The ideal associated to a code

Coding Theory Seminar

E. Martínez-Moro

Instituto de Investigación en Matemáticas
Universidad de Valladolid

References

A Combinatorial Commutative Algebra Approach to Complete Decoding (2013) PhD Thesis. I. Marquez-Corbella.

Outline

Reference
- Gröbner representation

Gröbner basis
- Gröbner representation of binary codes

Computing coset leaders
- Computing a test set

Border of a code

Further topics

Notation

- $\mathbb{K}$: arbitrary field, $\mathbb{Z}$: ring of integers.
- $\mathbb{Z}_q$: ring of integers modulo q, $\mathbb{F}_q$: finite field with q elements $(q = p^r)$.
- $\mathbb{K}[\mathbf{X}]$: The polynomial ring in n variables $\mathbf{X} = X_1, X_2, \ldots, X_n$ over $\mathbb{K}$.

Characteristic crossing functions :

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

where:

- 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.

Notation

- $\mathbb{K}$: arbitrary field, $\mathbb{Z}$: ring of integers.
- $\mathbb{Z}_q$: ring of integers modulo q, $\mathbb{F}_q$: finite field with q elements ($q = p^r$).
- $\mathbb{K}[\mathbf{X}]$: The polynomial ring in n variables $\mathbf{X} = X_1, X_2, \ldots, X_n$ over $\mathbb{K}$.

Characteristic crossing functions :

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

where:

- 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.

Notation

Let $\mathbf{a} = (a_1, \ldots, a_n)$ be an element of $\mathbb{Z}_q^n$ we set

$$\mathbf{X}^{\blacktriangle \mathbf{a}} = X_1^{\blacktriangle a_1} \cdots X_n^{\blacktriangle a_n}.$$

Gröbner representation

Let $\{\mathbf{e}_i \mid i \in \{1, \ldots, n\}\}$ be a canonical basis of $\mathbb{F}_2^n$. 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:
  - $\mathbf{0} \in \mathcal{N}$
  - $\mathbf{n} \in \mathcal{N} \setminus \{\mathbf{0}\} \Longrightarrow \exists i \in \{1, \ldots, n\} \ : \ \mathbf{n} = \mathbf{n}' + \mathbf{e}_i$ with $\mathbf{n}' \in \mathcal{N}$
- $\phi : \ \mathcal{N} \times \{\mathbf{e}_i\}_{i=1}^n \ \longrightarrow \ \mathcal{N}$
- that maps each pair $(\mathbf{n}, \mathbf{e}_i)$ to the element of $\mathcal{N}$ representing the coset of $\mathbf{n} + \mathbf{e}_i$.

Gröbner representation

Some references on Gröbner representation 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.

Stop!!!

See the witheboard for a really quick intro to Gröbner basis.

Gröbner representation of binary codes

The word **Gröbner** is NOT CASUAL.

1. Consider:
   - The binomial ideal:

$$I_2(\mathcal{C}) = \left\langle \mathbf{X}^{\blacktriangle \mathbf{w}_1} - \mathbf{X}^{\blacktriangle \mathbf{w}_2} \mid \mathbf{w}_1 - \mathbf{w}_2 \in \mathcal{C} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]$$

   - A degree compatible ordering $\prec$.
2. Compute a Gröbner basis $\mathcal{G}$ of $I_2(\mathcal{C})$ w.r.t. $\prec$.
3. Then we can take:
   - $\mathcal{N}$ as the vectors $\mathbf{w}$ such that $\mathbf{X}^{\mathbf{w}}$ is a standard monomial in $\mathcal{G}$.
   - ϕ as the multiplications tables of the standard monomials times the variables x_i for $i = 1, \ldots, n$ modulo the ideal $I_2(\mathcal{C})$.

Gröbner representation of binary codes

Theorem [Borges-Borges-Fitzpatrick-Martínez (2008)] Given the rows of a generator matrix of an $[n, k]$ binary code $\mathcal{C}$ labelled by $\mathbf{w}_1, \ldots, \mathbf{w}_k$, then:

$$I_2(\mathcal{C}) = \left\langle \; \{\mathbf{X}^{\blacktriangle \mathbf{w}_i} - 1\}_{i=1,\ldots,k} \;\; \bigcup \;\; \left\{x_i^2 - 1\right\}_{i=1,\ldots,n} \; \right\rangle$$

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 $\mathcal{C}$:

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

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 $\mathcal{C}$:

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

Example 1

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

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

- $\mathcal{N} = \{ \ \mathbf{0}, \ \mathbf{e}_1, \ \mathbf{e}_2, \mathbf{e}_3, \ \mathbf{e}_4, \ \mathbf{e}_5, \mathbf{e}_6, \ \mathbf{e}_1 + \mathbf{e}_6 \ \}$

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

Example 1

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

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

- $\mathcal{N} = \{\ \mathbf{0},\ \mathbf{e}_1,\ \mathbf{e}_2, \mathbf{e}_3,\ \mathbf{e}_4,\ \mathbf{e}_5, \mathbf{e}_6,\ \mathbf{e}_1 + \mathbf{e}_6\ \}$

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

Instituto de Matemáticas

Computing coset leaders

Algorithm 5.1: Computing all the coset leader of a binary code $\mathcal{C}$

Data: A weight compatible ordering $\prec$ and a parity check matrix H $\mathcal{C}$.

Result: The set of coset leaders $\mathrm{CL}(\mathcal{C})$ and $(\mathcal{N}, \phi)$ a GR for $\mathcal{C}$.

$\mathtt{List} \longleftarrow [0]$; $\mathcal{N} \longleftarrow \emptyset$; $r \longleftarrow 0$; $\mathrm{CL}(\mathcal{C}) \longleftarrow \emptyset$; $\mathcal{S} \longleftarrow \emptyset$;

while $\mathtt{List} \neq \emptyset$ **do**

  $\mathbf{t} \longleftarrow \mathtt{NextTerm}[\mathtt{List}]$; $\mathbf{s} \longleftarrow \mathbf{t}H^T$;

  $j \longleftarrow \mathtt{Member}[s, \mathcal{S}]$;

  if $j \neq \mathtt{false}$ **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**

      $\mathrm{CL}(\mathcal{C})[\mathbf{t}_j] \longleftarrow \mathrm{CL}\mathcal{C}[\mathbf{t}_j] \cup \{\mathbf{t}\}$;

      $\mathtt{List} \longleftarrow \mathtt{InsertNext}[\mathbf{t}, \mathtt{List}]$;

  else

    $r \longleftarrow r + 1$; $\mathbf{t}_r \longleftarrow \mathbf{t}$; $\mathcal{N} \longleftarrow \mathcal{N} \cup \{\mathbf{t}_r\}$;

    $\mathrm{CL}(\mathcal{C})[\mathbf{t}_r] \longleftarrow \{\mathbf{t}_r\}$; $\mathcal{S} \longleftarrow \mathcal{S} \cup \{\mathbf{s}\}$;

    $\mathtt{List} = \mathtt{InsertNext}[\mathbf{t}_r, \mathtt{List}]$;

    for $k \in \mathrm{supp}(\mathbf{t}_r) \ : \ \mathbf{t}_r = \mathbf{t}' + \mathbf{e}_k$ *with* $\mathbf{t}' \in \mathcal{N}$ **do**

      $\phi(\mathbf{t}', \mathbf{e}_k) \longleftarrow \mathbf{t}_r$;

      $\phi(\mathbf{t}_r, \mathbf{e}_k) \longleftarrow \mathbf{t}'$;

Computing coset leaders

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

Example 1. (Cont.)

- Using algorithm 5.1, 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

Instituto de Matemáticas

Extra info.

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 α_i is the $\sharp$ of cosets with weight i.
- **Number of coset leaders in each coset**.

Example 1. (Cont.)

$\nu(\mathcal{C}) = 1,\ \rho(\mathcal{C}) = 2,\ \mathrm{WDCL} = \left[\ 1, 6, 1, 0, 0, 0\ \right]$ and

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

Computing a test set

Algorithm 5.2: Algorithm for computing a test-set 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 the set of leader codewords $\mathrm{L}(\mathcal{C})$ for $\mathcal{C}$.

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

Computing a test set

- The difference between Algorithm 5.1 are the Steps in red.

Theorem[Borges-Borges-Márquez-Martínez]. The subset $\mathrm{L}(\mathcal{C})$ is a test-set for $\mathcal{C}$.

Instituto de Matemáticas

Computing a test set

- With the subset of **leader codewords** $(\mathrm{LC}(\mathcal{C}))$ we can computes the subset $\mathrm{CL}(\mathbf{y})$ of coset leaders corresponding to the coset $\mathbf{y}+\mathcal{C}$.

Algorithm 5.3: Computing the set $\mathrm{CL}(\mathbf{y})$

Data: A vector $\mathbf{y} \in \mathbb{F}_2^n$ and the **set of leader codewords** $\mathrm{L}(\mathcal{C})$ **of** $\mathcal{C}$.
Result: The **subset** $\mathrm{CL}(\mathbf{y})$ of coset leaders of $\mathbf{y}+\mathcal{C}$.

```
Compute a coset leader of y + C by gradient-like decoding using the
test-set L(C) ;
y ⟵ N(y); S ⟵ {y}; L ⟵ L(C);
while there exists c ∈ L : w_H(y − c) = w_H(y) do
    y ⟵ y − c; S ⟵ S ∪ {y};
    L ⟵ L − {c};
Return S
```

Border of a code

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:

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

$\mathrm{head}(\mathbf{b}) + \mathrm{tail}(\mathbf{b}) \in \mathcal{C}$.

Border of a code

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

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

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

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

$\mathrm{head}(\mathbf{b}) + \mathrm{tail}(\mathbf{b}) \in \mathcal{C}$.

Instituto de Matemáticas

Border of a code

The information in the border is somehow **redundant**, we can reduce the number of codewords in it by defining the Reduced Border of a code as follows:

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 $\mathrm{supp}\,(\mathrm{head}(\mathbf{h})) \subseteq \mathrm{supp}\,(\mathrm{head}(\mathbf{b}))$.
- For every two different elements $\mathbf{h}_1$ and $\mathbf{h}_2$ in $R(\mathcal{C})$ neither $\mathrm{supp}(\mathrm{head}(\mathbf{h}_1)) \subseteq \mathrm{supp}\,(\mathrm{head}(\mathbf{h}_2))$ nor $\mathrm{supp}(\mathrm{head}(\mathbf{h}_2)) \subseteq \mathrm{supp}\,(\mathrm{head}(\mathbf{h}_1))$ is verified.

Border of a code

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 Barg's GDD**.

Instituto de Matemáticas

Further topics

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

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

$\neq$ 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 $I(H^\perp)$