UiT THE ARCTIC UNIVERSITY OF NORWAY

Faculty of Science and Technology

Department of Mathematics and Statistics

Homological methods applied to theory of codes and matroids

—

Anna Karpova

MAT-3900 Master's thesis in mathematics *May 2015*

Abstract

In this thesis we first give a survey of linear error-correcting codes, and how many of their most important properties only depend on the matroids derived from their parity check matrices. We also introduce the Stanley-Reisner ring associated to the simplicial complex of the independent sets of a matroid.

We then recall in particular how some important properties of linear codes, including their generalized weight polynomials, are dependent only on the $\mathbb{Z}$-graded Betti numbers for the Stanley-Reisner rings of their associated matroids, and the so-called elongations of these matroids. We will use this fact to find the generalized weight polynomials of simplex codes and Reed-Müller codes of the first order.

Acknowledgements

First of all, I would like to thank my supervisor, Professor Trygve Johnsen, for his supervision during the last two years. I highly appreciate his help, expert advice and good suggestions. I would also like to express thanks to my co-supervisor Hugues Verdure for the lecture notes on Coding and Matroid theory and very helpful advice. Without their help I would not have been able to complete this thesis.

I am grateful to my university fellows. I have enjoyed studying with them during my two years in Tromsø. Studying and working on the thesis at the UIT The Arctic University of Norway have given me a great experience.

My special thanks goes to my family, especially my mother, for her support and constant encouragement.

Contents

Introduction

This thesis is about studying linear codes, matroids and simplicial complexes, and concepts related to them. We are going to see that it is very natural to study matroids, in connection with codes.

The main contribution in the thesis is the computation of the generalized weight polynomials for large classes of codes. Concretely in this thesis we shall consider the simplex codes (duals of Hamming codes), and Reed-Müller codes of the first order.

In order to do this we will present a series of concepts and objects from algebra and combinatorics and coding theory. A large part of the thesis in a natural way will be devoted to the presentation of these objects.

The thesis is structured as follows:

Our aim in Chapter 1 is to define block codes, linear codes and matroids (via various sets of axioms). The text in Chapter 1 is to a great extent based on picking relevant material from [14], and the main purpose is to define concepts and fundamental properties that will be used later.

In Chapter 2 we will explain how one can obtain matroids from codes and give the definition of minimum distance and weight hierarchy of matroids for the purpose of sketching the deep connection between codes and matroids. We will end this chapter by giving an example which shows how some matroids do not come from codes.

Chapter 3 is concerned with viewing the matroids appearing as special cases of simplicial complexes, being a concept originating from algebraic topology. Here we will also introduce and describe various algebraic and homological concepts and notions associated with simplicial complexes, in particular their Betti numbers over a given field, with different gradings.

Chapter 4 is about half of the thesis and it is dedicated to generalized weight polynomials. We may find them in two ways, in terms of Betti numbers and the other method was given in [9]. In this chapter we will also work with examples, including the simplex and Reed-Müller codes where we explicitly can find the Betti numbers of matroids and elongations of matroids. Therefore we will be able to describe properties of these codes, including higher weight distributions of the codes. It is important to note that we shall prove here the theorem, which states that the Reed-Müller code of the first order has a pure resolution of its associated Stanley-Reisner ideal. We need it in order to find Betti numbers applying the formula given in [2].

Chapter 1

Basic definitions

1.1 Linear codes

In this section, we will give definitions of linear codes, code parameters, weight hierarchy and weight distribution. We will also introduce the dual of a linear code.

Definition 1.1. An alphabet is a finite set of symbols.

Definition 1.2. Let q be an integer. Then a q-ary code is a set of r-tuples $(a_1, \ldots, a_r)$ (r may vary) where $a_i \in A$ and A is an alphabet with q elements. An element $(a_1, \ldots, a_r)$ in this set is called a codeword; r is the length of the codeword.

If r is fixed, then it is called a q-ary block code.
$(a_1, \ldots, a_n) \in A^n$ is just a word. Of course,

$$\{codewords\} \subset \{words\}.$$

The first important parameter of a code is the following:

Definition 1.3. The length n of a block code is equal to the length of any codeword.

Definition 1.4. Consider the alphabet A and A^n be the set of all words of length n. Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be two words. The Hamming distance between x and y is

$$d(x, y) = \#\{i, x_i \neq y_i\}.$$

If the alphabet is a field $A = \mathbb{F}_q$, then the weight of the codeword $x = (x_1, \ldots, x_n)$ is

$$wt(x) = \#\{i, x_i \neq 0\} = d(x, (0, \ldots, 0)).$$

Example 1.1.1. Let

$$x = (0, 1, 1, 2),$$
$$y = (1, 1, 1, 1).$$

Then the Hamming distance between x and y is 2, and the weight of x is 3.

Proposition 1.1. *The Hamming distance is a distance on the code, that is*

$$d(x, y) = 0 \Longleftrightarrow x = y,$$

$$d(x, y) = d(y, x),$$

$$d(x, y) \leqslant d(x, z) + d(z, y).$$

Proof. See [14]. □

Here is another important parameter of a code:

Definition 1.5. The minimum distance of a code $\mathcal{C}$ is

$$d = Min\{d(x, y) \mid x, y \in \mathcal{C}, x \neq y\}.$$

Any q-ary block code is an $(n, M, d)_q$ code. It means that we have a q-ary block code of length n with M codewords and minimum distance d.

Example 1.1.2. Binary code $\mathcal{C}$ of length $n = 5$ with $M = 4$ codewords and minimum distance $d = 3$ given by its set of codewords

$$\{00000, 01011, 10101, 11110\}.$$

Definition 1.6. A linear code over the finite field $\mathbb{F}_q$ is a vector subspace of the vector space $\mathbb{F}_q^n$.

Property. Let V be a vector space over a finite field $\mathbb{F}_q$, of finite dimension $k = dim_{\mathbb{K}}(V)$. Then

$$\#V = q^k.$$

From the property it follows that instead of writing that a linear code is a q-ary (n, q^k, d) code, we will say that the code is a $[n, k, d]_q$ code. Then a $[n, k, d]_q$ code is a linear code over $\mathbb{F}_q$ with length n, dimension k (and therefore cardinality q^k) and minimum distance d. We may omit d in the notation if the minimum distance is not specified.

Remark 1.1. The all zero vector is always a codeword of any linear code.

Remark 1.2. To describe a linear code, we only need to describe a basis. Then all the other codewords are linear combinations of this basis (of the vectors in the basis).

Example 1.1.3. Let $\mathcal{C}$ be the $[4,2]_3$ code, with basis $v_1 = 1011$ and $v_2 = 0112$. Then the set of codewords are of the form $\lambda_1 v_1 + \lambda_2 v_2$ and given in the following table:

λ_1	λ_2	*codeword*
0	0	0000
0	1	0112
0	2	0221
1	0	1011
1	1	1120
1	2	1202
2	0	2022
2	1	2101
2	2	2210

It is easy to see that all the non-zero codewords have weight 3. This is therefore a $[4,2,3]_3$ code. This code is in fact MDS and constant weight.

Definition 1.7. Any linear code whose minimum distance satisfies

$$d = n - k + 1,$$

is called maximum distance separable (MDS).

Definition 1.8. A code where all codewords, except for the zero codeword, have the same Hamming weight is called constant weight.

Lemma 1.1. *Let x, y be two codewords of a code. Then*

$$d(x,y) = wt(x-y).$$

Proof. See [14]. □

Theorem 1.1. *Let $\mathcal{C}$ be a linear code. Then the minimum distance (also called the Hamming weight of the code) is*

$$d = Min\{wt(x) \mid x \in \mathcal{C} - \{(0, \ldots, 0)\}\}.$$

Proof. See [14]. □

Definition 1.9. The support of a codeword $x = (x_1, \ldots, x_n)$ is

$$Supp(x) = \{i \mid x_i \neq 0\}$$

$$(wt(x) = \#Supp(x)).$$

If S is a set of codewords, then the support of S is just the union of the supports of the codewords

$$Supp(\mathcal{S}) = \bigcup_{x \in \mathcal{S}} Supp(x) = \{i \mid \exists x \in \mathcal{S}, x_i \neq 0\}.$$

Property. Let $\mathcal{C}$ be a linear code. Then the minimal distance d is

$$d = Min\{\#Supp(\mathcal{D}) \mid \mathcal{D} \text{ is a subcode of dimension 1 of } \mathcal{C}\}.$$

Proof. See [14]. □

Definition 1.10. Let $\mathcal{C}$ be a $[n, k]_q$ linear code. Then the generalized Hamming weights are

$$d_i = Min\{\#Supp(\mathcal{D}) \mid \mathcal{D} \text{ is a subcode of dimension } i \text{ of } \mathcal{C}\},$$

where $1 \leqslant i \leqslant k$. The sequence $(d_1, \ldots, d_k)$ is called the weight hierarchy of the code.

Remark 1.3. From the previous property, $d = d_1$. The k-th generalized Hamming weight d_k should be n, otherwise the code is degenerate, and can be replaced by a code with smaller length.

Lemma 1.2. *If $v_1, \ldots, v_k$ is a basis of a $[n, k]$ code $\mathcal{C}$, then*

$$Supp(\mathcal{C}) = \bigcup_{1 \leqslant i \leqslant k} Supp(v_i).$$

Proof. See [14]. □

Remark 1.4. The support of a code is equal to the union of the supports of a given basis, but usually, $d(\mathcal{C}) \neq Min\{wt(v_i), i \in \{1, \ldots, k\}\}$.

Proposition 1.2. *The weight hierarchy of a code is a strictly increasing sequence*

$$d_1 < d_2 < \ldots < d_k.$$

Proof. See [14]. □

Definition 1.11. Let $\mathcal{C}$ be a linear code. $\mathcal{C}$ has
1 codeword of weight 0,
m_1 codewords of weight 1,
m_2 codewords of weight 2,
$\cdots$,
m_n codewords of weight n.
Then $\{1, m_1, \ldots, m_n\}$ is called the weight distribution of $\mathcal{C}$.

As we have mentioned earlier, in order to describe a linear code, we just need to find a basis of the code. This gives rise to the following definition:

Definition 1.12. Let $\mathcal{C}$ be a $[n, k]_q$ linear code. Then a $k \times n$ matrix over $\mathbb{F}_q$ whose rows form a basis of $\mathcal{C}$ is called a generator matrix.

Remark 1.5. Generator matrices are not unique.
For example,

$$G_1 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

and

$$G_2 = \begin{bmatrix} 0 & 1 & 1 & 2 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

describe the same code, but $G_1 \neq G_2$.

Example 1.1.4. The constant weight code of Example 1.1.3 has generator matrix

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

Definition 1.13. Let $\mathcal{C}, \mathcal{D}$ be two $[n, k]$ linear codes over the field $\mathbb{F}_q$. Then the codes are equivalent if we can obtain $\mathcal{D}$ from $\mathcal{C}$ by a succession of the following operations:

1. permutation of the positions of the code
2. multiplication of the symbols at a fixed position by a non-zero constant.

Proposition 1.3. *Two equivalent linear codes have the same parameters: length, cardinality and minimal distance.*

Proof. See [14]. □

Definition 1.14. A generator matrix of the form

$$[I_k \mid A]$$

where I_k is the $k \times k$ identity matrix and A is a $k \times (n-k)$ matrix, is called a generator matrix of standard form.

Remark 1.6. Generator matrices of standard form are not unique for equivalent codes.

We want to define the parity check matrix of a code, but first we need some definitions.

Definition 1.15. Let $u, v \in \mathbb{F}_q^n$ be two vectors. Write $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$. Then the inner product is

$$u \cdot v = \sum_{i=1}^{n} u_i v_i.$$

The inner product is a bilinear form, that is, it is linear on each component of the cartesian product (bilinear), and its target is the set of scalars of the vector space (form).

Definition 1.16. A bilinear form $f \colon V \times V \longrightarrow \mathbb{K}$ is said to be:

- Symmetric if $f(x, y) = f(y, x)$ for all $x, y \in E$,
- Nondegenerate if $f(x, y) = 0 \, \forall y \in V \Rightarrow x = 0$ and $f(x, y) = 0 \, \forall x \in V \Rightarrow y = 0$.

Let $\mathcal{C}$ be a $[n, k]_q$ code with generator matrix G. Let $\mathcal{C}^\perp$ be the orthogonal of the code for the usual inner product

$$\mathcal{C}^\perp = \{w \in \mathbb{F}_q^n \text{ such that } w \cdot c = 0 \, \forall c \in \mathcal{C}\}.$$

Since the inner product is a nondegenerate symmetric bilinear form, we know that $\mathcal{C}^\perp$ is a $[n, n-k]_q$ code. A generator matrix H of $\mathcal{C}^\perp$ is therefore a $(n-k) \times n$ matrix with entries in $\mathbb{F}_q$, and whose rows are a basis of $\mathcal{C}^\perp$.

Definition 1.17. Let $\mathcal{C}$ be a $[n,k]_q$ linear code. Then the $[n,n-k]_q$ linear code $\mathcal{C}^\perp$ is called the dual of the code.

Theorem 1.2 (Wei's duality)**.** *Let $\mathcal{C}$ be a $[n,k]_q$ linear code, and $\mathcal{C}^\perp$ its dual code. Let $d_1 < \ldots < d_k$ and $e_1 < \ldots < e_{n-k}$ the weight hierarchies of $\mathcal{C}$ and $\mathcal{C}^\perp$ respectively. Then*

$$\{d_1, \ldots, d_k, n+1-e_1, \ldots, n+1-e_{n-k}\} = \{1, \ldots, n\}$$

Proof. See [15]. $\square$

Definition 1.18. A generator matrix of $\mathcal{C}^\perp$ is called a parity check matrix of $\mathcal{C}$.

Proposition 1.4. *If G, H are a generator matrix and a parity check matrix for $\mathcal{C}$ respectively, then they are a parity check matrix and a generator matrix for $\mathcal{C}^\perp$ respectively.*

Proof. See [14]. $\square$

Theorem 1.3. *Let $\mathcal{C}$ be a linear $[n,k]_q$ code given by a generator matrix G under standard form, say*

$$G = [I_k \ | \ A].$$

Then a parity check matrix for $\mathcal{C}$ is given by

$$H = [-A^t \ | \ I_{n-k}].$$

Proof. See [14]. $\square$

Definition 1.19. A parity check matrix of the form $H = [B \ | \ I_{n-k}]$ is said to be in standard form.

Example 1.1.5. Given the $[5,2]$ linear code $\mathcal{C}$ over $\mathbb{F}_3$.
Its generator matrix is

$$G = \left[\begin{array}{cc|ccc} 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 2 & 2 \end{array}\right] = \left[\ I_2 \mid A\ \right].$$

Let us find the matrix $-A^t$

$$-A^t = -\begin{bmatrix} 2 & 2 \\ 0 & 2 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 2 & 1 \end{bmatrix}.$$

Then we have

$$H = \left[\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 & 1 \end{array}\right].$$

1.2 Matroids

In this section, we will give definitions of matroids via various set of axioms, and cardinality and rank of matroids. As in the previous section, we will introduce the notion of duality of matroids.

1.2.1 Independent sets of a matroid

Matroids have many (equivalent) definitions.

Definition 1.20. A matroid on a finite set E is a set $\mathcal{I} \subset 2^E$ satisfying the following axioms:

(I_1) $\varnothing \in \mathcal{I}$,

(I_2) If $I_1 \in \mathcal{I}$ and $I_2 \subset I_1$, then $I_2 \in \mathcal{I}$,

(I_3) If I_1 and I_2 are both elements of $\mathcal{I}$ with $|I_1| < |I_2|$, then there exists $x \in I_2 \setminus I_1$ such that $I_1 \cup \{x\} \in \mathcal{I}$.

Definition 1.21. Two matroids $M_1 = (E_1, \mathcal{I}_1)$ and $M_2 = (E_2, \mathcal{I}_2)$ are isomorphic if there exists a bijection $\phi \colon E_1 \longrightarrow E_2$ such that

$$X \in \mathcal{I}_1 \Leftrightarrow \phi(X) \in \mathcal{I}_2.$$

Example 1.2.1. Let V be a vector space over $\mathbb{K}$ and $v_1, \ldots, v_n$ be vectors in V. We consider the set

$$\mathcal{I} = \{X \in 2^{\{1,\ldots,n\}}, \{v_k, k \in X\} \text{ is a linearly independent set}\}.$$

Then the $M = (\{1, \ldots, n\}, \mathcal{I})$ is a matroid. A matroid isomorphic to such a matroid is called a vector matroid.
If the v_i are the columns of a matrix A, then the associated vector matroid is denoted by $M[A]$.

Example 1.2.2. Let $E = \{1, 2, 3, 4, 5\}$, and consider

$$\mathcal{I} = \{\varnothing, 1, 2, 4, 5, \{1, 2\}, \{2, 4\}, \{2, 5\}, \{4, 5\}\}.$$

Then $M = (E, \mathcal{I})$ is not a matroid. Let $I_1 = \{1\}$ and $I_2 = \{4, 5\}$. Neither $\{1\} \cup \{4\}$ nor $\{1\} \cup \{5\}$ are independent.

Example 1.2.3. Let $E = \{1, 2, 3, 4, 5\}$ with

$$\mathcal{I} = \{\varnothing, 1, 2, 4, 5, \{1, 2\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{4, 5\}\}.$$

Then we could verify the axioms and see that $M = (E, \mathcal{I})$ is a matroid in this case.

Definition 1.22. The elements of $\mathcal{I}$ are called the independent sets of $M = (E, \mathcal{I})$. The maximal independent sets (for inclusion) are called bases of M. They are denoted by $\mathcal{B}$. The subsets of E that are not independent are called dependent. The minimal (for inclusion) dependent sets are called circuits and denoted by $\mathcal{C}$.

Definition 1.23. Let $M = (E, \mathcal{I})$ be a matroid. If $\{e\} \in \mathcal{C}$, then e is called a loop. If $\{e_1, e_2\} \in \mathcal{C}$, then e_1 and e_2 are called parallel elements.

Theorem 1.4. *A matroid over the ground set E is entirely defined by its set of bases, or by its set of circuits. Namely we have:*

$$\mathcal{I} = \{X \subset E,\ \exists B \in \mathcal{B},\ X \subset B\}$$

and

$$\mathcal{I} = \{X \subset E,\ \forall \sigma \in \mathcal{C},\ \sigma \not\subset X\}.$$

Proof. See [14]. □

1.2.2 Bases of a matroid

Proposition 1.5. *If B_1, $B_2 \in \mathcal{B}$, then $|B_1| = |B_2|$.*

Proof. See [14]. □

Proposition 1.6 (Base change)**.** *Let B_1, B_2 be two distinct bases of a matroid. Let $x \in B_2 \setminus B_1$. Then there exists $y \in B_1 \setminus B_2$ such that $B_2 \cup \{y\} \setminus \{x\}$ is a basis of the matroid.*

Proof. See [14]. □

Definition 1.24. Let E be a finite set and $\mathcal{B} \subset 2^E$. We say that $\mathcal{B}$ is a set of bases if it satisfies the two following axioms

(B_1) $\mathcal{B} \neq \varnothing$,

(B_2) $\forall B_1, B_2 \in \mathcal{B}$, $\forall x \in B_2 \setminus B_1$, $\exists y \in B_1 \setminus B_2$, $B_2 \cup \{y\} \setminus \{x\} \in \mathcal{B}$.

Corollary 1.1. *Let $M = (E, \mathcal{I})$ be a matroid. Then its set of bases $\mathcal{B}$ is a set of bases (in the sense of the definition).*

Proof. See [14]. □

Lemma 1.3. *Let $\mathcal{B}$ be a set of bases on E. Then all the elements in $\mathcal{B}$ have the same cardinality.*

Proof. See [14]. □

And we can now describe a matroid as the set of bases:

Theorem 1.5. *Let $\mathcal{B}$ be a set of bases on E. Let $\mathcal{I} = \{X \subset B, B \in \mathcal{B}\}$. Then $M(\mathcal{B}) = (E, \mathcal{I})$ is a matroid, whose set of bases is $\mathcal{B}$.*

Proof. See [14]. □

Example 1.2.4. Consider

$$\mathcal{B} = \{\{1,2,3\}, \{1,4,5\}, \{2,3,6\}, \{4,5,6\}\}.$$

Then M with this set of bases is not a matroid. The first axiom is trivial and it is easy to check that the couple $\{\{2,3,6\}, \{4,5,6\}\}$ doesn't satisfy the axiom (B_2). Let $B_1 = \{2,3,6\}$ and $B_2 = \{4,5,6\}$. Then $x = \{4\} \in B_2 \setminus B_1$ and $\exists y \in B_1 \setminus B_2 = \{2,3\}$, let us take $y = \{3\}$, such that $\{4,5,6\} \cup \{3\} \setminus \{4\} = \{3,5,6\} \notin \mathcal{B}$. If we take $y = \{2\}$, then $\{4,5,6\} \cup \{2\} \setminus \{4\} = \{2,5,6\}$ is not a base either, and therefore we get the conclusion.

Example 1.2.5. Let E be a finite set of cardinality n. Let $0 \leqslant m \leqslant n$, and let

$$\mathcal{B} = \{X \subset E, \ |X| = m\}.$$

Then $\mathcal{B}$ is the set of bases of a matroid, called the uniform matroid of rank m. The axiom (B_1) is obvious, while axiom (B_2) is also easy: if $B_1 \neq B_2$ and $x \in B_1 - B_2$, then any $y \in B_2 - B_1$ is such that $B_1 - \{x\} \cup \{y\}$ has cardinality m, and is therefore in $\mathcal{B}$. It is denoted by $U_{m,E}$. We write $U_{m,n}$ if $E = \{1, \ldots, n\}$.

1.2.3 Rank function

Definition 1.25. Let $M = (E, \mathcal{I})$ be a matroid. The rank of the matroid M is the function

$$\begin{array}{rccc} r: & 2^E & \longrightarrow & \mathbb{N} \\ & X & \longmapsto & Max\{|I|, I \subset X, I \in \mathcal{I}\}. \end{array}$$

The nullity function of M is $n\colon 2^E \longrightarrow \mathbb{N}$ defined by $n(X) = |X| - r(X)$. By abuse of notation, we shall write $r(M) = r(E)$.

We could have given another definition using bases:

Proposition 1.7. *Let $X \subset E$, then*

$$r(X) = Max\{|B \cap X|, B \in \mathcal{B}\}.$$

Proof. See [14]. □

Proposition 1.8. *The rank function of a matroid $M = (E, \mathcal{I})$ satisfies the following properties:*

(R_1) $r(\varnothing) = 0$,

(R_2) *If $X \subset E$ and $x \in E$, then $r(X) \leqslant r(X \cup \{x\}) \leqslant r(X) + 1$,*

(R_3) *If $X \subset E$ and $x, y \in E$ are such that $r(X \cup \{x\}) = r(X \cup \{y\}) = r(X)$, then $r(X \cup \{x, y\}) = r(X)$.*

Proof. See [14]. □

These properties are equivalent to the following ones:

Proposition 1.9. *Let $r\colon 2^E \longrightarrow \mathbb{N}$ be a function. Then the 3 following properties:*

(R'_1) $0 \leqslant r(X) \leqslant |X|$,

(R'_2) *If $X \subset Y \subset E$, $r(X) \leqslant r(Y)$,*

(R'_3) *If $X \subset Y \subset E$, $r(X \cap Y) + r(X \cup Y) \leqslant r(X) + r(Y)$*

are equivalent to the properties (R_1), (R_2) and (R_3).

Proof. See [14]. □

We are now able to give a third definition of a matroid:

Theorem 1.6. *Let E be a finite set and $r\colon 2^E \longrightarrow \mathbb{N}$ a function satisfying (R_1), (R_2) and (R_3) (or alternatively (R_1'), (R_2') and (R_3')). Then if*

$$\mathcal{I} = \{I \in 2^E, r(I) = |I|\},$$

then $(E,\mathcal{I})$ is a matroid, with set of bases

$$\mathcal{B} = \{I \in 2^E, r(E) = r(I) = |I|\},$$

and rank r.

Proof. See [14]. □

Example 1.2.6. Let $\mathbb{K}$ be a field, and $\mathbb{L}$ be a field extension of $\mathbb{K}$. Let $E = \{l_1, \ldots, l_s\} \in \mathbb{L}$. Then the function

$$\begin{array}{cccc} r: & 2^E & \longrightarrow & \mathbb{N} \\ & \{l_{i_1}, \ldots, l_{i_s}\} & \longmapsto & trdeg(\mathbb{K}(l_{i_1}, \ldots, l_{i_s}) : \mathbb{K}) \end{array}$$

is the rank function of a matroid. A matroid isomorphic to such a matroid is called an algebraic matroid.

Remark 1.7. Every vector matroid is algebraic. But the converse is not true. There are some algebraic matroids that are not vector matroids (over any field).

Proposition 1.10. *Let A be a $k \times n$ matrix with $k \leqslant n$. Then the rank function of the matroid $M[A]$ is given by:*

$$r_{M[A]}(X) = rank(A[X])$$

where $A[X]$ is the matrix formed by the columns of A indexed by X.

Proof. See [14]. □

1.2.4 Circuits of a matroid

Proposition 1.11. *The circuits $\mathcal{C}$ of a matroid satisfy the following properties:*

(C_1) $\varnothing \notin \mathcal{C}$,

(C_2) *If* $C_1, C_2 \in \mathcal{C}$ *with* $C_1 \subset C_2$, *then* $C_1 = C_2$,

(C_3) *If* $C_1, C_2 \in \mathcal{C}$ *are distinct and not disjoint, then for any* $e \in C_1 \cap C_2$, *there exists* $C_3 \in \mathcal{C}$ *such that* $C_3 \subset (C_1 \cup C_2) - \{e\}$.

Proof. See [14]. □

Remark 1.8. The property (C_3) is often called the weak (or global) elimination axiom for circuits, as opposed to the strong (or local) elimination axiom for circuits below.

Proposition 1.12. *Let E be a finite set and $\mathcal{C}$ be a set of subsets of E. Let (C_3') be the following property:*

$$(C_3') : \quad \begin{array}{c} \text{If } C_1, C_2 \in \mathcal{C} \text{ are distinct and not disjoint,} \\ \text{then for any } e \in C_1 \cap C_2 \text{ and } f \in C_1 \setminus C_2, \text{ there exists } C_3 \in \mathcal{C} \\ \text{such that } f \in C_3 \subset (C_1 \cup C_2) - \{e\}. \end{array}$$

Then the properties (C_1), (C_2) and (C_3) are equivalent to the properties (C_1), (C_2) and (C_3').

Proof. See [14]. □

Lemma 1.4. *If $M = (E, \mathcal{I})$ is a matroid with rank function r. Then a subset $X \subset E$ is dependent if and only if*

$$r(X) \leqslant |X| - 1.$$

In particular, if X is a circuit, then

$$r(X) = |X| - 1.$$

Proof. See [14]. □

Theorem 1.7. *Let E be a finite set, and $\mathcal{C} \subset 2^E$ satisfying the axioms (C_1), (C_2) and (C_3). Let*

$$\mathcal{I} = \{X \subset E,\ \nexists C \in \mathcal{C},\ C \subset X\}.$$

Then $(E, \mathcal{I})$ is a matroid whose set of circuits is $\mathcal{C}$.

Proof. See [14]. □

Example 1.2.7. Let $G = (V, E)$ be a graph. Then the set of minimal cycles of the graph is the set of circuits of a matroid. A matroid isomorphic to such a matroid is called a graphic matroid.

Remark 1.9. It can be shown that all graphic matroids are vector matroids (and therefore algebraic matroids). But there are some vector matroids that are not graphic.

1.2.5 Duality

Lemma 1.5. *Let M be a matroid on the ground set E with set of bases $\mathcal{B}$. Let $B_1, B_2 \in \mathcal{B}$ distinct. Let $x \in B_1 - B_2$. Then there exists $y \in B_2 - B_1$ such that $B_2 - \{y\} \cup \{x\} \in \mathcal{B}$.*

Proof. See [14]. □

Theorem 1.8. *Let M be a matroid on the ground set E with set of bases $\mathcal{B}$. Let*

$$\overline{\mathcal{B}} = \{E - B, B \in \mathcal{B}\}.$$

Then $M(\overline{\mathcal{B}})$ is a matroid over E.

Proof. See [14]. □

Definition 1.26. Let M be a matroid on the ground set E and set of bases $\mathcal{B}$. Then the matroid on E and set of bases $\overline{\mathcal{B}}$ is called the dual of M, and denoted by M^*.

Remark 1.10. We have of course that $(M^*)^* = M$.

Example 1.2.8. The dual of the uniform matroid of rank m, $U_{m,n}$ is the uniform matroid $U_{n-m,n}$.

Definition 1.27. Let M be a matroid. Then

- The elements of $\mathcal{I}(M^*)$ are the coindependent sets of M
- The elements of $\mathcal{B}(M^*)$ are the cobases of M
- The elements of $\mathcal{C}(M^*)$ are the cocircuits of M
- The rank function of M^* is the corank function of M
- A coloop of M is a loop of M^*.

Proposition 1.13. *Let M be a matroid of rank r on the ground set E. Then the rank of M^* (or the corank of M) is $\#E - r$.*

Proof. See [14]. □

Theorem 1.9. *Let M be a matroid of rank function r. Then the rank function r^* of M^* is given by*

$$r^*(X) = |X| + r(E - X) - r(M), \forall X \subset E.$$

Proof. See [14]. □

Corollary 1.2. *Let M be a matroid of nullity function n. Then the nullity function n^* of M^* is given by*

$$n^*(X) = |X| + n(E - X) - n(E).$$

Theorem 1.10. *Let M, N be two matroids. Then*

$$M \approx N \Longleftrightarrow M^* \approx N^*.$$

Proof. See [14]. □

Theorem 1.11. *If A is a $k \times n$ matrix of the form $A = [I_k \mid A']$ then $M[A]^* = M[B]$ for $B = [-A'^t \mid I_{n-k}]$.*

Proof. See [14]. □

Example 1.2.9. Given the vector matroid $M[A]$, associated to the following matrix

$$A = \left[\begin{array}{cc|ccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{array}\right] \text{ over } \mathbb{F}_2.$$

Then the matroid $M[B] = M[A]^*$, where

$$B = \left[\begin{array}{cc|ccc} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

gives the dual of the matroid $M[A]$.

Theorem 1.12. *If M is a vector matroid, then M^* is also a vector matroid.*

Proof. Follows from the previous theorem. $\square$

The class of vector matroids is closed under duality.

1.2.6 Elongations and truncations of matroids

Let M be a matroid on $E = \{1, \dots, n\}$ with rank $r(M) = r(E)$.

Definition 1.28. $E(M)$ is called the elongation of a matroid M if for any $X \subseteq E$

$$r_{E(M)}(X) = Min\{r_M(X) + 1, |X|\}.$$

This is well-defined, since $r_{E(M)}$ satisfies the axioms for rank function. We need to check the following:

(R_1) $r_{E(M)}(\varnothing) = 0$,

(R_2) If $X \subset E$ and $x \in E$, then $r_{E(M)}(X) \leqslant r_{E(M)}(X \cup \{x\}) \leqslant r_{E(M)}(X) + 1$,

(R_3) If $X \subset E$ and $x, y \in E$ are such that $r_{E(M)}(X \cup \{x\}) = r_{E(M)}(X \cup \{y\}) = r_{E(M)}(X)$, then $r_{E(M)}(X \cup \{x, y\}) = r_{E(M)}(X)$.

Proof. (R_1) $r_{E(M)}(\varnothing) = Min\{r_M(\varnothing) + 1, |\varnothing|\} = Min\{0 + 1, 0\} = 0$.
(R_2) By the definition $r_{E(M)}(X \cup \{x\}) = Min\{r_M(X \cup \{x\}) + 1, |X \cup \{x\}|\}$.
Then we have to verify that

$$Min\{r_M(X) + 1, |X|\} \leqslant Min\{r_M(X \cup \{x\}) + 1, |X \cup \{x\}|\} \leqslant$$

$$\leqslant Min\{r_M(X) + 1, |X|\} + 1 = Min\{r_M(X) + 2, |X| + 1\}.$$

But this is true since:

$$r_M(X) + 1 \leqslant r_M(X \cup \{x\}) + 1 \leqslant r_M(X) + 2,$$

since r_M satisfies (R_2) and

$$|X| \leqslant |X \cup \{x\}| \leqslant |X| + 1.$$

We will leave the proof for the third axiom. □

Definition 1.29. For $i = 0, \ldots, n - r(M)$ define a matroid $M_{(i)}$, which is an i-th elongation

$$M_{(i)} = \underbrace{E(E(\ldots E(M)))}_{i \text{ times}}.$$

Proposition 1.14. *The independent sets of the matroid $M_{(i)}$ are*

$$\mathcal{I}(M_{(i)}) = \{\sigma \in E \mid n(\sigma) \leqslant i\}.$$

Remark 1.11. It is asserted in the article [6].

Example 1.2.10. Consider the matroid in Example 2.1.1 with bases $\mathcal{B} = \{\{1,2\},\{1,4\},\{2,3\},\{3,4\}\}$. We want to calculate independent sets of $M_{(i)}$, by using the formula: $\mathcal{I}(M_{(i)}) = \{\sigma \in E \mid n(\sigma) \leqslant i\}$.

Computations of nullity function for every $\sigma \in E$ are listed in the table below.

Then for $0 \leqslant i \leqslant 2$, we have

$$\mathcal{I}(M_{(0)}) = \{\sigma \in E \mid n(\sigma) \leqslant 0\} = \{\varnothing, 1, 2, 3, 4, \{1,2\}, \{1,4\}, \{2,3\}, \{3,4\}\}.$$
$$\mathcal{I}(M_{(1)}) = \{\varnothing, 1, 2, 3, 4, \{1,2\}, \{1,4\}, \{2,3\}, \{3,4\}, \{1,3\}, \{2,4\}, \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}\}.$$
$$\mathcal{I}(M_{(2)}) = \{\varnothing, 1, 2, 3, 4, \{1,2\}, \{1,4\}, \{2,3\}, \{3,4\}, \{1,3\}, \{2,4\}, \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \{1,2,3,4\}\}.$$

σ	$r(\sigma)$	$n(\sigma)$
$\{1,2,3,4\}$	2	2
$\{1,2,3\}$	2	1
$\{1,2,4\}$	2	1
$\{1,3,4\}$	2	1
$\{2,3,4\}$	2	1
$\{1,2\}$	2	0
$\{1,3\}$	1	1
$\{1,4\}$	2	0
$\{2,3\}$	2	0
$\{2,4\}$	1	1
$\{3,4\}$	2	0
1	1	0
2	1	0
3	1	0
4	1	0
$\varnothing$	0	0

The matroid $M_{(i)}$ is the elongation of M to rank $r(M)+i$.

The rank function of $M_{(i)}$ for a matroid M with rank function r is denoted by r_i.

In example 1.2.10 we observe

$$r_0(E) = r(E) = 2,$$

$$r_1(E) = r(E) + 1 = 3,$$

$$r_2(E) = r(E) + 2 = 4.$$

For all matroids M we have:

Proposition 1.15. *The rank function r_i of $M_{(i)}$ satisfies:*

$$r_i(X) = Min\{r_M(X) + i, |X|\}.$$

Proof. Follows immediately from Definition 1.28. □

Corollary 1.3. *The rank of $M_{(i)}$ is $r_i(E) = r(E)+i$, for all $0 \leqslant i \leqslant n-r(E)$.*

Definition 1.30. $T(M)$ is called the truncation of a matroid M if for any $X \subseteq E$

$$r_{T(M)}(X) = Min\{r_M(X), r(M) - 1\}.$$

This is well-defined, since $r_{T(M)}$ satisfies the axioms for rank function.

Definition 1.31. For $i = 0, \ldots, r(M)$ define a matroid $M^{(i)}$, which is an i-th truncation

$$M^{(i)} = \underbrace{T(T(\ldots T(M)))}_{i \text{ times}}.$$

Proposition 1.16. *The independent sets of the matroid $M^{(i)}$ are*

$$\mathcal{I}(M^{(i)}) = \{\sigma \in \mathcal{I} \mid |\sigma| \leqslant r(M) - i\}.$$

Proof. Follows immediately from Definition 1.30. □

Definition 1.32. The rank function of $M^{(i)}$ for a matroid M with rank function r is called r^i.

For all matroids M we have:

Proposition 1.17. *The rank function r^i of $M^{(i)}$ satisfies:*

$$r^i(X) = Min\{r_M(X), r(M) - i\}.$$

Proof. Follows from Definition 1.30. □

Corollary 1.4. *The rank of $M^{(i)}$ is $r^i(E) = r - i$, for all $0 \leqslant i \leqslant r(E)$.*

Example 1.2.11 (Continuation of Example 1.2.10). Let us try to find $\mathcal{I}(M^{(1)})$, having applied the following formula:

$$\mathcal{I}(M^{(1)}) = \{\sigma \in E \mid r^1(\sigma) = |\sigma|\},$$

where $r^1(\sigma) = Min\{r(\sigma), r - 1\}$. Then in the case of our example

$$r^1(\sigma) = \begin{cases} 0, & \text{if } \sigma = \varnothing; \\ 1, & \text{if } \sigma \neq \varnothing \end{cases}$$

and

$$\mathcal{I}(M^{(1)}) = \{\varnothing, 1, 2, 3, 4\};$$
$$r^2(\sigma) = 0, \text{ for all } \sigma$$

and

$$\mathcal{I}(M^{(2)}) = \{\varnothing\}.$$

Proposition 1.18. *(a)* $r_{E(M^*)}(X) = r_{[T(M)]^*}(X)$*, where* $X \subseteq E$*;*

(b) $r(M^*_{(i)})(\sigma) = r([M^{(i)}]^*)(\sigma)$*, where* $\sigma \subseteq E$*.*

Proof. For the part (a): Recall the definition of $r^*(X) = |X| + r(E-X) - r(E)$. Consider the right part of our equality

$$\begin{aligned} r^*_{T(M)}(X) &= |X| + r_{T(M)}(E-X) - r_{T(M)}(E) = \\ &= |X| + Min\{r(E-X), r-1\} - Min\{r(E), r-1\} = \\ &= |X| + Min\{r(E-X), r-1\} - (r-1). \end{aligned}$$

If $r(E-X) = r(E)$, then we get $|X| + (r-1) - (r-1) = |X|$.
If $r(E-X) < r(E)$, then we get $|X| + r(E-X) - (r-1)$.
Consider the left part

$$\begin{aligned} r_{E(M^*)}(X) &= Min\{r^*(X)+1, |X|\} = \\ &= Min\{|X| + r(E-X) - r(E) + 1, |X|\}. \end{aligned}$$

If $r(E-X) = r(E)$, then we get $|X|$.
If $r(E-X) < r(E)$, then we get $|X| + r(E-X) - r(E) + 1$. Then we see that the right part is equal to the left one, which is the required result.

The proof for (b) follows in a similar way. □

Example 1.2.12. Let $M = U_{m,n}$ for $1 \leqslant m \leqslant n-1$.
Then

$$E(M) = U_{m+1,n};$$
$$T(M) = U_{m-1,n}$$

Proof. Let us look at rank functions $r_{E(M)}(X)$ and $r_{U_{m+1,n}}(X)$, where $X \subseteq E$.

$$r_{U_{m+1,n}}(X) = \begin{cases} |X|, & \text{if } |X| < m+1; \\ m+1, & \text{if } |X| \geqslant m+1 \end{cases}$$

$$\begin{aligned} r_{E(M)}(X) &= Min\{r_M(X)+1, |X|\} = \\ &= \begin{cases} Min\{|X|+1, |X|\}, & \text{if } |X| < m; \\ Min\{m+1, |X|\}, & \text{if } |X| \geqslant m+1 \end{cases} = \\ &= \begin{cases} |X|, & \text{if } |X| < m; \\ m+1, & \text{if } |X| \geqslant m+1 \end{cases} = r_{U_{m+1,n}}(X). \end{aligned}$$

Similarly it can be shown for a truncation. □

In general:

$$M_{(i)} = U_{m+i,n}, \text{ for } i = 0, 1, \ldots, n-m;$$

$$M^{(i)} = U_{m-i,n}, \text{ for } i = 0, 1, \ldots, m.$$

We will now give an illustration of Proposition 1.18.

Given the matroid $M = U_{2,5}$, then its dual $M^* = U_{3,5}$.
Compute $E(M^*) = E(U_{3,5}) = U_{4,5}$ and $T(M)^* = U_{1,5}^* = U_{4,5}$, it follows that part (a) is fulfilled.
When $i = 2$: $(M^*)_{(2)} = (U_{3,5})_{(2)} = U_{5,5}$ and $(M^{(2)})^* = (U_{0,5})^* = U_{5,5}$, therefore part (b) is also fulfilled.

Chapter 2

Codes and matroids

2.1 From linear codes to matroids

Let $\mathcal{C}$ be a $[n,k]_q$ linear code. G is a generator matrix of $\mathcal{C}$. H is a parity check matrix of $\mathcal{C}$.

Definition 2.1. The matroid associated to the code is

$$M_{\mathcal{C}} = M[H].$$

Remark 2.1. Let $\mathcal{C}$ be a $[n,k]_q$ linear code defined by a parity check matrix H_1. Let H_2 be another parity check matrix of $\mathcal{C}$. Then

$$M[H_1] = M[H_2].$$

The analogous statement is also true for generator matrices.

We have:

$$M_{\mathcal{C}} = M[H] = M[G]^* = (M_{\mathcal{C}^\perp})^*$$

if $G = [I_k \mid A]$ and $H = [-A^t \mid I_{n-k}]$ are of standard form.

Theorem 2.1. *Let $\mathcal{C}$ be a $[n,k]_q$ code. Then $M_{\mathcal{C}}$ is a matroid on $\{1,\ldots,n\}$ of rank $n-k$ and*

$$M_{\mathcal{C}}^* = M_{\mathcal{C}^\perp}.$$

Proof. One has

$$M_{\mathcal{C}} = M[H] = M[G]^* = (M_{\mathcal{C}^\perp})^*.$$

The first and third equalities are just Definition 2.1.
For the equality $M[H] = M[G]^*$, it follows from Theorem 2.2.8 of [12] if G can be taken to be of standard form. A more detailed analysis of column permutations in question gives that this is true also for other G. □

Lemma 2.1. *Let M be a matroid with rank function r and let $i \geqslant 0$. Let us denote*

$$Min\{|X|, X \subset E, |X| - r(X) = i\} = e_i,$$

$$Min\{|X|, X \subset E, |X| - r(X) \geqslant i\} = E_i,$$

Then we have $e_i = E_i$.

Proof. It is easy to see that $E_i \leqslant e_i$. It follows from

$$A \subset B \Rightarrow Min(A) \geqslant Min(B).$$

Let $X \subset E$ such that $|X| - r(X) \geqslant i$ and $|X| = E_i$ with the property $|X| - r(X)$ minimal. We claim that $|X| - r(X) = i$. If not, then let $x \in X$. Let's take $Y = X - \{x\}$.

$$|Y| = |X| - 1 \Rightarrow |Y| - r(Y) < i.$$

We can also say

$$|Y| - r(Y) \leqslant i - 1.$$

From (R_2), we have the following

$$r(Y) = r(X - \{x\}) \leqslant r(X) \leqslant r(Y) + 1.$$

Then

$$|X| - r(X) \leqslant |X| - r(Y) = |Y| + 1 - r(Y) \leqslant i - 1 + 1 = i.$$

Therefore $|X| - r(X) = i \Rightarrow e_i = E_i$. □

Theorem 2.2. *Let $\mathcal{C}$ be a $[n, k]_q$ code and $1 \leqslant i \leqslant k$. Then*

$$d_i = Min\{|X|, X \subset \{1, \ldots, n\} \textit{ such that } |X| - r(X) = i\}$$

where r is the rank function of $M_{\mathcal{C}}$.

Proof. Let $X \subset \{1, \ldots, n\}$ such that $|X| = e_i$ and $|X| - r(X) = i$.
Consider

$$\mathcal{C}(X) = \{c \in \mathcal{C} \text{ such that } c_x = 0 \text{ as soon as } x \notin X \text{ and } c \cdot H^t = [0]\}.$$

Easy to see that it is a subcode of $\mathcal{C}$ and $Supp(\mathcal{C}(X)) \subset X$. We claim that

$$\mathcal{C}(X) \approx KerH[x]^t.$$

This is true, since if

$$w \in \mathcal{C}(X) \subset \mathcal{C} \Rightarrow w \cdot H^t = [0] \Rightarrow w' \cdot H[x]^t = [0],$$

w' being w without zeroes outside X. For the other inclusion

$$u \in KerH[x]^t, u = [u_1, \ldots, u_m] \text{ then } w = [u_1, ..., 0, 0, 0, ..., u_m],$$

$$\text{where zeroes outside } X \text{ and } w \cdot H^t = [0].$$

By the theorem of the dimension

$$\dim(\mathcal{C}(X)) = \dim KerH[x]^t = |X| - \dim ImH[x]^t = |X| - r(X) = i.$$

$$d_i = Min\{|Supp\,\mathcal{D}|, \mathcal{D} \text{ is of dimension } i\} \leqslant |Supp(\mathcal{C}(X)) \leqslant |X| = e_i.$$

Let $\mathcal{D}$ is a subcode of dimension i such that $|Supp\,\mathcal{D}| = d_i$.
Denote $X = Supp(\mathcal{D})$. Consider $\mathcal{C}(X)$.

$$\mathcal{D} \subset \mathcal{C}(X) \subset \mathcal{C}$$

$$Supp\,\mathcal{D} \subset Supp(\mathcal{C}(X)) \subset X$$

Since $Supp(\mathcal{D}) = X$ it follows that $Supp(\mathcal{C}(X)) = X$.

$$\dim(\mathcal{C}(X)) \geqslant \dim \mathcal{D} = i.$$

Recall

$$E_i = Min\{|X|, X \subset \{1, \ldots, n\}, |X| - r(X) \geqslant i\}$$

$$|X| - r(X) \geqslant i.$$

$$E_i \leqslant |X| = |Supp(\mathcal{D})| = d_i.$$

□

Remark 2.2. By Lemma 2.1 we also have

$$d_i = Min\{|X|, X \subset E, |X| - r(X) = i\} = e_i = E_i.$$

Now we can define the Hamming weights of a matroid.

Definition 2.2. Let M be a matroid on $E = \{1, \ldots, n\}$ of rank function r. Let $1 \leqslant i \leqslant |E| - r(E)$. Then the i-th Hamming weight of M is

$$d_i(M) = Min\{|X|, X \subset E, |X| - r(X) = i\}.$$

Example 2.1.1. Given a matroid M with bases $\mathcal{B} = \{\{1,2\},\{1,4\},\{2,3\},\{3,4\}\}$. We want to find Hamming weights

$$d_i = Min\{|X|, n(X) = i\}.$$

The nullity function $n(X) = 0 \Longleftrightarrow r(X) = |X| \Longleftrightarrow X \in \mathcal{I}$.
In our case $n(X) = 0$ for $X = \varnothing, 1, 2, 3, 4, \{1,2\}, \{1,4\}, \{2,3\}, \{3,4\}$. For other ones give the table:

X	$n(X)$
$\{1,3\}$	$2-1=1$
$\{2,4\}$	1
$\{1,2,3\}$	$3-2=1$
$\{1,2,4\}$	1
$\{1,3,4\}$	1
$\{2,3,4\}$	1
$\{1,2,3,4\}$	$4-2=2$

Then the Hamming weights of M are

$$d_1 = Min\{|X|, n(X) = 1\} = 2,$$

$$d_2 = Min\{|X|, n(X) = 2\} = 4.$$

Proposition 2.1. *Let M be a matroid. Then $d_1 < d_2 < \ldots < d_{n-r}$.*

Remark 2.3. This result is proved in [14].

Definition 2.3. Let M be a matroid on E. Let $n = |E|$. Then the weight hierarchy of M is $d_1 < \ldots < d_{n-r}$ where $r = r(M)$.

Theorem 2.3 (Wei's duality). *Let M be a matroid on E of rank r and $n = |E|$. Let*

$$d_1 < \ldots < d_{n-r}$$

be the weight hierarchy of M.
Let M^* is a matroid on E of rank $n - r$. Let

$$e_1 < \ldots < e_r$$

be the weight hierarchy of the dual matroid M^*. Then

$$\{d_1, \ldots, d_{n-r}\} \cup \{n+1-e_1, \ldots, n+1-e_r\} = \{1, \ldots, n\}$$

and the union is disjoint.

Proof. This theorem was proved in [10]. □

Definition 2.4. Let M be a matroid on $E = \{1, \ldots, n\}$ of rank function r. Then the minimum distance of the matroid M

$$d = d_1(M) = Min\{|X|, X \subset E, |X| - r(X) = 1\}.$$

Remark 2.4. Note that $d_1(M[H])$ is equal to the minimum distance of $\mathcal{C}$ if H is a parity check matrix for a linear code $\mathcal{C}$.
One may also observe that the minimum distance of the code equals to the size of the smallest circuit in the matroid represented by the parity check matrix.

Proposition 2.2. *Let $\mathcal{C}$ be a $[n, k]$ code with weight hierarchy*

$$d_1(\mathcal{C}), \ldots, d_k(\mathcal{C})$$

where $k = dim(\mathcal{C})$.
Let $M_{\mathcal{C}}$ be a matroid associated to the code $\mathcal{C}$ with its weight hierarchy

$$d_1(M_{\mathcal{C}}), \ldots, d_k(M_{\mathcal{C}}).$$

Then

$$d_1(\mathcal{C}) = d_1(M_{\mathcal{C}}), \ldots, d_k(\mathcal{C}) = d_k(M_{\mathcal{C}}).$$

Proof. Look at the Theorem 2.2 and Definition 2.2. We see that the Hamming weights of a code and the Hamming weights of a matroid associated to the code are expressed in the same way. □

Example 2.1.2. Let us study the code $\mathcal{C}$ with generator matrix G over $\mathbb{F}_2$.

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} = \left[\begin{array}{c|c} I_2 & A \end{array} \right], \text{ where } A = I_2.$$

Then H can be taken to be

$$H = \left[\begin{array}{c|c} -A^t & I_2 \end{array} \right] = \left[\begin{array}{c|c} I_2 & I_2 \end{array} \right] = G \text{ also.}$$

Then by looking at independent columns of the parity check matrix H, the matroid associated to the code $\mathcal{C}$ is

$$M_{\mathcal{C}} = \{12, 14, 23, 34\}.$$

We compute the Hamming weights of the code

$$d_1 = Min\{wt(1010, 0101, 1111)\} = Min\{2, 2, 4\} = 2,$$

$$d_2 = Min\{|Supp(\mathcal{D})|, \mathcal{D} \text{ is a subcode of dimension } 2\} = \{|Supp(\mathcal{C})|\} = 4.$$

We see that they are the same as in Example 2.1.1.

The next example shows how non-representable matroids do not come from codes. First we mention the following definition:

Definition 2.5. Let M_1, M_2 be matroids on E_1 and E_2 respectively and $E_1 \cap E_2 = \varnothing$.
Let

$$\mathcal{I} = \{I_1 \cup I_2 \mid I_1 \in \mathcal{I}_{M_1}, I_2 \in \mathcal{I}_{M_2}\}.$$

The sum of two matroids M_1 and M_2 is the matroid

$$M_1 \oplus M_2 = (E_1 \cup E_2, \mathcal{I}).$$

Example 2.1.3. Let $E = \{1, \ldots, 7\}$. Then for the bases of the Fano matroid F_7 (See Figure 2.1) we have

$$\mathcal{B}_{F_7} = \{\text{subsets of cardinality 3 except}$$

$$\{2,4,6\}, \{4,5,7\}, \{5,6,7\}, \{1,4,5\}, \{3,5,6\}, \{1,2,5\}, \{2,3,5\}\}.$$

Let us define another matroid with the exception that the circle in the below diagram is missing. It is called the anti-Fano matroid F_7^- (See Figure 2.2) and for the bases of F_7^- we have

$$\mathcal{B}_{F_7^-} = \{\text{subsets of cardinality 3 except}$$

$\{11,12,14\},\{12,13,14\},\{8,11,12\},\{10,12,13\},\{8,9,12\},\{9,10,12\}\}.$

F_7 is representable over a field $\mathbb{K}$ if and only if $char(\mathbb{K}) = 2$,

F_7^- is representable over a field $\mathbb{K}$ if and only if $char(\mathbb{K}) \neq 2$. But the direct sum of a Fano matroid and an anti-Fano matroid is an example for a matroid which is not representable over any field.

$$M = F_7 \oplus F_7^-$$

is not a matroid of the form $M_{\mathcal{C}}$ for any linear code $\mathcal{C}$ over any $\mathbb{F}_q$, since $M = M[H]$ would force M to be representable over $\mathbb{F}_q$.

The set of bases of M on $\{1,2,\ldots,14\}$ is

$$\mathcal{B} = \{B_1 \cup B_2\},$$

where B_1 could be any subset of cardinality 3 of $\{1,2,\ldots,7\}$ among those drawn on Figure 2.1, and B_2 could be any subset of cardinality 3 of $\{8,9,\ldots,14\}$ among those drawn on Figure 2.2. The rank of M is 6 and we know that $n = 14$. Then we could compute

$$d_1, d_2, \ldots, d_{14-6} = d_8.$$

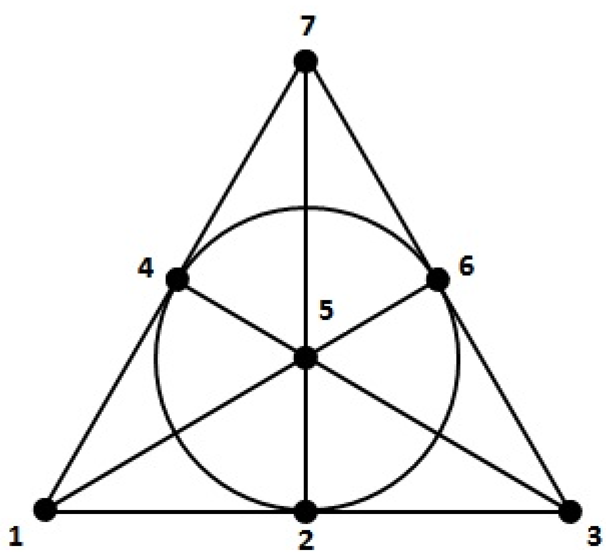

Figure 2.1: Fano matroid

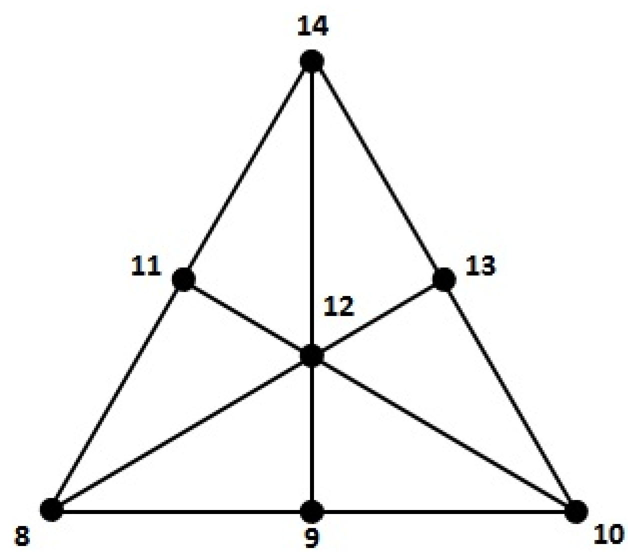

Figure 2.2: Anti-Fano matroid

We are going to calculate only d_1 and d_2.

Take $X = \{9, 11\}$. We see that $|X| = 2$ and $r(X) = 1$. Therefore

$$d_1(M) = Min\{|X|, X \subset E, |X| - r(X) = 1\} = 2.$$

$d_2 = 3$ since $|X| - r(X) = 3 - 1 = 2$ if $X = \{9, 11, 13\}$ (and $d_2 > d_1$).

Remark 2.5. In this case d_1 has no interpretation as a minimum distance of a code.

Chapter 3

Stanley-Reisner rings and Betti numbers

3.1 Simplicial complexes

Let E be a finite set, for simplicity we may take $E = \{1, 2, ..., n\}$.

Definition 3.1. A simplicial complex on E is a $\Delta \subset 2^E$ such that if $\sigma_1 \in \Delta$ and $\sigma_2 \subset \sigma_1$, then $\sigma_2 \in \Delta$.

Definition 3.2. A simplex is a subset of E (or an element of 2^E).

Definition 3.3. A face of Δ is $\sigma \in \Delta$.
A facet of Δ is a maximal face (for inclusion).
$\mathcal{N}(\Delta)$ is the set of minimal non-faces (for inclusion).

Remark 3.1. A simplicial complex is entirely given by its set of facets.

Let $\mathbb{K}$ be a field. Denote $S = \mathbb{K}[x_1, \ldots, x_n]$ be the polynomial ring in n variables over $\mathbb{K}$. Let $I \subset S$ is an ideal.

Definition 3.4. A monomial is a polynomial of the form

$$\underline{x}^{\underline{a}} = \prod_{i=1}^{n} x_i^{a_i},$$

where $a_i \geq 0$.

Remark 3.2. The product of two such monomials is a monomial

$$\underline{x}^{\underline{a}} \cdot \underline{x}^{\underline{b}} = \underline{x}^{\underline{a+b}}.$$

Definition 3.5. A monomial ideal I of S is an ideal generated by monomials.

Definition 3.6. A monomial $\underline{x}^{\underline{a}} = x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ is squarefree if each a_i is 0 or 1.

Definition 3.7. A monomial ideal is squarefree if it is generated by square free monomials.

Definition 3.8. If $\sigma = \{i_1, i_2, ..., i_r\} \subset E$, then

$$x^\sigma = \prod x_{i_1} x_{i_2} ... x_{i_r}.$$

Clearly x^σ is squarefree, and any squarefree monomial can be written as x^σ, for some $\sigma \subset E$.

Definition 3.9. Let Δ be a simplicial complex on E. The Stanley-Reisner ideal of Δ is the squarefree monomial ideal

$$I_\Delta = < x^\sigma, \sigma \in \mathcal{N}(\Delta) > = < x^\sigma, \sigma \notin \Delta > .$$

Definition 3.10. The Stanley-Reisner ring of a simplicial complex is

$$R_\Delta = S/I_\Delta.$$

Proposition 3.1. *Let M be a matroid, and $\mathcal{I}(M)$=$\{$independent sets of $M\}$. Then $\mathcal{I}(M) \subset 2^E$ is a simplicial complex.*

Proof. Let M be a matroid on a finite set E with $\mathcal{I}(M) \subset 2^E$. Then it satisfies the properties (I_1), (I_2), (I_3). From this we can get the following:

$$\text{if } I_1 \in \mathcal{I}(M) \text{ and } I_2 \subset I_1, \text{ then } I_2 \in \mathcal{I}(M),$$

that are exactly the property for simplicial complexes. □

Proposition 3.2. *The Stanley-Reisner ring/ideal of a matroid M will be the Stanley-Reisner ring/ideal of the simplicial complex $\Delta = \mathcal{I}(M)$.*

3.2 Gradings

Definition 3.11. A ring R is a $\mathbb{Z}$-graded ring if it can be written

$$R = \bigoplus_{i \in \mathbb{Z}} R_i,$$

and $R_i \cdot R_j \subset R_{i+j}$ for all $i, j \in \mathbb{Z}$.

Definition 3.12. A homogeneous polynomial is a polynomial whose nonzero monomials all have the same degree.

In particular, $S = \mathbb{K}[x_1, \ldots, x_n]$ has a $\mathbb{Z}$-grading in the following way

$$S_i = 0 \text{ if } i < 0,$$

$$S_0 = \mathbb{K} \subset S,$$

$$S_i = \{\text{homogeneous polynomials of degree } i\} \text{ for } i > 0.$$

Definition 3.13. A finitely generated module M over S is called $\mathbb{Z}$-graded if

$$M = \bigoplus_{i \in \mathbb{Z}} M_i,$$

and $S_i \cdot M_j \subset M_{i+j}$ for all $i, j \in \mathbb{Z}$.

Definition 3.14. An S-module M is called $\mathbb{Z}^n$-graded if

$$M = \bigoplus_{\underline{a} \in \mathbb{Z}^n} M_{\underline{a}},$$

and $S_{\underline{a}} \cdot M_{\underline{b}} \subset M_{\underline{a}+\underline{b}}$ for all $\underline{a}, \underline{b} \in \mathbb{Z}^n$.

Moreover, S has a $\mathbb{Z}^n$-grading

$$S = \bigoplus_{\underline{a} \in \mathbb{Z}^n_+} S_{\underline{a}},$$

where

$$S_{\underline{a}} = \begin{cases} 0, & \text{if } \underline{a} \notin \mathbb{Z}^n_+, \\ \mathbb{K}x^{\underline{a}}, & \text{if } \underline{a} \in \mathbb{Z}^n_+. \end{cases}$$

Observation. *Let $I \subset S$ be an ideal. Then*

(i) I is a $\mathbb{Z}$-graded submodule of S if and only if I can be generated by homogeneous polynomials. In this case S/I is also $\mathbb{Z}$-graded.

(ii) I is a $\mathbb{Z}^n$-graded submodule of S if and only if I can be generated by monomials. In this case S/I is also $\mathbb{Z}^n$-graded.

Proof. For (i), see p. 6 in [4]. Part (ii) follows in a similar way. □

3.3 Graded free resolutions

Let M and N be finitely generated $\mathbb{Z}$-graded S-modules.

Definition 3.15. A $\mathbb{Z}$-graded S-module homomorphism from M to N is an S-module homomorphism $\phi\colon M \to N$, where $\phi(M_i) \subset N_i$ for all $i \in \mathbb{Z}$. Likewise a $\mathbb{Z}^n$-graded S-module homomorphism of two $\mathbb{Z}^n$-graded S-modules M and N is an S-module homomorphism $\phi\colon M \to N$, such that $\phi(M_{\underline{a}}) \subset N_{\underline{a}}$ for all $\underline{a} \in \mathbb{Z}^n$.

Let R be a ring.

Definition 3.16. An exact sequence of R-modules is a sequence of R-modules and R-module homomorphisms

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\phi_i} M_i \xrightarrow{\phi_{i-1}} M_{i-1} \longrightarrow \cdots ,$$

where $Ker(\phi_{i-1}) = Im(\phi_i)$ for all i.

Remark 3.3. An exact sequence of $\mathbb{Z}$-graded S-modules is an exact sequence of S-modules where each homomorphism ϕ_i is $\mathbb{Z}$-graded.

Definition 3.17. The $\mathbb{Z}$-graded S-module $S(d)$ is defined as

$$S(d)_r = S_{d+r},$$

for all $d, r \in \mathbb{Z}$. It is called a shift of S by d.

Definition 3.18. A long exact sequence

$$\mathbb{F} : \cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

of $\mathbb{Z}$-graded S-modules with $F_i = \bigoplus_j S(-j)^{\beta_{ij}}$ is called a $\mathbb{Z}$-graded free S-resolution of M.

Let M be a finitely generated $\mathbb{Z}$-graded S-module.

Definition 3.19. A $\mathbb{Z}$-graded free S-resolution $\mathbb{F}$ of M is called minimal if for all i, the image of $F_{i+1} \longrightarrow F_i$ is contained in $\mathfrak{m}F_i$, where $\mathfrak{m} =< x_1, \ldots, x_n >$ is a graded maximal ideal.

Proposition 3.3. *Let M be a finitely generated $\mathbb{Z}$-graded S-module and*

$$\mathbb{F} : \cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

a minimal $\mathbb{Z}$-graded free S-resolution of M with $F_i = \bigoplus_j S(-j)^{\beta_{ij}}$ for all i. Then

$$\beta_{ij} = \dim_{\mathbb{K}} Tor_i^S(\mathbb{K}, M)_j$$

for all i and j.

Remark 3.4. The proof can be found in [4], and the definition of the functor $Tor_i^S(\mathbb{K}, M)_j$ in [1, p.159-160].

Definition 3.20. The numbers β_{ij} are called the $\mathbb{Z}$-graded Betti numbers of M.

Remark 3.5. As one sees from this formula, two different minimal $\mathbb{Z}$-graded free S-resolutions of M will give the same Betti numbers.

In the sequence of Proposition 3.3 we may also forget about the grading, and just look at it as an exact sequence of S-modules.
Since $S(-j) \simeq S$ for all j as S-modules, we may view F_i as

$$\bigoplus_j S^{\beta_{ij}} \cong S^{\sum_j \beta_{ij}}.$$

We set

$$\beta_i = \sum_j \beta_{ij}.$$

Then the minimal free resolution becomes

$$\mathbb{F} : \cdots \longrightarrow S^{\beta_2} \longrightarrow S^{\beta_1} \longrightarrow S^{\beta_0} \longrightarrow M \longrightarrow 0$$

The β_i are called the ungraded Betti numbers. These numbers are also consequently the same for all minimal free resolutions.

Definition 3.21. A minimal free resolution

$$0 \longrightarrow F_l \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

with $\mathbb{Z}^n$-graded modules

$$F_i = \bigoplus_{\underline{a} \in \mathbb{Z}^n} S(-\underline{a})^{\beta_{i,\underline{a}}}$$

is called a minimal $\mathbb{Z}^n$-graded free S-resolution of M.

Proposition 3.4. *The $\beta_{i,\underline{a}}$ are independent on the minimal free resolution of M.*

Remark 3.6. By [4], p.126, $\beta_{i,\underline{a}} = \dim_{\mathbb{K}} Tor_i^S(\mathbb{K}, M)_{\underline{a}}$, for all such minimal $\mathbb{Z}^n$-graded resolutions.

Definition 3.22. The $\beta_{i,\underline{a}}$ are called the $\mathbb{Z}^n$-graded Betti numbers of M over the field $\mathbb{K}$.

3.4 Betti numbers of Stanley-Reisner rings

In the next chapter we will look in particular at resolutions of S-modules of the type

$$R_\Delta = S/I_\Delta,$$

in other words Stanley-Reisner rings.

Let Δ be a simplicial complex as in Section 3.1.

Definition 3.23. The ungraded, $\mathbb{Z}$-graded, $\mathbb{Z}^n$-graded Betti numbers of Δ will be the ungraded, $\mathbb{Z}$-graded, $\mathbb{Z}^n$-graded Betti numbers of the module $M = R_\Delta$.

Remark 3.7. Whenever we have a matroid M, we may therefore study the $\mathbb{Z}$-graded resolution of the simplicial complex Δ, where faces are sets in $\mathcal{I}(M)$. In particular if we have a linear code $\mathcal{C}$, we can obtain the matroid associated to this code and also study the $\mathbb{Z}$-graded resolution of the simplicial complex.

Example 3.4.1. Start with the binary code $\mathcal{C}$ with parity check matrix

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

Hence $\mathcal{C}^{\perp}$ has generator matrix H and therefore following parity check matrix

$$\left[\ -A^t \mid I_2\ \right] = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \text{ over } \mathbb{F}_2.$$

Then this is a generator matrix G for $\mathcal{C}$ and we have

$$\mathcal{C} = \{0000, 1110, 1001, 0111\}.$$

The minimum distance of the code $\mathcal{C}$

$$d(\mathcal{C}) = Min\{wt(x), x \neq (0\ldots0)\} = Min\{3,2,3\} = 2.$$

The bases of

$$M_{\mathcal{C}} = M[H] = \{\{1,2\},\{1,3\},\{2,3\},\{2,4\},\{3,4\}\}.$$

The circuits are $\{\{1,4\},\{1,2,3\},\{2,3,4\}\}$. The Stanley-Reisner ideal is

$$I_\Delta = < x_1x_4, x_1x_2x_3, x_2x_3x_4 > .$$

A resolution of $R_\Delta = S/I_\Delta$ "ends" like this:

$$\cdots \longrightarrow S^3 = S \oplus S \oplus S \xrightarrow{\phi_2} S \xrightarrow{\phi_1} R_\Delta(= S/I_\Delta) \longrightarrow 0 \qquad (3.1)$$

In order to get $Im(\phi_2) = Ker(\phi_1) = I_\Delta$, we use

$$\phi_2 \colon (s_1, s_2, s_3) \to (s_1x_1x_4 + s_2x_1x_2x_3 + s_3x_2x_3x_4).$$

This works well for ungraded resolutions, but for $\mathbb{Z}$-graded modules we get $\phi_2((S^3)_i) \nsubseteq S_i$.
Describe $(S^3)_i = (S^{(1)} \oplus S^{(2)} \oplus S^{(3)})_i$. For all i we have

$$(S^3)_i = S_i^{(1)} \oplus S_i^{(2)} \oplus S_i^{(3)}.$$

But: If we think of $e_1 = (1,0,0), e_2 = (0,1,0), e_3 = (0,0,1)$ as members of $S(-2), S(-3), S(-3)$ respectively, then they are graded of degrees $2,3,3$ respectively, and we see that $\phi_2(e_1)$ has degree 2, $\phi_2(e_2)$ has degree 3, $\phi_2(e_3)$ has degree 3. This implies that $\phi_2(h)$ has degree d_h for any homogeneous element h of $S(-2) \oplus S(-3) \oplus S(-3)$ of degree d_h.
Hence the resolution "ends" with

$$\cdots \longrightarrow S(-2) \oplus S(-3) \oplus S(-3) \xrightarrow{\phi_2} S \xrightarrow{\phi_1} R_\Delta \longrightarrow 0 \qquad (3.2)$$

as a $\mathbb{Z}$-graded resolution. Hence $\beta_{1,2} = 1, \beta_{1,3} = 2$ and $\beta_{1,j} = 0$, for all $j \neq 2, 3$.
In a similar way as a $\mathbb{Z}^n$-graded resolution it is

$$\cdots \longrightarrow S(-(1,0,0,1)) \oplus S(-(1,1,1,0)) \oplus S(-(0,1,1,1)) \xrightarrow{\phi_2} S \xrightarrow{\phi_1} R_\Delta \longrightarrow 0 \tag{3.3}$$

Hence $\beta_{1,(-1,0,0,-1)} = \beta_{1,(-1,-1,-1,0)} = \beta_{1,(0,-1,-1,-1)} = 1$ and $\beta_{1,\underline{a}} = 0$, for all other $\underline{a}$.

Let us study how we can find $d(\mathcal{C})$ from the resolutions 3.2 and/or 3.3.

First: By Theorem 8.4 in [5] $d(\mathcal{C})$ is a "size" of the smallest relation between two columns of H.

Then it is also the smallest cardinality of the circuits of $M_{\mathcal{C}} = M[H]$.

Then it is also the smallest absolute value of any shift in F_1.

Then it is $Min\{j \mid \beta_{1,j} \neq 0\}$. Since $\beta_{1,2} = 1, \beta_{1,3} = 2$ and $\beta_{1,j} = 0$, for all other j, we conclude that $Min\{j \mid \beta_{1,j} \neq 0\}$ is 2.
It turns out that the resolution in 3.1 can be completed

$$0 \longrightarrow S^2 \xrightarrow{\phi_3} S^3 \xrightarrow{\phi_2} S \xrightarrow{\phi_1} R_\Delta \longrightarrow 0$$

$$(N_1, N_2) = N_1(1,0) + N_2(0,1) \longrightarrow (x_2x_3N_1, -x_4N_1, 0) + (x_2x_3N_2, 0, -x_1N_2).$$

$$\phi_3(N_1, N_2) = \phi_3(N_1(1,0) + N_2(0,1)) = N_1\phi_3(1,0) + N_2\phi_3(0,1) =$$
$$= (x_2x_3(N_1 + N_2), -x_4N_1, -x_1N_2).$$

This becomes a $\mathbb{Z}$-graded S-module homomorphism if we write it

$$0 \longrightarrow S(-4)^2 \xrightarrow{\phi_3} S(-2) \oplus S(-3)^2 \xrightarrow{\phi_2} S \xrightarrow{\phi_1} R_\Delta \longrightarrow 0$$

To show that this is an exact sequence, one must verify that: $\phi_2 \circ \phi_3 = 0$, which is the same as $Im(\phi_3) \subseteq Ker(\phi_2)$, and in addition that $Ker(\phi_2) \subseteq Im(\phi_3)$, and also ϕ_3 is injective.
First we prove: $\phi_2 \circ \phi_3 = 0$.

$$(1,0) \xrightarrow{\phi_3} (x_2x_3, -x_4, 0)$$

$$(0,1) \xrightarrow{\phi_3} (x_2x_3, 0, -x_1)$$

Remember that

$$(s_1, s_2, s_3) \xrightarrow{\phi_2} (s_1x_1x_4 + s_2x_1x_2x_3 + s_3x_2x_3x_4).$$

We then see the following

$$\phi_2(\phi_3(1,0)) = \phi_2(x_2x_3, -x_4, 0) = x_1x_4x_2x_3 + (-x_4)x_1x_2x_3 + 0 = 0,$$

$$\phi_2(\phi_3(0,1)) = \phi_2(x_2x_3, 0, -x_1) = x_1x_4x_2x_3 + 0 + (-x_1)x_2x_3x_4 = 0.$$

Hence $\phi_2 \circ \phi_3 = 0$, so $Im(\phi_3) \subseteq Ker(\phi_2)$. It is easy to check that ϕ_3 is injective. To show $Ker(\phi_2) \subseteq Im(\phi_3)$ (so that $Ker(\phi_2) = Im(\phi_3)$) is more difficult, and we omit the proof here.

A $\mathbb{Z}^n$-graded resolution becomes

$$0 \longrightarrow S(-(1,1,1,1))^2 \xrightarrow{\phi_3} S(-(1,0,0,1)) \oplus S(-(1,1,1,0)) \oplus S(-(0,1,1,1)) \xrightarrow{\phi_2} S \xrightarrow{\phi_1} R_\Delta \longrightarrow 0$$

In the last example $\beta_{i,\underline{a}} = 0$, unless $\underline{a}$ has coordinates 0 and 1. This turns out to be a general fact for all Stanley-Reisner rings of simplicial complexes.

Proposition 3.5. *For all i the $\mathbb{Z}^n$-graded Betti numbers of a Stanley-Reisner ring satisfy*

$$\beta_{i,\underline{a}} = 0,$$

unless $\underline{a}$ is of the type $(a_1, a_2, \ldots, a_n)$, where $a_r = 0$ or 1, for all r.

Definition 3.24. Let $\underline{a} = (a_1, a_2, \ldots, a_n)$, where $a_r = 0$ or 1, for all r. Then we let $\sigma_{\underline{a}}$ be the simplex $\{i_1, i_2, \ldots, i_s\}$, where we let the i_t be precisely the r such that $a_r = 1$.

Example 3.4.2. $\underline{a} = (-1, 0, 0, -1)$. Then $\sigma_{\underline{a}} = \{1, 4\}$.

Definition 3.25. For all Stanley-Reisner rings R_Δ, we denote $\beta_{i,\underline{a}}$ by $\beta_{i,\sigma}$, if $\sigma = \sigma_{\underline{a}}$.

Theorem 3.1. *Let M be a matroid, and R_Δ be the Stanley-Reisner ring of a simplicial complex. Then*

$$d_1(M) = Min\{j \mid \beta_{1,j} \neq 0\}.$$

Remark 3.8. This result is a special case of Theorem 3.2 below, and follows from that. But it also possible to obtain this result by generalizing from the observations done in the work with Example 3.4.1.
We recall:

$d(\mathcal{C})$ is a "size" of the smallest relation between two columns of H.
Then it is also the smallest cardinality of the circuits of $M_{\mathcal{C}} = M[H]$.
Then it is also the smallest absolute value of any shift in F_1.
Then it is $Min\{j \mid \beta_{1,j} \neq 0\}$.

In fact it is possible to generalize this:

Theorem 3.2. *For all $i = 1, \ldots, n-r$ we have*

$$d_i(M) = Min\{j \mid \beta_{i,j} \neq 0\}.$$

Remark 3.9. The proof of this theorem can be found in the article [7], where this result is Theorem 2 in that article.
In order for this result to have meaning there have to exist non-zero $\beta_{i,j}$ for $i = 1, 2, \ldots, n-r$. Hence there have to exist non-zero F_i for $i = 1, \ldots, n-r$. This leads to the following:

Definition 3.26. The length of the resolution

$$0 \longrightarrow F_l \longrightarrow \cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

is l if $F_0, F_1, F_2, \ldots, F_l$ all are non-zero.

Theorem 3.3 (Hilbert Syzygy Theorem)**.** *The length of a free resolution for simplicial complexes is at most n.*

Remark 3.10. See [11], p.11.

Proposition 3.6. *A matroid has a resolution with length $n - r$.*

Remark 3.11. This result is given as Corollary 3(b) in [7]. We observe that this length is precisely long enough to be able to apply the formula in Theorem 3.2.

There are two ways to prove these results. One way is to utilize the so called Auslander-Buchsbaum formula and the fact that $R_\Delta = S/I_\Delta$ is a Cohen-Macaulay ring, where Δ is the simplicial complex derived from a matroid.
Another way to prove it is to use the following result, given in [7]:

Proposition 3.7. $\beta_{i,\sigma} \neq 0 \Longleftrightarrow \sigma$ *is minimal in $n^{-1}(i)$, where $n\colon 2^E \longrightarrow \mathbb{Z}_+$ is the nullity function $\#E - r$.*

Remark 3.12. Since the image of the nullity function is $\{0, 1, \ldots, n-r\}$ we get non-zero $\beta_{i,j}$ for $0, 1, \ldots, n-r$.

Chapter 4

Generalized weight polynomials

4.1 Weight polynomials in terms of Betti numbers

Let $\mathcal{C}$ be a $[n,k]_q$-code (over $\mathbb{F}_q$). Let $\mathbb{F}_q \subseteq \mathbb{F}_Q$. That is only possible if $Q = q^m$, for some m.

Example 4.1.1. $\mathbb{F}_9 \subseteq \mathbb{F}_{9^3} = \mathbb{F}_{729}$.

Let

$$G = \begin{bmatrix} \underline{r}_1 \\ \underline{r}_2 \\ \vdots \\ \underline{r}_k \end{bmatrix}$$

be a generator matrix of $\mathcal{C}$ (with entries in $\mathbb{F}_q$).
What is $\mathcal{C} \otimes_{\mathbb{F}_q} \mathbb{F}_Q$?

$$\mathcal{C} \subseteq (\mathbb{F}_q)^n; \mathcal{C} = \text{ row space of } G \text{ in } (\mathbb{F}_q)^n \ .$$

$$\mathcal{C} \subseteq (\mathbb{F}_q)^n \subseteq (\mathbb{F}_Q)^n.$$

All the $\underline{r}_i$ are also vectors in $(\mathbb{F}_Q)^n$.
$\mathcal{C} \otimes_{\mathbb{F}_q} \mathbb{F}_Q$ is the row space of G, span $(\underline{r}_1, \ldots, \underline{r}_k)$ inside $(\mathbb{F}_Q)^n$.

We observe: $|\mathcal{C}| = q^k$, $|\mathcal{C} \otimes_{\mathbb{F}_q} \mathbb{F}_Q| = Q^k = (q^m)^k = q^{mk}$.

Let H be a parity check matrix for $\mathcal{C}$. H is an $(n-k) \times n$ matrix.
H will also be a parity check matrix for $\mathcal{C} \otimes_{\mathbb{F}_q} \mathbb{F}_Q$.

Let us denote $\mathcal{C} \otimes_{\mathbb{F}_q} \mathbb{F}_Q$ as $\mathcal{C}_Q$.
Then we have

$$\mathcal{C}_Q = (\text{ Row space of } H \text{ in } \mathbb{F}_Q^n\ )^{\perp}$$

and

$$\mathcal{C}_Q^{\perp} = (\text{ Row space of } H \text{ in } \mathbb{F}_Q^n\ ).$$

For any fixed (linear) code $\mathcal{C} \subseteq \mathbb{F}_q^n$ we can look at $n+1$ numbers

$$a_{\mathcal{C},0}, a_{\mathcal{C},1}, \ldots, a_{\mathcal{C},n},$$

where $a_{\mathcal{C},j}$ = the number of codewords of weight j.

For any $m \geqslant 1$, and $0 \leqslant j \leqslant n$, let

$$a_{\mathcal{C},j}^{(m)} = \text{ number of codewords of weight } j \text{ in } \mathcal{C}_Q, \text{ for } Q = q^m.$$

Proposition 4.1. *There exists a polynomial $P_{M,j}(Z) \in \mathbb{Z}[Z]$ with $\deg P_{M,j} \leqslant k$ such that $a_{\mathcal{C},j}^{(m)} = P_{M,j}(q^m)\ \ \forall m$.*

Proof. See [9]. □

These polynomials can be found from the properties of the matroid $M_{\mathcal{C}} = M[H]$. They are given in [6] as Proposition 3.1.

The formula is:

$$P_{M,j}(Z) = (-1)^j \sum_{|\sigma|=j} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)} \text{ for } 1 \leqslant j \leqslant n.$$

Example 4.1.2. Look at the example 3.4.1.
Given the binary code $\mathcal{C} = \{0000, 1110, 1001, 0111\}$ with parity check matrix

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

and generator matrix

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

From our code $\mathcal{C}$ we can obtain the matroid $M_{\mathcal{C}} = M[H]$ on the ground set $E = \{1, 2, 3, 4\}$.
Compute the nullity function for every $\gamma \in E$. Results are represented in table:

γ	$\lvert\gamma\rvert$	$r(\gamma)$	$n(\gamma)$
$\varnothing$	0	0	0
1	1	1	0
2	1	1	0
3	1	1	0
4	1	1	0
$\{1,2\}$	2	2	0
$\{1,3\}$	2	2	0
$\{1,4\}$	2	1	1
$\{2,3\}$	2	2	0
$\{2,4\}$	2	2	0
$\{3,4\}$	2	2	0
$\{1,2,3\}$	3	2	1
$\{1,2,4\}$	3	2	1
$\{1,3,4\}$	3	2	1
$\{2,3,4\}$	3	2	1
$\{1,2,3,4\}$	4	2	2

Using the following formula

$$P_j(Z) = (-1)^j \sum_{|\sigma|=j} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)} \text{ for } 0 \leqslant j \leqslant n,$$

find polynomials $P_j(Z)$ for $0 \leqslant j \leqslant 4$.

$$P_0(Z) = (-1)^0 \sum_{|\sigma|=0} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)}.$$

$\sigma = \varnothing$ gives $\gamma = \varnothing$. Then

$$P_0(Z) = (-1)^0 \cdot (-1)^0 \cdot Z^0 = 1.$$

Thus there is only one codeword of weight 0 in $\mathcal{C}_Q$.

$$P_1(Z) = (-1) \sum_{|\sigma|=1} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)}.$$

$\sigma = \{1\}$ gives $\gamma = \varnothing$, $\gamma = \{1\}$;
$\sigma = \{2\}$ gives $\gamma = \varnothing$, $\gamma = \{2\}$;

$\sigma = \{3\}$ gives $\gamma = \varnothing$, $\gamma = \{3\}$;
$\sigma = \{4\}$ gives $\gamma = \varnothing$, $\gamma = \{4\}$.

$$P_1(Z) = (-1)\left[4 \cdot ((-1)^0 Z^0 + (-1)^1 Z^0)\right] = 0,$$

hence in $\mathcal{C}_Q$ there are no codewords of weight 1.

$$P_2(Z) = (-1)^2 \sum_{|\sigma|=2} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)}.$$

$\sigma = \{1,2\}$ gives $\gamma = \varnothing$, $\gamma = \{1\}$, $\gamma = \{2\}$, $\gamma = \{1,2\}$;
$\sigma = \{1,3\}$ gives $\gamma = \varnothing$, $\gamma = \{1\}$, $\gamma = \{3\}$, $\gamma = \{1,3\}$;
$\vdots$
$\sigma = \{3,4\}$ gives $\gamma = \varnothing$, $\gamma = \{3\}$, $\gamma = \{4\}$, $\gamma = \{3,4\}$.

$$\begin{gathered} P_2(Z) = 5 \cdot \left((-1)^0 Z^0 + 2 \cdot (-1) Z^0 + (-1)^2 Z^0\right) + \\ +((-1)^0 Z^0 + 2 \cdot (-1) Z^0 + (-1)^2 Z^1)) = Z - 1. \end{gathered}$$

We observe, for example: in $\mathcal{C} = \mathcal{C}_2$ we have $P_2(Q) = P_2(2) = 2 - 1 = 1$ codeword of weight 2.
In $\mathcal{C}_4 = \mathcal{C}_{2^2}$ we have $P_2(Q) = P_2(4) = 4 - 1 = 3$ codewords of weight 2.

$$P_3(Z) = (-1)^3 \sum_{|\sigma|=3} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)}$$

$\sigma = \{1,2,3\}$ gives $\gamma = \varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}$;
$\sigma = \{1,2,4\}$ gives $\gamma = \varnothing, \{1\}, \{2\}, \{4\}, \{1,2\}, \{1,4\}, \{2,4\}, \{1,2,4\}$;
$\sigma = \{1,3,4\}$ gives $\gamma = \varnothing, \{1\}, \{3\}, \{4\}, \{1,3\}, \{1,4\}, \{3,4\}, \{1,3,4\}$;
$\sigma = \{2,3,4\}$ gives $\gamma = \varnothing, \{2\}, \{3\}, \{4\}, \{2,3\}, \{2,4\}, \{3,4\}, \{2,3,4\}$.

$$\begin{gathered} P_3(Z) = -\Big(2 \cdot [(-1)^0 Z^0 + 3 \cdot (-1)^1 Z^0 + 3 \cdot (-1)^2 Z^0 + (-1)^3 Z^1] + \\ +2 \cdot [(-1)^0 Z^0 + 3 \cdot (-1)^1 Z^0 + 2 \cdot (-1)^2 Z^0 + (-1)^2 Z^1 + (-1)^3 Z^1]\Big) = \\ = -(2 - 2Z) = 2Z - 2. \end{gathered}$$

As above, we observe that in $\mathcal{C}_2$ we have $P_3(Q) = P_3(2) = 2 \cdot 2 - 2 = 2$ codewords of weight 3.
In $\mathcal{C}_4 = \mathcal{C}_{2^2}$ we have $P_3(Q) = P_3(4) = 2 \cdot 4 - 2 = 6$ codewords of weight 3, and so on.

$$P_4(Z) = (-1)^4 \sum_{|\sigma|=4} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)}$$

$$\sigma = \{1,2,3,4\} \text{ gives } \gamma = \varnothing, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \\ \{2,4\}, \{3,4\}, \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \{1,2,3,4\}.$$

$$P_4(Z) = (-1)^0 Z^0 + 4 \cdot (-1)^1 Z^0 + 5 \cdot (-1)^2 Z^0 + (-1)^2 Z^1 + \\ +4 \cdot (-1)^3 Z^1 + (-1)^4 Z^2 = Z^2 - 3Z + 2.$$

Observe in $\mathcal{C}_2$ we have $P_4(Q) = P_4(2) = 2^2 - 3 \cdot 2 + 2 = 0$ codewords of weight 4.
In $\mathcal{C}_4 = \mathcal{C}_{2^2}$ we have $P_4(Q) = P_4(4) = 4^2 - 3 \cdot 4 + 2 = 6$ codewords of weight 4.

Remark 4.1. In general we see that in $\mathcal{C}_Q$ there are: 1 codeword of weight 0, and 0 codewords of weight 1, and $Q-1$ codewords of weight 2, and $2Q-2$ codewords of weight 3, and $Q^2 - 3Q + 2$ codewords of weight 4. The sum is Q^2, which is the number of all codewords in $\mathcal{C}_Q$, which has dimension 2 over $\mathbb{F}_Q$.

As an extra check we list the codewords of weights $0,1,2,3,4$ for $\mathcal{C}_4$.
Let $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$. The codewords are:
$\{0,0,0,0\}$ of weight 0;
$\{1,0,0,1\}$, $\{\alpha,0,0,\alpha\}$ and $\{\beta,0,0,\beta\}$ of weight 2;
$\{1,1,1,0\}$, $\{\alpha,\alpha,\alpha,0\}$, $\{\beta,\beta,\beta,0\}$, $\{0,1,1,1\}$, $\{0,\alpha,\alpha,\alpha\}$, $\{0,\beta,\beta,\beta\}$ of weight 3;
$\{\beta,1,1,\alpha\}$, $\{\alpha,1,1,\beta\}$, $\{\beta,\alpha,\alpha,1\}$, $\{1,\alpha,\alpha,\beta\}$, $\{\alpha,\beta,\beta,1\}$, $\{1,\beta,\beta,\alpha\}$ of weight 4.

4.1.1 Weight polynomials in terms of Betti numbers

It is also possible to find the $P_j(Z)$ in a different way. In [6] one finds the following result:

Theorem 4.1. *The coefficient of Z^l in P_j is equal to*

$$\sum_{i=0}^{n} (-1)^i \Big(\beta_{i,j}(I_{M_{(l-1)}}) - \beta_{i,j}(I_{M_{(l)}}) \Big)$$

for each $1 \leqslant j \leqslant n$.

Let us exemplify the last theorem, but we should first give the following lemma:

Lemma 4.1. *$\beta_{i,j}(R_\Delta) = \beta_{i-1,j}(I_\Delta)$ for any Stanley-Reisner ring R_Δ and corresponding Stanley-Reisner ideal I_Δ.*

Proof. If this is a minimal free resolution of $R_\Delta = S/I_\Delta$

$$\cdots \longrightarrow F_2 \longrightarrow F_1 \xrightarrow{\psi} S \xrightarrow{\phi} R_\Delta \longrightarrow 0$$

$Ker(\phi) = I_\Delta = Im(\psi)$ then

$$\cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow I_\Delta \longrightarrow 0$$

is a minimal free resolution of I_Δ.
It stands to reason that $\beta_{i,j}(R_\Delta) = \beta_{i-1,j}(I_\Delta)$. □

Example 4.1.3. Again look at the example 3.4.1.
We have already found $\beta_{0,2}(I_{M_{(0)}}) = 1$, $\beta_{0,3}(I_{M_{(0)}}) = 2$, $\beta_{1,4}(I_{M_{(0)}}) = 2$ and all other $\beta_{i,j}(I_{M_{(0)}}) = 0$.
We need to know the Betti numbers of $I_{M_{(1)}}$ and $I_{M_{(2)}}$. Begin with finding the elongations $M_{(1)}$ and $M_{(2)}$. The independent sets of $M_{(i)}$ are

$$\mathcal{I}(M_{(i)}) = \{\sigma \in E \mid n(\sigma) \leqslant i\}.$$

Then we have

$$\mathcal{I}(M_{(1)}) = \{\sigma \in E \mid n(\sigma) \leqslant 1\} = \{\text{all subsets of } E \text{ except } E\},$$

$$\mathcal{I}(M_{(2)}) = \{\sigma \in E \mid n(\sigma) \leqslant 2\} = 2^E \text{ (all subsets of } E)$$

and

$$r_0(M) = r_0(M_{(0)}) = 2,$$
$$r_1(M_{(1)}) = 3,$$
$$r_2(M_{(2)}) = 4.$$

We also know that any matroid M has a resolution with length $n - r(M)$.
For $M_{(1)}$ we get:

$$0 \longrightarrow S(-4) \longrightarrow S \longrightarrow R_\Delta \longrightarrow 0,$$

and it follows that $\beta_{0,4}(I_{M_{(1)}}) = 1$.
For $M_{(2)}$ we get:

$$0 \longrightarrow S \longrightarrow S \longrightarrow 0,$$

this implies $\beta_{0,0}(I_{M_{(2)}}) = 1$ and all other $\beta_{i,j}(I_{M_{(2)}}) = 0$.

Substitute all our Betti numbers into the formula in Theorem 4.1. Let us assume $\beta_{i,j}(I_{M_{(l)}}) = 0$ whenever $l \notin [0, n - r(M)]$.
For the case $j = 1$ the coefficient of Z^l is equal to

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,1}(I_{M_{(l-1)}}) - \beta_{i,1}(I_{M_{(l)}})\Big).$$

For $l = 0$:

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,1}(I_{M_{(-1)}}) - \beta_{i,1}(I_{M_{(0)}})\Big)= (-1)^0(0-0) + \ldots = 0.$$

For $l = 1$:

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,1}(I_{M_{(0)}}) - \beta_{i,1}(I_{M_{(1)}})\Big)= 0.$$

For $l = 2$:

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,1}(I_{M_{(1)}}) - \beta_{i,1}(I_{M_{(2)}})\Big)= 0.$$

When $j = 2$ the coefficient of Z^l is equal to

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,2}(I_{M_{(l-1)}}) - \beta_{i,2}(I_{M_{(l)}})\Big).$$

For $l = 0$:

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,2}(I_{M_{(-1)}}) - \beta_{i,2}(I_{M_{(0)}})\Big)= (-1)^0(0-1) = -1.$$

For $l = 1$:

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,2}(I_{M_{(0)}}) - \beta_{i,2}(I_{M_{(1)}})\Big)= (-1)^0(1-0) = 1.$$

For $l = 2$:

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,2}(I_{M_{(1)}}) - \beta_{i,2}(I_{M_{(2)}})\Big)= 0.$$

For the case $j = 3$ the coefficient of Z^l is equal to

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,3}(I_{M_{(l-1)}}) - \beta_{i,3}(I_{M_{(l)}})\Big).$$

For $l = 0$:

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,3}(I_{M_{(-1)}}) - \beta_{i,3}(I_{M_{(0)}})\Big) = (-1)^0(0-2) = -2.$$

For $l = 1$:

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,3}(I_{M_{(0)}}) - \beta_{i,3}(I_{M_{(1)}})\Big) = (-1)^0(2-0) = 2.$$

For $l = 2$:

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,3}(I_{M_{(1)}}) - \beta_{i,3}(I_{M_{(2)}})\Big) = 0.$$

When $j = 4$ the coefficient of Z^l is equal to

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,4}(I_{M_{(l-1)}}) - \beta_{i,4}(I_{M_{(l)}})\Big).$$

For $l = 0$:

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,4}(I_{M_{(-1)}}) - \beta_{i,4}(I_{M_{(0)}})\Big) = (-1)^0(0-0) + (-1)^1(0-2) = 2.$$

For $l = 1$:

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,4}(I_{M_{(0)}}) - \beta_{i,4}(I_{M_{(1)}})\Big) = (-1)^0(0-1) + (-1)^1(2-0) = -3.$$

For $l = 2$:

$$\sum_{i=0}^{4}(-1)^i\Big(\beta_{i,4}(I_{M_{(1)}}) - \beta_{i,4}(I_{M_{(2)}})\Big) = (-1)^0(1-0) = 1.$$

We list all results in table:

Z^l	Z^0	Z^1	Z^2
$j=1$	0	0	0
$j=2$	-1	1	0
$j=3$	-2	2	0
$j=4$	2	-3	1

We will now look at relations between Hamming weights and generalized weight polynomials of matroids. The following result is given without proof in [6]:

Proposition 4.2.

$$d_i(M) = \min\{j \mid \deg P_{M,j} = i\}.$$

Proof. We know

$$d_i = \min\{|X| \mid n(X) = i\}.$$

Also we know

$$\deg P_j = \max\{n(X) \mid |X| = j\}.$$

We then have the following

$$\begin{aligned} \min\{j \mid \deg P_j = i\} &= \min\{j \mid \max\{n(X) \mid |X| = j\} = i\} = \\ &= \min\{|X| \mid n(X) = i\} = d_i. \end{aligned}$$

□

Example 4.1.4. Look at the Example 4.1.2 and compute $d_i(M)$ by using the formula from the last proposition. Then formally $d_0 = 0$,

$$d_1 = \min\{j \mid \deg P_{M,j} = 1\} = 2,$$

$$d_2 = \min\{j \mid \deg P_{M,j} = 2\} = 4.$$

As an extra result we will give the following

Proposition 4.3. *For all j, with $j \geqslant d_i$, we have:*

$$\deg P_{M,j} = \max\{i \mid d_i \leqslant j\}.$$

Proof.

$$\begin{aligned}\deg P_{M,j} &= \max\{i \mid n(\sigma) \geqslant i, \text{ for some } \sigma \text{ with } |\sigma| = j\} = \\ &= \max\{i \mid d_i \leqslant j\}.\end{aligned}$$

□

Example 4.1.5. In the Example 4.1.2 we have found the polynomials:

$$P_0 = 1,$$

$$P_1 = 0,$$

$$P_2 = Z - 1,$$

$$P_3 = 2Z - 2,$$

$$P_4 = Z^2 - 3Z + 2.$$

Let us find degrees of these polynomials $\deg P_j$, $0 \leqslant j \leqslant 4$, having applied the formula above. Then we have

$$\deg P_0 = \max\{i \mid d_i \leqslant 0\} = 0,$$

$$\deg P_1 = \max\{i \mid d_i \leqslant 1\} = 0,$$

$$\deg P_2 = \max\{i \mid d_i \leqslant 2\} = 1,$$

$$\deg P_3 = \max\{i \mid d_i \leqslant 3\} = 1,$$

$$\deg P_4 = \max\{i \mid d_i \leqslant 4\} = 2.$$

Remark 4.2. In [3] one defines for linear codes:
$k_j(\mathcal{C})$ = maximum dimension of any subcode $\mathcal{C}'$ with $|Supp\,\mathcal{C}'| \leqslant j$ and

$$m_j(\mathcal{C}) = \min\{|Supp\,\mathcal{D}| \mid \mathcal{D} \text{ is a subcode of } \mathcal{C},\ \dim \mathcal{D} = j\}.$$

This is what we call $d_j(\mathcal{C})$ in our thesis.
Moreover one shows:

$$d_j(\mathcal{C}) = \min\{i \mid k_i \geqslant j\},$$

$$k_j(\mathcal{C}) = \max\{i \mid d_i \leqslant j\}.$$

Comparing these formulas to our Proposition 4.2 and Proposition 4.3, it is clear that the $\deg P_{M,j}$ are the same as the so-called dimension/length profiles k_j described by Forney, when M is the matroid $M_{\mathcal{C}}$ of a linear code.

The observations above also enable us to achieve results about elongations of matroids, given the weight polynomials of the original matroid.

Proposition 4.4. *Let $k \geqslant 1$. If*

$$P_{M_{(k-1)},j}(Z) = a_n Z^n + a_{n-1}Z^{n-1} + \ldots + a_1 Z + a_0,$$

then

$$P_{M_{(k)},j}(Z) = a_n Z^{n-1} + a_{n-1}Z^{n-2} + \ldots + a_2 Z + (a_1 + a_0).$$

Proof. Recall the formula for $P_{M,j}(Z)$:

$$P_{M,j}(Z) = (-1)^j \sum_{|\sigma|=j} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)} \text{ for } 1 \leqslant j \leqslant n.$$

Then we have

$$P_{M_{(1)},j}(Z) = (-1)^j \sum_{|\sigma|=j} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_{(1)}(\gamma)} \text{ for } 1 \leqslant j \leqslant n$$

and we know the following formula:

$$r_{(1)}(\gamma) = \min\{r(\gamma) + 1, |\gamma|\}.$$

Thus we can find the nullity function

$$\begin{aligned} n_{(1)}(\gamma) &= \max\{|\gamma| - r(\gamma) - 1, |\gamma| - |\gamma|\} = \\ &= \max\{n(\gamma) - 1, 0\}. \end{aligned}$$

For each $Z^{n(\gamma)} \longrightarrow Z^{n_{(1)}(\gamma)}$

$$P_{M_{(1)},j}(Z) = Z^{\max\{n(\gamma)-1,0\}} = \begin{cases} Z^{n(\gamma)-1}, & \text{if } n(\gamma) - 1 \geqslant 1; \\ Z^0 = 1, & \text{if } n(\gamma) = 0. \end{cases}$$

□

Corollary 4.1.

$$d_i(M_{(1)}) = d_{i+1}(M), \text{ for } i = 1, 2, \ldots$$

Proof. By previous result

$$d_{i+1}(M) = \min\{j \mid \deg P_{M,j} = i + 1\}$$

and

$$d_i(M_{(1)}) = \min\{j \mid \deg P_{M_{(1)},j} = i\}.$$

But these numbers are equal by Proposition 4.4. □

4.1.2 Herzog-Kühl equations

Definition 4.1. Let R be a ring. The Krull dimension $\dim R$ of R is the supremum of the length of chains of prime ideals

$$\mathcal{P}_0 \subset \mathcal{P}_1 \subset \ldots \subset \mathcal{P}_n.$$

Let M be a finitely generated graded R-module.

Definition 4.2. The Hilbert function is

$$\begin{array}{rccc} H(M,i): & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & i & \longmapsto & \dim_{\mathbb{K}} M_i. \end{array}$$

The Hilbert series is the Laurent series

$$H_M(t) = \sum_{i\in\mathbb{Z}} (\dim_{\mathbb{K}} M_i) t^i \in \mathbb{Z}[t, t^{-1}].$$

Let $R = S/I$ be a standard $\mathbb{K}$-graded algebra of Krull dimension d, $S = \mathbb{K}[x_1, \ldots, x_n]$ is the standard graded polynomial ring and I is a graded ideal of S. There exists a Laurent polynomial $Q_R \in \mathbb{Z}[t, t^{-1}]$ such that $Q_R(1) > 0$ and

$$H_R(t) = \frac{Q_R(t)}{(1-t)^d}$$

where $d = \dim R$.

Remark 4.3. The order of the pole of $H_R(t)$ at $t = 1$ is the Krull dimension of R.

Let a minimal free S-resolution of R be

$$0 \longrightarrow F_p \longrightarrow F_{p-1} \longrightarrow \cdots \longrightarrow F_0 \longrightarrow R \longrightarrow 0$$

with

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

It is known that

$$H_{F_i}(t) = \sum_{j\in\mathbb{Z}} \beta_{i,j} H_{S(-j)}(t)$$

and

$$H_{S(-j)}(t) = t^j H_S(t) = \frac{t^j}{(1-t)^n}.$$

Then the Hilbert series of R may be computed as the alternating sum of the Hilbert series of each of the terms in our resolution:

$$H_R(t) = \sum_{i=0}^{p}(-1)^i \sum_{j\in\mathbb{Z}} \beta_{i,j} \frac{t^j}{(1-t)^n}.$$

We can write $H_R(t)$ as

$$H_R(t) = \frac{Q_R(t)}{(1-t)^d} \times \frac{(1-t)^{n-d}}{(1-t)^{n-d}} = \frac{(1-t)^{n-d}\, Q_R(t)}{(1-t)^n}.$$

Then we have

$$(1-t)^{n-d}\, Q_R(t) = \sum_{i=0}^{p}(-1)^i \sum_{j\in\mathbb{Z}} \beta_{i,j} t^j.$$

Let $0 \leqslant k \leqslant n-d$. We differentiate k times. Then the left part of the equality is

$$\frac{\partial^k}{\partial t^k}(1-t)^{n-d}\, Q_R(t) = \sum_{l=0}^{k}\binom{k}{l}\frac{\partial^l}{\partial t^l}[(1-t)^{n-d}]\cdot \frac{\partial^{k-l}}{\partial t^{k-l}}\, Q_R(t) =$$

$$= \sum_{l=0}^{k}\binom{k}{l}(n-d)(n-d-1)\dots(n-d-(l-1))(-1)^l(1-t)^{n-d-l}\cdot \frac{\partial^{k-l}}{\partial t^{k-l}}\, Q_R(t).$$

We apply that at $t=1$. When $k < n-d$, then $n-d-l \geqslant 1$ and $\frac{\partial^k}{\partial t^k}(1-t)^{n-d}\, Q_R(t)|_{t=1} = 0$.
When $k = n-d$:

$$\begin{aligned}
\frac{\partial^k}{\partial t^k}(1-t)^{n-d}\, Q_R(t)|_{t=1} &= (n-d)(n-d-1)\dots(n-d-(n-d-1))(-1)^{n-d}\, Q_R(1) = \\
&= (n-d)!(-1)^{n-d}\, Q_R(1).
\end{aligned}$$

The right part of the equality is

$$\begin{aligned}
\frac{\partial^k}{\partial t^k}\Big[\sum_{i=0}^{p}(-1)^i \sum_{j\in\mathbb{Z}} \beta_{i,j} t^j\Big]\Big|_{t=1} &= \sum_{i=0}^{p}(-1)^i \sum_{j\in\mathbb{Z}} \beta_{i,j}\, j(j-1)\dots(j-k+1)\cdot t^{j-k}|_{t=1} = \\
&= \sum_{i=0}^{p}(-1)^i \sum_{j\in\mathbb{Z}} \beta_{i,j}\, j(j-1)\dots(j-k+1).
\end{aligned}$$

When $0 \leqslant k < n-d$:

$$\sum_{i=0}^{p}(-1)^i \sum_{j\in\mathbb{Z}} j(j-1)\dots(j-k+1)\beta_{i,j} = 0.$$

$$k=0\colon\ \sum_{i=0}^{p}(-1)^i \sum_{j\in\mathbb{Z}} \beta_{i,j} = 0,$$

$$k=1\colon\ \sum_{i=0}^{p}(-1)^i \sum_{j\in\mathbb{Z}} j\,\beta_{i,j} = 0,$$

$$k=2\colon\ \sum_{i=0}^{p}(-1)^i \sum_{j\in\mathbb{Z}} j(j-1)\beta_{i,j} = \sum_{i=0}^{p}(-1)^i \sum_{j\in\mathbb{Z}} j^2\beta_{i,j} = 0,$$

$$\dots$$

For $0 \leqslant k < n-d$, we have $\sum_{i=0}^{p}(-1)^i \sum_{j\in\mathbb{Z}} j^k\beta_{i,j} = 0$. These equations are called the Herzog-Kühl equations.

4.1.3 Betti numbers of Simplex codes

Let G be a generator matrix of a linear code $\mathcal{C}$, with column vectors $\underline{c}_i$. The $\underline{c}_i$ can be viewed as points of $\mathbb{P} = \mathbb{P}_q^{k-1}$. Then

$$d_1(\mathcal{C}) = n - \max\ \text{number of } \underline{c}_i \text{ in } H_1,$$

where the maximum is taken over all hyperplanes

$$H_1\colon a_1X_1 + \ldots + a_kX_k = 0 \text{ in } \mathbb{P}.$$

Moreover

$$d_r(\mathcal{C}) = n - \max\ \text{number of } \underline{c}_i \text{ in } H_r,$$

where the maximum is taken over all codim r-linear spaces H_r in $\mathbb{P}$. These H_r are intersections of r independent planes

$$\begin{aligned} a_{11}X_1 + \ldots + a_{1k}X_k &= 0 \\ &\vdots \\ a_{r1}X_1 + \ldots + a_{rk}X_k &= 0 \end{aligned}$$

Remark 4.4. This result was found in the article [13].

Definition 4.3. The simplex code $\mathcal{S}_q(k)$ is the dual of the Hamming code $Ham(r,q)$ over $\mathbb{F}_q$. Just like the Hamming codes they are only defined up to linear code equivalence.

Remark 4.5. The code $Ham(r,q)$ is a $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]_q$ code.

A generator matrix G for $\mathcal{S}_q(k)$ is

$$G = \begin{bmatrix} \underline{c}_1 & \underline{c}_2 & \dots & \underline{c}_{N_k} \end{bmatrix},$$

where the $\underline{c}_i$ represent all points of $\mathbb{P}^{k-1}_{\mathbb{F}_q}$.

Remark 4.6. The number of columns in G is

$$q^{k-1} + q^{k-2} + \ldots + q + 1 = \frac{q^k - 1}{q - 1} = N_k.$$

For all hyperplanes in $\mathbb{P}$ we observe: All of its points are among the $\underline{c}_i$, so

$$d_1 = n - \#\text{ (points in any fixed hyperplane)} = n - \#\text{ (points in } \mathbb{P}^{k-2}).$$

Thus:

$$d_1 = \#\text{ (points in } \mathbb{P}^{k-1}) - \#\text{ (points in } \mathbb{P}^{k-2}) = q^{k-1}.$$

Let us choose to write

$$G = \begin{bmatrix} \underline{r}_1 \\ \underline{r}_2 \\ \vdots \\ \underline{r}_k \end{bmatrix}.$$

A codeword of $\mathcal{C}$ is a linear combination $\underline{w} = a_1\underline{r}_1 + \ldots + a_k\underline{r}_k$.
The number of zeroes in $\underline{w}$ is equal to the number of columns $\underline{c}_i$ that satisfy $a_1X_1 + \ldots + a_kX_k = 0 \in H_w =$ points in $\underline{c}_i$ contained in $H_w =$
$=$ just the number of points in $\mathbb{P}^{k-2}$.

$$wt(\underline{w}) = n - \#\text{ (points in } \mathbb{P}^{k-2}) = q^{k-1} \text{ again.}$$

Hence any codeword in $\mathcal{C}$, except 0, has weight q^{k-1}. Thus we have proved:

Proposition 4.5. *The simplex code $\mathcal{S}_q(k)$ has minimum distance q^{k-1} and is a constant weight code.*

For constant weight linear codes we can also determine the entire weight hierarchy.

Proposition 4.6. *For the simplex code $\mathcal{S}_q(k)$ we have*

$$d_i = d\frac{q^i - 1}{q^{i-1}(q-1)} \text{ for } i = 1, \dots, k.$$

Remark 4.7. This formula is given in [8].

Definition 4.4. The resolution $F_l \longrightarrow \cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0$ is pure if it has the form

$$S(-d_l)^{\beta_{l,d_l}} \longrightarrow \cdots \longrightarrow S(-d_1)^{\beta_{1,d_1}} \longrightarrow S(-d_0)^{\beta_{0,d_0}}.$$

From [8] we also have:

Proposition 4.7. *The simplex code $\mathcal{S}_q(k)$ has a pure resolution, and the Betti numbers of its non-zero terms are*

$$\beta_{i,d_i} = \begin{bmatrix} k \\ i \end{bmatrix}_q q^{\frac{i(i-1)}{2}}$$

where

$$\begin{bmatrix} k \\ i \end{bmatrix}_q = \frac{f(k,q)}{f(i,q)f(k-i,q)}$$

and $f(n,q) = \prod_{i=1}^{n}(q^i - 1)$.

Theorem 4.2. *If the Stanley-Reisner ring of a matroid has a pure resolution, then its elongations also have pure resolutions.*

Proof. To prove this theorem one needs:
Theorem 1 in [7]: $\beta_{i,\sigma} \neq 0 \Longleftrightarrow \sigma$ is minimal in $\mathcal{N}_i$ ($\mathcal{N}_i = \{\sigma \mid n(\sigma) = i\}$) and the formula that we obtained in the proof of Proposition 4.4

$$n_{(1)}(\sigma) = \max\{0, n(\sigma) - 1\}.$$

Then we have the following

$$\{\sigma \mid \beta_{i,\sigma}(I_{M_{(1)}}) \neq 0\} = \{\sigma \mid \beta_{i+1,\sigma}(I_M) \neq 0\} \text{ for } i \geqslant 1,$$

which completes the proof of theorem. ∎

Example 4.1.6. Let us find the Betti numbers of the simplex code $\mathcal{S}_2(3)$ which is the dual of the Hamming code $Ham(3,2)$ over $\mathbb{F}_2$. The number of columns in generator matrix G is

$$N_k = \frac{q^k - 1}{q - 1} = \frac{2^3 - 1}{2 - 1} = 7.$$

The generator matrix

$$G = \left[\begin{array}{cccc} \underline{c}_1 & \underline{c}_2 & \dots & \underline{c}_7 \end{array} \right],$$

where the $\underline{c}_i$ represent all points of $\mathbb{P}^2_{\mathbb{F}_2}$. The minimum distance of $\mathcal{S}_2(3)$ is

$$d = d_1 = q^{k-1} = 2^{3-1} = 4.$$

It follows that $\mathcal{S}_2(3)$ is a $[7,3,4]_2$ code.

Having used the formula in Proposition 4.6 we find

$$d_2 = q^{k-2}(q+1) = 2 \cdot (2+1) = 6,$$

$$d_3 = d\frac{q^3 - 1}{q^{3-1}(q-1)} = 4 \cdot \frac{2^3 - 1}{2^2(2-1)} = 7.$$

The weight hierarchy is $(d_1, d_2, d_3) = (4, 6, 7)$.

We can now calculate the Betti numbers applying the formula

$$\beta_{i,d_i} = \left[\begin{array}{c} k \\ i \end{array} \right]_q q^{\frac{i(i-1)}{2}}$$

where

$$\left[\begin{array}{c} k \\ i \end{array} \right]_q = \frac{f(k,q)}{f(i,q)f(k-i,q)}$$

and $f(n,q) = \prod_{i=1}^{n}(q^i - 1)$. Then we get

$$\beta_{1,d_1} = \left[\begin{array}{c} 3 \\ 1 \end{array} \right]_2 2^0 = 7,$$

$$\beta_{2,d_2} = \left[\begin{array}{c} 3 \\ 2 \end{array} \right]_2 2^1 = 14,$$

$$\beta_{3,d_3} = \left[\begin{array}{c} 3 \\ 3 \end{array} \right]_2 2^3 = 8,$$

and the resolution of the Stanley-Reisner ring of M

$$0 \longrightarrow S(-7)^8 \longrightarrow S(-6)^{14} \longrightarrow S(-4)^7 \longrightarrow S \longrightarrow S/I \longrightarrow 0.$$

When M has $d_1, \dots, d_k$ where $k = n - r(M)$ its first elongation $M_{(1)}$ has rank $r+1 = (7-3)+1 = 5$. The number of d_i is $n-(r+1) = (n-r)-1 = k-1$. Then we can obtain only d_1, d_2 for $M_{(1)}$ in this case. The following formula is given in [6] as Corollary 5.2.:

$$d_i(M_{(l+1)}) = d_{i+1}(M_{(l)}).$$

Then

$$d_1(M_{(1)}) = d_2(M) = 6,$$
$$d_2(M_{(1)}) = d_3(M) = 7.$$

The second elongation $M_{(2)}$ has rank $r+2 = 4+2 = 6$. The number of d_i is $n-(r+2) = (n-r)-2 = k-2$. Then we obtain only d_1 for $M_{(2)}$.

$$d_1(M_{(2)}) = d_2(M_{(1)}) = 7.$$

It turns out that $M_{(1)}$, $M_{(2)}$ are the uniform matroids $U(5,7)$ and $U(6,7)$ respectively. The resolutions look like:

$$M_{(1)}\colon 0 \longrightarrow S(-7)^a \longrightarrow S(-6)^b \longrightarrow S \longrightarrow S/I \longrightarrow 0,$$

$$M_{(2)}\colon 0 \longrightarrow S(-7)^c \longrightarrow S \longrightarrow S/I \longrightarrow 0.$$

We can calculate a by using the formula from the Example 3 in the article [7]:

$$a = \binom{n-1}{r}\binom{n}{n} = \binom{6}{5}\binom{7}{7} = 6.$$

We have the equality $a+1 = b$, so $b = 7$. It is clear that $c = 1$ in the case of $M_{(2)}$. We get the following minimal free resolutions

$$M_{(1)}\colon 0 \longrightarrow S(-7)^6 \longrightarrow S(-6)^7 \longrightarrow S \longrightarrow S/I \longrightarrow 0,$$

$$M_{(2)}\colon 0 \longrightarrow S(-7)^1 \longrightarrow S \longrightarrow S/I \longrightarrow 0.$$

Thus we found the Betti numbers of M and its elongations:

$$\beta_{0,4}(I_M) = 7, \beta_{1,6}(I_M) = 14, \beta_{2,7}(I_M) = 8,$$

$$\beta_{0,6}(I_{M_{(1)}}) = 7, \beta_{1,7}(I_{M_{(1)}}) = 6,$$

$$\beta_{0,7}(I_{M_{(2)}}) = 1.$$

Use these Betti numbers to find the generalized weight polynomials. Recall the formula in Theorem 4.1:

$$\sum_{i=0}^{n}(-1)^i\Big(\beta_{i,j}(I_{M_{(l-1)}}) - \beta_{i,j}(I_{M_{(l)}})\Big)$$

for each $1 \leqslant j \leqslant n$. Let us assume $\beta_{i,j}(I_{M_{(l)}}) = 0$ whenever $l \notin [0, n-r(M)]$. For the cases $j = 1, 2, 3$ the coefficient of Z^l is equal to 0 for all $l \in [0, 3]$. When $j = 4$ the coefficient of Z^l is equal to

$$\sum_{i=0}^{7}(-1)^i\Big(\beta_{i,4}(I_{M_{(l-1)}}) - \beta_{i,4}(I_{M_{(l)}})\Big).$$

For $l = 0$:

$$\sum_{i=0}^{7}(-1)^i\Big(\beta_{i,4}(I_{M_{(-1)}}) - \beta_{i,4}(I_{M_{(0)}})\Big) = (-1)^0(0-7) = -7.$$

For $l = 1$:

$$\sum_{i=0}^{7}(-1)^i\Big(\beta_{i,4}(I_{M_{(0)}}) - \beta_{i,4}(I_{M_{(1)}})\Big) = (-1)^0(7-0) = 7.$$

For $l = 2$ and $l = 3$ the coefficients are equal to 0.
For the case $j = 5$ the coefficient of Z^l is equal to 0 for all $l \in [0, 3]$.
When $j = 6$ the coefficient of Z^l is equal to

$$\sum_{i=0}^{7}(-1)^i\Big(\beta_{i,6}(I_{M_{(l-1)}}) - \beta_{i,6}(I_{M_{(l)}})\Big).$$

For $l = 0$:

$$\sum_{i=0}^{7}(-1)^i\Big(\beta_{i,6}(I_{M_{(-1)}}) - \beta_{i,6}(I_{M_{(0)}})\Big) = (-1)^1(0-14) = 14.$$

For $l = 1$:

$$\sum_{i=0}^{7}(-1)^i\Big(\beta_{i,6}(I_{M_{(0)}}) - \beta_{i,6}(I_{M_{(1)}})\Big) = (-1)^0(0-7) + (-1)^1(14-0) = -21.$$

For $l = 2$:

$$\sum_{i=0}^{7}(-1)^i\Big(\beta_{i,6}(I_{M_{(1)}}) - \beta_{i,6}(I_{M_{(2)}})\Big) = (-1)^0(7-0) = 7.$$

For $l = 3$:

$$\sum_{i=0}^{7}(-1)^i\Big(\beta_{i,6}(I_{M_{(2)}}) - \beta_{i,6}(I_{M_{(3)}})\Big) = 0.$$

When $j = 7$ the coefficient of Z^l is equal to

$$\sum_{i=0}^{7}(-1)^i\Big(\beta_{i,7}(I_{M_{(l-1)}}) - \beta_{i,7}(I_{M_{(l)}})\Big).$$

For $l = 0$:

$$\sum_{i=0}^{7}(-1)^i\Big(\beta_{i,7}(I_{M_{(-1)}}) - \beta_{i,7}(I_{M_{(0)}})\Big) = (-1)^2(0-8) = -8.$$

For $l = 1$:

$$\sum_{i=0}^{7}(-1)^i\Big(\beta_{i,7}(I_{M_{(0)}}) - \beta_{i,7}(I_{M_{(1)}})\Big) = (-1)^1(0-6) + (-1)^2(8-0) = 14.$$

For $l = 2$:

$$\sum_{i=0}^{7}(-1)^i\Big(\beta_{i,7}(I_{M_{(1)}}) - \beta_{i,7}(I_{M_{(2)}})\Big) = (-1)^0(0-1) + (-1)^1(6-0) = -7.$$

For $l = 3$:

$$\sum_{i=0}^{7}(-1)^i\Big(\beta_{i,7}(I_{M_{(2)}}) - \beta_{i,7}(I_{M_{(3)}})\Big) = (-1)^0(1-0) = 1.$$

We list all results in table:

Z^l	Z^0	Z^1	Z^2	Z^3
$j=0$	1	0	0	0
$j=1$	0	0	0	0
$j=2$	0	0	0	0
$j=3$	0	0	0	0
$j=4$	-7	7	0	0
$j=5$	0	0	0	0
$j=6$	14	-21	7	0
$j=7$	-8	14	-7	1

Example 4.1.7. Let us find the Betti numbers of the simplex code $\mathcal{S}_2(4)$ which is the dual of the Hamming code $Ham(4,2)$ over $\mathbb{F}_2$. The number of columns in generator matrix G is

$$N_k = \frac{q^k-1}{q-1} = \frac{2^4-1}{2-1} = 15.$$

The minimum distance of $\mathcal{S}_2(4)$ is

$$d = d_1 = q^{k-1} = 2^{4-1} = 8.$$

It follows that $\mathcal{S}_2(4)$ is a $[15,4,8]_2$ code.

Having used the formula in Proposition 4.6 we find

$$d_2 = q^{k-2}(q+1) = 2^2(2+1) = 12,$$

$$d_3 = d\frac{q^3-1}{q^{3-1}(q-1)} = 8\cdot\frac{2^3-1}{2^2(2-1)} = 14,$$

$$d_4 = d\frac{q^4-1}{q^{4-1}(q-1)} = 8\cdot\frac{2^4-1}{2^3(2-1)} = 15.$$

The weight hierarchy is $(d_1,d_2,d_3,d_4) = (8,12,14,15)$.

We can now calculate the Betti numbers applying the formula

$$\beta_{i,d_i} = \left[\begin{array}{c} k \\ i \end{array}\right]_q q^{\frac{i(i-1)}{2}}$$

where

$$\left[\begin{array}{c} k \\ i \end{array}\right]_q = \frac{f(k,q)}{f(i,q)f(k-i,q)}$$

and $f(n,q) = \prod_{i=1}^{n}(q^i - 1)$. Then we get

$$\beta_{1,d_1} = \begin{bmatrix} 4 \\ 1 \end{bmatrix}_2 2^0 = 15,$$

$$\beta_{2,d_2} = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_2 2^1 = 70,$$

$$\beta_{3,d_3} = \begin{bmatrix} 4 \\ 3 \end{bmatrix}_2 2^3 = 120,$$

$$\beta_{4,d_4} = \begin{bmatrix} 4 \\ 4 \end{bmatrix}_2 2^6 = 64,$$

and the resolution of the ideal I of M

$$0 \longrightarrow S(-15)^{64} \longrightarrow S(-14)^{120} \longrightarrow S(-12)^{70} \longrightarrow S(-8)^{15} \longrightarrow I_M \longrightarrow 0.$$

When M has $d_1, \ldots, d_k$ where $k = n - r(M)$ its first elongation $M_{(1)}$ has rank $r+1 = (15-4)+1 = 12$. The number of d_i is $n-(r+1) = (n-r)-1 = k-1$. Then we can obtain d_1, d_2, and d_3 for $M_{(1)}$ in this case. The following formula is given in [6] as Corollary 5.2.:

$$d_i(M_{(l+1)}) = d_{i+1}(M_{(l)}).$$

Then

$$d_0(M_{(1)}) = 0,$$
$$d_1(M_{(1)}) = d_2(M) = 12,$$
$$d_2(M_{(1)}) = d_3(M) = 14,$$
$$d_3(M_{(1)}) = d_4(M) = 15.$$

The second elongation $M_{(2)}$ has rank $r+2 = 11+2 = 13$. The number of d_i is $n-(r+2) = (n-r)-2 = k-2$. Then we obtain only d_1, d_2 for $M_{(2)}$.

$$d_1(M_{(2)}) = d_2(M_{(1)}) = 14,$$

$$d_2(M_{(2)}) = d_3(M_{(1)}) = 15.$$

The third elongation $M_{(3)}$ has rank $r+3 = 11+3 = 14$. The number of d_i is $n-(r+3) = (n-r)-3 = k-3$. Then we obtain only d_1 for $M_{(3)}$.

$$d_1(M_{(3)}) = d_2(M_{(2)}) = 15.$$

The resolutions look like:

$$M_{(1)}\colon 0 \longrightarrow S(-15)^{?} \longrightarrow S(-14)^{?} \longrightarrow S(-12)^{?} \longrightarrow I_{M_{(1)}} \longrightarrow 0,$$

$$M_{(2)}\colon 0 \longrightarrow S(-15)^{a} \longrightarrow S(-14)^{b} \longrightarrow I_{M_{(2)}} \longrightarrow 0,$$

$$M_{(3)}\colon 0 \longrightarrow S(-15)^{c} \longrightarrow I_{M_{(3)}} \longrightarrow 0.$$

It turns out that $M_{(2)}$, $M_{(3)}$ are the uniform matroids $U(13,15)$ and $U(14,15)$ respectively. We can calculate a by using the formula from the Example 3 in the article [7]:

$$a = \binom{n-1}{r}\binom{n}{n} = \binom{14}{13}\binom{14}{14} = 14.$$

We have the equality $a+1=b$, so $b=15$. It is clear that $c=1$ in the case of $M_{(3)}$.

In order to find the β_{i,d_i} of $M_{(1)}$ we will use the following formula given in [2]:

$$\beta_{i,d_i} = (-1)^i \cdot t \cdot \prod_{k\neq i} \frac{1}{(d_k - d_i)} \quad \text{where } t \in \mathbb{Q}.$$

Then we have

$$\beta_{1,d_1} = (-1)^1 \cdot t \cdot \prod_{k\neq 1} \frac{1}{(d_k - d_1)} = \frac{-t}{(0-12)(14-12)(15-12)} = \frac{t}{72},$$

$$\beta_{2,d_2} = (-1)^2 \cdot t \cdot \prod_{k\neq 2} \frac{1}{(d_k - d_2)} = \frac{t}{(0-14)(12-14)(15-14)} = \frac{t}{28},$$

$$\beta_{3,d_3} = (-1)^3 \cdot t \cdot \prod_{k\neq 3} \frac{1}{(d_k - d_3)} = \frac{-t}{(0-15)(12-15)(14-15)} = \frac{t}{45}.$$

We have the equality

$$1 + \frac{t}{28} = \frac{t}{72} + \frac{t}{45},$$

whence it follows that $t = 2520$ and $\beta_{1,d_1} = 35$, $\beta_{2,d_2} = 90$, $\beta_{3,d_3} = 56$. Now the minimal free resolutions are

$$M_{(1)}\colon 0 \longrightarrow S(-15)^{56} \longrightarrow S(-14)^{90} \longrightarrow S(-12)^{35} \longrightarrow I_{M_{(1)}} \longrightarrow 0,$$

$$M_{(2)}\colon 0 \longrightarrow S(-15)^{14} \longrightarrow S(-14)^{15} \longrightarrow I_{M_{(2)}} \longrightarrow 0,$$

$$M_{(3)} \colon 0 \longrightarrow S(-15)^1 \longrightarrow I_{M_{(3)}} \longrightarrow 0.$$

Thus we found the Betti numbers of M and its elongations:

$$\beta_{0,8}(I_M) = 15, \beta_{1,12}(I_M) = 70, \beta_{2,14}(I_M) = 120, \beta_{3,15}(I_M) = 64,$$

$$\beta_{0,12}(I_{M_{(1)}}) = 35, \beta_{1,14}(I_{M_{(1)}}) = 90, \beta_{2,15}(I_{M_{(1)}}) = 56,$$
$$\beta_{0,14}(I_{M_{(2)}}) = 15, \beta_{1,15}(I_{M_{(2)}}) = 14,$$
$$\beta_{0,15}(I_{M_{(3)}}) = 1.$$

Use these Betti numbers to find the generalized weight polynomials. Recall the formula in Theorem 4.1:

$$\sum_{i=0}^{n} (-1)^i \Big(\beta_{i,j}(I_{M_{(l-1)}}) - \beta_{i,j}(I_{M_{(l)}}) \Big)$$

for each $1 \leqslant j \leqslant n$. Let us assume $\beta_{i,j}(I_{M_{(l)}}) = 0$ whenever $l \notin [0, n - r(M)]$. For the cases $j = 1, 2, \ldots, 7$ the coefficient of Z^l is equal to 0 for all $l \in [0, 4]$. When $j = 8$ the coefficient of Z^l is equal to

$$\sum_{i=0}^{15} (-1)^i \Big(\beta_{i,8}(I_{M_{(l-1)}}) - \beta_{i,8}(I_{M_{(l)}}) \Big).$$

For $l = 0$:

$$\sum_{i=0}^{15} (-1)^i \Big(\beta_{i,8}(I_{M_{(-1)}}) - \beta_{i,8}(I_{M_{(0)}}) \Big) = (-1)^0 (0 - 15) = -15.$$

For $l = 1$:

$$\sum_{i=0}^{15} (-1)^i \Big(\beta_{i,8}(I_{M_{(0)}}) - \beta_{i,8}(I_{M_{(1)}}) \Big) = (-1)^0 (15 - 0) = 15.$$

For $l = 2$, $l = 3$ and $l = 4$ the coefficients are equal to 0.
For the cases $j = 9, 10, 11$ the coefficient of Z^l is equal to 0 for all $l \in [0, 4]$. When $j = 12$ the coefficient of Z^l is equal to

$$\sum_{i=0}^{15} (-1)^i \Big(\beta_{i,12}(I_{M_{(l-1)}}) - \beta_{i,12}(I_{M_{(l)}}) \Big).$$

For $l = 0$:

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,12}(I_{M_{(-1)}}) - \beta_{i,12}(I_{M_{(0)}})\Big) = (-1)^1(0-70) = 70.$$

For $l = 1$:

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,12}(I_{M_{(0)}}) - \beta_{i,12}(I_{M_{(1)}})\Big) = (-1)^0(0-35) + (-1)^1(70-0) = -105.$$

For $l = 2$:

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,12}(I_{M_{(1)}}) - \beta_{i,12}(I_{M_{(2)}})\Big) = (-1)^0(35-0) = 35.$$

For $l = 3$ and $l = 4$ the coefficients are equal to 0.
For the case $j = 13$ the coefficient of Z^l is equal to 0 for all $l \in [0, 4]$.
When $j = 14$ the coefficient of Z^l is equal to

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,14}(I_{M_{(l-1)}}) - \beta_{i,14}(I_{M_{(l)}})\Big).$$

For $l = 0$:

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,14}(I_{M_{(-1)}}) - \beta_{i,14}(I_{M_{(0)}})\Big) = (-1)^2(0-120) = -120.$$

For $l = 1$:

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,14}(I_{M_{(0)}}) - \beta_{i,14}(I_{M_{(1)}})\Big) = (-1)^1(0-90) + (-1)^2(120-0) = 210.$$

For $l = 2$:

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,14}(I_{M_{(1)}}) - \beta_{i,14}(I_{M_{(2)}})\Big) = (-1)^0(0-15) + (-1)^1(90-0) = -105.$$

For $l = 3$:

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,14}(I_{M_{(2)}}) - \beta_{i,14}(I_{M_{(3)}})\Big) = (-1)^0(15-0) = 15.$$

For $l = 4$:

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,14}(I_{M_{(3)}}) - \beta_{i,14}(I_{M_{(4)}})\Big) = 0.$$

When $j = 15$ the coefficient of Z^l is equal to

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,15}(I_{M_{(l-1)}}) - \beta_{i,15}(I_{M_{(l)}})\Big).$$

For $l = 0$:

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,15}(I_{M_{(-1)}}) - \beta_{i,15}(I_{M_{(0)}})\Big) = (-1)^3(0-64) = 64.$$

For $l = 1$:

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,15}(I_{M_{(0)}}) - \beta_{i,15}(I_{M_{(1)}})\Big) = (-1)^2(0-56) + (-1)^3(64-0) = -120.$$

For $l = 2$:

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,15}(I_{M_{(1)}}) - \beta_{i,15}(I_{M_{(2)}})\Big) = (-1)^1(0-14) + (-1)^2(56-0) = 70.$$

For $l = 3$:

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,15}(I_{M_{(2)}}) - \beta_{i,15}(I_{M_{(3)}})\Big) = (-1)^0(0-1) + (-1)^1(14-0) = -15.$$

For $l = 4$:

$$\sum_{i=0}^{15}(-1)^i\Big(\beta_{i,15}(I_{M_{(3)}}) - \beta_{i,15}(I_{M_{(4)}})\Big) = (-1)^0(1-0) = 1.$$

We list all results in table:

Z^l	Z^0	Z^1	Z^2	Z^3	Z^4
$j=0$	1	0	0	0	0
$j=1$	0	0	0	0	0
$j=2$	0	0	0	0	0
$j=3$	0	0	0	0	0
$j=4$	0	0	0	0	0
$j=5$	0	0	0	0	0
$j=6$	0	0	0	0	0
$j=7$	0	0	0	0	0
$j=8$	-15	15	0	0	0
$j=9$	0	0	0	0	0
$j=10$	0	0	0	0	0
$j=11$	0	0	0	0	0
$j=12$	70	-105	35	0	0
$j=13$	0	0	0	0	0
$j=14$	-120	210	-105	15	0
$j=15$	64	-120	70	-15	1

4.1.4 Betti numbers of Reed-Müller codes

Definition 4.5. Reed-Müller code $\mathcal{RM}_q(1,k-1)$ (for example, $\mathcal{RM}_2(1,3)$) is a linear $[q^{k-1},k]$ code over $\mathbb{F}_q$. It is also defined by a generator matrix

$$G = \left[\ \underset{\sim}{c}_1 \quad \underset{\sim}{c}_2 \quad \dots\ \right],$$

where we don't pick all the points in $\mathbb{P}^{k-1}$, but just some of them.

Here in $\mathbb{P}^{k-1}$ containing $q^{k-1}+q^{k-2}+\ldots+1$ points we only pick those that are in an affine piece $\mathbb{A}^{k-1} \subseteq \mathbb{P}^{k-1}$.

In the example $k=3+1=4$ and $n=q^{k-1}=2^{4-1}=8$. Then

$$G = \begin{array}{c} x_0 \\ x_1 \\ x_2 \\ x_3 \end{array} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

and the affine piece we choose is $x_0 = 1$.

$$d_1 = n - \max \text{ number of points in a hyperplane } H,$$

where points are taken from the affine piece $A_0 = \mathbb{P}^{k-1} - H_0$.
In other words

$$d_1 = n - \max |H \cap A_0|.$$

We have two possibilities for hyperplanes H:

(1) $H = H_0$. Then $H \cap A_0 = \varnothing$.

(2) $H \neq H_0$. Then: $|H \cap A_0| = |H \setminus (H \cap H_0)| = |H| \setminus |H \cap H_0| = (q^{k-2} + q^{k-3} + \ldots) - (q^{k-3} + q^{k-4} + \ldots) = q^{k-2}$.

Then $\mathcal{RM}_q(1, k-1)$ is a two weight code over $\mathbb{F}_q$. It has two weights: n and $n - q^{k-2}$.

For the next Hamming weight we have:

$$d_2 = n - \max |L_2 \cap A_0|, \text{ for some codim 2-space } L_2 = H_1 \cap H_2 \subseteq \mathbb{P}^{k-1}.$$

We rewrite:

$$L_2 \cap A_0 = L_2 - (L_2 \cap H_0) = L_2 - ((H_1 \cap H_2) \cap H_0).$$

Again we have two possibilities:

(1) $H_0 \supseteq H_1 \cap H_2$. Then $|L_2 \cap H_0| = |L_2| = |\mathbb{P}^{k-3}|$, and $L_2 \cap A_0 = \varnothing$.

(2) $H_0 \not\supseteq H_1 \cap H_2$. Then $|L_2 \cap H_0| = |(H_1 \cap H_2) \cap H_0| = |\mathbb{P}^{k-4}|$.

One of the support weights is $n - |\varnothing| = n$.
For (2): $|L_2 \cap A_0| = |\mathbb{P}^{k-3}| - |\mathbb{P}^{k-4}| = q^{k-3}$, so we get another weight $n - q^{k-3}$.

As a consequence, proceeding in an analogous manner, for $d_3, d_4, \ldots$ we obtain

$$\begin{aligned} d_1 &= n - q^{k-2}, \\ d_2 &= n - q^{k-3}, \\ d_3 &= n - q^{k-4}, \\ d_4 &= n - q^{k-5}, \\ &\ldots, \\ d_{k-1} &= n - q^0 = n - 1, \\ d_k &= n. \end{aligned}$$

Moreover, for each $i = 1, 2, \ldots, k-1$, we see that for subcodes of $\mathcal{C}$ of dimension i, there are only two possible support weights, n and $n - q^{k-i-1}$.

Theorem 4.3. *The Reed-Müller code $\mathcal{C} = \mathcal{RM}_q(1, k-1)$ has a pure resolution of its associated Stanley-Reisner ideal.*

Proof. Let us clarify why the resolution of the ideal I_M is pure.
We must prove that for every h $\beta_{h,\sigma} \neq 0$ only for σ, with $|\sigma| = d_h$.

$$\beta_{h,j} = \sum_{|\sigma|=j} \beta_{h,\sigma}.$$

But we also have

$$\beta_{h,\sigma} \neq 0 \iff \sigma \text{ is minimal in } \mathcal{N}_h.$$

So we must prove that all minimal sets in $\mathcal{N}_h$ have the same cardinality (which is d_h).

We have Reed-Müller code $\mathcal{C}$ (linear code in general) with generator matrix

$$G = \begin{bmatrix} \underline{c}_1 & \underline{c}_2 & \ldots & \underline{c}_n \end{bmatrix},$$

n points in $\mathbb{P} = \mathbb{P}^{k-1}$.
Let $\underline{c}_{i_1}, \ldots, \underline{c}_{i_s}$ be the points contained in a (codim h)-plane L_h in $\mathbb{P}$. L_h is given by independent equations

$$\begin{aligned} d_{11}X_1 + \ldots + d_{1n}X_n &= 0 \\ &\vdots \\ d_{h1}X_1 + \ldots + d_{hn}X_n &= 0 \end{aligned}$$

For the coefficient matrix D we have $D \cdot \overline{X}^T = 0$.

Choose to write

$$G = \begin{bmatrix} \underline{r}_1 \\ \underline{r}_2 \\ \vdots \\ \underline{r}_n \end{bmatrix}.$$

Then the subcode $\mathcal{K}$ of $\mathcal{C}$ given by

$$\text{Span} \begin{cases} d_{11}\vec{r}_1 + \ldots + d_{1n}\vec{r}_n \\ \qquad \vdots \\ d_{h1}\vec{r}_1 + \ldots + d_{hn}\vec{r}_n \end{cases}$$

has zeroes in positions $i_1, \dots, i_s$, and

$$Supp\,(\mathcal{K}) = E \setminus \{i_1, \dots, i_s\},$$

so

$$W(\mathcal{K}) = |Supp\,(\mathcal{K})| = n - s = n - |A_0 \cap L_h|.$$

In this case, let $\underline{c}_{j_1}, \dots, \underline{c}_{j_t}$ be the remaining columns. Hence $t = n - s$.
Then $\sigma_t = \{j_1, \dots, j_t\} = Supp\,(\mathcal{K})$. This implies $n(\sigma_t) \geqslant h$.
Let a parity check matrix for $\mathcal{C}$ be

$$H = \left[\begin{array}{cccc} \underline{a}_1 & \underline{a}_2 & \dots & \underline{a}_n \end{array}\right].$$

Every word in $\mathcal{K}$ is a linear relation between the $\underline{a}_i$, for $i \in Supp\,(\mathcal{K})$. Since there are h linearly independent codewords in $\mathcal{K}$ we have h linearly independent relations between the $\underline{a}_i$, for $i \in Supp\,(\mathcal{K})$. Hence $n(\sigma_t) \geqslant h$.
We claim that for Reed-Müller codes, and $h = 1, 2, \dots, k-1$ we have: $n(\sigma_t) = h$ for all the $\mathcal{K}$ with $t = n - s = n - q^{k-i-1}$, and that these σ_t are inclusion minimal among the $X \subseteq E$, with $n(X) = h$, and that these σ_t are the only $X \subseteq E$ that are inclusion minimal among the $X \subseteq E$ with $n(X) = h$.

- If $n(\sigma_t) = h + p$, $p \geqslant 1$ then $\underline{c}_{i1}, \dots, \underline{c}_{is}$ would be contained in a codim $(h+p)$-space. But the maximum number in such a space is $q^{n-h-p-1}$. But $s = q^{n-h-1} > q^{n-h-p-1}$ impossible.
- If strict subset $S \subsetneq \sigma_t$ with $n(S) = h$, then $E \setminus S$ would be contained in codim plane L_h. Impossible since $|E \setminus S| > q^{n-h-1}$. Hence the σ_t are inclusion minimal for all the $\mathcal{K}$ with support weight $n - q^{k-i-1}$.

Let us write H as

$$H = \left[\begin{array}{cccccccc} \underline{a}_1 & \underline{a}_2 & \dots & \underline{a}_t & \underline{a}_{t+1} & \dots & \underline{a}_n \end{array}\right].$$

Then $X = \{1, 2, \dots, t\}$, $Y = \{t+1, \dots, n\}$. We assume that:

$$n(X) = h,$$
$$\mathcal{N}_h = \{\sigma \subseteq E \mid n(\sigma) = h\},$$
$$X \text{ is minimal in } \mathcal{N}_h.$$

Since $n(X) = h$, there exist h independent relations between $\underline{a}_1, \dots, \underline{a}_t$. This gives a subcode $\mathcal{K}_h \subseteq \mathcal{C}$, with $Supp\,(\mathcal{K}_h) \subseteq X$.
In fact: $Supp\,(\mathcal{K}_h) = X$. If $Supp\,(\mathcal{K}_h) = X' \subsetneq X$ then you would have the same h independent relations between the columns corresponding to X', then $n(X') = h$ also. But then X is not minimal in $\mathcal{N}_h$. But from what we have already seen there are only two possibilities for $Supp\,(\mathcal{K}_h)$ (identifying $E = A_0$):

(1) $Supp\,(\mathcal{K}_h) = E(= A_0) = X$.

(2) $Supp\,(\mathcal{K}_h) = A_0 \setminus (A_0 \cap L_h) = X$ for some (codim h)-plane.

In case (1) $n(X) = n(E) = |X| - r(X) = n - (n-k) = k$.
In case (2) $n(X) = h$. So case (2) is the only possible if $h < k$, since we know $n(X) = h$.
For $h = k$ we see that a (codim h)-plane in $\mathbb{A}_0$ is $\varnothing$. Case (1) $\mathbb{A}_0 = E = X$. Case (2) $\mathbb{A}_0 \setminus \varnothing = \mathbb{A}_0 = X$.
This argument works well for $h = 1, \dots, k-1$. For $h = k$ there is no difference between (1) and (2), and $X = E(= \mathbb{A}_0)$. $\square$

Example 4.1.8. Let us find the Betti numbers of the Reed-Müller code $\mathcal{RM}_q(1,3)$ which is a $[q^3, 4]$ code over $\mathbb{F}_q$.

The Hamming weights of $\mathcal{RM}_q(1,3)$ are

$$\begin{aligned} d_0 &= 0, \\ d_1 &= n - q^{k-2} = q^3 - q^2, \\ d_2 &= n - q^{k-3} = q^3 - q, \\ d_3 &= n - q^{k-4} = q^3 - 1, \\ d_4 &= n = q^3. \end{aligned}$$

In order to find the β_{h,d_h} we will apply the formula that we already used before:

$$\beta_{h,d_h} = (-1)^h \cdot t \cdot \prod_{k \neq h} \frac{1}{(d_k - d_h)} \text{ where } t \in \mathbb{Q}.$$

Then we have

$$\begin{aligned} \beta_{1,d_1} &= (-1)^1 \cdot t \cdot \frac{1}{(0 - q^3 + q^2)(-q + q^2)(-1 + q^2)q^2} = \\ &= \frac{t}{q^5(q-1)^2(q^2-1)}, \end{aligned}$$

$$\begin{aligned}\beta_{2,d_2} &= (-1)^2 \cdot t \cdot \frac{1}{(0-q^3+q)(-q^2+q)(-1+q)q} = \\ &= \frac{t}{q^3(q-1)^2(q^2-1)},\end{aligned}$$

$$\begin{aligned}\beta_{3,d_3} &= (-1)^3 \cdot t \cdot \frac{1}{(0-q^3+1)(-q^2+1)(-q+1)} = \\ &= \frac{t}{(q^3-1)(q^2-1)(q-1)},\end{aligned}$$

$$\beta_{4,d_4} = (-1)^4 \cdot t \cdot \frac{1}{(0-q^3)(q^3-q^2-q^3)(q^3-q-q^3)(q^3-1-q^3)} = \frac{t}{q^6}.$$

Due to Herzog-Kühl equations we have the equality

$$1 + \frac{t}{q^3(q-1)^2(q^2-1)} + \frac{t}{q^6} = \frac{t}{q^5(q-1)^2(q^2-1)} + \frac{t}{(q^3-1)(q^2-1)(q-1)},$$

whence it follows that $t = q^6(q^3-1)(q^2-1)(q-1)$ and $\beta_{1,d_1} = q(q^2+q+1)$, $\beta_{2,d_2} = q^3(q^2+q+1)$, $\beta_{3,d_3} = q^6$ and $\beta_{4,d_4} = (q^3-1)(q^2-1)(q-1)$. The resolution of the ideal I of M is

$$0 \longrightarrow S(-d_4)^{\beta_{4,d_4}} \longrightarrow S(-d_3)^{\beta_{3,d_3}} \longrightarrow S(-d_2)^{\beta_{2,d_2}} \longrightarrow S(-d_1)^{\beta_{1,d_1}} \longrightarrow I_M \longrightarrow 0.$$

When M has rank $r = n-k = q^3-4$ its first elongation $M_{(1)}$ has rank $r+1 = (q^3-4)+1 = q^3-3$. The number of d_i is $n-(r+1) = (n-r)-1 = k-1 = 3$. Thus we have to find d_1, d_2, and d_3 for $M_{(1)}$. We already know the following formula:

$$d_i(M_{(l+1)}) = d_{i+1}(M_{(l)}).$$

Then

$$d_0 = 0,$$

$$d_1(M_{(1)}) = d_2(M) = q^3 - q,$$

$$d_2(M_{(1)}) = d_3(M) = q^3 - 1,$$

$$d_3(M_{(1)}) = d_4(M) = q^3.$$

The second elongation $M_{(2)}$ has rank $r+2=q^3-2$. The number of d_i is $n-(r+2)=(n-r)-2=k-2=2$. Then we have to find only d_1, d_2 for $M_{(2)}$.

$$d_1(M_{(2)}) = d_2(M_{(1)}) = q^3-1,$$
$$d_2(M_{(2)}) = d_3(M_{(1)}) = q^3.$$

The third elongation $M_{(3)}$ has rank $r+3=q^3-1$. The number of d_i is $n-(r+3)=(n-r)-3=k-3=1$. Then we have to find only d_1 for $M_{(3)}$.

$$d_1(M_{(3)}) = d_2(M_{(2)}) = q^3.$$

The resolutions look like:

$$M_{(1)}\colon 0 \longrightarrow S(-q^3)^a \longrightarrow S(-(q^3-1))^b \longrightarrow S(-(q^3-q))^c \longrightarrow I_{M_{(1)}} \longrightarrow 0,$$
$$M_{(2)}\colon 0 \longrightarrow S(-q^3)^d \longrightarrow S(-(q^3-1))^e \longrightarrow I_{M_{(2)}} \longrightarrow 0,$$
$$M_{(3)}\colon 0 \longrightarrow S(-q^3)^{f=1} \longrightarrow I_{M_{(3)}} \longrightarrow 0.$$

In the case when $q=2$ the first elongation $M_{(1)}$ is the uniform matroid $U(q^3-3,q^3)$, otherwise it is not uniform. Then the Betti numbers can be found as usual:

$$c = (-1)^1\cdot t\cdot \frac{1}{(-q^3+q)(-1+q)q} = \frac{t}{q^2(q-1)^2(q+1)},$$
$$b = (-1)^2\cdot t\cdot \frac{1}{(-q^3+1)(-q+1)\cdot 1} = \frac{t}{(q^3-1)(q-1)},$$
$$a = (-1)^3\cdot t\cdot \frac{1}{(-q^3)(-q)(-1)} = \frac{t}{q^4}.$$

Due to Herzog-Kühl equations we have the equality

$$1+\frac{t}{(q^3-1)(q-1)} = \frac{t}{q^2(q-1)^2(q+1)} + \frac{t}{q^4},$$

whence it follows that $t=q^4(q^3-1)(q^2-1)$ and $c=\beta_{1,d_1}=q^2(q^2+q+1)$, $b=\beta_{2,d_2}=q^4(q+1)$ and $a=\beta_{3,d_3}=(q^3-1)(q^2-1)$.

It remains to find the Betti numbers of $M_{(2)}$ and $M_{(3)}$. They are the uniform matroids $U(q^3-2,q^3)$ and $U(q^3-1,q^3)$ respectively.
We can calculate d by using the formula for MDS-codes:

$$d = \binom{n-1}{r}\binom{n}{n} = \binom{q^3-1}{q^3-2}\binom{q^3}{q^3} = q^3-1.$$

We have the equality $d+1=e$, so $e=q^3$.

As can be seen from the above we have found the following:

$$\beta_{0,q^3-q^2}(I_M) = q(q^2+q+1),$$
$$\beta_{1,q^3-q}(I_M) = q^3(q^2+q+1),$$
$$\beta_{2,q^3-1}(I_M) = q^6,$$
$$\beta_{3,q^3}(I_M) = (q^3-1)(q^2-1)(q-1),$$

$$\beta_{0,q^3-q}(I_{M_{(1)}}) = q^2(q^2+q+1),$$
$$\beta_{1,q^3-1}(I_{M_{(1)}}) = q^4(q+1),$$
$$\beta_{2,q^3}(I_{M_{(1)}}) = (q^3-1)(q^2-1),$$

$$\beta_{0,q^3-1}(I_{M_{(2)}}) = q^3,$$
$$\beta_{1,q^3}(I_{M_{(2)}}) = q^3-1,$$

$$\beta_{0,q^3}(I_{M_{(3)}}) = 1.$$

Use these Betti numbers to find the generalized weight polynomials by the formula:

$$\sum_{i=0}^{n}(-1)^i\Big(\beta_{i,j}(I_{M_{(l-1)}}) - \beta_{i,j}(I_{M_{(l)}})\Big)$$

for each $1 \leqslant j \leqslant n$. Assuming $\beta_{i,j}(I_{M_{(l)}}) = 0$ whenever $l \notin [0,4]$, we get the following coefficients of Z^l and present them in table:

Z^l	Z^0	Z^1	Z^2	Z^3	Z^4
$j=0$	1	0	0	0	0
$j=1$	0	0	0	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$j=q^3-q^2-1$	0	0	0	0	0
$j=q^3-q^2$	$-q(q^2+q+1)$	$q(q^2+q+1)$	0	0	0
$j=q^3-q^2+1$	0	0	0	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$j=q^3-q-1$	0	0	0	0	0
$j=q^3-q, q>1$	$q^3(q^2+q+1)$	$-q^2(q+1)(q^2+q+1)$	$q^2(q^2+q+1)$	0	0
$j=q^3-q+1, q>2$	0	0	0	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$j=q^3-2, q>2$	0	0	0	0	0
$j=q^3-1$	$-q^6$	$q^4(q^2+q+1)$	$-q^3(q^2+q+1)$	q^3	0
$j=q^3$	$(q^3-1)(q^2-1)(q-1)$	$-q(q^3-1)(q^2-1)$	$q^2(q^3-1)$	$-q^3$	1

Now we consider some particular case of the previous example:

Example 4.1.9. Let us find the GWP of the Reed-Müller code $\mathcal{RM}_2(1,3)$ which is a $[8,4]$ code over $\mathbb{F}_2$.

The weight hierarchy of this code is $(d_1,d_2,d_3,d_4)=(4,6,7,8)$.

The Betti numbers of M and its elongations are:

$$\beta_{0,4}(I_M)=14, \beta_{1,6}(I_M)=56, \beta_{2,7}(I_M)=64, \beta_{3,8}(I_M)=21,$$

$$\beta_{0,6}(I_{M_{(1)}})=28, \beta_{1,7}(I_{M_{(1)}})=48, \beta_{2,8}(I_{M_{(1)}})=21,$$
$$\beta_{0,7}(I_{M_{(2)}})=8, \beta_{1,8}(I_{M_{(2)}})=7,$$
$$\beta_{0,8}(I_{M_{(3)}})=1.$$

The generalized weight polynomials are presented in table:

Z^l	Z^0	Z^1	Z^2	Z^3	Z^4
$j=0$	1	0	0	0	0
$j=1$	0	0	0	0	0
$j=2$	0	0	0	0	0
$j=3$	0	0	0	0	0
$j=4$	-14	14	0	0	0
$j=5$	0	0	0	0	0
$j=6$	56	-84	28	0	0
$j=7$	-64	112	-56	8	0
$j=8$	21	-42	28	-8	1

For the matroid M corresponding to $\mathcal{RM}_q(1,3)$ we have calculated β_{1,d_1}, β_{2,d_2}, β_{3,d_3}, and β_{4,d_4}.

Remark 4.8. For each h, we have:

$$\beta_{h,d_h} = \sum_{\sigma \text{ minimal in } \mathcal{N}_h} \beta_{h,\sigma} = \beta_{h,\sigma} \cdot |\{\text{minimal elements in } \mathcal{N}_h\}|$$

if the $\beta_{h,\sigma}$ are equal for all σ minimal in $\mathcal{N}_h$.

For $h = 1$, it is clear, since $M|_\sigma \cong S^{d_1-2}$, and the $\beta_{h,\sigma}$ are computable from the reduced homology of $M|_\sigma$, using Hochster's formula given in [4]:

$$\beta_{h,\sigma}(S/I_M) = \beta_{h-1,\sigma}(I_M) = Tor^s_{h-1}(I_M,\mathbb{K})_\sigma = \tilde{h}_{d_h-h-1}(M|_\sigma).$$

Lemma 4.2. *Let $E = \mathbb{A}_q^{k-1}$, $\sigma_1, \sigma_2 \subset E$ and assume there exists an isomorphism $\phi\colon E \to E$ with $\phi(\sigma_1) = \sigma_2$ and such that $\phi(M^*|_{\sigma_1}) = M^*|_{\sigma_2}$. Then*

$$M|_{\sigma_1} \cong M|_{\sigma_2}.$$

Proof. The assumption of the lemma says precisely that: $r_{M^*|_{\sigma_2}}(\phi(\tau)) = r_{M^*|_{\sigma_1}}(\tau)$, for all $\tau \subset \sigma_1 \Leftrightarrow \phi(\tau) \subset \sigma_2$.

$$r_M(\phi(\tau)) = |\phi(\tau)| + r_{M^*}(\phi(\tau)) - r_{M^*}(E)$$

$$\begin{aligned} r_M(\phi(\tau)) &= r_{M|_{\sigma_2}}(\phi(\tau)) = \\ &= |\tau| + r_{M^*|_{\sigma_2}}(\phi(\tau)) - r_{M^*}(E) = \\ &= |\tau| + r_{M^*|_{\sigma_1}}(\tau) - r_{M^*}(E) = \\ &= |\tau| + r_{M^*}(\tau) - r_{M^*}(E) = \\ &= r_M(\tau) = r_{M|_{\sigma_1}}(\tau). \end{aligned}$$

Then it follows that $M|_{\sigma_2} \cong M|_{\sigma_1}$, which is what we set out to prove. $\square$

Recall that the σ are the complements of (codim h)-planes L_h in $\mathbb{A}^{k-1}$. Let $M|_\sigma$ is determined by a matrix H, then $(M^*)|_\sigma = (M|_\sigma)^*$ is determined by a matrix G.
For σ_1 the complement of one (codim h)-plane is H_1.
For σ_2 the complement of another (codim h)-plane is H_2.

Given independent equations (σ is the complement of a hyperplane H, which could be H_1 or H_2)

$$\begin{aligned} b_{11}X_1 + \ldots + b_{1,k-1}X_{k-1} &= 0 \\ b_{21}X_1 + \ldots + b_{2,k-1}X_{k-1} &= 0 \\ &\vdots \\ b_{h1}X_1 + \ldots + b_{h,k-1}X_{k-1} &= 0 \end{aligned}$$

σ_0 is the complement of hyperplane H_0 defined by

$$\begin{aligned} X_1 &= 0 \\ X_2 &= 0 \\ &\vdots \\ X_h &= 0 \end{aligned}$$

Let the generator matrix G, whose corresponding matroid is M^*, be

$$G = \begin{array}{c} X_0 \\ X_1 \\ \vdots \\ X_h \\ \end{array} \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \end{bmatrix}$$

We will show that all other (codim h)-planes

$$\begin{aligned} L_1(\vec{X}) &= 0 \\ L_2(\vec{X}) &= 0 \\ &\vdots \\ L_h(\vec{X}) &= 0 \end{aligned}$$

give the same matroid. We have

$$\begin{bmatrix} b_{11} & \dots & b_{1,k-1} \\ \vdots & \ddots & \vdots \\ b_{h1} & \dots & b_{h,k-1} \end{bmatrix} \begin{bmatrix} X_1 \\ \vdots \\ X_{k-1} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

We can find $k-1-h$ additional rows (choose arbitrary)

$$\begin{bmatrix} b_{h+1,1} & \dots & b_{h+1,k-1} \\ \vdots & \ddots & \vdots \\ b_{k-1,1} & \dots & b_{k-1,k-1} \end{bmatrix}.$$

such that $B = [b_{ij}]$ is a square matrix and $\det(B) \neq 0$.
Let B be the map $\mathbb{A}^{k-1} \longrightarrow \mathbb{A}^{k-1}$, where $\vec{V} \longrightarrow B\vec{V}$.
Let $\vec{V_1}, \vec{V_2}, \dots, \vec{V_s}$ be vectors in $\mathbb{A}^{k-1}$. Then these are linearly independent if and only if $B\vec{V_1}, B\vec{V_2}, \dots, B\vec{V_s}$ are linearly independent. Hence we have

$$B\vec{X} = \begin{bmatrix} L_1(\vec{X}) \\ \vdots \\ L_{k-1}(\vec{X}) \end{bmatrix}.$$

We want to know what happens to $\begin{bmatrix} 1 \\ \vec{V} \end{bmatrix}$.

$$\begin{bmatrix} 1 \\ B\vec{V} \end{bmatrix} = B' \begin{bmatrix} 1 \\ \vec{V} \end{bmatrix} \text{ for } B' = \begin{bmatrix} 1 & 0 \\ 0 & B \end{bmatrix}.$$

Then:

$$B' \begin{bmatrix} 1 \\ \vec{V} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & B \end{bmatrix} \begin{bmatrix} 1 \\ \vec{V} \end{bmatrix} = \begin{bmatrix} 1 \\ B\vec{V} \end{bmatrix}.$$

The argument with B and B' shows that there exists an isomorphism $\phi\colon E \longrightarrow E$ such that $\phi(M^*|_{\sigma_1}) = M^*|_{\sigma_2}$, where ϕ is

$$\begin{bmatrix} 1 \\ \vec{V} \end{bmatrix} \longrightarrow B' \begin{bmatrix} 1 \\ \vec{V} \end{bmatrix} \text{ and } B'\colon \sigma_1 \longrightarrow \sigma_0.$$

This induces $M^*|_{\sigma_1} \xrightarrow{\phi_1} M^*|_{\sigma_0}$.
We have the following maps

$$\begin{tikzcd} \sigma_1 \arrow[rr, "\phi_1"] \arrow[dr, "\phi"'] & & \sigma_0 \\ & \sigma_2 \arrow[ur, "\phi_2"'] & \end{tikzcd}$$

If $\phi_1(M^*|_{\sigma_1}) = M^*|_{\sigma_0}$, and $\phi_2(M^*|_{\sigma_2}) = M^*|_{\sigma_0}$, it follows that $M^*|_{\sigma_2} = \phi_2^{-1}(M^*|_{\sigma_0}) = \phi_2^{-1}(\phi_1(M^*|_{\sigma_1})) = (\phi_2^{-1} \circ \phi_1)(M^*|_{\sigma_1}) = \phi(M^*|_{\sigma_1})$. Thus we can use the previous lemma.

Corollary 4.2.

$$\tilde{h}_{d_h-h-1}(M|_\sigma) = \beta_{h,\sigma}(M) = \frac{\beta_{h,d_h}}{|\{\textit{minimal elements in } \mathcal{N}_h\}|} = \frac{\beta_{h,d_h}}{q^h \cdot \begin{bmatrix} k-1 \\ h \end{bmatrix}_q}.$$

Remark 4.9. The second equality follows from [9].

Example 4.1.10. Let us illustrate the corollary using the example 4.1.8. First we find the Gaussian binomials $q^h \cdot \begin{bmatrix} 3 \\ h \end{bmatrix}_q$.

$$\begin{aligned}
h = 1\colon &\quad q \cdot \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q = q\tfrac{q^3-1}{q-1};\\
h = 2\colon &\quad q^2 \cdot \begin{bmatrix} 3 \\ 2 \end{bmatrix}_q = q^2\tfrac{q^3-1}{q-1};\\
h = 3\colon &\quad q^3 \cdot \begin{bmatrix} 3 \\ 3 \end{bmatrix}_q = q^3.
\end{aligned}$$

When $h = 4$ the Gaussian binomial is equal to 1.

Then we have

$$\begin{aligned}
\beta_{1,\sigma}(M) &= \frac{\beta_{1,d_1}}{\frac{q(q^3-1)}{q-1}} = \frac{q(q-1)(q^2+q+1)}{q(q^3-1)} = 1,\\
\beta_{2,\sigma}(M) &= \frac{\beta_{2,d_2}}{\frac{q^2(q^3-1)}{q-1}} = \frac{q^3(q-1)(q^2+q+1)}{q^2(q^3-1)} = q,\\
\beta_{3,\sigma}(M) &= \frac{\beta_{3,d_3}}{q^3} = \frac{q^6}{q^3} = q^3,\\
\beta_{4,\sigma}(M) &= \beta_{4,d_4} = (q^3-1)(q^2-1)(q-1).
\end{aligned}$$

$$\beta_{1,\sigma}(M_{(1)}) = \frac{\beta_{1,d_1}}{\frac{q^2(q^3-1)}{q-1}} = \frac{q^2(q-1)(q^2+q+1)}{q^2(q^3-1)} = 1,$$
$$\beta_{2,\sigma}(M_{(1)}) = \frac{\beta_{2,d_2}}{q^3} = q(q+1),$$
$$\beta_{3,\sigma}(M_{(1)}) = \beta_{3,d_3} = (q^3-1)(q^2-1).$$

$$\beta_{1,\sigma}(M_{(2)}) = \frac{\beta_{1,d_1}}{q^3} = 1,$$
$$\beta_{2,\sigma}(M_{(2)}) = \beta_{2,d_2} = q^3 - 1.$$

$$\beta_{1,\sigma}(M_{(3)}) = \beta_{1,d_1} = 1.$$

The final result of this subsection gives us the formulas in order to find the Betti numbers of the Reed-Müller code of the first order.

Example 4.1.11. We are going to find the Betti numbers in general for the Reed-Müller code $\mathcal{RM}_q(1, k-1)$, and all its elongations.

Recall that the Hamming weights of $\mathcal{RM}_q(1, k-1)$ are

$$d_h = \begin{cases} 0, & \text{if } h = 0; \\ q^{k-h-1}(q^h - 1), & \text{if } h = 1, \dots, k-1; \\ q^{k-1}, & \text{if } h = k. \end{cases}$$

In order to get the β_{h,d_h} we will again apply the formula:

$$\beta_{h,d_h} = (-1)^h \cdot t \cdot \prod_{k \neq h} \frac{1}{(d_k - d_h)} \text{ where } t \in \mathbb{Q}.$$

Look at the following expression when $1 \leqslant h \leqslant k-1$

$$\frac{1}{d_i - d_h} = \begin{cases} \frac{1}{-d_h} = \frac{-1}{q^{k-h-1}(q^h-1)}, & \text{if } i = 0; \\ \frac{1}{q^{k-i-1}(q^i-1) - q^{k-h-1}(q^h-1)} = \frac{1}{q^{k-1}(q^{-h}-q^{-i})}, & \text{if } i = 1, \dots, k-1 \text{ and } i \neq h; \\ \frac{1}{q^{k-1} - q^{k-h-1}(q^h-1)} = \frac{1}{q^{k-h-1}}, & \text{if } i = k. \end{cases}$$

If $h = 0$, then $\beta_{0,d_0} = (-1)^0 \cdot t \cdot \prod_{i \neq 0} \frac{1}{(d_i - d_0)} = 1$ and it follows that

$$\begin{aligned}
t &= \prod_{h=1}^{k} d_h = \prod_{h=1}^{k-1} q^{k-h-1}(q^h-1)\cdot q^{k-1} = \\
&= \prod_{h=1}^{k-1}(q^h-1)\Big[q^{k-1+\sum_{h=1}^{k-1} k-h-1}\Big] = q^{\frac{k(k-1)}{2}}\prod_{h=1}^{k-1}(q^h-1).
\end{aligned}$$

$$\begin{aligned}
\beta_{h,d_h} &= (-1)^h\cdot t\cdot \prod_{\substack{i=0\\ i\neq h}}^{k}\frac{1}{(d_i-d_h)} = \\
&= (-1)^h\cdot q^{\frac{k(k-1)}{2}}\prod_{i=1}^{k-1}(q^i-1)\cdot\frac{(-1)}{q^{k-h-1}(q^h-1)}\cdot \\
&\quad \prod_{i=1}^{h-1}\frac{1}{q^{k-1}(q^{-h}-q^{-i})}\prod_{i=h+1}^{k-1}\frac{1}{q^{k-1}(q^{-h}-q^{-i})}\cdot\frac{1}{q^{k-h-1}}.
\end{aligned}$$

Let us deal with two last products separately:

$$\begin{aligned}
\prod_{i=1}^{h-1}\frac{1}{q^{k-1}(q^{-h}-q^{-i})} &= \prod_{i=1}^{h-1}\frac{1}{q^{k-h-1}(1-q^{h-i})} = \\
&= \frac{1}{q^{(h-1)(k-h-1)}}\prod_{s=1}^{h-1}\frac{1}{1-q^s} = \frac{(-1)^{h-1}}{q^{(h-1)(k-h-1)}}\prod_{s=1}^{h-1}\frac{1}{q^s-1}.
\end{aligned}$$

$$\begin{aligned}
\prod_{i=h+1}^{k-1}\frac{1}{q^{k-1}(q^{-h}-q^{-i})} &= \prod_{i=h+1}^{k-1}\frac{1}{q^{k-i-1}(q^{i-h}-1)} = \\
&= \prod_{t=1}^{k-h-1}\frac{1}{q^{k-t-h-1}(q^t-1)} = \frac{1}{q^{(k-h-1)^2}}\cdot\frac{\prod_{t=1}^{k-h-1}q^t}{\prod_{t=1}^{k-h-1}(q^t-1)} = \\
&= \frac{q^{\frac{(k-h-1)(k-h)}{2}}}{q^{(k-h-1)^2}}\cdot\frac{1}{\prod_{t=1}^{k-h-1}(q^t-1)} = \frac{q^{\frac{(k-h-1)(-k+h+2)}{2}}}{\prod_{t=1}^{k-h-1}(q^t-1)}.
\end{aligned}$$

Then

$$\begin{aligned}
\beta_{h,d_h} &= (-1)^h \cdot q^{\frac{k(k-1)}{2}} \prod_{i=1}^{k-1}(q^i-1) \cdot \frac{(-1)}{q^{k-h-1}(q^h-1)} \cdot \\
&\quad \frac{(-1)^{h-1}}{q^{(h-1)(k-h-1)}} \cdot \frac{1}{\prod_{s=1}^{h-1}(q^s-1)} \cdot \frac{q^{\frac{(k-h-1)(-k+h+2)}{2}}}{\prod_{t=1}^{k-h-1}(q^t-1)} \cdot \frac{1}{q^{k-h-1}} = \\
&= \frac{\prod_{i=1}^{k-1}(q^i-1)}{\prod_{i=1}^{h}(q^i-1) \cdot \prod_{i=1}^{k-h-1}(q^i-1)} \cdot q^{\frac{h^2+h}{2}} = q^{\frac{h^2+h}{2}} \cdot \begin{bmatrix} k-1 \\ h \end{bmatrix}_q .
\end{aligned}$$

We consider the case when $h = k$:

$$\begin{aligned}
\beta_{k,d_k} &= (-1)^k \cdot t \cdot \prod_{i=0}^{k-1} \frac{1}{(d_i-d_k)} = \\
&= (-1)^k \cdot q^{\frac{k(k-1)}{2}} \prod_{i=1}^{k-1}(q^i-1) \cdot \frac{(-1)}{q^{k-1}} \cdot \prod_{i=1}^{k-1} \frac{(-1)}{q^{k-i-1}} = \\
&= \frac{q^{\frac{k(k-1)}{2}} \prod_{i=1}^{k-1}(q^i-1)}{q^{(k-1)^2} \prod_{i=1}^{k-1} q^{-i} \cdot q^{k-1}} = \frac{\prod_{i=1}^{k-1}(q^i-1) \cdot q^{k(k-1)}}{q^{(k-1)^2} \cdot q^{k-1}} = \\
&= \prod_{i=1}^{k-1}(q^i-1).
\end{aligned}$$

We may also get formulas for the j-th elongation $M_{(j)}$.

$$\begin{aligned}
t &= \prod_{s=1}^{k-j} d_s(M) = \prod_{s=j+1}^{k-1} q^{k-s-1}(q^s-1) \cdot q^{k-1} = \\
&= q^{\frac{k^2+j^2-2kj+3j-k}{2}} \prod_{s=j+1}^{k-1} (q^s-1).
\end{aligned}$$

Look at the following expression when $0 < l < k-j$

$$\frac{1}{d_i-d_l} = \begin{cases} \frac{-1}{q^{k-1}-q^{k-j-1-l}}, & \text{if } i = 0; \\ \frac{1}{q^{k-j-1-l}-q^{k-j-1-i}}, & \text{if } i = 1, \ldots, k-j-1 \text{ and } i \neq l; \\ \frac{1}{q^{k-j-1-l}}, & \text{if } i = k-j. \end{cases}$$

Then

$$\begin{aligned}
\beta_{l,d_l} &= (-1)^l \cdot t \cdot \frac{(-1)}{q^{k-1} - q^{k-j-1-l}} \prod_{i=1}^{l-1} \frac{1}{q^{k-j-1-l} - q^{k-j-1-i}} \prod_{i=l+1}^{k-j-1} \frac{1}{q^{k-j-1-l} - q^{k-j-1-i}} \\
&\cdot \quad \frac{1}{q^{k-j-1-l}} = (-1)^l \cdot t \cdot \frac{(-1)}{q^{k-j-1-l}(q^{l+j}-1)} \prod_{i=1}^{l-1} \frac{1}{q^{k-j-1-l}(1-q^{l-i})} \\
&\quad \prod_{i=l+1}^{k-j-1} \frac{1}{q^{k-j-1-i}(q^{i-l}-1)} \cdot \frac{1}{q^{k-j-1-l}} = \\
&= \quad t \cdot \frac{1}{q^{k-j-1-l}(q^{l+j}-1)} \cdot \frac{1}{q^{(k-j-1-l)(l-1)}} \prod_{s=1}^{l-1} \frac{1}{(q^s-1)} \prod_{p=1}^{k-j-1-l} \frac{1}{q^p} \prod_{s=1}^{k-j-1-l} \frac{1}{(q^s-1)}.
\end{aligned}$$

We gather the powers of q:

$$\begin{aligned}
& q^{\frac{k^2+j^2-2kj+3j-k}{2}} \cdot \frac{1}{q^{(k-j-1-l)l}} \cdot \frac{1}{\prod_{p=1}^{k-j-1-l} q^p} = \\
= \quad & q^{\frac{k^2+j^2-2kj+3j-k}{2}} \cdot \frac{1}{q^{kl-jl-l-l^2+\frac{(k-j-1-l)(k-j-l)}{2}}} = \\
= \quad & q^{\frac{k^2+j^2-2kj+3j-k}{2}} \cdot \frac{1}{q^{\frac{k^2+j^2-l^2-2kj-k+j-l}{2}}} = q^{\frac{l^2+l+2j}{2}}.
\end{aligned}$$

So we have

$$\begin{aligned}
\beta_{l,d_l} \quad &= \quad q^{\frac{l^2+l+2j}{2}} \cdot \frac{\prod_{s=j+1}^{k-1}(q^s-1)}{(q^{l+j}-1)\prod_{s=1}^{l-1}(q^s-1)\prod_{s=1}^{k-j-1-l}(q^s-1)} = \\
&= \quad q^{\frac{l^2+l+2j}{2}} \cdot \frac{q^{k-1}-1}{q^{l+j}-1} \begin{bmatrix} k-2-j \\ l-1 \end{bmatrix}_q \begin{bmatrix} k-2 \\ j \end{bmatrix}_q .
\end{aligned}$$

It remains to look at the case when $l = k-j$.

$$\frac{1}{d_i - d_{k-j}} = \begin{cases} \frac{-1}{d_{k-j}} = \frac{-1}{q^{k-1}}, & \text{if } i = 0; \\ \frac{-1}{q^{k-j-1-i}}, & \text{if } i \neq k-j. \end{cases}$$

Then

$$\begin{aligned}
\beta_{k-j,d_{k-j}} &= (-1)^{k-j} \cdot t \cdot \prod_{i=1}^{k-j-1} \frac{(-1)}{q^{k-j-1-i}} \cdot \frac{(-1)}{q^{k-1}} = \\
&= (-1)^{k-j} \cdot t \cdot (-1)^{k-j+1} \cdot \prod_{m=1}^{k-j-2} \frac{1}{q^m} \cdot \frac{(-1)}{q^{k-1}} = \\
&= q^{\frac{k^2+j^2-2kj+3j-k}{2}} \prod_{s=j+1}^{k-1} (q^s - 1) \cdot \frac{1}{q^{k-1}} \cdot \frac{1}{q^{\frac{(k-j-1)(k-j-2)}{2}}} = \\
&= \prod_{s=j+1}^{k-1} (q^s - 1).
\end{aligned}$$

4.2 Another way of finding out the GWP

Definition 4.6. The generalized weight enumerator is given by

$$W_{\mathcal{C}}^{(r)}(X, Y) = \sum_{j=0}^{n} A_j^{(r)} X^{n-j} Y^j,$$

where $A_j^{(r)} = |\{\mathcal{D} \subseteq \mathcal{C} \mid \dim \mathcal{D} = r, wt(\mathcal{D}) = j\}|$.

The following results are given in [9]:

Proposition 4.8. *Let $\mathcal{C}$ be a $[n, k]$ code over $\mathbb{F}_q$. Then the generalized weight polynomial is equal to*

$$P_j(q^m) = \sum_{r=0}^{m} A_j^{(r)} \prod_{i=0}^{r-1} (q^m - q^i).$$

Theorem 4.4. *The generalized weight enumerators of the Reed-Müller code $\mathcal{RM}_q(1, k-1)$ are given by*

$$W_{\mathcal{RM}_q(1,k-1)}^{(r)}(X, Y) = \begin{bmatrix} k-1 \\ r-1 \end{bmatrix}_q Y^n + q^r \begin{bmatrix} k-1 \\ r \end{bmatrix}_q X^{q^{k-1-r}} Y^{q^{k-1} - q^{k-1-r}}$$

for $0 < r < k$.

Example 4.2.1. Look at the Reed-Müller code $\mathcal{RM}_2(1,3)$ from the example 4.1.9.
The generalized weight enumerators of this code for $0 < r < 4$ are

$$W^{(r)}_{\mathcal{RM}_2(1,3)}(X,Y) = \begin{bmatrix} 3 \\ r-1 \end{bmatrix}_2 Y^8 + 2^r \begin{bmatrix} 3 \\ r \end{bmatrix}_2 X^{2^{3-r}} Y^{2^3 - q^{3-r}}.$$

$$W^{(1)}_{\mathcal{RM}_2(1,3)}(X,Y) = \begin{bmatrix} 3 \\ 0 \end{bmatrix}_2 Y^8 + 2 \begin{bmatrix} 3 \\ 1 \end{bmatrix}_2 X^4 Y^4,$$

$$W^{(2)}_{\mathcal{RM}_2(1,3)}(X,Y) = \begin{bmatrix} 3 \\ 1 \end{bmatrix}_2 Y^8 + 4 \begin{bmatrix} 3 \\ 2 \end{bmatrix}_2 X^2 Y^6,$$

$$W^{(3)}_{\mathcal{RM}_2(1,3)}(X,Y) = \begin{bmatrix} 3 \\ 2 \end{bmatrix}_2 Y^8 + 8 \begin{bmatrix} 3 \\ 3 \end{bmatrix}_2 XY^7.$$

Then we have

$$A_0^{(0)} = 1, A_8^{(1)} = \begin{bmatrix} 3 \\ 0 \end{bmatrix}_2 = 1, A_8^{(2)} = \begin{bmatrix} 3 \\ 1 \end{bmatrix}_2 = 7, A_8^{(3)} = \begin{bmatrix} 3 \\ 2 \end{bmatrix}_2 = 7,$$

$$A_4^{(1)} = 2 \begin{bmatrix} 3 \\ 1 \end{bmatrix}_2 = 14, A_6^{(2)} = 4 \begin{bmatrix} 3 \\ 2 \end{bmatrix}_2 = 28, A_7^{(3)} = 8 \begin{bmatrix} 3 \\ 3 \end{bmatrix}_2 = 8, A_8^{(4)} = 1.$$

The generalized weight polynomials are

$$P_0(Q) = \sum_{r=0}^{m} A_0^{(r)} \prod_{i=0}^{r-1} (q^m - q^i) = 1;$$

$$P_1(Q) = P_2(Q) = P_3(Q) = 0;$$

$$P_4(Q) = \sum_{r=0}^{m} A_4^{(r)} \prod_{i=0}^{r-1} (q^m - q^i) = 14(Q-1);$$

$$P_5(Q) = 0;$$

$$P_6(Q) = \sum_{r=0}^{m} A_6^{(r)} \prod_{i=0}^{r-1} (q^m - q^i) = 28(Q-1)(Q-2);$$

$$P_7(Q) = \sum_{r=0}^{m} A_7^{(r)} \prod_{i=0}^{r-1} (q^m - q^i) = 8(Q-1)(Q-2)(Q-4);$$

$$
\begin{aligned}
P_8(Q) &= \sum_{r=0}^{m} A_8^{(r)} \prod_{i=0}^{r-1} (q^m - q^i) = (Q-1) + 7(Q-1)(Q-2) + \\
&+ 7(Q-1)(Q-2)(Q-4) + (Q-1)(Q-2)(Q-4)(Q-8) = \\
&= (Q-1)(Q^3 - 7Q^2 + 21Q - 21).
\end{aligned}
$$

4.3 Questions for further work

1. Will the resolutions of the Stanley-Reisner rings derived from Reed-Müller code of the second order (higher order) be pure?

2. Does our method of finding the GWP of codes, by using Betti numbers of associated matroids and elongations, work better than the method briefly described in Section 4.2, following [9]? There one transforms data about generalized weight enumerators over the code over the fixed alphabet $\mathbb{F}_q$, to data of the usual weights of codes over infinitely many extensions of $\mathbb{F}_q$ (the GWP). Is there any case when this method from [9] does not work, but where our method works?

Bibliography

[1] Eisenbud, D., *Commutative Algebra with a View Toward Algebraic Geometry*. Graduate Texts in Mathematics, 150. Springer-Verlag, 1995.

[2] Fløystad, G., *Boij-Söderberg theory: Introduction and survey*. Progress in Commutative Algebra, 1, De Gryiter, p. 1-54, 2012.

[3] Forney, G.D., Jr., *Dimension/Length Profiles and Trellis Complexity of Linear Block Codes*. IEEE Trans. Inform. Theory, vol. 40, no. 6, pp. 1741–1752, Nov. 1994.

[4] Herzog, J., Hibi, T., *Monomial Ideals*. Graduate Texts in Mathematics, 260. Springer-Verlag London Limited, 2011.

[5] Hill, R., *A First Course in Coding Theory*. Oxford University Press, Oxford, 1986

[6] Johnsen, T., Roksvold, J., Verdure, H., *A generalization of weight polynomials to matroids*, arXiv: 1311.6291, 2013.

[7] Johnsen, T., Verdure, H., *Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids*. Appl. Algebra Engrg. Comm. Comput. 24 (2013), no. 1, 73–93.

[8] Johnsen, T., Verdure, H., *Stanley-Reisner resolution of constant weight linear codes*, Des. Codes Cryptogr. 72(2) (2014), 471–481.

[9] Jurrius, R.P.M.J., *Weight enumeration of codes from finite spaces*, Des. Codes Cryptogr.,63, p. 321-330, 2012

[10] Larsen, A.H., *Matroider og lineære koder*, Master thesis in algebra, University of Bergen, 2005.

[11] Miller, E., Sturmfels, B., *Combinatorial Commutative Algebra*. Graduate Texts in Mathematics, 227. Springer, New York, 2005.

[12] Oxley, J., *Matroid theory*. Oxford University Press, Oxford, 1992.

[13] Tsfasman, M.A., Vladut, S.G., *Geometric Approach to Higher Weights.* IEEE Trans. Inform. Theory, vol. 41, no. 6, pp. 1564–1588, Nov. 1995.

[14] Verdure, H., *Code and Matroid Theory*. Lecture Notes, University of Tromsø, 2013.

[15] Wei, V., *Generalized Hamming weights for linear codes.* IEEE Trans. Inform. Theory 37 (1991), no. 5, 1412–1418.

UNIVERSITY OF TROMSØ