

Betti Numbers and Generalized Hamming Weights

Irene Márquez-Corbella, Edgar Martínez-Moro

► **To cite this version:**

Irene Márquez-Corbella, Edgar Martínez-Moro. Betti Numbers and Generalized Hamming Weights. 22nd Conference on Applications of Computer Algebra (ACA 2016), Aug 2016, Kassel, Germany. hal-01409298

HAL Id: hal-01409298

<https://hal.inria.fr/hal-01409298>

Submitted on 5 Dec 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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 \mathcal{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 \mathcal{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 \mathcal{C} can be obtained from the monomial ideal associated with a test-set for \mathcal{C} . Moreover, recall that in [3] we use the Gröbner representation of a linear code \mathcal{C} to provide a test-set for \mathcal{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 $\text{rank}(M)$. 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 $\mathcal{C}(M)$. For all $\sigma \in E$, the *nullity 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 collection 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 $\mathcal{C}(M)$ is the null space of a representation matrix of M . Furthermore, the dimension of $\mathcal{C}(M)$ 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:

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

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, $I_M := \langle \mathbf{x}^\sigma \mid \sigma \in \mathcal{C} \rangle$ where \mathcal{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,*

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

1.2 Matroids and linear codes

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

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

A *test-set* $\mathcal{T}_{\mathcal{C}}$ for \mathcal{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 $\mathbf{t} \in \mathcal{T}_{\mathcal{C}}$ such that $w_H(\mathbf{y} - \mathbf{t}) < w_H(\mathbf{y})$.

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

$$d_r(\mathcal{C}) = \min \{ \text{supp}(D) \mid D \subseteq \mathcal{C} \text{ and } \text{rank}(D) = r \}$$

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

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

where $\mathbf{u} \in \mathbb{Z}_{\geq 0}^{n(q-1)}$. The total degree of $\mathbf{X}^{\mathbf{u}}$ is the sum $\text{deg}(\mathbf{X}^{\mathbf{u}}) = \sum_{i=1}^n \sum_{j=1}^{q-1} u_{i,j}$. When $\mathbf{u} = (0, \dots, 0)$, 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 \mathcal{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 $\mathbb{F}_q = \langle \alpha^j \mid j = 1, \dots, q - 1 \rangle \cup \{0\}$, i.e.

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

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

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.

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

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:

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

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

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

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

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

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

Remark 1 In the binary case, given a generator matrix $G \in \mathbb{F}_2^{k \times n}$ of an $[n, k]_2$ -code \mathcal{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 \mathcal{C} as the binomial ideal:

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

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

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

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

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

Example 1 Consider the $[6, 3, 2]_2$ binary code \mathcal{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 \mathcal{C} may be defined as the following ideal:

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

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

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

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 \mathcal{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 and only if H and H' are parity check matrices of the same code \mathcal{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 \mathcal{C} be the set of all circuits of M . Consider \mathcal{T} a collection of cycles of M with the following property: $\bigcup_{\tau \in \mathcal{C}} \tau = \bigcup_{\tau \in \mathcal{T}} \tau$. We define the ideal $I_{\mathcal{T}} = \langle \mathbf{x}^\sigma \mid \sigma \in \mathcal{T} \rangle$.

Conjecture 1 *Let $\beta'_{i,\alpha}$ the \mathbb{N}^E -graded betti number of $I_{\mathcal{T}}$, related with the minimal free resolution of $R = \frac{\mathbb{K}[X]}{I_{\mathcal{T}}}$ 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 \mathcal{C} using a Test-set for \mathcal{C} , in other words, by computing a Grobner basis of the ideal associated to \mathcal{C} .

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

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

Example 2 *Now we use the same code of Example 1. In this case the support of a test-set $T_{\mathcal{C}}$ is given by: $\mathcal{T} = \{\{2, 3, 5\}, \{2, 3, 4, 6\}, \{4, 5, 6\}, \{1, 6\}\}$ i.e. we consider the ideal: $I_{\mathcal{T}} = \langle x_2x_3x_5, x_2x_3x_4x_6, x_4x_5x_6, x_1x_6 \rangle \subseteq \mathbb{K}[x_1, \dots, x_6]$. 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. *Grobner 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 code-words set of some linear codes*. Advances in Mathematics of Communications (AMC). 5(2): 233-244, 2011.