x^4 \end{bmatrix}, \begin{bmatrix} 1 \\ 1+x+x^5 \end{bmatrix} \right\}$$

for $\widetilde{C}$.

QC-LDPC codes

Therefore, the associated module $\widetilde{C}$ is given by

$$\widetilde{C} = \left\langle \begin{bmatrix} 1+x+x^2 \\ 1+x+x^2 \end{bmatrix}, \begin{bmatrix} x^4-1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ x^4-1 \end{bmatrix} \right\rangle .$$

Via Buchberger's Algorithm, one finds the Gröbner basis

$$\widetilde{G} = \left\{ \begin{bmatrix} 1+x+x^2 \\ 1+x+x^2 \end{bmatrix}, \begin{bmatrix} x^4-1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ x^4-1 \end{bmatrix}, \begin{bmatrix} 1+x \\ x+x^4 \end{bmatrix}, \begin{bmatrix} 1 \\ 1+x+x^5 \end{bmatrix} \right\}$$

for $\widetilde{C}$.

Whence, its reduced Gröbner basis is given by

$$\widetilde{G_R} = \left\{ \begin{bmatrix} 0 \\ x^4-1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\} .$$

QC-LDPC codes

Therefore, the associated module $\widetilde{C}$ is given by

$$\widetilde{C} = \left\langle \begin{bmatrix} 1 + x + x^2 \\ 1 + x + x^2 \end{bmatrix}, \begin{bmatrix} x^4 - 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ x^4 - 1 \end{bmatrix} \right\rangle.$$

Via Buchberger's Algorithm, one finds the Gröbner basis

$$\widetilde{G} = \left\{ \begin{bmatrix} 1 + x + x^2 \\ 1 + x + x^2 \end{bmatrix}, \begin{bmatrix} x^4 - 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ x^4 - 1 \end{bmatrix}, \begin{bmatrix} 1 + x \\ x + x^4 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 + x + x^5 \end{bmatrix} \right\}$$

for $\widetilde{C}$.

Whence, its reduced Gröbner basis is given by

$$\widetilde{G_R} = \left\{ \begin{bmatrix} 0 \\ x^4 - 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}.$$

It follows that the rows of the matrix

$$\widetilde{G_R} = \begin{bmatrix} g_{11} & g_{12} \\ 0 & g_{22} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & x^4 - 1 \end{bmatrix}$$

generate $\widetilde{C}$.

QC-LDPC codes

By Proposition 3.1, $\dim C = 4$ in $\mathbb{F}_2^8$. Furthermore, via Proposition 3.2, one obtains the generator matrix

$$G_S = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

for C.

QC-LDPC codes

By Proposition 3.1, $\dim C = 4$ in $\mathbb{F}_2^8$. Furthermore, via Proposition 3.2, one obtains the generator matrix

$$G_S = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

for C.

Permutating conveniently the columns of G_S, we get the matrix

$$G'_S = \left[\begin{array}{c|c} I_4 & I_4 \end{array}\right],$$

which generates an equivalent code to C, say C'.

QC-LDPC codes

By Proposition 3.1, $\dim C = 4$ in $\mathbb{F}_2^8$. Furthermore, via Proposition 3.2, one obtains the generator matrix

$$G_S = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

for C.
Permutating conveniently the columns of G_S, we get the matrix

$$G'_S = \left[\begin{array}{c|c} I_4 & I_4 \end{array} \right],$$

which generates an equivalent code to C, say C'.
In such case, the associated parity-check matrix H'_S of C' is

$$H'_S = \left[\begin{array}{c|c} I_{8-4} & I_4^T \end{array} \right] = \left[\begin{array}{c|c} I_4 & I_4 \end{array} \right],$$

which follows Definition 4.1.

QC-LDPC codes

By Proposition 3.1, $\dim C = 4$ in $\mathbb{F}_2^8$. Furthermore, via Proposition 3.2, one obtains the generator matrix

$$G_S = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

for C.
Permutating conveniently the columns of G_S, we get the matrix

$$G'_S = \left[\ I_4 \ \middle|\ I_4\ \right],$$

which generates an equivalent code to C, say C'.
In such case, the associated parity-check matrix H'_S of C' is

$$H'_S = \left[\ I_{8-4} \ \middle|\ I_4^T\ \right] = \left[\ I_4 \ \middle|\ I_4\ \right],$$

which follows Definition 4.1.

Conclusion: C has an equivalent QC-LDPC code.

QC-LDPC codes

Our goal in this work (in progress) is to establish a parallel with the Gröbner basis theory for modules in order to provide conditions and/or algorithms allowing us to verify if a quasi-cyclic code, given its generator(s),

- has an equivalent LDPC code or is itself an LDPC code.
- has an equivalent code generated by a vector having minimal Hamming weight.

QC-LDPC codes

Our goal in this work (in progress) is to establish a parallel with the Gröbner basis theory for modules in order to provide conditions and/or algorithms allowing us to verify if a quasi-cyclic code, given its generator(s),

- has an equivalent LDPC code or is itself an LDPC code.
- has an equivalent code generated by a vector having minimal Hamming weight.

Contents

Perspectives

We also intend to extend Conjecture 3.1 (in the case it is true) and to link the Gröbner basis theory for modules (or even for ideals) to

Perspectives

We also intend to extend Conjecture 3.1 (in the case it is true) and to link the Gröbner basis theory for modules (or even for ideals) to

- Code-based Cryptography;

Perspectives

We also intend to extend Conjecture 3.1 (in the case it is true) and to link the Gröbner basis theory for modules (or even for ideals) to

- Code-based Cryptography;
- Coding and/or decoding of quasi-cyclic codes ([2]);

Perspectives

We also intend to extend Conjecture 3.1 (in the case it is true) and to link the Gröbner basis theory for modules (or even for ideals) to

- Code-based Cryptography;
- Coding and/or decoding of quasi-cyclic codes ([2]);
- Lattices from codes ([3], [1]).

Bibliography

- ALIASGARI, M., SADEGHI, M.-R., PANARIO, D. "Grobner Bases for Lattices and an Algebraic Decoding Algorithm". *IEEE Transactions on Communications*, vol. 61, no. 4, pp. 1222-1230, 2013.
- BRANCO DA SILVA, P. R., and SILVA, D. “Multilevel LDPC Lattices With Efficient Encoding and Decoding and a Generalization of Construction D ". *IEEE Transactions on Information Theory*, vol. 65, no. 5, pp. 3246-3260, 2019.
- CHEN, S., KURKOSKI, B. M., and ROSNES, E. “Construction D’ Lattices from Quasi-Cyclic Low-Density Parity-Check Codes". *2018 IEEE 10th International Simposium on Turbo Codes & Interative Information Processing (ISTC)*, pp. 1-5, 2018.
- COX, D., LITTLE, J., and O’SHEA, D. *Using Algebraic Geometry*. Springer, New York, 2005.
- HUFFMAN, W. C., KIM, J.- L., and SOLÉ, P. *Concise Encyclopedia of Coding Theory*. Springer, Boca Raton, 2021.
- LALLY, K., and FITZPATRICK, P., "Algebraic Structure of Quasi-cyclic Codes". *Discrete Applied Mathematics 111*, 2001.
- SKJÆRBÆK, T. *Quasi-cyclic Codes Represented by Gröbner Basis*. Thesis, Aalborg University, 2010.

Thank you!

Contact: m192298@dac.unicamp.br