mathematics

MDPI

Article

Free Resolutions and Generalized Hamming Weights of Binary Linear Codes

Ignacio García-Marco [1], Irene Márquez-Corbella [1,*], Edgar Martínez-Moro [2] and Yuriko Pitones [3]

[1] Departamento Matemáticas, Estadística e I.O. and Instituto de Matemáticas y Aplicaciones (IMAULL), Sección de Matemáticas, Universidad de La Laguna, Apartado de Correos 456, 38200 La Laguna, Spain; iggarcia@ull.edu.es
[2] Institute of Mathematics, University of Valladolid, 47011 Valladolid, Spain; edgar.martinez@uva.es
[3] Departamento de Matemáticas, Universidad Autónoma Metropolitana-Iztapalapa, Mexico City 09310, Mexico; ypitones@xanum.uam.mx
* Correspondence: imarquec@ull.edu.es

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

Keywords: generalized Hamming weight; graded free resolution; second distance; binary code

MSC: 13P10; 94B05

Citation: García-Marco, I.; Márquez-Corbella, I.; Martínez-Moro, E.; Pitones, Y. Free Resolutions and Generalized Hamming Weights of Binary Linear Codes. *Mathematics* **2022**, *10*, 2079. https://doi.org/10.3390/math10122079

Academic Editor: Takayuki Hibi

Received: 2 May 2022
Accepted: 13 June 2022
Published: 15 June 2022

1. Introduction

The study of the Generalized Hamming Weights (GHWs) has been motivated by several applications in cryptography [1] and they characterize the performance of a linear code when used for a given channel. There are few families of codes for which the complete generalized weight hierarchy is known, for example: first-order Reed–Muller codes, binary Reed–Muller codes, the Hamming code and its dual, extended Hamming codes, and the Golay code; see [1]. On the other side, there has been extensive research on GHWs and the second distance, particularly for some classes of codes; see, for example, [2–12] and the references therein. However, for the general case of a linear code, few properties are known.

In their seminal paper [13], Johnsen and Verdure showed how the GHWs of a linear code could be computed from a minimal graded free resolution of a monomial ideal associated with the set of codewords of minimal support of the code. This paper outlines a great avenue of research; see, for example, [14–23]. The main drawbacks of the method proposed in [13] are that: (1) one needs to know the whole set of codewords of minimal support of the code, which is typically a huge set, and (2) one has to compute a minimal graded free resolution of an ideal with many generators, which has a high computational cost. Therefore, it would be desirable to find more efficient ways of computing the GHWs.

In the present work, we explore if one can find a set (smaller than the set of all codewords of minimal support) that provides us with some information on the GHWs in the case of binary codes. The selected set of codewords is the so-called Gröbner test set related to the binomial ideal associated with a code defined in [24]. In this paper, it was proven that one can decode using this set and that the minimal distance of the code (i.e., the first GHW) can be derived from it. Thus, somehow, some of the relevant information of the code lies in it. Moreover, in [24] it was also shown how to compute

the Gröbner test set avoiding some of the most common disadvantages when one uses a Gröbner basis. In this paper, we will show how one can also compute the second GHW of a binary linear code from the binomial ideal associated with the code without the need of computing the complete set of codewords of minimal support of the code, as in [13]. Moreover, in Theorem 3 we bound the remaining GHWs with the resolution of a monomial ideal associated with this new set.

1.1. Literature Review

We can group the references of this article into five blocks:

1. Applications of the results in other areas: why is it interesting to know the Generalized Hamming Weights (GHWs) of a linear code? [1].
2. Determination of the GHWs for particular families of linear codes [1–12].
3. How the GHWs of a linear code could be computed from a free resolution of a monomial ideal associated with the set of codewords of minimal support. After the original article [13], many others have elaborated on the topic [14–23].
4. Interest and algorithms to compute Gröbner test-sets for linear codes [24–26].
5. The rest of the references are reference books and articles on the topics of combinatorial commutative algebra, matroid and coding theory.

1.2. Motivation and Contribution

The study of GHWs for linear codes is a hot topic in Coding Theory since it can be applied in information theory. However, there are just a few families of codes for which the complete generalized weight hierarchy is known. In 2013, Johnsen and Verdure [13] showed how the GHWs of a linear code could be computed from a minimal graded free resolution of a monomial ideal associated with the set of codewords of minimal support of the code, denoted by $\mathcal{M}_{\mathcal{C}}$.

In this work, given a linear code $\mathcal{C}$, we look for a structure smaller than $\mathcal{M}_{\mathcal{C}}$ that provides us some information about the GHWs. In particular, for a long time the second and third authors have conjectured that a Gröbner test-set (which is a subset of $\mathcal{M}_{\mathcal{C}}$) determines the GHWs of a linear code (see Section 3 for a precise statement of the conjecture). This conjecture was supported by computational evidence but unfortunately this is not true, as shown in Example 5. Although this is not true, in Theorems 2 and 3, which are the main results of ths paper, we prove that at least the first and second GHWs of a binary linear code can be computed using this set. Moreover, we obtain an upper bound for the other GHWs.

1.3. Outline of This Article

We outline the structure of this article here. In Section 2, we revise some results on GHW, free resolutions and the ideal associated with a code. Section 3 briefly covers the false conjecture and some experiments that drove us to conduct this study. In Section 4, we show our main results. Finally, in Section 5, we show some future lines of research and some conjectures related to the topic that we hope will be helpful for future research.

2. GHW and Minimal Supports

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 the 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 subspace $\mathcal{C}$ in $\mathbb{F}_q^n$ is called a *linear code*. The elements of $\mathcal{C}$ are called *codewords*. The *basic parameters* of $\mathcal{C}$ are its length, its dimension and its 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. 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 $\mathcal{C}$.

Definition 1. *Let $\mathcal{C}$ be a linear code, we say that a codeword $\mathbf{m}$ has minimal support if it is nonzero and* $\mathrm{supp}(\mathbf{m})$ *does not contain the support of any other nonzero codeword. We will denote by $\mathcal{M}_\mathcal{C}$ the set of codewords of minimal support of $\mathcal{C}$.*

Note that computing a set of codewords of minimal support is a hard problem for a general linear code, as the minimum distance of the code needs to be found, and, thus, it is harder to tackle the problem of complete maximum-likelihood decoding; see [27,28].

Definition 2. *Let $\mathcal{C}$ be a linear code and D be a subcode of $\mathcal{C}$; we define* the support of D, *denoting* $\mathrm{supp}(D)$ *as the set of not-always-zero bit positions of D, i.e.,*

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

It is clear that if D is a one-dimensional subcode then, the support of D is equal to the Hamming weight of any of its nonzero codewords, i.e., $d_1(\mathcal{C}) = \delta(\mathcal{C})$. Based on this idea, the *h-th generalized Hamming weight* of $\mathcal{C}$, denoted $d_h(\mathcal{C})$, is the size of the smallest support of an h-dimensional subcode of $\mathcal{C}$ with $h = 1, 2, \ldots, k(\mathcal{C})$. That is, if D_h is the set of all linear subspaces of the linear code $\mathcal{C}$ of dimension h, then

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

Some basic facts on the Generalized Hamming Weights (GHW) are provided in the following proposition.

Proposition 1 ([1])**.** *Let $\mathcal{C}$ be a linear code. Then:*

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)* $d_h(\mathcal{C}) \leq n(\mathcal{C}) - k(\mathcal{C}) + h$.

From now on, we assume that $\mathcal{C}$ is a nondegenerate code, that is, $d_{k(\mathcal{C})}(\mathcal{C}) = n(\mathcal{C})$.

The GHWs $d_1(\mathcal{C}), \ldots, d_{k(\mathcal{C})}(\mathcal{C})$ are completely determined by the underlying linear matroid structure of the code in a nontrivial manner, and the method of obtaining them is not efficient as that used in [13]. Of course, as pointed out before, calculating $d_1(\mathcal{C})$ is equivalent to the problem of complete decoding linear codes [28]; hence, one cannot expect a computationally efficient approach. Given a positive integer ℓ,, we define $[\ell] = \{1, \ldots, \ell\}$ and $[\ell]_0 = \{0, \ldots, \ell\}$.

Definition 3. *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 the simplicial complex*

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

Then, the pair $\mathcal{M} = ([n], \Delta)$ is the linear matroid associated with the code $\mathcal{C}$. *The collection Δ of subsets of $[n]$ are called* independent sets *of this matroid. A subset of $[n]$ that does not belong to Δ is called a* dependent set. *Minimal dependent subsets of $[n]$ are known as* circuits *of $\mathcal{M}$.*

We refer to [29] for a brief introduction on the theory of simplicial complexes, and to [30] for a thorough study of matroids.

Definition 4. *Let $\mathbb{K}$ be any field. We denote by I_Δ the ideal in the polynomial ring $R = \mathbb{K}[X_1, \ldots, X_n]$ over $\mathbb{K}$ 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 minimally generated by the monomials supported on the circuits of $\mathcal{M}$ or, equivalently, supported on the set $\mathcal{M}_C$ of codewords of minimal support of $\mathcal{C}$.

$$I_\Delta = \left\langle \prod_{i\in \mathrm{supp}(\mathbf{c})} X_i \mid \mathbf{c} \in \mathcal{M}_\mathcal{C} \right\rangle. \tag{1}$$

The quotient $R_\Delta = R/I_\Delta$ is called the *Stanley–Reisner* ring associated with Δ and is a finitely generated standard graded $\mathbb{K}$-algebra of dimension $n(\mathcal{C}) - k(\mathcal{C})$. Thus, one may consider a minimal graded free resolution of R_Δ. The study of monomial ideals and their minimal graded free resolutions is a very active area of research; we refer the reader to [31,32] for some fairly recent account on the topic. Since the generators of I_Δ are supported in the set of circuits of a matroid, by [33], one has that Δ is shellable and this implies that R_Δ is Cohen–Macaulay. So, by the Auslander–Buchsbaum formula, the projective dimension of R_Δ (i.e., the length of any minimal graded free resolution of R_Δ) is $k(\mathcal{C})$ and it looks like

$$0 \longrightarrow F_{k(\mathcal{C})} \longrightarrow F_{k(\mathcal{C})-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow R_\Delta \longrightarrow 0 \tag{2}$$

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

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

We will refer to Equation (2) as a minimal graded free resolution of $\mathcal{C}$. The non-negative integers $\beta_{i,j}$ are called *Betti numbers* of $\mathcal{C}$ and do not depend on the choice of the parity check matrix H or the minimal free resolution of R_Δ. Moreover, since I_Δ comes from the set of circuits of a matroid, these numerical invariants do not even depend on the chosen ground field $\mathbb{K}$ (see [33]) and, thus, they only depend on the code $\mathcal{C}$.

In [13], Johnsen and Verdure describe the GHWs of a linear code $\mathcal{C}$ in terms of the shifts of the minimal graded free resolution of a Stanley–Reisner ideal I_Δ associated with $\mathcal{C}$. More precisely, they proved the following:

Theorem 1 ([13]). *Let $\mathcal{C}$ be a q-ary linear code. Then,*

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

Example 1 (Toy example). *Let $\mathcal{C}$ be the binary nondegenerate $[6,3]$ code with generator matrix*

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

One can check that the set of codewords of minimal support is

$$\mathcal{M}_\mathcal{C} = \left\{ \begin{array}{lll} w_1 = 100001, & w_2 = 100110, & w_3 = 011010, \\ w_4 = 000111, & w_5 = 111100, & w_6 = 011101 \end{array} \right\}$$

Its Stanley–Reisner ring is $R_\Delta = R/I_\Delta$, *where* $R = \mathbb{F}_2[x_1, \ldots, x_6]$ *and the ideal* I_Δ *is generated by the monomials associated with* $\mathcal{M}_\mathcal{C}$. *If we compute a graded minimal free resolution of* R_Δ, *we obtain the following Betti diagram:*

	0	1	2	3
0	1	0	0	0
1	0	1	0	0
2	0	3	2	0
3	0	2	7	4

where the entry of the row indexed by i *and column indexed by* j *indicates the value* $\beta_{j,i+j}$ *(for example* $\beta_{3,5} = 7$*). Hence, by Theorem 1, we have* $d_1(\mathcal{C}) = 2$, $d_2(\mathcal{C}) = 4$ *and* $d_3(\mathcal{C}) = 6$.

This result shows that the determination of the Betti numbers of the monomial ideal I_Δ related to a code completely determine the weight hierarchy. However, as mentioned before, this is usually a hard problem [28] except in some special cases. For example, Johnsen and Verdure in [16] explicitly determine the Betti Numbers for MDS codes, since the minimal free resolution of these codes is linear. Moreover, in [16] the authors prove that the resolution of the first-order Reed–Muller code is pure. A similar result can be deduced for constant weight codes [15]. Thus, simplex codes or dual Hamming codes, which are constant weight codes, also have a pure resolution, although it is not necessarily linear.

Remark 1. *The resolution* (2) *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.

One of the main disadvantages of the method proposed by Johnsen and Verdure is that the generators of I_Δ correspond to the supports of all minimal support of $\mathcal{C}$. In general, the whole set of codewords of minimal support can be huge and computationally expensive to obtain and, in many cases, computing a minimal graded free resolution of an ideal with that many generators is unaffordable. The rest of this work is devoted to computing a simpler and smaller structure than the whole set of codewords of minimal support that allows to know partial information about the GHWs of the code.

Test-Sets of a Binary Code

From now on, we will restrict our study to binary codes. Let $\mathcal{C}$ be a binary linear code. Let X be a vector with $n = n(\mathcal{C})$ variables $x_1, \ldots, x_n$. A monomial in X is a product of the form $X^\mathbf{a} := \prod_{i=1}^n x_i^{a_i}$, where $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$. The total degree of $X^\mathbf{a}$ is $\deg(X^\mathbf{a}) = \sum_{i=1}^n a_i$. When $\mathbf{a} = \mathbf{0}$, note that $X^\mathbf{a} = \mathbf{1}$. The polynomial ring $\mathbb{K}[X]$ is the set of all polynomials in X with coefficients in $\mathbb{K}$, where $\mathbb{K}$ denotes an arbitrary field.

Remark 2. *By using notation, we will write* $X^\mathbf{a}$ *with* $\mathbf{a} \in \mathbb{F}_2^n$. *In this case, we understand that the classes of* $0, 1$ *are replaced by the same symbols regarded as integers. Moreover, we will use the notation* X^I *for the square free monomial with support* $I \subset [n]$, *that is,*

$$X^I = \prod_{i \in I} x_i \text{ with } I \subseteq [n].$$

Let $g = X^A - X^B$ *be a binomial with* $A, B \subseteq [n]$, *we define* $\operatorname{supp}(g) = A \cup B$. *We say that* g *is in* standard form *if* $A \cap B = \emptyset$ *or, equivalently, if* $\operatorname{supp}(g) = A \sqcup B$, *where* $\sqcup$ *denotes the disjoint union of* A *and* B.

Definition 5. *Let* $\mathbb{K}$ *be any field; we define the* ideal associated with $\mathcal{C}$ over $\mathbb{K}$ *as the binomial ideal:*

$$I(\mathcal{C}) = \langle X^\mathbf{a} - X^\mathbf{b} \mid \mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n, \mathbf{a} + \mathbf{b} \in \mathcal{C} \rangle + \langle x_i^2 - 1 \mid i \in [n] \rangle \subseteq \mathbb{K}[X]. \tag{3}$$

Note that $I(\mathcal{C})$ is a zero-dimensional ideal since the quotient ring $R = \mathbb{K}[X]/I(\mathcal{C})$ is a finite-dimensional vector space (i.e., $\dim_{\mathbb{K}}(R) < \infty$). Moreover, its dimension is equal to the number of *cosets* in $\mathbb{F}_2^n/\mathcal{C}$. For $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$, one has that $X^{\mathbf{a}} - X^{\mathbf{b}} \in I(\mathcal{C})$ if and only if $\mathbf{a} - \mathbf{b} \in \mathcal{C}$. The following result shows how to obtain a set of generators of the ideal $I(\mathcal{C})$ from a generator matrix of $\mathcal{C}$.

Proposition 2 ([24]). *Let $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ be the row vectors of a generator matrix for $\mathcal{C}$. Then,*

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

If we fix a term order $\prec$, then the *leading term* of a polynomial f with respect to $\prec$, denoted by $\mathrm{LT}_\prec(f)$, is the largest monomial among all monomials which occur with nonzero coefficient in the expansion of f. Let I be an ideal in $\mathbb{K}[X]$; then, the *initial ideal* $\mathrm{in}_\prec(I)$ is the monomial ideal generated by the leading term of all the polynomials in I, i.e., $\mathrm{in}_\prec(I) = \langle\{\mathrm{LT}_\prec(f) \mid f \in I\}\rangle$. By definition, $\mathrm{in}_\prec(I)$ is a monomial ideal and, thus, it has a unique minimal generating set formed by monomials. These monomials will be called *minimal generators of* $\mathrm{in}_\prec(I)$.

Definition 6. *A finite set of nonzero polynomials $\mathcal{G} = \{g_1, \ldots, g_m\}$ of the ideal I is a Gröbner basis of I with respect to the term order $\prec$ if the leading terms of the elements of $\mathcal{G}$ generate the initial ideal $\mathrm{in}_\prec(I)$. Moreover, $\mathcal{G}$ is reduced if*

1. *g_i is monic (i.e., its leading coefficient is 1) for all $i \in [m]$;*
2. *None of the monomials appearing in the expansion of g_j is divisible by $\mathrm{LT}_\prec(g_i)$ for all $i \neq j$.*

For a given monomial order $\prec$, every ideal has a unique reduced Gröbner basis (see, e.g., [34]). Since $I(\mathcal{C})$ is generated by binomials (differences of monomials), then all its reduced Gröbner bases consist of binomials (see [35]). In [24], it is shown that, if $\mathcal{C}$ is a binary code and we fix a degree compatible term order $\prec$ on $\mathbb{K}[X]$, then the reduced Gröbner basis $\mathcal{G}_\prec$ for the code ideal $I(\mathcal{C})$ can be computed by a linear algebra (an FGLM-like) algorithm. Moreover, the reduction provided by $\mathcal{G}_\prec$ gives a decoding procedure. Along the way, they also prove that the support of every binomial in $\mathcal{G}_\prec$ different from $x_i^2 - 1$ for $i = 1, \ldots, n$ provides a codeword of minimal support of $\mathcal{C}$, and that there is a word of Hamming weight $d_1(\mathcal{C})$ that can be obtained in this way. More precisely:

Proposition 3 ([24]). *Let $\mathcal{G}_\prec$ be the reduced Gröbner basis of $I(\mathcal{C})$ with respect to a degree compatible term order $\prec$. For every binomial $X^{\mathbf{a}} - X^{\mathbf{b}} \in \mathcal{G}_\prec - \{x_i^2 - 1 \mid i \in [n]\}$, then $\mathbf{a} + \mathbf{b} \in \mathbb{F}_2^n$ is a codeword of minimal support of $\mathcal{C}$. Moreover, there exists $X^{\mathbf{a}} - X^{\mathbf{b}} \in \mathcal{G}_\prec$ such that $\mathrm{w}_H(\mathbf{a} + \mathbf{b}) = d_1(\mathcal{C})$.*

This result motivates the definition of a $\mathcal{G}_\prec$-test, which by the above proposition is a subset of the set of codewords of minimal support and contains a word of minimum weight.

Definition 7. *Given a binary code $\mathcal{C}$ and a degree compatible term order $\prec$, we will call the $\mathcal{G}_\prec$-test set of $\mathcal{C}$ to the subset of codewords of minimal support of $\mathcal{C}$ whose supports are given by the binomials in the reduced Gröbner basis of $I(\mathcal{C})$ different from $x_i^2 - 1$ for all $i \in [n]$.*

Example 2. *Here, we expand on Example 1. Then, the ideal associated with $\mathcal{C}$ over R is defined as*

$$I(\mathcal{C}) = \left\langle \{\ x_1x_6 - 1, \quad x_2x_3x_5 - 1, \quad x_4x_5x_6 - 1\ \} \cup \left\{x_i^2 - 1\right\}_{i\in[6]} \right\rangle \subseteq R$$

Now, we consider the degree reverse lexicographic order $\prec$ with $x_6 \prec \ldots \prec x_1$. Then, the reduced Gröbner basis $\mathcal{G}_\prec$ of $I(\mathcal{C})$ with respect to $\prec$ has 14 elements. An a $\mathcal{G}_\prec$-test-set of $\mathcal{C}$ is given

by codewords of $\mathcal{M}_\mathcal{C}$ whose supports are given by those binomials of $\mathcal{G}_\prec$ different from $x_i^2 - 1$, i.e., the set

$$\{\ w_1 = 100001,\quad w_3 = 011010,\quad w_4 = 000111,\quad w_6 = 011101\ \} \subseteq \mathcal{M}_\mathcal{C}.$$

3. On a False Conjecture

Note that the second and the third authors of this work have previously conjectured the following:

Conjecture (false) *If one considers the monomial ideal M associated with the supports of the binomials in the $\mathcal{G}_\prec$-test set, then $d_i = \min\{j \mid \beta_{i,j}(R/M) \neq 0\}$ for $i \in \{1, \ldots, k(\mathcal{C})\}$; that is, the $\mathcal{G}_\prec$-test set determines the GHWs of the codes.*

This conjecture was supported by computational evidence (see Examples 3 and 4 for some examples proving this conjecture), but unfortunately this is not true, as shown by a counterexample 5. Theorem 3 in Section 4 in this paper will prove this fact for $i = 2$ (and it was known for $i = 1$ [24]). Note also that in [25], the authors show that from the Graver basis associated with $I(\mathcal{C})$, one can purge the set of codewords of minimal support of $\mathcal{C}$, i.e., $\mathcal{M}_\mathcal{C}$.

Example 3. *We continue expanding on Example 1 and have computed the Betti diagram associated with $R_\Delta = R/I_\Delta$, where I_Δ is generated by the monomials associated with $\mathcal{M}_\mathcal{C}$. Then, in Example 2, we compute a $\mathcal{G}_\prec$-test-set $\mathcal{T}_\mathcal{C}$ of $\mathcal{C}$ with respect to the degree reverse lexicographic order $\prec$. Note that $\mathcal{T}_\mathcal{C} \subset \mathcal{M}_\mathcal{C}$ with just 4 elements. If we consider M the corresponding monomial ideal related to $\mathcal{T}_\mathcal{C}$ and compute a graded minimal free resolution of R/M, we obtain the following Betti diagram:*

	0	1	2	3
0	1	0	0	0
1	0	1	0	0
2	0	2	1	0
3	0	4	4	2

The Betti numbers of R/M are smaller than those of R_Δ and in this example the sequence

$$(\min\{j \mid \beta_{i,j} \neq 0\}; 1 \leq i \leq 3) = (2, 4, 6),$$

coincides with the GHWs of $\mathcal{C}$.

The following example is a less trivial case where the difference between our structure $\mathcal{T}_\mathcal{C}$ and the set of codewords of minimal support of $\mathcal{C}$, $\mathcal{M}_\mathcal{C}$, is larger.

Example 4. *Let $\mathcal{C}$ be the binary nondegenerate $[14, 9]$-code with generator matrix*

$$G = \begin{pmatrix} 1&1&0&1&0&0&0&0&0&1&0&0&0&0 \\ 1&1&1&1&0&1&0&0&1&1&0&0&0&1 \\ 0&0&1&0&0&1&1&1&1&1&0&1&1&0 \\ 1&1&0&1&1&1&0&0&1&1&0&0&0&1 \\ 0&1&1&1&1&0&0&1&0&0&1&0&1&1 \\ 0&0&1&1&0&1&1&0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&1&0&1&1&1&0&1&0 \\ 0&1&0&1&1&0&1&0&1&1&0&1&1&0 \\ 1&1&1&1&1&1&0&1&0&0&0&0&1&0 \end{pmatrix} \in \mathbb{F}_2^{9\times 14}$$

Its Stanley–Reisner ring is $R_\Delta = R/I_\Delta$, where $R = \mathbb{F}_2[x_1, \ldots, x_{14}]$ and I_Δ is minimally generated by 147 monomials. If we compute a graded minimal free resolution of R_Δ, we obtain the following Betti diagram:

	0	1	2	3	4	5	6	7	8	9
0	1	0	0	0	0	0	0	0	0	0
1	0	2	0	0	0	0	0	0	0	0
2	0	8	5	0	0	0	0	0	0	0
3	0	34	82	48	8	0	0	0	0	0
4	0	52	441	897	753	289	42	0	0	0
5	0	51	1345	7410	18309	25248	21008	10579	2990	366

Hence, by Theorem 1, we have that the GHWs are

$$(d_1(\mathcal{C}), \ldots, d_9(\mathcal{C})) = (2, 4, 6, 7, 9, 10, 12, 13, 14).$$

Moreover, if we consider $\prec$ the graded degree lexicographic order with $x_1 \succ \cdots \succ x_{14}$, we find that the $\mathcal{G}_\prec$-test set has 24 elements. If we consider M, the corresponding monomial ideal, and compute a graded minimal free resolution of R/M, we obtain the following Betti diagram:

	0	1	2	3	4	5	6	7	8	9
0	1	0	0	0	0	0	0	0	0	0
1	0	2	0	0	0	0	0	0	0	0
2	0	6	3	0	0	0	0	0	0	0
3	0	13	38	17	2	0	0	0	0	0
4	0	3	92	194	130	35	3	0	0	0
5	0	0	83	599	1410	1621	1040	378	71	5
6	0	0	0	0	2	5	4	1	0	0

As one can observe, the Betti numbers of R/M are smaller than those of R_Δ. Moreover, in this example, the sequence $(\min\{j \mid \beta_{i,j} \neq 0\}; 1 \leq i \leq 9)$ is given by $(2, 4, 6, 7, 9, 10, 12, 13, 14)$ and it coincides with the GHWs of $\mathcal{C}$.

Example 5. *Let $\mathcal{C}$ be the binary nondegenerate $[10, 7]$-code with a generator matrix*

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

Its Stanley–Reisner ring is $R_\Delta = R/I_\Delta$, where $R = \mathbb{F}_2[x_1, \ldots, x_{10}]$ and I_Δ is minimally generated by 42 monomials. If we compute a graded minimal free resolution of R_Δ, we obtain 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

Hence, from Theorem 1, we have $d_1(\mathcal{C}) = 2$, $d_2(\mathcal{C}) = 4$, $d_3(\mathcal{C}) = 5$, $d_4(\mathcal{C}) = 6$, $d_5(\mathcal{C}) = 8$, $d_6(\mathcal{C}) = 9$, $d_7(\mathcal{C}) = 10$.

If we compute a $\mathcal{G}_\prec$-test set T with respect to the degree reverse lexicographical order, we find that T has only 10 elements. By computing a minimal graded free resolution of R/M being the ideal $M := \langle \{X^{\mathbf{c}} \mid \mathbf{c} \in T\} \rangle$, we obtain 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 can recover the correct values of $d_1(\mathcal{C}), d_2(\mathcal{C}), d_3(\mathcal{C})$ from this resolution but not $d_i(\mathcal{C})$ for $i = 4, 5, 6, 7$.

The experiments we conducted to prove the aforementioned conjecture yielded the results in Section 4 and we propose some further conjectures and future work based on the experimental evidence showed in Section 5.

4. Second GHW Obtained from a $\mathcal{G}_\prec$-Test Set

In this section, we will explain how to compute the second generalized Hamming weight from a $\mathcal{G}_\prec$-test set. Throughout this section, $\mathcal{C}$ will denote a binary linear code and 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 $\mathbb{K}[X]$. The following result is a technical lemma whose proof is just an easy exercise in set theory. We will denote by $A \triangle B$ the *symmetric difference* of the subsets $A, B \subseteq [n]$, which is the set of elements which are in the union of the two sets $A \cup B$, minus their intersection $A \cap B$. Moreover, for a set A, its cardinality is denoted by $|A|$.

Lemma 1. *Let $A, B \subseteq X$ with $|A \cap B| > \frac{|A|}{2}$. Then, $C = A \triangle B$ satisfies the following statements:*

1. $A \cup B = A \cup C$
2. $|A \cap C| < \frac{|A|}{2}$
3. $|C| < |B|$.

Consider the set $\mathbf{M}$ of codewords in $\mathcal{C}$ belonging to a linear subspace of dimension two of minimal support, more precisely,

$$\mathbf{M} = \{\mathbf{m} \in \mathcal{C} \mid \exists \mathbf{m}' \in \mathcal{C} \text{ such that } d_2(\mathcal{C}) = \operatorname{supp}(\langle \mathbf{m}, \mathbf{m}' \rangle)\}, \tag{4}$$

and define $\mathbf{m}_1, \mathbf{m}_2 \in \mathbf{M}$ as follows:

(a) $\mathbf{m}_1 := \min_\prec(\mathbf{M})$, i.e., $\mathbf{m}_1$ is the smallest codeword with respect to $\prec$ in $\mathbf{M}$;
(b) $\mathbf{m}_2 := \min_\prec\{\mathbf{m} \in \mathbf{M} \mid d_2(\mathcal{C}) = \operatorname{supp}(\langle \mathbf{m}_1, \mathbf{m} \rangle)\}$, i.e, $\mathbf{m}_2$ is the smallest codeword with respect to $\prec$ such that $d_2(\mathcal{C}) = \operatorname{supp}(\langle \mathbf{m}_1, \mathbf{m}_2 \rangle)$.

With these conditions, we define:

$$I = \operatorname{supp}(\mathbf{m}_1) \quad \text{and} \quad J = \operatorname{supp}(\mathbf{m}_2).$$

Remark 3. *Since $\prec$ is degree compatible and, by Lemma 1, we have that*

$$|I \cap J| \leq \frac{|I|}{2} \leq \frac{|J|}{2}.$$

Proposition 4. *There exists a binomial $f \in \mathcal{G}_\prec \subseteq \mathbb{K}[X]$ such that* $\operatorname{supp}(f) = I$.

Proof. Consider $f = X^{I_1} - X^{I_2} \in I(\mathcal{C})$ any binomial with $I = I_1 \sqcup I_2$, $|I_1| - 1 \leq |I_2| \leq |I_1|$ and $X^{I_1} \succ X^{I_2}$, we will show that $f \in \mathcal{G}_\prec$. For proving this, it suffices to check that:

(a) $X^{I_1} = \operatorname{LT}_\prec(f)$ is a minimal generator of $\operatorname{in}_\prec(I(\mathcal{C}))$;
(b) $X^{I_2} \notin \operatorname{in}_\prec(I(\mathcal{C}))$.

Proof of (a). By contradiction, suppose that there exists a binomial $h = X^{K_1} - X^{K_2} \in \mathcal{G}_\prec$ with $K = K_1 \sqcup K_2$, $\mathrm{LT}_\prec(h) = X^{K_1}$ (and, in particular, $|K_1| \geq |K_2|$) such that $K_1 \neq I_1$ and X^{I_1} is divisible by X^{K_1}, i.e., $K_1 \subsetneq I_1$.

Claim: $d_2(\mathcal{C}) \leq |I \cup K| - 1$.

Proof of the claim: We have that $|K_2| \leq |K_1| \leq |I_1| - 1 \leq |I_2|$. Then, $|K| < |I|$ and, in particular, $X^K \prec X^I \prec X^J$. Hence, by the choice of $\mathbf{m}_2$, we have that $|I \cup J| < |I \cup K|$ and the *Claim* follows.

From the previous *Claim*, we have that

$$\begin{aligned} |I \cup J| &= d_2(\mathcal{C}) \leq |I \cup K| - 1 \\ &= |I \cup K_2| - 1 \quad (\text{since } K_1 \subsetneq I) \\ &= |I| + |K_2| - |I \cap K_2| - 1 \\ &\leq |I| + |K_1| - |I \cap K_2| - 1 \quad (\text{since } X^{K_1} \succ X^{K_2}). \end{aligned}$$

Thus,

$$|I| + |J| - |I \cap J| = |I \cup J| \leq |I| + |K_1| - |I \cap K_2| - 1$$

or equivalently $|J| - |I \cap J| \leq |K_1| - |I \cap K_2| - 1$. Thus,

$$\begin{aligned} |I_1| - \frac{1}{2} &\leq \frac{|I|}{2} \leq \frac{|J|}{2} \leq |J| - |I \cap J| \quad (\text{by Remark 3}) \\ &\leq |K_1| - |I \cap K_2| - 1 \leq |K_1| - 1. \end{aligned}$$

Therefore, $|I_1| \leq |K_1| - \frac{1}{2}$ and $K_1 \subsetneq I_1$, a contradiction.

Proof of (b). By contradiction, we assume that there exists $h = X^{K_1} - X^{K_2} \in \mathcal{G}_\prec$ such that $\mathrm{LT}_\prec(h) = X^{K_1}$ divides X^{I_2} or, equivalently, $K_1 \subseteq I_2$. Then $K_2 \prec K_1 \prec I_2 \prec I_1$ and, in particular, $X^K \prec X^I \prec X^J$. Hence, by the choice of $\mathbf{m}_2$, we have that $|I \cup J| < |I \cup K|$.

$$\begin{aligned} d_2(\mathcal{C}) &= |I \cup J| \leq |I \cup K| - 1 = |I \cup K_2| - 1 = |I| + |K_2| - |I \cap K_2| - 1 \\ &\leq |I| + |K_2| - 1 \leq |I| + |K_1| - 1. \end{aligned}$$

Therefore, $|J| - |I \cap J| \leq |K_1| - 1$. From Remark 3, we deduce that

$$|I_2| \leq \frac{|I|}{2} \leq \frac{|J|}{2} \leq |J| - |I \cap J| \leq |K_1| - 1.$$

Therefore, $|I_2| < |K_1|$ and $K_1 \subseteq I_2$, which is a contradiction. □

One can check that the same result (and the same proof) holds for all I' such that $I' = \mathrm{supp}(\mathbf{m})$ with $\mathbf{m} \in \mathbf{M}$ and $|I'| = |I|$. As a consequence of this observation we have that:

Corollary 1. *If $|I| = |J|$. Then, we can always find binomials $f, g \in \mathcal{G}_\prec \subseteq \mathbb{K}[X]$ such that* $\mathrm{supp}(f) = I$ *and* $\mathrm{supp}(g) = J$.

We found that I is always involved in the supports associated with $\mathcal{G}_\prec$ and that if J has the same cardinal as them, the second GHW can also be derived from the Gröbner basis. Let us now prove the general case.

Proposition 5. *There exists a binomial $g \in \mathcal{G}_\prec \subseteq \mathbb{K}[X]$ such that* $\mathrm{supp}(g) = J$.

Proof. From Remark 3, we know that $|I \cap J| \leq |J|/2$, so one may consider

$$g = X^{I \cap J} X^{J_1} - X^{J_2} \in I(\mathcal{C}),$$

such that $J_1 \cup J_2 = J - I$, $J_1 \cap J_2 = \emptyset$ and $|J_2| + 1 \geq |I \cap J| + |J_1| \geq |J_2|$. Our goal is to prove that g (or $-g$) is in $\mathcal{G}_\prec$. We split the proof into two:

Case $\mathrm{LT}_\prec(g) = X^{I\cap J}X^{J_1}$**.** We are going to see that $g \in \mathcal{G}_\prec$. First, we show that $X^{I\cap J}X^{J_1}$ is a minimal generator of $\mathrm{in}_\prec(I(\mathcal{C}))$. By contradiction, suppose that there is a binomial $h = X^{K_1} - X^{K_2} \in \mathcal{G}_\prec$ with $\mathrm{LT}_\prec(h) = X^{K_1}$ such that $K_1 \subsetneq (I \cap J) \cup J_1$, and denote $K = K_1 \sqcup K_2$. We have that $|J_2| \geq |I \cap J| + |J_1| - 1 \geq |K_1| \geq |K_2|$ and, in particular, $|J| > |K|$.

However,

$$\begin{array}{rcl} d_2(\mathcal{C}) & = & |I \cup J| = |I| + |J| - |I \cap J| \\ & = & |I| + |J_1| + |J_2| \\ & \geq & |I| + |J_1| + |K_2| \\ & \geq & |I \cup K|, \end{array}$$

which cannot happen by the choice of $J = \mathrm{supp}(\mathbf{m}_2)$. Therefore, $X^{I\cap J}X^{J_1}$ is a minimal generator of $\mathrm{in}_\prec(I(\mathcal{C}))$.

Now, we will show that $X^{J_2} \notin \mathrm{in}_\prec(I(\mathcal{C}))$. Since $X^{I\cap J}X^{J_1}$ is a minimal generator of $\mathrm{in}_\prec(I(\mathcal{C}))$, then there exists $h = X^{I\cap J}X^{J_1} - X^L \in \mathcal{G}_\prec$. We have that $X^L \notin \mathrm{in}_\prec(I(\mathcal{C}))$ and let us see that $L = J_2$. Suppose that $L \neq J_2$, then $0 \neq h - g = x^{J_2} - x^L \in I(\mathcal{C})$ and $X^{J_2} \succ X^L$, because $X^L \notin \mathrm{in}_\prec(I(\mathcal{C}))$. However,

$$|I \cup \mathrm{supp}(h)| \leq |I| + |J_1| + |L| \leq |I| + |J_1| + |J_2| = |I \cup J| = d_2(\mathcal{C}),$$

which is a contradiction.

Case $\mathrm{LT}_\prec(g) = X^{J_2}$**.** We are going to see that $-g \in \mathcal{G}_\prec$. First, we show that X^{J_2} is a minimal generator of $\mathrm{in}_\prec(I(\mathcal{C}))$. Suppose that there exists a binomial $h = X^{K_1} - X^{K_2} \in \mathcal{G}_\prec$ with $X^{K_1} \succ X^{K_2}$ and $K_1 \subsetneq J_2$. Consider $L := J \triangle K$, we have that $L \subseteq (J - K_1) \cup K_2$ and, hence, $X^L \prec X^{J-K_1}X^{K_2} \prec X^J$. However,

$$|I \cup L| \leq |I \cup (J - K_1) \cup K_2| \leq |I \cup J| - |K_1| + |K_2| \leq |I \cup J| = d_2(\mathcal{C}),$$

and again it is a contradiction.

We will show now that $X^{I\cap J}X^{J_1} \notin \mathrm{in}_\prec(I(\mathcal{C}))$, by contradiction. Suppose that $X^{I\cap J}X^{J_1} \in \mathrm{in}_\prec(I(\mathcal{C}))$, then there exists a binomial $X^{I\cap J}X^{J_1} - X^L$ in $I(\mathcal{C})$. Consider now $K = (I \cap J) \cup J_1 \cup L$, again one can compute that $|I \cup J| \geq |I \cup K|$ and that $K \prec J$, which again contradicts the choice of $\mathbf{m}_2$. □

From the above results, the main theorems of this paper will follow.

Theorem 2. *Let $\prec$ be a degree-compatible order in $\mathbb{K}[X]$; then, there are f, g in the reduced Gröbner basis $\mathcal{G}_\prec$ of $I(\mathcal{C})$ with respect to $\prec$, such that $d_2 = |\mathrm{supp}(f) \cup \mathrm{supp}(g)|$.*

Example 6. *Let $\mathcal{C}$ be the binary nondegenerate $[6, 3]$-code with a generator matrix*

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

One can check that every codeword different from 0 is a codeword of minimal support and, hence, there are 7 codewords of minimal support, namely $w_1 = 111000, w_2 = 110011$, $w_3 = 101101$, $w_4 = 100110$, $w_5 = 101110, w_6 = 010101, w_7 = 001011$. Moreover, we have that $d_1(\mathcal{C}) = 3$ and $d_2(\mathcal{C}) = 5$ and $d_3(\mathcal{C}) = 6$ and the set $\mathbf{M}$ described in (4) coincides with $\mathcal{C} - \{0\}$.

Consider the degree reverse lexicographic order $\prec_1$ with $x_6 \prec_1 \cdots \prec_1 x_1$; then,

- $\mathbf{m}_1 := \min_{\prec_1}(\mathbf{M}) = 001011 = w_7$;
- $\mathbf{m}_2 := \min_{\prec_1}\{\mathbf{m} \in \mathbf{M} \,|\, d_2(\mathcal{C}) = \mathrm{supp}(\langle \mathbf{m}_1, \mathbf{m}\rangle)\} = 010101 = w_6$.

The reduced Gröbner basis $\mathcal{G}_1$ of $I(\mathcal{C})$ with respect to $\prec_1$ has 20 elements. As proved in Proposition 4, the binomial $f = x_5x_6 - x_3$ belongs to G_1 and has $\operatorname{supp}(f) = \operatorname{supp}(w_7) = \{3,5,6\}$ *and, by Proposition 5, the binomial $g = x_4x_6 - x_2$ belongs to $\mathcal{G}_1$ and has* $\operatorname{supp}(g) = \operatorname{supp}(w_6) = \{2,4,6\}$. *Moreover,* $d_2 = |\operatorname{supp}(f) \cup \operatorname{supp}(g)| = |\operatorname{supp}(\langle w_6, w_7\rangle)| = |\{2,3,4,5,6\}| = 5$.

If we consider the degree reverse lexicographic order $\prec_2$ with $x_1 \prec_2 \cdots \prec_2 x_6$, then

- $\mathbf{m}_1' := \min_{\prec_2}(\mathbf{M}) = 111000 = w_1$;
- $\mathbf{m}_2' := \min_{\prec_2}\{\mathbf{m} \in \mathbf{M} \mid d_2(\mathcal{C}) = \operatorname{supp}(\langle \mathbf{m}_1', \mathbf{m}\rangle)\} = 100110 = w_4$.

The reduced Gröbner basis $\mathcal{G}_2$ of $I(\mathcal{C})$ with respect to $\prec_2$ has 20 elements. As proved in Proposition 4, the binomial $f' = x_1x_2 - x_3$ belongs to $\mathcal{G}_2$ and has $\operatorname{supp}(f) = \operatorname{supp}(w_1) = \{1,2,3\}$ *and, as proved in Proposition 5, the binomial $g' = x_1x_4 - x_5$ belongs to $\mathcal{G}_2$ and has* $\operatorname{supp}(g) = \operatorname{supp}(w_4) = \{1,4,5\}$. *Moreover,*

$$d_2 = |\operatorname{supp}(f') \cup \operatorname{supp}(g')| = |\operatorname{supp}(\langle w_1, w_4\rangle)| = |\{1,2,3,4,5\}| = 5.$$

As a consequence, we have that the two first GHWs $d_1(\mathcal{C})$ and $d_2(\mathcal{C})$ can be obtained from the minimal graded free resolution associated with the supports in the $\mathcal{G}_\prec$-test set. Moreover, from this resolution one can also obtain upper bounds for all the $d_i(\mathcal{C})$ where $i \in [k(\mathcal{C})]$. More precisely, we have the following:

Theorem 3. *Let $\mathcal{C} \subseteq \mathbb{F}_2^n$ be a binary code, $\prec$ a degree compatible monomial order in R. Let T denote the $\mathcal{G}_\prec$-test, define the square-free monomial ideal*

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

and 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

$$F_i = \bigoplus_{j\in\mathbb{N}} R(-j)^{\beta_{i,j}(R/M)} \text{ for } i \in [p]_0.$$

Then,

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

Proof. From Proposition 3, every $\mathbf{c} \in T$ is a codeword of minimal support and, hence, $\{X^{\mathbf{c}} \mid \mathbf{c} \in T\}$ is a subset of the generators of the monomial ideal supported on all the codewords of minimal support. Thus, (a) and (b) follow from Theorem 1.

The rest of the proof concerns (c). Again by Proposition 3, $\{X^{\mathbf{c}} \mid \mathbf{c} \in T\}$ is the minimal monomial generating set of M. Since $\beta_{1,i}(R/M)$ equals the number of minimal generators of M of degree i, then $\beta_{1,i}(R/M) = |\{\mathbf{c} \in T \mid \mathrm{w}_H(c) = i\}.|$ By Proposition 3, there is a $\mathbf{c} \in T$ such that $\mathrm{w}_H(\mathbf{c}) = d_1$ and, thus,

$$d_1(\mathcal{C}) = \min\{\mathrm{w}_H(\mathbf{c}) \mid \mathbf{c} \in T\} = \min\{i \mid \beta_{1,i}(R/M) \neq 0\}.$$

Assume now that $T = \{\mathbf{c}_1, \ldots, \mathbf{c}_r\}$, and consider $\mathcal{T}$ the Taylor resolution of $M = \langle X^{\mathbf{c}_1}, \ldots, X^{\mathbf{c}_r}\rangle$. The first steps of this resolution are given by

$$\mathcal{T} : \cdots \longrightarrow F_2' \xrightarrow{\varphi_2} F_1' \longrightarrow R \longrightarrow R/M \longrightarrow 0,$$

where $F_i' := \oplus_{\substack{|I|=i \\ I\subset[r]}} R(-|\operatorname{supp}\langle \mathbf{c}_j \mid j \in I\rangle|)$ and $F_1' := \oplus_{1\leq i\leq r} R(-|\operatorname{supp}(\mathbf{c}_i)|)$. Hence, the shifts in the second step of $\mathcal{T}$ are given by $|\operatorname{supp}\langle \mathbf{c}_i, \mathbf{c}_j\rangle|$ for $1 \leq i < j \leq r$ and, as a

consequence, $d_2(\mathcal{C}) \leq \min\{|\text{supp}\langle \mathbf{c}_i, \mathbf{c}_j\rangle| \,|\, 1 \leq i < j \leq r\}$. Moreover, by Theorem 2, this is indeed an inequality.

In general, the Taylor resolution is not minimal (it is usually very far from minimal). However, it can be pruned to obtain a minimal one. Consider now

$$\mathcal{F} : \cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow R \longrightarrow R/M \longrightarrow 0,$$

a minimal graded free resolution of R/M obtained after pruning the Taylor one. As we said before, $\{X^{\mathbf{c}_1}, \ldots, X^{\mathbf{c}_r}\}$ is the minimal monomial generating set of M and, hence, $F_1' = F_1$. As a consequence, $\min\{i \,|\, \beta_{2,i}(R/M) \neq 0\} = \min\{|\text{supp}\langle \mathbf{c}_i, \mathbf{c}_j\rangle| \,|\, 1 \leq i < j \leq r\} = d_2(\mathcal{C})$. □

5. Conclusions

In this work, we build on the results of Borges-Quintana et al. [24] and propose $\mathcal{G}_\prec$-test sets as a smaller structure from where one can obtain the values of $d_1(\mathcal{C})$ and $d_2(\mathcal{C})$ and upper bounds on $d_i(\mathcal{C})$ for all $i \geq 3$, provided $\mathcal{C}$ is a binary code. Several experiments with SageMath [36] suggest that Theorem 3 can also be extended for $i = 3$. More precisely:

Question 1. *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*

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

Is $d_3(\mathcal{C}) = \min\{i \,|\, \beta_{3,i}(R/M) \neq 0\}$?

In Example 5, one has that the projective dimension (i.e., the number of steps of the resolution) of R/M is $\text{pd}(R/M) = 6$, while the dimension of $\mathcal{C}$ is $k(\mathcal{C}) = 7$. In all the counterexamples to the original conjecture that we found, it turns out that $\text{pd}(R/M) < k(\mathcal{C})$. This motivates us to ask if the conjecture holds provided that $\text{pd}(R/M) = k(\mathcal{C})$. More precisely:

Question 2. *Whenever $\text{pd}(R/M) = k(\mathcal{C})$, is it true that*

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

for all $i \in \{1, \ldots, k(\mathcal{C})\}$?

Additionally, the following questions naturally arise:

Question 3. *What is in between the test set and the complete set of codewords of minimal support? I.e., can we characterize a mid-way structure that provides the complete set of GHWs?*

A possible candidate for the 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 and can be computed by the algorithm proposed in [26]. For example, for the $[7,4]$ binary Hamming code, i.e., the code with the generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{4\times 7},$$

has 14 codewords of minimal support, half of them with weight 3, and the rest with weight 4. Moreover, the sequence of GHWs is $(d_1(\mathcal{C}), \ldots, d_4(\mathcal{C})) = (3,5,6,7)$. One has that all the $\mathcal{G}_\prec$-test sets when $\prec$ ranges over all degree-compatible orderings consist of the 7 codewords of Hamming weight 3. If one computes the Betti diagram of the monomial ideal $M \subset \mathbb{F}_2[x_1, \ldots, x_7]$ corresponding to this set, one obtains the following:

	0	1	2	3	4
0	1	0	0	0	0
1	0	0	0	0	0
2	0	7	0	0	0
3	0	0	21	21	6

Hence, the sequence $(\min\{j \mid \beta_{i,j} \neq 0\}; 1 \leq i \leq 4) = (3,5,6,7)$ coincides with the sequence of GHWs of the code $\mathcal{C}$.

Question 4. *Can we say something in the nonbinary case?*

In order to answer this question, one could try to apply the techniques in [25], where a generalization of the ideal $I(\mathcal{C})$ for nonbinary codes is studied.

Finally, we would like to point out that Gorla and Ravagnani [23] recently extended and generalized the results of Johnsen and Verdure [13] to compute the generalized weights of a code with respect to a different notions of weight.

Question 5. *Can these generalized weights be computed from a $\mathcal{G}_{\prec}$-test set of $\mathcal{C}$?*

Author Contributions: Investigation, I.G.-M., I.M.-C., E.M.-M. and Y.P. All authors have read and agreed to the published version of the manuscript.

Funding: Ignacio García-Marco and Irene Márquez-Corbella were supported by the grant PID2019-105896GB-I00 funded by MCIN/AEI/10.13039/501100011033 and MACACO (ULL Research Projects). Edgar Martínez-Moro 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". Yuriko Pitones was partially supported by research grant SEGIB-Fundación Carolina.

Acknowledgments: We would like to thank E. Gorla (University of Neuchatel, Switzerland) for her valuable comments and suggestions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wei, V.K. Generalized Hamming weights for linear codes. *IEEE Trans. Inf. Theory* **1991**, *37*, 1412–1418. [CrossRef]
2. Feng, G.L.; Tzeng, K.K.; Wei, V.K. On the generalized Hamming weights of several classes of cyclic codes. *IEEE Trans. Inf. Theory* **1992**, *38*, 1125–1130. [CrossRef]
3. van der Geer, G.; van der Vlugt, M. The second generalized Hamming weight of the dual codes of double-error correcting binary BCH-codes. *Bull. Lond. Math. Soc.* **1995**, *27*, 82–86. [CrossRef]
4. González Sarabia, M.; Rentería, M.C. The second generalized Hamming weight of some evaluation codes arising from complete bipartite graphs. *Int. J. Contemp. Math. Sci.* **2009**, *4*, 1345–1352.
5. Güneri, C.; Özbudak, F. Improvements on generalized Hamming weights of some trace codes. *Des. Codes Cryptogr.* **2006**, *39*, 215–231. [CrossRef]
6. Helleseth, T.; Kløve, T.; Ytrehus, Ø. Generalized Hamming weights of linear codes. *IEEE Trans. Inf. Theory* **1992**, *38*, 1133–1140. [CrossRef]
7. Janwa, H.; Lal, A.K. On the generalized Hamming weights of cyclic codes. *IEEE Trans. Inf. Theory* **1997**, *43*, 299–308. [CrossRef]
8. Lee, K. Bounds for generalized Hamming weights of general AG codes. *Finite Fields Appl.* **2015**, *34*, 265–279. [CrossRef]
9. Munuera, C.; Ramirez, D. The second and third generalized Hamming weights of Hermitian codes. *IEEE Trans. Inf. Theory* **1999**, *45*, 709–712. [CrossRef]
10. Shim, C.; Chung, H. On the second generalized Hamming weight of the dual code of a double-error-correcting binary BCH code. *IEEE Trans. Inf. Theory* **1995**, *41*, 805–808. [CrossRef]
11. Wei, V.K.; Yang, K. On the generalized Hamming weights of product codes. *IEEE Trans. Inf. Theory* **1993**, *39*, 1709–1713. [CrossRef]
12. Beelen, P.; Datta, M. Generalized Hamming weights of affine Cartesian codes. *Finite Fields Their Appl.* **2018**, *51*, 130–145. [CrossRef]
13. Johnsen, T.; Verdure, H. Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids. *Appl. Algebra Eng. Commun. Comput.* **2013**, *24*, 73–93. [CrossRef]
14. Garrousian, M.; Tohăneanu, S.O. Minimum distance of linear codes and the α-invariant. *Adv. Appl. Math.* **2015**, *71*, 190–207. [CrossRef]
15. Ghorpade, S.; Singh, P. Pure resolutions, linear codes, and Betti numbers. *J. Pure Appl. Algebra* **2020**, *224*, 106385. [CrossRef]

16. Johnsen, T.; Verdure, H. Stanley-Reisner resolution of constant weight codes. *Des. Codes Cryptogr.* **2014**, *72*, 471–481. [CrossRef]
17. Johnsen, T.; Roksvold, J.; Verdure, H. Betti numbers associated to the facet ideal of a matroid. *Bull. Braz. Math. Soc. (N.S.)* **2014**, *45*, 727–744. [CrossRef]
18. Johnsen, T.; Roksvold, J.; Verdure, H. A generalization of weight polynomials to matroids. *Discrete Math.* **2016**, *339*, 632–645. [CrossRef]
19. Johnsen, T.; Verdure, H. Generalized Hamming weights for almost affine codes. *IEEE Trans. Inf. Theory* **2017**, *63*, 1941–1953. [CrossRef]
20. Johnsen, T.; Verdure, H. Relative generalized Hamming weights and extended weight polynomials of almost affine codes. In *Coding Theory and Applications*; Lecture Notes in Comput. Sci.; Springer: Cham, Switzerland, 2017; Volume 10495, pp. 207–216. [CrossRef]
21. Johnsen, T.; Verdure, H. Higher weight spectra of Veronese codes. *IEEE Trans. Inf. Theory* **2020**, *66*, 3538–3546. [CrossRef]
22. Johnsen, T.; Verdure, H. Greedy weights for matroids. *Des. Codes Cryptogr.* **2021**, *89*, 387–405. [CrossRef]
23. Gorla, E.; Ravagnani, A. Generalized weights of codes over rings and invariants of monomial ideals. *arXiv* **2022**, arXiv:2201.05813.
24. Borges-Quintana, M.; Borges-Trenard, M.; Fitzpatrick, P.; Martínez-Moro, E. Gröbner bases and combinatorics for binary codes. *Appl. Algebra Eng. Commun. Comput.* **1996**, *19*, 1–45. [CrossRef]
25. Márquez-Corbella, I.; Martínez-Moro, E.; Suárez-Canedo, E. On the ideal associated to a linear code. *Adv. Math. Commun.* **2016**, *10*, 229–254. [CrossRef]
26. Dück, N.; Márquez-Corbella, I.; Martínez-Moro, E. On the fan associated to a linear code. In *Coding Theory and Applications*; CIM Ser. Math. Sci.; Springer: Cham, Switzerland, 2015; Volume 3, pp. 153–160.
27. Berlekamp, E.R.; McEliece, R.J.; van Tilborg, H.C.A. On the inherent intractability of certain coding problems. *IEEE Trans. Inf. Theory* **1978**, *24*, 384–386. [CrossRef]
28. Barg, A. Complexity issues in coding theory. In *Handbook of Coding Theory*; Cambridge University Press: Cambridge, UK, 1998; Volumes I and II, pp. 649–754.
29. Miller, E.; Sturmfels, B. *Combinatorial Commutative Algebra*; Graduate Texts in Mathematics; Springer: New York, NY, USA, 2005; Volume 227, pp. xiv+417.
30. Oxley, J.G. *Matroid Theory*; Oxford Science Publications; The Clarendon Press; Oxford University Press: New York, NY, USA, 1992; pp. xii+532.
31. Herzog, J.; Hibi, T. *Monomial Ideals*; Graduate Texts in Mathematics; Springer: London, UK, 2011.
32. Villarreal, R. *Monomial Algebras*; Chapman & Hall/CRC Monographs and Research Notes in Mathematics; CRC Press: Boca Raton, FL, USA, 2018.
33. Björner, A. The homology and shellability of matroids and geometric lattices. In *Matroid Applications*; Encyclopedia Math. Appl.; Cambridge University Press: Cambridge, UK, 1992; Volume 40, pp. 226–283.
34. Adams, W.W.; Loustaunau, P. *An Introduction to Gröbner Bases*; Graduate Studies in Mathematics; American Mathematical Society: Providence, RI, USA, 1994; Volume 3, pp. xiv+289.
35. Eisenbud, D.; Sturmfels, B. Binomial ideals. *Duke Math. J.* **2008**, *84*, 393–411. [CrossRef]
36. The Sage Developers. SageMath, the Sage Mathematics Software System (Version 9.5). 2022. Available online: https://www.sagemath.org (accessed on 1 May 2022).