Free Resolutions and Generalized Hamming Weights

Coding Theory and Cryptography – A conference in honor of Joachim Rosenthal's 60th birthday. Zurich, July 2022

I. García-Marco, I. Márquez- Corbella, E. Martínez-Moro y Y. Pitones

imUVa Instituto de Investigación en Matemáticas

Universidad de Valladolid

Abstract

In this work, we explore the relationship between free resolution of some monomial ideals and Generalized Hamming Weights (GHWs) of binary codes. More precisely, we look for a structure smaller than the set of codewords of minimal support that provides us some information about the GHWs. We prove that the first and second generalized Hamming weight of a binary linear code can be computed (by means of a graded free resolution) from a set of monomials associated to a binomial ideal related with the code. Moreover, the remaining weights are bounded by the Betti numbers for that set.

This work was partially supported by the Spanish MICINN PID2019-105896GB-I00 and MASCA and MACACO (ULL Research Projects). Third author was supported in part by Grant PGC2018-096446-B-C21 funded by MCIN/AEI/10.13039/501100011033 and by "ERDF A way of making Europe". Fourth author was supported by SEGIB-Fundación Carolina Grant and SNI México.

Introduction

Let $\mathbb{F}_q$ be a finite field with q elements. Given two vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, the Hamming distance between $\mathbf{x}$ and $\mathbf{y}$ is defined as

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i \mid x_i \neq y_i\}|,$$

where $|\cdot|$ denotes the cardinality of the set.

The Hamming weight of $\mathbf{x}$ is given by $\mathrm{w}_H(\mathbf{x}) = d_H(\mathbf{x}, \mathbf{0})$, where $\mathbf{0}$ denotes de zero vector in $\mathbb{F}_q^n$. The support of $\mathbf{x}$ is the set $\mathrm{supp}(\mathbf{x}) = \{i \mid x_i \neq 0\}$. A linear subespace $\mathcal{C}$ in $\mathbb{F}_q^n$ is called a linear code.

The basic parameters of $\mathcal{C}$ are length, dimension, and minimum distance, which are denoted by $n(\mathcal{C}), k(\mathcal{C})$, and $\delta(\mathcal{C})$, respectively. In this case, we call $\mathcal{C}$ an $[n(\mathcal{C}), k(\mathcal{C}), \delta(\mathcal{C})]_q$ linear code.

Introduction (Cont.)

We define a generator matrix of $\mathcal{C}$ to be a matrix G over $\mathbb{F}_q$ of size $k(\mathcal{C}) \times n(\mathcal{C})$ whose row vectors span $\mathcal{C}$, while a *parity check matrix* of $\mathcal{C}$ is a matrix H over $\mathbb{F}_q$ of size $(n(\mathcal{C}) - k(\mathcal{C})) \times n(\mathcal{C})$ whose null space is $\mathcal{C}$.

We will say that a codeword $\mathbf{m} \in \mathcal{C}$ is a minimal support codeword if it is non-zero and $\mathrm{supp}(\mathbf{m})$ is not contained in the supports of any other codewords of $\mathcal{C}$. We will denote by $\mathcal{M}_{\mathcal{C}}$ the set of codewords of minimal support of $\mathcal{C}$.

Introduction (Cont.)

Let $\mathcal{C}$ be a linear code and D be a subcode of $\mathcal{C}$, we define the support of D, denoted $\mathrm{supp}(D)$ as the set of not-always-zero bit positions of D, i.e.,

$$\mathrm{supp}(D) = \{i \mid \exists \mathbf{c} \in D \text{ with } c_i \neq 0\}.$$

Note that if D is a one-dimensional subcode then, the support of D is equal to the Hamming weight of the nonzero codeword. Based on this idea, we define the h-th generalized Hamming weight of $\mathcal{C}$, denoted $d_h(\mathcal{C})$, to be the size of the smallest support of an h-dimensional subcode of $\mathcal{C}$ with $h = 1, 2, \ldots, k(\mathcal{C})$. i.e. let D_h be the set of all linear subspaces of the linear code $\mathcal{C}$ of dimension h then,

$$d_h(\mathcal{C}) = \min\{|supp(E)| \mid E \in D_h\}.$$

Introduction (Cont.)

Thus $d_1(\mathcal{C}) = \delta(\mathcal{C})$. Moreover [Wei 91]

1. $1 \leq d_1(\mathcal{C}) < d_2(\mathcal{C}) < \ldots < d_{k(\mathcal{C})}(\mathcal{C}) \leq n(\mathcal{C})$
2. **(Generalized Singleton Bound)** $d_h(\mathcal{C}) \leq n(\mathcal{C}) - k(\mathcal{C}) + h$. When $h = 1$, this is the Singleton bound.

$\mathcal{C}$ is nondegenerate if and only if $d_{k(\mathcal{C})} = n(\mathcal{C})$.

There are few families of codes for which it is known the complete generalized weight hierarchy as for example: first-order Reed-Muller codes, binary Reed-Muller codes, Hamming code and its dual, Extended Hamming codes, Golay code. However, for the general case, few properties are known.

GHW and simplicial compl.

Notation.- From now on, given a positive integer ℓ, we define $[\ell] = \{1, \ldots, \ell\}$ and $[\ell]_0 = \{0, \ldots, \ell\}$.

Let $\mathcal{C}$ be a $[n, k]_q$ code and let H be a parity check matrix of $\mathcal{C}$. Let H_i denote the i-th column of H and define

$$\Delta = \left\{ \sigma \in 2^{[n]} \mid \{H_i \mid i \in \sigma\} \text{ is linearly independent over } \mathbb{F}_q \right\}.$$

Then, the pair $\mathcal{M} = ([n], \Delta)$ is the matroid associated to the code $\mathcal{C}$. The collection Δ of subsets of $[n]$ are called *independent sets* of this matroid. Minimal dependent subsets of $[n]$ are known as circuits of $\mathcal{M}$.
Moreover, Δ is a simplicial complex.

GHW and simplicial compl.

We denote by I_Δ the ideal of the polynomial ring $R = \mathbb{K}[X_1, \ldots, X_n]$ generated by all square-free monomials supported on elements that are not in Δ, i.e.

$$\prod_{i \in \tau} X_i \text{ with } \tau \in 2^{[n]} \setminus \Delta$$

That is, I_Δ is the ideal generated by monomials supported on the circuits of $\mathcal{M}$, or equivalently supported on codewords of minimal support of $\mathcal{C}$.

$$I_\Delta = \left\langle \prod_{i \in \mathrm{supp}(\mathbf{c})} X_i \mid \mathbf{c} \in \mathcal{M}_\mathcal{C} \right\rangle$$

GHW and simplicial compl. (Cont.)

The quotient $R_\Delta = R/I_\Delta$ is called the Stanley-Reisner ring associated to Δ. R_Δ is a finitely generated standard graded $\mathbb{K}$-algebra of dimension $n(\mathcal{C}) - k(\mathcal{C})$. Thus, it has a minimal graded free resolution. Moreover, Δ is shellable and this implies that R_Δ is Cohen-Macaulay.

GHW and simplicial compl. (Cont.)

$$F_{k(\mathcal{C})} \longrightarrow F_{k(\mathcal{C})-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow R_\Delta \longrightarrow 0$$

where $F_0 = R$ and each F_i is a graded free R-module of the form

$$F_i = \bigoplus_{j \in \mathbb{Z}} R(-j)^{\beta_{i,j}} \text{ for } i \in [k(\mathcal{C})]_0 \,.$$

We will call it graded minimal free resolution of $\mathcal{C}$. The nonnegative integers $\beta_{i,j}$ are called Betti numbers of $\mathcal{C}$ and they depend only on $\mathcal{C}$ and not on the choice of H or the minimal free resolution of R_Δ.

GHW and simplicial compl. (Cont.)

Johnsen and Verdure showed that the Betti numbers of a code $\mathcal{C}$ contain information about all the generalized Hamming weights $d_i(\mathcal{C})$ with $i \in [k(\mathcal{C})]$.

§Result .-

$$d_i(\mathcal{C}) = \min\{j \mid \beta_{i,j} \neq 0\} \text{ for } j \in [k(\mathcal{C})]\}$$

From this result it is clear that explicit determination of Betti numbers of codes completely determine the code parameters of a linear code. However, this is usually a hard problem except in some special cases.

GHW and simplicial compl. (Cont.)

For example they explicitly determine the Betti Numbers for MDS codes since the minimal free resolution of these codes is linear. They alos proved that the resolution of the first order Reed-Muller code is pure. And a similar result can be deduced for constant weight codes. Thus, simplex codes or dual Hamming codes, which are constant weight codes also have pure resolution, although not necessarily linear.

The resolution is said to be pure of type $(d_0, \ldots, d_{k(\mathcal{C})})$ if for each $i \in [k]_0$, the Betti number $\beta_{i,j}$ is nonzero if and only if $j = d_i$. If, in addition $d_1, \ldots, d_k$ are consecutive, then the resolution is said to be linear.

The ideal associated with a code

We define the ideal associated to $\mathcal{C}$ as the binomial ideal

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

Note that $I(\mathcal{C})$ is a zero-dimensional ideal since the quotient ring $\mathbb{K}[X]/I(\mathcal{C})$ is a finite-dimensional vector space. Moreover, its dimension is equal to the number of *cosets* in $\mathbb{F}_2^{n(\mathcal{C})}/\mathcal{C}$.

§Result .- Let $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ be the row vectors of a generator matrix for $\mathcal{C}$. Then

$$I(\mathcal{C}) = \left\langle \{X^{\mathbf{w}_i} - 1\}_{i \in [k(\mathcal{C})]} \cup \{x_i^2 - 1\}_{i \in [n(\mathcal{C})]} \right\rangle$$

The ideal associated with a code (Cont)

An ordering $\prec$ on $\mathbb{K}[X]$ is said to be degree (weight) compatible if $\deg(X^{\mathbf{a}}) < \deg(X^{\mathbf{b}})$ implies that $X^{\mathbf{a}} \prec X^{\mathbf{b}}$ for all monomials $X^{\mathbf{a}}, X^{\mathbf{b}} \in \mathbb{K}[X]$.

From now on, let $\mathcal{G}_\prec$ be the reduced Gröbner basis of the ideal $I(\mathcal{C})$ with respect to $\prec$, where we take $\prec$ to be any degree compatible ordering on $\mathbb{K}[X]$. We define the set

$$\mathcal{B}_\prec = \mathcal{G}_\prec - \left\{x_i^2 - 1\right\}_{i \in [n(\mathcal{C})]}.$$

The test-set $\mathcal{T}_\prec$ is the set of supports of binomials in $\mathcal{B}_\prec$.

The ✗ conjecture

Let $\mathcal{C}$ be the binary non-degenerate $[6, 3]$-code with parity check matrix

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

The Stanley-Reisner ideal is $R_\Delta = R/I_\Delta$ where

$$I_\Delta = \left\langle \; x_1x_6, x_4x_5x_6, x_1x_4x_5, x_2x_3x_5, x_2x_3x_4x_6, x_1x_2x_3x_4 \; \right\rangle$$

If we compute a graded minimal free resolution of R_Δ

$$0 \longrightarrow R(-6)^4 \longrightarrow R(-4)^2 \oplus R(-5)^7 \longrightarrow R(-2)^1 \oplus R(-3)^3 \oplus R(-4)^2 \longrightarrow R \longrightarrow R_\Delta \longrightarrow 0$$

and we get $d_1(\mathcal{C}) = 2$, $d_2(\mathcal{C}) = 4$, $d_3(\mathcal{C}) = 6$.

The ✗ conjecture (Cont.)

While if we compute a reduced Gröbner basis of $I(\mathcal{C})$ with respect to the degree reverse lexicographical order we obtain a test-set given by

$$I_{\mathcal{T}} = \left\langle \; x_1x_6, x_2x_3x_5, x_2x_3x_4x_6, x_4x_5x_6 \; \right\rangle$$

Now we compute a graded minimal free resolution of $R_{\mathcal{T}}$ we get

$$0 \longrightarrow R(-6)^2 \longrightarrow R(-4) \oplus R(-5)^4 \longrightarrow R(-2)^1 \oplus R(-3)^2 \oplus R(-4)^1 \longrightarrow R \longrightarrow R_{\Delta} \longrightarrow 0$$

and we recover $d_1(\mathcal{C}) = 2$, $d_2(\mathcal{C}) = 4$, $d_3(\mathcal{C}) = 6$.

The ✗ conjecture (Cont.)

Let $\mathcal{C}$ be the binary non-degenerate $[10, 7]$-code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{7\times 10}$$

The ✗ conjecture (Cont.)

If we compute a graded minimal free resolution of R_Δ we get the following Betti diagram

	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	0	4	0	0	0	0	0	0
2	0	18	48	32	7	0	0	0
3	0	20	214	637	874	637	242	38

thus $d_1(\mathcal{C}) = 2$, $d_2(\mathcal{C}) = 4$, $d_3(\mathcal{C}) = 5$, $d_4(\mathcal{C}) = 6$, $d_5(\mathcal{C}) = 8$, $d_6(\mathcal{C}) = 9$, $d_7(\mathcal{C}) = 10$.

The ✗ conjecture (Cont.)

While if we compute a reduced Gröbner basis of $I(\mathcal{C})$ with respect to the degree reverse lexicographical order we obtain a test-set with the following Betti diagram.

	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	0	4	0	0	0	0	0
2	0	4	14	5	0	0	0
3	0	2	23	56	48	17	2

Thus, we get $d_1(\mathcal{C}), d_2(\mathcal{C}), d_3(\mathcal{C})$ but not $d_i(\mathcal{C})$ for $i = 4, 5, 6, 7$.

d_1 and d_2 ✓

§Result [García-Márquez-M.-Pitones].- Let $\mathcal{C} \subseteq \mathbb{F}_2^n$ be a binary code, $\prec$ a degree compatible monomial order and Let $\mathcal{T}$ denote the $\mathcal{G}_\prec$-test and $M := \langle \{X^{\mathbf{c}} \mid \mathbf{c} \in \mathcal{T}\} \rangle$. If we consider a minimal graded free resolution of R/M $0 \longrightarrow F_p \longrightarrow \cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow R \longrightarrow R/M \longrightarrow 0$, where each F_i is a graded free R-module of the form $F_i = \bigoplus_{j \in \mathbb{N}} R(-j)^{\beta_{i,j}(R/M)}$ for $i \in [p]_0$. Then,

- $p \leq k$
- $d_i(\mathcal{C}) \leq \min\{j \mid \beta_{i,j}(R/M) \neq 0\}$ *for all* $j \in \{3, \ldots, p\}$, and
- $d_i(\mathcal{C}) = \min\{j \mid \beta_{i,j}(R/M) \neq 0\}$, *for* $i = 1, 2$.

Note that computing the test-set is much more 'easy' than the set of minimal code words. Anyway one can not expect it to be computationally affordable since it is an NP-problem.

More conjectures

- What is in between $\mathcal{T}_\prec$ and $\mathcal{M}$? A possible candidate fot that intermediate set could be the union of all $\mathcal{G}_\prec$-test sets for all $\prec$ degree compatible orderings. In general, this set can be smaller than the whole set of codewords of minimal support.
- Let $\mathcal{C} \subseteq \mathbb{F}_2^n$ be a binary code, $\prec$ a degree compatible monomial order in R. Consider the $\mathcal{G}_\prec$-test set T and define the square-free monomial ideal

$$M := \langle \{X^{\mathbf{c}} \mid \mathbf{c} \in T\} \rangle \subseteq R.$$

  Is $d_3(\mathcal{C}) = \min\{i \mid \beta_{3,i}(R/M) \neq 0\}$?
- Can we characterize when both resolutions have not the *same size* or the *non-zero Betti numbers are in the same position on the Betti table*?

More conjectures

- When they are not the same, do we always have one column less in the Betti table?
- Whenever $\mathrm{pd}(R/M) = k(\mathcal{C})$, is it true that

$$d_i(\mathcal{C}) = \min\{j \mid \beta_{i,j}(R/M) \neq 0\}$$

  for all $i \in \{1, \ldots, k(\mathcal{C})\}$?
- Gorla and Ravagnani recently extended and generalized the results of Johnsen and Verdure to compute generalized weights of a code with respect to a different notions of weight. Can these generalized weights be computed from a $\mathcal{G}_{\prec}$-test set of $\mathcal{C}$?
- ...

Paper and references

Thanks for your attention!