Betti Numbers and Generalized Hamming Weights

Irene Márquez-Corbella and Edgar Martínez-Moro

Dept. of Mathematics, Statistics and O. Research, University of La Laguna, Spain. irene.marquez.corbella@ull.es
Institute of Mathematics, University of Valladolid, Spain. Edgar.Martinez@uva.es

We can associate to each linear code $\mathscr{C}$ defined over a finite field the matroid $M[H]$ of its parity check matrix H. For any matroid M one can define its generalized Hamming weights which are the same as those of the code $\mathscr{C}$. In [2] the authors show that the generalized Hamming weights of a matroid are determined by the $\mathbb{N}$-graded Betti numbers of the Stanley-Reisner ring of the simplicial complex whose faces are the independent set of M. In this talk we go a step further. Our practical results indicate that the generalized Hamming weights of a linear code $\mathscr{C}$ can be obtained from the monomial ideal associated with a test-set for $\mathscr{C}$. Moreover, recall that in [3] we use the Gröbner representation of a linear code $\mathscr{C}$ to provide a test-set for $\mathscr{C}$.

Our results are still a work in progress, but its applications to Coding Theory and Cryptography are of great value.

1 Notation and Prerequisites

We begin with an introduction of basic definitions and some known results. By $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{F}_q$ (where q is a primer power) we denote the set of positive integers, the set of integers and the finite field with q elements, respectively.

Definition 1 *A matroid M is a pair (E,I) consisting of a finite set E called ground set and a collection I of subsets of E called independent sets, satisfying the following conditions:*

1. *The empty set is independent, i.e. $\emptyset \in I$*
2. *If $A \in I$ and $B \subset A$, then $B \in I$*
3. *If $A,B \in I$ and $|A| < |B|$, then there exists $e \in B \setminus A$ such that $A \cup \{e\} \in I$*

Let $M = (E,I)$ be a matroid. A maximal independent subset of E is called a *basis* of M. A direct consequence of the previous definition is that all bases of M have the same cardinality. Thus, we define the *rank* of the matroid M as the cardinality of any basis of M, denoted by $\operatorname{rank}(M)$. A subset E that does not belong to I is called *dependent set*. Minimal dependent subsets of E are known as *circuits* of M. A set is said to be a *cycle* if it is a disjoint union of circuits. The collection of cycles of M is denoted by $\mathscr{C}(M)$. For all $\sigma \in E$, the *nulity function* of σ is given by $n(\sigma) := |\sigma| - \text{rank}(M_\sigma)$ with $\text{rank}(M_\sigma) = \max\{|A| \mid A \in I \text{ and } A \subset \sigma\}$, i.e. the restriction of $\text{rank}(M)$ to the subsets of σ.

Let us consider an $m \times n$ matrix A in $\mathbb{F}_q$ whose columns are indexed by $E = \{1, \dots, n\}$ and take I to be the collection of subsets J of E for which the column vectors $\{A_j \mid j \in J\}$ are linearly independent over $\mathbb{F}_q$. Then (E, I) defines a matroid denoted by $M[A]$. A matroid $M = (E, I)$ is $\mathbb{F}_q$-representable if it is isomorphic to $M[A]$ for some $A \in \mathbb{F}_q^{m \times n}$. Then the matrix A is called the representation matrix of M. The following well known results describes the relation between the colleciton of all cycles of a matroid M and its representation matrix.

Proposition 1 *Let $M = (E, I)$ be a $\mathbb{F}_q$-representable matroid. Then $\mathscr{C}(M)$ is the null space of a representation matrix of M. Furthermore, the dimension of $\mathscr{C}(M)$ is $|E| - \text{rank}(M)$.*

Let Δ be a simplicial complex on the finite ground set E. Let $\mathbb{K}$ be a field and let $\mathbf{x}$ be the indeterminates $\mathbf{x} = \{x_e \mid e \in E\}$. The *Stanley-Reisner* ideal of Δ is, by definition,

$$I_\Delta = \langle \mathbf{x}^\sigma \mid \sigma \notin \Delta \rangle$$

The *Stanley-Reisner ring* of I_Δ, denoted by R_Δ, is defined to be the quotient ring $R_\Delta = \frac{\mathbb{K}[\mathbf{x}]}{I_\Delta}$. This ring has a minimal free resolution as $\mathbb{N}^E$-graded module:

$$0 \longleftarrow R_\Delta \longleftarrow P_0 \longleftarrow P_1 \longleftarrow \cdots \longleftarrow P_l \longleftarrow 0$$

where each P_i is given by $P_i = \bigoplus_{\alpha \in \mathbb{N}^E} \mathbb{K}[\mathbf{x}](-\alpha)^{\beta_{i,\alpha}}$. We write $\beta_{i,\alpha}$ for the $\mathbb{N}^E$-graded Betti Numbers of Δ.

1.1 Matroids and Simplicial complex

A matroid $M = (E, I)$ is a simplicial complex whose faces are the independent sets. Thus, $I_M := \langle \mathbf{x}^\sigma \mid \sigma \in \mathscr{C} \rangle$ where $\mathscr{C}$ is the set of all circuits of M. Define $N_i = \{\sigma \in N \mid n(\sigma) = d\}$.

Theorem 1 ([2]Theorem 1) *Let M be a matroid on the ground set E. Let $\sigma \subset E$. Then, $\beta_{i,\sigma} \neq 0$ if and only if σ is minimal in N_i.*

Definition 2 *Let $M = (E, I)$ be a matroid, we define the generalized Hamming weights of M to be $d_i = \min\{|\sigma| \mid n(\sigma) = i\}$.*

Corollary 1 *Let M be a matroid on the ground set E. Then,*

$$d_i = \min\{d \mid \beta_{i,d} \neq 0 \quad \textit{for all} \quad 1 \leq i \leq |E| - \text{rank}(M)\}.$$

1.2 Matroids and linear codes

An $[n,k]_q$ linear code $\mathscr{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$. We define a *generator matrix* of $\mathscr{C}$ to be a $k\times n$ matrix G whose row vectors span $\mathscr{C}$, while a *parity check matrix* of $\mathscr{C}$ is an $(n-k)\times n$ matrix H whose null space is $\mathscr{C}$.

Let us denote by $\mathrm{d}_H(\cdot,\cdot)$ and $\mathrm{w}_H(\cdot)$ the *Hamming distance* and the *Hamming weight* on $\mathbb{F}_q^n$, respectively. We write d for the *minimum Hamming distance* of the code $\mathscr{C}$, which is equal to its minimum weight. Thus, the error correcting capability of $\mathscr{C}$ is $t=\left\lfloor\frac{d-1}{2}\right\rfloor$ where $\lfloor\cdot\rfloor$ is the greatest integer function. For every codeword $\mathbf{c}\in\mathscr{C}$ its *support*, $\mathrm{supp}(\mathbf{c})$, is defined as its support as a vector in $\mathbb{F}_q^n$, i.e. $\mathrm{supp}(\mathbf{c})=\{i\mid c_i\neq 0\}$. We will denote by $\mathscr{M}_{\mathscr{C}}$ the set of codewords of minimal support of $\mathscr{C}$.

A *test-set* $\mathscr{T}_{\mathscr{C}}$ for $\mathscr{C}$ is a set of codewords such that for every word $\mathbf{y}\in\mathbb{F}_q^n$, either $\mathbf{y}$ belongs to the set of coset leaders, or there exists an element $\mathbf{t}\in\mathscr{T}_{\mathscr{C}}$ such that $\mathrm{w}_H(\mathbf{y}-\mathbf{t})<\mathrm{w}_H(\mathbf{y})$.

Definition 3 *The r^{th} generalized Hamming weight of $\mathscr{C}$ denoted by $d_r(\mathscr{C})$ is the smallest support of an r-dimensional subcode of $\mathscr{C}$. That is,*

$$d_r(\mathscr{C})=\min\{\mathrm{supp}(D)\mid D\subseteq\mathscr{C} \textit{ and } \mathrm{rank}(D)=r\}$$

In [3] the authors associate a binomial ideal to an arbitrary linear code provided by the rows of a generator matrix and the relations given by the additive table of the defining field.

Let $\mathbf{X}$ denote n vector variables $X_1,\ldots,X_n$ such that each variable X_i can be decomposed into $q-1$ components $x_{i,1},\ldots,x_{i,q-1}$ with $i=1,\ldots,n$. A monomial in $\mathbf{X}$ is a product of the form:

$$\mathbf{X}^{\mathbf{u}}=X_1^{\mathbf{u}_1}\cdots\mathbf{X}_n^{\mathbf{u}_n}=\left(x_{1,1}^{u_{1,1}}\cdots x_{1,q-1}^{u_{1,q-1}}\right)\cdots\left(x_{n,1}^{u_{n,1}}\cdots x_{n,q-1}^{u_{n,q-1}}\right)$$

where $\mathbf{u}\in\mathbb{Z}_{\geq 0}^{n(q-1)}$. The total degree of $\mathbf{X}^{\mathbf{u}}$ is the sum $\deg(\mathbf{X}^{\mathbf{u}})=\sum_{i=1}^n\sum_{j=1}^{q-1}u_{i,j}$. When $\mathbf{u}=(0,\ldots,0)$, note that $\mathbf{X}^{\mathbf{u}}=1$. Then, the polynomial ring $\mathbb{K}[\mathbf{X}]$ is the set of all polynomials in $\mathbf{X}$ with coefficients in $\mathbb{K}$.

Recall that the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic. A generator of the cyclic group $\mathbb{F}_q^*$ is called a primitive element of $\mathbb{F}_q$, i.e. $\mathbb{F}_q$ consist of 0 and all powers from 1 to $q-1$ of that primitive element. Let α be a primitive element of $\mathbb{F}_q$. We define by $\mathscr{R}_{X_i}$, the set of all the binomials on the variables X_i associated to the relations given by the additive table of the field $\mathbb{F}_q=\left\langle\alpha^j\mid j=1,\ldots,q-1\right\rangle\cup\{0\}$, i.e.

$$\mathscr{R}_{X_i}=\left\{\ \{x_{i,u}x_{i,v}-x_{i,w}\mid\alpha^u+\alpha^v=\alpha^w\}\quad\cup\quad\{x_{i,u}x_{i,v}-1\mid\alpha^u+\alpha^v=0\}\ \right\}$$

with $i = 1, \dots, n$. Note that there are $\binom{q}{2}$ different binomials in $\mathscr{R}_{X_i}$. We define $\mathscr{R}_{\mathbf{X}}$ as the ideal generated by the union of all binomial ideals $\mathscr{R}_{X_i}$, i.e. $\mathscr{R}_{\mathbf{X}} = \left\langle \cup_{i=1}^{n} \mathscr{R}_{X_i} \right\rangle$

We will use the following characteristic crossing functions. These applications aim at describing a one-to-one correspondence between the finite field $\mathbb{F}_q$ with q elements and the standard basis of $\mathbb{Z}^{q-1}$, denoted as $E_q = \{\mathbf{e}_1, \dots, \mathbf{e}_{q-z}\}$ where $\mathbf{e}_i$ is the unit vector with a 1 in the i-th coordinate and 0's elsewhere.

$$\Delta : \quad \mathbb{F}_q \quad \longrightarrow \quad E_q \cup \{\mathbf{0}\} \subseteq \mathbb{Z}^{q-1} \qquad \text{and} \qquad \nabla : \quad E_q \cup \{\mathbf{0}\} \quad \longrightarrow \quad \mathbb{F}_q$$

1. The map Δ replaces the element $\mathbf{a} = \alpha^i \in \mathbb{F}_q$ by the vector $\mathbf{e}_i$ and $0 \in \mathbb{F}_q$ by the zero vector $\mathbf{0} \in \mathbb{Z}^{q-1}$.

2. The map ∇ recovers the element $\alpha^j \in \mathbb{F}_q$ from the unit vector $\mathbf{e}_j$ and the zero element $0 \in \mathbb{F}_q$ from the zero vector $\mathbf{0} \in \mathbb{Z}^{q-1}$.

These maps will be used with matrices and vectors acting coordinate-wise. Although Δ is not a linear function. Note that we have:

$$\mathbf{X}^{\Delta \mathbf{a}} \cdot \mathbf{X}^{\Delta \mathbf{b}} = \mathbf{X}^{\Delta \mathbf{a} + \Delta \mathbf{b}} = \mathbf{X}^{\Delta(\mathbf{a}+\mathbf{b})} \mod \mathscr{R}_{\mathbf{X}} \text{ for all } \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n.$$

Let $\mathscr{C}$ be an $[n,k]_q$ linear code. We define the *ideal associated* to $\mathscr{C}$ as the binomial ideal:

$$I(\mathscr{C}) = \left\langle \left\{ \mathbf{X}^{\Delta \mathbf{a}} - \mathbf{X}^{\Delta \mathbf{b}} \mid \mathbf{a} - \mathbf{b} \in \mathscr{C} \right\} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]$$

Given the rows of a generator matrix $\mathscr{C}$, labelled by $\{\mathbf{w}_1, \dots, \mathbf{w}_k\} \subseteq \mathbb{F}_q^n$, we define the following ideal:

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

Theorem 2 *[3][Theorem 2.3]* $I(\mathscr{C}) = I_+(\mathscr{C})$

Remark 1 *In the binary case, given a generator matrix $G \in \mathbb{F}_2^{k \times n}$ of an $[n,k]_2$-code $\mathscr{C}$ and let label its rows by $\{\mathbf{w}_1, \dots, \mathbf{w}_k\} \subseteq \mathbb{F}_2^n$. We define the ideal associated to $\mathscr{C}$ as the binomial ideal:*

$$I_+(\mathscr{C}) = \left\langle \ \left\{ \mathbf{X}^{\mathbf{w}_i} - 1 \right\}_{i=1,\dots,k} \ \cup \ \left\{ x_i^2 - 1 \right\}_{i=1,\dots,n} \ \right\rangle \subseteq \mathbb{K}[\mathbf{X}]$$

Now, let $\mathscr{G} = \{g_1, \dots, g_s\}$ be the reduced Gröbner basis of the ideal $I_+(\mathscr{C})$ with respect to $\succ$, where we take $\succ$ to be any degree compatible ordering on $\mathbb{K}[\mathbf{X}]$ with

$X_1 \prec \ldots \prec X_n$. By Lemma [3][Lemma 3.3] we know that all elements of $\mathscr{G} \setminus \mathscr{R}_{\mathbf{X}}$ are in standard form, so for $g_i \in \mathscr{G} \setminus \mathscr{R}_{\mathbf{X}}$ with $i = 1, \ldots, s$, we define

$$g_i = \mathbf{X}^{\Delta \mathbf{g}_i^+} - \mathbf{X}^{\Delta \mathbf{g}_i^-} \quad \text{with} \quad \mathbf{X}^{\Delta \mathbf{g}_i^+} \succ \mathbf{X}^{\Delta \mathbf{g}_i^-} \quad \text{and} \quad \mathbf{g}_i^+ - \mathbf{g}_i^- \in \mathscr{C}.$$

Using [3][Proposition 4], we know that the set $\mathscr{T} = \left\{ \mathbf{g}_i^+ - \mathbf{g}_i^- \mid i = 1, \ldots, s \right\}$ is a test-set for $\mathscr{C}$.

Example 1 *Consider the* $[6,3,2]_2$ *binary code* $\mathscr{C}$ *defined by the following generator matrix:*

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

Let us label the rows of G *by* $\mathbf{w}_1$ *and* $\mathbf{w}_2$*. By the previous theorem, the ideal associated to the linear code* $\mathscr{C}$ *may be defined as the following ideal:*

$$\begin{array}{rcl} I_+(\mathscr{C}) & = & \left\langle \ \left\{ \mathbf{X}^{\mathbf{w}_i} - 1 \right\}_{i=1,2} \quad \cup \quad \left\{ \mathscr{R}_{X_i} \right\}_{i=1,\ldots,6} \ \right\rangle \\ & = & \left\langle \ \left\{ \begin{array}{c} x_1 x_6 - 1 \\ x_2 x_3 x_5 - 1 \\ x_4 x_5 x_6 - 1 \end{array} \right\} \quad \cup \quad \left\{ x_i^2 - 1 \right\}_{i=1,\ldots,6} \ \right\rangle \end{array}$$

If we compute a reduced Gröbner basis $\mathscr{G}$ *of* $I_+(\mathscr{C})$ *we obtained a test-set consisting of* 4 *codewords:*

$$\mathscr{T}_{\mathscr{C}} = \{(1,0,0,0,0,1), (0,1,1,0,1,0), (0,1,1,1,1,0,1), (0,0,0,1,1,1)\}$$

For fuller discussion of this algebraic structure see [4, 1] and the references therein.

The connection between linear codes and matroids will turn out to be fundamental for the development of the subsequent results. Thus, a brief review will be provided here.

Given an $m \times n$ matrix H in $\mathbb{F}_q$, then H can be seen not only as the representation matrix of the $\mathbb{F}_q$-representable matroid $M[H]$ but also as a parity check matrix of an $[n,k]$-code $\mathscr{C}$. Furthermore, there exists a one to one correspondence between $\mathbb{F}_q$-representable matroids and linear codes, since for any $H, H' \in \mathbb{F}_q^{m \times n}$, $M[H] = M[H']$ if an only if H and H' are parity check matrices of the same code $\mathscr{C}$. This association enables us to work with $\mathbb{F}_q$-representable matroids and linear codes as if they were the same object and thus we can conclude some properties of linear codes using tools from matroid theory and vice-versa.

2 Our Conjecture

Let $M = (E, I)$ be a matroid and $\mathscr{C}$ be the set of all circuits of M. Consider $\mathscr{T}$ a collection of cycles of M with the following property: $\bigcup_{\tau\in\mathscr{C}} \tau = \bigcup_{\tau\in\mathscr{T}} \tau$. We define the ideal $I_{\mathscr{T}} = \langle \mathbf{x}^{\sigma} \mid \sigma \in \mathscr{T} \rangle$.

Conjecture 1 *Let $\beta'_{i,\alpha}$ the $\mathbb{N}^E$-graded betti number of $I_{\mathscr{T}}$, related with the minimal free resolution of $R = \frac{\mathbb{K}[X]}{I_{\mathscr{T}}}$ as $\mathbb{N}^E$-graded module. Then, we have a similar result as Theorem 1 and Corollary 1.*

If we talk about linear codes, the conjecture allows us to compute the set of generalized Hamming weight of a linear code $\mathscr{C}$ using a Test-set for $\mathscr{C}$, in other words, by computing a Grobner basis of the ideal associated to $\mathscr{C}$.

Corollary 2 *Let $\mathscr{T}_{\mathscr{C}}$ be a test-set for the linear code $\mathscr{C}$. Consider the monomial ideal: $I_{\mathscr{T}_{\mathscr{C}}} = \langle \mathbf{x}^{\sigma} \mid \sigma \in \mathscr{T}_{\mathscr{C}} \rangle$. Let $\beta'_{i,\alpha}$ the $\mathbb{N}^E$-graded betti numbers of $I_{\mathscr{T}_{\mathscr{C}}}$. Then,*

$$d_i(\mathscr{C}) = \min\left\{d \mid \beta'_{i,d} \neq 0\right\} \text{ for } 1 \leq i \leq n-k$$

Example 2 *Now we use the same code of Example 1. In this case the support of a test-set $T_{\mathscr{C}}$ is given by: $\mathscr{T} = \{\{2,3,5\},\{2,3,4,6\},\{4,5,6\},\{1,6\}\}$ i.e. we consider the ideal: $I_{\mathscr{T}} = \langle x_2x_3x_5, x_2x_3x_4x_6, x_4x_5x_6, x_1x_6\rangle \subseteq \mathbb{K}[x_1,\ldots,x_6]$. We get the Betti diagram*

	1	2	3
1	1		
2	2	1	
3	1	4	2

Thus $\beta'_{1,2}$, $\beta'_{2,4}$ and $\beta'_{3,6}$ are the minimal $\beta'_{i,d} \neq 0$ with $i = 1,2,3$. Or equivalently, $d_1 = 2$, $d_2 = 4$ and $d_3 = 6$.

References

[1] M. Borges-Quintana, M.A. Borges-Trenard, P. FitzPatrick and E. Martínez-Moro. *Gröbner bases and combinatorics for binary codes*. Applicable Algebra in Engineering, Communication and Computing. 19(5): 393-411, 2008.

[2] J. T. Johnsen and H. Verdure. *Hamming weights and Betti numbers of Stanley–Reisner rings associated to matroids*. Applicable Algebra in Engineering, Communication and Computing. 24(1): 73-93, 2013.

[3] I. Márquez-Corbella, E. Martínez-Moro and E. Suárez-Canedo. *On the ideal associated to a linear code*. Advances in Mathematics of Communications (AMC). 10(2): 229-254, 2016.

[4] I. Márquez-Corbella and E. Martínez-Moro. *Algebraic structure of the minimal support codewords set of some linear codes*. Advances in Mathematics of Communications (AMC). 5(2): 233-244, 2011.