A semigroup approach to Complete Decoding linear and modular codes

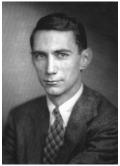
Irene Márquez-Corbella

Instituto de Investigación en Matemáticas Universidad de Valladolid
Grupo Singacom

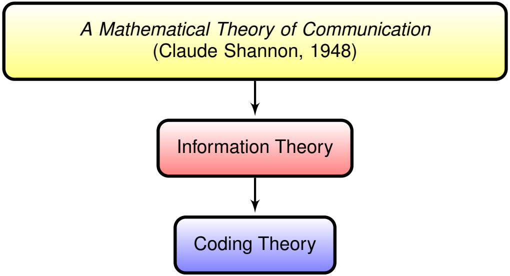
Jornadas de Álgebra, Geometría algebraica y Singularidades.

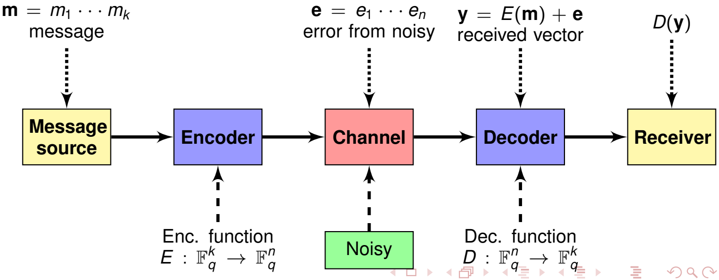
Contents

INTRODUCTION TO CODING THEORY



Claude Shannon
(1916-2001)





INTRODUCTION TO LINEAR CODES

$[n, k]$ linear code over $\mathbb{F}_q$

$\mathcal{C}$

k-dimensional subspace of $\mathbb{F}_q^n$

Generator Matrix: $G \in \mathbb{F}_q^{k\times n}$ whose rows form a basis of $\mathcal{C}$

Parity-check matrix: $H \in \mathbb{F}_q^{(n-k)\times n}$ whose nullspace is generated by the codewords of $\mathcal{C}$

Minimum distance of $\mathcal{C}$:

$$d(\mathcal{C}) = \min_{\substack{\mathbf{c}_1,\mathbf{c}_2\in\mathcal{C}\\ \mathbf{c}_1\neq\mathbf{c}_2}} \{d_{\mathrm{H}}(\mathbf{c}_1,\mathbf{c}_2)\} = \min_{\substack{\mathbf{c}\in\mathcal{C}\\ \mathbf{c}\neq\mathbf{0}}} \{w_{\mathrm{H}}(\mathbf{c})\}$$

Hamming distance of $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ is $d_{\mathrm{H}}(\mathbf{x},\mathbf{y}) = |\{i \mid x_i \neq y_i\}|$

Hamming weight of $\mathbf{x} \in \mathbb{F}_q^n$ is $w_{\mathrm{H}}(\mathbf{x}) = |\{i \mid x_i \neq 0\}|$

Ideal associated to $\mathcal{C}$

$$I(\mathcal{C}) = \left\langle \left\{ \mathbf{X}^{\mathbf{a}} - \mathbf{X}^{\mathbf{b}} \mid \mathbf{a} - \mathbf{b} \in \mathcal{C} \right\} \right\rangle$$

The General Decoding Problem

➜**Our goal:** $D(E(\mathbf{m}) + \text{noise}) = \mathbf{m}$

Maximum Likelihood Decoding (MLD)

Given a received word $\mathbf{y} \in \mathbb{F}_q^n$, find $\mathbf{x}$ that maximizes the probability:
$\mathbb{P}(\mathbf{y} \text{ received } / \mathbf{x} \text{ sent})$

On symmetric channel MLD ➜ Minimum Distance Decoding (MDD)
Output the closest codeword in Hamming distance to the received word.

Unique Decoder
Find a unique codeword that minimizes the Hamming distance to the received vector.

Complete Decoder
Find all codewords nearest to the received vector.

Complete Minimum Distance Decoding

Given a received vector $\mathbf{y} \in \mathbb{F}_q^n$ find one of the closest codewords in $\mathcal{C}$.

The General Decoding Problem

First idea: Brute Force

Compute the Hamming distance of the received word with all codewords.
➜ The complexity is $\mathcal{O}\left(nq^k\right)$

➜ Known complete decoding methods with complexity asymptotically less than that of exhaustive search can be divided mainly into three groups:

1. **Syndrome Decoding**
2. **Gradient Descent Decoding**
3. **Information Set Decoding**

Syndrome Decoding

Let $\mathcal{C}$ be an $[n, k]$ code in $\mathbb{F}_q$.

Let $\mathbf{x} \in \mathbb{F}_q^n$, the set $\mathbf{x} + \mathcal{C}$ is called a coset of $\mathcal{C}$.

- Two vectors $\mathbf{x}$ and $\mathbf{y}$ belong to the same coset $\iff \mathbf{y} - \mathbf{x} \in \mathcal{C}$.
- The cosets form a **partition** of the space $\mathbb{F}_q^n$ into q^{n-k} **classes** each containing q^k **elements**.

The words of **minimal Hamming weight** in the cosets of $\mathbb{F}_q^n/\mathcal{C}$ are the set of **coset leaders** for $\mathcal{C}$.

- $\mathrm{CL}(\mathcal{C})$: Set of coset leaders of $\mathcal{C}$.
- $\mathrm{CL}(\mathbf{y})$: Subset of coset leaders corresponding to the coset $\mathcal{C} + \mathbf{y}$.

Choose a parity check matrix H for $\mathcal{C}$. The Syndrome of a vector $\mathbf{x} \in \mathbb{F}_2^n$ is the vector

$$S(\mathbf{x}) = H\mathbf{x}^T \in \mathbb{F}_q^{n-k}$$

- The syndrome of a codeword is $\mathbf{0}$.
- Two vectors that differ by a codeword have the same syndrome, i.e.

$$H\mathbf{y}^T = H(\mathbf{c} + \mathbf{e})^T = \mathbf{0} + H\mathbf{e}^T$$

Theorem:

Two vectors belong to the same coset $\iff$ They have the same syndrome.

Syndrome Decoding

Let $\mathcal{C}$ be an $[n, k]$ code in $\mathbb{F}_q$.

Classical Syndrome Decoding

1. Construct the **syndrome lookup table**.

   i.e. enumerate the cosets of $\mathcal{C}$ in $\mathbb{F}_q^n$, choose a coset leader for each coset and compute its syndrome.
2. If $\mathbf{y}$ is the received word $\Rightarrow$ Determine from the table which coset leader $\mathbf{e}$ satisfies that $S(\mathbf{y}) = S(\mathbf{e})$.
3. Decode $\mathbf{y}$ as $\mathbf{y} - \mathbf{e} \in \mathcal{C}$.

The precomputation of this method **grows exponentially** with the length of the code $\sim \mathcal{O}\left(nq^{n-k}\right)$.

Ejemplo de Descodificación por Síndrome I

- La siguiente matriz

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \in \mathbb{F}_2^{3\times 6}$$

genera un código de parámetros $[n = 6, k = 3, d = 3]$.

- Un ejemplo de palabra del código es:

$$(0, 1, 1) \cdot G = (0, 1, 1, 0, 1, 1)$$

.

- Una matriz de paridad del código es:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{3\times 6}$$

Observamos que $G \cdot H^T = 0$.

- Este código detecta $d - 1 = 2$ errores y puede corregir $\left\lfloor \frac{d-1}{2} \right\rfloor = 1$ error.

Ejemplo de Descodificación por Síndrome II

Syndrome	Coset Leader
000	$\mathbf{0}$
001	$\mathbf{e}_6$
010	$\mathbf{e}_5$
011	$\mathbf{e}_1$
100	$\mathbf{e}_4$
101	$\mathbf{e}_2$
110	$\mathbf{e}_3$
111	$\mathbf{e}_1+\mathbf{e}_4,\ \mathbf{e}_2+\mathbf{e}_5,\ \mathbf{e}_3+\mathbf{e}_6$

TABLE: Tabla de Síndromes para $\mathcal{C}$

➜ Recibimos el vector $\mathbf{y}=(1,1,0,1,0,0)\in\mathbb{F}_2^6$.

Calculamos su síndrome $S(\mathbf{y})=H\mathbf{y}^T=010$.

Descodificamos $\mathbf{y}$ por $\mathbf{y}-\mathbf{e}_5=(1,1,0,1,1,0)$.

➜ Recibimos el vector $\mathbf{y}=(1,0,0,1,0,0)\in\mathbb{F}_2^6$.

Calculamos su síndrome $S(\mathbf{y})=H\mathbf{y}^T=111$.

La clase de equivalencia de $\mathbf{y}$ tiene 3 coset leaders. Existen por lo tanto tres posibles soluciones:

1. $\mathbf{y}+\mathbf{e}_1+\mathbf{e}_4=\mathbf{0}$,
2. $\mathbf{y}+\mathbf{e}_2+\mathbf{e}_5=(1,1,0,1,1,0)$
3. $\mathbf{y}+\mathbf{e}_3+\mathbf{e}_6=(1,0,1,1,0,1)$

GRADIENT DESCENT DECODING

Let $\mathcal{C}$ be an $[n, k]$ code in $\mathbb{F}_q$.

TEST-SET

A **Test-set** for $\mathcal{C}$ is a subset $\mathcal{T}_{\mathcal{C}} \subset \mathcal{C}$ such that foe every vector $\mathbf{y} \in \mathbb{F}_q^n$ either $\mathbf{y} \in \mathrm{CL}(\mathcal{C})$ or there exists $\mathbf{t} \in \mathcal{T}_{\mathcal{C}}$ such that $\mathrm{w}_H(\mathbf{y} - \mathbf{t}) < \mathrm{w}_H(\mathbf{y})$.

GENERAL PRINCIPLE

1. Precomputed and stored in memory a Test-set $\mathcal{T}_{\mathcal{C}}$ for $\mathcal{C}$ in advance.
2. Recursively inspect the Test-set $\mathcal{T}_{\mathcal{C}}$ for the existence of an adequate element which is subtracted from the current vector.

The complexity is $\mathcal{O}(n|\mathcal{T}_{\mathcal{C}}|)$.

INTRODUCTION TO GRÖBNER BASIS

- $\mathbb{K}[\mathbf{x}]$ = polynomial ring in n variables over the field $\mathbb{K}$
- $[X]$ = set of monomials of $\mathbb{K}[\mathbf{x}] = \left\{ \mathbf{x}^{\mathbf{a}} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \ : \mathbf{a} \in \mathbb{Z}^n_{\geq 0} \right\}$
- A **term order** on $\mathbb{K}[\mathbf{x}]$ is a total well-ordering $\succ$ on $[X]$ such that:

$$\mathbf{x}^{\mathbf{a}} \succ \mathbf{x}^{\mathbf{b}} \Rightarrow \mathbf{x}^{\mathbf{a}+\mathbf{c}} \succ \mathbf{x}^{\mathbf{b}+\mathbf{c}} \text{ for all } \mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{Z}^n_{\geq 0}.$$

Example: *degree lexicographic order* (deglex)

$$\mathbf{x}^{\mathbf{a}} \succ_{\texttt{deglex}} \mathbf{x}^{\mathbf{b}} \Longleftrightarrow \deg(\mathbf{x}^{\mathbf{a}}) > \deg(\mathbf{x}^{\mathbf{b}}) \text{ or } \deg(\mathbf{x}^{\mathbf{a}}) = \deg(\mathbf{x}^{\mathbf{b}}) \text{ and } \mathbf{a} \succ_{\texttt{lex}} \mathbf{b}$$

- **Leading term** of $f(\mathbf{x}) \in \mathbb{K}[\mathbf{x}]$ w.r.t. $\prec$ = $\mathrm{LT}_{\prec}(f)$.
- Let I be an ideal in $\mathbb{K}[\mathbf{x}]$, the **initial ideal** is $\mathrm{in}_{\prec}(I) = \langle \mathrm{LT}_{\prec}(f) \ : \ f \in I \rangle$.

GRÖBNER BASIS

A finite subset $\mathcal{G}$ of $\mathcal{I}$ is a Gröbner basis w.r.t the term order $\succ$ if

$$\mathrm{in}_{\succ}(\mathcal{I}) = \langle \mathrm{LT}_{\succ}(g) \ : \ g \in \mathcal{G} \rangle .$$

THEOREM

If $\succ$ is fixed, then every ideal $\mathcal{I} \subseteq \mathbb{K}[\mathbf{x}]$ has a unique reduced Gröbner basis.

The reduced Gröbner basis $\mathcal{G}$ can be computed from any generating set of $\mathcal{I}$ by a method introduced by Bruno Buchberger in 1965.

2 BINARY CODES

- Gröbner representation
- Computing coset leaders
- Gradient Descent Decoding

➜ Throughout this section $\mathcal{C}$ will be a **binary linear code** of length n and dimension k, i.e. a k-dimensional linear subspace of $\mathbb{F}_2^n$.

➜ This section essentially follows:

M. Borges-Quintana, M.A. Borges-Trenard, I. Márquez-Corbella and E. Martínez-Moro, *An Algebraic view to gradient descent decoding*, In Information Theory Workshop (ITW), 2010, pages 1-4.

M. Borges-Quintana, M.A. Borges-Trenard, I. Márquez-Corbella and E. Martínez-Moro, *Computing coset leaders and leader codewords of binary codes*, Submitted, 2012.

➜ Both are joint works:

- M. Borges-Quintana (University of Oriente - Santiago de Cuba).
- M.A. Borges-Trenard (University of Oriente - Santiago de Cuba).
- E. Martínez-Moro (University of Valladolid - Spain).

BINARY CODES

➜ Let $\mathcal{C}$ be an $[n, k]$ binary code.

Characteristic crossing functions:

$$\blacktriangledown : \mathbb{Z}^s \longrightarrow \mathbb{Z}_2^s \quad \text{and} \quad \blacktriangle : \mathbb{Z}_2^s \longrightarrow \mathbb{Z}^s .$$

- The map $\blacktriangledown$ is reduction modulo 2.
- The map $\blacktriangle$ replaces the class of $0, 1$ by the same symbols regarded as integers.

THEOREM [BORGES-BORGES-FITZPATRICK-MARTÍNEZ (2008)]

Let $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ label the rows of a generator matrix for $\mathcal{C}$.

$$I(\mathcal{C}) = \left\langle \left\{ \mathbf{X}^{\blacktriangle \mathbf{w}_i} - 1 \right\}_{i=1,\ldots,k} \bigcup \left\{ x_j^2 - 1 \right\}_{j=1,\ldots,n} \right\rangle$$

THEOREM [BORGES-BORGES-FITZPATRICK-MARTÍNEZ (2008)]

Any reduced **Gröbner basis** $\mathcal{G}$ of $I(\mathcal{C})$ relative to a degree compatible ordering induce a **test-set** for $\mathcal{C}$.

COROLLARY

$\mathrm{Red}(\mathbf{X}^{\mathbf{a}}, \mathcal{G}) = \mathbf{X}^{\mathbf{e}}$ provides a **coset leader** even if $\mathrm{w}_H(\mathbf{e}) \geq t$

Gröbner representation of binary codes

Let $\{\mathbf{e}_i \mid i \in \{1,\ldots,n\}\}$ be a canonical basis of $\mathbb{F}_2^n$.

Gröbner representation

A Gröbner representation of an $[n,k]$ binary linear code $\mathcal{C}$ is a pair $(\mathcal{N},\phi)$ where:

- $\mathcal{N}$ is transversal of the cosets in $\mathbb{F}_2^n/\mathcal{C}$ verifying that:
  - ➜ $\mathbf{0} \in \mathcal{N}$
  - ➜ $\mathbf{n} \in \mathcal{N} \setminus \{\mathbf{0}\} \implies \exists i \in \{1,\ldots,n\} \ : \ \mathbf{n} = \mathbf{n}' + \mathbf{e}_i$ with $\mathbf{n}' \in \mathcal{N}$
- $\phi : \quad \mathcal{N} \times \{\mathbf{e}_i\}_{i=1}^n \longrightarrow \mathcal{N}$

➜ that maps each pair $(\mathbf{n},\mathbf{e}_i)$ to the element of $\mathcal{N}$ representing the coset of $\mathbf{n}+\mathbf{e}_i$.

Some references on Gröbner representation of codes and its implementations:

M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick and E. Martínez-Moro, *Gröbner bases and combinatorics for binary codes*, Appl. Algebra Engrg. Comm. Comput. Volume 19, no.5, 393–411, 2008.

M. Borges-Quintana, M.A. Borges-Trenard and E. Martínez-Moro, *A Gröbner bases structure associated to linear codes*, J. Discrete Math. Sci. Cryptogr. Volume 10, no.2, 151–191, 2007.

M. Borges-Quintana, M. A. Borges-Trenard and E. Martínez-Moro. *A general framework for applying FGLM techniques to linear codes.* Lectures Notes in Comput. Sci., AAECC 16, volume 3857, 76-86, 2006.

M. Borges-Quintana, M. A. Borges-Trenard and E. Martínez-Moro. *GBLA-LC: Gröbner bases by Linear Algebra and Linear Codes.* ICM 2006. Mathematical Software, EMS, 604-605, 2006.

Gröbner representation of binary codes

Example 1

Let $\mathcal{C}$ be a $[6,3,3]$ binary code with generator matrix G and parity check matrix H given by:

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \quad \text{and} \quad H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

➜ Binomial ideal associated to $\mathcal{C}$:

$$I_2(\mathcal{C}) = \left\langle \{x_1x_4x_5x_6 - 1, x_2x_5x_6 - 1, x_3x_4x_6 - 1\} \cup \left\{x_i^2 - 1\right\}_{i=1,\ldots,6} \right\rangle$$

➜ The reduced Gröbner basis of $I_2(\mathcal{C})$w.r.t. `degrevlex` order with $x_1 < \ldots < x_6$:

$$\left\{ \begin{array}{l} x_6x_5 - x_3, \quad x_6x_4 - x_2, \quad x_6x_3 - x_5, \quad x_6x_2 - x_4, \\ x_5x_4 - x_6x_1, \quad x_5x_3 - x_6, \quad x_5x_2 - x_1, \quad x_5x_1 - x_2, \\ x_4x_3 - x_1, \quad x_4x_2 - x_6, \quad x_4x_1 - x_3, \\ x_3x_2 - x_6x_1, \quad x_3x_1 - x_4, \\ x_2x_1 - x_5 \end{array} \right\} \cup \left\{x_i^2 - 1\right\}_{i=1,\ldots,6}$$

➜ which correspond to: $\mathcal{N} = \{ \ \mathbf{0}, \ \mathbf{e}_1, \ \mathbf{e}_2, \mathbf{e}_3, \ \mathbf{e}_4, \ \mathbf{e}_5, \mathbf{e}_6, \ \mathbf{e}_1 + \mathbf{e}_6 \ \}$

$$\begin{array}{lll} [\mathbf{0}, \ [2,3,4,5,6,7]], & [\mathbf{e}_1, \ [1,5,6,3,4,8]], & [\mathbf{e}_2, \ [5,1,8,2,7,6]], \\ [\mathbf{e}_3, \ [6,8,1,7,2,5]], & [\mathbf{e}_4, \ [3,2,7,1,2,5]], & [\mathbf{e}_5, \ [4,7,2,8,1,3]], \\ [\mathbf{e}_6, \ [8,6,5,4,3,1]], & [\mathbf{e}_1 + \mathbf{e}_6, \ [7,4,3,6,5,2]] & \end{array}$$

Computing coset leaders

Algorithm 2.1: Algorithm for computing all the coset leader of a binary code $\mathcal{C}$

Data: A weight compatible ordering $\prec$ and a parity check matrix H of a binary code $\mathcal{C}$.
Result: The set of coset leaders $\mathrm{CL}(\mathcal{C})$ and $(\mathcal{N}, \phi)$ a Gröbner representation for $\mathcal{C}$.

$\texttt{List} \longleftarrow [0]; \mathcal{N} \longleftarrow \emptyset; r \longleftarrow 0; \mathrm{CL}(\mathcal{C}) \longleftarrow \emptyset; \mathcal{S} \longleftarrow \emptyset;$
while $\texttt{List} \neq \emptyset$ **do**
  $\mathbf{t} \longleftarrow \texttt{NextTerm}[\texttt{List}]; \mathbf{s} \longleftarrow \mathbf{t}H^T;$
  $j \longleftarrow \texttt{Member}[\mathbf{s}, \mathcal{S}];$
  if $j \neq \texttt{false}$ **then**
    for $k \in \mathrm{supp}(\mathbf{t}) \ : \ \mathbf{t} = \mathbf{t}' + \mathbf{e}_k$ *with* $\mathbf{t}' \in \mathcal{N}$ **do**
      $\phi(\mathbf{t}', \mathbf{e}_k) \longleftarrow \mathbf{t}_j$
    if $\mathrm{w}_H(\mathbf{t}) = \mathrm{w}_H(\mathbf{t}_j)$ **then**
      $\mathrm{CL}(\mathcal{C})[\mathbf{t}_j] \longleftarrow \mathrm{CL}\mathcal{C}[\mathbf{t}_j] \cup \{\mathbf{t}\};$
      $\texttt{List} \longleftarrow \texttt{InsertNext}[\mathbf{t}, \texttt{List}];$
  else
    $r \longleftarrow r + 1; \mathbf{t}_r \longleftarrow \mathbf{t}; \mathcal{N} \longleftarrow \mathcal{N} \cup \{\mathbf{t}_r\};$
    $\mathrm{CL}(\mathcal{C})[\mathbf{t}_r] \longleftarrow \{\mathbf{t}_r\}; \mathcal{S} \longleftarrow \mathcal{S} \cup \{\mathbf{s}\};$
    $\texttt{List} = \texttt{InsertNext}[\mathbf{t}_r, \texttt{List}];$
    for $k \in \mathrm{supp}(\mathbf{t}_r) \ : \ \mathbf{t}_r = \mathbf{t}' + \mathbf{e}_k$ *with* $\mathbf{t}' \in \mathcal{N}$ **do**
      $\phi(\mathbf{t}', \mathbf{e}_k) \longleftarrow \mathbf{t}_r;$
      $\phi(\mathbf{t}_r, \mathbf{e}_k) \longleftarrow \mathbf{t}';$

➜ **Complexity:** $n|\mathrm{CL}(\mathcal{C})| \Rightarrow$ has **near-optimal performance**.

➜ Using algorithm 2.1, we obtain the following list of coset leaders:

Coset Leaders $\mathrm{CL}(\mathcal{C})$	
$\mathrm{CL}(\mathcal{C})_0$	$[\mathbf{0}]$
$\mathrm{CL}(\mathcal{C})_1$	$[\mathbf{e}_1],\ [\mathbf{e}_2],\ [\mathbf{e}_3],\ [\mathbf{e}_4],\ [\mathbf{e}_5],\ [\mathbf{e}_6]$
$\mathrm{CL}(\mathcal{C})_2$	$[\mathbf{e}_1+\mathbf{e}_6,\ \mathbf{e}_2+\mathbf{e}_3,\ \mathbf{e}_4+\mathbf{e}_5]$

TABLE: List of coset leaders in Example 1

➜ The algorithm could be adapted without incrementing the complexity to obtain the following **additional information**:

- **Newton radius** $(\nu(\mathcal{C}))$:
  Largest weight of any vector that can be uniquely corrected.
- **Covering radius** $(\rho(\mathcal{C}))$:
  Smallest integer *s* such that $\mathbb{F}_q^n$ is the union of the spheres of radius *s* centered at the codewords of $\mathcal{C}$.
- **Weight Distribution of the Coset leaders** (WDCL):
  List $(\alpha_0, \ldots, \alpha_n)$ where *alpha*$_i$ is the number of cosets with weight *i*.
- **Number of coset leaders in each coset**.

➜ **In our example:** $\nu(\mathcal{C}) = 1$, $\rho(\mathcal{C}) = 2$, $\mathrm{WDCL} = \left[\ 1, 6, 1, 0, 0, 0\ \right]$ and

$$\sharp\,(\mathrm{CL}) = \left[\begin{array}{l} 1, \\ 1, 1, 1, 1, 1, 1 \\ 3 \end{array}\right].$$

Gradient Descent Decoding (GDD)

Classical Syndrome Decoding

1. Construct the **syndrome lookup table**.

   i.e. enumerate the cosets of $\mathcal{C}$ in $\mathbb{F}_q^n$, choose a coset leader for each coset and compute its syndrome.

2. If $\mathbf{y}$ is the received word $\Rightarrow$ Determine from the table which coset leader $\mathbf{e}$ satisfies that $S(\mathbf{y}) = S(\mathbf{e})$.
3. Decode $\mathbf{y}$ as $\mathbf{y} - \mathbf{e} \in \mathcal{C}$.

The precomputation of this method **grows exponentially** with the length of the code.

- **Main advantage of GDD**: this task is broken into smaller steps.
- In the literature there are two GDD for binary codes proposed independently by Liebler and Ashikmin and Barg.
- **Both algorithms can be seen as two ways of understanding the reduction associated to the Gröbner representation of the code!!!**

LIEBLER'S GRADIENT DESCENT DECODING

Algorithm 2.2: I-GDDA

Data: $\mathbf{y} \in \mathbb{F}_2^n$ the received word.
Result: A codeword $\mathbf{c} \in \mathcal{C}$ that is closest to $\mathbf{y}$.

```
while w_H(y) ≠ 0 do
    Compute y' ∈ F_2^r such that
    d_H(y, y') = 1 and w_H(ȳ) ≥ w_H(ȳ');
    y := y';
end
return c = y;
```

See:

R. Liebler.
Implementing gradient descent decoding.
Michigan Math. J., volume 58, Issue 1, 285-291, 2009.

SOME REMARKS:

- In each step of the Algorithm 2.2 the vector $\mathbf{y}$ changes between different cosets of $\mathbb{F}_2^n/\mathcal{R}_{\mathcal{C}}$ until it arrives to the $\overline{\mathbf{0}}$ coset, i.e. $\mathbf{y} \in \mathcal{C}$.
- This is essentially the **syndrome decoding algorithm** broken up in smaller steps.

Liebler's Gradient Descent Decoding vs. Gröbner representation

We define the **reduction of an element** $\mathbf{n} \in \mathcal{N}$ relative to e_i as the element $\mathbf{n}' = \phi(\mathbf{n}, e_i) \in \mathcal{N}$, denoted by $\mathbf{n} \rightarrow_i \mathbf{n}'$.

➜ For each $\mathbf{y} \in \mathbb{F}_2^n$, $\mathbf{y} = \mathbf{0} + \sum_j e_{i_j}$ for some $i_j \in \{1, \ldots, n\}$

➜ Thus we can **iterate a finite number of reductions** to find the closest codeword.

➜ This gives us the following GDDA:

➜ See resemblance with **Liebler's Algorithm**.

Algorithm 2.3: $(\mathcal{N}, \phi)$- reduction

Data: $(\mathcal{N}, \phi)$ a Gröbner representation for $\mathcal{C}$ w.r.t. a total degree ordering and the received word $\mathbf{y} \in \mathbb{F}_2^n$.
Result: A codeword $\mathbf{c} \in \mathcal{C}$ that minimized the Hamming distance $\mathrm{d}_H(\mathbf{c}, \mathbf{y})$.

$\mathbf{y} = \sum_{j=1}^{s} \mathbf{e}_{i_j}$ i.e. $\mathrm{supp}(\mathbf{y}) = \{i_1, \ldots, i_s\}$

Forward Step: // Compute $n \in \mathcal{N}$ corresponding to the coset $\mathbf{y} + \mathcal{C}$, i.e. $\mathbf{n} \in \mathrm{CL}(\mathbf{y})$

$\mathbf{n} \longleftarrow \mathbf{0}$
for $j \leftarrow 1$ **to** s **do**
  $\mathbf{n} \longrightarrow_{i_j} \mathbf{n}'$ // i.e. $\mathbf{n}' = \phi(\mathbf{n}, \mathbf{e}_{i_j})$
  $\mathbf{n} \longleftarrow \mathbf{n}'$

Backward Step:

while $\mathbf{n} \neq \mathbf{0}$ **do**
  Find $i \in \{1, \ldots, n\}$ such that $\mathrm{w}_H(\mathbf{n}) > \mathrm{w}_H(\phi(\mathbf{n}, \mathbf{e}_i))$
  $\mathbf{y} \longleftarrow \mathbf{y} + \mathbf{e}_i$
  $\mathbf{n} \longleftarrow \phi(\mathbf{n}, \mathbf{e}_i)$

Return $\mathbf{c} = \mathbf{y}$

Ashikmin-Barg's Gradient Descent Decoding

Algorithm 2.4: ts-GDDA

Data: $\mathbf{y} \in \mathbb{F}_2^n$ the received word and a Test Set $\mathcal{T}$ for $\mathcal{C}$.
Result: A codeword $\mathbf{c} \in \mathcal{C}$ that is closest to $\mathbf{y}$.

```
c := 0;
while no t ∈ T is found such that w_H(y − t) < w_H(y) do
    c := c + t;
    y := y − t;
end
return c;
```

See:

A. Ashikhmin and A. Barg.
Minimal vectors in linear codes.
IEEE Trans. Inform.Theory, volume 44, 2010-2017, 1998.

Some remarks:

- This algorithm **stays entirely in one coset** of the code until it arrive to a coset leader.
- If $\mathcal{T} = \mathcal{M}_{\mathcal{C}}$ the algorithm 2.4 performs *Complete Minimum Distance Decoding*.

Ashikmin-Barg's Gradient Descent Decoding vs. Gröbner representation I

- Associated to the Gröbner representation $(\mathcal{N}, \phi)$ for the binary code $\mathcal{C}$ we can define the **border of a code**:

$$\mathcal{B}(\mathcal{C}) = \left\{ (\mathbf{n} + \mathbf{e}_i, \phi(\mathbf{n}, \ \mathbf{e}_i)) \ \middle| \ \begin{array}{c} \mathbf{n} + \mathbf{e}_i \neq \phi(\mathbf{n}, \mathbf{e}_i), \mathbf{n} \in \mathcal{N} \\ \text{and} \quad i \in \{1, \ldots, n\} \end{array} \right\}$$

- Let $\mathbf{b} = (\mathbf{b}_1, \mathbf{b}_2) \in \mathcal{B}(\mathcal{C})$ we define:

$$\mathrm{head}(\mathbf{b}) = \mathbf{b}_1 \in \mathbb{F}_2^n \quad \text{and} \quad \mathrm{tail}(\mathbf{b}) = \mathbf{b}_2 \in \mathbb{F}_2^n$$

- $\mathrm{head}(\mathbf{b}) + \mathrm{tail}(\mathbf{b}) \in \mathcal{C}$.
- The information in the border is somehow **redundant**, we can reduce the number of codewords in it by defining the following structure.

Reduced Border of a code

Let $\prec$ be a term ordering. A subset $R(\mathcal{C}) \subseteq B(\mathcal{C})$ is called the *reduced border of the code* $\mathcal{C}$ w.r.t. $\prec$ if it fulfills the following conditions:

- For each element in the border $\mathbf{b} \in B(\mathcal{C})$ there exists an element $\mathbf{h}$ in $R(\mathcal{C})$ such that $\mathrm{supp}\left(\mathrm{head}(\mathbf{h})\right) \subseteq \mathrm{supp}\left(\mathrm{head}(\mathbf{b})\right)$.
- For every two different elements $\mathbf{h}_1$ and $\mathbf{h}_2$ in $R(\mathcal{C})$ neither $\mathrm{supp}(\mathrm{head}(\mathbf{h}_1)) \subseteq \mathrm{supp}\left(\mathrm{head}(\mathbf{h}_2)\right)$ nor $\mathrm{supp}(\mathrm{head}(\mathbf{h}_2)) \subseteq \mathrm{supp}\left(\mathrm{head}(\mathbf{h}_1)\right)$ is verified.

Ashikmin-Barg's Gradient Descent Decoding vs. Gröbner representation II

Proposition:

Let us consider the set of codewords in $\mathcal{C}$ given by

$$M_{\mathrm{Red}_{\prec}}(\mathcal{C}) = \{\mathrm{head}(\mathbf{b}) + \mathrm{tail}(\mathbf{b}) \mid \mathbf{b} \in R(\mathcal{C})\}$$

Then $M_{\mathrm{Red}_{\prec}}(\mathcal{C})$ corresponds to a subset of codewords of minimal support of $\mathcal{C}$, $\mathcal{M}_{\mathcal{C}}$.

➜ Thus $\mathcal{R}(\mathcal{C})$ **is a minimal test-set that allow Ashikmin-Barg's GDD**.

3 MODULAR CODES

- Relationship to integer linear programming
- Minimal support codewords
- How to reduce the complexity?

➜ Throughout this section $\mathcal{C}$ will be a **modular code** of length n defined over $\mathbb{Z}_q$, i.e. a submodule of $\left(\mathbb{Z}_q^n, +\right)$.

➜ The result of this section are joint work with E. Martínez-Moro from University of Valladolid (Spain) and appeared in:

I. Márquez-Corbella and E. Martínez-Moro,
Algebraic structure of the minimal support codewords set of some linear codes,
Adv. Math. Commun. 5(2):233-244, 2011.

I. Márquez-Corbella and E. Martínez-Moro,
Decomposition of Modular Codes for Computing Test Sets and Graver Basis,
Mathematics in Computer Science, 6:147-165, 2012.

THE IDEAL ASSOCIATED WITH A MODULAR CODE

➜ Let $\mathcal{C}$ be an $[n,k]$ modular code over $\mathbb{Z}_m$.

Characteristic crossing functions:

$$\blacktriangledown : \mathbb{Z}^s \longrightarrow \mathbb{Z}_m^s \quad \text{and} \quad \blacktriangle : \mathbb{Z}_m^s \longrightarrow \mathbb{Z}^s .$$

- The map $\blacktriangledown$ is reduction modulo m.
- The map $\blacktriangle$ replaces the class of $0, 1, \ldots, m-1$ by the same symbols regarded as integers.

THEOREM:[MÁRQUEZ-MARTÍNEZ (2011)]

Given a generator matrix $G \in \mathbb{Z}_q^{k\times n}$ of $\mathcal{C}$ and let label its rows by $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\} \subseteq \mathbb{Z}_q^n$. The following ideal match the ideal $I(\mathcal{C})$:

$$I_m(\mathcal{C}) = \left\langle \ \left\{\mathbf{X}^{\mathbf{w}_j} - 1\right\}_{j=1,\ldots,k} \ \cup \ \left\{x_i^q - 1\right\}_{i=1,\ldots,n} \ \right\rangle \subseteq \mathbb{K}[\mathbf{X}]$$

Relationship to Integer Linear Programming

Modular Integer Program Problem

Let $A \in \mathbb{Z}_q^{m \times n}$, $\mathbf{b} \in \mathbb{Z}_q^m$ and $\mathbf{w} \in \mathbb{R}^n$, we define

$$\mathrm{IP}_{A,\mathbf{w},q}(\mathbf{b}) = \left\{ \begin{array}{l} \text{Minimize } \mathbf{w} \cdot \blacktriangle\mathbf{u} \\ \text{subject to } \left\{ \begin{array}{ll} A\mathbf{u}^t \equiv \mathbf{b} & \mod q \\ \mathbf{u} \in \mathbb{Z}_q^n \end{array} \right. \end{array} \right.$$

$\neq$ except for the binary case

Minimum Distance Decoding (MDD)

Let $\mathcal{C}$ be a linear $[n, k]$ code. Given a received word $\mathbf{y} \in \mathbb{F}_q^n$ **MDD** is to find a codeword $\mathbf{x} \in \mathcal{C}$ that minimizes the Hamming distance $\mathrm{d}_H(\mathbf{x}, \mathbf{y})$.

Test-Set

A *test-set* for $\mathrm{IP}_{A,\mathbf{w},q}(\mathbf{b})$ is a subset $\mathcal{T}_{\succ_w} \subseteq \ker_{\mathbb{Z}_q}(A)$ such that for each non-optimal solution $\mathbf{u}$ there exists $t \in \mathcal{T}_{\succ_\mathbf{w}}$ such that $\mathbf{u} - t$ is also a solution and $t \succ_\mathbf{w} 0$.

$\neq$ except for the binary case

Test-Set

A *test-set* for the code $\mathcal{C}$ is a subset

$$\mathcal{T} \subseteq \mathcal{C}$$

such that for every vector $\mathbf{y} \in \mathbb{F}_q^n$ either $\mathbf{y} \in \mathcal{C}$ or there exists a $t \in \mathcal{T}$ such that $w_H(\mathbf{y} - t) < w_H(\mathbf{y})$

We can define the ideal associated to $\mathrm{IP}_{A,\mathbf{w},q}(\mathbf{b})$ as

$$I(A^\perp) = \left\langle \left\{ \mathbf{x}^{\blacktriangle\mathbf{w}_j} - 1 \right\}_{j=1}^{k} \cup \left\{ x_i^q - 1 \right\}_{i=1}^{q} \right\rangle$$

where $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\} \subseteq \mathbb{Z}_q^n$ is a set of $\mathbb{Z}_q$-generators of the row space of the matrix $A \in \mathbb{Z}_q^{m \times n}$.

A reduced Gröbner basis of $I(A^\perp)$ induced a test-set for $\mathrm{IP}_{A,\mathbf{w},q}(\mathbf{b})$

Universal Test-Set for $IP_{H,q}(\mathbf{b}) \supseteq$ Codewords of minimal support of $\mathcal{C}$

A Graver basis of $I(H^\perp)$

GRAVER BASIS

B. STURMFELS, *Gröbner bases bases and Convex Polytopes*

➜ The ideal associated to the $\mathbb{Z}$-kernel of the matrix $A \in \mathbb{Z}^{m\times n}$ is:

$$I_A = \langle \{ \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \mid \mathbf{u} \in \ker_{\mathbb{Z}}(A) \} \rangle.$$

$\mathcal{U}_A$ = Universal Gröbner basis of I_A.

➜ A binomial $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ in I_A is called **primitive** if there exists no other binomial $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-}$ in I_A such that $\mathbf{x}^{\mathbf{v}^+}$ divides $\mathbf{x}^{\mathbf{u}^+}$ or $\mathbf{x}^{\mathbf{v}^-}$ divides $\mathbf{x}^{\mathbf{u}^-}$.

Gr_A= Graver basis of I_A= set of primitive binomials of I_A.

PROPOSITION

$$\mathcal{U}_A \subseteq \mathrm{Gr}_A$$

How to compute a Graver basis

Lawrence lifting

The Lawrence lifting of the integer matrix $A \in \mathbb{Z}^{m\times n}$ is the enlarge matrix

$$\Lambda(A) = \left(\begin{array}{c|c} A & 0 \\ \hline 1 & 1 \end{array}\right) \in \mathbb{Z}^{(m+n)\times 2n}$$

Where $1 \in \mathbb{Z}^{n\times n}$ is the identity matrix and $0 \in \mathbb{Z}^{m\times n}$ is the zero matrix.

- $\ker(\Lambda(A)) = \{(\mathbf{u}, -\mathbf{u}) \mid \mathbf{u} \in \ker(A)\}$.
- $I_{\Lambda(A)} = \left\langle \mathbf{x}^{\mathbf{u}^+}\mathbf{y}^{\mathbf{u}^-} - \mathbf{x}^{\mathbf{u}^-}\mathbf{y}^{\mathbf{u}^+} \mid \mathbf{u} \in \ker(A) \right\rangle \subseteq \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n]$.

Theorem (Sturmfels)

For a Lawrence type matrix $\Lambda(A) \in \mathbb{Z}^{(m+n)\times n}$ the following sets of binomials coincide:

$$Gr_{\Lambda(A)} = \mathcal{U}_{\Lambda(A)} = G,$$

where G is any reduced Gröbner basis of the ideal $I_{\Lambda(A)}$.

Algorithm 3.1: Algorithm for computing the Graver basis of I_A

Data: An integer matrix $A \in \mathbb{Z}^{m\times n}$.
Result: The Graver basis of I_A, Gr_A.

1 We choose any term order on $\mathbb{K}[\mathbf{x}, \mathbf{y}]$;
2 We defined the Lawrence lifting of the matrix $A := \Lambda(A)$;
3 We compute a reduced Gröbner basis of $I_{\Lambda(A)}$;
4 We substitute the variable $\mathbf{y}$ by $\mathbf{1}$;

Minimal support codewords

Minimal support codeword

A nonzero codeword $\mathbf{m}$ in $\mathcal{C}$ is a *minimal support codeword* if there is no other codeword $\mathbf{c} \in \mathcal{C}$ such that

$$\mathrm{supp}(\mathbf{c}) \subseteq \mathrm{supp}(\mathbf{m}).$$

➜ We denote by $\mathcal{M}_{\mathcal{C}}$ the set of codewords of minimal support of $\mathcal{C}$.

Theorem [Márquez-Martínez 2011]

Choose a parity check matrix $H \in \mathbb{Z}_q^{(n-k)\times n}$ for $\mathcal{C}$.

➜ $\mathcal{M}_{\mathcal{C}}$ is a subset of the Graver basis of H.

Corollary

$\mathcal{M}_{\mathcal{C}}$ can be computed from any Gröbner basis of the ideal

$$\left\langle \left\{ \mathbf{x}^{\blacktriangle \mathbf{w}_1} \mathbf{z}^{\blacktriangle \mathbf{w}_1 (q-1)} - 1, \ldots, \mathbf{x}^{\blacktriangle \mathbf{w}_k} \mathbf{z}^{\blacktriangle \mathbf{w}_k (q-1)} - 1 \right\} \cup \left\{ x_i^q - 1 \right\}_{i=1}^n \cup \left\{ z_i^q - 1 \right\}_{i=1}^n \right\rangle$$

where $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\} \subseteq \mathbb{Z}_q^n$ are the rows of a generator matrix of $\mathcal{C}$.

I. Márquez-Corbella and E. Martínez-Moro,
Algebraic Structure of the minimal support codewords set of some linear codes,
Advances in Mathematics of Communications, volume 5, No. 2, 233-244, 2011.

How to reduce the complexity? I

1. **FGLM technique to compute a Gröbner basis**

- We know a set of generators of the ideal $I(\mathcal{C})$:

$$I(\mathcal{C}) = \left\langle \ \left\{\mathbf{X}^{\blacktriangle \mathbf{w}_i} - 1\right\}_{i=1,\ldots,k} \quad \bigcup \quad \left|\left\{X_i^q - 1\right\}_{i=1}^n \ \right\rangle$$

where $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\} \subseteq \mathbb{Z}_q^n$ are rows of a generator matrix of $\mathcal{C}$.

➜ In order to compute a Gröbner basis of $I(\mathcal{C})$ we can use FGLM-techniques.

M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick and E. Martínez-Moro,
Gröbner bases and combinatorics for binary codes,
Appl. Algebra Engrg. Comm. Comput. Volume 19, no.5, 393–411, 2008.

- This procedure is completely general and it has the following advantages:
  - The problem of **growth of the total degree** do not have to be considered since the total degree of the binomials involved is bounded by $n \times q$.
  - The problem of **coefficient growth** do not have to be considered since we can take as base field $\mathbb{K} = \mathbb{F}_2$.
  - All the steps can be carried out as Gaussian elimination steps.

How to reduce the complexity? II

2 Decomposition of modular codes

- We can reduce the complexity by using the decomposition of a given code as "gluing" of smaller ones.

Our aim is to explicitly define a procedure that:

1. (Decomposition) Find a decomposition of an $[n, k]$-code $\mathcal{C}$ into the m-gluing of two (or more) smaller codes, denoted by $\{\mathcal{C}_\alpha\}_{\alpha\in A}$.
2. Compute $\mathcal{M}_{\mathcal{C}_\alpha}$ the set of codewords of minimal support of $\mathcal{C}_\alpha$ for each $\alpha \in A$.
3. (Gluing) Compute $\mathcal{M}_{\mathcal{C}}$ from $\{\mathcal{M}_{\mathcal{C}_\alpha}\}_{\alpha\in A}$.

➜ **Parallel computing** is well suited for **Step 2**.
➜ A similar process can be defined to compute the **Gröbner test-set** for a **binary code**.

- The concept of "glue" was already used by other authors:

J.C. Rosales,
On presentations of subsemigroups of $\mathbb{N}^n$,
Semigroup Forum, 55(2):152-159, 1997.

A. Thoma,
Construction of set theoretic complete intersection via semigroup gluing,
Beiträge Algebra Geom., 41(1):195-198, 2000.

J.I. García-García, M.A. Moreno-Frías and A. Vigneron-Tenorio.
On glued semigroups.
arXiv: 1104.2836v2, 2011.

Decomposition of modular codes I

➜ **Direct Sum**

$$G = \left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right) \in \mathbb{Z}_m^{k\times n} \quad \Longleftrightarrow \quad I(\mathcal{C}) = I(\mathcal{C}_1) + I(\mathcal{C}_2)$$

$$A_i \in \mathbb{Z}_m^{k_i \times n_i} \quad \Longleftrightarrow \quad \text{length of } \mathcal{C}_i = n_i \text{ and } \dim(\mathcal{C}_i) = \mathrm{rank}(A_i) = k_i$$

➜ **1-gluing**

$$G = \left(\begin{array}{c|c} A_1 & 0 \\ \hline b_1 & b_2 \\ \hline 0 & A_2 \end{array}\right) \in \mathbb{Z}_m^{k\times n} \quad \Longleftrightarrow \quad I(\mathcal{C}) = I(\hat{\mathcal{C}}_1) + I(\hat{\mathcal{C}}_2) + \left\langle \mathbf{X}^{\alpha} - \mathbf{Y}^{\beta} \right\rangle$$

with $\mathrm{rank}(b_i) = 1$

$$G_1 = \left(\begin{array}{c|c} A_1 & 0 \\ \hline b_1 & * \end{array}\right) \quad \text{and} \quad G_2 = \left(\begin{array}{c|c} * & b_2 \\ \hline 0 & A_2 \end{array}\right)$$

Decomposition of modular codes II

➜ **3-gluing**

$$G = \left(\begin{array}{c|c} A_1 & 0 \\ \hline B_1 & B_2 \\ \hline 0 & A_2 \end{array}\right) \in \mathbb{Z}_m^{k\times n} \quad \Longleftrightarrow \quad I(\mathcal{C}) = I(\mathcal{C}_1) + I(\mathcal{C}_2) + \left\langle \left\{ \mathbf{X}^{\alpha_i} - \mathbf{Y}^{\beta_i} \right\}_{i=1,2,3} \right\rangle$$

with $\operatorname{rank}(B_i) = 2$

$$G_1 = \left(\begin{array}{c|c} A_1 & 0 \\ \hline B_1 & *_1 I_m \end{array}\right) \quad \text{and} \quad G_2 = \left(\begin{array}{c|c} *_2 I_m & B_2 \\ \hline 0 & A_2 \end{array}\right)$$

with $*_1 + *_2 = 0$.

4 LINEAR CODES

- Applications to other classes of codes

➜ Throughout this section $\mathcal{C}$ will be **an $[n, k]$ linear code** in $\mathbb{F}_q^n$, i.e. a k-dimensional linear subspace of $\mathbb{F}_q^n$.

➜ This section essentially follows:

M. Borges-Quintana, M.A. Borges-Trenard, I. Márquez-Corbella and E. Martínez-Moro, *An Algebraic View to Gradient Descend Decoding for an arbitrary linear code*, Submitted

I. Márquez-Corbella, E. Martínez-Moro and E. Suárez-Canedo *On the ideal associated to any linear code*, Submitted.

➜ Which are joint works:

- M. Borges-Quintana (University of Oriente - Santiago de Cuba).
- M.A. Borges-Trenard (University of Oriente - Santiago de Cuba).
- E. Martínez-Moro (University of Valladolid - Spain).
- E. Suárez-Canedo (University of Valladolid - Spain).

DECODING LINEAR CODES

➜ Let α be a **primitive element** of $\mathbb{F}_q^*$.

Characteristic crossing functions:

$$\nabla : \{0,1\}^{q-1} \longrightarrow \mathbb{F}_q \quad \text{and} \quad \Delta : \mathbb{Z}_q \longrightarrow \{0,1\}^{q-1} .$$

- The map Δ replace $\begin{cases} \text{the element } \mathbf{a} = \alpha^j \in \mathbb{F}_q^* \text{ by the unit vector } \mathbf{e}_j \in \mathbb{Z}^{m-1} \\ \text{and } 0 \text{ by the zero vector } \mathbf{0} \in \mathbb{Z}^{q-1}. \end{cases}$
- The map ∇ recovers the element $j_1\alpha + j_2\alpha^2 + \ldots + j_{q-1}$ from the binary vector $(j_1, \ldots, j_{q-1})$.

➜ Let $\mathbf{X}$ denotes n vector variables $X_1, \ldots, X_n$

➜ Each variable X_i is decomposed into $q-1$ components: $x_{i1} \cdots x_{iq-1}$

➜ Let $\mathbf{a} \in \mathbb{F}_q^n$ we adopt the following notation:

$$\begin{aligned} \mathbf{X}^{\mathbf{a}} &= X_1^{a_1} \cdot X_2^{a_2} \cdots X_n^{a_n} \\ &= \left(x_{11} \cdots x_{1q-1}\right)^{\Delta a_1} \cdot \left(x_{21} \cdots x_{2q-1}\right)^{\Delta a_2} \cdots \left(x_{n1} \cdots x_{nq-1}\right)^{\Delta a_n} \end{aligned}$$

Key idea: For all $\mathbf{a} \in \mathbb{F}_q^n$: $\deg\left(\mathbf{X}^{\mathbf{a}}\right) = \mathrm{w}_H(\mathbf{a})$.
Weight compatible ordering on $\mathbb{F}_q^n$ = Total degree ordering on $\mathbb{K}[\mathbf{X}]$

Decoding Linear Codes

Theorem: Ideal Associated to $\mathcal{C}$

Given the rows of a generator matrix of $\mathcal{C}$, labelled by $\mathbf{w}_1, \ldots, \mathbf{w}_k$. The following ideal match the ideal $I(\mathcal{C})$:

$$I_+(\mathcal{C}) = \left\langle \left\{\mathbf{X}^{\alpha^j \mathbf{w}_i} - 1\right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}} \bigcup \left\{\mathcal{R}_{X_i}(T_+)\right\}_{i=1,\ldots,n} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]$$

where $\mathcal{R}_{X_i}(T_+)$ consist of all the binomials on the variable X_i associated to the relations given by the additive table of the field $\mathbb{F}_q = \langle \alpha \rangle$, i.e.

$$\mathcal{R}_{X_i}(T_+) = \left\{ \begin{array}{c} \{x_{iu}x_{iv} - x_{iw} \mid \alpha^u + \alpha^v = \alpha^w\} \\ \{x_{iu}x_{iv} - 1 \mid \alpha^u + \alpha^v = 0\} \end{array} \right\}$$

Moreover:

1. We compute a Gröbner representation of $\mathcal{C}$.
2. We show that the binomials involved in the reduced Gröbner basis of $I_+(\mathcal{C})$ w.r.t. a degree compatible ordering define a test-set for $\mathcal{C}$.
3. We define two gradient descent decoding algorithms.
4. We discuss an alternative for the computation of the Gröbner basis of $I_+(\mathcal{C})$.
5. We compute the set of codewords of minimal support of $\mathcal{C}$.

Decoding Linear Codes

Theorem: Ideal Associated to $\mathcal{C}$

Given the rows of a generator matrix of $\mathcal{C}$, labelled by $\mathbf{w}_1, \ldots, \mathbf{w}_k$. The following ideal match the ideal $I(\mathcal{C})$:

$$I_+(\mathcal{C}) = \left\langle \left\{ \mathbf{X}^{\alpha^j \mathbf{w}_i} - 1 \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}} \bigcup \left\{ \mathcal{R}_{X_i}(T_+) \right\}_{i=1,\ldots,n} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]$$

where $\mathcal{R}_{X_i}(T_+)$ consist of all the binomials on the variable X_i associated to the relations given by the additive table of the field $\mathbb{F}_q = \langle \alpha \rangle$, i.e.

$$\mathcal{R}_{X_i}(T_+) = \left\{ \begin{array}{c} \{x_{iu}x_{iv} - x_{iw} \mid \alpha^u + \alpha^v = \alpha^w\} \\ \{x_{iu}x_{iv} - 1 \mid \alpha^u + \alpha^v = 0\} \end{array} \right\}$$

Moreover:

1. We compute a Gröbner representation of $\mathcal{C}$.
2. We show that the binomials involved in the reduced Gröbner basis of $I_+(\mathcal{C})$ w.r.t. a degree compatible ordering define a test-set for $\mathcal{C}$.
3. We define two gradient descent decoding algorithms.
4. We discuss an alternative for the computation of the Gröbner basis of $I_+(\mathcal{C})$.
5. We compute the set of codewords of minimal support of $\mathcal{C}$.

Decoding Linear Codes

Theorem: Ideal Associated to $\mathcal{C}$

Given the rows of a generator matrix of $\mathcal{C}$, labelled by $\mathbf{w}_1, \ldots, \mathbf{w}_k$. The following ideal match the ideal $I(\mathcal{C})$:

$$I_+(\mathcal{C}) = \left\langle \left\{ \mathbf{X}^{\alpha^j \mathbf{w}_i} - 1 \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}} \bigcup \left\{ \mathcal{R}_{X_i}(T_+) \right\}_{i=1,\ldots,n} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]$$

where $\mathcal{R}_{X_i}(T_+)$ consist of all the binomials on the variable X_i associated to the relations given by the additive table of the field $\mathbb{F}_q = \langle \alpha \rangle$, i.e.

$$\mathcal{R}_{X_i}(T_+) = \left\{ \begin{array}{c} \{x_{iu}x_{iv} - x_{iw} \mid \alpha^u + \alpha^v = \alpha^w\} \\ \{x_{iu}x_{iv} - 1 \mid \alpha^u + \alpha^v = 0\} \end{array} \right\}$$

Moreover:

1. We compute a Gröbner representation of $\mathcal{C}$.
2. We show that the binomials involved in the reduced Gröbner basis of $I_+(\mathcal{C})$ w.r.t. a degree compatible ordering define a test-set for $\mathcal{C}$.
3. We define two gradient descent decoding algorithms.
4. We discuss an alternative for the computation of the Gröbner basis of $I_+(\mathcal{C})$.
5. We compute the set of codewords of minimal support of $\mathcal{C}$.

DECODING LINEAR CODES

THEOREM: IDEAL ASSOCIATED TO $\mathcal{C}$

Given the rows of a generator matrix of $\mathcal{C}$, labelled by $\mathbf{w}_1, \ldots, \mathbf{w}_k$. The following ideal match the ideal $I(\mathcal{C})$:

$$I_+(\mathcal{C}) = \left\langle \left\{ \mathbf{X}^{\alpha^j \mathbf{w}_i} - 1 \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}} \bigcup \left\{ \mathcal{R}_{X_i}(T_+) \right\}_{i=1,\ldots,n} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]$$

where $\mathcal{R}_{X_i}(T_+)$ consist of all the binomials on the variable X_i associated to the relations given by the additive table of the field $\mathbb{F}_q = \langle \alpha \rangle$, i.e.

$$\mathcal{R}_{X_i}(T_+) = \left\{ \begin{array}{c} \{x_{iu}x_{iv} - x_{iw} \mid \alpha^u + \alpha^v = \alpha^w\} \\ \{x_{iu}x_{iv} - 1 \mid \alpha^u + \alpha^v = 0\} \end{array} \right\}$$

Moreover:

1. We compute a Gröbner representation of $\mathcal{C}$.
2. We show that the binomials involved in the reduced Gröbner basis of $I_+(\mathcal{C})$ w.r.t. a degree compatible ordering define a test-set for $\mathcal{C}$.
3. We define two gradient descent decoding algorithms.
4. We discuss an alternative for the computation of the Gröbner basis of $I_+(\mathcal{C})$.
5. We compute the set of codewords of minimal support of $\mathcal{C}$.

DECODING LINEAR CODES

THEOREM: IDEAL ASSOCIATED TO $\mathcal{C}$

Given the rows of a generator matrix of $\mathcal{C}$, labelled by $\mathbf{w}_1, \ldots, \mathbf{w}_k$. The following ideal match the ideal $I(\mathcal{C})$:

$$I_+(\mathcal{C}) = \left\langle \left\{ \mathbf{X}^{\alpha^j \mathbf{w}_i} - 1 \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}} \bigcup \left\{ \mathcal{R}_{X_i}(T_+) \right\}_{i=1,\ldots,n} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]$$

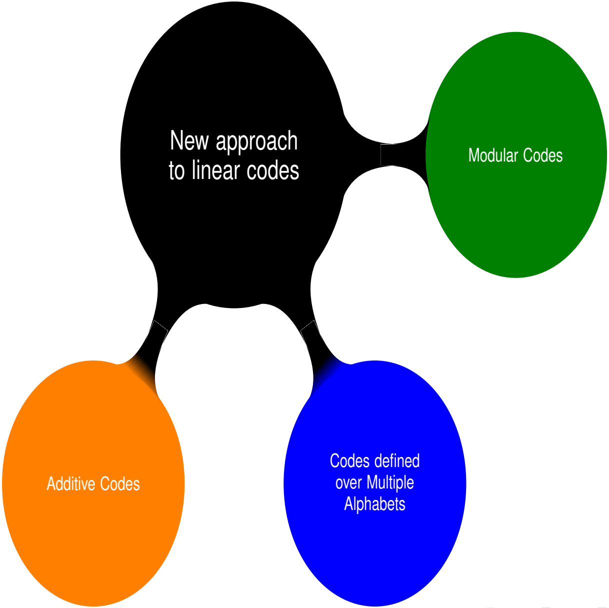
where $\mathcal{R}_{X_i}(T_+)$ consist of all the binomials on the variable X_i associated to the relations given by the additive table of the field $\mathbb{F}_q = \langle \alpha \rangle$, i.e.

$$\mathcal{R}_{X_i}(T_+) = \left\{ \begin{array}{c} \{x_{iu}x_{iv} - x_{iw} \mid \alpha^u + \alpha^v = \alpha^w\} \\ \{x_{iu}x_{iv} - 1 \mid \alpha^u + \alpha^v = 0\} \end{array} \right\}$$

Moreover:

1. We compute a Gröbner representation of $\mathcal{C}$.
2. We show that the binomials involved in the reduced Gröbner basis of $I_+(\mathcal{C})$ w.r.t. a degree compatible ordering define a test-set for $\mathcal{C}$.
3. We define two gradient descent decoding algorithms.
4. We discuss an alternative for the computation of the Gröbner basis of $I_+(\mathcal{C})$.
5. We compute the set of codewords of minimal support of $\mathcal{C}$.

Applications to other classes of codes



MODULAR CODES

➜ *Let $\mathcal{C}$ be an $[n, k]$ modular code defined over $\mathbb{Z}_m$*

Characteristic crossing functions:

$$\nabla_m : \{0,1\}^{m-1} \longrightarrow \mathbb{Z}_m \quad \text{and} \quad \underline{\Delta_m} : \mathbb{Z}_m \longrightarrow \{0,1\}^{m-1}.$$

- The map $\underline{\Delta_m}$ replace $\begin{cases} \text{the element } j \in \mathbb{Z}_m \setminus \{0\} \text{ by the unit vector } \mathbf{e}_j \in \mathbb{Z}^{m-1} \\ \text{and } 0 \text{ by the zero vector } \mathbf{0} \in \mathbb{Z}^{m-1}. \end{cases}$
- The map $\overline{\nabla_m}$ recovers the element $j_1 + 2j_2 + \ldots + (m-1)j_{m-1}$ from the binary vector $(j_1, \ldots, j_{m-1})$.

➜ Let $\mathbf{X}$ denotes n vector variables $X_1, \ldots, X_n$

➜ Each variable X_i is decomposed into $m-1$ components: $x_{i1} \cdots x_{im-1}$

➜ Let $\mathbf{a} \in \mathbb{Z}_m^n$ we adopt the following notation:

$$\begin{aligned} \mathbf{X}^{\mathbf{a}} &= X_1^{a_1} \cdot X_2^{a_2} \cdots X_n^{a_n} \\ &= (x_{11} \cdots x_{1m-1})^{\Delta a_1} \cdot (x_{21} \cdots x_{2m-1})^{\Delta a_2} \cdots (x_{n1} \cdots x_{nm-1})^{\Delta a_n} \end{aligned}$$

Ideal associated to $\mathcal{C}$:

$$I_+(\mathcal{C}) = \left\langle \left\{ \mathbf{X}^{\mathbf{g}_i} - 1 \right\}_{i=1,\ldots,k} \cup \left\{ \mathcal{R}_{X_i}(T_+) \right\}_{i=1,\ldots,n} \right\rangle$$

where $\mathcal{R}_{X_i}(T_+)$ consists of all binomials on the vector variable X_i associated to the relations given by the additive table of $\mathbb{Z}_m$

Multiple Alphabets

➜ *Let $\mathcal{C}$ be an $[n,k]$ modular code defined over* $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$

Characteristic crossing functions:

$$\nabla_m : \{0,1\}^{m-1} \longrightarrow \mathbb{Z}_m \quad \text{and} \quad \Delta_m : \mathbb{Z}_m \longrightarrow \{0,1\}^{m-1}.$$

- The map Δ_m replace $\begin{cases} \text{the element } j \in \mathbb{Z}_m \setminus \{0\} \text{ by the unit vector } \mathbf{e}_j \in \mathbb{Z}^{m-1} \\ \text{and } 0 \text{ by the zero vector } \mathbf{0} \in \mathbb{Z}^{m-1}. \end{cases}$
- The map ∇_m recovers the element $j_1 + 2j_2 + \ldots + (m-1)j_{m-1}$ from the binary vector $(j_1, \ldots, j_{m-1})$.

➜ Let $\mathbf{X}$ denotes n vector variables $X_1, \ldots, X_n$

➜ Each variable X_i is decomposed into $m_i - 1$ components: $x_{i1} \cdots x_{im_i-1}$

➜ Let $\mathbf{a} \in \mathbb{Z}_m^n$ we adopt the following notation:

$$\begin{aligned} \mathbf{X}^{\mathbf{a}} &= X_1^{a_1} \cdot X_2^{a_2} \cdots X_n^{a_n} \\ &= \left(x_{11} \cdots x_{1m_1-1}\right)^{\Delta a_1} \cdot \left(x_{21} \cdots x_{2m_2-1}\right)^{\Delta a_2} \cdots \left(x_{n1} \cdots x_{nm_n-1}\right)^{\Delta a_n} \end{aligned}$$

Ideal associated to $\mathcal{C}$:

$$I_+(\mathcal{C}) = \left\langle \left\{ \mathbf{x}^{\mathbf{g}_i} - 1 \right\}_{i=1,\ldots,k} \cup \left\{ \mathcal{R}_{X_i}(T_+) \right\}_{i=1,\ldots,n} \right\rangle$$

$\Rightarrow \mathcal{R}_{X_i}(T_+)$ could be different for each i

where $\mathcal{R}_{X_i}(T_+)$ consists of all binomials on the vector variable X_i associated to the relations given by the additive table of $\mathbb{Z}_m$

Additive codes

- Given the rows of a generator matrix of $\mathcal{C}$ labelled by $\{\mathbf{g}_1, \ldots, \mathbf{g}_k\} \subseteq \mathbb{F}_{q_1}$. The set of codewords of $\mathcal{C}$ are defined as:

$$\left\{\alpha_1 \mathbf{g}_1 + \ldots + \alpha_k \mathbf{g}_k \mid \alpha_i \in \mathbb{F}_{q_2} \text{ for } i = 1, \ldots, k\right\}$$

- Let α be a primitive element of $\mathbb{F}_{q_2}$.

Ideal associated to $\mathcal{C}$:

$$I_+(\mathcal{C}) = \left\langle \left\{ \mathbf{X}^{\alpha^j \mathbf{g}_i} - 1 \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots q_2-1}} \cup \left\{ \mathcal{R}_{X_i}(T_+) \right\}_{i=1,\ldots,n} \right\rangle$$

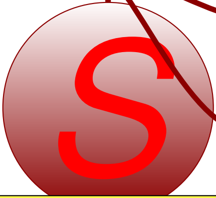
where $\mathcal{R}_{X_i}(T_+)$ consists of all binomials on the vector variable X_i associated to the relations given by the additive table of $\mathbb{Z}_{q_1}$

Introduction to Semigroups

S is assumed to be **finitely generated**

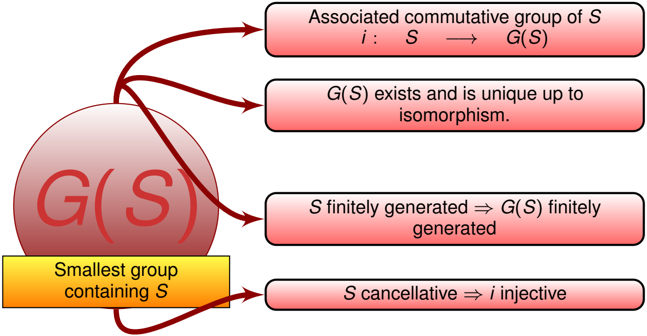
S is **cancellative** $\Rightarrow \mathbf{m}+\mathbf{n}=\mathbf{m}+\mathbf{n}'$ with $\mathbf{m},\mathbf{n},\mathbf{n}' \in S$ then $\mathbf{n}=\mathbf{n}'$.

S is **combinatorially finite** $\Rightarrow$ exists finitely many ways to write every $\mathbf{a} \in S \setminus \{\mathbf{0}\}$ as a sum $\mathbf{a} = \mathbf{a}_1 + \ldots + \mathbf{a}_s$ with $\mathbf{a}_i \in S \setminus \{\mathbf{0}\}$.



Commutative semigroup with an identity element

Introduction to Semigroups



Semigroup Algebra

- The choice of a system of generators $\{\mathbf{n}_1, \ldots, \mathbf{n}_r\}$ of S induces a natural semigroup morphism

$$\begin{array}{cccc} \pi: & \mathbb{N}^r & \longrightarrow & S \\ & \mathbf{e}_i & \longmapsto & \mathbf{n}_i \\ & \mathbf{a} & \longmapsto & \sum_{i=1}^r a_i \mathbf{n}_i \end{array}$$

- **Semigroup algebra of S:** We write $\mathbb{K}[S]$ for the $\mathbb{K}$-vector space:

$$\mathbb{K}[S] = \left\{ \sum_{\mathbf{n} \in S} a_{\mathbf{n}} \mathbf{t}^{\mathbf{n}} \mid a_{\mathbf{n}} \in \mathbb{K} \right\}$$

endowed with a multiplication which is $\mathbb{K}$-linear and satisfies that $\mathbf{t}^{\mathbf{a}} \cdot \mathbf{t}^{\mathbf{b}} = \mathbf{t}^{\mathbf{a}+\mathbf{b}}$ with $\mathbf{a}, \mathbf{b} \in S$.

- π defines a $\mathbb{K}$-algebra morphism:

$$\begin{array}{cccc} \varphi: & \mathbb{K}[\mathbf{X}] & \longrightarrow & \mathbb{K}[S] \\ & X_i & \longmapsto & \mathbf{t}^{\mathbf{n}_i} \end{array}$$

- **Semigroup ideal associated to S:** $I(S) = \ker(\varphi)$, i.e.

$$I(S) = \left\langle \left\{ \mathbf{X}^{\mathbf{a}} - \mathbf{X}^{\mathbf{b}} \mid \sum_{i=1}^r a_i \mathbf{n}_i = \sum_{i=1}^r b_i \mathbf{n}_i \text{ with } \mathbf{a}, \mathbf{b} \in \mathbb{N}^r \right\} \right\rangle .$$

Lattices

- We describe the **lattice** $\mathcal{L}$ as

$$\mathcal{L} = \left\{ \mathbf{u} \in \mathbb{Z}^r \mid \sum_{i=1}^{r} u_i \mathbf{n}_i = \mathbf{0} \right\} \subseteq \mathbb{Z}^r.$$

  i.e. set of integer solutions of the system $A\mathbf{X} = \mathbf{0}$ where $A = \{\mathbf{n}_1, \ldots, \mathbf{n}_r\}$ is a fix system of generators of S

- Given a lattice $\mathcal{L} \subset \mathbb{Z}^r$, the binomial ideal

$$I_{\mathcal{L}} = \left\langle \left\{ \mathbf{X}^{\mathbf{a}} - \mathbf{X}^{\mathbf{b}} \mid \mathbf{a} - \mathbf{b} \in \mathcal{L} \right\} \right\rangle$$

  is called the **lattice ideal associated to $\mathcal{L}$**.

- If $I_{\mathcal{L}} = I(S)$, then we have an **exact sequence** of abelian groups given by:

$$0 \longrightarrow \mathcal{L} \longrightarrow G(\mathbb{N}^r) = \mathbb{Z}^r \longrightarrow G(S) \longrightarrow 0.$$

The semigroup associated with a modular code

Characteristic crossing functions:

$$\blacktriangledown : \quad \mathbb{Z}^s \longrightarrow \mathbb{Z}_m^s \qquad \text{and} \qquad \blacktriangle : \quad \mathbb{Z}_m^s \longrightarrow \mathbb{Z}^s$$

- The map $\blacktriangledown$ is reduction modulo m.
- The map $\blacktriangle$ replace the class of $0, 1, \ldots, m-1$ by the same symbols regarded as integers.

➜ Let $\mathcal{C}$ be an $[n, k]$ **modular** code over $\mathbb{Z}_m$ with generator and parity check matrices:

$$G = \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & \ddots & \vdots \\ \boxed{g_{i1} \quad \cdots \quad g_{in}} \\ \vdots & \ddots & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix} \in \mathbb{Z}_m^{k \times n} \qquad H = \begin{pmatrix} h_{11} & \cdots & h_{1i} & \cdots & h_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ h_{l1} & \cdots & h_{li} & \cdots & h_{ln} \end{pmatrix} \in \mathbb{Z}_m^{l \times n}$$

$\mathbf{g}_i \qquad \mathbf{h}_i$

Ideal associated to $\mathcal{C}$:

$$I_m(\mathcal{C}) = \left\langle \left\{ \mathbf{X}^{\mathbf{g}_i} - 1 \right\}_{i=1,\ldots,k} \cup \left\{ X_j^m - 1 \right\} \right\rangle$$

➜ Provides $\mathcal{M}_{\mathcal{C}}$.

➜ Does not allow Complete Decoding.

Proposition:

Consider the semigroup S generated by $\{\mathbf{h}_i\}_{i=1,\ldots,n}$ then

$$I_m(\mathcal{C}) = I(S)$$

The semigroup associated with a modular code

Proposition:

Let $\mathcal{C}$ be an $[n,k]$ modular code over $\mathbb{Z}_m$ and $H \in \mathbb{Z}_m^{(n-k)\times n}$ be a parity check matrix of $\mathcal{C}$. Consider the commutative semigroup S finitely generated by $\{\mathbf{h}_i\}_{i=1,\ldots,n}$ where $\mathbf{h}_j$ denotes the j-th column of H. Then:

1. $I(S) = I_m(\mathcal{C})$.
2. S in not combinatorially finite.
3. $S = G(S) \subseteq \mathbb{Z}_m^{n-k}$, i.e. $S = -S$.
4. $G(S)$ is a torsion group since $m\mathbf{a} \equiv \mathbf{0} \mod m, \ \forall \mathbf{a} \in S$.
5. The lattice $\mathcal{L}_1 = \left\{ \mathbf{u} \in \mathbb{Z}^n \mid \sum_{i=1}^n u_i \mathbf{h}_i \equiv 0 \mod m \right\}$ is the set $\blacktriangle\mathcal{C} + (m\mathbb{Z}^n)$.

   Then $I_m(\mathcal{C}) = I_{\mathcal{L}_1}$ and we have the following exact sequence of abelian groups:

$$\boxed{0 \longrightarrow \mathcal{L}_1 \longrightarrow G(\mathbb{N}^n) = \mathbb{Z}^n \longrightarrow G(S) = S \longrightarrow 0}$$

ANOTHER REPRESENTATION FOR MODULAR CODES

Characteristic crossing functions:

$$\nabla : \{0,1\}^{m-1} \longrightarrow \mathbb{Z}_m \quad \text{and} \quad \Delta : \mathbb{Z}_m \longrightarrow \{0,1\}^{m-1}.$$

- The map Δ replace $\begin{cases} \text{the element } j \in \mathbb{Z}_m \setminus \{0\} \text{ by the unit vector } \mathbf{e}_j \in \mathbb{Z}^{m-1} \\ \text{and 0 by the zero vector } \mathbf{0} \in \mathbb{Z}^{m-1}. \end{cases}$
- The map ∇ recovers the element $j_1 + 2j_2 + \ldots + (m-1)j_{m-1}$ from the binary vector $(j_1, \ldots, j_{m-1})$.

➜ Let $\mathbf{X}$ denotes n vector variables $X_1, \ldots, X_n$

➜ Each variable X_i is decomposed into $m-1$ components: $x_{i1} \cdots x_{im-1}$

➜ Let $\mathbf{a} \in \mathbb{Z}_m^n$ we adopt the following notation:

$$\begin{aligned} \mathbf{X}^{\mathbf{a}} &= X_1^{a_1} \cdot X_2^{a_2} \cdots X_n^{a_n} \\ &= (x_{11} \cdots x_{1m-1})^{\Delta a_1} \cdot (x_{21} \cdots x_{2m-1})^{\Delta a_2} \cdots (x_{n1} \cdots x_{nm-1})^{\Delta a_n} \end{aligned}$$

Ideal associated to $\mathcal{C}$:

$$I_+(\mathcal{C}) = \left\langle \left\{ \mathbf{x}^{\mathbf{g}_i} - 1 \right\}_{i=1,\ldots,k} \cup \left\{ \mathcal{R}_{X_i}(T_+) \right\}_{i=1,\ldots,n} \right\rangle$$

where $\mathcal{R}_{X_i}(T_+)$ consists of all binomials on the vector variable X_i associated to the relations given by the additive table of $\mathbb{Z}_m$

PROPOSITION:

Consider the semigroup S generated by $\{j\mathbf{h}_i\}_{\substack{i=1,\ldots n \\ j=1,\ldots,m-1}}$ then

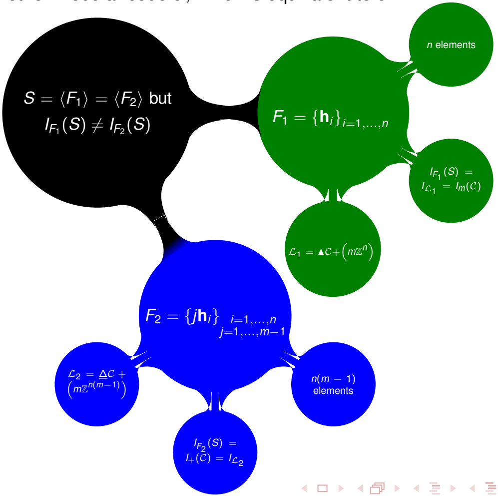
$$I_+(\mathcal{C}) = I(S)$$

➜ Provides $\mathcal{M}_{\mathcal{C}}$.

➜ Allows Complete Decoding.

The semigroup associated with a modular code

- Let $H \in \mathbb{Z}_m^{(n-k)\times n}$ be a parity check matrix of $\mathcal{C}$ whose columns are $\{\mathbf{h}_i\}_{i=1,\ldots,n}$.
  1. Row operations on H yields to a new set $\hat{F}$: $S = \left\langle \hat{F} \right\rangle$
  2. Column operations on H gives the same semigroup S but associated with another modular code $\hat{\mathcal{C}}$, which is equivalent to $\mathcal{C}$.



The semigroup associated with a linear code

Characteristic crossing functions:

$$\nabla : \quad \{0,1\}^{q-1} \longrightarrow \mathbb{F}_q \quad \text{and} \quad \Delta : \quad \mathbb{Z}_q \longrightarrow \{0,1\}^{q-1} \, .$$

- The map Δ replace $\begin{cases} \text{the element } \mathbf{a} = \alpha^j \in \mathbb{F}_q^* \text{ by the unit vector } \mathbf{e}_j \in \mathbb{Z}^{m-1} \\ \text{and } 0 \text{ by the zero vector } \mathbf{0} \in \mathbb{Z}^{q-1}. \end{cases}$
- The map $\overline{\nabla}$ recovers the element $j_1\alpha + j_2\alpha^2 + \ldots + j_{q-1}$ from the binary vector $(j_1, \ldots, j_{q-1})$.

➜ Let $\mathbf{X}$ denotes n vector variables $X_1, \ldots, X_n$

➜ Each variable X_i is decomposed into $q-1$ components: $x_{i1} \cdots x_{iq-1}$

➜ Let $\mathbf{a} \in \mathbb{F}_q^n$ we adopt the following notation:

$$\begin{aligned} \mathbf{X}^{\mathbf{a}} &= X_1^{a_1} \cdot X_2^{a_2} \cdots X_n^{a_n} \\ &= \left(x_{11} \cdots x_{1q-1}\right)^{\Delta a_1} \cdot \left(x_{21} \cdots x_{2q-1}\right)^{\Delta a_2} \cdots \left(x_{n1} \cdots x_{nq-1}\right)^{\Delta a_n} \end{aligned}$$

Ideal associated to $\mathcal{C}$:

$$I_+(\mathcal{C}) = \left\langle \left\{ \mathbf{X}^{\alpha^j \mathbf{g}_i} - 1 \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}} \cup \left\{ \mathcal{R}_{X_i}(T_+) \right\}_{i=1,\ldots,n} \right\rangle$$

where $\mathcal{R}_{X_i}(T_+)$ consists of all binomials on the vector variable X_i associated to the relations given by the additive table of $\mathbb{F}_m$

➜ Provides $\mathcal{M}_{\mathcal{C}}$.

➜ Allows Complete Decoding.

Proposition:

Consider the semigroup S generated by $\left\{\alpha^j \mathbf{h}_i\right\}_{\substack{i=1,\ldots,n \\ j=1,\ldots,q-1}}$ then

$$I_+(\mathcal{C}) = I(S)$$

THE SEMIGROUP ASSOCIATED WITH A LINEAR CODE

PROPOSITION:

Let $\mathcal{C}$ be an $[n,k]$ code over $\mathbb{F}_q$ and $H \in \mathbb{F}_q^{(n-k)\times n}$ be a parity check matrix of $\mathcal{C}$. Consider the commutative semigroup S finitely generated by $\left\{\alpha^j \mathbf{h}_i\right\}_{\substack{i=1,\ldots,n \\ j=1,\ldots,q-1}}$ where $\mathbf{h}_j$ denotes the j-th column of H. Then:

1. $I(S) = I_+(\mathcal{C})$.
2. S in not combinatorially finite.
3. $S = G(S) = \mathbb{F}_q^{n-k}$, i.e. $S = -S$.
4. $G(S)$ is a torsion group since $p\mathbf{a} = 0$ in $\mathbb{F}_q$, $q = p^r$ $\forall \mathbf{a} \in S$.
5. The lattice $\mathcal{L}_2 = \left\{ \mathbf{u} \in \mathbb{Z}^{n(q-1)} \mid \sum_{i=1}^{n} \sum_{j=1}^{q-1} u_{ij}\alpha^j \mathbf{h}_i = 0 \text{ in } \mathbb{F}_q \right\}$ is the set $\Delta\mathcal{C} + \left(p\mathbb{Z}^{n(q-1)}\right)$.

   Then $I_m(\mathcal{C}) = I_{\mathcal{L}_2}$ and we have the following exact sequence of abelian groups:

$$\boxed{0 \longrightarrow \mathcal{L}_2 \longrightarrow G\left(\mathbb{N}^{n(q-1)}\right) = \mathbb{Z}^{n(q-1)} \longrightarrow G(S) = S = \mathbb{F}_q^{n-k} \longrightarrow 0.}$$

Another representation for linear codes

- Consider $\mathbb{F}_q$ with $q = p^s$.
- Let $f(X)$ be any irreducible polynomial of degree s over $\mathbb{F}_p$ and β any root of $f(X)$.

Characteristic crossing functions:

$$\blacktriangledown : \mathbb{Z}^s \longrightarrow \mathbb{F}_q \quad \text{and} \quad \blacktriangle : \mathbb{F}_q \longrightarrow \mathbb{Z}^s$$

- The map $\blacktriangle$ replaces the class of the elements $\mathbf{a} = a_0 + a_1\beta + \ldots + a_{s-1}\beta^{s-1} \in \mathbb{F}_q$ with $\left(a_0, \ldots, a_{s-1}\right) \in \mathbb{F}_p^s$ by the vector $\blacktriangle\left(a_0, \ldots, a_{s-1}\right) \in \mathbb{Z}^s$.
- $\blacktriangledown$ recovers the element $\blacktriangledown a_0 + \blacktriangledown a_1\beta + \ldots + \blacktriangledown a_{s-1}\beta^{s-1}$ from the integer vector $\left(a_0, \ldots, a_{s-1}\right)$.

- Let $\mathbf{Y}$ denotes n vector variables $Y_1, \ldots, Y_n$
- Each variable Y_i is decomposed into s components: $y_{i1} \cdots y_{is}$
- Let $\mathbf{a} \in \mathbb{F}_q^n$ we adopt the following notation:

$$\mathbf{Y}^{\mathbf{a}} = Y_1^{a_1} \cdots Y_n^{a_n} = (y_{11} \cdots y_{1s})^{\blacktriangle a_1} \cdots (y_{n1} \cdots y_{ns})^{\blacktriangle a_n}$$

Ideal associated to $\mathcal{C}$:

$$I_m(\mathcal{C}) = \left\langle \left\{ \mathbf{Y}^{\mathbf{g}_i} - 1 \right\}_{i=1,\ldots,k} \cup \left\{ y_{ij}^p - 1 \right\}_{\substack{i=1,\ldots,n \\ j=1,\ldots,s}} \right\rangle$$

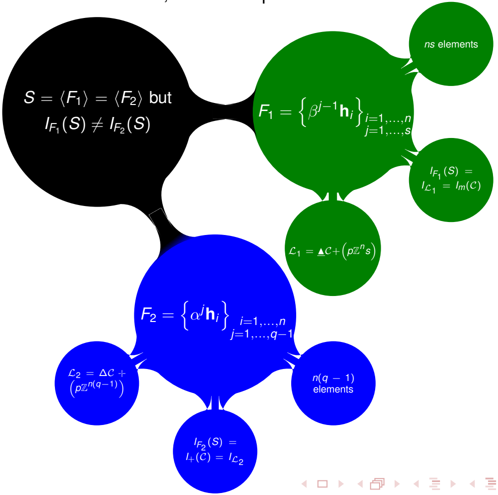
Proposition:

Consider the semigroup S generated by $\left\{ \beta^{j-1}\mathbf{h}_i \right\}_{\substack{i=1,\ldots,n \\ j=1,\ldots,s}}$ then

$$I_m(\mathcal{C}) = I(S)$$

THE SEMIGROUP ASSOCIATED WITH A LINEAR CODE

- Let $H \in \mathbb{F}_q^{(n-k)\times n}$ be a parity check matrix of $\mathcal{C}$ whose columns are $\{\mathbf{h}_i\}_{i=1,\ldots,n}$.
  1. Row operations on H yields to a new set $\hat{F} : S = \langle \hat{F} \rangle$
  2. Column operations on H gives the same semigroup S but associated with another linear code $\hat{\mathcal{C}}$, which is equivalent to $\mathcal{C}$.



Conclusions

Digital Representation

The generating set $F = \{\mathbf{n}_1, \ldots, \mathbf{n}_r\}$ of a semigroup S is called a *digital representation* of S if every element $\mathbf{m} \in S$ can be written as

$$\sum_{i=1}^{r} a_i \mathbf{n}_i \text{ with } a_1, \ldots, a_r \in \{0,1\} \subseteq \mathbb{N}.$$

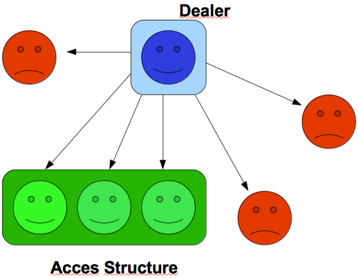
The choice of **digital representations** of S provides not only complete decoding algorithms but also the set of codewords of minimal support.

CRYPTOGRAPHY

From Greek: *Krypto* “hidden, secret”+ *Graphos* “writting”= “hidden writing”.

➜ Make unintelligible messages to potential adversaries.

Complete Decoding has applications in **secret sharing schemes**.



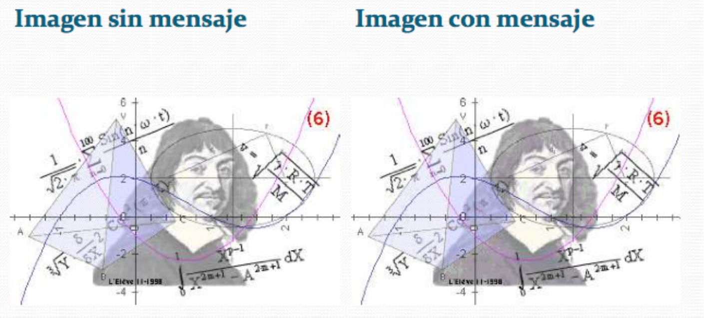
- ➜ Every linear code can be used to construct a secret sharing scheme.
- ➜ The set of codewords of minimal support describe completely the minimal access structure of these schemes.

STEGANOGRAPHY

ESTEGANOGRAFÍA

From Greek: *Steganos* “covered”+ *Graphos* “writing”.

➜ The hiding of information through a covert channel with the purpose of preventing the detection of a hidden message.



Thanks!!