Università degli studi di Genova

Scuola di scienze matematiche, fisiche e naturali

Corso di laurea in matematica

Tesi di laurea magistrale

Generalised Hamming weights

Relatrice:
Prof. Emanuela De Negri

Candidato:
Diego Parodi

Anno accademico
2022-2023

Contents

Ringraziamenti

Anzitutto, ringrazio calorosamente la prof. Emanuela de Negri per avermi seguito durante la stesura della tesi e per essere stata sempre disponibile.

Inoltre, ci tengo a ringraziare la mia famiglia che mi ha sostenuto durante tutti questi anni, permettendomi di dedicarmi allo studio senza troppe preoccupazioni.

Infine, ci tengo a ringraziare anche gli amici che sono stati al mio fianco per tutto questo tempo, soprattutto nei momenti di difficoltà.

Notations

We will use the following notations:

$\mathbb{F}_q$ denotes the field with q elements, where q is a prime power.

If n is a positive integer, $[n]$ denotes the set $\{1, 2, ..., n\}$.

If S is a subset of a vector space V, $\langle S \rangle$ denotes the subspace of V generated by S.

Likewise, if S is a subset of a commutative ring R, (S) denotes the ideal of R generated by S.

If X is a set, its cardinality is denoted by $|X|$ and its power set is denoted by 2^X.

If X and Y are sets, Y^X denotes the set of functions $X \to Y$. When $Y = k$ is a field, k^X will be considered as a vector space with pointwise addition and scalar multiplication.

$\mathbb{Z}_+$ denotes the set of (strictly) positive integers.

The projective space of dimension r over a field k will be denoted by $\mathbb{P}^r_k$.

If A and B are sets, $A \backslash B$ denotes the set of elements of A which are not in B.

Introduction

The generalised Hamming weights of a linear code are a natural generalisation of the notion of minimum distance, which have some applications in the context of code-based cryptography, for example to type II wire-tap channels (see [3]).

We will see how to associate a matroid to each linear code and how the notion of generalised Hamming weight naturally carries over to matroids. This will allow us to use techniques from commutative algebra and matroid theory to relate the generalised Hamming weights of a matroid to the Betti numbers of its associated Stanley-Reisner rings, through a famous result of Johnsen and Verdure [5].

Along the way, we will also see how to relate the Hamming weights of a matroid to those of its dual, in a way that generalises a famous result of Wei [3].

Finally, we notice that using Johnsen-Verdure's theorem to calculate the generalised Hamming weights of a code is very inefficient, and study a different approach based on the theory of Gröbner bases, which is still an open area of research [7].

Chapter 1

Generalised Hamming weights of linear codes

In this chapter we define and give some basic properties of the generalised Hamming weights of a linear code.

We briefly recall a couple of fundamental definitions

Definition 1.1. *Let q be a prime power, n a positive integer*

i) An $[n, k]$-code over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$.

ii) If $x \in \mathbb{F}_q^n$, its support is $\mathrm{supp} x = \{i \in [n] : x_i \neq 0\}$.

iii) The weight of x is $w(x) = |\mathrm{supp} x|$.

iv) If C is an $[n, k]$-code, its minimum distance is

$$d(C) = \min\{w(x) : x \in C \backslash \{0\}\}.$$

If $d(C) = d$, we say that C is an $[n, k, d]$-code.

v) A subcode of C is just a subspace of C.

We can generalise the notions of support and weight to all subset of $\mathbb{F}_q^n$.

Definition 1.2. *The support of $S \subseteq \mathbb{F}_q^n$ is*

$$\mathrm{supp}(S) = \{i \in [n] : \exists x \in S \ s.t. \ x_i \neq 0\}.$$

In other words, it is the set of indices $i \in [n]$ such that at least one element of S has non-zero i-th coordinate.

The weight of S, denoted by $w(S)$, is the cardinality of its support:

$$w(S) = |\mathrm{supp}(S)|.$$

Proposition 1.1. *Let $S, T \subseteq \mathbb{F}_q^n$, then* *i)* $\operatorname{supp}(S \cup T) = \operatorname{supp}(S) \cup \operatorname{supp}(T)$.

ii) *If* $S \subseteq T$ *then* $\operatorname{supp}(S) \subseteq \operatorname{supp}(T)$.

iii) $\operatorname{supp}(\langle S \rangle) = \operatorname{supp}(S)$.

Proof. *i*) and *ii*) are straightforward and the inclusion $\operatorname{supp}(S) \subseteq \operatorname{supp}(\langle S \rangle)$ follows from *ii*), so it remains to prove the opposite inclusion. Let $i \in \operatorname{supp}(\langle S \rangle)$, then there is some $x \in \langle S \rangle$ such that $x_i \neq 0$. There are also $y_1, .., y_c \in S$ and $\lambda_1, ..., \lambda_c \in \mathbb{F}_q$ such that $x = \lambda_1 y_1 + ... + \lambda_c y_c$, and we have that

$$x_i = \lambda_1 y_{1i} + ... + \lambda_c y_{ci} \neq 0$$

so there must be some j such that $y_{ji} \neq 0$, otherwise, if they were all zero, x_i would also be zero. But $y_j \in S$, therefore $i \in \operatorname{supp}(S)$. □

As an immediate consequence, we have that, if $x \in \mathbb{F}_q^n$, then $w(x) = w(\langle x \rangle)$. But then we can express the minimum distance of a linear code C as

$$d(C) = \min\{w(D) : D \text{ is a 1-dimensional subcode of } C\}.$$

This might seem a bit convoluted, but it lands itself to the following generalization:

Definition 1.3. *Let C be an $[n, k]$-code over $\mathbb{F}_q$ and let $r \in [k]$. The r-th generalised Hamming weight of C is*

$$d_r(C) = \min\{w(D) : D \textit{ is a k-dimensional subcode of } C\}.$$

Remark. $d_k(C) = w(C)$, which is the number of indices $i \in [n]$ such that not all elements of C have i-th coordinate equal to zero. Some authors work under the assumption that $d_k(C) = n$, which is not restrictive since, if $d_k(C) < n$, this means that some of the coordinates are effectively useless and we can remove them. More precisely, we can obtain an equivalent code of length equal to $d_k(C)$ by projecting onto the subspace of $\mathbb{F}_q^n$ generated by the elements of the canonical basis which correspond to the indices in the support of C. We won't work under this assumption.

Remark. It is not hard to see that the generalised Hamming weights of a code are invariant under code equivalence.

Proposition 1.2. *Let C be an $[n, k]$-code, $r \in [k]$.*

i) $d_1(C) < d_2(C) < ... < d_k(C)$.

ii) *Generalised singleton bound:* $d_r(C) \leq n - k + r$.

Proof. To see *i*), let $r \in [k - 1]$ and let D be an $r + 1$-dimensional subcode of C such that $w(D) = d_{r+1}(C)$. Let $i \in \operatorname{supp}(D)$, $D' = \{x \in D : x_i = 0\}$. D' is clearly a subcode of C and its dimension is r. To see this, let $y_1, ..., y_c$ be a basis of D' and let $z \in D$ such that $z_i = 1$ (it exists because $i \in \operatorname{supp}(D)$).

Then $y_1, ..., y_c, z$ is a basis for D since they are clearly linearly independent and, if $x \in D$, we have that $x = (x - x_i z) + x_i z$, with $x - x_i z \in D'$, therefore they also generate D. But then $c + 1 = r + 1$, so $c = \dim D = r$ and so $d_r(C) \leq w(D') < w(D) = d_{r+1}(C)$.

ii) follows by observing that

$$n \geq d_k(C) \geq d_{k-1}(C) + 1 \geq d_{k-2}(C) + 2 \geq ... \geq d_r(C) + k - r \qquad \forall r \in [k].$$

□

We say that an $[n, k]$-code C is r-MDS if equality holds in the generalised singleton bound for $d_r(C)$, that is, if $d_r(C) = n - k + r$. Notice that 1-MDS codes are the usual MDS codes. Moreover, it is not hard to see that, if C is r-MDS, then it is s-MDS for all $s \geq r$.

We recall a couple more definitions.

Definition 1.4. *Let C be an $[n, k]$-code over $\mathbb{F}_q$.*

i) A generator matrix for C is a $k \times n$ matrix over $\mathbb{F}_q$ whose rows generate C.

ii) A parity-check matrix for C is a $(n - k) \times n$ matrix H over $\mathbb{F}_q$ such that

$$x \in C \iff Hx^T = 0.$$

We shall see in the next result that the generalised Hamming weights of a code only depend on the linear dependence relations between the columns of any of its parity check matrices.

Proposition 1.3. *Let C be an $[n, k]$-code with parity check matrix H, whose columns we will denote by $h_1, ..., h_n$, and let $l \in [n]$, $r \in [k]$. Then the following are equivalent:*

i) $d_r(C) \leq l$.

ii) There exists an $r \times n$ matrix X with entries in $\mathbb{F}_q$ such that $HX^T = 0$, with maximum rank and with at most l non zero columns.

iii) There exist a subset $I \subseteq [n]$ such that $|I| = l$ and $|I| - \dim\langle h_i : i \in I \rangle \geq r$.

Proof. We first prove that *i)* holds if and only if *ii)* holds. By definition, $d_r(C) \leq l \iff$ there exists an r-dimensional subcode D of C such that $w(D) \leq l$.

To see that $i) \implies ii)$, let D be an r-dimensional subcode of C such that $w(D) \leq l$, also let $x_1, ..., x_r$ be a basis of D and denote the j^{th} coordinate of x_i by x_{ij}. Finally, let X be the $r \times n$ matrix with entries x_{ij}. Since $x_i \in C$ for all i, we have that $HX^T = 0$ and, since they are linearly independent, $\text{rk}X = r$. Moreover, if $I = \operatorname{supp} D$, every element of D has support contained in I, this is true in particular for the x_i, but this means that every column of X which correspond to an index not in I is zero, so that X has at most l nonzero columns since by hypothesis $w(D) = |I| \leq l$.

ii) $\implies$ *i*) is straightforward: just take D to be the subcode generated by the rows of X.

Let's now prove that *ii*) $\implies$ *iii*). Let $I \subseteq [n]$ such that $|I| = l$ and the j^{th} column of X is zero for all $j \notin I$. Let $\phi : \mathbb{F}_q^I \to \mathbb{F}_q^{n-k}$, $(a_i)_{i\in I} \mapsto \sum_{i\in I} a_i h_i$. If $x_1, ..., x_r$ are the rows of X, for all $i \in [r]$ let y_i be the element of $\mathbb{F}_q^I$ defined by $y_{ij} = x_{ij}$ for all $j \in I$. Then, since all the columns of X not indexed by an element of I are zero, $y_1, ..., y_r$ are linearly independent. For the same reason, $\phi(y_i) = Hx_i^T = 0$ for all $i \in [r]$. Therefore, the y_i are r linearly independent elements of $\ker\phi$. By the rank-nullity theorem we have

$$r \le \dim\ker\phi = l - \dim \mathrm{Im}\phi = |I| - \dim\langle h_i : i \in I\rangle.$$

Finally, let's prove that *iii*) $\implies$ *ii*). Let $\phi : \mathbb{F}_q^I \to \mathbb{F}_q^{n-k}$, $(a_i)_{i\in I} \mapsto \sum_{i\in I} a_i h_i$ as before, then, again thanks to the rank-nullity theorem,

$$\dim\ker\phi = l - \dim \mathrm{Im}\phi = l - \dim\langle h_i : i \in I\rangle \ge r.$$

Therefore there exist $y_1, ..., y_r \in \ker\phi$ that are linearly independent. Let $x_1, ..., x_r \in \mathbb{F}_q^n$ be defined by $x_{ij} = \begin{cases} y_j & j \in I \\ 0 & j \notin I \end{cases}$, then, if X is the $r \times n$ matrix with $x_1, ..., x_r$ as rows, X has maximum rank because the x_i are linearly independent and clearly $HX^T = 0$.

□

Corollary 1.3.1. *Let C be an $[n, k]$-code with parity-check matrix H and $r \in [k]$. Then*

$$d_r(C) = \min\{|I| : I \subseteq [n] \text{ and } |I| - \dim\langle h_i : i \in I\rangle \ge r\},$$

where $h_1, ..., h_n$ are the columns of H.

Chapter 2

Simplicial complexes and matroids

In this chapter, we briefly recall some facts about simplicial complexes, matroids and their Stanley-Reisner rings, which will be useful later on.

2.1 Simplicial complexes

Before we introduce matroids, we briefly introduce a more general mathematical structure.

Definition 2.1. *A simplicial complex is a pair $\mathcal{K} = (K, \Delta)$ where K is a finite set and Δ is a collection of subsets of K with the following properties:*

i) $\emptyset \in \Delta$.

ii) If $F \in \Delta$ and $E \subseteq F$ then $E \in \Delta$.

If $\mathcal{K} = (K, \Delta)$ is a simplicial complex,

1. *K is called the ground set of $\mathcal{K}$.*
2. *The elements of Δ are called faces.*
3. *The dimension of a face $F \in \Delta$ is $\dim F = |F| - 1$.*
4. *The dimension of $\mathcal{K}$ is $\max\{\dim F : F \in \Delta\}$.*
5. *The maximal elements of Δ are called facets.*
6. *A subset of K that is not in Δ is called a non-face.*

Remark. One might think of a simplicial complex $\mathcal{K}$ in the following way: take a point for each vertex of $\mathcal{K}$, that is, for every $x \in K$ such that $\{x\} \in \Delta$. Then, for every pair of distinct points x, y such that $\{x, y\} \in \Delta$, connect x and y with a segment, then for every face of dimension 2, connect its three points with a triangle and so on. The points which are not vertices are left out, so some authors require that every point of the ground set is a vertex in the definition. Besides this detail, this construction allows one to think of a simplicial complex in a geometric way.

2.2 Matroids

Definition 2.2. *A matroid is a simplicial complex $\mathcal{M} = (M, \mathcal{I})$ which satisfies the following additional property (M is the ground set and $\mathcal{I}$ is the set of faces):*

iii) For all $\sigma, \tau \in \mathcal{I}$ such that $|\sigma| < |\tau|$, there exists $x \in \tau \backslash \sigma$ such that $\sigma \cup \{x\} \in \mathcal{I}$.

Some of the definitions we previously introduced for simplicial complexes have different names in the context of matroids: if $\mathcal{M} = (M, \mathcal{I})$ is a matroid,

1. The elements of $\mathcal{I}$ are called independent sets.
2. The maximal elements of $\mathcal{I}$ are called bases.
3. A subset of M that is not independent is called dependent.
4. A minimal dependent subset of M is called a circuit.

Remark. This definition might seem a bit obscure at first, but it actually is an abstraction of the notion of linear independence, as the next example shows. That's also why we use a different terminology in this context.

Example. Let V be a vector space, $x_1, ..., x_n \in V$. Let

$$\mathcal{M}(x_1, ..., x_n) = ([n], \mathcal{I}),$$

where $\mathcal{I} = \{\sigma \subseteq [n] : \text{ the } x_i, \text{ with } i \in \sigma, \text{ are linearly independent}\}$. $\mathcal{M}(x_1, ..., x_n)$ is clearly a simplicial complex. It is actually a matroid, this comes from the following basic linear algebra fact: if $v_1, ..., v_n, w_1, ..., w_m \in V$, $m > n$, $v_1, ..., v_n$ are linearly independent and $w_1, ..., w_m$ are also linearly independent, then there is some $i \in [m]$ such that $v_1, ..., v_n, w_i$ are linearly independent.

Definition 2.3. *We call $\mathcal{M}(x_1, ..., x_n)$ the matroid associated to $x_1, ..., x_n$. If the x_i are the columns of a matrix H, we denote it by $\mathcal{M}_H$ and we call it the matroid associated to H.*

The aforementioned linear algebra fact can be used to prove that two bases of a finitely generated vector space have the same cardinality. There is an analogous result for matroids:

Proposition 2.1. *Any two bases of a matroid have the same cardinality.*

Proof. Let B_1, B_2 be two bases of a matroid $\mathcal{M}$. Assume by contradiction that they don't have the same cardinality. Then one of them, let's say B_1, has more elements than the other. But B_1 and B_2 are independent, therefore there exists $x \in B_1 \backslash B_2$ such that $B_2 \cup \{x\}$ is independent, which contradicts the maximality of B_2. □

Definition 2.4. *Let $\mathcal{M} = (M, \mathcal{I})$ be a matroid.*

- *The rank of $\mathcal{M}$, denoted by $\rho(\mathcal{M})$, is the cardinality of any of its bases.*
- *If $\sigma \subseteq M$, let $\mathcal{I}|_\sigma = \{\tau \in \mathcal{I} : \tau \subseteq \sigma\}$. Then $\mathcal{M}|_\sigma = (\sigma, \mathcal{I}|_\sigma)$, which is clearly a matroid, is called the restriction of $\mathcal{M}$ to σ.*
- *We also denote the rank of $\mathcal{M}|_\sigma$ by $\rho(\sigma)$. The function ρ that maps $\sigma \subseteq M$ to $\rho(\sigma)$ is called the rank function of $\mathcal{M}$.*
- *The nullity of σ is $n(\sigma) = |\sigma| - \rho(\sigma)$.*

Remark. $\rho(\sigma)$ is the cardinality of the largest independent set contained σ. In particular, $\rho(\mathcal{M}) = \dim \mathcal{M} + 1$.

We defined matroids in terms of independent sets, but one can define matroids in various equivalent ways. The next theorems say that we can define a matroid by specifying its bases, its rank function, its nullity function or its circuits. Their proof can be found in [1], with the exception of theorem 2.4 which follows in part from theorem 2.3.

Theorem 2.2. *Let $\mathcal{M}$ be a matroid, $\mathcal{B}$ its set of bases, then*

B1) $\mathcal{B} \neq \emptyset$.

B2) *If $B_1, B_2 \in \mathcal{B}$ and $B_1 \neq B_2$, then for all $x_1 \in B_1 \backslash B_2$, there exists $x_2 \in B_2 \backslash B_1$ such that $(B_1 \backslash \{x_1\}) \cup \{x_2\} \in \mathcal{B}$.*

Moreover, if $\mathcal{B} \subseteq 2^M$ satisfies B1) and B2), there exist a unique matroid structure on M that has the elements of $\mathcal{B}$ as bases. It is obtained by declaring a subset of M to be independent if and only if it is contained in an element of $\mathcal{B}$.

Theorem 2.3. *Let $\mathcal{M}$ be a matroid, ρ its rank function, then*

R1) *$\rho(\sigma) \leq |\sigma|$ for all $\sigma \subseteq M$.*

R2) *If $\sigma \subseteq \tau \subseteq M$, then $\rho(\sigma) \leq \rho(\tau)$.*

R3) *For all $\sigma, \tau \subseteq M$, $\rho(\sigma \cup \tau) + \rho(\sigma \cap \tau) \leq \rho(\sigma) + \rho(\tau)$.*

Moreover, if $\rho : 2^M \to \mathbb{N}$ is a function that satisfies R1), R2) and R3), there is a unique matroid structure on M whose rank function is ρ, it is obtained by declaring a subset σ of M to be indepenent if and only if $\rho(\sigma) = |\sigma|$.

Theorem 2.4. *Let $\mathcal{M}$ be a matroid, n its nullity function, then*

N1) *$n(\sigma) \leq |\sigma|$ for all $\sigma \subseteq M$.*

N2) If $\sigma \subseteq \tau \subseteq M$, then $n(\sigma) \leq n(\tau)$.

N3) For all $\sigma, \tau \subseteq M$, $n(\sigma \cup \tau) + n(\sigma \cap \tau) \geq n(\sigma) + n(\tau)$.

Moreover, if $n : 2^M \to \mathbb{N}$ is a function that satisfies N1), N2) and N3), there is a unique matroid structure on M whose nullity function is n, it is obtained by declaring a subset σ of M to be indepenent if and only if $n(\sigma) = 0$.

Theorem 2.5. *Let $\mathcal{M}$ be a matroid, $\mathcal{C}$ its set of circuits, then*

C1) $\emptyset \notin \mathcal{C}$.

C2) If $\sigma, \tau \in \mathcal{C}$ and $\sigma \subseteq \tau$, then $\sigma = \tau$.

C3) If $\sigma, \tau \in \mathcal{C}$ and $x \in \sigma \cap \tau$, then there exists $\eta \in \mathcal{C}$ such that $\eta \subseteq (\sigma \cup \tau) \backslash \{x\}$ (that is, $(\sigma \cup \tau) \backslash \{x\}$ is dependent).

Moreover, if $\mathcal{C} \subseteq 2^M$ satisfies C1), C2) and C3), there exist a unique matroid structure on M that has the elements of $\mathcal{C}$ as circuits. It is obtained by declaring a subset of M to be independent if and only if it does not contain an element of $\mathcal{C}$ as a subset.

2.3 Stanley-Reisner rings and their Betti numbers

Stanley-Reisner rings are a useful algebraic invariant that can be associated to simplicial complexes and, in particular, to matroids.

Definition 2.5. *Let $\mathcal{K} = (K, \Delta)$ be a simplicial complex, k a field. Let $S = k[\mathbf{x}]$ be the polynomial ring in $|K|$ indeterminates $\mathbf{x} = \{x_e : e \in K\}$. If $F \subseteq K$, let $\mathbf{x}^F = \prod_{e \in F} x_e$.*

i) The Stanley-Reisner ideal of $\mathcal{K}$ is

$$I_{\mathcal{K}} = (\mathbf{x}^F : F \notin \Delta).$$

ii) The Stanley-Reisner ring associated to $\mathcal{K}$ is $R_{\mathcal{K}} = S/I_{\mathcal{K}}$.

Remark. $I_{\mathcal{K}}$ is a monomial ideal with minimal set of generators

$$\{\mathbf{x}^F : F \text{ is a minimal non-face of } \mathcal{K}\}.$$

Notice that the monomial ideals in $S = k[X_1, ..., X_n]$ are precisely those ideals which are homogeneous with respect to the canonical $\mathbb{Z}^n$ grading of S, that is, the $\mathbb{Z}^n$-grading $S = \bigoplus_{\alpha \in \mathbb{Z}^n} S_\alpha$, where $S_\alpha = k$ for all $\alpha \in \mathbb{N}^n$ and $S_\alpha = 0$ otherwise.

In particular, $R_{\mathcal{K}}$ admits a minimal free resolution as a $\mathbb{Z}^K$-graded module of the form

$$0 \to F_p \xrightarrow{\partial_p} ... \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} R_{\mathcal{K}} \to 0,$$

where each F_i is a free $\mathbb{Z}^K$-graded S-module, which can be written as

$$F_i = \bigoplus_{\alpha \in \mathbb{Z}^K} S(-\alpha)^{\beta_{i,\alpha}}$$

The resolution being minimal means that $\ker \partial_i \subseteq \mathfrak{m} F_i$ for all i, where $\mathfrak{m}$ is the maximal ideal $(x_e : e \in K)$.

We also have that p and the $\beta_{i,\alpha}$ are independent of the choice of minimal resolution:

- p is the projective dimension of $R_{\mathcal{K}}$: it is the minimal length of a $\mathbb{Z}^K$-graded projective resolution of $R_{\mathcal{K}}$.
- For each i and for each $\alpha \in \mathbb{Z}^K$, $\beta_{i,\alpha} = \dim_k \operatorname{Tor}_i(R_{\mathcal{K}}, k)_\alpha$, where we see k as an S-module by identifying it with the quotient $S/\mathfrak{m}$.

The $\beta_{i,\alpha}$ are called the $\mathbb{Z}^K$-graded, or multi-graded, Betti numbers of $\mathcal{K}$ over k and are denoted by $\beta_{i,\alpha}(\mathcal{K}, k)$.

We can also see S as a $\mathbb{Z}$-graded algebra: $S = \bigoplus_{d \in \mathbb{Z}} S_d$, where S_d is the space of all homogeneous polynomials of degree d in S if $d \geq 0$, and $S_d = 0$ otherwise. Since monomials are homogeneous, we have that $R_{\mathcal{K}}$ is also $\mathbb{Z}$-graded and we can define the $\mathbb{Z}$-graded Betti numbers of $\mathcal{K}$ over k, denoted by $\beta_{i,d}(\mathcal{K}, k)$ for all $d \in \mathbb{Z}$, in the same way by considering a minimal $\mathbb{Z}$-graded resolution of $R_{\mathcal{K}}$. However, notice that a minimal $\mathbb{Z}^K$-graded resolution of $R_{\mathcal{K}}$ is also minimal as a $\mathbb{Z}$-graded resolution. The reason is that the unique $\mathbb{Z}^K$-homogeneous maximal ideal of S is also its unique $\mathbb{Z}$-homogeneous maximal ideal, which is $\mathfrak{m}$. Finally, notice that, if $\alpha \in \mathbb{Z}^K$ and $|\alpha| = \sum_{e \in K} \alpha_e$, $S(-\alpha)$, when seen as an $\mathbb{Z}$-graded S-module, is just $S(-|\alpha|)$. Therefore, for all i, we have

$$F_i = \bigoplus_{\alpha \in \mathbb{Z}^K} S(-\alpha)^{\beta_{i,\alpha}(\mathcal{K},k)} = \bigoplus_{d \in \mathbb{Z}} S(-d)^{\sum_{|\alpha|=d} \beta_{i,\alpha}(\mathcal{K},k)},$$

hence

$$\beta_{i,d}(\mathcal{K}, k) = \sum_{|\alpha|=d} \beta_{i,\alpha}(\mathcal{K}, k)$$

for all i, d. Finally, we also have the global Betti numbers:

$$\beta_i(\mathcal{K}, k) := \sum_{d \in \mathbb{N}} \beta_{i,d}(\mathcal{K}, k) = \sum_{\alpha \in \mathbb{N}^K} \beta_{i,\alpha}(\mathcal{K}, k),$$

which are just the ranks of the free $S-$modules appearing in the minimal graded resolution, disregarding their grading.

2.4 Simplicial Homology and Hochster's theorem

Let $\mathcal{K} = (K, \Delta)$ be a d-dimensional simplicial complex and let k be a field. For all $i \in \mathbb{N}$ let F_i be the set of i-dimensional faces of $\mathcal{K}$ and let V_i be the free vector space on F_i, that is, its elements are formal k-linear combinations of elements of F_i. Suppose that the elements of K are ordered by a total ordering ω (for example, if $K = [n]$ there is a canonical way to order the elements of K).

For all $i \in \mathbb{N}$ and for all $F \in F_i$, let $\partial_{i,\omega}(F) = \sum_{x\in F} \varepsilon_{\omega,F}(x)(F\backslash\{x\}) \in V_{i-1}$, then extend $\partial_{i,\omega}$ to V_i by linearity. One can prove that $\partial_{i,\omega} \circ \partial_{i+1,\omega} = 0$ for all $i \in \mathbb{N}$, thus we obtain a complex of vector spaces

$$\cdots \to V_i \xrightarrow{\partial_{i,\omega}} V_{i-1} \to \cdots \to V_1 \xrightarrow{\partial_{1,\omega}} V_0 \to 0.$$

This is called the (reduced) chain complex of $\mathcal{K}$. Its homology in position i is the vector space

$$\tilde{H}_i(\mathcal{K}, k) := \ker \partial_{i,\omega}/\mathrm{Im}\partial_{i+1,\omega}.$$

Its dimension will be denoted by $\tilde{h}_i(\mathcal{K}, k)$. We omitted ω in the notation because, up to isomorphism, $\tilde{H}_i(\mathcal{K}, k)$ does not depend on the choice of ω. A famous result of Hochster (see [2]) relates the multi-graded Betti numbers of a simplicial complex to the homology of its subcomplexes:

Theorem 2.6 (Hochster)**.** *Let $\mathcal{K} = (K, \Delta)$ be a simplicial complex and let $\alpha \in \mathbb{Z}^K$. Also, let $E = \{x \in K : \alpha_x \neq 0\}$ and let $\mathcal{K}|_E$ be the simplicial complex (E, Δ_E), where $\Delta_E = \{F \cap E : F \in \Delta\} = \{F \in \Delta : F \subseteq E\}$. Then*

i) If $\alpha \notin \{0, 1\}^K$ then $\beta_{i,\alpha}(\mathcal{K}, k) = 0$.

ii) If $\alpha \in \{0, 1\}^K$ then

$$\beta_{i,\alpha}(\mathcal{K}, k) = \tilde{h}_{|E|-i-1}(\mathcal{K}|_E, k).$$

As a consequence, the multi-indices which can give non-zero Betti numbers are only the ones with values in $\{0, 1\}$, but we have a bijection $2^K \to \{0, 1\}^K$, $E \mapsto \mathbf{1}_E$, where $\mathbf{1}_E$ is the function that sends $i \in E$ to 1 and $i \notin E$ to 0. Thus, if $E \subseteq K$, we let $\beta_{i,E}(\mathcal{K}, k) := \beta_{i,\mathbf{1}_E}(\mathcal{K}, k)$.

Chapter 3

Generalised Hamming weights of matroids

In this chapter, we define generalised Hamming weights in the context of matroids, in a way that generalises the previous definition we gave in the context of linear codes. In order to do so, we shall briefly see how to associate a matroid to a linear code.

3.1 Matroids associated to linear codes

Let k be a field, V a vector space over k, $v_1, ..., v_n \in V$ and

$$f : k^n \to V,\ x \mapsto \sum_{i=1}^{n} x_i v_i.$$

Proposition 3.1. *$\mathcal{M}(v_1, ..., v_n)$ is uniquely determined by $\ker f$ as a subspace of k^n. More precisely, we have that $\sigma \subseteq [n]$ is dependent if and only if there exists $x \in \ker f \backslash \{0\}$ such that $\operatorname{supp} x \subseteq \sigma$.*

Proof. $\sigma \subseteq [n]$ is dependent $\iff$ $\{v_i : i \in \sigma\}$ is a set of linearly dependent vectors $\iff$ There are x_i, with $i \in \sigma$, not all zero such that $\sum_{i \in \sigma} x_i v_i = 0$ $\iff$ There exists $x \in \ker f \backslash \{0\}$ such that $\operatorname{supp} x \subseteq \sigma$. □

As a consequence, if C is a linear code, the matroid associated to a parity check matrix H of C does not depend on the choice of H because $C = \ker f$, where $f : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k},\ x \mapsto \sum_{i=1}^{n} x_i h_i = Hx^T$ and $h_1, ..., h_n$ are the columns of H.

Definition 3.1. *The matroid associated to a linear code C, denoted by $\mathcal{M}_C$, is the matroid associated to any of its parity-check matrices.*

Remark. If C is an $[n, k]$-code, $\rho(\mathcal{M}_C) = n - k$ and $n(\mathcal{M}_C) = k$.

Example. Let $C = H_3(2)$ be the binary Hamming code with parameter 2. C is a $[7,4]$-code with parity check matrix

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

The columns of H are all the non zero vectors in $\mathbb{F}_2^3$, denote them by $h_1, ..., h_7$. Notice that any two columns of H are linearly independent.

We have that $\rho(\mathcal{M}_C) = n - k = 3$, so, in order to find all the bases of $\mathcal{M}_C$, we just need to find all the independent subsets of cardinality 3. Since linear combinations over F_2 are just sums, and since $-1 = 1$ in $\mathbb{F}_2$, the independent subsets of $\mathcal{M}_C$ with three elements are just all the subsets $\{i, j, k\}$ such that $h_i \neq h_j + h_k$.

Now, let's try to find the rank function of $\mathcal{M}_C$. Any two columns of a H are linearly independent, so every subset of $[7]$ with two or less elements is independent and therefore has rank equal to its cardinality. A subset of cardinality 3 is dependent if and only if it is of the form $\{i, j, k\}$ such that $h_i = h_j + h_k$, in which case it has rank 2, otherwise it has rank 3. Now, take a subset $\sigma \subseteq [7]$ such that $|\sigma| \geq 4$ and take $i, j \in \sigma$ such that $i \neq j$. Since $h_i \neq h_j$, we have that $h_i + h_j \neq 0$, therefore $h_i + h_j = h_k$ for some k because the columns of H are all the nonzero vectors in $\mathbb{F}_2^3$, but then, since $|\sigma| \geq 4$, there certainly is some $l \in \sigma$ such that $l \neq i$, $l \neq j$ and $l \neq k$, so $h_l \neq h_i + h_j$, therefore $\{i, j, l\} \subseteq \sigma$ is independent and σ has rank 3. To summarize, we have that

- The subsets of rank 0 and 1 are the empty set and the singletons respectively.
- The subsets of rank 2 are those with two elements and those of the form $\{i, j, k\}$ such that $h_k \neq h_i + h_j$.
- The subsets of rank 3 are all the others, in particular all subsets of cardinality at least 4 have rank 3.

3.2 Generalised Hamming weights of matroids

Recall that, if C is am $[n, k]$-code with parity check matrix H, the generalised Hamming weights of C can be described as follows:

$$d_r(C) = \min\{|I| : I \subseteq [n] \text{ and } |I| - \dim\langle h_i : i \in I\rangle \geq r\} \text{ for all } r = 1, ..., k$$

It is not hard to see that $\dim\langle h_i : i \in I\rangle$ is the rank of I as a subset of the matroid $\mathcal{M}_C$, therefore we have that

$$d_r(C) = \min\{|\sigma| : \sigma \subseteq [n] \text{ and } n(\sigma) \geq r\}.$$

Therefore we can generalise the definition to matroids as follows:

Definition 3.2. *Let $\mathcal{M} = (M, \mathcal{I})$ be a matroid, $r \in \mathbb{Z}_+$. If there exists $\sigma \subseteq M$ such that $n(\sigma) \geq r$, we say that the r^{th} generalised Hamming weight of $\mathcal{M}$ exists, and define it as*

$$d_r(\mathcal{M}) = \min\{|\sigma| : \sigma \subseteq M,\ n(\sigma) \geq r\}.$$

Proposition 3.2. *Let $\mathcal{M} = (M, \mathcal{I})$ be a matroid, $r \in \mathbb{Z}_+$.*

i) $d_r(\mathcal{M})$ exists if and only if $r \leq n(M)$.

ii) $d_r(\mathcal{M}) < d_{r+1}(\mathcal{M})$ for all r.

iii) $d_r(\mathcal{M}) = \min\{|\sigma| : \sigma \subseteq M,\ n(\sigma) = r\}$.

Proof. Let's prove *i*). First, suppose that $d_r(\mathcal{M})$ exists, that is, there exists $\sigma \subseteq M$ such that $n(\sigma) \geq r$, but then $n(\sigma) \geq s$ for all $s \leq r$. Therefore, if $d_r(\mathcal{M})$ exists, $d_s(\mathcal{M})$ also exists for all $s \leq r$ and $d_{n(\mathcal{M})}(\mathcal{M})$ clearly exists, therefore $d_r(\mathcal{M})$ exists for all $r \leq n(M)$. If $d_r(\mathcal{M})$ existed for some $r > n(M)$ then there would be some $\sigma \subseteq M$ such that $n(\sigma) \geq r > n(M)$, but this is impossible because of theorem 2.4.

Let's now prove *ii*). That $d_r(\mathcal{M}) \leq d_{r+1}(\mathcal{M})$ is clear, since, when we calculate $d_{r+1}(\mathcal{M})$, the minimum is taken over a smaller set. Now, let $\sigma \subseteq M$ such that $n(\sigma) \geq r + 1$ and let B be a basis of σ, $x \in \sigma \backslash B$ (which exists because $|\sigma \backslash B| = n(\sigma) > 0$). It is clear, then, that B is a basis of $\sigma \backslash \{x\}$, therefore $n(\sigma \backslash \{x\}) = n(\sigma) - 1 \geq r$. As a consequence, $d_r(\mathcal{M}) \leq d_{r+1}(\mathcal{M}) - 1 < d_{r+1}(\mathcal{M})$.

Finally, let's prove *iii*). Suppose that $\{|\sigma| : \sigma \subseteq M,\ n(\sigma) \geq r\}$ attains its minimum at $\tau \subseteq M$. Suppose by contradiction that $n(\tau) > r$. Then, if B is a basis of τ and $x \in \tau \backslash B$, we have that $n(\tau \backslash \{x\}) = n(\tau) - 1 \geq r$, with $|\tau \backslash \{x\}| < |\tau|$, which contradicts the minimality of $|\tau|$. □

We refer to the increasing sequence $d_1(\mathcal{M}), \ldots, d_{n(\mathcal{M})}(\mathcal{M})$ as the weight hierarchy of $\mathcal{M}$.

Example. Let r, n be positive integers with $r \leq n$. The uniform matroid $U_{r,n}$ is the matroid that has $[n]$ as its ground set and whose independent sets are the subsets of $[n]$ with cardinality less than or equal to r. One can easily check that $U_{r,n}$ is indeed a matroid. If $\sigma \subseteq [n]$, the rank of σ is $\rho(\sigma) = \min\{r, |\sigma|\}$, as if $|\sigma| \leq r$ then $|\sigma|$ is independent, whereas if $|\sigma| > r$ then any subset of σ of cardinality r is a basis of σ. Thus we have that

$$n(\sigma) = |\sigma| - \min\{r, |\sigma|\} = \max\{|\sigma| - r, 0\}$$

Therefore, if $k \leq n(U_{r,m}) = n - r$,

$$d_k(U_{r,m}) = \min\{|\sigma| : \sigma \subseteq [n],\ \max\{|\sigma| - r, 0\} = k\}$$
$$= \min\{|\sigma| : \sigma \subseteq [n],\ |\sigma| = r + k\} = r + k$$

Thus the weight hierarchy of $U_{r,n}$ is $r + 1, r + 2, \ldots, n$.

Example. Let C be the Hamming code $H_3(2)$. In the previous chapter, we found the rank function of $\mathcal{M}_C$, so we can also easily find the nullity function:

- The subsets of nullity 0 are the independent ones, i.e. the ones of cardinality less than 3 and those of the form $\{i, j, k\}$ such that $h_k \neq h_i + h_j$.
- The subsets of nullity 1 are those of the form $\{i, j, k\}$ such that $h_k = h_i + h_j$ and all the ones with 4 elements.
- The subsets of nullity 2, 3 and 4 are, respectively, those of cardinality 5, 6 and 7.

But then it immediately follows that the weight hierarchy of C is $3, 5, 6, 7$. Notice that $d_2(C) = 5 = 7 - 4 + 2 = n - k + 2$, so C is 2-MDS.

3.3 Generalised Hamming weights of Hamming codes

In this section, we calculate the Hamming weights of all Hamming codes. In order to do that, we will interpret the matroids associated to them in a more geometric way. First of all, we briefly recall their definition.

Definition 3.3. *Let $r \in \mathbb{N}$, $r \geq 2$. A q-ary code C is said to be a Hamming code with defining parameter r if it has a parity check matrix whose columns form a maximal subset of pairwise linearly independent vectors of $\mathbb{F}_q^r$.*

We also recall a couple of important properties:

i) A q-ary Hamming code with parameter r always exists: just take a code with a parity check matrix whose columns form a full set of representatives of the equivalence classes in $\mathbb{P}_{\mathbb{F}_q}^{r-1}$ (that is, each column belongs to only one class and each class contains one of the columns).

ii) Any two q-ary Hamming codes with parameter r are equivalent, we thus denote them by $H_r(q)$.

iii) $H_r(q)$ is a $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]$-code.

Now we define a class of matroid associated to finite projective spaces.

Definition 3.4. *Let $r \in \mathbb{Z}_+$. The q-ary projective matroid of dimension r is the matroid, which we denote by $\mathcal{PM}(r, q)$, with ground set $\mathbb{P}_{\mathbb{F}_q}^r$ and where we declare $\sigma \subseteq \mathbb{P}_{\mathbb{F}_q}^r$ to be independent if and only if the smallest hyperplane of $\mathbb{P}_{\mathbb{F}_q}^r$ containing σ has dimension equal to $|\sigma| - 1$, where a hyperplane of $\mathbb{P}_{\mathbb{F}_q}^r$ is just the image under the natural projection $\pi : \mathbb{F}_q^{r+1} \backslash \{0\} \to \mathbb{P}_{\mathbb{F}_q}^r$, $x \mapsto [x]$ of a nonzero subspace of $\mathbb{F}_q^{r+1}$, and its dimension is one less than the dimension of that subspace.*

For example, any two distinct points of $\mathbb{P}_{\mathbb{F}_q}^r$ form an independent subset, whereas three point that lie on the same line form a dependent subset.

Lemma 3.3. *$\mathcal{PM}(q, r)$ is a matroid and it is isomorphic to $\mathcal{M}_{H_{r+1}(q)}$.*

Proof. Let H be a parity check matrix of $H_{r+1}(q)$ such that its columns form a maximal set of pairwise linearly independent vectors in $\mathbb{F}_q^{r+1}$. Denote its columns by $h_1, ..., h_n$ and let $\phi : [n] \to \mathbb{P}^r_{\mathbb{F}_q}$, $i \mapsto [h_i]$, where $n = \frac{q^{r+1}-1}{q-1}$. Clearly, ϕ is a bijection, moreover, it is not hard to see that $\sigma \subset \mathbb{P}^r_{\mathbb{F}_q}$ is independent if and only if $\phi^{-1}(\sigma)$ is an independent set of $\mathcal{M}_{H_{r+1}(q)}$. From this, both claims follow. □

The rank of a subset $\sigma \subseteq \mathbb{P}^r_{\mathbb{F}_q}$ is one plus the dimension of the smallest hyperplane of $\mathbb{P}^r_{\mathbb{F}_q}$ containing σ. In particular, $n(\mathbb{P}^r_{\mathbb{F}_q}) = |\mathbb{P}^r_{\mathbb{F}_q}| - \rho(\mathbb{P}^r_{\mathbb{F}_q})| = \frac{q^{r+1}-1}{q-1} - (r+1)$.

We are now going to rigorously calculate the Hamming weights of $\mathcal{PR}(r,q)$, but, before we do that, we give a heuristic motivation as to why we should expect them to be what they are. Let $k = n(\mathbb{P}^r_{\mathbb{F}_q}) = \frac{q^{r+1}-1}{q-1} - (r+1)$ and $i \in [k]$. Let's try to construct a subset σ with nullity i and with the least possible cardinality. Let P, Q be two distinct points in $\mathbb{P}^r_{\mathbb{F}_q}$, then $\{P, Q\}$ is independent, so we need to add at least i points. If we were to add a point not lying on the line joining P and Q, then we would increase the cardinality of σ without increasing its nullity. If instead we only add points on the line joining P and Q we increase both the nullity and the cardinality of σ at the same rate, however we can only do this until the line joining P and Q, which has cardinality $q + 1 = \frac{q^2-1}{q-1}$, gets filled. So we can do this if $i \leq \frac{q^2-1}{q-1} - 2$, otherwise at some point we need to add at least one point R which is not on the line, then the best thing to do is to fill the plane generated by P, Q and R, which has cardinality $\frac{q^3-1}{q-1}$, and we can do this if $i \leq \frac{q^3-1}{q-1} - 3$, otherwise we need to add a fourth point not on the plane and so on. As a consequence, one would expect that $d_i = i + s$ if $\frac{q^{s-1}-1}{q-1} - (s-1) < i \leq \frac{q^s-1}{q-1} - s$, where $d_i = d_i(\mathcal{PM}(r,q))$.

Before we continue, notice that the sequence $\left(\frac{q^n-1}{q-1} - n\right)_{n \in \mathbb{Z}_+}$ is strictly increasing. One can check this, for example, with the formula $\frac{q^n-1}{q-1} = 1 + q + q^2 + ... + q^{n-1}$.

Theorem 3.4. *Let $r \in \mathbb{Z}_+$, $i \in \left[\frac{q^{r+1}-1}{q-1} - (r+1)\right]$, $s \in \mathbb{Z}_+$ such that*

$$\frac{q^{s-1}-1}{q-1} - (s-1) < i \leq \frac{q^s-1}{q-1} - s.$$

Then $d_i(\mathcal{P}M(r,q)) = i + s$.

Moreover, the Hamming weights of $\mathcal{PM}(r,q)$ are the elements of the complement of $\{\frac{q^s-1}{q-1} + 1 : 0 \leq s \leq r\}$ in $\left[\frac{q^{r+1}-1}{q-1}\right]$.

Proof. Let $m_i = \min\{\rho(\sigma) : n(\sigma) = i\}$, then $d_i(\mathcal{PM}(r,q)) = m_i + i$ and we just need to prove that $m_i = s$. If we take an independent subset $\sigma \subseteq \mathbb{P}^r_{\mathbb{F}_q}$ with cardinality s, then the smallest hyperplane containing σ has cardinality $n = \frac{q^s-1}{q-1}$ and, since $i \leq n - s$, we can find i points in the hyperplane which are not contained in σ. If we add those points to σ, we obtain a subset with nullity i and rank s, so $m_i \leq s$.

If $s = 2$, then we get that $m_i \leq 2$, but 2 is also the minimal rank of a dependent subset of $\mathbb{P}^r_{\mathbb{F}_q}$, therefore $m_i = 2$, so we assume from now on that $s \geq 3$.

Assume, by contradiction, that $m_i < s$, then there exists $\sigma \subseteq \mathbb{P}^r_{\mathbb{F}_q}$ with nullity i and such that $\rho(\sigma) \leq s-1$. In other words, σ is contained in a hyperplane H of dimension $s-2$, but then $i = n(\sigma) \leq n(H) = |H| - \rho(H) = \frac{q^{s-1}-1}{q-1} - (s-1)$, which is a contradiction.

The second claim follows from observing that the indices i such that $\frac{q^{s-1}-1}{q-1} - (s-1) < i \leq \frac{q^s-1}{q-1} - s$ give rise to the Hamming weights

$$\frac{q^{s-1}-1}{q-1} + 2, \frac{q^{s-1}-1}{q-1} + 3, ..., \frac{q^s-1}{q-1}$$

If we put these together for all s, we get all the integers between 1 and $\frac{q^{r+1}-1}{q-1}$, except for the ones of the form $\frac{q^s-1}{q-1} + 1$, with $0 \leq s \leq r$. □

Corollary 3.4.1. *The generalised Hamming weight of the Hamming code $H_r(q)$ are the elements in the complement of $\{\frac{q^s-1}{q-1} + 1 : 0 \leq s \leq r-1\}$ in $\left[\frac{q^r-1}{q-1}\right]$.*

Corollary 3.4.2. *$H_r(q)$ is $\left(\frac{q^{r-1}-1}{q-1} - r + 2\right)$-MDS and is not $\left(\frac{q^{r-1}-1}{q-1} - r + 1\right)$-MDS.*

Proof. The last integer in $\left[\frac{q^r-1}{q-1}\right]$ which is not a Hamming weight of $H_r(q)$ is $\frac{q^{r-1}-1}{q-1} + 1$, so $\frac{q^{r-1}-1}{q-1} + 2$ is a Hamming weight and the there are exactly r positive integers before it which are not Hamming weights, therefore it is the $\left(\frac{q^{r-1}-1}{q-1} - r + 2\right)^{th}$ one, but the singleton bound for this weight is

$$\frac{q^r-1}{q-1} - \left(\frac{q^r-1}{q-1} - r\right) + \left(\frac{q^{r-1}-1}{q-1} - r + 2\right) = \frac{q^{r-1}-1}{q-1} + 2$$

which proves that $H_r(q)$ is $\left(\frac{q^{r-1}-1}{q-1} - r + 2\right)$-MDS.

The weight before this one is $\frac{q^{r-1}-1}{q-1}$ and the same reasoning leads to the fact that it is one less than its corresponding singleton bound. □

Remark. The generalised Hamming weights of $H_r(2)$ are the integers in $[2^r - 1]$ which are not powers of 2.

Example. We previously calculated the weight Hierarchy of $H_3(2)$ to be 3,5,6,7, which is also what we get when we remove the powers of 2 from the integers between 1 and 7.

Chapter 4

Duality

Recall that, given an $[n, k]$ code C over $\mathbb{F}_q$, its dual is

$$C^{\perp} := \{x \in \mathbb{F}_q^n : x \cdot y = 0 \text{ for all } y \in C\}$$

where $x \cdot y = x_1 y_1 + ... + x_n y_n$. $C^{\perp}$ is an $[n, n-k]$-code, and one might be interested in knowing its minimum distance in terms of some parameters of C. There is indeed an interesting relationship, as stated by a famous result of MacWilliams. Recall that the enumerator polynomial of C is defined as $A_C(z) = \sum_{x \in C} z^{w(x)}$.

Theorem 4.1 (MacWilliams)**.** *Let C be an $[n, k]$-code over $\mathbb{F}_q$, A its enumerator polynomial and B the enumerator polynomial of $C^{\perp}$. Then*

$$B(z) = \frac{1}{|C|}(1 + (q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right).$$

If $A_C(z) = \sum_{i=0}^{n} A_i z^i$, the minimum distance of C is the minimum $i > 0$ such that $A_i \neq 0$, so MacWilliams' theorem allows one to calculate the minimum distance of $C^{\perp}$, provided that we know the enumerator polynomial of C.

One might ask if there is some relationship between the Generalised Hamming weights of C and those of $C^{\perp}$. The following theorem, due to Wei, gives a nice relationship between the two:

Theorem 4.2 (Wei's duality theorem)**.** *Let C be an $[n, k]$ code, $d_1, ..., d_k$ the generalised Hamming weights of C, $d_1^{\perp}, ..., d_{n-k}^{\perp}$ the generalised Hamming weights of $C^{\perp}$, then*

$$[n] = \{n+1-d_1, ..., n+1-d_k\} \uplus \{d_1^{\perp}, ..., d_{n-k}^{\perp}\}.$$

where $A \uplus B$ denotes the disjoint union of A and B. In other words, the weight hierarcy of $C^{\perp}$ is the sequence which forms the complement of the sequence $n+1-d_k, ..., n+1-d_1$ in $[n]$.

A direct proof, along with some examples, can be found in [3].

Definition 4.1. *Let $r \in \mathbb{Z}_+$, q be a prime power. The simplex code $S_r(q)$ is the dual of the Hamming code $H_r(q)$. It is a $\left[\frac{q^r-1}{q-1}, r\right]$-code.*

Corollary 4.2.1.

$$d_i(S_r(q)) = q^{r-1} + q^{r-2} + ... + q^{r-i} \text{ for all } i \in [r].$$

Proof. By Corollary 3.4.1, the complement of the weight hierarchy of $H_r(q)$ in $\left[\frac{q^r-1}{q-1}\right]$ is $\left\{\frac{q^s-1}{q-1} + 1 : 0 \leq s \leq r-1\right\}$, so, by Wei's duality theorem, the generalised Hamming weights of $S_r(q)$ are those of the form

$$\begin{aligned}\frac{q^r-1}{q-1} + 1 - \frac{q^s-1}{q-1} - 1 &= 1 + q + q^2 + ... + q^{r-1} - (1 + q + q^2 - ... + q^{s-1}) \\ &= q^s + q^{s+1} + ... + q^{r-1}\end{aligned}$$

If we put these in ascending order, the i^{th} one is $q^{r-1} + ... + q^{r-i}$. □

Example. Let $C = \langle(1, 1, ..., 1)\rangle$ be the repetition code of length n over $\mathbb{F}_q$, which is an $[n, 1]$-code. Its dual is the parity check code of length n, with generator matrix

$$\begin{bmatrix} 1 & 0 & \dots & 0 & -1 \\ 0 & 1 & \dots & 0 & -1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -1 \end{bmatrix}$$

which is an $[n, n-1]$-code. C has only one generalised Hamming weight, which is its minimum distance $d_1 = n$, therefore, by the previous theorem, the weight hierarchy of $C^\perp$ is $2, 3, ..., n$.

In this chapter, we generalise Wei's result to matroids, but first we need to introduce the notion of dual matroid.

4.1 The dual of a matroid

Let $\mathcal{M} = (M, \mathcal{I})$ be a matroid, $\mathcal{B}$ its set of bases and $\mathcal{B}^* := \{\sigma \subseteq M : M \backslash \sigma \in \mathcal{B}\}$.

Theorem 4.3. *$\mathcal{B}^*$ is a set of bases for a matroid structure on M.*

We refer to [1] for a proof of this fact.

Definition 4.2. *The dual matroid of $\mathcal{M}$, denoted by $\mathcal{M}^*$ is the matroid whose ground set is M and whose set of bases is $\mathcal{B}^*$.*

We can also describe the independent sets, nullity function, rank function and circuits of $\mathcal{M}^*$.

Theorem 4.4. *Let $\mathcal{I}^*$, ρ^*, n^*, $\mathcal{C}^*$ be, respectively, the independent sets, the rank function, the nullity function and the circuits of $\mathcal{M}^*$. Let also $\sigma \subseteq M$. Then* *i)* $\sigma \in \mathcal{I}^* \iff M \backslash \sigma$ *contains a basis of* $\mathcal{M}$.

ii) $\rho^*(\sigma) = \rho(M\backslash\sigma) + |\sigma| - \rho(M)$.

iii) $n^*(\sigma) = n(M\backslash\sigma) + |\sigma| - n(M)$.

iv) $\sigma \in \mathcal{C}^* \iff M\backslash\sigma$ *is maximal among the subsets of* M *which do not contain a basis.*

Remark. $\rho^*(M) = n(M)$ and, analogously, $n^*(M) = \rho(M)$.
Also, it is clear that $\mathcal{M}^{**} = \mathcal{M}$.

A priori, it is not clear how this construction is related to the notion of dual code. The following result is of key importance to this.

Theorem 4.5. *Let* C *be an* $[n,k]$*-code over* $\mathbb{F}_q$, $C^\perp$ *its dual, then*

$$\mathcal{M}_{C^\perp} = (\mathcal{M}_C)^*.$$

In order to prove this, the following definition will be useful.

Definition 4.3. *Let* $\mathcal{M} = (M, \mathcal{I})$ *be a matroid. We say that* $\sigma \subseteq M$ *is spanning if it contains a basis of* $\mathcal{M}$.

Remark. If $\mathcal{M} = \mathcal{M}(v_1, ..., v_n)$ for some vectors $v_1, ..., v_n$ in a vector space V, then $\sigma \subseteq [n]$ is spanning if and only if $\langle v_1, ..., v_n\rangle = \langle v_i : i \in \sigma\rangle$.

Remark. Let $\mathcal{M} = (M, \mathcal{I})$ be a matroid, then $\sigma \subseteq M$ is independent in $\mathcal{M}^*$ if and only if $M\backslash\sigma$ is spanning in $\mathcal{M}$.

We need a couple of lemmas in order prove theorem 4.5.

Lemma 4.6. *Let* V *be a vector space over a field* k, $\phi_1, ..., \phi_n \in V^*$, *where* V^* *denotes the dual of* V. *If* $\psi \in V^*$, *then*

$$\psi \in \langle \phi_1, ..., \phi_n\rangle \iff \bigcap_{i=1}^{n} \ker \phi_i \subseteq \ker \psi.$$

Proof. The " $\implies$ " implication is clear since, if $\psi = \sum_i \lambda_i \phi_i$ and if $\phi_i(x) = 0$ for all i, then $\psi(x) = 0$.

We prove the opposite implication by induction on n. When $n = 1$, we have $\ker \phi_1 \subseteq \ker \psi$. If $\phi_1 = 0$ then $\psi = 0$ and we are done, otherwise there exists $x \in V$ such that $\phi_1(x) = 1$. If $y \in V$, then $\phi_1(y - \phi_1(y)x) = 0$, therefore $y - \phi_1(y)x \in \ker\phi_1 \subseteq \ker\psi$, so $\psi(y) = \phi_1(y)\psi(x)$ for all $y \in V$.

If $n > 1$, let $W = \ker \phi_n$, then

$$\bigcap_{i=1}^{n-1} \ker(\phi_i|_W) = \bigcap_{i=1}^{n-1} \ker\phi_i \cap W = \bigcap_{i=1}^{n} \ker\phi_i \cap W \subseteq \ker\psi \cap W = \ker(\psi|_W).$$

By induction, there are $\lambda_1, ..., \lambda_{n-1} \in k$ such that $\psi|_W = \sum_{i=1}^{n-1} \lambda_i \phi_i|_W$, but this means that

$$W = \ker\phi_n \subseteq \ker\left(\psi - \sum_{i=1}^{n-1} \lambda_i\phi_i\right).$$

We are back to the case "$n = 1$", which we already proved, so there exist $\lambda_n \in k$ such that $\psi - \sum_{i=1}^{n-1} \lambda_i \phi_i = \lambda_n \phi_n$. □

Lemma 4.7. *Let V be a vector space over a field k, $v_1, ..., v_n \in V$ and $C = \{x \in k^n : \sum_{i=1}^{n} x_i v_i = 0\}$. Let also $v_i^* : C \to k,\ x \mapsto x_i$ for all $i \in [n]$. Then*

$$\mathcal{M}(v_1, ..., v_n)^* = \mathcal{M}(v_1^*, ..., v_n^*).$$

Proof. Let $\sigma \subseteq [n]$. If σ is an independent set of $\mathcal{M}(v_1, ..., v_n)^*$ then, by definition, $[n]\backslash\sigma$ is a spanning set of $\mathcal{M}(v_1, ..., v_n)$, so, for all $i \in \sigma$, we have that $v_i \in \langle v_j : j \in [n]\backslash\sigma\rangle$. This implies that for all $i \in \sigma$ there is some $x \in k^n$ such that $\operatorname{supp} x \subseteq [n]\backslash\sigma$ and $x - e_i \in C$, where e_i is the vector of k^n whose entries are all zero, except for the i^{th} entry which is equal to 1. This is because there are x_j, with $j \in [n]\backslash\sigma$, such that $v_i = \sum_{j\in[n]\backslash\sigma} x_j v_j$.

Let's prove that σ is an independent set of $\mathcal{M}(v_1^*, ..., v_n^*)$. Let $\lambda_i \in k$ for all $i \in \sigma$ such that $\sum_{i\in\sigma} \lambda_i v_i^* = 0$. If $j \in \sigma$, then there is some $x \in k^n$ such that $x - e_j \in C$ and $\operatorname{supp} x \subseteq [n]\backslash\sigma$, so

$$0 = \sum_{i\in\sigma} \lambda_i v_i^*(x - e_j) = \sum_{i\in\sigma} \lambda_i (x_i - \delta_{ij}) = -\sum_{i\in\sigma} \lambda_i \delta_{ij} = -\lambda_j$$

where we have used that, since $\operatorname{supp} x \subseteq [n]\backslash\sigma$, $x_i = 0$ for all $i \in \sigma$. Since j is arbitrary, this means that the λ_j are all zero and it follows that the v_j^*, with $j \in \sigma$, are linearly independent.

Let's now assume that σ is an independent set of $\mathcal{M}(v_1^*, ..., v_n^*)$ and let's prove that σ is also an independent set of $\mathcal{M}(v_1, ..., v_n)^*$, or, equivalently, that $[n]\backslash\sigma$ is a spanning set of $\mathcal{M}(v_1, ..., v_n)$. Let $j \in \sigma$, then $v_j^* \notin \langle v_i^* : i \in \sigma\backslash\{j\}\rangle$. By lemma 4.6, we have that

$$\bigcap_{i\in\sigma\backslash\{j\}} \ker v_i^* \not\subseteq \ker v_j^*$$

so there exists $x \in C$ such that $v_i^*(x) = x_i = 0$ for all $i \in \sigma\backslash\{j\}$ and $v_j^*(x) = x_j \neq 0$. More succintly, there is $x \in C$ such that $j \in \operatorname{supp} x \subseteq [n]\backslash\sigma \cup \{j\}$. But then,

$$\sum_{i=1}^{n} x_i v_i = x_j v_j + \sum_{i\in[n]\backslash\sigma} x_i v_i = 0.$$

Dividing by x_j and isolating v_j, this implies that $v_j \in \langle v_i : i \in [n]\backslash\sigma\rangle$. Since this is true for all $j \in \sigma$, this means that $[n]\backslash\sigma$ is a spanning set of $\mathcal{M}(v_1, ..., v_n)$, which is what we wanted to prove. □

Remark. We say that a matroid is k-representable if it is isomorphic to one of the form $\mathcal{M}(v_1, ..., v_n)$, for some vectors $v_1, ..., v_n$ belonging to some vector space V over k. The previous lemma implies that the dual of a k-representable matroid is k-representable.

Proof of theorem 4.5. Let H be a parity-check matrix of C and denote its columns by $h_1, ..., h_n$. By lemma 4.7, $\mathcal{M}_C^* = \mathcal{M}(h_1, ..., h_n)^* = \mathcal{M}(h_1^*, ..., h_n^*)$, where $h_i^* : C \to \mathbb{F}_q,\ x \mapsto x_i$. By proposition 3.1, $\mathcal{M}(h_1^*, ..., h_n^*)$ is uniquely determined by $\ker f$, where $f : \mathbb{F}_q^n \to C^*,\ x \mapsto \sum_{i=1}^n x_i h_i^*$. But

$$f(x) = 0 \iff \sum_{i=1}^n x_i h_i^* = 0 \iff \sum_{i=1}^n x_i h_i^*(y) = 0 \text{ for all } y \in C$$

$$\iff \sum_{i=1}^n x_i y_i = x \cdot y = 0 \text{ for all } y \in C \iff x \in C^\perp$$

Therefore $\ker f = C^\perp$ and $\mathcal{M}_C^* = \mathcal{M}(h_1^*, ..., h_n^*) = \mathcal{M}_{C^\perp}$. □

4.2 Wei duality for matroids

Wei's duality theorem has a strightforward generalisation to matroids.

Theorem 4.8 (Wei duality for matroids). *Let $\mathcal{M}$ be a matroid with nullity k and cardinality n, $d_1, ..., d_k$ its generalised Hamming weights and $d_1^*, ..., d_{n-k}^*$ the generalised Hamming weights of its dual. Then*

$$[n] = \{d_1, ..., d_k\} \uplus \{n + 1 - d_1^*, ..., n + 1 - d_{n-k}^*\}.$$

Proof. Let $S = \{d_1, ..., d_k\}$, $T = \{n + 1 - d_1^*, ..., n + 1 - d_{n-k}^*\}$. Since $|S| = k$ and $|T| = n - k$, we just need to prove that S and T are disjoint. Assume, by contradiction, that they aren't disjoint, then there exist indices i, j such that $d_i = n + 1 - d_j^*$. Let $\sigma \subseteq M$ such that $|\sigma| = d_i$ and $n(\sigma) \geq i$. If $\tau = M \backslash \sigma$, we have that $|\tau| = n - |\sigma| = n - d_i = d_j^* - 1 < d_j^*$, so $n^*(\tau) \leq j - 1$ because otherwise we would have a set with nullity at least j, but with cardinality less than $d_j(\mathcal{M}^*)$.

By theorem 4.4,

$$j - 1 \geq n^*(\tau) = n(M \backslash \tau) + |\tau| - n(M)$$

$$= n(\sigma) + |M| - |\sigma| - n(M) \geq i + n - d_i - k.$$

Since the double dual of a matroid is the matroid itself, the roles of i and j in what we said before can be interchanged and we also get

$$i - 1 \geq j + n - d_j^* - n^*(M) = j + n - d_j^* - \rho(M)$$

$$= j + n - d_j^* - n + k = j - d_j^* + k.$$

Putting all this together, we get

$$j - 1 \geq i + n - d_i - k \geq j - d_j^* + k + 1 + n - d_i - k$$

$$= j - (d_i + d_j^*) + n + 1 = j - (n + 1) + n + 1 = j.$$

which is a contradiction. □

Example. The weight hierarchy of $U_{r,n}$ is $r+1, r+2, ..., n$. If we apply Wei duality for matroids to calculate the weight hierarchy of $U_{r,n}^*$, we get $n-r+1, n-r+2, ..., n$. This is no surprise: a subset σ of $[n]$ is a spanning subset for $U_{r,n}$ if and only if $|\sigma| \geq r$, so $|\sigma|$ is independent for $U_{r,n}^*$ if and only if $|[n] \backslash \sigma| \geq r$, but this is true if and only if $|\sigma| \leq n-r$, so $U_{r,n}^* = U_{n-r,n}$.

Chapter 5

Hamming weights and Betti numbers

Our next goal is to describe the generalised Hamming weights of a matroid through its $\mathbb{Z}$-graded Betti numbers. In order to do so, we first have to reinterpret the nullity of a subset of a matroid as a way to count the non-redundant circuits contained in it. Most of the following results come from [5].

5.1 Non-redundancy of circuits

Throughout this section, let $\mathcal{M} = (M, \mathcal{I})$ be a matroid and $\mathcal{C}$ its set of circuits.

Definition 5.1. *Let X be a set and $\Sigma \subseteq 2^X$. We say that Σ is non-redundant, if for all $\tau \in \Sigma$*

$$\bigcup_{\sigma \in \Sigma \setminus \{\tau\}} \sigma \subsetneq \bigcup_{\sigma \in \Sigma} \sigma.$$

In other words, Σ is non-redundant if, when taking the union of its elements, we can't exclude any of them if we don't want to get a smaller set.

Notice that Σ is non-redundant if and only if for each $\sigma \in \Sigma$ we can always find $x \in \sigma$ such that $x \notin \tau$ for all $\tau \in \Sigma \setminus \{\sigma\}$.

We are particularly interested in sets of non-redundant circuits in a matroid.

Remark. If $\sigma \subseteq M$ then $C \subseteq \sigma$ is a circuit of $\mathcal{M}$ if and only if it is a circuit of $\mathcal{M}|_\sigma$. In other words, the circuits of $\mathcal{M}|_\sigma$ are precisely the circuits of $\mathcal{M}$ contained in σ.

Definition 5.2. *The degree of non-redundancy of $\mathcal{M}$ is*

$$\deg(\mathcal{M}) = \max\{|\Sigma| : \Sigma \subseteq \mathcal{C} \textit{ and } \Sigma \textit{ is non-redundant}\}.$$

In other words, it is the maximal number of non-redundant circuits contained in M. If $\sigma \subseteq M$, we denote $\deg(\mathcal{M}|_\sigma)$ by $\deg(\sigma)$, which, by the previous remark, is also the maximal number of non-redundant circuits of $\mathcal{M}$ contained in σ.

We shall prove, after a couple of lemmas, that $\deg(\sigma) = n(\sigma)$ for all $\sigma \subseteq M$.

Lemma 5.1. *Let $\Sigma \subseteq \mathcal{C}$ be non-redundant, $\tau = \bigcup_{\sigma \in \Sigma} \sigma$. Then $n(\tau) \geq |\Sigma|$.*

Proof. Let's prove this by induction on $s = |\Sigma|$. If $s = 1$, the τ is itself a circuit. If we remove any element from τ we get, by definition, an independent set, and τ itself is dependent, so $\rho(\tau) = |\tau| - 1$ and therefore $n(\tau) = 1$.

Now, let $s > 1$, and assume that the claim is true for $s - 1$. Let $\sigma_0 \in \Sigma$, $\Sigma_0 = \Sigma \backslash \{\sigma_0\}$ and $\tau_0 = \bigcup_{\sigma \in \Sigma_0} \sigma$. Then, by induction and *N3)*,

$$n(\tau) = n(\tau_0 \cup \sigma_0) \geq n(\tau_0) + n(\sigma_0) - n(\tau_0 \cap \sigma_0) \geq s - n(\tau_0 \cap \sigma_0)$$

Let $x \in \sigma_0$ such that $x \notin \sigma$ for all $\sigma \in \Sigma_0$, which exists because Σ is non-redundant. In other words, $x \in \sigma_0 \backslash \tau_0$, but then $\tau_0 \cap \sigma_0 \subseteq \sigma_0 \backslash \{x\}$, which, since σ_0 is a circuit, implies that $\tau_0 \cap \sigma_0$ is independent and therefore that $n(\sigma_0 \cap \tau_0) = 0$.

□

Corollary 5.1.1. $\deg(\mathcal{M}) \leq n(\mathcal{M})$.

Proof. Let Σ be a set of non-redundant circuits of $\mathcal{M}$ with maximal cardinality, so that $|\Sigma| = \deg(\mathcal{M})$. Then, by *N1)* and the previous lemma,

$$n(\mathcal{M}) \geq n\left(\bigcup_{\sigma \in \Sigma} \sigma\right) \geq |\Sigma| = \deg(\mathcal{M})$$

□

The following proposition is a strengthening of the third defining axiom for the circuits of a matroid.

Proposition 5.2. *Let σ, τ be distinct circuits, $x \in \sigma \cap \tau$, $y \in \sigma \backslash \tau$. Then there exists a circuit ρ such that*

$$y \in \rho \subseteq (\sigma \cup \tau) \backslash \{x\}.$$

Proof. Let's prove this by induction on $n = |\sigma \cup \tau|$.

The starting point of the induction has to be $n = 3$, as if $n \leq 2$ then, by *C2)*, it is not hard to see that σ and τ would have to be disjoint.

When $n = 3$, by *C2)* and the other hypotheses, we must have $\sigma = \{a, b\}$, $\tau = \{a, c\}$, therefore $x = a$, $y = b$. If $\rho \subseteq (\sigma \cup \tau) \backslash \{x\} = \{b, c\}$ is a circuit, we can't have $\rho = \{b\}$ or $\rho = \{c\}$ because of *C2)*, so the only possibility is $\rho = \{a, b\}$, which contains $y = b$.

Assume now that $n > 3$ and that the claim is true for $m < n$. Let ρ be a circuit such that $\rho \subseteq (\sigma \cup \tau) \backslash \{x\}$. If $y \in \rho$ we are done, so let's assume $y \notin \rho$.

By *C2)*, since $\rho \neq \sigma$, there exists $z \in \rho \backslash \sigma \subseteq \tau$. So $z \in \rho \cap \tau$ and $x \in \tau \backslash \rho$. Also, note that $y \notin \rho \cup \tau$, so $|\rho \cup \tau| < |\sigma \cup \tau| = n$, but then, by induction, there exists a circuit η such that $x \in \eta \subseteq (\rho \cup \tau) \backslash \{z\}$.

Now, we have that $y \notin \eta$, since $y \notin \tau$ and $y \notin \rho$, so $y \in \sigma \backslash \eta$. We also have that $x \in \eta \cap \sigma$ and that $|\sigma \cup \eta| < n$, since $z \notin \eta$ and $z \notin \sigma$. Therefore, by induction, there exists a circuit ζ such that $y \in \zeta \subseteq (\sigma \cup \eta) \backslash \{x\}$

But $\eta \subseteq \rho \cup \tau \subseteq \sigma \cup \tau$, so the proof is complete.

□

Lemma 5.3. *Let Σ be a maximal set of non-redundant circuits. Then*

$$\bigcup_{\sigma \in \Sigma} \sigma = \bigcup_{\sigma \in \mathcal{C}} \sigma.$$

Proof. Let $\tau = \bigcup_{\sigma \in \Sigma} \sigma$ and assume by contradiction that there is a circuit ρ such that $\rho \nsubseteq \tau$, so there exists $x \in \rho \backslash \tau$.

For each $\sigma \in \Sigma$, let $x_\sigma \in \sigma$ such that $x_\sigma \notin \sigma'$ for all $\sigma' \in \Sigma \backslash \{\sigma\}$.

The set of circuits that contain x is non-empty by hypothesis. If γ is a circuit that contains x and x_σ for some $\sigma \in \Sigma$, then $\gamma \neq \sigma$, $x \in \gamma \backslash \sigma$ and $x_\sigma \in \sigma \cap \gamma$, therefore, by the previous proposition, there exists a circuit γ' such that $x \in \gamma' \subseteq (\gamma \cup \sigma) \backslash \{x_\sigma\}$.

In other words, if we have a circuit that contains x and some x_σ, we can alway find a circuit that contains x and that does not contain x_σ. Therefore, by applying this enough times to ρ, we can find a circuit σ_0 such that $x \in \sigma_0$ and $x_\sigma \notin \sigma_0$ for all $\sigma \in \Sigma$, but this means that $\Sigma \cup \{\sigma_0\}$ is non-redundant, which contradicts its maximality. □

Theorem 5.4. $n(\sigma) = \deg(\sigma)$ *for all $\sigma \subseteq M$.*

Proof. Let $\sigma \subseteq M$. It remains to prove that $\deg(\sigma) \geq n(\sigma)$. It is enough to prove that there exist $n(\sigma)$ non-redundant circuits contained in σ.

If $n(\sigma) = 0$ then σ is independent and it doesn't contain any circuit. If $n(\sigma) = 1$, then $\sigma = \tau \cup \{x\}$ with τ independent and $x \notin \tau$, but then σ can contain at most one circuit, since if there were two distinct circuits γ, γ' contained in σ, both would have to contain x but then, by *C2)*, $\gamma \cup \gamma' \backslash \{x\} \subseteq \tau$ would have to be dependent. Therefore the lemma is true if $n(\sigma) = 0$ or $n(\sigma) = 1$.

Assume by contradiction that the theorem doesn't hold for all $\sigma \subseteq M$, and let $\sigma \subseteq M$ be minimal for inclusion such that the theorem doesn't hold for σ. By the previous remarks, $n(\sigma) \geq 2$, so σ is dependent and we can find a circuit $\tau \subseteq \sigma$. Let $x \in \tau$, $\sigma' = \sigma \backslash \{x\}$. Since σ is minimal, the lemma holds for σ', so there exist $n(\sigma')$ non-redundant circuits contained in σ'.

Now, $n(\sigma')$ is the smallest number of elements we have to remove from σ' in order to get an independent subset, and likewise for σ, so, since σ' is obtained from σ by removing an element, we have that $n(\sigma) \leq n(\sigma') + 1$, or, equivalently, that $n(\sigma') \geq n(\sigma) - 1$.

Therefore we can find at least $n(\sigma) - 1$ non-redundant circuits in σ', and therefore in σ. Denote them by $\tau_1, ..., \tau_{n(\sigma)-1}$. Moreover,

$$x \in \tau \backslash \bigcup_{i=1}^{n(\sigma)-1} \tau_i,$$

so the τ_i don't cover all of the circuits of σ, but then lemma 5.3 implies that there is a circuit $\tau_{n(\sigma)}$ contained in σ such that $\tau_1, ..., \tau_{n(\sigma)}$ are non-redundant, which is a contradiction.

□

5.2 Generalised Hamming weights and Betti numbers

In this section, we use the previous results to prove that the $\mathbb{Z}$-graded betti numbers of a matroid completely determine its weight hierarchy. In order to do that, we need Hochster's theorem along with the following result, which describes the homology of matroids. For a proof, see [4].

Theorem 5.5. *Let $\mathcal{M}$ be a matroid and k be a field, then*

$$\tilde{h}_i(\mathcal{M}, k) = \begin{cases} 0 & i \neq \rho(\mathcal{M}) - 1 \\ (-1)^{\rho(\mathcal{M})-1}\chi(\mathcal{M}) & i = \rho(\mathcal{M}) - 1 \end{cases}$$

where $\chi(\mathcal{M})$ is the Euler characteristic of $\mathcal{M}$, which can be defined in general for a simplicial complex $\mathcal{K}$ as

$$\chi(\mathcal{K}) = \sum_{i \geq 0} (-1)^{i-1} f_i(\mathcal{K})$$

where $f_i(\mathcal{K})$ denotes the number of faces of $\mathcal{K}$ that have cardinality i.

An immediate consequence of this theorem is that $\tilde{h}_i(\mathcal{M}, k)$ does not depend on the field k. By relating these numbers with the Betti numbers of $\mathcal{M}$, through Hochster's theorem, we shall soon see that they also do not depend on the choice of k.

Remark. In the literature, the f_i are frequently defined for $i \geq 0$ as the number of *i-dimensional* faces, that is, the number of faces of cardinality $i+1$ and the Euler characteristic is defined as $\sum_{i\geq 0}(-1)^i f_i$. This is 1 more than the Euler characteristic as we defined it because we also count the empty set, which is the only face of cardinality 0.

Definition 5.3. *Let $\mathcal{M} = (M, \mathcal{I})$ be a matroid, $e \in M$. We say that*

i) e is a loop if is not contained in any basis of $\mathcal{M}$.

ii) e is an isthmus if it is contained in every basis of $\mathcal{M}$.

Remark. e is an isthmus of $\mathcal{M}$ if and only if it is a loop of $\mathcal{M}^*$.

Proposition 5.6. *Let $\mathcal{M}$ be a matroid. Then $\chi(\mathcal{M}) = 0$ if and only if $\mathcal{M}$ has an isthmus.*

We omit the proof since it's a bit long and outside of our scope, but the fact that, if $\mathcal{M}$ has an ishmus, then $\chi(M) = 0$ is true in general for simplicial complexes: if a simplicial complex has a vertex which is contained in every facet, then its Euler characteristic is zero.

One can expect this, since, if one looks at the complex geometrically, it follows that one can contract every facet to the common vertex and so the complex is "contractible", so we should expect its Euler characteristic, as we defined it, to be zero (one less than the standard definition). The reverse implication is not true for simplicial complexes in general, but it turns out to be true for matroids.

Lemma 5.7. *Let $\mathcal{M} = (M, \mathcal{I})$ be a matroid, $e \in M$, then*

$$e \text{ is an isthmus} \iff e \text{ is not contained in any circuit.}$$

Proof. First, assume that e is an isthmus and suppose, by contradiction, that it was contained in a circuit σ, then $\sigma\backslash\{e\}$ would be independent and therefore contained in some basis τ, which would also contain e, but then $\sigma \subseteq \tau$ which is a contradiction since σ is dependent and τ is independent.

Now assume that e is not contained in any circuit and let τ be a basis. If τ did not contain e, $\tau \cup \{e\}$ would be dependent and would therefore contain a circuit σ, which would necessarily have to contain e, but this isn't possible since e is contained in no circuit. □

Now, let $\mathcal{M} = (M, \mathcal{I})$ be a matroid, $N_i = \{\sigma \subseteq M : n(\sigma) = i\}$.

Theorem 5.8. *Let k be a field, $\sigma \subseteq M$, then*

$$\beta_{i,\sigma}(\mathcal{M}, k) = \begin{cases} 0 & i \neq n(\sigma) \\ (-1)^{\rho(\sigma)-1}\chi(\mathcal{M}|_\sigma) & i = n(\sigma) \end{cases}$$

Moreover,

$$\beta_{i,\sigma}(\mathcal{M}, k) \neq 0 \iff n(\sigma) = i \text{ and } \sigma \text{ is minimal in } N_i.$$

Proof. Let us denote $\beta_{i,\sigma}(\mathcal{M}, k)$ simply by $\beta_{i,\sigma}$ for brevity.

From Hochster's theorem and theorem 5.5, we have that

$$\beta_{i,\sigma} = \tilde{h}_{|\sigma|-i-1}(\mathcal{M}|_\sigma, k) = \begin{cases} 0 & |\sigma| - i - 1 \neq \rho(\sigma) - 1 \\ (-1)^{\rho(\sigma)-1}\chi(\mathcal{M}|_\sigma) & |\sigma| - i - 1 = \rho(\sigma) - 1 \end{cases}$$

and the first part is proved, since $|\sigma| - i - 1 = \rho(\sigma) - 1 \iff i = n(\sigma)$.

As a consequence, we have that

$$\beta_{i,\sigma} \neq 0 \iff n(\sigma) = i \text{ and } \chi(\mathcal{M}|_\sigma) \neq 0$$

From proposition 5.6 and lemma 5.7, it follows that a matroid has zero Euler characteristic if and only if it is not the union of its circuits, therefore $\beta_{i,\sigma} \neq 0$ if and only if $n(\sigma) = i$ and σ is the union of the circuits contained in it. It thus remains to prove that this is true if and only if σ is minimal in N_i.

Assume that $n(\sigma) = i$ and that σ is the union of the circuits contained in it, let $\tau \in N_i$ such that $\tau \subseteq \sigma$. From theorem 5.4, we can find i non-redundant circuits $\tau_1, ..., \tau_i$ in τ, and therefore in σ as well, but, since $n(\sigma) = \deg(\sigma) = i$, it follows that $\tau_1, ..., \tau_i$ form a maximal set of non-redundant circuits in σ. From lemma 5.3,

$$\sigma = \bigcup_{\gamma \in \mathcal{C}_\sigma} \gamma = \bigcup_{j=1}^{i} \tau_i \subseteq \tau$$

where $\mathcal{C}_\sigma$ denotes the set of circuits contained in σ.

Now assume that σ is minimal in N_i, let $\tau_1, ..., \tau_i$ be a maximal set of non-redundant circuits contained in σ and let $\tau = \bigcup_{j=1}^{i} \tau_j$. By lemma 5.3, τ is the union of all circuits contained in σ and by theorem 5.4 we also have that $\tau \in N_i$, but $\tau \subseteq \sigma$ and σ is minimal in N_i, so $\sigma = \tau$ and the proof is complete. □

Corollary 5.8.1. *The multigraded, $\mathbb{Z}$-graded and global Betti numbers of a matroid do not depend on the field over which they are calculated.*

In light of this, we will denote the multigraded, $\mathbb{Z}$-graded and global Betti numbers of a matroid $\mathcal{M}$ by $\beta_{i,\sigma}(\mathcal{M})$, $\beta_{i,j}(\mathcal{M})$ and $\beta_i(\mathcal{M})$ respectively.

We are now able to express the generalised Hamming weights of a matroid in terms of its $\mathbb{Z}$-graded Betti numbers. This result was proved by Johnsen and Verdure in [5].

Theorem 5.9 (Johnsen-Verdure). *Let $\mathcal{M} = (M, \mathcal{I})$ be a matroid, $i \in [n(M)]$, then*

$$d_i(\mathcal{M}) = \min\{d \in \mathbb{N} : \beta_{i,d}(\mathcal{M}) \neq 0\}.$$

Proof. Let m denote the quantity on the right hand side of the equation. Let $\sigma \in N_i$ such that $|\sigma| = d_i(\mathcal{M})$, then σ is minimal and $\beta_{i,\sigma}(\mathcal{M}) \neq 0$ by the previous theorem, but then $\beta_{i,|\sigma|}(\mathcal{M}) = \sum_{|\tau|=|\sigma|} \beta_{i,\tau}(\mathcal{M}) > 0$, therefore $|\sigma| = d_i(\mathcal{M}) \geq m$.

We have that $\beta_{i,m}(\mathcal{M}) = \sum_{|\sigma|=m} \beta_{i,\sigma}(\mathcal{M}) \neq 0$, so there exists $\sigma \subseteq M$ such that $|\sigma| = m$ and $\beta_{i,\sigma}(\mathcal{M}) \neq 0$, but then, by the previous theorem, σ is minimal in N_i, in particular $d_i(\mathcal{M}) \leq |\sigma| = m$. □

Remark. In order to calculate the Betti numbers of a simplicial complex, one needs to know the minimal generators of its Stanley-Reisner ideal, which correspond to its minimal non-faces. In the case of a matroid, this amounts to knowing its circuits. If the matroid is associated to a linear code C, its circuits are the minimal supports of the non-zero codewords in C.

Example. Let C be the binary code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Its set of codewords with minimal support is

$$S = \{100001, 011010, 000111, 111100, 011101\},$$

therefore, its Stanley-Reisner ideal is

$$I = (x_1x_6, x_1x_2x_5, x_4x_5x_6, x_1x_2x_3x_4, x_2x_3x_4x_6).$$

If one computes a minimal resolution of R/I, where $R = k[x_1, x_2, x_3, x_4, x_5, x_6]$, one gets 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 indexed by the i^{th} row and the j^{th} column corresponds to $\beta_{j,i+j}$, as it is customary to do since it is well known that the Betti numbers $\beta_{i,j}$ with $j < i$ are zero. Therefore, by theorem 5.9, we have $d_1(C) = 2$, $d_2(C) = 4$ and $d_3(C) = 6$.

While very interesting from a theoretical perspecrive, there are two main practical issues with this approach:

1. In order to use theorem 5.9, one needs to know all the minimal supports of the non-zero elements of C, which, for long codes, can be quite big.

2. One also needs to calculate the free resolution of a monomial ideal with a big number of generators, which is quite expensive from a computational perspective.

In the next chapter we introduce a technique, based on Gröbner bases, which allows us to get some informations on the Hamming weights of a binary codes without having to find all the minimal supports.

Chapter 6

Test sets for binary codes

In this chapter, we introduce the notion of test set, which will allow us to bound the Hamming weights of a binary code by calculating the Betti numbers of a monomial ideal which is smaller than the Stanley-Reisner ideal, and thus more computationally manageable. We will also discuss when this bound is attained, along with some open problems. From now on, we restrict our attention on binary codes, though some of the results and definitions that we discuss have been generalised to q-ary codes, for example see [6].

6.1 The ideal associated to a binary code

From now on, let k be a field. We begin by introducing some notation.

Definition 6.1. *Let $n \in \mathbb{Z}_+$, $I \subseteq [n]$ and $a \in \mathbb{F}_2^n$. If $X_1, ..., X_n$ are the variables of the polynomial ring $k[X_1, ..., X_n]$, we define*

- $X^I = \prod_{i \in I} X_i$.
- $X^a = \prod_{i=1}^n X_i^{a_i}$*, where, with abuse of notation, we identify the classes of* 0 *and* 1 *in* $\mathbb{F}_2$ *with the non negative integers* 0 *and* 1.

Remark. If $a \in \mathbb{F}_2^n$, then $X^a = X^{\operatorname{supp} a}$, in particular, $X^0 = 1$. Also notice that, for a and b in $\mathbb{F}_2^n$, $\operatorname{supp}(a+b) = \operatorname{supp} a \triangle \operatorname{supp} b$, where the triangle denotes the symmetric difference: for two sets A and B, their symmetric difference is $A \triangle B = (A \cup B) \setminus (A \cap B)$.

Moreover, notice that, if I and J are disjoint, then $X^{I \cup J} = X^I X^J$.

Definition 6.2. *Let C be a binary code of length n. The ideal associated to C over k is*

$$I(C) = \left(X^a - X^b : a, b \in \mathbb{F}_2^n,\ a + b \in C\right) + \left(X_i^2 - 1 : i \in [n]\right).$$

Remark. In a sense, the ideal $I(C)$ captures the relationships between the elements of the group $\mathbb{F}_2^n / C$ in a polynomial setting: the binomials $X_i^2 - 1$ are there because every element should have order 2, and the binomials $X^a - X^b$ are there because, if $a+b = a-b \in C$, then a and b represent the same elements in the quotient.

Notice that, if $J = (X_i^2 - 1 : i \in [n])$ and $a, b \in \mathbb{F}_2^n$, then $X^{a+b} \equiv X^a X^b$ mod J.

The next proposition shows how to present $I(C)$ with a smaller set of generators.

Proposition 6.1. *Let C be an $[n,k]$-code and $w_1, ..., w_k$ the rows of a generator matrix of C, then*

$$I(C) = (X^{w_i} - 1 : i \in [k]) + (X_i^2 - 1 : i \in [n]).$$

Proof. Let K be the ideal on the right hand side and let $J = (X_i^2 - 1 : i \in [n])$ as before. It is clear that $K \subseteq I(C)$, so it only remains to prove the reverse inclusion. Let $a, b \in \mathbb{F}_2^n$ such that $a + b \in C$ and let's prove that $X^a - X^b \in K$. Since both ideals contain J, we can perform all our calculations modulo J. We have that

$$X^a - X^b \equiv X^a (X^b)^2 - X^b \equiv (X^{a+b} - 1)X^b \mod J,$$

so it suffices to prove that $X^{a+b} - 1 \in K$, but $a + b \in C = \langle w_1, ..., w_k \rangle$, so $a + b = \sum_{i \in S} w_i$ for some subset $S \subseteq [n]$ (that's because linear combinations over $\mathbb{F}_2$ are just sums). But then

$$X^{a+b} - 1 \equiv X^{\sum_{i\in S} w_i} - 1 \equiv \prod_{i \in S} X^{w_i} - 1 \mod J.$$

Let $S = \{i_1, ..., i_l\}$ and $m_j = X^{w_{i_j}}$, then

$$\prod_{i \in S} X^{w_i} - 1 = m_1 ... m_l - 1$$

$$= m_1 ... m_l - m_1 ... m_{l-1} + m_1 ... m_{l-1} - ... + m_1 m_2 - m_1 + m_1 - 1$$

$$= m_1 ... m_{l-1}(m_l - 1) + m_1 ... m_{l-2}(m_{l-1} - 1) + ... + m_1 - 1 \in J,$$

because $m_j - 1 = X^{w_{i_j}} - 1 \in J$ for all j. □

6.2 A quick review of Gröbner bases

For this section, let $S = k[X_1, ..., X_n]$ be fixed. We give a quick summary of term orders, multivariate polynomial division and Gröbner bases.

Definition 6.3. *A term order on S is an order relation $\leq$ on the set of monomials of S which satisfies the following properties*

i) $\leq$ is total, that is, given two monomials m_1 and m_2, then $m_1 \leq m_2$ or $m_2 \leq m_1$.

ii) *If m_1, m_2 and m_3 are monomials and $m_1 \leq m_2$, then $m_1 m_3 \leq m_2 m_3$.*

iii) *If m_1, m_2 are monomials and $m_1 | m_2$, then $m_1 \leq m_2$.*

We say that $\leq$ is degree-compatible if $m_1 \leq m_2 \implies \deg m_1 \leq \deg m_2$.

A term order $\leq$ also satisfies the following properties which, given *i)* and *ii)*, are both equivalent to *iii)*:

iv) $\leq$ is a well order, that is, every nonempty subset of monomials has a minimum with respect to $\leq$.

v) $1 < X_i$ for all $i \in [n]$.

Remark. If $\leq$ is a degree-compatible term order and $\deg m_1 < \deg m_2$, then $m_1 < m_2$ since, if this wasn't the case, we would have $m_2 \leq m_1$ which implies $\deg m_2 \leq \deg m_1$.

Example. The most intuitive term order on S is probably the lexicographic order, abbreviated as LEX:

$X^\alpha \leq_{LEX} X^\beta$ if and only if they are equal or, if i is the smallest index such that $\alpha_i \neq \beta_i$, then $\alpha_i < \beta_i$, for example $X_1X_2X_3^2 <_{LEX} X_1X_2^2 <_{LEX} X_1^2$. One can think of LEX as the way words are ordered in the dictionary. LEX is not degree-compatible, as the example we just made shows.

We also have the degree-lexicographic order, abbreviated DEGLEX, where $X^\alpha \leq_{DLEX} X^\beta$ if and only if $\deg X^\alpha < \deg X^\beta$ or $\deg X^\alpha = \deg X^\beta$ and $X^\alpha \leq_{LEX} X^\beta$. DEGLEX is clearly degree-compatible.

A useful non-example is the reverse-lexicographic order (REVLEX):
$X^\alpha \leq_{RLEX} X^\beta$ if and only if $\alpha_n > \beta_n$ or $\alpha_n = \beta_n$ and $\alpha_{n-1} > \beta_{n-1}$ or $\alpha_n = \beta_n$, $\alpha_{n-1} = \beta_{n-1}$ and $\alpha_{n-2} > \beta_{n-2}$ and so on. Basically, the "bigger" monomials are the ones that have "less" indeterminates with big indices, for example $X_1X_3 <_{RLEX} X_2^2$. This order relation satisfies *i)* and *ii)*, but not *iii)* as, for example, $X_1 <_{RLEX} 1$.

Finally, we have the degree-reverse-lexicographic order (DEGREVLEX): $X^\alpha \leq_{DRL} X^\beta$ if and only if $\deg X^\alpha < \deg X^\beta$ or $\deg X^\alpha = \deg X^\beta$ and $X^\alpha \leq_{RLEX} X^\beta$. This is a term-order and, although a bit counterintuitive, it turns out to be more efficient than LEX and DEGLEX.

Definition 6.4. *Let $f \in S\backslash\{0\}$, $\leq$ a term order on S, $I \subseteq S$ an ideal.*

i) *The support of f is the set of monomials of S which appear in f with a non-zero coefficient.*

ii) *The leading term of f is the biggest monomial, with respect to $\leq$, in the support of f. It is denoted by $\mathrm{LT}_\leq(f)$.*

iii) *The leading coefficient of f, dentoed by $\mathrm{LC}_\leq(f)$ is the coefficient of $\mathrm{LT}_\leq(f)$ in f.*

iv) *The initial ideal of I is the monomial ideal, denoted by $\mathrm{LT}_\leq(I)$, which is generated by the leading terms of the elements of I.*

If $I = (f_1, ..., f_c)$ is an ideal of S, one might hope that $\mathrm{LT}_{\leq}(I) = (\mathrm{LT}_{\leq}(f_1), ..., \mathrm{LT}_{\leq}(f_c))$. This is not always the case, for example, let $I = (X+Y, X+2Y) \subseteq \mathbb{Q}[X,Y]$ and let $\leq$ be any term order such that $X > Y$, then $\mathrm{LT}_{\leq}(X+Y) = \mathrm{LT}_{\leq}(X+2Y) = X$, so $(\mathrm{LT}_{\leq}(X+Y), \mathrm{LT}_{\leq}(X+2Y)) = (X)$, but actually $I = (X,Y)$, so $\mathrm{LT}_{\leq}(I) = (X,Y)$.

Definition 6.5. *Let I be an ideal of S, $\leq$ a term order on S. A Gröbner basis of I, with respect to $\leq$, is a subset $\mathcal{G} \subseteq I \backslash \{0\}$ such that $\mathrm{LT}_{\leq}(I) = (\mathrm{LT}_{\leq}(g) : g \in \mathcal{G})$. We say that $\mathcal{G}$ is reduced if*

i) $\mathrm{LC}_{\leq}(g) = 1$ *for all $g \in \mathcal{G}$.*

ii) $\mathrm{LT}_{\leq}(g) \not| \mathrm{LT}_{\leq}(h)$ *for all $g, h \in \mathcal{G}$ such that $g \neq h$.*

iii) For all $g \in \mathcal{G}$, $\mathrm{LT}_{\leq}(g)$ is the only monomial in $\mathrm{LT}_{\leq}(I)$ which is also in the support of g.

Given a term order on S, every ideal I of S has a finite Gröbner basis. Moreover, it has a unique reduced Gröbner basis (which is finite as well). It can be found algorithmically, starting from a finite set of generators of I, through a process called Buchberger's algorithm, which is based on a generalisation of polynomial division to multivariate polynomials.

Remark. A reduced Gröbner basis of an ideal I can always be obtained form a Gröbner basis $\mathcal{G}'$ in the following way: take $h_1, ..., h_c \in \mathcal{G}'$ such that their leading terms form a minimal set of generators for $\mathrm{LT}_{\leq}(I)$, and make them monic by dividing them by their leading coefficient. For each i, if there is some monomial m in the support of h_i, other than the leading term, which is also in $\mathrm{LT}_{\leq}(I)$, then $\mathrm{LT}_{\leq}(h_j)|m$, so we can subtract some multiple of h_j from h_i in order to remove m from the support of h_i. This only alters the monomials in the support of h_i smaller than m, so we can repeat this process over and over until $\operatorname{supp} h_i \cap \mathrm{LT}_{\leq}(I) = \{\mathrm{LT}_{\leq}(h_i)\}$.

In particular, we have that $f \in I$ is in the reduced Gröbner basis of I if and only if it is monic, $\mathrm{LT}_{\leq}(f)$ is a minimal generator of $\mathrm{LT}_{\leq}(I)$ and all the other monomials appearing f are not in $\mathrm{LT}_{\leq}(I)$.

Definition 6.6. *Let $f, g_1, ..., g_c \in S$, $\leq$ a term order on S. A multivariate polynomial division of f by $g_1, ..., g_c$, with respect to $\leq$, is an expression of the form*

$$f = \sum_{i=1}^{c} q_i g_i + r$$

such that

i) For all i, either $q_i = 0$ or $q_i \neq 0$ and $\mathrm{LT}_{\leq}(q_i g_i) \leq \mathrm{LT}_{\leq}(f)$.

ii) Either $r = 0$ or $r \neq 0$ and $\mathrm{LT}_{\leq}(r)$ is not divisible by $\mathrm{LT}_{\leq}(g_i)$ for any i.

We call r the remainder of the division.

Multivariate polynomial division can always be carried out algorithmically, like ordinary polynomial division: we divide the leading term of f by the leading term of g_1, then we multiply the result by g_1 and we subtract it from f, we them continue until the leading term of f is not divisible by the leading term of g_1. Then we do the same thing with g_2, g_3 and so on. The result, however, is usually not unique, as we would expect since polynomial rings in more than one variable are not principal ideal domains.

We now briefly describe Buchberger's algorithm, for a fixed term order $\leq$ on $S = k[X_1, ..., X_n]$.

Definition 6.7. *Given $g_1, ..., g_c \in S \backslash \{0\}$, the S-polynomials associated to $g_1, ..., g_c$ are*

$$S_{ij}(\mathfrak{g}) = \frac{m_j}{m_{ij}} g_i - \frac{m_i}{m_{ij}} g_j;$$

where $m_i = \mathrm{LT}_{\leq}(g_i)$, $m_{ij} = \gcd(m_i, m_j)$ and $\mathfrak{g}$ denotes the list $g_1, ..., g_c$.

Theorem 6.2 (Buchberger's criterion)**.** *Let $g_1, ..., g_c \in S$, $I = (g_1, ..., g_c)$. The following are equivalent:*

i) $g_1, ..., g_c$ is a Gröbner basis for I.

ii) For all $i < j$, every multivariate polynomial division of $S_{ij}(\mathfrak{g})$ by $g_1, ..., g_c$ gives a zero remainder.

iii) For all $i < j$ there exist a multivariate polynomial division of $S_{ij}(\mathfrak{g})$ by $g_1, ..., g_c$ with zero remainder.

We now describe Buchberger's algorithm applied to an ideal I of S generated by the list of polynomials $\mathfrak{g} = g_1, ..., g_c$:

1. Divide all the S-polynomials associated to $\mathfrak{g}$ by $g_1, ..., g_c$.

2. If all the remainders are zero, then $g_1, ..., g_c$ is a Gröbner basis of I and we are done. Otherwise, as soon a non zero remainder r is found, add it to the list $\mathfrak{g}$ and repeat step 1.

The algorithm has to eventually stop, since, whenever we find a non zero remainder, we increase the ideal $(\mathrm{LT}_{\leq}(g) : g \in \mathfrak{g})$, but S is noetherian.

The utility of Gröbner bases is that, through multivariate polynomial division, they give ways to algorithmically solve a lot of commutative algebra problems in the setting of polynomial rings. For example, given an ideal I generated by polynomials $g_1, ..., g_c$ and $f \in S$, we can test whether or not $f \in I$: use Buchberger algorithm to find a Gröbner basis $h_1, ...h_d$ of I and perform a multivariate polynomial division of f by $h_1, ..., h_d$, then $f \in I$ if and only if the remainder is zero.

6.3 The reduced Gröbner basis of the ideal associated to a code

We now turn our attention back to binary codes. For the remainder of this chapter, fix a binary $[n,k]$-code C and a degree-compatible term order $\leq$ on $S = k[X_1, ..., X_n]$. Denote by $\mathcal{G}_{\leq}(C)$ the unique reduced Gröbner basis of $I(C)$ with respect to $\leq$.

Remark. Let $a, b \in \mathbb{F}_2^n$. Then $X^a - X^b \in I(C) \iff a + b \in C$. One direction is clear and follows from the definition, the other is a bit more delicate to prove. One way is to identify $S/I(C)$ with the group algebra of $\mathbb{F}_2^n/C$.

Proposition 6.3. *$\mathcal{G}_{\leq}(C) = \{X^{u_1} - X^{v_1}, ..., X^{u_c} - X^{v_c}\} \cup \{X_i^2 - 1 : i \in S\}$ for some $u_1, ..., u_c, v_1, ..., v_c \in \mathbb{F}_2^n$, $S \subseteq [n]$. Moreover, for all $i \in [c]$:*

i) $\operatorname{supp} u_i \cap \operatorname{supp} v_i = \emptyset$.

ii) $X^{u_i} > X^{v_i}$.

iii) $u_i + v_i \in C$.

iv) $w(v_i) \leq w(u_i)$.

Proof. Recall that a generating set for $I(C)$ is $\{X^{w_i} - 1 : i \in [k]\} \cup \{X_j^2 - 1 : j \in [n]\}$. Let's calculate the S-polynomials:

- A direct computation shows that the S-polynomial associated to $X^{w_i} - 1$, $X^{w_j} - 1$ is of the form $X^a - X^b$ for some $a, b \in \mathbb{F}_2^n$.
- The S-polynomial associated to $X_i^2 - 1$, $X_j^2 - 1$ is $X_j^2 - X_i^2 = X_j^2 - 1 - (X_i^2 - 1)$, so we can exclude it since it gives zero remainder.
- The S-polynomial associated to $X^{w_i} - 1$, $X_j^2 - 1$ is either $X_j^2 - X^{w_i}$ if $j \notin \operatorname{supp} w_i$, in which case it gives a zero remainder and we can exclude it, or $X^{w_i - e_j} - X_j$ if $j \in \operatorname{supp} w_i$, where $e_j = (0, ..., 0, 1, 0, ..., 0)$, with the 1 in the j^{th} position.

In any case, we either get a polynomial which we can exclude or a binomial of the form $X^a - X^b$, with $a, b \in \mathbb{F}_2^n$. It is not hard to see that the remainder of a multivariate polynomial division of a binomial by a list of binomials is again a binomial and, since we also have the $X_i^2 - 1$ in the list of binomials by which we divide, we must end up with binomials of the form $X^a - X^b$ such that $a, b \in \mathbb{F}_2^n$, since, as long as some monomial in the support is not square-free, we can divide it by some $X_j^2 - 1$.

So we proved that we can always find a Gröbner basis of the form $\mathcal{G}' = \{X^{u_1} - X^{v_1}, ..., X^{u_c} - X^{v_c}\} \cup \{X_i^2 - 1 : i \in [n]\}$ for some $u_1, ..., u_c, v_1, ..., v_c \in \mathbb{F}_2^n$ and property *iii)* has to be satisfied because of the previous remark. Another remark in the previous section explained how to get a reduced Gröbner basis from any Gröbner basis. It is not hard to see that, when applying it to $\mathcal{G}'$, we still get a set of square-free binomials along with some of the $X_i^2 - 1$.

Property *ii)* has to be satisfied because a reduced Gröbner basis, by definition, only contains monic polynomials, and *iv)* follows from the fact that $\leq$ is degree-compatible, so it remains to prove *i)*. Let $i \in [c]$, then we can express u_i, v_i as $u_i = u_i' + a$ and $v_i = v_i' + a$ such that $\operatorname{supp} u_i' \cap \operatorname{supp} v_i' = \emptyset$ and $\operatorname{supp} a = \operatorname{supp} u_i \cap \operatorname{supp} v_i$. But then $u_i' + v_i' = u_i + v_i \in C$, so $X^{u_i'} - X^{v_i'} \in I(C)$ so, since $\mathcal{G}_{\leq}(C)$ is a Gröbner basis, there exists some j such that $X^{u_j} | X^{u_i'} | X^{u_i}$. Since $\mathcal{G}_{\leq}(C)$ is reduced, we must have $i = j$, so $X^{u_i'} = X^{u_i}$ and $u_i' = u_i$, but then $a = 0$, so $\operatorname{supp} a = \operatorname{supp} u_i \cap \operatorname{supp} v_i = \emptyset$.

□

Remark. Some binomials of the form $X_i^2 - 1$ can be left out, but this only happens if either a binomial of the form $X_i - X_j$, with $X_i > X_j$, or $X_i - 1$ ends up in the Gröbner basis.

Example. Let C be the $[5, 3]$ binary code with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

By proposition 6.1, a set of generators of $I(C)$ is

$$X_2X_3X_4 - 1, X_1X_2X_5 - 1, X_1X_4X_5 - 1,$$

$$X_1^2 - 1, X_2^2 - 1, X_3^2 - 1, X_4^2 - 1, X_5^2 - 1, X_6^2 - 1.$$

Starting from this, one can calculate the reduced Gröbner basis of C with respect to DEGREVLEX and it turns out to have 14 elements.

The following result is of key importance.

Theorem 6.4. *Let* $X^u - X^v \in \mathcal{G}_{\leq}(C) \backslash \{X_i^2 - 1 : i \in [n]\}$*, then* $u + v \in C$ *is a codeword with minimal support. Moreover, there exists* $X^a - X^b \in \mathcal{G}_{\leq}(C) \backslash \{X_i^2 - 1 : i \in [n]\}$ *such that* $w(a + b) = d_1(C)$*.*

Proof. Let $a \in C \backslash \{0\}$ such that $\operatorname{supp} a \subseteq \operatorname{supp}(u + v) = \operatorname{supp} u \uplus \operatorname{supp} v$. Let $b, c \in \mathbb{F}_2^n$ such that $\operatorname{supp} b \subseteq \operatorname{supp} u$, $\operatorname{supp} c \subseteq \operatorname{supp} v$ and $a = b + c$ (if $S = \operatorname{supp} u \cap \operatorname{supp} a$ and $T = \operatorname{supp} v \cap \operatorname{supp} a$, then b is the element of $\mathbb{F}_2^n$ that has ones in the entries indexed by S and all zeroes elsewhere, and likewise for c).

But then, $X^b - X^c \in I(C)$, so, since $\mathcal{G}_{\leq}(C)$ is a Gröbner basis and since both X^b and X^c are square-free monomials, there exists $X^s - X^t \in \mathcal{G}_{\leq}(C) \backslash \{X_i^2 - 1 : i \in [n]\}$ such that X^s divides the leading term of $X^b - X^c$, which is either X^b or X^c. However, if it were X^c, we would have $X^s | X^c | X^v$, so $X^v \in \mathrm{LT}_{\leq}(I(C))$, but this is impossible because $\mathcal{G}_{\leq}(C)$ is reduced. Therefore, $X^s | X^b | X^u$, but then, again because $\mathcal{G}_{\leq}(C)$ is reduced, we must have $X^s - X^t = X^u - X^v$.

As a consequence, $X^u = X^b$, so $b = u$ and $X^b - X^c - (X^u - X^v) = X^v - X^c \in I(C)$. If this weren't zero, its leading term, would be X^v, since clearly $X^c | X^v$, but this would imply that $X^v \in \mathrm{LT}_{\leq}(I(C))$, which cannot be the case because the Gröbner basis is reduced. Therefore $X^b - X^c = X^u - X^v$ and so $a = u + v$.

We have proved the firs part, now we have to prove that there is a binomial $X^u - X^v$ in the reduced Gröbner basis such that $w(u+v) = d$, where $d = d_1(C)$. Let $a \in C$ such that $w(a) = d$, and let $b, c \in \mathbb{F}_2^n$ be such that $a = b + c$, with $w(b) = \lfloor \frac{d}{2} \rfloor + 1$. Then $X^b - X^c \in I(C)$, so $\mathrm{LT}_{\leq}(X^b - X^c) = X^b \in \mathrm{LT}_{\leq}(I(C))$ and there is some $X^u - X^v \in \mathcal{G}_{\leq}(C) \backslash \{X_i^2 - 1 : i \in [n]\}$ such that $X^u | X^b$, in particular $\operatorname{supp} u \subseteq \operatorname{supp} b$ (we have $\mathrm{LT}_{\leq}(X^b - X^c) = X^b$ because $\deg X^b = w(b) > w(c) = \deg(X^c)$ and $\leq$ is degree-compatible).

Let $a' = a + u + v = b + u + c + v \in C$. If $a' = 0$ then $u + v = a$ and we are done, so assume that $a' \neq 0$.

Notice that, since $\operatorname{supp}(b+u) = \operatorname{supp} b \backslash \operatorname{supp} u$, we have $w(b+u) = w(b) - w(u)$. We also have the following chain of inequalities:

$$w(a') = w(a+u+v) \leq w(b+u) + w(c+v) \leq w(b+u) + w(c) + w(v)$$

$$= w(b) - w(u) + w(c) + w(v) \leq w(b) + w(c) = w(a) = d.$$

But $a' \in C \backslash \{0\}$, so all the inequalities above must be equalities. In particular, the last inequality being an equality implies $w(v) = w(u)$.

If $b = u$ then $w(v) = w(u) > w(c)$ and $a' = c + v \in C \backslash \{0\}$, so $X^v - X^c \in I(C)$ which implies that $\mathrm{LT}_{\leq}(X^v - X^c) = X^v \in \mathrm{LT}_{\leq}(I(C))$, which is impossible since the Gröbner basis is reduced, therefore $b \neq u$. More precisely, $\operatorname{supp} u \subsetneq \operatorname{supp} b$, hence $w(u) < w(b)$. But then we have

$$w(u+v) = w(u) + w(v) = 2w(u) \leq 2(w(b) - 1) = 2 \left\lfloor \frac{d}{2} \right\rfloor \leq d.$$

Since $u + v \in C \backslash \{0\}$ we must have $w(u+v) = d$. □

Motivated by this result, we give the following

Definition 6.8. *The $\mathcal{G}_{\leq}$-test set of C is the set of elements of C of the form $u + v$ such that $X^u - X^v \in \mathcal{G}_{\leq}(C) \backslash \{X_i^2 - 1 : i \in [n]\}$. We will denote this set by $\mathcal{T}_{\leq}(C)$.*

Example. We continue with the previous example, where we have a code C with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

We already mentioned that $\mathcal{G}_{\leq}(C)$ has 14 elements. The $\mathcal{G}_{\leq}$-test set of C is

$$\mathcal{T}_{\leq}(C) = \{100001,\ 011010,\ 000111,\ 011101\}$$

whereas the set of all codewords of minimal supports also contains 100110 and 111100.

In the following example, the difference between the $\mathcal{T}_{\leq}(C)$ and the set of all the minimal codewords is much more prominent:

Example. Let C be the $[14, 9]$-code with generator matrix

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

and let $\leq$ be DEGREVLEX. The Stanley-Reisner ideal of the matroid associated to C is minimally generated by 147 monomials, whereas the $\mathcal{T}_{\leq}(C)$ only has 24 elements.

We remarked at the end of chapter 4 that, in order to get the generalised Hamming weights of C from a minimal graded free resolution of its associated matroid, one needs to know all the minimal supports of the nonzero elements of C, but we just showed that, in the binary case, in order to get the first Hamming weight it's enough to look at the $\mathcal{G}_{\leq}$-test set.

Our hope is that the same is true for the higher weights, that is, if J is the monomial ideal generated by the monomials of the form X^a such that a is in the $\mathcal{G}_{\leq}$ test set of C, we hope that

$$d_i(C) = \min\{j : \beta_{ij}(S/J) \neq 0\}.$$

Unluckily, this is not always the case. For example, it might happen that S/J has projective dimension strictly less than the projective dimension of S/I, which is k, in which case the minimum on the right hand side of the equation doesn't even make sense for i greater than the projective dimension of S/J.

Example. Let C be the $[10, 7]$-binary code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Let I be the Stanley-Reisner ideal of $\mathcal{M}_C$ and J be the ideal generated by the X^a, with $a \in \mathcal{T}_{\leq}(C)$, where we take $\leq$ to be DEGREVLEX. The Betti table for S/I is:

	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

As a consequence, by theorem 5.9, the weight hierarchy of C is (2,4,5,6,8,9,10). On the other hand, the Betti table for S/J is

	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

from which we would get the weight hierarchy (2,4,5,7,8,9), which does not coincide with the weight hierarchy of C.

Example. For the $[14, 9]$-code we described before, one can show that we can actually recover the Hamming weight from the $\mathcal{G}_{\leq}$-test set.

6.4 Test sets and Hamming weights

For the remainder of this section, let J be the monomial ideal generated by the monomials of the form X^a, with a in $\mathcal{T}_{\leq}(C)$. The following theorem shows that what we hope was an equality is at least an inequality that bounds the generalised Hamming weights of C from above. The following results come from [7].

Theorem 6.5. *Let p be the projective dimension of S/J, then $p \leq k$ and, for all $i \leq p$,*

$$d_i(C) \leq \min\{j : \beta_{ij}(S/J) \neq 0\}.$$

Proof. This follows from the fact that the minimal generators of J are a subset of the minimal generators of I, and that's because all the codewords in $\mathcal{T}_{\leq}(C)$ have minimal support. □

Corollary 6.5.1.

$$d_1(C) = \min\{j : \beta_{ij}(S/J) \neq 0\}$$

Proof. $\beta_{1j}(S/J)$ is the number of minimal generators of J of degree j, and we know, by theorem 6.4, that there is a codeword a in the $\mathcal{G}_{\leq}$-test set of C whose weight is $d_1(C)$, but then X^a is a minimal generator of J of degree $d_1(C)$, so that $d_1(C) \geq \min\{j : \beta_{1j}(S/J) \neq 0\}$, and thanks to theorem 6.5 we know that the opposite inequality holds as well. □

For the remainder of this section, our goal is to prove that equality holds in theorem 6.5 when $i = 2$. In order to do that, we need a couple of results.

Lemma 6.6. *Let A, B be finite sets such that $|A \cap B| > \frac{|A|}{2}$, then*

i) $|A \backslash B| < \frac{|A|}{2}$

ii) $|A \triangle B| < |B|$

Proof. $A = (A\backslash B) \uplus (A \cap B)$, so $|A| = |A\backslash B| + |A \cap B| < |A\backslash B| + \frac{|A|}{2}$ and *i*) follows. Furthermore, $A \triangle B = (A\backslash B) \uplus (B\backslash A)$, so $|A\triangle B| < \frac{|A|}{2} + |B\backslash A| < |A \cap B| + |B\backslash A| = |B|$. □

Now, define $\mathcal{A}$, a_1 and a_2 as follows:

1. $\mathcal{A} = \{a \in C : \exists b \in C \text{ s.t. } d_2(C) = w(\langle a, b\rangle)\}$.
2. $a_1 \in \mathcal{A}$ is such that $X^{a_1} = \min_{\leq}\{X^a : a \in \mathcal{A}\}$.
3. $a_2 \in \mathcal{A}$ is such that $X^{a_2} = \min_{\leq}\{X^a : a \in \mathcal{A} \text{ and } d_2(C) = w(\langle a, a_1\rangle)\}$.

Recall that $\leq$ is a degree-compatible term order on S. In other words, $\mathcal{A}$ is the set of codewords contained in a 2-dimensional subcode of minimal weight, a_1 is the smallest element of $\mathcal{A}$ w.r.t. the order relation $a \leq b \iff X^a \leq X^b$ and a_2 is the smallest elements that generates a 2-dimensional subcode of minimal weight with a_1.

Remark. $X^{a_1} \leq X^{a_2} \leq X^{a_1+a_2}$, so, since $\leq$ is degree-compatible, we have $w(a_1) \leq w(a_2) \leq w(a_1 + a_2)$. If $I_1 = \operatorname{supp} a_1$ and $I_2 = \operatorname{supp} a_2$, then we have $|I_1| \leq |I_2| \leq |I_1 \triangle I_2|$. Thanks to lemma 6.6, it follows that

$$|I_1 \cap I_2| \leq \frac{|I_1|}{2} \leq \frac{|I_2|}{2}.$$

We are going to prove that we can find a_1 and a_2 in $\mathcal{T}_{\leq}(C)$, from which the main result regarding $d_2(C)$ will follow.

Proposition 6.7. *$a_1 \in \mathcal{T}_{\leq}(C)$.*

Proof. Let $a_1 = u + v$, with $\operatorname{supp} u \cap \operatorname{supp} v = \emptyset$ and $w(u) = \lceil \frac{w(a_1)}{2} \rceil$. In particular, $w(u) \geq w(v) \geq w(u) - 1$. Then $f = X^u - X^v \in I(C)$ and, since $\leq$ is degree-compatible, we have $\mathrm{LT}_{\leq}(f) = X^u$ if $w(u) > w(v)$. If $w(u) = w(v)$ and $X^v > X^u$, then we can interchange u and v so that $\mathrm{LT}_{\leq}(f) = X^u$.

Let $X^a - X^b \in \mathcal{G}_{\leq}(C)$ such that $X^a | X^u$, which is equivalent to $\operatorname{supp} a \subseteq \operatorname{supp} u$. Assume, by contradiction, that $\operatorname{supp} a \subsetneq \operatorname{supp} u$, then we have

$$w(b) \leq w(a) \leq w(u) - 1 \leq w(v) \leq w(u).$$

As a consequence, $w(a + b) < w(u + v) = w(a_1)$, in particular $X^{a+b} < X^{a_1} < X^{a_2}$, so, by the choice of a_2, $w(\langle a + b, a_1\rangle) = |\operatorname{supp}(a + b) \cup I_1| > d_2(C)$. Hence,

$$|I_1| + |I_2| - |I_1 \cap I_2| = |I_1 \cup I_2| = d_2(C) \leq |\operatorname{supp}(a + b) \cup I_1| - 1$$

$$= |\operatorname{supp} b \cup I_1| - 1 \leq |\operatorname{supp} b| + |I_1| - |\operatorname{supp} b \cap I_1| \leq |\operatorname{supp} a| + |I_1| - |\operatorname{supp} b \cap I_1| - 1$$

where the third equality follows from $\operatorname{supp} a \subseteq \operatorname{supp} u \subseteq I_1$ and the last inequality follows from $X^b \leq X^a$. Consequently,

$$|I_2| - |I_1 \cap I_2| \leq |\operatorname{supp} a| - |\operatorname{supp} b \cap I_1| - 1 \leq w(a) - 1.$$

Thus, by the previous remark,

$$w(a) = w(a) - 1 + 1 \geq |I_2| - |I_1 \cap I_2| + 1 \geq |I_2| - \frac{1}{2}|I_2| + 1 = \frac{1}{2}|I_2| + 1$$
$$\geq \frac{1}{2}|I_1| + 1 = \frac{w(a_1)}{2} + 1 > w(u);$$

which is a contradiction. This proves that X^u is a minimal generator of $\mathrm{LT}_{\leq}(I(C))$.

In order to prove that f is in $\mathcal{G}_{\leq}(C)$, we still need to check that $X^v \notin \mathrm{LT}_{\leq}(I(C))$. Assume by contradiction that this wasn't the case, then there is $X^a - X^b \in \mathcal{G}_{\leq}(C)$ such that $X^a | X^v$ or, equivalently, $\operatorname{supp} a \subseteq \operatorname{supp} v$. But then, $X^b < X^a \leq X^v < X^u$ and, in particular, $X^{a+b} < X^{u+v} = X^{a_1} < X^{a_2}$. One then proceeds as above, and gets $w(v) < w(a)$, which is a contradiction since $\operatorname{supp} a \subseteq \operatorname{supp} v$.

□

Proposition 6.8. *$a_2 \in \mathcal{T}_{\leq}(C)$.*

Proof. Let $u_1, u_2, v \in \mathbb{F}_2^n$ such that

1. $\operatorname{supp} u_1$, $\operatorname{supp} u_2$ and $\operatorname{supp} v$ are pairwise disjoint.
2. $\operatorname{supp} v = I_1 \cap I_2$.
3. $\operatorname{supp} u_1 \uplus \operatorname{supp} u_2 = I_2 \backslash I_1$.
4. $w(u_2) = \lfloor \frac{w(a_2)}{2} \rfloor$.

That we can choose u_1, u_2 and v such that they satisfy 1,2 and 3 is clear. Since $|I_1 \cap I_2| \leq \frac{|I_2|}{2}$, we also have $|I_2 \backslash I_1| \geq \frac{|I_2|}{2} = \frac{w(a_2)}{2}$ and that's why we can also choose u_1, u_2 and v so that they satisfy 4.

Since the supports of u_1, u_2 and v_3 partition the support of a_2 in such a way that $|\operatorname{supp} u_2| = \lfloor \frac{1}{2} |\operatorname{supp} a_2| \rfloor$, we have $w(u_2) + 1 \geq w(u_1) + w(v) \geq w(u_2)$.

Now, let

$$g = X^{u_1+v} - X^{u_2}.$$

Notice that, since their supports coincide, $u_1 + u_2 + v = a_2$. In particular, $g \in I(C)$ and therefore there exists $X^a - X^b \in \mathcal{G}_{\leq}(C)$ such that $X^a | \mathrm{LT}_{\leq}(g)$. A priori, it is not clear what the leading term of g is, so we study both cases with the goal of proving that either g or $-g$ is in the reduced Gröbner basis. In any case, it will follow that $a_2 \in \mathcal{T}_{\leq}(C)$.

Case 1 : $\mathrm{LT}_{\leq}(g) = X^{u_1+v}$. In this case, $X^a | X^{u_1+v}$, so $\operatorname{supp} a \subseteq \operatorname{supp} u_1 \uplus \operatorname{supp} v = \operatorname{supp} u_1 \uplus I_1 \cap I_2 \subseteq I_2$. Assume by contradiction that the inclusion was strict, then $w(b) \leq w(a) \leq w(u_1 + v) - 1 = w(u_1) + w(v) - 1 \leq w(u_2)$, so $w(a+b) \leq w(u_1 + u_2 + v) - 1 = w(a_2) - 1 < w(a_2)$, but then

$$d_2(C) = |I_1 \cup I_2| = |I_1| + |I_2 \backslash I_1| = |I_1| + w(u_1) + w(u_2)$$

$$\geq |I_1| + w(u_1) + w(a) \geq |I_1| + w(u_1) + w(b)$$

$$\geq |I_1 \cup \operatorname{supp} u_1 \cup \operatorname{supp} b| = |I_1 \cup \operatorname{supp}(u_1 + v) \cup \operatorname{supp} b|$$

$$\geq |I_1 \cup \operatorname{supp} a \cup \operatorname{supp} b = |I_1 \cup \operatorname{supp}(a + b)|,$$

which is a contradiction because $|I_1 \cup \operatorname{supp}(a+b)| = w(\langle a_1, a+b\rangle)$, with $X^{a+b} < X^{a_2}$.

Therefore, $a = u_1 + v$ and $X^{u_1+v} - X^b \in \mathcal{G}_{\leq}(C)$, in particular $X^b \notin \mathrm{LT}_{\leq}(I(C))$. Suppose by contradiction that $b \neq u_2$, then $0 \neq X^a - X^b - g = X^{u_2} - X^b \in I(C)$ and $X^{u_2} > X^b$ because $X^b \notin \mathrm{LT}_{\leq}(I(C))$. However,

$$|I_1 \cup \operatorname{supp}(a + b)| = |I_1 \cup \operatorname{supp} u_1 \cup \operatorname{supp} v \cup \operatorname{supp} b|$$

$$= |I_1 \cup \operatorname{supp} u_1 \cup \operatorname{supp} b| \leq |I_1| + w(u_1) + w(b)$$

$$\leq |I_1| + w(u_1) + w(u_2) = |I_1| + |I_2 \backslash I_1| = |I_1 \cup I_2| = d_2(C),$$

which is a contradiction because we would have $|I_1 \cup \operatorname{supp}(a + b)| = w(\langle a_1, a + b\rangle) = d_2(C)$, with $X^{a+b} = X^{u_1+v}X^b < X^{u_1+v}X^{u_2} = X^{a_2}$.

Case 2: $\mathrm{LT}_{\leq}(g) = X^{u_2}$. One proceeds as above by first showing that $a = u_2$ and then that $b = u_1 + v$. For the first part, one can check that, if $a \neq u_2$, then $c = a + b + a_2$ would have to satisfy $w(\langle a_1, c\rangle) = d_2(C)$ with $X^c < X^{a_2}$, a contradiction. One can also check that, if $b \neq u_1 + v$, this would imply $w(a_1, u_1 + v + b) = d_2(C)$ with $X^{u_1+v+b} < X_2^a$, which again, is a contradiction.

□

The next theorem is then a trivial consequence of the two preceding propositions.

Theorem 6.9. *There exist $a_1, a_2 \in \mathcal{T}_{\leq}(C)$ such that*

$$d_2(C) = |\operatorname{supp} a_1 \cup \operatorname{supp} a_2| = w(\langle a_1, a_2\rangle).$$

In order to prove the main theorem, we will use the following result, which can be used to construct the second module of a minimal graded free resolution of a monomial ideal.

Theorem 6.10. *Let $m_1, ..., m_c \in S$ be monomials and let*

$$\phi : \bigoplus_{i=1}^{c} S(-\deg m_i) \to S,\ e_i \mapsto m_i;$$

where e_i denotes the vector with i^{th} entry equal to 1 and all the other entries equal to 0. For all $i, j \in [c]$ let $m_{ij} = \mathrm{GCD}(m_i, m_j)$ and

$$\sigma_{ij}(m_1, ..., m_c) = \frac{m_j}{m_{ij}} e_i - \frac{m_i}{m_{ij}} e_j.$$

Then

i) $\sigma_{ij}(m_1, ..., m_c)$ *is homogeneous of degree equal to* $\deg \operatorname{lcm}(m_i, m_j)$.

ii) $\ker \phi = \langle \sigma_{ij}(m_1, ..., m_c) : 1 \leq i < j \leq c \rangle$.

Remark. If $a, b \in \mathbb{F}_2^n$, then $\operatorname{lcm}(X^a, X^b) = X^{\operatorname{supp} a \cup \operatorname{supp} b}$ has degree equal to $w(\langle a, b \rangle)$.

Let $\mathfrak{m} = (X_1, ..., X_n)$ be the unique homogeneous maximal ideal of S.

Lemma 6.11. *Let M be a finitely generated graded S-module, generated by the homogeneous elements $x_1, ..., x_c$. If $x_i \notin \mathfrak{m}M$, there exists $I \subseteq [c]$ containing i such that the x_j with $j \in I$ form a minimal set of generators of M.*

Proof. $x_1, ..., x_c$ generate M, therefore their classes generate $M/\mathfrak{m}M$. We also know that the class of x_i is not zero, so we can extract a basis of $M/\mathfrak{m}M$ from the classes of $x_1, ..., x_c$ containing x_i, but then, from a consequence of Nakayama's lemma, their representatives form a minimal set of generators of M. □

Theorem 6.12.

$$d_2(C) = \min\{j : \beta_{2,j}(S/J) \neq 0\}.$$

Proof. We will prove this by explicitly constructing the first three modules of a minimal graded free resolution

$$... \xrightarrow{\partial_{i+1}} F_i \xrightarrow{\partial_i} ... \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} S/J \to 0$$

of S/J. Let $\mathcal{T}_{\leq}(C) = \{a_1, ..., a_c\}$. According to theorem 6.9, there are i, j with $i \neq j$ such that $w(\langle a_i, a_j \rangle) = d_2(C)$. Up to reordering the elements of $\mathcal{T}_{\leq}(C)$, we may assum without loss of generality that $i = 1$ and $j = 2$.

We construct F_0 and F_1 as follows:

F_0 is just S with the standard grading and ∂_0 is the quotient map.

$F_1 = \bigoplus_{i=1}^{c} S(-w(a_i))$ and ∂_1 sends e_i to X^{a_i}, where e_i is the vector with a 1 in the i^{th} position and all zeroes elsewhere.

So far, $\ker \partial_0 = J \subseteq \mathfrak{m}F_0 = \mathfrak{m}$ because J is a nontrivial monomial ideal, and $\ker \partial_1 \subseteq \mathfrak{m}F_1$ because the X^{a_i} are minimal homogeneous generators of J. In light of theorem 6.10, we would like to construct F_2 and ∂_2 as follows:

$$F_2 = \bigoplus_{1 \leq i < j \leq c} S(-\deg \operatorname{lcm}(X^{a_i}, X^{a_j})) = \bigoplus_{1 \leq i < j \leq c} S(-w(\langle a_i, a_j \rangle)),$$

$$\partial_2 : F_2 \to F_1, \ e_{ij} \mapsto \sigma_{ij},$$

where $\sigma_{ij} = \sigma_{ij}(X^{a_1}, ..., X^{a_c})$.

However, the σ_{ij} might not be a minimal set of generators of $\ker \partial_1$. Nonetheless, σ_{12} has degree $\deg \operatorname{lcm}(X^{a_1}, X^{a_2}) = w(\langle a_1, a_2 \rangle) = d_2(C)$, which is smaller than or equal to the degree of all the other σ_{ij}s. This implies that $\ker \partial_1$ is non zero in degree $d_2(C)$ and zero in degree i for all $i < d_2(C)$, but then σ_{12} cannot lie in $\mathfrak{m} \ker \partial_1$ since, otherwise, it would have degree strictly greater than $d_2(C)$.

Hence, by lemma 6.11, there is a minimal set of generators of $\ker \partial_1$ of the form $\{\sigma_{ij} : (i,j) \in I\}$, for some $I \subseteq [n]^2$ such that $(1,2) \in I$. Then, we construct F_2 and ∂_2 as follows:

$$F_2 = \bigoplus_{(i,j)\in I} S(-w(\langle a_i, a_j\rangle)),$$

$$\partial_2 : F_2 \to F_1,\ e_{ij} \mapsto \sigma_{ij}.$$

In this case we do have that $\ker \partial_2 \subseteq \mathfrak{m}F_2$, so we can keep constructing a minimal resolution by minimally presenting $\ker \partial_2$ and so on. In particular, we have that

$$\min\{j : \beta_{2j}(S/J) \neq 0\} = \min\{j : F_2 \text{ is not zero in degree } j\} = d_2(C).$$

□

There are still some open problems regarding the $\mathcal{G}_{\leq}$-test set of a code, for example:

1. Can we always recover $d_3(C)$ from the Betti numbers of S/J?

2. When the projective dimension of S/J is equal to k, can we recover all the Hamming weights of C from the Betti numbers of S/J?

Bibliography

[1] J. Oxley, *Matroid Theory*, Oxford University Press, 1992

[2] J. Herzog, T. Hibi, *Monomial Ideals*, Springer, 2011

[3] V.K. Wei, *Generalized Hamming weights for linear codes*, IEEE Transantions on Information Theory, 1991

[4] A. Björner, *The Homology and Shellability of Matroids and Geometric Lattices.*, Cambridge University Press, 1992

[5] T. Johnsen, H. Verdure, *Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids*, Springer Science and Business Media, 2013

[6] I. Márquez-Corbella, E. Martínez-Moro, E. Suárez Canedo, *On the ideal associated to a liner code*, 2015, arXiv:1206.5124

[7] I. García-Marcol, I. Márquez-Corbella, E. Martínez-Moro, Y. Pitones, *Free resolutions and generalized Hamming weights of binary linear codes*, 2022, arXiv:2203.17194