Combinatorics of minimal support codewords

Irene MÁRQUEZ CORBELLA, Edgar MARTÍNEZ MORO
imarquez@agt.uva.es, edgar@maf.uva.es

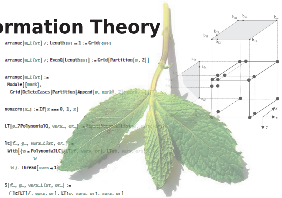
SINGACOM group
University of Valladolid, Spain
http://www.singacom.uva.es

16/04/2010

Soria Summer School on Computational Mathematics

Hosted by SINGACOM, Universidad de Valladolid
12-16 July 2010. Soria, Spain

Algebraic Geometric Modelling in Information Theory (AGMINT)



The research group **SINGACOM** of Valladolid University (Spain) is organizing an International School on Algebraic Geometric Modelling in Information Theory from 12 to 16 July 2010 in Soria, Spain.

The main aim of this school is to bring together specialists, researchers and students working on various aspects of Computer Algebra, Geometry, Information Theory and related areas and their applications.

The academic program consists of a school on topics of current interest taught by leading experts. Also, there will be afternoon working sessions where interested postgraduate students can show their work in progress.

Advance of the program

C1) Network coding
Olav Geil
Department of Mathematical Sciences, Aalborg University Denmark

C2) S-Boxes, APN Functions and Related Structures
Gary MacGuire
Claude Shannon Institute for Discrete Mathematics, Coding and Cryptography,Ireland

C3) SAGE: A basic overview for coding and cryptography
David Joyner
Mathematics Department. U. S. Naval Academy, USA

C4) Steganography from a coding theory point of view
Carlos Munuera
SINGACOM group, Universidad de Valladolid, Spain

C5) Semigroups, codes and privacy applications
Maria Bras-Amorós
Departament d'Enginyeria Informàtica i Matemàtiques
Universitat Rovira i Virgili, Spain

Participation: The school is open to all mathematicians interested in the topics covered. Postdocs, PhD students, Postgraduate (master) are encouraged to apply. The number of places is limited to 30 people.The application procedure and other

Directors of the school:

Antonio Campillo López (SINGACOM, UVa)
campillo@agt.uva.es

Edgar Martínez Moro (SINGACOM, UVa)
edgar@maf.uva.es

Local committee (SINGACOM):

Edgar Martínez Moro
University of Valladolid, edgar@maf.uva.es

Diego Ruano Benito
Aalborg University, diego@math.aau.dk

Fernando Hernando
University College Cork, F.Hernando@ucc.ie

Irene Márquez Corbella
University of Valladolid, iremarquez@gmail.com

Abstract

- **Complete Decoding** for binary linear codes can be regarded as an integer programming with binary arithmetic conditions.
- Conti and Traverso in [6] propose an algorithm which uses Gröbner bases to solve integer programming.
- Ikegami and Kaji in [12] extended this algorithm to solve integer programming with modulo arithmetic conditions.
- It is natural to consider for those problems the **Graver basis** associated to them which turn to be the set of minimal codewords in the binary case.
- **Interest of the set of minimal codewords:**
  - They had been related to gradient-like decoding algorithm.
  - They describe the minimal access structure in secret sharing schemes based on linear codes.

Overview

Linear programming problem

Linear programming problem

Let consider the matrix $A \in \mathbb{R}^{m \times n}$ and the vectors $\mathbf{b} \in \mathbb{R}^m$ and $\mathbf{w} \in \mathbb{R}^n$, we define $\mathrm{IP}_{A,\mathbf{w}}(\mathbf{b})$ as:

$$\mathrm{LP}_{A,\mathbf{w}}(\mathbf{b}) = \begin{cases} \text{minimize } & \mathbf{w} \cdot \mathbf{u} \\ \text{subject to } & \begin{cases} A\mathbf{u}^t = \mathbf{b} \\ \mathbf{u} \geq 0 \end{cases} \end{cases}$$

- A vector is **feasible** if it satisfies all the constraints.
- A feasible vector is **optimal** if its minimizes the objective function.
- The linear constraints define a convex polytope = **feasible region**.
- The most famous method for solving $\mathrm{LP}_{A,\mathbf{w}}(\mathbf{b})$ is the **simplex method**.

Integer linear programming

Integer linear programming problem

Let consider the matrix $A \in \mathbb{Z}^{m\times n}$ and the vectors $\mathbf{b} \in \mathbb{Z}^m$ and $\mathbf{w} \in \mathbb{R}^n$, we define $\mathrm{IP}_{A,\mathbf{w}}(\mathbf{b})$ as:

$$\mathrm{IP}_{A,\mathbf{w}}(\mathbf{b}) = \begin{cases} \text{minimize} & \mathbf{w}\cdot\mathbf{u} \\ \text{subject to} & \begin{cases} A\mathbf{u}^t = \mathbf{b} \\ \mathbf{u} \in \mathbb{Z}^n_{\geq 0} \end{cases} \end{cases}$$

- The general integer program is ***NP*-complete**.
- Specific methods to solve $\mathrm{IP}_{A,\mathbf{w}}(\mathbf{b})$:
  1. *Gomory's cutting plane method*
  2. *Branching and bounding methods*

Gröbner basis

Let $\mathbb{K}$ be a field and $\mathbb{K}[\mathbf{x}] := \mathbb{K}[x_1, \ldots, x_n]$ its ring of polynomials in n variables.
If $\mathbf{a} = (a_1, \ldots, a_n)$ we write $\mathbf{x}^{\mathbf{a}} = x_1^{a_1} \cdots x_n^{a_n}$.

Definition: Monomial ordering

A monomial ordering on the set of all the monomials in $\mathbb{K}[\mathbf{x}]$ is a total and well-ordering on $\mathbb{Z}^n_{\geq 0}$.
Example: *Lexicographical ordering*
It is such that $\mathbf{x}^{\mathbf{a}} >_{lex} \mathbf{x}^{\mathbf{b}}$ if $\mathbf{a} \neq \mathbf{b}$ and the first nonzero term in $(a_1 - b_1, \ldots, a_n - b_n)$ is positive.

Definition: Gröbner basis

Let $<$ be a monomial ordering on $\mathbb{K}[\mathbf{x}]$ and $\mathcal{I} \subset \mathbb{K}[\mathbf{x}]$ be an ideal.
A *Gröbner basis* of $\mathcal{I}$ is a finite set of generators $g_1, \ldots, g_m$ of $\mathcal{I}$ such that every leading monomial of a polynomial $p \in \mathcal{I}$ is a multiple of a leading monomial of a generator g_k.

Gröbner basis can be used to recover the solution or to eliminate unknowns in a system equation.

Theorem: Elimination property

Let $<$ be a monomial ordering on $\mathbb{K}[\mathbf{x}]$ with $x_1 < x_2 < \ldots < x_n$. Let $\mathcal{I}$ be an ideal and $\mathcal{G}$ a Gröbner basis of $\mathcal{I}$ for $<$.
$\forall i : 1 \leq i \leq n, \quad \mathcal{G} \cap \mathbb{K}[x_1, \ldots, x_i]$ is a Gröbner basis of the ideal $\mathcal{I} \cap \mathbb{K}[x_1, \ldots, x_i]$

Some Notation

- Every $\mathbf{u} \in \mathbb{Z}^n$ can be written uniquely as $\mathbf{u} = \mathbf{u}^+ - \mathbf{u}^-$ where $\mathbf{u}^+, \mathbf{u}^- \in \mathbb{N}^n$ and have disjoint supports.
- The **support of a vector u** $\in \mathbb{Z}^n$ is the set

$$\mathrm{supp}(\mathbf{u}) = \{i \ : \ u_i \neq 0\} \subseteq \{1, \ldots, n\}.$$

- The **normal form of a polynomial** f is the unique remainder obtained by dividing f with respect to the Gröbner basis $\mathcal{G}$ and is denoted by $\mathrm{nf}_{\mathcal{G}_{\succ_\mathbf{w}}}(f)$.
- We will use the following *characteristic crossing* functions :

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

where s is determined by context and the spaces may also be matrix spaces.

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

➜ Both maps act coordinate-wise.
➜ These maps will be used with matrices and vectors, themselves regarded as maps, acting on the right.

Conti-Traverso Algorithm

In [6] Conti and Traverso introduced a Gröbner basis based algorithm to solve $\mathrm{IP}_{A,\mathbf{w}}$.

Conti-Traverso algorithm

- **INPUT:** $A \in \mathbb{Z}^{m\times n}$, $\mathbf{b} \in \mathbb{Z}^m$ and $\mathbf{w} \in \mathbb{R}^n$.
- **OUTPUT:** An optimal solution of $\mathrm{IP}_{A,\mathbf{w}}(\mathbf{b})$.

1. Define an ideal I related with the constraint equations and a monomial order $\succ_{\mathbf{w}}$ induced by the cost vector.
2. Compute a Gröbner basis $\mathcal{G}$ of I with respect to $\succ_{\mathbf{w}}$.
3. For any non-optimal solution $\mathbf{u}$ of $\mathrm{IP}_{A,\mathbf{w}}(\mathbf{b})$, compute the normal form of the monomial $\mathbf{x}^{\mathbf{u}}$ by $\mathcal{G}$ with respect to $\succ_{\mathbf{w}}$, $\mathrm{nf}_{\mathcal{G}_{\succ_{\mathbf{w}}}}(\mathbf{x}^{\mathbf{u}}) = \mathbf{x}^{\mathbf{u}'}$
4. Return the exponent vector of the normal form, $\mathbf{u}'$

- The ideal I is the toric ideal $I = \langle \{\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \ : \ \mathbf{u} \in \ker_{\mathbb{Z}}(A)\}\rangle$.
- We define the term order $\succ_{\mathbf{w}}$ induced by the cost vector $\mathbf{w} \in \mathbb{Z}^n$ as:

$$\alpha \succ_{\mathbf{w}} \beta \Leftrightarrow \begin{cases} \text{either } \mathbf{w}\cdot\alpha \succ \mathbf{w}\cdot\beta \\ \text{or } \mathbf{w}\cdot\alpha = \mathbf{w}\cdot\beta, \quad \alpha \succ \beta, \text{ for } \succ \text{ a fixed ordering.} \end{cases}$$

Test-set

Test-set

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

- ➜ The binomials involved in the reduced Gröbner basis $\mathcal{G}_{\succ_\mathbf{w}}$ induce a (uniquely defined) test set for $\mathrm{IP}_{A,\mathbf{w}}$.
- ➜ The existence of a finite test-set $\mathcal{T}_{\succ_\mathbf{w}}$ gives a trivial gradient descent method for finding the optimal solution of the problem $\mathrm{IP}_{A,\mathbf{w}}(\mathbf{b})$

Ikegami-Kaji algorithm

Modular integer programming problem

Let consider the integer $q \geq 2$, the matrix $A \in \mathbb{Z}_q^{m\times n}$ and the vectors $\mathbf{b} \in \mathbb{Z}_q^m$ and $\mathbf{w} \in \mathbb{R}^n$ we define $\mathrm{IP}_{A,\mathbf{w},q}(\mathbf{b})$ as:

$$\mathrm{IP}_{A,\mathbf{w},q}(\mathbf{b}) = \begin{cases} \text{minimize} \quad \mathbf{w} \cdot \blacktriangle\mathbf{u} \\ \text{subject to} \quad \begin{cases} A\mathbf{u}^t \equiv \mathbf{b} \mod q \\ \mathbf{u} \in \mathbb{Z}_q^n \end{cases} \end{cases}$$

Extended Conti-Traverso algorithm

- **INPUT:** $A \in \mathbb{Z}_q^{m\times n}$, $\mathbf{b} \in \mathbb{Z}_q^m$, $\mathbf{w} \in \mathbb{R}^n$ and $q \in \mathbb{Z}_{\geq 2}$
- **OUTPUT:** An optimal solution of $\mathrm{IP}_{A,\mathbf{w},q}(\mathbf{b})$.

- Compute a Gröbner basis $\mathcal{G}$ of I_A with respect to an adapted monomial order $\succ_{\mathbf{w}}$.
- For any non-optimal solution $\mathbf{u}$ of $\mathrm{IP}_{A,\mathbf{w}}(\mathbf{b})$, compute the normal form of the monomial $\mathbf{x}^{\mathbf{u}}$ by $\mathcal{G}$ with respect to $\succ_{\mathbf{w}}$.
- Return the exponent vector of the normal form.

Ikegami-Kaji algorithm

In [12] Ikegami and Kaji adapted the ideas of the Conti-Traverso algorithm to solve the modular integer programming problem.

- The $\mathbb{Z}_q$-kernel of the matrix $A \in \mathbb{Z}_q^{m\times n}$ is given by the **elimination ideal** $I = I_A \cap \mathbb{K}[\mathbf{x}]$ where

$$I_A = \left\langle \{\phi_i - x_i\}_{i=1}^{n}, \{y_j^q - 1\}_{j=1}^{m} \right\rangle \subseteq \mathbb{K}[\mathbf{x},\mathbf{y}], \text{ and } \phi_i = \prod_{j=1}^{m} y_j^{a_{i,j}}.$$

  I.e. we can see the ideal related to the $\mathbb{Z}_q$-kernel of A as an elimination ideal of the $\mathbb{Z}$-kernel of the matrix $(\blacktriangle A, q\cdot I_m) \in \mathbb{Z}^{m\times(m+n)}$.

- A monomial order $\succ_{\mathbf{w}}$ on $\mathbb{K}[\mathbf{x},\mathbf{y}]$ **is adapted to the problem** $\mathrm{IP}_{A,\mathbf{w},q}(\mathbf{b})$ if it is an elimination order for $\mathbb{K}[\mathbf{x}]$ and it is compatible with $\mathbf{w}$, i.e. for any $\mathbf{u}$, $\mathbf{v} \in \mathbb{Z}_q^n$ such that

$$\mathbf{y}^{\blacktriangle(A\mathbf{u}^t)} \equiv \mathbf{y}^{\blacktriangle(A\mathbf{v}^t)} \mod \langle y_j^q - 1\rangle_{j=1}^{m}$$

  if $\mathbf{w}\cdot\mathbf{u} \succ \mathbf{w}\cdot\mathbf{v}$ then $\mathbf{x}^{\mathbf{u}} \succ_{\mathbf{w}} \mathbf{x}^{\mathbf{v}}$.

Consider $\mathcal{G}_{\succ_{\mathbf{w}}}$ a Gröbner basis of the ideal I_A w.r.t an adapted monomial order $\succ_{\mathbf{w}}$ then the Conti-Traverso algorithm is extended to the modular case as follows:

Theorem(Ikegami-Kaji, 2003)

Given the monomial $\mathbf{y}^{\blacktriangle\mathbf{b}}$ and let the normal form w.r.t $\mathcal{G}_{\succ_{\mathbf{w}}}$ be $\mathrm{nf}_{\mathcal{G}_{\succ_{\mathbf{w}}}}(\mathbf{y}^{\blacktriangle b}) = \mathbf{x}^{\mathbf{u}'}$, then $\blacktriangledown\mathbf{u}'$ will give an optimal solution of the problem $\mathrm{IP}_{A,\mathbf{w},q}(\mathbf{b})$.

➜ PROBLEMS

- There are $m \times n$ variables involved in the Gröbner basis computation, and the complexity of the Buchberger algorithm grows strongly in the number of variables.
- There is no an specific method for computing the Gröbner basis, except the Bucberger's algorithm

Note that the general problem in Gröbner basis computation known as *coefficient growth* does not affect in this cases since we can always take $\mathbb{K} = \mathbb{F}_2$ since the information of the ideal is only encoded in the exponents.

➜ SOLUTIONS

- Try to use Urbanke-Di Biase [9] philosophy, i.e. reduce the number of variables to n by defining directly the ideal in $\mathbb{K}[\mathbf{x}]$.
- Use BBFM-syzygy based method to compute the reduced Gröbner basis.

Describing the kernel in $\mathbb{K}[\mathbf{x}]$

For a matrix $A \in \mathbb{Z}_q^{m\times n}$ we will consider the following ideal:

$$I(A) = \langle \{\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}} \;:\; A \cdot \blacktriangledown(\mathbf{a}-\mathbf{b}) \equiv 0 \mod q\}\rangle$$

We consider the linear subespace:

$$\{u \in \mathbb{Z}_q^n | \mathbf{u} \cdot a \equiv 0 \mod q, \; \forall \mathbf{a} \text{ a row of } A\}$$

And $A^{\perp}$ be the matrix whose rows generate such linear subespace.
The following result extends the binary case in [3]

Theorem 1 (Márquez-Martínez 2010)

Let $\{w_1, \ldots, w_k\} \subseteq \mathbb{Z}_q^n$ a set of generators of the row space of the matrix $A \in \mathbb{Z}_q^{k\times n}$ and consider any vector $\mathbf{a},\ \mathbf{b} \in \mathbb{Z}^n$. The following conditions are equivalent:

1. $A^{\perp} \cdot \blacktriangledown\mathbf{a} \equiv A^{\perp} \cdot \blacktriangledown\mathbf{b} \mod q$.
2. $\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}} \in I(A^{\perp})$.
3. $\exists \mathbf{t}_1,\ \mathbf{t}_2 \in \mathbb{K}[\mathbf{x}]$ and $\lambda_1, \ldots, \lambda_k \in \mathbb{Z}^n$ such that

$$\mathbf{x}^{\mathbf{a}+(q-1)\mathbf{b}}\mathbf{t}_1^q = \mathbf{t}_2^q \prod_{j=1}^{s} \mathbf{x}^{\lambda_i \blacktriangle \mathbf{w}_i}.$$

Proof

Describing the kernel in $\mathbb{K}[\mathbf{x}]$

For a matrix $A \in \mathbb{Z}_q^{m \times n}$ we will consider the following ideal:

$$I(A) = \langle \{ \mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}} \ : \ A \cdot \blacktriangledown(\mathbf{a} - \mathbf{b}) \equiv 0 \mod q \} \rangle$$

We consider the linear subespace:

$$\{ u \in \mathbb{Z}_q^n | \mathbf{u} \cdot a \equiv 0 \mod q, \ \forall \mathbf{a} \text{ a row of } A \}$$

And $A^{\perp}$ be the matrix whose rows generate such linear subespace.
The following result extends the binary case in [3]

Theorem 1 (Márquez-Martínez 2010)

Let $\{w_1, \ldots, w_k\} \subseteq \mathbb{Z}_q^n$ a set of generators of the row space of the matrix $A \in \mathbb{Z}_q^{k \times n}$ and consider any vector $\mathbf{a}, \ \mathbf{b} \in \mathbb{Z}^n$. The following conditions are equivalent:

1. $A^{\perp} \cdot \blacktriangledown \mathbf{a} \equiv A^{\perp} \cdot \blacktriangledown \mathbf{b} \mod q$.
2. $\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}} \in I(A^{\perp})$.
3. $\exists \mathbf{t}_1, \ \mathbf{t}_2 \in \mathbb{K}[\mathbf{x}]$ and $\lambda_1, \ldots, \lambda_k \in \mathbb{Z}^n$ such that

$$\mathbf{x}^{\mathbf{a}+(q-1)\mathbf{b}} \mathbf{t}_1^q = \mathbf{t}_2^q \prod_{j=1}^{s} \mathbf{x}^{\lambda_j \blacktriangle \mathbf{w}_j}.$$

Proof

Describing the kernel in $\mathbb{K}[\mathbf{x}]$

Let us define the following ideal

$$\blacktriangle I = \langle \{\mathbf{x}^{\blacktriangle \mathbf{w}_1} - 1, \ldots, \mathbf{x}^{\blacktriangle \mathbf{w}_k} - 1\} \cup \{x_i^q - 1\}_{i=1}^n \rangle$$

Where $\{w_1, \ldots, w_k\} \subseteq \mathbb{Z}_q^n$ is a set of generators of the row space of the matrix A.

Theorem 2 (Márquez-Martínez 2010)

$$\blacktriangle I = I(A^\perp) = I_A \cap \mathbb{K}[\mathbf{x}]$$

◂ Proof

Note:

The matrix $A^\perp$ plays the role of the non negative matrix that Urbanke and Di Biase look for, thus the previous theorem can be seen as a generalization of the setting in [9] for getting rid of the variables concerning $\mathbf{y}$ in I_A.

Describing the kernel in $\mathbb{K}[\mathbf{x}]$

Let us define the following ideal

$$\blacktriangle I = \langle \{\mathbf{x}^{\blacktriangle \mathbf{w}_1} - 1, \ldots, \mathbf{x}^{\blacktriangle \mathbf{w}_k} - 1\} \cup \{x_i^q - 1\}_{i=1}^n \rangle$$

Where $\{w_1, \ldots, w_k\} \subseteq \mathbb{Z}_q^n$ is a set of generators of the row space of the matrix A.

Theorem 2 (Márquez-Martínez 2010)

$$\blacktriangle I = I(A^\perp) = I_A \cap \mathbb{K}[\mathbf{x}]$$

Proof

Note:

The matrix $A^\perp$ plays the role of the non negative matrix that Urbanke and Di Biase look for, thus the previous theorem can be seen as a generalization of the setting in [9] for getting rid of the variables concerning $\mathbf{y}$ in I_A.

FGLM-based trick

For computing a **Gröbner basis** of $I_A \cap \mathbb{K}[\mathbf{x}]$ w.r.t a degree compatible order we can use the FGLM-based trick presented in [3], since we know a set of generators of the ideal given by:

$$\left\{\mathbf{x}^{\blacktriangle \mathbf{w}_1} - 1, \ldots, \mathbf{x}^{\blacktriangle \mathbf{w}_1} - 1\right\} \cup \left\{x_i^q - 1\right\}_{i=1}^n .$$

Definition of syzygy

Let $F = \{f_1, \ldots, f_s\}$. A syzygy on the leading terms $\mathrm{LT}_{f_1}, \ldots, \mathrm{LT}_{f_r}$ of F is an s-tuple of polynomials $S = (h_1, \ldots, h_s) \in \mathbb{K}[\mathbf{x}]^s$ such that: $\sum_{i=1}^{s} h_i \cdot \mathrm{LT}(f_i) = 0$.

Idea of the FGLM-based trick

- Let consider:
  - The ideal $I \subseteq \mathbb{K}[\mathbf{x}]$ generated by the set $F = \{f_1, \ldots, f_r\}$.
  - The module $M \subseteq \mathbb{K}[\mathbf{x}]^{r+1}$ generated by the set $F' = \{-1, f_1, \ldots, f_r\}$
- Note that each syzygy on the module $M \subseteq \mathbb{K}[\mathbf{x}]^{r+1}$ points to an element in the ideal $I \subseteq \mathbb{K}[\mathbf{x}]$.
- Consider the syzygies:$(f_1, 1, 0, \ldots, 0), \ldots, (f_r, 0, \ldots, 0, 1)$
- They are a Gröbner basis of the syzygy module M w.r.t a POT ordering induced from an ordering $\succ$ in $\mathbb{K}[\mathbf{x}]$ and the weight vector $(1, \mathrm{LT}_{\succ}(f_1), \ldots, \mathrm{LT}_{\succ}(f_r))$
- Now we use the FGLM idea and run through the terms of $\mathbb{K}[x]^{r+1}$ in adequate TOP ordering.
- This reveals the Gröbner basis of the ideal I in the first component.

FGLM-based trick

- The above procedure is completely general.
- In has the following advantages:
  1. The problem of **growth of the total degree** not have to be considered, since the total degree of the binomials involved is bounded by $n \times q$.
  2. The problem of **coeficient growth** not have to be considered, since we can always take $\mathbb{K} = \mathbb{F}_2$.
  3. All steps can be carried out as Gaussian elimination steps (See [3] for an implementation).

Complete decoding

- Let $q = 2$ and $H_{\mathfrak{C}}$ be the parity check matrix of a linear code $\mathfrak{C}$ over $\mathbb{F}_2$.

$$\Rightarrow \mathfrak{C} = \{\mathbf{u} \in \mathbb{Z}_2^n \ : \ H_{\mathfrak{C}} \mathbf{u}^t \equiv 0 \mod 2\}.$$

- Let $\begin{cases} \mathbf{c} \in \mathfrak{C} \text{ be transmitted vector} \\ \overline{\mathbf{e}} \in \mathbb{Z}_2^n \text{ be the error vector} \\ \mathbf{r} \equiv \mathbf{c} + \overline{\mathbf{e}} \mod 2 \text{ be the received vector} \end{cases}$
- The **MLD** is equivalent to choose the error vector $\mathbf{e} \in \mathbb{Z}_2^n$ which minimizes the Hamming weight subject to $H\mathbf{e}^t \equiv H\mathbf{r}^t \mod 2$.
- Let $\mathbf{1} = (1, \ldots, 1)$, then $w_H(\mathbf{e}) = \mathbf{1} \cdot \mathbf{e}$.
- Therefore **solving the program**

$$\mathrm{IP}_{H,\mathbf{1},2}(\mathbf{b}) = \begin{cases} \text{minimize } \mathbf{1} \cdot \blacktriangle\mathbf{u} \\ \text{subject to } \begin{cases} H\mathbf{u}^t \equiv \mathbf{b} \mod q \\ \mathbf{u} \in \mathbb{Z}_q^n \end{cases} \end{cases}$$

Where $\mathbf{b} = H\mathbf{r}^t \in \mathbb{Z}_2^k$ **is equivalent to complete decoding b**.

- This is the approach in [12] and we have just shown that is equivalent to the approach in [3].
- The reduced Gröbner basis associated to the problem provides us a ”minimal” **test set** whose elements are the binomials associated to minimal codewords.
- Thus this complete decoding scheme is equivalent to the gradient decoding in Barg [1] which is proven to be equivalent to Lieber [14] approach (see [5]).

Research problem

- Unfortunately, for $q \geq 2$ Hamming metric can not be stated as the objective function of a linear programming problem, since:

$$\min\{\mathbf{w} \cdot \mathbf{u}\} \neq \min\{w_H(\mathbf{u})\}.$$

- In [4] Borges-Borges-Martínez skipped the problem for $q = p^r$ with p prime.

- **Research problem:** Can be this Hamming-like objective function be managed in a similar way for general (non-modular) integer programming problem?

We hope so!!!, we are working on it.

Graver basis

- (UGB_A): The **Universal Gröbner basis of A** is the union of all reduced Gröbner basis of the ideal I_A for every generic monomial ordering.
- A binomial $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \in I_A$ is **primitive** if

$$\nexists \mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-} \in I_A \ : \ \mathbf{x}^{\mathbf{v}^+} / \mathbf{x}^{\mathbf{u}^+} \text{ and } \mathbf{x}^{\mathbf{v}^-} / \mathbf{x}^{\mathbf{u}^-}.$$

- (Gr_A): The **Graver basis** is the set of all primitive binomials in I_A.
- A **circuit** of A is a non-zero primitive vector $\mathbf{u} \in \ker_{\mathbb{Z}}(A)$ such that its support is minimal. We denote $\mathcal{C}_A$ the set of circuits of A.
- We have that

$$\mathcal{C}_A \subseteq \mathrm{UGB}_A \subseteq \mathrm{Gr}_A$$

(See [18], Proposition 4.11 for a proof).

Conformal integer

For $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^n$ we say that $\mathbf{u}$ *is conformal to* $\mathbf{v}$, denoted $\mathbf{u} \sqsubset \mathbf{v}$ if $|\mathbf{u}_i| \leq |\mathbf{v}_i|$ and $\mathbf{u}_i \cdot \mathbf{v}_i > 0$ for all $i = 1, \ldots, n$.

- Note $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ is primitive $\Leftrightarrow \mathbf{u} \in \mathbb{Z}^n$ is minimal w.r.t. $\sqsubset$.
- $\mathrm{Gr}_A =$ Set of conformal minimal nonzero integer dependencies on A.

Graver basis

Universal test set

A set $\mathcal{U}_A \subseteq \ker_{\mathbb{Z}}(A)$ is an *universal test set* for IP_A if $\mathcal{U}_A$ contains a test set for the family of integer programs $\mathrm{IP}_{A,\mathbf{w}}$ for every generic $\mathbf{w}$.

- The **Graver basis** Gr_A and the **universal Gröbner basis** UGB_A of A are **universal test set** for A.

Laurence lifting

Laurence lifting

The *Laurence lifting* of the matrix $A \in \mathbb{Z}^{m \times n}$ is the enlarged matrix

$$\Lambda(A) = \begin{pmatrix} A & 0_{m \times n} \\ \mathrm{I_n} & \mathrm{I_n} \end{pmatrix} \in \mathbb{Z}^{(m+n) \times 2n}$$

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

The matrices A and $\Lambda(A)$ have isomorphic kernels, indeed

$$\ker(\Lambda(A)) = \{(\mathbf{u}, -\mathbf{u}) \ : \ \mathbf{u} \in \ker(A)\}. \tag{1}$$

The toric ideal $I_{\Lambda(A)}$ is an homogeneous prime ideal defined as:

$$I_{\Lambda(A)} = \langle \mathbf{x}^{\mathbf{u}^+} \mathbf{y}^{\mathbf{u}^-} - \mathbf{x}^{\mathbf{u}^-} \mathbf{y}^{\mathbf{u}^+} \ : \ \mathbf{u} \in \ker(A) \rangle. \tag{2}$$

Theorem (Sturmfels-Thomas, 1998, [18] Theorem 7.1)

For the matrix $\Lambda(A)$ the following sets coincide:

1. *The Graver basis of $\Lambda(A)$.*
2. *The universal Gröbner basis of $\Lambda(A)$.*
3. *Any reduced Gröbner basis of $\Lambda(A)$.*
4. *Any minimal generating set of $\Lambda(A)$ (up to scalar multiples).*

Laurence lifting

Theorem of Sturmfels-Thomas suggest the following algorithm for computing a Graver basis of A.

Algorithm for computing a Graver basis of A

1. We choose any term order on $\mathbb{K}[\mathbf{x}, \mathbf{y}]$.
2. We compute a reduced Gröbner basis of $\Lambda(A)$, by Theorem of Sturmfels-Thomas, any reduced Gröbner basis of $\Lambda(A)$ is also a Graver basis of $\Lambda(A)$.
3. Thus for each element in the Graver basis $\mathbf{x}^{\alpha}\mathbf{y}^{\beta} - \mathbf{x}^{\beta}\mathbf{y}^{\alpha}$, the element $\mathbf{x}^{\alpha} - \mathbf{x}^{\beta}$ belongs to the Graver basis of A.

Modular case

Laurent lifting for the modulo q

Let now consider the matrix $A \in \mathbb{Z}_q^{m\times n}$, following the works of A. Vigneron-Tenorio and P. Pison-Casares [16] and [15], we can define the Laurent lifting for the modulo q case as follows.

$$\Lambda(A)_q = \begin{pmatrix} A & 0_{q,m\times n} \\ \mathrm{I}_{q,n} & \mathrm{I}_{q,n} \end{pmatrix} \in \mathbb{Z}_q^{(m+n)\times 2n}$$

Where $I_{q,n} \in \mathbb{Z}_q^{n\times n}$ is the identity matrix and $0_{q,m\times n} \in \mathbb{Z}_q^{m\times n}$ is the zero matrix.

- We can see the ideal related to the $\mathbb{Z}_q$-kernel of $\Lambda(A)_q$ as an elimination ideal of the $\mathbb{Z}$-kernel of the matrix:

$$\begin{pmatrix} \blacktriangle A & 0_{m\times n} & q\cdot I_m \\ I_n & I_n & 0_{n\times m} \end{pmatrix} \in \mathbb{Z}^{(m+n)\times(2n+m)}$$

- Then we have a similar result to that in the previous slide relating the $\mathbb{Z}_q$-kernel of A and the $\mathbb{Z}_q$-kernel of $\Lambda(A)_q$ and how to compute the Gaver basis.
- Note that again we can use the modified version of the FGLM-based algorithm.

Minimal support

Consider a code $\mathfrak{C} \subseteq \mathbb{Z}_q^n$ with parity check matrix $H_{\mathfrak{C}}$.

Minimal support

- A codeword **m** has **minimal support** if its non-zero and $\mathrm{supp}(m)$ is not contained in the supports of any other codewords.

Lemma:

Two minimal support codewords of $\mathfrak{C} \subseteq \mathbb{Z}_q^n$ with the same support should be one scalar multiple of the other.

We define the **set of codewords of minimal support of the code** as a set containing a representative of all the minimal support codewords of the code modulo scalar multiplication.

Theorem 3 (Márquez-Martínez 2010)

The set of codewords of minimal support of the code $\mathfrak{C} \subseteq \mathbb{Z}_q^n$ corresponds to the Graver basis of $H_{\mathfrak{C}}$ where $H_{\mathfrak{C}}$ is a parity check matrix of $\mathfrak{C}$.

Proof

- This theorem gives us a procedure to compute the set of codewords of minimal support of codes defined on $\mathbb{Z}_q$.
  - In particular for codes over $\mathbb{F}_p$ with p prime.
  - But not for the case p^r since $\mathbb{F}_{p^r} \not\equiv \mathbb{Z}_{p^r}$.

Minimal support

Consider a code $\mathfrak{C} \subseteq \mathbb{Z}_q^n$ with parity check matrix $H_{\mathfrak{C}}$.

Minimal support

➜ A codeword **m** has **minimal support** if its non-zero and $\mathrm{supp}(m)$ is not contained in the supports of any other codewords.

Lemma:

Two minimal support codewords of $\mathfrak{C} \subseteq \mathbb{Z}_q^n$ with the same support should be one scalar multiple of the other.

We define the **set of codewords of minimal support of the code** as a set containing a representative of all the minimal support codewords of the code modulo scalar multiplication.

Theorem 3 (Márquez-Martínez 2010)

The set of codewords of minimal support of the code $\mathfrak{C} \subseteq \mathbb{Z}_q^n$ corresponds to the Graver basis of $H_{\mathfrak{C}}$ where $H_{\mathfrak{C}}$ is a parity check matrix of $\mathfrak{C}$.

◂ Proof

➤ This theorem gives us a procedure to compute the set of codewords of minimal support of codes defined on $\mathbb{Z}_q$.

- In particular for codes over $\mathbb{F}_p$ with p prime.
- But not for the case p^r since $\mathbb{F}_{p^r} \not\equiv \mathbb{Z}_{p^r}$.

Minimal support

Corollary

The set of codewords of minimal support of the code $\mathfrak{C} \subseteq \mathbb{Z}_q^n$ can be computed from the ideal:

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

where $\mathbf{w}_i$ for $i = 1, \ldots, k$ are the rows of a generator matrix of $\mathfrak{C}$.

Example

Consider $\mathfrak{C}$ the $[7, 4, 3]$ Hamming code over $\mathbb{F}_2$.

- It has 16 codewords of weights $0, 3, 4, 7$.
- All the 14 codewords of weight 3 or 4 are minimal
- The only non minimal codewords are **0** and **1**.

➤ The **Gröbner test** set for H w.r.t. a dp ordering we get:

$$\begin{gathered}\{x_3x_7 + x_1, x_1x_7 + x_3, x_5x_6 + x_1, x_4x_6 + x_3, x_3x_6 + x_4, x_2x_6 + x_7, \\ x_1x_6 + x_5, x_4x_5 + x_7, x_3x_5 + x_2, x_2x_5 + x_3, x_1x_5 + x_6, x_3x_4 + x_6, \\ x_2x_4 + x_1, x_1x_4 + x_2, x_2x_3 + x_5, x_1x_3 + x_7, x_1x_2 + x_4\} \cup \{x_i^2 - 1\}_{i=1}^7\end{gathered}$$

which gives us the 7 minimal codewords of weight 3.

➤ The dp Gröbner basis of the **Lawrence lifting** used for computing the Graver basis has 155 elements representing :

- 7 words of the Gröbner test set.
- 7 minimal codewords of weight 4.

Research problem

Research problem:

There is a close relationship between minimal support codewords and minimal elements in matroids.

- We have decomposition theorems for binary matroids that give us a matroid as a composition of smaller ones.
- **Can these results be use to decompose also the Graver basis?**

We hope so!!!, we are working on it.

Bibliography I

A. Barg,
Complexity Issues in Coding Theory,
Electronic Colloquium on Computational Complexity (ECCC) **4** (1997), no. 4.

T. Bogart, A.N. Jensen and R.R. Thomas,
The circuit ideal of a vector configuration,
J. Algebra **308** (2007), no. 23, 518–542.

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. **19** (2008), no. 5, 393–411.

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

M. Borges-Quintana, M.A. Borges-Trenard, I. Márquez-Corbella and E. Martínez-Moro,
On the Border of a Binary Code
Submitted to Jour.Comp. Applied Maths. (2009).

Bibliography II

P. Conti and C. Traverso,
Buchberger algorithm and integer programming,
Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991), Lecture Notes in Comput. Sci. **539** (1991), 130–139.

G.B. Dantzig,
Linear Programming and Extensions,
Princeton University Press, (1963).

G.B. Dantzig,
Reminiscences about the origins of linear programming,
Operations Resarch Letters **1** (1982), 43–48.

F. Di Biase and R. Urbanke,
An algorithm to calculate the kernel of certain polynomial ring homomorphisms,
Experiment. Math. **4** (1995), no. 3, 227–234.

R. Dorfman,
The discovery of linear programming,
Annals of the History of Computing **6** (1984), 283–295.

Bibliography III

T.Y. Hwang,
Decoding linear block codes for minimizing word error rate,
IEEE Trans. Inform. Theory **25** (1979), 733–737.

D. Ikegami and Y. Kaji,
Maximum likelihood decoding for linear block codes using Gröbner bases,
IEICE Trans. Fund. Electron. Commun. Comput. Sci. E86-A , **3** (2003) 643–651.

H. Ohsugi,, D. Ikegami, T. Kitamura and T. Hibi,
Gröbner bases bases of certain zero-dimensional ideals arising in coding theory,
Adv. in Appl. Math., **31** (2003) no. 2, 420–432.

R. Liebler,
Implementing gradient descent decoding
Michigan Math,**58**, Issue 1 (2009), 285–291.

P. Pisón-Casares and A.Vigneron-Tenorio,
Ideales de semigrupos con torsión: Cáculos mediante maplev
Actas del EACA'96, (1996).

Bibliography IV

P. Pisón-Casares and A. Vigneron-Tenorio,
On Lawrence semigroups
Journal of Symbolic Computation, **43** (2008), 804–810.

A. Schrijver,
Theory of Linear and Integer Programming
Wiley-Interscience, (1996).

B. Sturmfels,
Gröbner bases bases and Convex Polytopes
University Lecture Series, **8**, American Mathematical Society, Providence, RI, (1996).

Thank you for your attention

Proof of Theorem 1

- Let $\mathbf{x}$ denote n variables $x_1, \ldots, x_n$ and $\mathbf{y}$ denote m variables $y_1, \ldots, y_m$.
- Consider the ring homomorphism Θ defined by:

$$\begin{array}{rccc} \Theta : & \mathbb{K}[\mathbf{x}] & \longrightarrow & \mathbb{K}[\mathbf{y}] \\ & \mathbf{x}^{\mathbf{u}} & \longmapsto & \Theta(\mathbf{x}^{\mathbf{u}}) = \mathbf{y}^{A\mathbf{u}^t} \end{array}$$

- Let defined the binomial ideal J_q as $J_q = \langle \{y_i^q - 1\}_{i=1}^m \rangle \subseteq \mathbb{K}[\mathbf{y}]$

For the proof of **Theorem 1** we need the following **Lemma 1** and **Lemma 2**

Lema 1: (Ikegami-Kaji, 2003)

$$A\mathbf{u}^t \equiv \mathbf{b} \mod q \iff \Theta(\mathbf{x}^{\blacktriangle\mathbf{u}}) \equiv \mathbf{y}^{\blacktriangle\mathbf{b}} \mod J_q$$

Lemma 2:

$$f \in I_A \cap \mathbb{K}[\mathbf{x}] \iff f \in \mathbb{K}[\mathbf{x}] \text{ and } \Theta(f) \equiv 0 \mod J_q$$

Proof of Lemma 2:

$\Rightarrow$ Let $f \in I_A \cap \mathbb{K}[\mathbf{x}]$, by representing f with the generators of I_A we have:
$f(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n \lambda_i(\phi_i - x_i) + \sum_{j=1}^m \beta_j(y_j^q - 1)$ with $\lambda_i, \beta_j \in \mathbb{K}[\mathbf{x}, \mathbf{y}], \forall i, j$.

$$\begin{aligned} \Theta(f) &= f(\Theta(x_1), \ldots, \Theta(x_n), y_1, \ldots, y_m) \\ &= \sum_{i=1}^n \Theta(\lambda_i)(\phi_i - \Theta(x_i)) + \sum_{j=1}^m \Theta(\beta_j)(y_j^q - 1) \equiv 0 \mod J_q \end{aligned}$$

$\Leftarrow$ See [12], Lemma 7.

Proof of Theorem 1

- Let **x** denote n variables $x_1, \ldots, x_n$ and **y** denote m variables $y_1, \ldots, y_m$.
- Consider the ring homomorphism Θ defined by:

$$\begin{array}{rccc} \Theta: & \mathbb{K}[\mathbf{x}] & \longrightarrow & \mathbb{K}[\mathbf{y}] \\ & \mathbf{x}^{\mathbf{u}} & \longmapsto & \Theta(\mathbf{x}^{\mathbf{u}}) = \mathbf{y}^{A\mathbf{u}^t} \end{array}$$

- Let defined the binomial ideal J_q as $J_q = \langle \{y_i^q - 1\}_{i=1}^m \rangle \subseteq \mathbb{K}[\mathbf{y}]$

For the proof of **Theorem 1** we need the following **Lemma 1** and **Lemma 2**

Lema 1: (Ikegami-Kaji, 2003)

$$A\mathbf{u}^t \equiv \mathbf{b} \mod q \iff \Theta(\mathbf{x}^{\blacktriangle \mathbf{u}}) \equiv \mathbf{y}^{\blacktriangle \mathbf{b}} \mod J_q$$

Lemma 2:

$$f \in I_A \cap \mathbb{K}[\mathbf{x}] \iff f \in \mathbb{K}[\mathbf{x}] \text{ and } \Theta(f) \equiv 0 \mod J_q$$

Proof of Lemma 2:

$\Rightarrow$ Let $f \in I_A \cap \mathbb{K}[\mathbf{x}]$, by representing f with the generators of I_A we have: $f(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n \lambda_i(\phi_i - x_i) + \sum_{j=1}^m \beta_j(y_j^q - 1)$ with $\lambda_i, \beta_j \in \mathbb{K}[\mathbf{x}, \mathbf{y}], \forall i, j$.

$$\begin{aligned} \Theta(f) &= f(\Theta(x_1), \ldots, \Theta(x_n), y_1, \ldots, y_m) \\ &= \sum_{i=1}^n \Theta(\lambda_i)(\phi_i - \Theta(x_i)) + \sum_{j=1}^m \Theta(\beta_j)(y_j^q - 1) \equiv 0 \mod J_q \end{aligned}$$

$\Leftarrow$ See [12], Lemma 7.

Proof of Theorem 1

- Equivalence between 1 and 2:

  By **Lemma 2**: $\mathbf{x^a} - \mathbf{x^b} \in I(A^\perp) \Leftrightarrow \Theta(\mathbf{x^a} - \mathbf{x^b}) \equiv 0 \mod J_q$.

  $\Leftrightarrow \mathbf{y}^{(\blacktriangle A)^\perp \cdot \mathbf{a}} \equiv \mathbf{y}^{(\blacktriangle A)^\perp \cdot \mathbf{b}} \mod J_q$

  $\Leftrightarrow$ By **Lemma 1**: $A^\perp \cdot \blacktriangledown \mathbf{a} \equiv A^\perp \cdot \blacktriangledown \mathbf{b} \mod q$.

- Let define the homomorphism Φ from $\mathbb{K}[\mathbf{x}]$ to $\mathbb{Z}_q^n$ as:

$$\begin{array}{cccc} \Phi : & \mathbb{K}[\mathbf{x}] & \longrightarrow & \mathbb{Z}_q^n \\ & \mathbf{x^a} & \longmapsto & \Phi(\mathbf{x^a}) = ((\blacktriangledown a_1), \ldots, (\blacktriangledown a_n)) \end{array}$$

- For all $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^n$ the following properties holds:

  1. $\Phi(\mathbf{x^a}) = \Phi(\mathbf{x^b}) \Longleftrightarrow \exists \mathbf{t}_1, \mathbf{t}_2 \in \mathbb{K}[\mathbf{x}]$ such that $\mathbf{t}_1^q \mathbf{x^a} = \mathbf{t}_2^q \mathbf{x^b}$.
  2. $\Phi(\mathbf{x^a}) - \Phi(\mathbf{x^b}) = \Phi(\mathbf{x^a}) + (q-1)\Phi(\mathbf{x^b}) = \Phi(\mathbf{x}^{\mathbf{a}+(q-1)\mathbf{b}})$.
  3. $\mathbf{x^a} - \mathbf{x^b} \in I(A^\perp) \Leftrightarrow \Phi(\mathbf{x^a}) - \Phi(\mathbf{x^b}) \in \langle \{\mathbf{w}_1, \ldots, \mathbf{w}_k\} \rangle$ Since
     $\mathbf{x^a} - \mathbf{x^b} \in I(A^\perp) \Leftrightarrow A^\perp \cdot \blacktriangledown(\mathbf{a} - \mathbf{b}) \equiv 0 \mod q$
     $\Leftrightarrow \blacktriangledown(a - b) \in \langle \{\mathbf{w}_1, \ldots, \mathbf{w}_k\} \rangle$.

Proof of Theorem 1

$2 \Rightarrow 3$ If $\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}} \in I(A^{\perp})$ we have can write the vector $\Phi(\mathbf{x}^{\mathbf{a}}) - \Phi(\mathbf{x}^{\mathbf{b}})$ as

$$\Phi(\mathbf{x}^{\mathbf{a}}) - \Phi(\mathbf{x}^{\mathbf{b}}) = \Phi(\mathbf{x}^{\mathbf{a}+(q-1)\mathbf{b}}) = \sum_{i=1}^{k} \lambda_i \blacktriangle \mathbf{w}_i = \Phi(\prod_{i=1}^{k} \mathbf{x}^{\lambda_i \blacktriangle \mathbf{w}_i}).$$

with $\lambda_i \in \mathbb{Z}^n$. By property 1, there exists $\mathbf{t}_1, \mathbf{t}_2 \in \mathbb{K}[\mathbf{x}]$ such that

$$\mathbf{t}_1^q \mathbf{x}^{\mathbf{a}+(q-1)\mathbf{b}} = \mathbf{t}_2^q \prod_{i=1}^{k} \mathbf{x}^{\lambda_i \blacktriangle \mathbf{w}_i}.$$

$2 \Leftarrow 3$ If there exists $\mathbf{t}_1, \mathbf{t}_2 \in \mathbb{K}[\mathbf{x}]$ and $\lambda_1, \ldots, \lambda_k \in \mathbb{Z}^n$ such that

$$\mathbf{t}_1^q \mathbf{x}^{\mathbf{a}+(q-1)\mathbf{b}} = \mathbf{t}_2^q \prod_{i=1}^{k} \mathbf{x}^{\lambda_i \blacktriangle \mathbf{w}_i}.$$

Hence

$$\Phi(\mathbf{x}^{\mathbf{a}}) - \Phi(\mathbf{x}^{\mathbf{b}}) = \Phi(\mathbf{x}^{\mathbf{a}+(q-1)\mathbf{b}}) = \Phi(\prod_{i=1}^{k} \mathbf{x}^{\lambda_i \blacktriangle \mathbf{w}_i}) = \sum_{i=1}^{k} \lambda_i \blacktriangle \mathbf{w}_i$$

and we may conclude that the vector $\Phi(\mathbf{x}^{\mathbf{a}}) - \Phi(\mathbf{x}^{\mathbf{b}})$ is a linear combination of the set $\{\blacktriangle \mathbf{w}_1, \ldots \blacktriangle \mathbf{w}_k\}$ which implies that $\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}} \in I(\blacktriangle((\blacktriangledown A)^{\perp}))$.

Return

Proof of Theorem 2

$\blacktriangle I \subseteq I(A^\perp)$

It is clear that $\blacktriangle I \subseteq I(A^\perp)$ since all binomials in the generating set of $\blacktriangle I$ belongs to $I(A^\perp)$.

$I(A^\perp) \subseteq \blacktriangle I$

It is enough to prove that any binomial $\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}}$ of $I(A^\perp)$ belongs to $\blacktriangle I$.

- By **Theorem 1**: $\exists \mathbf{t}_1,\ \mathbf{t}_2 \in \mathbb{K}[\mathbf{x}]$ and $\lambda_1, \ldots, \lambda_k \in \mathbb{Z}^n$ such that
$$\mathbf{x}^{\mathbf{a}+(q-1)\mathbf{b}}\mathbf{t}_1^q = \mathbf{t}_2^q \prod_{j=1}^{s} \mathbf{x}^{\lambda_j \blacktriangle \mathbf{w}_j}.$$
- If $\mathbb{Z}_1 - 1,\ \mathbb{Z}_2 - 1 \in \blacktriangle I$, since $\mathbb{Z}_1\mathbb{Z}_2 - 1 = (\mathbb{Z}_1 - 1)\cdot \mathbb{Z}_2 + (\mathbb{Z}_2 - 1)$, we have
$$\mathbb{Z}_1 \cdot \mathbb{Z}_2 - 1 \in \blacktriangle I.$$
- Therefore $\prod_{i=1}^{k} \mathbf{x}^{\blacktriangle \mathbf{w}_i} - 1 \in \blacktriangle I$ and
$$\prod_{j=1}^{k} \mathbf{x}^{\lambda_j \mathbf{w}_j} - 1 = (\prod_{j=1}^{k} \mathbf{x}^{\mathbf{w}_j} - 1) \cdot \prod_{j\,:\,\lambda_j > 0} \mathbf{x}^{(\lambda_j - 1)\mathbf{w}_j} + \ldots + (\prod_{j\,:\,\lambda_j > r} \mathbf{x}^{\mathbf{w}_j} - 1) \in \blacktriangle I$$
- This implies that $\mathbf{t}_1^q \mathbf{x}^{\mathbf{a}+(q-1)\mathbf{b}} - 1 = \mathbf{t}_2^q \prod_{j=1}^{k} \mathbf{x}^{\lambda_j \blacktriangle \mathbf{w}_j} - 1 \in \blacktriangle I$. Since
$$\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}} = \mathbf{x}^{\mathbf{b}}(\mathbf{x}^{\mathbf{a}+(q-1)\mathbf{b}} - 1) - \mathbf{x}^{\mathbf{a}}(\mathbf{x}^{q\mathbf{b}} - 1) \in \blacktriangle I,$$
we may conclude that $I(A^\perp) = \blacktriangle I$.

Proof of Theorem 2

$\blacktriangle I \subseteq I(A^\perp)$

It is clear that $\blacktriangle I \subseteq I(A^\perp)$ since all binomials in the generating set of $\blacktriangle I$ belongs to $I(A^\perp)$.

$I(A^\perp) \subseteq \blacktriangle I$

It is enough to prove that any binomial $\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}}$ of $I(A^\perp)$ belongs to $\blacktriangle I$.

- By **Theorem 1**: $\exists \mathbf{t}_1,\ \mathbf{t}_2 \in \mathbb{K}[\mathbf{x}]$ and $\lambda_1, \ldots, \lambda_k \in \mathbb{Z}^n$ such that
$$\mathbf{x}^{\mathbf{a}+(q-1)\mathbf{b}}\mathbf{t}_1^q = \mathbf{t}_2^q \prod_{j=1}^{s} \mathbf{x}^{\lambda_j \blacktriangle \mathbf{w}_j}.$$
- If $\mathbb{Z}_1 - 1,\ \mathbb{Z}_2 - 1 \in \blacktriangle I$, since $\mathbb{Z}_1\mathbb{Z}_2 - 1 = (\mathbb{Z}_1 - 1)\cdot\mathbb{Z}_2 + (\mathbb{Z}_2 - 1)$, we have
$$\mathbb{Z}_1 \cdot \mathbb{Z}_2 - 1 \in \blacktriangle I.$$
- Therefore $\prod_{i=1}^{k} \mathbf{x}^{\blacktriangle \mathbf{w}_i} - 1 \in \blacktriangle I$ and
$$\prod_{j=1}^{k} \mathbf{x}^{\lambda_j \mathbf{w}_j} - 1 = \Big(\prod_{j=1}^{k} \mathbf{x}^{\mathbf{w}_j} - 1\Big) \cdot \prod_{j\,:\,\lambda_j > 0} \mathbf{x}^{(\lambda_j - 1)\mathbf{w}_j} + \ldots + \Big(\prod_{j\,:\,\lambda_j > r} \mathbf{x}^{\mathbf{w}_j} - 1\Big) \in \blacktriangle I$$
- This implies that $\mathbf{t}_1^q \mathbf{x}^{\mathbf{a}+(q-1)\mathbf{b}} - 1 = \mathbf{t}_2^q \prod_{j=1}^{k} \mathbf{x}^{\lambda_j \blacktriangle \mathbf{w}_j} - 1 \in \blacktriangle I$. Since
$$\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}} = \mathbf{x}^{\mathbf{b}}(\mathbf{x}^{\mathbf{a}+(q-1)\mathbf{b}} - 1) - \mathbf{x}^{\mathbf{a}}(\mathbf{x}^{q\mathbf{b}} - 1) \in \blacktriangle I,$$
we may conclude that $I(A^\perp) = \blacktriangle I$.

Proof of Theorem 2

$\blacktriangle I \subseteq I_A \cap \mathbb{K}[\mathbf{x}]$

- First we note that:
  1. $\Theta(\mathbf{x}^{\blacktriangle \mathbf{w}_i} - 1) = 0$, since $A \cdot A^{\perp} = 0$.
  2. $$\begin{aligned} \Theta(x_i^q - 1) &= \Theta(\mathbf{x}^{q\mathbf{e}_i} - 1) = \mathbf{y}^{(\blacktriangle(A^{\perp})(q\mathbf{e}_i)} - 1 \\ &\equiv \sum_{j\,:\,b_{ij}\neq 0} B_j(y_j^q - 1) \equiv 0 \mod J_q \end{aligned}$$

  where $(\blacktriangle A)^{\perp} = (b_{ij}) \in \mathbb{Z}^{m\times n}$, $B_j \in \mathbb{K}[\mathbf{y}]$ and $\mathbf{e}_i$ represent the unit vector of the standard basis of $\mathbb{Z}^n$.
- By **Lemma 2**: all binomial in the generating set of $\blacktriangle I$ belongs to $I_A \cap \mathbb{K}[\mathbf{x}]$.

$I_A \cap \mathbb{K}[\mathbf{x}] \subseteq \blacktriangle I$

- Since $I_A \cap \mathbb{K}[\mathbf{x}]$ is a binomial ideal, it is generated by binomial.
- Thus, let consider a binomial $f = \mathbf{x}^{\mathbf{u}} - \mathbf{x}^{\mathbf{v}} \in I_A \cap \mathbb{K}[\mathbf{x}]$ with $\mathbf{u}, \ \mathbf{v} \in \mathbb{Z}^n$.
- By **Lemma 2**: $\Theta(f) = \mathbf{y}^{\blacktriangle(A^{\perp})\cdot\mathbf{u}^t} - \mathbf{y}^{\blacktriangle(A^{\perp})\cdot\mathbf{v}^t} \equiv 0 \mod J_q$.
- By **Lemma 1**: $A^{\perp} \cdot \blacktriangledown\mathbf{u} \equiv A^{\perp} \cdot \blacktriangledown\mathbf{v} \mod q$.
- By **Theorem 1**: we conclude that $f \in I(A^{\perp}) = \blacktriangle I$.

Return

Proof of Theorem 3

Theorem 3 (Márquez-Martínez 2010)

The set of codewords of minimal support of the code $\mathfrak{C} \subseteq \mathbb{Z}_q^n$ corresponds to the Graver basis of $\blacktriangle A$ where A is a parity check matrix of $\mathfrak{C}$.

Let $\begin{cases} \mathbf{m}, & \text{be a codeword of minimal support of the code } \mathfrak{C}; \\ \mathrm{Gr}_{\blacktriangle A}, & \text{the Graver basis of } \blacktriangle A. \end{cases}$

Assume that $\mathbf{m} \notin \mathrm{Gr}_{\blacktriangle A} \Rightarrow \mathbf{x}^{\mathbf{m}^+} - \mathbf{x}^{\mathbf{m}^-} \in I_{\blacktriangle A}$ is not primitive.

Hence $\exists \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \in I_{\blacktriangle A} : \mathbf{u} \sqsubset \mathbf{m}$, contradicting the fact that $\mathbf{m}$ has minimal support.

The opposite follows from the definition. Return

Proof of Theorem 3

Theorem 3 (Márquez-Martínez 2010)

The set of codewords of minimal support of the code $\mathfrak{C} \subseteq \mathbb{Z}_q^n$ corresponds to the Graver basis of $\blacktriangle A$ where A is a parity check matrix of $\mathfrak{C}$.

Let $\begin{cases} \mathbf{m}, & \text{be a codeword of minimal support of the code } \mathfrak{C}; \\ \mathrm{Gr}_{\blacktriangle A}, & \text{the Graver basis of } \blacktriangle A. \end{cases}$

Assume that $\mathbf{m} \notin \mathrm{Gr}_{\blacktriangle A} \Rightarrow \mathbf{x}^{\mathbf{m}^+} - \mathbf{x}^{\mathbf{m}^-} \in I_{\blacktriangle A}$ is not primitive.

Hence $\exists \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \in I_{\blacktriangle A} : \mathbf{u} \sqsubset \mathbf{m}$, contradicting the fact that $\mathbf{m}$ has minimal support.

The opposite follows from the definition. Return