Codes, arrangements, matroids, and their polynomial links

Copyright © 2012 by Relinde Jurrius.
Unmodified copies may be freely distributed.

A catalogue record is available from the Eindhoven University of Technology Library.
ISBN: 978-90-386-3194-3

Printed by Wöhrmann Printing Service, Zutphen, The Netherlands

Codes, arrangements, matroids, and their polynomial links

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de
Technische Universiteit Eindhoven, op gezag van de
rector magnificus, prof.dr.ir. C.J. van Duijn, voor een
commissie aangewezen door het College voor
Promoties in het openbaar te verdedigen
op woensdag 29 augustus 2012 om 16.00 uur

door

Relinde Petronella Maria Johanna Jurrius

geboren te Haarlem

Dit proefschrift is goedgekeurd door de promotor:

prof.dr. H.C.A. van Tilborg

Copromotor:
dr. G.R. Pellikaan

Codes, arrangements, matroids, and their polynomial links

Many mathematical objects are closely related to each other. While studying certain aspects of a mathematical object, one tries to find a way to “view” the object in a way that is most suitable for a specific problem. Or, in other words, one tries to find the best way to model the problem. Many related fields of mathematics have evolved from one another this way. In practice, it is very useful to be able to transform a problem into other terminology: it gives a lot more available knowledge and that can be helpful to solve a problem.

This thesis deals with various closely related fields in discrete mathematics, starting from linear error-correcting codes and their weight enumerator. We can generalize the weight enumerator in two ways, to the extended and generalized weight enumerators. The set of generalized weight enumerators is equivalent to the extended weight enumerator.

Summarizing and extending known theory, we define the two-variable zeta polynomial of a code and its generalized zeta polynomial. These polynomials are equivalent to the extended and generalized weight enumerator of a code.

We can determine the extended and generalized weight enumerator using projective systems. This calculation is explicitly done for codes coming from finite projective and affine spaces: these are the simplex code and the first order Reed-Muller code. As a result we do not only get the weight enumerator of these codes, but it also gives us information on their geometric structure. This is useful information in determining the dimension of geometric designs.

To every linear code we can associate a matroid that is representable over a finite field. A famous and well-studied polynomial associated to matroids is the Tutte polynomial, or rank generating function. It is equivalent to the extended weight enumerator. This leads to a short proof of the MacWilliams relations for the extended weight enumerator.

For every matroid, its flats form a geometric lattice. On the other hand, every geometric lattice induces a simple matroid. The Tutte polynomial of a matroid determines the coboundary polynomial of the associated geometric lattice. In the case of simple matroids, this becomes a two-way equivalence.

Another polynomial associated to a geometric lattice (or, more general, to a poset) is

the Möbius polynomial. It is not determined by the coboundary polynomial, neither the other way around. However, we can give conditions under which the Möbius polynomial of a simple matroid together with the Möbius polynomial of its dual matroid defines the coboundary polynomial. The proof of these relations involves the two-variable zeta polynomial, that can be generalized from codes to matroids.

Both matroids and geometric lattices can be truncated to get an object of lower rank. The truncated matroid of a representable matroid is again representable. Truncation formulas exist for the coboundary and Möbius polynomial of a geometric lattice and the spectrum polynomial of a matroid, generalizing the known truncation formula of the Tutte polynomial of a matroid.

Several examples and counterexamples are given for all the theory. To conclude, we give an overview of all polynomial relations.

Outline and origin of research

It is common to start a thesis with a chapter that lists the necessary background information about the research topics of the thesis. Such a chapter summarizes definitions and known results that are necessary for understanding the new results. I choose to divide this background information into four chapters, treating linear codes (Chapter 1), projective systems and arrangements (Chapter 4), matroids (Chapter 7), and geometric lattices (Chapter 9). I think this outline improves readability of the thesis, especially for someone who is only interested in parts of the results.

The outline of this thesis is mainly taken from [58]. This paper gives an overview of the connections between codes, arrangements, and matroids. It originates from lecture notes for the 2009 Soria Summer School in Computational Mathematics. Since it gives a very thorough introduction to the subjects in the title, the introduction chapters on linear codes (Chapter 1) and matroids (Chapter 7) are highly condensed versions of the material in the paper. Chapter 4 on projective systems and arrangements is fairy similar to Section 4 of [58] and Chapter 9 on geometric lattices is like Section 7 of [58] but with less examples. Chapter 10 is roughly a copy of Section 8 in [58].

My research on weight enumerators and their generalizations, as well as the connection to matroids, started in the final project for my Masters degree. Chapter 2 on generalized and extended weight enumerators and Chapter 8 on the Tutte polynomial originate from my Master thesis [52]. This results were also presented at the Workshop on Coding and Cryptography [55].

Chapter 3 studies the zeta polynomial of a code and its generalizations. Most of this is a summary of known results, therefore this material is unpublished. The novelty is that it is written in the context of Chapter 2, showing clearly the close relation between the various generalizations of the zeta function and the similar generalizations of the weight enumerator. The theory is also used in Chapter 11.

Chapter 5 contains the results of my paper in *Designs, Codes and Cryptography* [53]. Chapter 6 reports on ongoing research on the coset leader weight enumerator. The first results on that topic were presented at the Symposium on Information Theory in the Benelux [56].

Most of my PhD research involves matroids and their associated polynomials. In Chapter 11 new results are explained about the relation between the Möbius and coboundary polynomial [54]. Chapter 13 contains new results on truncation [57]. Both papers will be published in a special issue of *Mathematics in Computer Science* on matroids in coding theory and related topics.

The spectrum polynomial is introduced in Chapter 12 and a concrete calculation is given. I was hoping to achieve new results on the link between the spectrum polynomial and the Tutte polynomial, but unfortunately was not able to. Therefore, Chapter 12 does not contain enough new information for publication.

Finally, in Chapter 14 an overview is given of the established polynomial links. Parts of this chapter come from [58].

New results

The new research in this thesis is published in three journal papers [53, 54, 57], two conference proceedings [55, 56] and a book chapter [58]. We summarize the new results contained in this thesis.

- A generalization of a method by Tsfasman and Vlădut to determine the generalized and extended weight enumerator.
- Establishing the two-way correspondence between the generalized and extended weight enumerator.
- An example showing that the generalized and extended weight enumerator are not enough to distinguish between codes with the same parameters.
- An overview of the relations between generalizations of the zeta function for codes introduced by Duursma and the generalized and extended weight enumerator.
- Determination of the generalized and extended weight enumerators for the q-ary Simplex codes and the q-ary first order Reed-Muller codes and a complete determination of the set of supports of subcodes and words in an extension code.
- Some preliminary results on the coset leader and list enumerator.
- Results on the connection between weight enumerators and the Tutte polynomial.
- A study of the relations between the Möbius and coboundary polynomial, including examples that show that the two polynomials do, in general, not determine each other.
- Results on the representation of the truncation of a matroid.
- A general approach to truncation formulas, leading to truncation formulas for the Möbius and spectrum polynomial.
- An overview of the relations between polynomials studied in this thesis.

Contents

Part I

Codes

1

Introduction to linear codes

The idea of *error-correcting codes* is to add redundant information to a message in such a way that it is possible to detect or even correct errors after transmission. In written language, this redundant information is already present: misspellings and typos in a text seldom lead to misinterpretation of the meaning of the text. In the sequences of zeros and ones used in digital communication, this redundant information is not automatically present.

Legend goes that Hamming was so frustrated the computer halted every time it detected an error after he handed in a stack of punch cards, he thought about a way the computer would be able not only to detect the error but also to correct it automatically. He came up with the nowadays famous code named after him. Whereas the theory of Hamming [45] is about the actual construction, the encoding and decoding of codes and uses tools from combinatorics and algebra, the approach of Shannon [84] leads to *information theory* and his theorems tell us what is and what is not possible in a probabilistic sense.

This thesis will focus on error-correcting codes as mathematical objects: we are not interested in the practical issues of encoding and decoding. Also, we will only consider *linear* codes. In this chapter we give the necessary definitions for our purpose. For a more thorough treatment of the theory of error-correcting codes, see Berlekamp [11], Blahut [16], MacWilliams and Sloan [70], or Van Lint [98].

1.1 Linear codes

Definition 1.1. Let q be a prime power, and let $\mathbb{F}_q$ be the finite field with q elements. A linear subspace of $\mathbb{F}_q^n$ of dimension k is called a *linear* $[n, k]$ *code* and is usually denoted by C. The elements of the code are called *(code)words*.

A code can be given by writing down all elements, but because the code is a linear subspace, it has a basis.

Definition 1.2. A *generator matrix* of a linear $[n, k]$ code C is a $k \times n$ matrix of full rank over $\mathbb{F}_q$ whose rows form a basis of C. It is usually denoted by G.

Note that this matrix is not unique. We can rewrite the definition of a code in terms of the generator matrix:

$$C = \{\mathbf{m}G : \mathbf{m} \in \mathbb{F}_q^k\}.$$

A second way to describe a linear code is not by its basis, but as the null space of a matrix.

DEFINITION 1.3. A *parity check matrix* of a linear $[n, k]$ code C is an $(n-k) \times n$ matrix of full rank over $\mathbb{F}_q$ such that C is the null space of this matrix. It is usually denoted by H.

Like the generator matrix, the parity check matrix is not unique. We can rewrite the definition of a code in terms of the parity check matrix:

$$C = \{\mathbf{c} \in \mathbb{F}_q^n : H\mathbf{c}^T = \mathbf{0}\}.$$

We will assume all our codes to be *nondegenerate*: there are no coordinates that are zero for all codewords, i.e., the generator matrix does not contain any zero columns.

1.2 Weight distributions

For a vector $\mathbf{x} \in \mathbb{F}_q^n$ the *support* is the set indexing its nonzero coordinates. The *(Hamming) weight* is the number of nonzero coordinates of the vector, i.e., the size of its support. So, the zero vector has weight 0 and the maximum possible weight is n. The *(Hamming) distance* between two vectors is the number of coordinates where the vectors differ. In a linear code C the minimum of all nonzero distances between codewords is called the *minimum distance*. Because C is assumed to be linear, this is equal to the minimum nonzero weight of the code. We summarize all this in the following definition:

DEFINITION 1.4. Let C be a linear $[n, k]$ code and let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$. Then we define

$$\begin{aligned} \mathrm{supp}(\mathbf{x}) &= \{i : x_i \neq 0\}, \\ \mathrm{wt}(\mathbf{x}) &= |\mathrm{supp}(\mathbf{x})|, \\ d(\mathbf{x}, \mathbf{y}) &= |\{i : x_i \neq y_i\}|, \\ d &= \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\} \\ &= \min\{\mathrm{wt}(\mathbf{x}) : \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}. \end{aligned}$$

The number of codewords $\mathbf{c} \in C$ with $\mathrm{wt}(\mathbf{c}) = w$ is denoted by A_w. Note that $A_0 = 1$ and that d is the smallest $w > 0$ for which $A_w > 0$. The numbers A_w for all $0 \leq w \leq n$ form the *weight distribution* of the code. They also form the coefficients of the *weight enumerator*:

DEFINITION 1.5. The (homogeneous) weight enumerator of a linear $[n, k]$ code C is the polynomial

$$W_C(X, Y) = \sum_{w=0}^{n} A_w X^{n-w} Y^w.$$

Another way to define the weight enumerator is

$$W_C(X, Y) = \sum_{\mathbf{c} \in C} X^{n-\mathrm{wt}(\mathbf{c})} Y^{\mathrm{wt}(\mathbf{c})}.$$

We will always use this homogeneous form of the weight enumerator. There is also the one-variable form, $W_C(Z)$, which is connected to the homogeneous form via $W_C(X, Y) = X^n W_C(YX^{-1})$ and $W_C(Z) = W_C(1, Z)$.

1.3 Duality

Let $< \, , \, >$ be the inner product on $\mathbb{F}_q^n$ given by the symmetric linear form $< \mathbf{x}, \mathbf{y} >= \sum_{i=1}^n x_i y_i$. Then the *dual code* of a linear $[n,k]$ code C over $\mathbb{F}_q$ is the subspace of $\mathbb{F}_q^n$ orthogonal to C with respect to $< \, , \, >$.

DEFINITION 1.6. Let C be a linear $[n,k]$ code over $\mathbb{F}_q$. Then the dual code is

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_q^n : < \mathbf{x}, \mathbf{c} >= 0 \text{ for all } \mathbf{c} \in C\}.$$

It is clear that the dual code is again a linear code of length n over $\mathbb{F}_q$ and has dimension $n-k$. Furthermore, $(C^\perp)^\perp = C$.

THEOREM 1.7. *Let C be a linear $[n,k]$ code over $\mathbb{F}_q$ with generator matrix G. Then $C^\perp$ is a linear $[n, n-k]$ code with parity check matrix G.*

PROOF. By definition, C is the row space of G. Since $C^\perp$ is the subspace orthogonal to C, it is the null space of G. Hence G is a parity check matrix for $C^\perp$. □

The minimum distance of the dual code is usually denoted by $d^\perp$. It is not determined by the minimum distance of the code itself. However, the weight enumerators of C and $C^\perp$ do determine each other.

THEOREM 1.8 (MacWilliams). *Let C be a linear $[n,k]$ code over $\mathbb{F}_q$. Then*

$$W_{C^\perp}(X,Y) = q^{-k} W_C(X + (q-1)Y, X - Y).$$

PROOF. See [70, Theorem 5.2.1] for a proof for binary codes. A general proof will be given via matroids in Theorem 2.19. □

1.4 MDS codes

The following proposition gives a method to determine the minimum distance of a code by looking at linear dependencies between the columns of a parity check matrix.

PROPOSITION 1.9. *Let H be a parity check matrix of a code C. Then the minimum distance d of C is the smallest integer d such that there are d columns of H that are linearly dependent.*

PROOF. Let $\mathbf{h}_1, \ldots, \mathbf{h}_n$ be the columns of H. Let $\mathbf{c}$ be a nonzero codeword of weight w. Let $\text{supp}(\mathbf{c}) = \{j_1, \ldots, j_w\}$ with $1 \leq j_1 < \ldots < j_w \leq n$. Then $H\mathbf{c}^T = 0$, so $c_{j_1}\mathbf{h}_{j_1} + \ldots + c_{j_w}\mathbf{h}_{j_w} = 0$ with $c_{j_i} \neq 0$ for all $i = 1, \ldots, w$. Therefore, the columns $\mathbf{h}_{j_1}, \ldots, \mathbf{h}_{j_w}$ are dependent.
Conversely, if $\mathbf{h}_{j_1}, \ldots, \mathbf{h}_{j_w}$ are dependent, then there exist constants $a_1, \ldots, a_w$, not all zero, such that $a_1\mathbf{h}_{j_1} + \ldots + a_w\mathbf{h}_{j_w} = 0$. Let $\mathbf{c}$ be the word defined by $c_j = 0$ if $j \neq j_i$ for all i, and $c_j = a_i$ if $j = j_i$ for some i. Then $H\mathbf{c}^T = 0$, hence $\mathbf{c}$ is a nonzero codeword of weight at most w. □

With this proposition, we can prove the following important bound for linear codes.

THEOREM 1.10 (Singleton bound). *Let C be a linear $[n, k]$ code over $\mathbb{F}_q$. Then $d \leq n - k + 1$.*

PROOF. Let H be a parity check matrix of C. This is an $(n - k) \times n$ matrix of rank $n - k$. The minimum distance of C is the smallest integer d such that H has d linearly dependent columns, by Proposition 1.9. This means that every $d - 1$ columns of H are linearly independent. Hence, the column rank of H is at least $d - 1$. By the fact that the column rank of a matrix is equal to the row rank, we have $n - k \geq d - 1$. This implies the Singleton bound. □

DEFINITION 1.11 (MDS code). A linear $[n, k]$ code C is called *maximum distance separable* if it achieves the Singleton bound, i.e., if $d = n - k + 1$.

THEOREM 1.12. *The dual of an MDS code is also an MDS code, with $d^\perp = k + 1$.*

PROOF. Let C be an MDS code and let H be a parity check matrix for C. The Singleton bound for the dual code $C^\perp$ tells us that $d^\perp \leq k + 1$. Suppose we have a word $\mathbf{c} \in C^\perp$ of weight w with $0 < w \leq k$. Then at least $n - k$ coordinates of $\mathbf{c}$ are zero. Take any $n - k$ of these coordinates, and let H' be the $(n - k) \times (n - k)$ submatrix of H consisting of the columns corresponding to these coordinates. The row rank of H' is strictly less than $n - k$, because a linear combination of them gives the chosen $n - k$ zero coordinates of $\mathbf{c}$. This means the column rank of H' is also strictly less then $n - k$. Hence we have found $n - k$ linearly dependent columns in H. But since $d = n - k + 1$, this contradicts Proposition 1.9. Therefore, there can not be a word of weight $0 < w \leq k$ in $C^\perp$, so $d^\perp = k + 1$ and $C^\perp$ is an MDS code. □

1.5 Cosets and syndromes

We define the distance between a vector $\mathbf{x} \in \mathbb{F}_q^n$ and the code C as the minimum of all distances between $\mathbf{x}$ and a codeword in C, so $d(C, \mathbf{x}) = \min\{d(\mathbf{c}, \mathbf{x}) : \mathbf{c} \in C\}$.

DEFINITION 1.13. The *covering radius* $\rho(C)$ of C is the maximum possible distance a vector $\mathbf{x} \in \mathbb{F}_q^n$ can have to the code. In other words, it is the smallest ρ such that $d(C, \mathbf{x}) \leq \rho$ for all $\mathbf{x} \in \mathbb{F}_q^n$.

Let $\mathbf{x}$ be a vector in $\mathbb{F}_q^n$. We call the set $\mathbf{x} + C = \{\mathbf{x} + \mathbf{c} : \mathbf{c} \in C\}$ the *coset* of $\mathbf{x}$ with respect to C. If $\mathbf{x}$ is a codeword, the coset is equal to the code itself. If $\mathbf{x}$ is not a codeword, the coset is not a linear subspace.

DEFINITION 1.14. A *coset leader* of $\mathbf{x} + C$ is an element of minimal weight in the coset $\mathbf{x} + C$.

The coset leader of the coset $\mathbf{x} + C$ is unique if $d(C, \mathbf{x}) \leq (d - 1)/2$. If $\rho(C)$ is the covering radius of the code, then there is at least one codeword $\mathbf{c}$ such that $d(\mathbf{c}, \mathbf{x}) \leq \rho(C)$. Hence the weight of a coset leader is at most $\rho(C)$.

We know we can write a linear code as the nullspace of its parity check matrix: $H\mathbf{c}^T = \mathbf{0}$ for all words $\mathbf{c} \in C$. For a vector $\mathbf{x} \in \mathbb{F}_q^n$ that is not in C, $H\mathbf{x}^T$ is not zero.

Definition 1.15. Let C be a linear $[n,k]$ code with parity check matrix H. For every $\mathbf{x} \in \mathbb{F}_q^n$, we call $\mathbf{s} = H\mathbf{x}^T$ the *syndrome* of $\mathbf{x}$. The syndrome is zero if and only if $\mathbf{x}$ is a codeword.

Note that all vectors in a coset $\mathbf{x} + C$ have the same syndrome $\mathbf{s} = H\mathbf{x}^T$, since for all codewords $\mathbf{c}$ we have $H(\mathbf{x}+\mathbf{c})^T = H\mathbf{x}^T + H\mathbf{c}^T = \mathbf{s} + \mathbf{0} = \mathbf{s}$.

1.6 Equivalence

We will now define what it means for two codes to be equivalent. There are several ways to do this. The most easy one is to call two linear $[n,k]$ codes over $\mathbb{F}_q$ equivalent if they are equal, i.e., if the row space of their generator matrices is the same. We are giving a more general definition, in order to let equivalent codes coincide with equivalent matroids and projective systems.

Definition 1.16. Two linear $[n,k]$ codes over $\mathbb{F}_q$ are called *equivalent* if their generator matrices are the same up to

- left multiplication with an invertible $k \times k$ matrix over $\mathbb{F}_q$;
- permutation of the columns;
- multiplication of columns with an element of $\mathbb{F}_q^*$.

The last property is sometimes referred to as *generalized equivalence* or *monomial equivalence*. Note that two equivalent codes have the same weight distribution.

1.7 Gaussian binomials and other products

The following definition is not directly related to linear codes, but we will use it mainly in the theory about weight enumerators of linear codes.

Definition 1.17. We introduce the following notations:

$$\begin{aligned} [m,r]_q &= \prod_{i=0}^{r-1}(q^m - q^i), \\ \langle r\rangle_q &= [r,r]_q, \\ \begin{bmatrix} k \\ r \end{bmatrix}_q &= \frac{[k,r]_q}{\langle r\rangle_q}. \end{aligned}$$

The first number is equal to the number of $m \times r$ matrices of rank r over $\mathbb{F}_q$. The second is the number of bases of $\mathbb{F}_q^r$. The third number is the *Gaussian binomial* and it represents the number of r-dimensional subspaces of $\mathbb{F}_q^k$. The following useful relation can easily be verified from the definitions:

$$[m,r]_q = \frac{q^{-r(m-r)}\langle m\rangle_q}{\langle m-r\rangle_q}.$$

2

The extended and generalized weight enumerator

The weight enumerator is an important and well-studied polynomial. Besides its intrinsic importance as a mathematical object, it is used in the probability treatment of codes. For example, the weight enumerator of a binary code is very useful if we want to study the probability that a received message is closer to a different codeword than to the codeword sent. (Or, rephrased: the probability that a maximum likelihood decoder makes a decoding error.) This chapter treats two generalizations of the weight enumerator of a linear code, how to compute them, and the connections between them. Most of the material in this chapter comes from [52] and [55].
The notion of the generalized weight enumerator was first introduced by Helleseth, Kløve and Mykkeltveit [49, 61] and later studied by Wei [101]. See also Simonis [85]. This notion has applications in the wire-tap channel II [78] and trellis complexity [42]. The weight enumerator of extension codes has been studied for example by Kløve [61], but never in the form of the extended weight enumerator. We generalize the method of Tsfasman and Vlădut [92] to determine the generalized and extended weight enumerator.

2.1 Generalized weight enumerators

Instead of looking at words of C, we consider all the subcodes of C of a certain dimension r. We say that the *support of a subcode* is equal to the union of all the supports of words in the subcode. The coordinates that are not in the support of the subcode are zero for all the words in the subcode. The *weight of a subcode* (also called the *effective length* or *support weight*) is the size of its support. The smallest weight for which a subcode of dimension r exists is called the r*-th generalized Hamming weight* of C. To summarize:

Definition 2.1. Let D be an r-dimensional subcode of a linear $[n, k]$ code C. Then we define

$$\begin{aligned} \mathrm{supp}(D) &= \bigcup_{\mathbf{c}\in D} \mathrm{supp}(\mathbf{c}), \\ \mathrm{wt}(D) &= |\mathrm{supp}(D)|, \\ d_r &= \min\{\mathrm{wt}(D) : D \subseteq C \text{ subcode}, \dim D = r\}. \end{aligned}$$

Note that $d_0 = 0$ and $d_1 = d$, the minimum distance of the code. If the code is nondegenerate, then $d_k = n$. We list two important facts about the generalized Hamming weights. The first theorem was proved in [101] and [61], the second theorem follows directly from the first and Theorem 1.10.

Theorem 2.2. *The generalized Hamming weights form a strictly increasing sequence, that is:*

$$d_0 < d_1 < d_2 < \ldots < d_k.$$

Theorem 2.3 (Generalized Singleton bound). *Let C be a linear $[n,k]$ code over $\mathbb{F}_q$. Then $d_r \leq n-k+r$.*

An MDS code attains the generalized Singleton bound for all $0 \leq r \leq k$ because of Theorem 2.2.

The number of subcodes with a given weight w and dimension r is denoted by $A_w^{(r)}$. Together they form the r*-th generalized weight distribution* of the code. Just as with the ordinary weight distribution, we can define a polynomial with the distribution as coefficients: the *generalized weight enumerator*.

Definition 2.4. For $0 \leq r \leq k$ the r-th generalized weight enumerator is given by

$$W_C^{(r)}(X,Y) = \sum_{w=0}^{n} A_w^{(r)} X^{n-w} Y^w,$$

where $A_w^{(r)} = |\{D \subseteq C \text{ subcode} : \dim D = r, \text{wt}(D) = w\}|$.

We can see from this definition that $A_0^{(0)} = 1$ and $A_0^{(r)} = 0$ for all $0 < r \leq k$. Furthermore, every 1-dimensional subspace of C contains $q-1$ nonzero codewords, so $(q-1)A_w^{(1)} = A_w$ for $0 < w \leq n$. This means we can find back the original weight enumerator by using

$$W_C(X,Y) = W_C^{(0)}(X,Y) + (q-1)W_C^{(1)}(X,Y).$$

The following notations are introduced to find a formalism for the computation of the weight enumerator. This method is based on Katsman and Tsfasman [60]. Later we will encounter two more methods: by matroids and the Tutte polynomial in Chapter 8 and by geometric lattices and the characteristic polynomial in Chapter 10.

Definition 2.5. For a subset J of $[n] := \{1,2,\ldots,n\}$ define

$$\begin{array}{rcl} C(J) & = & \{\mathbf{c} \in C : c_j = 0 \text{ for all } j \in J\}, \\ l(J) & = & \dim C(J). \end{array}$$

Thus the subcode $C(J)$ is the code C shortened by J, and embedded in $\mathbb{F}_q^n$ again. We give two lemmas about the determination of $l(J)$ that will become useful later.

Lemma 2.6. *Let C be a linear $[n,k]$ code with generator matrix G. Let $J \subseteq [n]$ and $|J| = t$. Let G_J be the $k \times t$ submatrix of G formed by the columns of G indexed by J, and let $r(J)$ be the rank of G_J. Then the dimension $l(J)$ is equal to $k - r(J)$.*

Proof. Let C_J be the code generated by G_J. Consider the projection map $\pi : C \to \mathbb{F}_q^t$ given by deleting the coordinates that are not indexed by J. Then π is a linear map, the image of C under π is C_J and the kernel is $C(J)$ by definition. It follows that $\dim C_J + \dim C(J) = \dim C$. So, $l(J) = k - r(J)$. □

Lemma 2.7. *Let d and $d^\perp$ be the minimum distance of C and $C^\perp$, respectively. Let $J \subseteq [n]$ and $|J| = t$. Then*

$$l(J) = \begin{cases} k-t, & \textit{for all } t < d^\perp, \\ 0, & \textit{for all } t > n-d. \end{cases}$$

Proof. Let $t > n-d$ and let $\mathbf{c} \in C(J)$. Then J is contained in the complement of $\mathrm{supp}(\mathbf{c})$, so $t \leq n - \mathrm{wt}(\mathbf{c})$. It follows that $\mathrm{wt}(\mathbf{c}) \leq n - t < d$, so $\mathbf{c}$ is the zero word and therefore $l(J) = 0$.
Let G be a generator matrix for C, then G is also a parity check matrix for $C^\perp$. We saw in Lemma 2.6 that $l(J) = k - r(J)$, where $r(J)$ is the rank of the matrix formed by the columns of G indexed by J. Let $t < d^\perp$, then every t-tuple of columns of G is linearly independent by Proposition 1.9, so $r(J) = t$ and $l(J) = k - t$. □

Note that by the Singleton bound we have $d^\perp \leq n-(n-k)+1 = k+1$ and $n-d \geq k-1$, so for $t = k$ both of the above cases apply. This is no problem, because if $t = k$ then $k - t = 0$. We furthermore introduce the following:

Definition 2.8. For $J \subseteq [n]$ and $r \geq 0$ an integer we define:

$$\begin{aligned} B_J^{(r)} &= |\{D \subseteq C(J) : D \text{ subspace of dimension } r\}|, \\ B_t^{(r)} &= \sum_{|J|=t} B_J^{(r)}. \end{aligned}$$

Note that $B_J^{(r)} = \begin{bmatrix} l(J) \\ r \end{bmatrix}_q$. For $r = 0$ this gives $B_t^{(0)} = \binom{n}{t}$. Therefore, we see that in general $l(J) = 0$ does not imply $B_J^{(r)} = 0$, because $\begin{bmatrix} 0 \\ 0 \end{bmatrix}_q = 1$. But if $r \neq 0$, we do have that $l(J) = 0$ implies $B_J^{(r)} = 0$ and $B_t^{(r)} = 0$.

Proposition 2.9. *Let r be an integer. Let d_r be the r-th generalized Hamming weight of C, and $d^\perp$ the minimum distance of the dual code $C^\perp$. Then we have*

$$B_t^{(r)} = \begin{cases} \binom{n}{t} \begin{bmatrix} k-t \\ r \end{bmatrix}_q & \textit{for all } t < d^\perp \\ 0 & \textit{for all } t > n - d_r. \end{cases}$$

Proof. The first case is a direct corollary of Lemma 2.7, since there are $\binom{n}{t}$ subsets $J \subseteq [n]$ with $|J| = t$. The proof of the second case goes analogously to the proof of the same lemma: let $|J| = t$, $t > n - d_r$ and suppose there is a subspace $D \subseteq C(J)$ of dimension r. Then J is contained in the complement of $\mathrm{supp}(D)$, so $t \leq n - \mathrm{wt}(D)$. It follows that $\mathrm{wt}(D) \leq n - t < d_r$, which is impossible, so such a D does not exist. So, $B_J^{(r)} = 0$ for all J with $|J| = t$ and $t > n - d_r$ and therefore $B_t^{(r)} = 0$ for $t > n - d_r$. □

We can check that the formula is well-defined: if $t < d^\perp$ then $l(J) = k - t$. If also $t > n - d_r$, we have $t > n - d_r \geq k - r$ by the generalized Singleton bound. This implies

$r > k - t = l(J)$, so $\begin{bmatrix} k-t \\ r \end{bmatrix}_q = 0$. The relation between $B_t^{(r)}$ and $A_w^{(r)}$ becomes clear in the next proposition.

PROPOSITION 2.10. *The following formula holds:*

$$B_t^{(r)} = \sum_{w=0}^{n} \binom{n-w}{t} A_w^{(r)}.$$

PROOF. We will count the elements of the set

$$\mathcal{B}_t^{(r)} = \{(D, J) : J \subseteq [n], |J| = t, D \subseteq C(J) \text{ subspace of dimension } r\}$$

in two different ways. For each J with $|J| = t$ there are $B_J^{(r)}$ pairs (D, J) in $\mathcal{B}_t^{(r)}$, so the total number of elements in this set is $\sum_{|J|=t} B_J^{(r)} = B_t^{(r)}$. On the other hand, let D be an r-dimensional subcode of C with $\mathrm{wt}(D) = w$. There are $A_w^{(r)}$ possibilities for such a D. If we want to find a J such that $D \subseteq C(J)$, we have to pick t coordinates from the $n - w$ all-zero coordinates of D. Summation over all w proves the given formula. □

Note that because $A_w^{(r)} = 0$ for all $w < d_r$, we can start summation at $w = d_r$. We can end summation at $w = n - t$ because for $t > n - w$ we have $\binom{n-w}{t} = 0$. Therefore, the formula can be rewritten as

$$B_t^{(r)} = \sum_{w=d_r}^{n-t} \binom{n-w}{t} A_w^{(r)}.$$

In practice, we will often prefer the summation given in the proposition.

THEOREM 2.11. *The generalized weight enumerator is given by:*

$$W_C^{(r)}(X, Y) = \sum_{t=0}^{n} B_t^{(r)} (X - Y)^t Y^{n-t}.$$

PROOF. By using the previous proposition, changing the order of summation and using the binomial expansion of $X^{n-w} = ((X - Y) + Y)^{n-w}$ we have

$$\begin{aligned}
\sum_{t=0}^{n} B_t^{(r)} (X - Y)^t Y^{n-t} &= \sum_{t=0}^{n} \sum_{w=0}^{n} \binom{n-w}{t} A_w^{(r)} (X - Y)^t Y^{n-t} \\
&= \sum_{w=0}^{n} A_w^{(r)} \left(\sum_{t=0}^{n-w} \binom{n-w}{t} (X - Y)^t Y^{n-w-t} \right) Y^w \\
&= \sum_{w=0}^{n} A_w^{(r)} X^{n-w} Y^w \\
&= W_C^{(r)}(X, Y).
\end{aligned}$$

In the second step, we can let the summation over t run up to $n - w$ instead of n because $\binom{n-w}{t} = 0$ for $t > n - w$. □

It is possible to determine the $A_w^{(r)}$ directly from the $B_t^{(r)}$, by using the next proposition.

Proposition 2.12. *The following formula holds:*

$$A_w^{(r)} = \sum_{t=n-w}^{n-d_r} (-1)^{n+w+t} \binom{t}{n-w} B_t^{(r)}.$$

Proof. For $w < d_r$ the summation is empty, which gives the correct formula $A_w^{(r)} = 0$. For $w \geq d_r$ we rewrite the generalized weight enumerator in the form of Theorem 2.11. By using the binomial expansion of $(X-Y)^t$, substituting $w = n-t+j$, and changing the order of summation we find that

$$\begin{aligned} W_C^{(r)}(X,Y) &= \sum_{t=0}^{n-d_r} B_t^{(r)} (X-Y)^t Y^{n-t} \\ &= \sum_{t=0}^{n-d_r} B_t^{(r)} \left(\sum_{j=0}^{t} \binom{t}{j} (-1)^j X^{t-j} Y^j \right) Y^{n-t} \\ &= \sum_{t=0}^{n-d_r} \sum_{w=n-t}^{n} B_t^{(r)} \binom{t}{t-n+w} (-1)^{w+t-n} X^{n-w} Y^w \\ &= \sum_{w=d_r}^{n} \sum_{t=n-w}^{n-d_r} (-1)^{n+w+t} \binom{t}{n-w} B_t^{(r)} X^{n-w} Y^w. \end{aligned}$$

The given formula follows from comparing with Definition 2.4 of the generalized weight enumerator. □

Note that, like in Proposition 2.10, we can take the summation up to n instead of $n-d_r$, because $B_t^{(r)} = 0$ for $t < n-d_r$ by Proposition 2.9.

2.2 Extended weight enumerator

Let G be the generator matrix of a linear $[n,k]$ code C over $\mathbb{F}_q$. Then we can form the $[n,k]$ code $C \otimes \mathbb{F}_{q^m}$ over $\mathbb{F}_{q^m}$ by taking all $\mathbb{F}_{q^m}$-linear combinations of the codewords in C. We call this the *extension code* of C over $\mathbb{F}_{q^m}$. We denote the number of codewords in $C \otimes \mathbb{F}_{q^m}$ of weight w by $A_{C\otimes\mathbb{F}_{q^m},w}$. We can determine the weight enumerator of such an extension code by using only the code C.

By embedding its entries in $\mathbb{F}_{q^m}$, we find that G is also a generator matrix for the extension code $C \otimes \mathbb{F}_{q^m}$. In Lemma 2.6 we saw that $l(J) = k - r(J)$. Because $r(J)$ is independent of the extension field $\mathbb{F}_{q^m}$, we have $\dim_{\mathbb{F}_q} C(J) = \dim_{\mathbb{F}_{q^m}} (C \otimes \mathbb{F}_{q^m})(J)$. This motivates the usage of U as a variable for q^m in the next definition.

Definition 2.13. Let C be a linear code over $\mathbb{F}_q$. Then we define

$$\begin{aligned} B_J(U) &= U^{l(J)} - 1, \\ B_t(U) &= \sum_{|J|=t} B_J(U). \end{aligned}$$

The *extended weight enumerator* is given by

$$W_C(X,Y,U) = X^n + \sum_{t=0}^{n} B_t(U)(X-Y)^t Y^{n-t}.$$

Note that $B_J(q^m)$ is the number of nonzero codewords in $(C \otimes \mathbb{F}_{q^m})(J)$.

PROPOSITION 2.14. *Let d and $d^\perp$ be the minimum distance of C and $C^\perp$ respectively. Then we have*

$$B_t(U) = \begin{cases} \binom{n}{t}(U^{k-t}-1) & \text{for all } t < d^\perp \\ 0 & \text{for all } t > n-d. \end{cases}$$

PROOF. The proof is similar to the proof of Proposition 2.9 and is a direct consequence of Lemma 2.7. For $t < d^\perp$ we have $l(J) = k-t$, so $B_J(U) = U^{k-t}-1$ and $B_t(U) = \binom{n}{t}(U^{k-t}-1)$. For $t > n-d$ we have $l(J) = 0$, so $B_J(U) = 0$ and $B_t(U) = 0$. □

THEOREM 2.15. *The following holds:*

$$W_C(X,Y,U) = \sum_{w=0}^{n} A_w(U) X^{n-w} Y^w$$

with $A_w(U) \in \mathbb{Z}[U]$ given by $A_0(U) = 1$ and

$$A_w(U) = \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(U)$$

for $0 < w \leq n$.

PROOF. Note that $A_w(U) = 0$ for $0 < w < d$ because the summation is empty. By substituting $w = n-t+j$ and reversing the order of summation, we have

$$\begin{aligned} W_C(X,Y,U) &= X^n + \sum_{t=0}^{n} B_t(U)(X-Y)^t Y^{n-t} \\ &= X^n + \sum_{t=0}^{n} B_t(U) \left(\sum_{j=0}^{t} \binom{t}{j} (-1)^j X^{t-j} Y^j \right) Y^{n-t} \\ &= X^n + \sum_{t=0}^{n} \sum_{j=0}^{t} (-1)^j \binom{t}{j} B_t(U) X^{t-j} Y^{n-t+j} \\ &= X^n + \sum_{t=0}^{n} \sum_{w=n-t}^{n} (-1)^{t-n+w} \binom{t}{t-n+w} B_t(U) X^{n-w} Y^w \\ &= X^n + \sum_{w=0}^{n} \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(U) X^{n-w} Y^w. \end{aligned}$$

Since the second term is zero for $w = 0$, we see that $W_C(X,Y,U)$ is of the form $\sum_{w=0}^{n} A_w(U) X^{n-w} Y^w$ with $A_w(U)$ of the form given in the theorem. □

Note that in the definition of $A_w(U)$ we can let the summation over t run up to $n-d$ instead of n, because $B_t(U)=0$ for $t>n-d$.

PROPOSITION 2.16. *The following formula holds:*

$$B_t(U)=\sum_{w=d}^{n-t}\binom{n-w}{t}A_w(U).$$

PROOF. We start with the extended weight enumerator in the form of Theorem 2.15 and then rewrite as follows.

$$\begin{aligned}
W_C(X,Y,U) &= X^n+\sum_{w=d}^{n}A_w(U)((X-Y)+Y)^{n-w}Y^w\\
&= X^n+\sum_{w=d}^{n}A_w(U)\left(\sum_{t=0}^{n-w}\binom{n-w}{t}(X-Y)^tY^{n-w-t}\right)Y^w\\
&= X^n+\sum_{w=d}^{n}\sum_{t=0}^{n-w}A_w(U)\binom{n-w}{t}(X-Y)^tY^{n-t}\\
&= X^n+\sum_{t=0}^{n}\sum_{w=d}^{n-t}\binom{n-w}{t}A_w(U)(X-Y)^tY^{n-t}
\end{aligned}$$

The given formula follows from comparing with Definition 2.13 of the extended weight enumerator. □

Note that, unlike in Proposition 2.10, we can not let the summation start at $w=0$. This is because $A_w(U)=1\neq 0$. We can let the summation run up to $w=n$, because the binomial is zero for $w>n-t$.

As we said before, the motivation for looking at the extended weight enumerator comes from the extension codes. In the next proposition we show that the extended weight enumerator for $U=q^m$ is indeed the weight enumerator of the extension code $C\otimes\mathbb{F}_{q^m}$.

PROPOSITION 2.17. *Let C be a linear $[n,k]$ code over $\mathbb{F}_q$. Then we have*

$$W_C(X,Y,q^m)=W_{C\otimes\mathbb{F}_{q^m}}(X,Y).$$

PROOF. For $w=0$ it is clear that $A_0(q^m)=A_{C\otimes\mathbb{F}_{q^m},0}=1$, so assume $w\neq 0$. It is enough to show that $A_w(q^m)=(q^m-1)A^{(1)}_{C\otimes\mathbb{F}_{q^m},w}$. First we have

$$\begin{aligned}
B_t(q^m) &= \sum_{|J|=t}B_J(q^m)\\
&= \sum_{|J|=t}|\{\mathbf{c}\in(C\otimes\mathbb{F}_{q^m})(J):\mathbf{c}\neq 0\}|\\
&= (q^m-1)\sum_{|J|=t}|\{D\subseteq(C\otimes\mathbb{F}_{q^m})(J):\dim D=1\}\\
&= (q^m-1)B_t^{(1)}(C\otimes\mathbb{F}_{q^m}).
\end{aligned}$$

We also know that $A_w(U)$ and $B_t(U)$ are related the same way as $A_w^{(1)}$ and $B_t^{(1)}$. Combining this proves the statement. □

Because of Proposition 2.17 we can interpret $W_C(X,Y,U)$ as the weight enumerator of the extension code over the algebraic closure of $\mathbb{F}_q$. For further applications, the next way of writing the extended weight enumerator will be useful.

PROPOSITION 2.18. *The extended weight enumerator of a linear code C can be written as*

$$W_C(X,Y,U) = \sum_{t=0}^{n} \sum_{|J|=t} U^{l(J)}(X-Y)^t Y^{n-t}.$$

PROOF. By rewriting and using the binomial expansion of $((X-Y)+Y)^n$, we get

$$\begin{aligned}
&\sum_{t=0}^{n} \sum_{|J|=t} U^{l(J)}(X-Y)^t Y^{n-t} \\
&= \sum_{t=0}^{n}(X-Y)^t Y^{n-t} \sum_{|J|=t} \left((U^{l(J)}-1)+1\right) \\
&= \sum_{t=0}^{n}(X-Y)^t Y^{n-t} \left(\sum_{|J|=t} (U^{l(J)}-1) + \binom{n}{t}\right) \\
&= \sum_{t=0}^{n} B_t(U)(X-Y)^t Y^{n-t} + \sum_{t=0}^{n} \binom{n}{t}(X-Y)^t Y^{n-t} \\
&= \sum_{t=0}^{n} B_t(U)(X-Y)^t Y^{n-t} + X^n \\
&= W_C(X,Y,U).
\end{aligned}$$

□

The MacWilliams identity we saw in Theorem 1.8 can be extended to the extended weight enumerator. We will give the proof of this theorem in Section 8.2.

THEOREM 2.19 (MacWilliams). *Let C be a code and let $C^\perp$ be its dual. Then the extended weight enumerator of C completely determines the extended weight enumerator of $C^\perp$ and vice versa, via the following formula:*

$$W_{C^\perp}(X,Y,U) = U^{-k} W_C(X+(U-1)Y, X-Y, U).$$

2.3 Connections

There is a connection between the extended weight enumerator and the generalized weight enumerators. We first prove the next proposition.

PROPOSITION 2.20. *Let C be a linear $[n,k]$ code over $\mathbb{F}_q$, and let C^m be the linear subspace consisting of the $m \times n$ matrices over $\mathbb{F}_q$ whose rows are in C. Then there is an isomorphism of $\mathbb{F}_q$-vector spaces between $C \otimes \mathbb{F}_{q^m}$ and C^m.*

Proof. First, fix an isomorphism $\varphi : \mathbb{F}_{q^m} \to \mathbb{F}_q^m$. (For example, let α be a primitive m-th root of unity in $\mathbb{F}_{q^m}$ and write an element of $\mathbb{F}_{q^m}$ in a unique way on the basis $(1, \alpha, \alpha^2, \ldots, \alpha^{m-1})$.) We now create a map $C \otimes \mathbb{F}_{q^m} \to C^m$ as follows. Let $\mathbf{c} = (c_1, \ldots, c_n)$ be a word in $C \otimes \mathbb{F}_{q^m}$. Apply φ coordinate-wise to $\mathbf{c}$, and write the $\varphi(c_i)$ as column vectors. This gives an $m \times n$ matrix over $\mathbb{F}_q$. The rows of this matrix are words of C, because C and $C \otimes \mathbb{F}_{q^m}$ have the same generator matrix. This map is clearly injective. There are $(q^m)^k = q^{km}$ words in $C \otimes \mathbb{F}_{q^m}$, and the number of elements of C^m is $(q^k)^m = q^{km}$, so our map is a bijection. Moreover, the map is $\mathbb{F}_q$-linear, so it gives an isomorphism of $\mathbb{F}_q$-vector spaces $C \otimes \mathbb{F}_{q^m} \to C^m$. □

Note that this isomorphism depends on the choice of an isomorphism $\varphi : \mathbb{F}_{q^m} \to \mathbb{F}_q^m$. The use of this isomorphism for the proof of Theorem 2.23 was suggested by Simonis [85]. We also need the next lemma.

Lemma 2.21. *Let $\mathbf{c} \in C \otimes \mathbb{F}_{q^m}$ and $M \in C^m$ the corresponding $m \times n$ matrix under a given isomorphism. Let $D \subseteq C$ be the subcode generated by the rows of M. Then* $\mathrm{supp}(\mathbf{c}) = \mathrm{supp}(D)$ *and hence* $\mathrm{wt}(\mathbf{c}) = \mathrm{wt}(D)$.

Proof. Since $\varphi : \mathbb{F}_{q^m} \to \mathbb{F}_q^m$ is an isomorphism, we have that $\varphi(c_i) = \mathbf{0}$ if and only if $c_i = 0$. Also, the i-th column of M is zero if and only if $i \notin \mathrm{supp}(D)$. Therefore,$\mathrm{wt}(\mathbf{c}) = \mathrm{wt}(D)$. □

Proposition 2.22. *Let C be a linear code over $\mathbb{F}_q$. Then the weight enumerator of an extension code and the generalized weight enumerator are connected via*

$$A_w(q^m) = \sum_{r=0}^{m} [m, r]_q A_w^{(r)}.$$

Proof. We count the number of words in $C \otimes \mathbb{F}_{q^m}$ of weight w in two ways, using the bijection of Proposition 2.20. The first way is just by substituting $U = q^m$ in $A_w(U)$: since $A_{C \otimes \mathbb{F}_{q^m}, w} = A_w(q^m)$ by Proposition 2.17, this gives the left side of the equation. For the second way we use Lemma 2.21. Fix a weight w and a dimension r. There are $A_w^{(r)}$ subcodes of C of dimension r and weight w. Every such subcode is generated by an $r \times n$ matrix whose rows are words of C. Left multiplication by a $m \times r$ matrix of rank r gives an element of C^m that generates the same subcode of C, and all such elements of C^m are obtained this way. The number of $m \times r$ matrices of rank r is $[m, r]_q$, so summation over all dimensions r gives

$$A_w(q^m) = \sum_{r=0}^{k} [m, r]_q A_w^{(r)}.$$

We can let the summation run up to m, because $A_w^{(r)} = 0$ for $r > k$ and $[m, r]_q = 0$ for $r > m$. This proves the given formula. □

This result first appears in [49, Theorem 3.2], although the term “generalized weight enumerator” was yet to be invented. In general, we have the following theorem.

THEOREM 2.23. *Let C be a linear code over $\mathbb{F}_q$. Then the extended weight enumerator and the generalized weight enumerators are connected via*

$$W_C(X,Y,U) = \sum_{r=0}^{k} \left(\prod_{j=0}^{r-1} (U - q^j) \right) W_C^{(r)}(X,Y).$$

PROOF. If we know $A_w^{(r)}$ for all r, we can determine $A_w(q^m)$ for every m. If we have $k+1$ values of m for which $A_w(q^m)$ is known, we can use Lagrange interpolation to find $A_w(U)$, for this is a polynomial in U of degree at most k. In fact, we have

$$A_w(U) = \sum_{r=0}^{k} \left(\prod_{j=0}^{r-1} (U - q^j) \right) A_w^{(r)}.$$

This formula has the right degree and is correct for $U = q^m$ for all integer values $m \geq 0$, so we know it must be the correct polynomial. Now the theorem follows. □

The converse of the theorem is also true: we can write the generalized weight enumerator in terms of the extended weight enumerator. We first give a combinatorial identity that we will use in several rewriting proofs. It is a generalization of Newton's binomial identity to the Gaussian binomial and can be proven by induction.

LEMMA 2.24. *For every positive integer r the following identity holds:*

$$\prod_{j=0}^{r-1} (Z - q^j) = \sum_{j=0}^{r} \begin{bmatrix} r \\ j \end{bmatrix}_q (-1)^{r-j} q^{\binom{r-j}{2}} Z^j.$$

THEOREM 2.25. *Let C be a linear code over $\mathbb{F}_q$. Then the generalized weight enumerator and the extended weight enumerator are connected via*

$$W_C^{(r)}(X,Y) = \frac{1}{\langle r \rangle_q} \sum_{j=0}^{r} \begin{bmatrix} r \\ j \end{bmatrix}_q (-1)^{r-j} q^{\binom{r-j}{2}} \, W_C(X,Y,q^j).$$

PROOF. We consider the generalized weight enumerator in terms of Theorem 2.11. Rewriting that expression gives the following:

$$\begin{aligned}
W_C^{(r)}(X,Y) &= \sum_{t=0}^{n} B_t^{(r)}(X-Y)^t Y^{n-t} \\
&= \sum_{t=0}^{n} \sum_{|J|=t} \begin{bmatrix} l(J) \\ r \end{bmatrix}_q (X-Y)^t Y^{n-t} \\
&= \sum_{t=0}^{n} \sum_{|J|=t} \left(\prod_{j=0}^{r-1} \frac{q^{l(J)} - q^j}{q^r - q^j} \right) (X-Y)^t Y^{n-t} \\
&= \frac{1}{\prod_{v=0}^{r-1}(q^r - q^v)} \sum_{t=0}^{n} \sum_{|J|=t} \left(\prod_{j=0}^{r-1} (q^{l(J)} - q^j) \right) (X-Y)^t Y^{n-t} \\
&= \frac{1}{\langle r \rangle_q} \sum_{t=0}^{n} \sum_{|J|=t} \sum_{j=0}^{r} \begin{bmatrix} r \\ j \end{bmatrix}_q (-1)^{r-j} q^{\binom{r-j}{2}} q^{j \cdot l(J)} (X-Y)^t Y^{n-t} \\
&= \frac{1}{\langle r \rangle_q} \sum_{j=0}^{r} \begin{bmatrix} r \\ j \end{bmatrix}_q (-1)^{r-j} q^{\binom{r-j}{2}} \sum_{t=0}^{n} \sum_{|J|=t} (q^j)^{l(J)} (X-Y)^t Y^{n-t} \\
&= \frac{1}{\langle r \rangle_q} \sum_{j=0}^{r} \begin{bmatrix} r \\ j \end{bmatrix}_q (-1)^{r-j} q^{\binom{r-j}{2}} W_C(X,Y,q^j).
\end{aligned}$$

In the fourth step, we use the identity in Lemma 2.24. The last step follows from Proposition 2.18. See also [1, 20, 61, 99, 87]. □

2.4 Application to MDS codes

We can use the theory in Sections 2.1 and 2.2 to calculate the weight distribution, generalized weight distribution, and extended weight distribution of a linear $[n,k]$ code C. This is done by determining the values $l(J)$ for each $J \subseteq [n]$. In general, we have to look at the 2^n different subcodes of C to find the $l(J)$, but for the special case of MDS codes we can find the weight distributions much faster.

Proposition 2.26. *Let C be a linear $[n,k]$ MDS code. Let $J \subseteq [n]$ and $|J| = t$. Then we have*

$$l(J) = \begin{cases} 0, & \text{for } t > k, \\ k-t, & \text{for } t \leq k. \end{cases}$$

So for a given t the value of $l(J)$ is independent of the choice of J.

Proof. We know that the dual of an MDS code is also MDS, so $d^\perp = k+1$. Now use $d = n-k+1$ in Lemma 2.7. □

Now that we know all the $l(J)$ for an MDS code, it is easy to find the weight distribution.

THEOREM 2.27. *Let C be an MDS code with parameters $[n,k]$. Then the generalized weight distribution is given by*

$$A_w^{(r)} = \binom{n}{w} \sum_{j=0}^{w-d} (-1)^j \binom{w}{j} \begin{bmatrix} w-d+1-j \\ r \end{bmatrix}_q .$$

The coefficients of the extended weight enumerator for $w > 0$ are given by

$$A_w(U) = \binom{n}{w} \sum_{j=0}^{w-d} (-1)^j \binom{w}{j} (U^{w-d+1-j} - 1).$$

PROOF. We will give the construction for the generalized weight enumerator here: the case of the extended weight enumerator is similar and is left as an exercise. We know from Proposition 2.26 that for an MDS code, $B_t^{(r)}$ depends only on the size of J, so $B_t^{(r)} = \binom{n}{t} \begin{bmatrix} k-t \\ r \end{bmatrix}_q$. Using this in the formula for $A_w^{(r)}$ and substituting $j = t - n + w$, we have

$$\begin{aligned} A_w^{(r)} &= \sum_{t=n-w}^{n-d_r} (-1)^{n+w+t} \binom{t}{n-w} B_t^{(r)} \\ &= \sum_{t=n-w}^{n-d_r} (-1)^{t-n+w} \binom{t}{n-w} \binom{n}{t} \begin{bmatrix} k-t \\ r \end{bmatrix}_q \\ &= \sum_{j=0}^{w-d_r} (-1)^j \binom{n}{w} \binom{w}{j} \begin{bmatrix} k+w-n-j \\ r \end{bmatrix}_q \\ &= \binom{n}{w} \sum_{j=0}^{w-d_r} (-1)^j \binom{w}{j} \begin{bmatrix} w-d+1-j \\ r \end{bmatrix}_q . \end{aligned}$$

In the second step, we are using the binomial equivalence

$$\binom{n}{t}\binom{t}{n-w} = \binom{n}{n-w}\binom{n-(n-w)}{t-(n-w)} = \binom{n}{w}\binom{w}{n-t}.$$

□

So for all MDS-codes the extended and generalized weight distributions are completely determined by the parameters $[n,k]$. But not all such codes are equivalent. We can conclude from this, that the generalized and extended weight enumerators are not enough to distinguish between codes with the same parameters. We illustrate the non-equivalence of two MDS codes by an example.

EXAMPLE 2.28. Let C be a linear $[n,3]$ MDS code over $\mathbb{F}_q$ and let $n \geq 5$. Because C is MDS we have $d = n-2 \geq 3$. We now view the n columns of G as distinct points in the projective plane $\mathbb{P}^2(\mathbb{F}_q)$, say $P_1, \ldots, P_n$. The MDS property that every k columns of G are independent is now equivalent to saying that no three points are on a line.

To see that these n points do not always determine an equivalent code, consider the following construction. Through the n points there are $\binom{n}{2} = N$ lines, the set $\mathcal{N}$. These lines determine (the generator matrix of) an $[n, 3]$ code $\hat{C}$. The minimum distance of the code $\hat{C}$ is equal to the total number of lines minus the maximum number of lines from $\mathcal{N}$ through an arbitrary point $P \in \mathbb{P}^2(\mathbb{F}_q)$. If $P \notin \{P_1, \ldots, P_n\}$ then the maximum number of lines from $\mathcal{N}$ through P is at most $\frac{1}{2}n$, since no three points of $\mathcal{N}$ lie on a line. If $P = P_i$ for some $i \in [n]$ then P lies on exactly $n-1$ lines of $\mathcal{N}$, namely the lines P_iP_j for $j \neq i$. Therefore, the minimum distance of $\hat{C}$ is $d = N - n + 1$.

We now have constructed an $[n, 3, N-n+1]$ code $\hat{C}$ from the original code C. Note that two codes $\hat{C}_1$ and $\hat{C}_2$ are generalized equivalent if C_1 and C_2 are generalized equivalent. The generalized and extended weight enumerators of an MDS code of length n and dimension k are completely determined by the pair (n, k), but this is not generally true for the weight enumerator of $\hat{C}$.

Take for example $n = 6$ and $q = 9$, then $\hat{C}$ is a $[15, 3, 10]$ code. Look at the codes C_1 and C_2 generated by the following matrices respectively, where $\alpha \in \mathbb{F}_9$ is a primitive element:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \alpha^5 & \alpha^6 \\ 0 & 0 & 1 & \alpha^3 & \alpha & \alpha^3 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & \alpha^7 & \alpha^4 & \alpha^6 \\ 0 & 0 & 1 & \alpha^5 & \alpha & 1 \end{pmatrix}.$$

Being both MDS codes, the weight distribution is $(1, 0, 0, 120, 240, 368)$. If we now apply the above construction, we get $\hat{C}_1$ and $\hat{C}_2$ generated by

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & \alpha^4 & \alpha^6 & \alpha^3 & \alpha^7 & \alpha & 1 & \alpha^2 & 1 & \alpha^7 & 1 \\ 0 & 1 & 0 & \alpha^7 & 1 & 0 & 0 & \alpha^4 & 1 & 1 & 0 & \alpha^6 & \alpha & 1 & \alpha^3 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & 0 & \alpha^7 & \alpha^2 & \alpha^3 & \alpha & 0 & \alpha^7 & \alpha^7 & \alpha^4 & \alpha^7 & \alpha & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & \alpha^3 & 0 & \alpha^6 & \alpha^6 & 0 & \alpha^7 & \alpha & \alpha^6 & \alpha^3 & \alpha \\ 0 & 0 & 1 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 & \alpha^7 & \alpha^4 & \alpha^3 & \alpha^5 & \alpha^2 & \alpha^4 & \alpha & \alpha^5 \end{pmatrix}.$$

The weight distributions of $\hat{C}_1$ and $\hat{C}_2$ are, respectively,

$$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 48, 0, 16, 312, 288, 64) \text{ and}$$
$$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 48, 0, 32, 264, 336, 48).$$

So the latter two codes are not generalized equivalent, and therefore not all $[6, 3, 4]$ MDS codes over $\mathbb{F}_9$ are generalized equivalent.

Another example was given in [86, 22] showing that two $[6, 3, 4]$ MDS codes could have distinct covering radii.

3

Zeta functions and their generalizations

The notion of a zeta function originates from the theory of algebraic curves. Via algebraic geometry codes Duursma extended the definition to linear codes [36, 37]. The zeta function admits two generalizations, along the same lines as the generalizations of the weight enumerator in Chapter 2. We can extend the field over which the code is defined: this leads to the two-variable zeta function. Looking at subcodes instead of codewords leads to the generalized zeta function.

Most of this chapter is a summary of known results from Duursma [39], but presented in a way to match with the previous chapter. The definition of the generalized zeta function via generalized binomial moments differs from the approach in [39]. Where Duursma uses the decomposition of zeta functions to define the generalized zeta function, we find in Theorem 3.8 new formulas that directly express the coefficients of the generalized zeta polynomial in terms of the generalized binomial moments.

The theory in this chapter is also used in Chapter 11. Following the literature, we will restrict ourselves in this chapter to codes with minimum distance and dual minimum distance at least three, i.e., $d, d^\perp \geq 3$.

3.1 The (two-variable) zeta function

The two-variable zeta polynomial is extensively studied by Duursma [39], who defined and studied the one-variable case in [36, 37].

Definition 3.1. Let C be a linear $[n, k, d]$ code over $\mathbb{F}_q$ with extended weight enumerator $W_C(X, Y, U)$. The *two-variable zeta polynomial* $P_C(T, U)$ of this code is the unique polynomial in $\mathbb{Q}[T, U]$ of degree at most $n-d$ in T such that if we expand the generating function

$$\frac{P_C(T,U)}{(1-T)(1-TU)}(Y(1-T)+XT)^n$$

as a power series in the variable T, we get

$$\ldots + \ldots T^{n-d-1} + \frac{W_C(X,Y,U)-X^n}{U-1}T^{n-d} + \ldots T^{n-d+1} + \ldots.$$

The quotient $Z_C(T,U) = P_C(T,U)/((1-T)(1-TU))$ is called the *two-variable zeta function.*

Just as with the extended weight enumerator, the variable U can be interpreted as the size of the finite field over which the code is defined. We will often refer to the zeta polynomial in the following form:

$$P_C(T,U) = \sum_{i=0}^{r} P_i(U)\, T^i.$$

The extended weight enumerator of an MDS code is completely determined by its parameters, see Theorem 2.27. So, even if there does not exist an MDS code with parameters $[n, n-d+1, d]$, we can formally define its extended weight enumerator $M_{n,d}$. The two-variable zeta polynomial of an MDS code does not even depend on the parameters of the code, just on the fact that it is MDS.

Proposition 3.2. *A code is MDS if and only if $P_C(T,U) = 1$.*

Proof. There are several proofs possible. We will expand the generating function in Definition 3.1 and show directly that we get the weight enumerator $M_{n,d}$ of the $[n, n-d+1, d]$ MDS code over $\mathbb{F}_q$. By splitting the fraction and using the power series of $1/(1-T)$ and $1/(1-TU)$, we get that

$$\frac{1}{(1-T)(1-TU)} = \frac{1}{U-1}\sum_{l=0}^{\infty}(U^{l+1}-1)T^l.$$

For the second part, we use the binomial expansion twice to get

$$(Y(1-T)+XT)^n = \sum_{j=0}^{n}\sum_{w=j}^{n}\binom{n}{w}\binom{w}{j}(-1)^{j+w}X^{n-w}Y^wT^{n-j}.$$

We multiply the two power series, and find the coefficient of T^{n-d}. We omit the $1/(U-1)$ factor, which is already in the right place. Because we only need the terms with $l+n-j = n-d$, we substitute $l = j-d$. We have to sum from $n-j=0$ to $n-j=n-d$, hence from $j=d$ to $j=n$. This gives

$$\begin{aligned}
&\sum_{j=d}^{n}(U^{j-d+1}-1)\sum_{w=j}^{n}\binom{n}{w}\binom{w}{j}(-1)^{j+w}X^{n-w}Y^w \\
&= \sum_{w=d}^{n}\sum_{j=d}^{w}(U^{j-d+1}-1)\binom{n}{w}\binom{w}{j}(-1)^{j+w}X^{n-w}Y^w \\
&= \sum_{w=d}^{n}\binom{n}{w}\sum_{j=0}^{w-d}(-1)^j\binom{w}{j}(U^{w-d+1-j}-1)X^{n-w}Y^w \\
&= M_{n,d} - X^n
\end{aligned}$$

as was to be shown. □

Theorem 3.3. *The zeta polynomial gives us a way to write the extended weight enumerator with respect to a basis of MDS weight enumerators:*

$$W_C(X,Y,U) = P_0(U)\, M_{n,d} + P_1(U)\, M_{n,d+1} + \ldots + P_r(U)\, M_{n,d+r}.$$

Proof. This follows directly from Definition 3.1 and Proposition 3.2. □

We treat some more properties of the two-variable zeta polynomial. The proofs are similar to the case of the one-variable zeta polynomial as treated in [39].

Proposition 3.4. *The degree of $P_C(T,U)$ in T is $n-d-d^\perp+2$.*

Proof. Assume that $P_r(U)$ is not zero and apply Theorem 3.3 to the dual code $C^\perp$. This expression starts with the dual of $M_{n,d^\perp+r}$. Since the dual of an MDS code is again an MDS code by Theorem 1.12, it is equal to $M_{n,n-d+2+r}$. Therefore, $n+2-d-r=d^\perp$ and hence $r=n-d-d^\perp+2$. □

A way to interpret this degree $n-d-d^\perp+2$ is to view it as a measure for how "far away" a code is from being MDS.

Proposition 3.5. *For the two-variable zeta polynomial of a code C and dual $C^\perp$ we have*

$$P_{C^\perp}(T,U) = P_C\left(\frac{1}{TU}, U\right) U^{n-k+1-d} T^{n-d-d^\perp+2}.$$

Proof. Apply the MacWilliams identity for the extended weight enumerator in Theorem 2.19 to the expression in Theorem 3.3. This gives that $W_{C^\perp}(X,Y,U)$ is equal to

$$\begin{aligned}
&= U^{-k} W_C(X+(U-1)Y, X-Y) \\
&= U^{-k}(P_0(U)\, M_{n,d}(X+(U-1)Y, X-Y) + \ldots \\
&\quad +P_r(U)\, M_{n,d+r}(X+(U-1)Y, X-Y)) \\
&= U^{-k}\left(P_r(U)\, U^{n-d-r+1}\, M_{n,n-d+2-r} + \ldots + P_0(U)\, U^{n-d-1}\, M_{n,n-d+2}\right)
\end{aligned}$$

and the Proposition follows. □

3.2 The generalized zeta function

In Definition 3.1 of the zeta function, the coefficient of T^{n-d} in the power series is exactly the first generalized weight enumerator $W_C^{(1)}(X,Y)$. This motivates the definition of a generalized zeta function of a linear code.

Duursma [39] uses normalized binomial moments to define the two-variable zeta polynomial. These binomial moments are quite similar to the $B_t^{(r)}$ we encountered in Section 2.1, because Duursma's k_S is equal to $l(J)$ for $S=[n]\setminus J$. To avoid confusion, the capital B is only used in the meaning of Section 2.1. We can generalize the normalized binomial moments in the following way:

DEFINITION 3.6. The *generalized binomial moments* of a linear code are given by

$$b_i^{(r)} = \begin{cases} B_{n-d_r-i}^{(r)}/\binom{n}{d_r+i}, & \text{for } 0 \leq i \leq n-d^\perp - d_r, \\ 0, & \text{for } i < 0, \\ \begin{bmatrix} k-n+i+d_r \\ r \end{bmatrix}_q, & \text{for } i > n - d^\perp - d_r. \end{cases}$$

This definition is well defined by Proposition 2.9.

DEFINITION 3.7. The *generalized zeta function* of a linear code is the generating function for the generalized binomial moments:

$$Z_C^{(r)}(T) = \sum_{i=0}^{\infty} b_i^{(r)} T^i.$$

THEOREM 3.8. *The generalized zeta function is a rational function given by*

$$Z_C^{(r)}(T) = \frac{P_C^{(r)}(T)}{(1-T)(1-qT)\cdots(1-q^rT)},$$

where $P_C^{(r)}(T)$ is a polynomial of degree $n - d^\perp - d_r + r + 1$ with coefficients given by

$$P_i^{(r)} = \sum_{j=0}^{r+1} \begin{bmatrix} r+1 \\ j \end{bmatrix}_q (-1)^j q^{\binom{j}{2}} b_{i-j}^{(r)}.$$

PROOF. We will first show the formula for the $P_i^{(r)}$, and then show that they are almost all zero, hence $P_i^{(r)}$ is indeed a polynomial. We start with a combinatorial statement, using Lemma 2.24.

$$\begin{aligned} \prod_{j=0}^{r}(1-q^jT) &= T^{r+1}\prod_{j=0}^{r}\left(\frac{1}{T} - q^j\right) \\ &= \sum_{j=0}^{r+1} \begin{bmatrix} r+1 \\ j \end{bmatrix}_q (-1)^{r+1-j} q^{\binom{r+1-j}{2}} T^{r+1-j} \\ &= \sum_{j=0}^{r+1} \begin{bmatrix} r+1 \\ j \end{bmatrix}_q (-1)^j q^{\binom{j}{2}} T^j. \end{aligned}$$

From this, we can find how $P_C^{(r)}(T)$ looks like:

$$\begin{aligned} P_C^{(r)}(T) &= Z_C^{(r)}(T)\cdot(1-T)(1-qT)\cdots(1-q^rT) \\ &= \left(\sum_{i=0}^{\infty} b_i^{(r)}T^i\right)\cdot\left(\sum_{j=0}^{r+1}\begin{bmatrix} r+1 \\ j \end{bmatrix}_q (-1)^j q^{\binom{j}{2}} T^j\right). \end{aligned}$$

If we look at the coefficient of T^i when we expand this function in the variable T, we get exactly the formula for $P_i^{(r)}$. For $i < 0$, this is clearly zero, because $b_i^{(r)} = 0$ for $i < 0$.

Therefore, it is left to show that $P_i^{(r)}=0$ for $i>n-d^\perp-d_r+r+1$.
Assume that $i>n-d^\perp-d_r+r+1$. Then we can determine the value for $P_i^{(r)}$ because we know the value of all $b_{i-j}^{(r)}$ for $0\leq j\leq r+1$ by Proposition 2.9. We put $s=k-n+i+d_r$, rewrite, use Lemma 2.24, put $j=r+1-j$, and rewrite some more. This gives

$$\begin{aligned}
P_i^{(r)} &= \sum_{j=0}^{r+1}\begin{bmatrix}r+1\\ j\end{bmatrix}_q(-1)^j q^{\binom{j}{2}} b_{i-j}^{(r)}\\
&= \sum_{j=0}^{r+1}\begin{bmatrix}r+1\\ j\end{bmatrix}_q(-1)^j q^{\binom{j}{2}} \begin{bmatrix}k-n+i-j+d_r\\ r\end{bmatrix}_q\\
&= \sum_{j=0}^{r+1}\begin{bmatrix}r+1\\ j\end{bmatrix}_q(-1)^j q^{\binom{j}{2}} \begin{bmatrix}s-j\\ r\end{bmatrix}_q\\
&= \sum_{j=0}^{r+1}\begin{bmatrix}r+1\\ j\end{bmatrix}_q(-1)^j q^{\binom{j}{2}} \prod_{i=0}^{r-1}\left(\frac{q^{s-j}-q^i}{q^r-q^i}\right)\\
&= \frac{1}{\langle r\rangle_q}\sum_{j=0}^{r+1}\begin{bmatrix}r+1\\ j\end{bmatrix}_q(-1)^j q^{\binom{j}{2}} \prod_{i=0}^{r-1}(q^{s-j}-q^i)\\
&= \frac{1}{\langle r\rangle_q}\sum_{j=0}^{r+1}\begin{bmatrix}r+1\\ j\end{bmatrix}_q(-1)^j q^{\binom{j}{2}} \sum_{i=0}^{r}\begin{bmatrix}r\\ i\end{bmatrix}_q(-1)^{r-i}q^{\binom{r-i}{2}}q^{i(s-j)}\\
&= \frac{1}{\langle r\rangle_q}\sum_{i=0}^{r}\begin{bmatrix}r\\ i\end{bmatrix}_q(-1)^{r-i}q^{\binom{r-i}{2}}q^{is}\sum_{j=0}^{r+1}\begin{bmatrix}r+1\\ j\end{bmatrix}_q(-1)^j q^{\binom{j}{2}}q^{-ij}\\
&= \frac{1}{\langle r\rangle_q}\sum_{i=0}^{r}\begin{bmatrix}r\\ i\end{bmatrix}_q(-1)^{r-i}q^{\binom{r-i}{2}}q^{is}\sum_{j=0}^{r+1}\begin{bmatrix}r+1\\ j\end{bmatrix}_q(-1)^{r+1-j} q^{\binom{r+1-j}{2}}q^{-i(r+1-j)}\\
&= \frac{1}{\langle r\rangle_q}\sum_{i=0}^{r}\begin{bmatrix}r\\ i\end{bmatrix}_q(-1)^{r-i}q^{\binom{r-i}{2}}q^{i(s+r+1)}\prod_{j=0}^{r}(q^{-i}-q^j)\\
&= \frac{1}{\langle r\rangle_q}\sum_{i=0}^{r}\begin{bmatrix}r\\ i\end{bmatrix}_q(-1)^{r-i}q^{\binom{r-i}{2}}q^{i(s+r+1)}q^{-i(r+1)}\prod_{j=0}^{r}(1-q^{j-i})\\
&= \frac{1}{\langle r\rangle_q}\sum_{i=0}^{r}\begin{bmatrix}r\\ i\end{bmatrix}_q(-1)^{r-i}q^{\binom{r-i}{2}}q^{is}\prod_{j=0}^{r}(1-q^{j-i}).
\end{aligned}$$

Since both i and j sum over the same range, the factor $1-q^{j-i}$ becomes zero in every term of the summation and thus this whole expression is equal to zero. This shows that the generalized zeta function is indeed a rational function of the given form. □

The next theorem shows that the generalized zeta function determines the generalized weight enumerator of the code.

Theorem 3.9. *If we expand the generating function $Z_C^{(r)}(T)\cdot(Y(1-T)+XT)^n$ in T, it has expansion*

$$\ldots+W_C^{(r)}(x,y)\;T^{n-d_r}+\ldots.$$

PROOF. We want to determine the coefficient of T^{n-d_r} in the generating function

$$\left(\sum_i b_i^{(r)} T^i\right) \cdot \left(\sum_{j=0}^{n}\sum_{w=j}^{n}\binom{n}{w}\binom{w}{j}(-1)^{j+w}X^{n-w}Y^wT^{n-j}\right).$$

We need the terms with $i+n-j=n-d_r$, so let $i=j-d_r$. Then changing the order of summation, setting $n-j=t$ and factoring out binomials gives that

$$\begin{aligned}
&\sum_{j=d_r}^{n} b_{j-d_r}^{(r)} \sum_{w=j}^{n}\binom{n}{w}\binom{w}{j}(-1)^{j+w}X^{n-w}Y^w \\
&= \sum_{w=d_r}^{n}\sum_{j=d_r}^{w} b_{j-d_r}^{(r)}\binom{n}{w}\binom{w}{j}(-1)^{j+w}X^{n-w}Y^w \\
&= \sum_{w=d_r}^{n}\sum_{t=n-w}^{n-d_r} b_{n-t-d_r}^{(r)}\binom{n}{w}\binom{w}{n-t}(-1)^{n-t+w}X^{n-w}Y^w \\
&= \sum_{w=d_r}^{n}\sum_{t=n-w}^{n-d_r} \frac{B_t^{(r)}}{\binom{n}{t}}\binom{n}{t}\binom{t}{n-w}(-1)^{n-t+w}X^{n-w}Y^w \\
&= \sum_{w=d_r}^{n}\sum_{t=n-w}^{n} B_t^{(r)}\binom{t}{n-w}(-1)^{n+t+w}X^{n-w}Y^w \\
&= \sum_{w=d_r}^{n} A_w^{(r)}X^{n-w}Y^w \\
&= W_C^{(r)}(X,Y)
\end{aligned}$$

which was to be proved. □

COROLLARY 3.10. *For all MDS codes, we have* $P_C^{(r)}=1$.

PROOF. From Theorem 3.8 we know that the degree of $P^{(r)}(T)$ is equal to $n-d^\perp-d_r+r+1$, so for MDS codes this degree is 0. Therefore, we only have to show that $P_0^{(r)}=1$. We use the formula in Theorem 3.8 for this:

$$P_0^{(r)}=\sum_{j=0}^{r+1}\begin{bmatrix} r+1 \\ j\end{bmatrix}_q(-1)^jq^{\binom{j}{2}}b_{-j}^{(r)}.$$

Since $b_i^{(r)}=0$ for $i<0$, the only nonzero term in the above summation is at $j=0$, so $P_0^{(r)}=b_0^{(r)}$. In Theorem 2.27 we found that $B_t^{(r)}=\binom{n}{t}\begin{bmatrix} k-t \\ r\end{bmatrix}_q$ for MDS codes. This means that

$$\begin{aligned} P_0^{(r)} &= b_0^{(r)} \\ &= B_{n-d_r}^{(r)} / \binom{n}{d_r} \\ &= \binom{n}{t} \begin{bmatrix} k-n+d_r \\ r \end{bmatrix}_q / \binom{n}{d_r} \\ &= \begin{bmatrix} r \\ r \end{bmatrix}_q \\ &= 1 \end{aligned}$$

as was to be shown. □

Because of the previous corollary, we can interpret the generalized zeta polynomial as a way to write a weight enumerator with respect to a "basis" of weight enumerators of MDS codes. This follows directly from the previous theory.

THEOREM 3.11. *Denote by $M_{n,d_r}^{(r)}$ the generalized weight enumerator of an MDS code of length n and minimum distance $d = d_r - r + 1$. Then the weight enumerator of a code with generalized zeta polynomial $P^{(r)}(T)$ is given by*

$$W_C^{(r)}(X,Y) = P_0^{(r)} M_{n,d_r-r+1}^{(r)} + P_1^{(r)} M_{n,d_r-r+2}^{(r)} + \ldots + P_{n-d^\perp-d_r+r+1}^{(r)} M_{n,n-d^\perp+2}^{(r)}.$$

Part II

Codes and arrangements

4

Introduction to arrangements

An *arrangement of hyperplanes* is simply an n-tuple of hyperplanes in some affine or projective space. If an arrangement is defined over the real affine space, an interesting question is in how many regions the real affine space is divided by the arrangement. The answer to this question is given by the characteristic polynomial, that we will encounter in Chapter 10. If an arrangement is defined over a projective space, it becomes the dual notion of a *projective system*. Important for our purposes are arrangements and projective systems defined over finite fields, because of their close relation to weight enumeration of linear codes.

In this chapter, we will only give the basic definitions of arrangements and projective systems. For a more extensive introduction, see for example Stanley [88] or Orlik and Terao [76]. The connection with weight enumeration is a summary of the work from Katsman, Tsfasman and Vlăduț [60, 92, 93].

4.1 Projective systems and hyperplane arrangements

Let $\mathbb{F}$ be a field. A *projective system* $\mathcal{P} = (P_1, \ldots, P_n)$ in $\mathbb{P}^r(\mathbb{F})$, the projective space over $\mathbb{F}$ of dimension r, is an n-tuple of points P_j in this projective space, such that not all these points lie in a hyperplane.

Let P_j be given by the homogeneous coordinates $(p_{0j} : p_{1j} : \ldots : p_{rj})$ and let $G_{\mathcal{P}}$ be the $(r+1) \times n$ matrix with $(p_{0j}, p_{1j}, \ldots, p_{rj})^T$ as j-th column. Then $G_{\mathcal{P}}$ has rank $r+1$, since not all points lie in a hyperplane. If $\mathbb{F}$ is a finite field, then $G_{\mathcal{P}}$ is the generator matrix of a nondegenerate code over $\mathbb{F}$ of length n and dimension $r+1$.

Conversely, let G be a generator matrix of a nondegenerate linear $[n,k]$ code C over $\mathbb{F}_q$, so G has no zero columns. Take the columns of G as homogeneous coordinates of points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$. This gives the projective system $\mathcal{P}_G$ over $\mathbb{F}_q$ of G. Note that for all extension codes of C, the associated projective system consists of the points of $\mathcal{P}_G$ embedded in $\mathbb{P}^{k-1}(\mathbb{F}_{q^m})$.

An n-tuple $(H_1, \ldots, H_n)$ of hyperplanes in $\mathbb{F}^k$ is called an *arrangement* in $\mathbb{F}^k$. We usually denote an arrangement by $\mathcal{A}$. The arrangement is called *simple* if all the n hyperplanes are mutually distinct. The arrangement is called *central* if all the hyperplanes are linear subspaces. A central arrangement is called *essential* if the intersection of all its hyperplanes is equal to $\{0\}$.

Let $G = (g_{ij})$ be a generator matrix of a nondegenerate linear $[n,k]$ code C, so G has no zero columns. Let H_j be the linear hyperplane in $\mathbb{F}_q^k$ with equation

$$g_{1j}X_1 + \cdots + g_{kj}X_k = 0.$$

The arrangement $(H_1, \ldots, H_n)$ associated with G will be denoted by $\mathcal{A}_G$. The arrangement associated with an extension code of C consists of the hyperplanes of $\mathcal{A}_G$ embedded in $\mathbb{F}_{q^m}^k$.

In case of a central arrangement one considers the hyperplanes in $\mathbb{P}^{k-1}(\mathbb{F})$. Note that projective systems and essential arrangements are dual notions and that there is a one-to-one correspondence between equivalence classes of nondegenerate $[n,k]$ codes over $\mathbb{F}_q$, equivalence classes of projective systems over $\mathbb{F}_q$ of n points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$, and equivalence classes of essential arrangements of n hyperplanes in $\mathbb{P}^{k-1}(\mathbb{F}_q)$.

4.2 Geometric interpretation of weight enumeration

We can write a codeword $\mathbf{c} \in C$ as $\mathbf{c} = \mathbf{x}G$, with $\mathbf{x} \in \mathbb{F}_q^k$. The i-th coordinate of $\mathbf{c}$ is zero if and only if the standard inner product of $\mathbf{x}$ and the i-th column of G is zero. In terms of projective systems: P_i is in the hyperplane perpendicular to $\mathbf{x}$. See Figure 4.1.

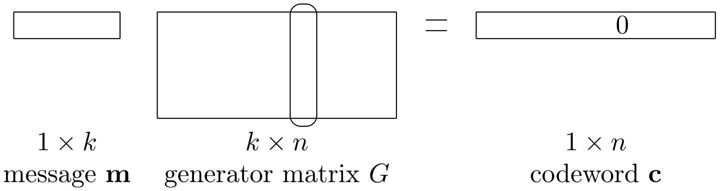


Figure 4.1: The geometric determination of the weight of a codeword

Proposition 4.1. *Let C be a linear nondegenerate $[n,k]$ code over $\mathbb{F}_q$ with generator matrix G. Let $\mathcal{P}_G$ be the projective system of G. The code has minimum distance d if and only if $n-d$ is the maximal number of points of $\mathcal{P}_G$ in a hyperplane of $\mathbb{P}^{k-1}(\mathbb{F}_q)$.*

Proof. See Katsman, Tsfasman and Vlădut [60, 92, 93]. □

We can translate Proposition 4.1 for an arrangement.

Proposition 4.2. *Let C be a nondegenerate code over $\mathbb{F}_q$ with generator matrix G and let $\mathbf{c}$ be a codeword $\mathbf{c} = \mathbf{x}G$ for some $\mathbf{x} \in \mathbb{F}_q^k$. Then $n - \mathrm{wt}(\mathbf{c})$ is equal to the number of hyperplanes in $\mathcal{A}_G$ through $\mathbf{x}$.*

Remark 4.3. Recall that in Definitions 2.5 and 2.13 we introduced $C(J)$ and $B_J(U)$ for the determination of the weight enumerator. Let $\mathcal{A}_G = (H_1, \ldots, H_n)$ be the arrangement associated to the nondegenerate code C. The encoding map $\mathbf{x} \mapsto \mathbf{x}G = \mathbf{c}$ from vectors $\mathbf{x} \in \mathbb{F}_q^k$ to codewords gives the following isomorphism of vectorspaces:

$$\bigcap_{j \in J} H_j \cong C(J).$$

Furthermore, $B_J(q)$ is equal to the number of nonzero codewords $\mathbf{c} \in C$ that are zero at all j in J and this is equal to the number of nonzero elements of the intersection $\bigcap_{j \in J} H_j$. A similar remark holds for words in an extension code $C \otimes \mathbb{F}_{q^m}$.

We can generalize this geometric interpretation of weight enumeration from words to subcodes of C. Let Π be a subspace of codimension r in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ and let M be an $r \times k$ matrix whose nullspace is Π. Then MG is an $r \times n$ matrix of full rank whose rows are a basis of a subcode $D \subseteq C$. This gives a one-to-one correspondence between subspaces of codimension r of $\mathbb{P}^{k-1}(\mathbb{F}_q)$ and subcodes of C of dimension r. See Figure 4.2. This correspondence is independent of the choice of M, G, and the basis of D; see [93] for details.

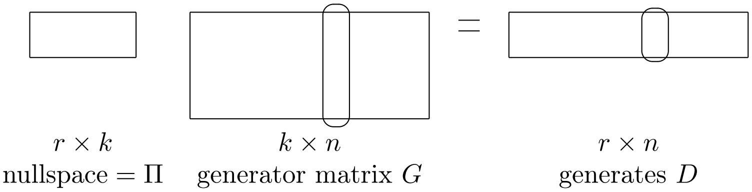


Figure 4.2: The geometric determination of the weight of a subcode

Theorem 4.4. *Let $D \subseteq C$ be a subcode of dimension r and $\Pi \subseteq \mathbb{P}^{k-1}(\mathbb{F}_q)$ the corresponding subspace of codimension r. Then a coordinate $i \in [n]$ is in $[n] \setminus \operatorname{supp}(D)$ if and only if the point $P_i \in \mathcal{P}_G$ is in Π.*

Proof. The i-th coordinate of D is zero for all words in D if and only if all elements in the basis of D have a zero in the i-th coordinate. This happens if and only if the i-th column of G is in the nullspace of M, or, equivalently, if the point $P_i \in \mathcal{P}_G$ is in Π. □

Corollary 4.5. *Let $D \subseteq C$ be a subcode of dimension r and $\Pi \subseteq \mathbb{P}^{k-1}(\mathbb{F}_q)$ the corresponding subspace of codimension r. Then the weight of D is equal to n minus the number of points $P_i \in \mathcal{P}_G$ that are in Π.*

A code C is called *projective* if $d(C^\perp) \geq 3$. Let G be a generator matrix of C. Then C is projective if and only if C is nondegenerate and any two columns of G are independent. Therefore, C is projective if and only if C is nondegenerate and the hyperplanes of $\mathcal{A}_G$ are mutually distinct.

5

Weight enumeration of codes from finite spaces

In the previous chapter, we have described a geometric method to determine the extended and generalized weight distribution of a code. We will apply this theory to projective systems coming from projective and affine spaces: the corresponding codes are the q-ary Simplex code and the q-ary first order Reed-Muller code. As a result of the calculations, we will not only determine the generalized and equivalent weight enumerators of these codes, but we also completely determine the set of supports of subcodes and words in an extension code.
This chapter is a copy of [53].

5.1 Codes from a finite projective space

Consider the projective system $\mathcal{P}$ that consists of all the points in $\mathbb{P}^{s-1}(\mathbb{F}_q)$ without multiplicities. The corresponding code is the Simplex code:

Definition 5.1. The q-ary Simplex code $\mathcal{S}_q(s)$ is a linear $[(q^s-1)/(q-1),s]$ code over $\mathbb{F}_q$. The columns of the generator matrix of the code are all possible nonzero vectors in $\mathbb{F}_q^s$, up to multiplication by a scalar.

The correspondence between $\mathcal{P}$ and the Simplex code is independent of the choice of a generator matrix. We use this correspondence to determine the extended weight enumerator of the Simplex code. We do this via the generalized weight enumerators.

Theorem 5.2. *The generalized weight enumerators of the Simplex code $\mathcal{S}_q(s)$ are, for $0 \leq r \leq s$, given by*

$$W_{\mathcal{S}_q(s)}(X,Y) = \begin{bmatrix} s \\ r \end{bmatrix}_q X^{(q^{s-r}-1)/(q-1)} Y^{(q^s-q^{s-r})/(q-1)}.$$

Proof. We use Corollary 4.5 to determine the weights of all subcodes of $\mathcal{S}_q(s)$. Fix a dimension r. Let $D \subseteq \mathcal{S}_q(s)$ be some subcode of dimension r that corresponds to the subspace $\Pi \subseteq \mathbb{P}^{s-1}(\mathbb{F}_q)$ of codimension r. The weight of D is equal to n minus the number of points in $\mathcal{P}$ that are in Π. Because all points of $\mathbb{P}^{s-1}(\mathbb{F}_q)$ are in $\mathcal{P}$, the weight is the same for all D and it is equal to n minus the total number of points in Π. This means the weight of D is equal to

$$\frac{q^s-1}{q-1}-\frac{q^{s-r}-1}{q-1}=\frac{q^s-q^{s-r}}{q-1}$$

and the theorem follows. □

From the previous calculation and Theorem 4.4 the next statement follows.

COROLLARY 5.3. *Let D be some subcode of dimension r of the Simplex code $\mathcal{S}_q(s)$. Then the points in $\mathcal{P}$ indexed by $[n]\setminus\operatorname{supp}(D)$ are all the points in the corresponding subspace Π of codimension r in $\mathbb{P}^{s-1}(\mathbb{F}_q)$.*

We can now write down the extended weight enumerator of the Simplex code:

THEOREM 5.4. *The extended weight enumerator of the Simplex code $\mathcal{S}_q(s)$ is equal to*

$$W_{\mathcal{S}_q(s)}(X,Y,U)=\sum_{r=0}^{s}\left(\prod_{j=0}^{r-1}(U-q^j)\right)\begin{bmatrix}s\\r\end{bmatrix}_q X^{(q^{s-r}-1)/(q-1)}Y^{(q^s-q^{s-r})/(q-1)}.$$

PROOF. We use the correspondence between the generalized and extended weight enumerator in Theorem 2.23:

$$\begin{aligned}W_{\mathcal{S}_q(s)}(X,Y,U)&=\sum_{r=0}^{s}\left(\prod_{j=0}^{r-1}(U-q^j)\right)W_{\mathcal{S}_q(s)}(X,Y)\\&=\sum_{r=0}^{s}\left(\prod_{j=0}^{r-1}(U-q^j)\right)\begin{bmatrix}s\\r\end{bmatrix}_q X^{(q^{s-r}-1)/(q-1)}Y^{(q^s-q^{s-r})/(q-1)}.\end{aligned}$$

□

In combination with the isomorphism of Proposition 2.20 and Lemma 2.21, we get the following consequence.

COROLLARY 5.5. *The points in $\mathcal{P}$ indexed by the complement of the support of a word of weight $(q^s-q^{s-r})/(q-1)$ in the extension code $\mathcal{S}_q(s)\otimes\mathbb{F}_{q^m}$ for $r\leq m$ are all the points in a subspace of $\mathbb{P}^{s-1}(\mathbb{F}_q)$ of codimension r and every subspace of $\mathbb{P}^{s-1}(\mathbb{F}_q)$ of codimension r occurs in this manner.*

EXAMPLE 5.6. We consider the Simplex code $\mathcal{S}_2(3)$. It is a binary $[7,3]$ code. Its extended weight enumerator has coefficients

$$\begin{aligned}A_0(U)&=1,\\A_1(U)&=0,\\A_2(U)&=0,\\A_3(U)&=0,\\A_4(U)&=7(U-1),\\A_5(U)&=0,\\A_6(U)&=7(U-1)(U-2),\\A_7(U)&=(U-1)(U-2)(U-4).\end{aligned}$$

Note that for any code we have $A_0(U) = 1$ for the zero word, and all other polynomials are divisible by $(U - 1)$ because over the "field of size one" we only have the zero word. In the binary case $U = 2$, the polynomials for $A_6(U)$ and $A_7(U)$ vanish and the code has only one nonzero weight. For $U = 2^2 = 4$, $A_7(U)$ still vanishes, it is a two-weight code. For $U = 2^3$ and higher extensions we get all three possible nonzero weights.

5.2 Codes from a finite affine space

It may sound a bit strange to talk about the projective system coming from an affine space. To solve this, remember that we can construct the finite affine space $\mathbb{A}^{s-1}(\mathbb{F}_q)$ by deleting a hyperplane from $\mathbb{P}^{s-1}(\mathbb{F}_q)$. Therefore, let the projective system $\mathcal{P}$ consists of all points in $\mathbb{P}^{s-1}(\mathbb{F}_q)$ minus the points in a hyperplane H of $\mathbb{P}^{s-1}(\mathbb{F}_q)$. Without loss of generality, we can choose H to be the hyperplane $X_1 = 0$. The corresponding code is (monomial equivalent to) the first order q-ary Reed-Muller code, and we can define it in the following way:

Definition 5.7. The first order q-ary Reed-Muller code $\mathcal{RM}_q(1, s-1)$ is a linear $[q^{s-1}, s]$ code over $\mathbb{F}_q$. The generator matrix consists of the all-one row, and the other positions in the columns of the generator matrix are all possible vectors in $\mathbb{F}_q^{s-1}$.

Note that the linear dependence between the columns of the generator matrix is now equal to the dependence between the corresponding affine points: this property is very useful if we want to talk about the matroid associated to the code, see [73].

We will use the projective system described above to determine the extended weight enumerator of the first order Reed-Muller code. We do this via the generalized weight enumerators.

Theorem 5.8. *The generalized weight enumerators of the first order Reed-Muller code $\mathcal{RM}_q(1, s-1)$ are, for $0 < r < s$, given by*

$$W^{(r)}_{\mathcal{RM}_q(1,s-1)}(X,Y) = \begin{bmatrix} s-1 \\ r-1 \end{bmatrix}_q Y^n + q^r \begin{bmatrix} s-1 \\ r \end{bmatrix}_q X^{q^{s-1-r}} Y^{q^{s-1}-q^{s-1-r}}.$$

The extremal cases are, as always, given by

$$\begin{aligned} W^{(0)}_{\mathcal{RM}_q(1,s-1)}(X,Y) &= X^n, \\ W^{(s)}_{\mathcal{RM}_q(1,s-1)}(X,Y) &= Y^n. \end{aligned}$$

Proof. We use Corollary 4.5 to determine the weights of all subcodes of $\mathcal{RM}_q(1, s-1)$. Fix a dimension r, with $0 \leq r \leq s$. Let $D \subseteq \mathcal{RM}_q(1, s-1)$ be some subcode of dimension r that corresponds to the subspace $\Pi \subseteq \mathbb{P}^{s-1}(\mathbb{F}_q)$ of codimension r. The weight of D is equal to n minus the number of points in $\mathcal{P}$ that are in Π. There are two possibilities:

1. $\Pi \subseteq H$;

2. $\Pi \nsubseteq H$.

In the first case, we cannot have $r = 0$, since then Π is the whole of $\mathbb{P}^{s-1}(\mathbb{F}_q)$ and this cannot be contained in the hyperplane H. So, let $r > 0$. Now none of the points of $\mathcal{P}$ are in Π, since no points of H are in $\mathcal{P}$. Therefore, $\operatorname{supp}(D) = [n]$ and $\operatorname{wt}(D) = n$. The number of such codes is equal to the number of subspaces of codimension $r-1$ in $H \cong PG(s-2, q)$, and this is $\begin{bmatrix} s-1 \\ r-1 \end{bmatrix}_q$. Hence for $0 < r \leq s$ we get the following term for the generalized weight enumerator:

$$\begin{bmatrix} s-1 \\ r-1 \end{bmatrix}_q Y^n.$$

In the second case, we do not have to consider $r = s$, since then Π is the empty set and this was already included in the previous case. So, let $r < s$. Now Π and H intersect in a subspace of codimension r in H. The points of $\mathcal{P}$ that are in Π, are all those points of Π that are not in $\Pi \cap H$. By the construction of the affine space $\mathbb{A}^{s-1}(\mathbb{F}_q)$, the points of $\Pi \setminus (\Pi \cap H)$ form a subspace of $\mathbb{A}^{s-1}(\mathbb{F}_q)$ of codimension r. The number of points in such a subspace is q^{s-1-r}, so $\operatorname{wt}(D) = n - q^{s-1-r} = q^{s-1} - q^{s-1-r}$. The number of such codes is equal to the number of subspaces of codimension r in $\mathbb{A}^{s-1}(\mathbb{F}_q)$, and this is $q^r \begin{bmatrix} s-1 \\ r \end{bmatrix}_q$. Therefore, this case gives the following term for the generalized weight enumerator, for $0 \leq r < s$:

$$q^r \begin{bmatrix} s-1 \\ r \end{bmatrix}_q X^{q^{s-1-r}} Y^{q^{s-1} - q^{s-1-r}}.$$

Summing up this two cases leads to the given formulas. □

From the previous calculation and Theorem 4.4 the next statement follows.

COROLLARY 5.9. *Let D be some subcode of dimension r of the first order Reed-Muller code $\mathcal{RM}_q(1, s-1)$. Then either $\operatorname{supp}(D) = [n]$ or the points in $\mathcal{P}$ indexed by $[n] \setminus \operatorname{supp}(D)$ are all the points in the corresponding subspace Π of codimension r in $\mathbb{A}^{s-1}(\mathbb{F}_q)$ and every subspace of $\mathbb{A}^{s-1}(\mathbb{F}_q)$ of codimension r occurs in this manner.*

We can now write down the extended weight enumerator of the first order Reed-Muller code:

THEOREM 5.10. *The extended weight enumerator of the first order Reed-Muller code $\mathcal{RM}_q(1, s-1)$ is equal to*

$$\begin{aligned} W_{\mathcal{RM}_q(1,s-1)}(X, Y, U) = \sum_{r=1}^{s} \left(\prod_{j=0}^{r-1} (U - q^j) \right) \begin{bmatrix} s-1 \\ r-1 \end{bmatrix}_q Y^n \\ + \sum_{r=0}^{s-1} \left(\prod_{j=0}^{r-1} (U - q^j) \right) q^r \begin{bmatrix} s-1 \\ r \end{bmatrix}_q X^{q^{s-1-r}} Y^{q^{s-1} - q^{s-1-r}}. \end{aligned}$$

PROOF. We use the correspondence between the generalized and extended weight enumerator in Theorem 2.23:

$$\begin{aligned}
W_{\mathcal{RM}_q(1,s-1)}(X,Y,U) &= \sum_{r=0}^{s}\left(\prod_{j=0}^{r-1}(U-q^j)\right) W_{\mathcal{S}_q(s)}(X,Y) \\
&= X^n + \sum_{r=1}^{s-1}\left(\prod_{j=0}^{r-1}(U-q^j)\right)\left(\begin{bmatrix} s-1 \\ r-1 \end{bmatrix}_q Y^n\right. \\
&\quad \left. + q^r \begin{bmatrix} s-1 \\ r \end{bmatrix}_q X^{q^{s-1-r}} Y^{q^{s-1}-q^{s-1-r}}\right) + Y^n \\
&= \sum_{r=1}^{s}\left(\prod_{j=0}^{r-1}(U-q^j)\right)\begin{bmatrix} s-1 \\ r-1 \end{bmatrix}_q Y^n \\
&\quad + \sum_{r=0}^{s-1}\left(\prod_{j=0}^{r-1}(U-q^j)\right) q^r \begin{bmatrix} s-1 \\ r \end{bmatrix}_q X^{q^{s-1-r}} Y^{q^{s-1}-q^{s-1-r}}.
\end{aligned}$$

□

In combination with the isomorphism of Proposition 2.20 and Lemma 2.21, we get the following consequence.

Corollary 5.11. *The points in $\mathcal{P}$ indexed by the complement of the support of a word of weight $q^{s-1} - q^{s-1-r}$ in the extension code $\mathcal{RM}_q(1, s-1) \otimes \mathbb{F}_{q^m}$ for $r \leq m$ are all the points in a subspace of $\mathbb{A}^{s-1}(\mathbb{F}_q)$ of codimension r.*

Example 5.12. We consider the Reed-Muller code $\mathcal{RM}_2(1,3)$. It is a binary $[8,4]$ code. Its extended weight enumerator has coefficients

$$\begin{aligned}
A_0(U) &= 1, \\
A_1(U) &= 0, \\
A_2(U) &= 0, \\
A_3(U) &= 0, \\
A_4(U) &= 14(U-1), \\
A_5(U) &= 0, \\
A_6(U) &= 28(U-1)(U-2), \\
A_7(U) &= 8(U-1)(U-2)(U-4), \\
A_8(U) &= (U-1)(U^3-7U^2+21U-21).
\end{aligned}$$

As noticed in Example 5.6, for any code we have $A_0(U) = 1$ for the zero word, and all other polynomials are divisible by $(U-1)$ because over the "field of size one" we only have the zero word. In the binary case $U = 2$, the polynomials for $A_6(U)$ and $A_7(U)$ vanish and we get a two-weight code. For $U = 2^2 = 4$, $A_7(U)$ still vanishes. For $U = 2^3$ and higher extensions we get all four possible nonzero weights.

This example and the previous Example 5.6 also illustrate that the binary Simplex code $\mathcal{S}_2(s)$ is equivalent to the binary Reed-Muller code $\mathcal{RM}_2(1,s)$ shortened at the first coordinate.

5.3 Application and links to other problems

We found direct formulas for the extended weight enumerator of the q-ary Simplex code and the q-ary first order Reed-Muller code. Following from this calculations, we found the geometrical structure of the supports of the subcodes and of words in extension codes. This triggers a lot of links with other problems in discrete mathematics and coding theory. The following list is by no means exhaustive, but it hopefully serves as encouragement and inspiration for further research.

Mphako [73] calculated the Tutte polynomial of the matroids coming from finite projective and affine spaces. She does this by using the equivalence between the Tutte polynomial and the coboundary polynomial, that we will treat in Chapter 10. The formulas found by Mphako indeed coincide with the extended weight enumerators we found in this chapter.

We calculated the extended weight enumerator for the first order (q-ary) Reed-Muller code. The weight enumeration of higher order Reed-Muller codes is an open problem. The generalized Hamming weights of q-ary Reed-Muller codes were found by Heijnen and Pellikaan [46].

It is known that the binary r-th order Reed-Muller codes $\mathcal{RM}_2(r,m)$ arise from the design of points and subspaces of codimension r in the affine space $\mathbb{A}^m(\mathbb{F}_2)$, see [5]. The q-ary analogue of this statement is treated in [6]. In Corollary 5.11 we saw that the complements of supports of the words in the extension code $\mathcal{RM}_q(1,s-1)\otimes\mathbb{F}_{q^m}$ contain the design of points and subspaces of codimension r in $\mathbb{A}^{s-1}(\mathbb{F}_q)$ for $r \leq m$. This suggests some kind of link between extension codes of the first order Reed-Muller code and the higher order Reed-Muller codes. If we can make this link explicit, it might lead to more insights to the weight enumeration of higher order Reed-Muller codes.

We encountered two types of two-weight codes in this paper: the first order Reed-Muller code, and the extension of the Simplex code $\mathcal{S}_q(s) \otimes \mathbb{F}_{q^2}$. How do these codes fit into the classification of two-weight codes from Calderbank and Kantor [28]? Is the quadratic extension code of the simplex code unique?

For every design, one can talk about its p-rank. Tonchev [91] generalized this concept to the *dimension* of a design, and formulated an analogue of the Hamada conjecture. Using the results in this chapter, Jungnickel and Tonchev [50] worked on the characterization of the classical geometric designs. This led to a new invariant for incidence structures [51].

6

The coset leader weight enumerator

The probability of error in error-detection can be expressed in terms of the weight enumerator of a code [63], and for error-correction the coset leader weight enumerator is used [70]. The coset leader weight enumerator is also used in steganography to compute the average of changed symbols [74, 75]. The computation of the weight enumerator of a code is NP-hard [12, 100]. The complexity of computing the coset leader weight enumerator of a code is considered extremely difficult [47]. The size of lists of nearest codewords is considered in the list decoding of Reed-Solomon codes [59, 90]. This motivates the definition of the list weight enumerator and its extension.
This chapter reports on ongoing research that was first presented in [56].

6.1 Coset leader and list weight enumerator

Definition 6.1. Let C be a $[n, k]$ linear code over $\mathbb{F}_q$ and let $\mathbf{y} \in \mathbb{F}_q^n$. The weight of the coset $\mathbf{y} + C$ is defined by

$$\mathrm{wt}(\mathbf{y} + C) = \min\{\mathrm{wt}(\mathbf{y} + \mathbf{c}) : \mathbf{c} \in C\}.$$

A coset leader is a choice of an element $\mathbf{y} \in \mathbb{F}_q^n$ of minimal weight in its coset, that is $\mathrm{wt}(\mathbf{y}) = \mathrm{wt}(\mathbf{y} + C)$. Let α_i be the number of cosets of C that are of weight i. Let λ_i be the number of $\mathbf{y}$ in $\mathbb{F}_q^n$ that are of minimal weight i in their coset. Then $\alpha_C(X, Y)$, the *coset leader weight enumerator* of C and $\lambda_C(X, Y)$, the *list weight enumerator* of C, are polynomials defined by

$$\alpha_C(X, Y) = \sum_{i=0}^{n} \alpha_i X^{n-i} Y^i \quad \text{and} \quad \lambda_C(X, Y) = \sum_{i=0}^{n} \lambda_i X^{n-i} Y^i.$$

See [47, 70]. The covering radius $\rho(C)$ of C is the maximal i such that $\alpha_i(C) \neq 0$.

We have $\alpha_i = \lambda_i = \binom{n}{i}(q-1)^i$ for all $i \leq (d-1)/2$, where d is the minimum distance of C. The coset leader weight enumerator gives a formula for the *probability of error*, that is the probability that the output of the decoder is the wrong codeword. In this decoding scheme the decoder uses the chosen coset leader as the error vector. See [70, Chap.1 §5]. The list weight enumerator is of interest in case the decoder has as output the list of all nearest codewords [59, 90].

Consider the functions $\alpha_i(U)$ and $\lambda_i(U)$ such that $\alpha_i(q^m)$ and $\lambda_i(q^m)$ are equal to the number of cosets of weight i and the number of elements in $\mathbb{F}_{q^m}^n$ of minimal weight i in its coset, respectively with respect to the extended code $C \otimes \mathbb{F}_{q^m}$.

DEFINITION 6.2. The *extended coset leader weight enumerator* and the *extended list weight enumerator* are defined by

$$\alpha_C(X,Y,U) = \sum_{i=0}^{n} \alpha_i(U) X^{n-i} Y^i \quad \text{and} \quad \lambda_C(X,Y,U) = \sum_{i=0}^{n} \lambda_i(U) X^{n-i} Y^i.$$

In [47, Theorem 2.1] it is shown that the function $\alpha_i(U)$ is determined by finitely many data for all extensions of $\mathbb{F}_q$. This shows by Lagrange interpolation, that the $\alpha_i(U)$ are polynomials in the variable U. In fact, let C be a linear $[n,k]$ code over $\mathbb{F}_q$. Then there are well defined nonnegative integers F_{ij} such that

$$\alpha_C(X,Y,U) = 1 + \sum_{i=1}^{n-k} \sum_{j=1}^{n-k} F_{ij}(U-1)(U-q)\cdots(U-q^{j-1})X^{n-i}Y^i.$$

This is similar to the expression of the extended weight enumerator in terms of the generalized weight enumerator in Proposition 2.22. See also [47, 62].

REMARK 6.3. Although the extended weight enumerator of a code contains a lot of information of a code, it does not determine the coset leader weight enumerator or even the covering radius of a code. See [22]. For instance all $[n,k,n-k+1]$ codes over $\mathbb{F}_q$ are MDS and have the same generalized and extended weight enumerator by Theorem 2.27 but the covering radius varies for fixed n,k and q.

As noted in Section 1.5, there is a one-to-one correspondence between cosets and syndromes. It is a well known fact that a coset leader corresponds to a minimal way to write its syndrome as a linear combination of the columns of a parity check matrix. This idea is formalized as follows.

DEFINITION 6.4. Let H be a parity check matrix of a linear $[n,k]$ code C over $\mathbb{F}_q$ and let $\mathbf{y}$ be a vector in $\mathbb{F}_q^n$. Let $\mathbf{s} = H\mathbf{y}^T$ be the syndrome of this word with respect to H. The *weight of* $\mathbf{s}$ *with respect to* H, also called the *syndrome weight* of $\mathbf{s}$, is defined by

$$\mathrm{wt}_H(\mathbf{s}) = \mathrm{wt}(\mathbf{y} + C).$$

Note that α_i is the number of syndromes in $\mathbb{F}_q^{n-k}$ with respect to H that are of weight i. See [47, Definition 2.1].

The geometric interpretation of the weight of a coset and the syndrome weight is as follows. Let $\mathbf{h}_j$ be the j-th column of H and let $J \subseteq [n]$. Let V_J be the vector subspace of $\mathbb{F}_q^{n-k}$ that is generated by the vectors $\mathbf{h}_j^T$ with $j \in J$. Then we define

$$\mathcal{V}_t = \bigcup_{|J|=t} V_J.$$

PROPOSITION 6.5. *Let* $\mathbf{s}$ *in* $\mathbb{F}_q^{n-k}$ *be a syndrome with respect to* H*. Then*

$$\mathrm{wt}_H(\mathbf{s}) = t \quad \textit{if and only if} \quad \mathbf{s} \in \mathcal{V}_t \setminus \mathcal{V}_{t-1}.$$

COROLLARY 6.6. *Let* C *be a linear* $[n,k]$ *code with parity check matrix* H*. Then* α_i *is the number of vectors that are in the span of* i *columns of* H *but not in the span of* $i-1$ *columns of* H*.*

Let J consist of t elements. If V_J has dimension t', then there is a $J' \subseteq J$ consisting of t' elements such that the $\mathbf{h}_i$ with $i \in J'$ are independent. As a result, $V_J = V_{J'}$. Now V_J is a subspace of the column space of H, which has dimension $n-k$. Hence there is an $I \subseteq [n]$ consisting of $n-k$ elements such that $J' \subseteq I$ and $\mathbf{h}_i$, $i \in I$ are independent. So

$$V_J = \bigcap_{i \in (I \setminus J')} V_{I \setminus \{i\}}$$

is an intersection of the $n-k-t'$ hyperplanes $V_{I\setminus\{i\}}$.

6.2 Examples

EXAMPLE 6.7. Let $C = \mathbb{F}_q^n$. Then $\lambda_C(X,Y,U) = \alpha_C(X,Y,U) = X^n$.

EXAMPLE 6.8. Let $C = \{0\}$. Then $\lambda_i(U) = \alpha_i(U) = \binom{n}{i}(U-1)^i X^{n-i} Y^i$ and $\lambda_C(X,Y,U) = \alpha_C(X,Y,U) = (X+(U-1)Y)^n$.

EXAMPLE 6.9. Let C be the dual of the $[n,1,n]$ repetition code. Then $\lambda_C(X,Y,U) = X^n + n(U-1)X^{n-1}Y$ and $\alpha_C(X,Y,U) = X^n + (U-1)X^{n-1}Y$.

EXAMPLE 6.10. Let C be the $[n,1,n]$ repetition code. Then this code has not such an easy description of $\lambda_C(X,Y,U)$ and $\alpha_C(X,Y,U)$ as the previous example. Apart from the known expressions for $\lambda_i(U)$ and $\alpha_i(U)$ for $i \leq (n-1)/2$ that hold for every code we have that $\lambda_{n-1}(U) = n\alpha_{n-1}(U)$ and $\alpha_{n-1}(U) = (U-1)(U-2)\cdots(U-n+1)$.

EXAMPLE 6.11. Let C be the binary Hamming code of length 7. This is the dual of the binary Simplex code $\mathcal{S}_2(3)$, see Example 5.6. Its parity check matrix consists of all possible nonzero vectors in $\mathbb{F}_2^3$, and the corresponding arrangement is shown in Figure 6.1.

We can determine the extended coset leader weight enumerator by Corollary 6.6. As always, we have $\alpha_0(U) = 1$, this is the code itself. There are seven projective points in the arrangement, so $\alpha_1(U) = 7(U-1)$. On each of the seven lines there are $(U+1)$ points, of which we counted already three per line, so $\alpha_2(U) = 7(U-1)(U-2)$. Since

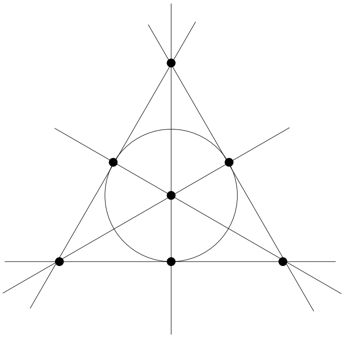


Figure 6.1: The hyperplane arrangement of the parity check matrix of the binary $[7,4]$ Hamming code.

$\alpha_0(U)+\alpha_1(U)+\alpha_2(U)+\alpha_3(U)=U^3$, the total number of cosets, we find that $\alpha_3(U)=(U-1)(U-2)(U-4)$.
We see that $\rho(C)=1$, $\rho(C\otimes\mathbb{F}_4)=2$ and $\rho(C\otimes\mathbb{F}_{2^m})=3$ for $m\geq 3$. The list weight enumerator is equal to

$$\begin{aligned}\lambda_C(X,Y,U) &= X^7+\\ &\quad 7(U-1)X^6Y+\\ &\quad 21(U-1)(U-2)X^5Y^2+\\ &\quad 28(U-1)(U-2)(U-4)X^4Y^3.\end{aligned}$$

6.3 Connections and duality properties

Research Problem 5.1 in [70, Chapter 5] asks whether the coset leader weight enumerator of C determines the coset leader weight enumerator of $C^\perp$, as is the case for the ordinary weight enumerator by the MacWilliams relations. This problem has a negative answer by [8]. The authors give three binary [15,3,7] codes that have the same coset leader weight enumerator, but the dual codes have mutually distinct coset leader weight enumerators. In fact a much smaller counterexample is possible, as we shall now show.

Example 6.12. The two codes of length 3 with parity check matrices $H_1=(110)$ and $H_2=(111)$ both have the same extended coset leader weight enumerator $X^3+(U-1)X^2Y$. But their dual codes have distinct extended coset leader weight enumerator, since

$$\begin{aligned}\alpha_{C_1^\perp}(X,Y,U) &= X^3+2(U-1)X^2Y+(U-1)XY^2,\\ \alpha_{C_2^\perp}(X,Y,U) &= X^3+3(U-1)X^2Y+(U-1)(U-2)XY^2.\end{aligned}$$

Note that the code $C_1^\perp$ is degenerate. A nondegenerate counterexample is obtained as follows.

Example 6.13. Let C_3 and C_4 be the two $[6,3]$ codes over $\mathbb{F}_2$ with generator matrices

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

The next table shows the coefficients of the extended coset leader weight enumerator and the extended list weight enumerator of the codes and their duals. The values for $i = 0$ are left out: they are all equal to 1.

	i	C_3	C_4
$\alpha_{C,i}$	1	$5(U-1)$	$5(U-1)$
	2	$2(U-1)(3U-5)$	$2(U-1)(3U-5)$
	3	$(U-1)(U-2)(U-3)$	$(U-1)(U-2)(U-3)$
$\alpha_{C^\perp,i}$	1	$4(U-1)$	$5(U-1)$
	2	$3(U-1)(2U-3)$	$2(U-1)(3U-5)$
	3	$(U-1)(U-2)(U-3)$	$(U-1)(U-2)(U-3)$
$\lambda_{C,i}$	1	$6(U-1)$	$6(U-1)$
	2	$2(U-1)(7U-12)$	$2(U-1)(7U-11)$
	3	$12(U-1)(U-2)(U-3)$	$13(U-1)(U-2)(U-3)$
$\lambda_{C^\perp,i}$	1	$6(U-1)$	$6(U-1)$
	2	$13(U-1)^2$	$2(U-1)(7U-11)$
	3	$12(U-1)(U-2)(U-3)$	$13(U-1)(U-2)(U-3)$

We see that the extended coset leader weight enumerator of the two codes are equal, but none of the other polynomials, so they are not defined by the extended coset leader weight enumerator. It is an open question if the list weight enumerator determines any of the polynomials $\alpha_C(X,Y,U)$, $\lambda_{C^\perp}(X,Y,U)$ and $W_C(X,Y,U)$.

The *Newton radius* measures up to which weight all cosets have a unique coset leader. It was introduced by Helleseth and Kløve in [48]. The Newton radius also indicates up to which term the coset leader weight enumerator and list weight enumerator coincide. Therefore, studying the Newton radius might give us more information on the open questions above.

Part III

Codes, arrangements and matroids

7

Introduction to matroids

Matroids were introduced by Whitney [107] and independently by Van der Waerden [97], axiomatizing and generalizing the concepts of "independence" in linear algebra and "cycle-free" in graph theory. Matroid theory makes it possible to study these concept in a more abstract way. Many topics in discrete mathematics have strong connections with matroid theory: for example graph theory, linear algebra, coding theory and projective geometry. Also, matroids have important applications in combinatorial optimization.
If we want to study links between various fields of discrete mathematics – like in this thesis – matroids are almost unavoidable. This chapter gives a short introduction of the necessary definitions. A characteristic of matroids is, that there are many ways to define them: for an overview of definitions, see Brylawsky's appendix in [105]. For more background reading on matroid theory, see Kung [66], Welsh [103], White [105, 106] or the latest edition of Oxley [77].

7.1 Matroids

Definition 7.1. A *matroid* M is a pair $(E,\mathcal{I})$ consisting of a finite set E and a collection $\mathcal{I}$ of subsets of E called the *independent sets*, such that the following three conditions hold.

(I.1) $\emptyset \in \mathcal{I}$.

(I.2) If $J \subseteq I$ and $I \in \mathcal{I}$, then $J \in \mathcal{I}$.

(I.3) If $I, J \in \mathcal{I}$ and $|I| < |J|$, then there exists a $j \in (J \setminus I)$ such that $I \cup \{j\} \in \mathcal{I}$.

A subset of E that is not independent is called *dependent*. A dependent subset of E for which deleting any element always gives an independent set, is a minimal dependent set or a *circuit*. An independent subset of E for which adding an extra element of E always gives a dependent set, is a maximal independent set or a *basis*. It follows from condition (I.3) that every basis has the same number of elements. This is called the *rank* of the matroid. We define the rank of a subset of E to be the size of the largest independent set contained in it. A subset of E for which adding an extra element of E always gives a set of higher rank, is a *closed set* or *flat*. (In fact, we can show that by adding an extra element to a subset, the rank will increase by at most one.) The *closure* of a subset of E is the intersection of all flats containing it. We summarize all this in the next definition.

Definition 7.2. For a matroid $(E, \mathcal{I})$ its dependent sets, circuits, bases, rank function and flats are defined by

$$\begin{aligned}
\mathcal{D} &= \{D \subseteq E : D \notin \mathcal{I}\},\\
\mathcal{C} &= \{C \subseteq E : C \notin \mathcal{I}, \forall c \in C : C \setminus \{c\} \in \mathcal{I}\},\\
r(J) &= \max\{|J'| : J' \subseteq J, J' \in \mathcal{I}\},\\
\mathcal{B} &= \{B \subseteq E : r(B) = |B| = r(E)\},\\
\mathcal{F} &= \{F \subseteq E : \forall e \in E \setminus F : r(F \cup \{e\}) > r(F)\},\\
\overline{J} &= \cap\{F \in \mathcal{F} : J \subseteq F\}.
\end{aligned}$$

All the properties defined above can each be used to determine a matroid completely. For an overview of equivalent (also called *cryptomorphic*) definitions of matroids, see [105, Appendix].

A well known and, in most cases, easy to handle matroid is the uniform matroid.

Definition 7.3. Let n and k be nonnegative integers such that $k \leq n$. Let $\mathcal{I}_{n,k} = \{I \subseteq [n] : |I| \leq k\}$. Then $U_{n,k} = ([n], \mathcal{I}_{n,k})$ is a matroid that is called the *uniform matroid* of rank k on n elements. A subset B of $[n]$ is a basis of $U_{n,k}$ if and only if $|B| = k$. The rank of a subset J is equal to its size if $|J| < k$ and otherwise equal to k. The dependent sets are the subsets of $[n]$ of size at least $k+1$. The matroid $U_{n,n}$ has no dependent sets and is called *free*.

Let $e, f \in E$ be elements of M. If $\{e\}$ is a dependent set, then e is called a *loop*. If e and f are two distinct elements that are not loops and $r(\{e, f\}) = 1$, then e and f are called *parallel*. A matroid is called *simple* if it has no loops and no parallel elements. For every matroid, we can delete loops and associate every parallel class to one element, to get another matroid. This matroid is the *simplification* $\overline{M}$ of the matroid.

Definition 7.4. Let $M_1 = (E_1, \mathcal{I}_1)$ and $M_2 = (E_2, \mathcal{I}_2)$ be matroids. A map $\varphi : E_1 \to E_2$ is called a *morphism of matroids* if $\varphi(I)$ is dependent in M_2 for all I that are dependent in M_1. The map is called an *isomorphism of matroids* if it is a morphism of matroids and there exists a map $\psi : E_2 \to E_1$ such that it is a morphism of matroids and it is the inverse of φ. The matroids are called *isomorphic* if there is an isomorphism of matroids between them.

7.2 Duality

Because a matroid is completely determined by its set of bases, we can define the *dual* of a matroid in the following way:

Definition 7.5. Let $M = (E, \mathcal{B})$ be a matroid defined by its set of bases. Then its *dual* is the matroid $M^* = (E, \mathcal{B}^*)$ with the same underlying set and set of bases

$$\mathcal{B}^* = \{E \setminus B : B \in \mathcal{B}\}.$$

We can express the rank function of the dual matroid in terms of the rank function of the matroid itself.

Proposition 7.6. *Let $(E,\mathcal{I})$ be a matroid with rank function r. Then the dual matroid has rank function r^* given by*

$$r^*(J) = |J| - r(E) + r(E \setminus J).$$

Proof. The proof is based on the observation that $r(J) = \max_{B\in\mathcal{B}} |B \cap J|$ and $B \setminus J = B \cap (E \setminus J)$.

$$\begin{aligned}
r^*(J) &= \max_{B\in\mathcal{B}^*} |B \cap J| \\
&= \max_{B\in\mathcal{B}} |(E \setminus B) \cap J| \\
&= \max_{B\in\mathcal{B}} |J \setminus B| \\
&= |J| - \min_{B\in\mathcal{B}} |J \cap B| \\
&= |J| - (|B| - \max_{B\in\mathcal{B}} |B \setminus J|) \\
&= |J| - r(E) + \max_{B\in\mathcal{B}} |B \cap (E \setminus J)| \\
&= |J| - r(E) + r(E \setminus J).
\end{aligned}$$

□

The following property links circuits to flats of rank $r^*(E) - 1$ in the dual matroid.

Proposition 7.7. *Let M be a matroid and let C be a circuit of M. Then the complement of C in E is a flat of M^* of rank $r^*(M^*) - 1$.*

Proof. First, we consider what happens if we add an element $c \in C$ to $E \setminus C$.

$$\begin{aligned}
r^*((E \setminus C) \cup \{c\}) &= |(E \setminus C) \cup \{c\}| - r(E) + r(C \setminus \{c\}) \\
&= |(E \setminus C)| + 1 - r(E) + r(C) \\
&= r^*(E \setminus C) + 1.
\end{aligned}$$

So $E \setminus C$ is a flat of M^*. Now we determine the rank of $E \setminus C$. By definition, $C \setminus \{c\}$ is an independent set, so it is a subset of a basis B of M. The complement $B^* = E \setminus B$ is a basis of M^* and therefore has rank $r^*(M^*)$. Because B^* is contained in $(E \setminus C) \cup \{c\}$, we have $r^*((E \setminus C) \cup \{c\}) = r^*(B^*) = r(M^*)$. This means $E \setminus C$ is a flat of rank $r^*(M^*) - 1$. □

A circuit of M^* is called a *cocircuit* of M. The flats of size $r(M) - 1$ are sometimes called *hyperplanes*, but we will not use this terminology to avoid confusion with hyperplane arrangements.

7.3 Matroids, arrangements and codes

Let G be a $k \times n$ matrix with entries in a field $\mathbb{F}$. Let E be the set $[n]$ indexing the columns of G and $\mathcal{I}_G$ be the collection of all subsets I of E such that the submatrix G_I

consisting of the columns of G at the positions of I are independent. Then $M_G = (E, \mathcal{I}_G)$ is a matroid. Suppose that $\mathbb{F}$ is a finite field and G_1 and G_2 are generator matrices of a code C, then $(E, \mathcal{I}_{G_1}) = (E, \mathcal{I}_{G_2})$. So, the matroid $M_C = (E, \mathcal{I}_C)$ of a code C is well defined by $(E, \mathcal{I}_G)$ for some generator matrix G of C. The function $r(J)$ as defined in Lemma 2.6 is exactly the rank function of the matroid M_C. Also, the matroids $(M_C)^*$ and $M_{C^\perp}$ are isomorphic.

If C is degenerate, then there is a position i such that $c_i = 0$ for every codeword $\mathbf{c} \in C$. All such positions correspond one-to-one with loops of M_C. If C is nondegenerate, then M_C has no loops, and the positions i and j with $i \neq j$ are parallel in M_C if and only if the i-th column of G is a scalar multiple of the j-th column. The code C is projective if and only if the arrangement $\mathcal{A}_G$ is simple if and only if the matroid M_C is simple. An $[n,k]$ code C is MDS if and only if the matroid M_C is the uniform matroid $U_{n,k}$.

Let J be a subset of $[n]$ and let $C(J)$ as in Definition 2.5. Then the closure $\overline{J}$ is equal to the complement in $[n]$ of the support of $C(J)$ and thus $C(J) = C(\overline{J})$.

A matroid M is called *realizable* or *representable* over the field $\mathbb{F}$ if there exists a matrix G with entries in $\mathbb{F}$ such that M is isomorphic with M_G. Linear codes correspond to matroids that are representable over finite fields. But this is not a one-to-one correspondence: codes that are not equivalent can correspond to the same matroid. See Theorem 2.27: MDS codes with the same parameters need not to be equivalent as codes, but they do correspond to the same uniform matroid. Also, a matroid can be representable over several finite fields of different characteristic: these representations clearly do not give equivalent codes.
Deciding whether a matroid is representable, and over which field, is an important topic in matroid theory. For more on representable matroids see Tutte [96] and Whittle [108, 109].

7.4 Internal and external activity

Let $M = (E, \mathcal{B})$ be a matroid. Let $B \in \mathcal{B}$ be a basis and e an element in $E \setminus B$. Then $B \cup \{e\}$ is a dependent set, so it contains a circuit. It is not difficult to show (but it needs a little more theory then explained in this chapter) that this circuit is unique: we call it the *fundamental circuit* of e with respect to B. It is clear that e has to be contained in its fundamental circuit. Dually, let $e \in B$. Then $(E \setminus B) \cup \{e\}$ is a dependent set in M^* and it contains a unique cocircuit. This cocircuit is called the *fundamental cocircuit* of e with respect to B. Fundamental circuits and cocircuits play an important role in the investigation of representable matroids.

DEFINITION 7.8. Let $M = (E, \mathcal{I})$ be a matroid and let ω be a linear order on E. Then the tuple $(E, \omega, \mathcal{I})$ is called an *ordered matroid*.

Choosing an ordering for a matroid can be compared to choosing a basis for a linear vector space (or, choosing a generator matrix for a linear code): it makes proving some theorems much easier, but you have to take care that the result is independent of the choice of the basis. In general, we will not assume any ordering on a matroid, unless it is specified otherwise.
Let M be an ordered matroid and let B be a basis of M. An element $e \in E \setminus B$ is called

externally B-active if it is the smallest element of its fundamental circuit with respect to B for the given ordering. An element $e \in B$ is *internally B-active* if it is the smallest element of its fundamental cocircuit with respect to B. The set of internally B-active elements in M is equal to the set of externally $E \setminus B$-active elements in M^*.

Definition 7.9. Let $M = (E, \mathcal{I})$ be an ordered matroid. The *external activity* $\epsilon(B)$ of a basis B is the number of externally B-active elements. The *internal activity* $\iota(B)$ of a basis B is the number of internally B-active elements.

In this thesis we will use ordered matroid only if we want to say something about internal and external activity. See Etienne and Las Vergnas [40] for more information about the topic. We will use Definition 7.9 in Chapter 12 to define the spectrum polynomial.

8
The Tutte polynomial

One of the most studied polynomials in matroid theory is the Tutte polynomial. It has its origin in graph theory, see [94, 95]. Its importance comes from the fact that the Tutte polynomial obeys a formula for *deletion and contraction*. Moreover, all matroid invariants that obey the same rule are evaluations of the Tutte polynomial. We refer to Brylawsky and Oxley [27] for an exhaustive treatment of this matter.

It was shown by Greene [43] that the weight enumerator of a linear code is one of the many matroid invariants that is determined by the Tutte polynomial. In this chapter we generalize the result of Greene to the extended and generalized weight enumerators. The result of Greene goes one way: the weight enumerator of a code is determined by the Tutte polynomial of the associated matroid, but not the other way around. For the extended weight enumerator and the set of generalized weight enumerators, this is a two-way equivalence: the extended weight enumerator determines the Tutte polynomial, and vice versa.

Just as Greene used his connection between the Tutte polynomial and the weight enumerator to give a proof of the MacWilliams identity, we will use the connection between the extended weight enumerator and the Tutte polynomial to prove the MacWilliams identity for the extended weight enumerator (see Theorem 2.19). Because of the two-way equivalence between the extended weight enumerator and the Tutte polynomial, the proof reduces to rewriting.

The results in this chapter originate from [52]. Closely related results on codes, matroids and MacWilliams type identities can be found in the work of Barg [9] and Britz et al. [18, 19, 17, 21, 23].

8.1 Weight enumerators and the Tutte polynomial

Definition 8.1. For a matroid $M = (E, \mathcal{I})$ with rank function r the *Whitney rank generating function* is defined by

$$R_M(X,Y) = \sum_{J \subseteq E} X^{r(E)-r(J)} Y^{|J|-r(J)}$$

and the *Tutte polynomial* is defined by

$$t_M(X,Y) = \sum_{J \subseteq E} (X-1)^{r(E)-r(J)}(Y-1)^{|J|-r(J)}.$$

In other words,

$$t_M(X,Y) = R_M(X-1, Y-1).$$

REMARK 8.2. Both polynomials had been studied for decades before they were discovered to be so closely related. For a nice historical overview, see Section 3.1 of [83]. The Tutte polynomial was originally defined on graphs. In matroid terms, this definition reads

$$t_M(X,Y) = \sum_{B \in \mathcal{B}} X^{\iota(B)} Y^{\epsilon(B)}$$

where $\iota(B)$ and $\epsilon(B)$ are the internal and external activity of the basis B as in Definition 7.9. This formula explains why the coefficients of the Tutte polynomial, just as the coefficients of the rank generating function, are always positive.

As we have seen, we can interpret a linear $[n,k]$ code C over $\mathbb{F}_q$ as a matroid via the columns of a generator matrix.

PROPOSITION 8.3. *Let C be an $[n,k]$ code over $\mathbb{F}_q$. Then the Tutte polynomial $t_C(X,Y)$ associated with the matroid M_C of the code C is*

$$t_C(X,Y) = \sum_{t=0}^{n} \sum_{|J|=t} (X-1)^{l(J)}(Y-1)^{l(J)-(k-t)}.$$

PROOF. This follows from $l(J) = k - r(J)$ by Lemma 2.6 and $r(M) = k$. □

This formula and Proposition 2.18 suggest the next connection between the weight enumerator and the Tutte polynomial. Greene [43] was the first to notice this connection.

THEOREM 8.4. *Let C be an $[n,k]$ code over $\mathbb{F}_q$. Then the following holds for the Tutte polynomial and the extended weight enumerator:*

$$W_C(X,Y,U) = (X-Y)^k Y^{n-k}\ t_C\left(\frac{X+(U-1)Y}{X-Y}, \frac{X}{Y}\right).$$

PROOF. By using Proposition 8.3 about the Tutte polynomial, rewriting, and Proposition 2.18 we get

$$\begin{aligned}
&(X-Y)^k Y^{n-k}\ t_C\left(\frac{X+(U-1)Y}{X-Y}, \frac{X}{Y}\right) \\
&= (X-Y)^k Y^{n-k} \sum_{t=0}^{n} \sum_{|J|=t} \left(\frac{UY}{X-Y}\right)^{l(J)} \left(\frac{X-Y}{Y}\right)^{l(J)-(k-t)} \\
&= (X-Y)^k Y^{n-k} \sum_{t=0}^{n} \sum_{|J|=t} U^{l(J)} Y^{k-t} (X-Y)^{-(k-t)} \\
&= \sum_{t=0}^{n} \sum_{|J|=t} U^{l(J)} (X-Y)^t Y^{n-t} \\
&= W_C(X,Y,U).
\end{aligned}$$

□

We use the extended weight enumerator here, because extending a code does not change the generator matrix and therefore leaves the matroid M_C invariant. The converse of this theorem is also true: the Tutte polynomial is completely defined by the extended weight enumerator.

Theorem 8.5. *Let C be an $[n,k]$ code over $\mathbb{F}_q$. Then the following holds for the extended weight enumerator and the Tutte polynomial:*

$$t_C(X,Y) = Y^n(Y-1)^{-k}W_C(1,Y^{-1},(X-1)(Y-1)).$$

Proof. The proof of this theorem is analogous to the proof of the previous theorem.

$$\begin{aligned}
&Y^n(Y-1)^{-k}W_C(1,Y^{-1},(X-1)(Y-1))\\
&= \quad Y^n(Y-1)^{-k}\sum_{t=0}^{n}\sum_{|J|=t}((X-1)(Y-1))^{l(J)}\,(1-Y^{-1})^tY^{-(n-t)}\\
&= \quad \sum_{t=0}^{n}\sum_{|J|=t}(X-1)^{l(J)}(Y-1)^{l(J)}Y^{-t}(Y-1)^tY^{-(n-t)}Y^n(Y-1)^{-k}\\
&= \quad \sum_{t=0}^{n}\sum_{|J|=t}(X-1)^{l(J)}(Y-1)^{l(J)-(k-t)}\\
&= \quad t_C(X,Y).
\end{aligned}$$

□

We see that the Tutte polynomial depends on two variables, while the extended weight enumerator depends on three variables. This is no problem, because the weight enumerator is given in its homogeneous form here: we can view the extended weight enumerator as a polynomial in two variables via $W_C(Z,U) = W_C(1,Z,U)$.
Greene [43] already showed that the Tutte polynomial determines the weight enumerator, but not the other way round. By using the extended weight enumerator, we get a two-way equivalence and the proof reduces to rewriting.

We can also give expressions for the generalized weight enumerator in terms of the Tutte polynomial, and the other way round. The first formula was found by Britz [21] and independently by Jurrius [52].

Theorem 8.6. *For the generalized weight enumerator of an $[n,k]$ code C and the associated Tutte polynomial we have that $W_C^{(r)}(X,Y)$ is equal to*

$$\frac{1}{\langle r\rangle_q}\sum_{j=0}^{r}\begin{bmatrix} r \\ j \end{bmatrix}_q (-1)^{r-j}q^{\binom{r}{j}}(X-Y)^kY^{n-k}\; t_C\left(\frac{X+(q^j-1)Y}{X-Y},\frac{X}{Y}\right).$$

And, conversely,

$$t_C(X,Y) = Y^n(Y-1)^{-k}\sum_{r=0}^{k}\left(\prod_{j=0}^{r-1}((X-1)(Y-1)-q^j)\right)W_C^{(r)}(1,Y^{-1}).$$

Proof. For the first formula, use Theorems 2.25 and 8.4. Use Theorems 2.23 and 8.5 for the second formula. □

8.2 MacWilliams type property for duality

For both codes and matroids we defined the dual structure. These objects obviously completely define there dual. But how about the various polynomials associated to a code and a matroid? Does a polynomial associated to a code/matroid determine the same polynomial associated to the dual code/matroid? We already saw that there is in fact such a relation for the weight enumerator and the extended weight enumerator, namely the MacWilliams identities in Theorem 1.8 and Theorem 2.19. To prove these theorems, we may use the relation between the extended weight enumerator and the Tutte polynomial, because of the following simple and very useful relation between the Tutte polynomial of a matroid and its dual.

Theorem 8.7. *Let $t_M(X,Y)$ be the Tutte polynomial of a matroid M, and let M^* be the dual matroid. Then*

$$t_M(X,Y) = t_{M^*}(Y,X).$$

Proof. Let M be a matroid on the set E. Then M^* is a matroid on the same set. By the definition of the dual matroid, we have $r^*(E) + r(E) = |E|$. In Proposition 7.6 we proved $r^*(J) = |J| - r(E) + r(E \setminus J)$. Substituting these relations into the definition of the Tutte polynomial for the dual code, gives

$$\begin{aligned} t_{M^*}(X,Y) &= \sum_{J\subseteq E} (X-1)^{r^*(E)-r^*(J)}(Y-1)^{|J|-r^*(J)} \\ &= \sum_{J\subseteq E} (X-1)^{r^*(E)-|J|-r(E\setminus J)+r(E)}(Y-1)^{r(E)-r(E\setminus J)} \\ &= \sum_{J\subseteq E} (X-1)^{|E\setminus J|-r(E\setminus J)}(Y-1)^{r(E)-r(E\setminus J)} \\ &= t_M(Y,X) \end{aligned}$$

In the last step, we use that the summation over all $J \subseteq E$ is the same as a summation over all $E \setminus J \subseteq E$. This proves the theorem. □

We will now prove Theorem 2.19:

$$W_{C^\perp}(X,Y,U) = U^{-k} W_C(X+(U-1)Y, X-Y, U).$$

Proof (Theorem 2.19). Let G be the matroid associated to the code. Using the previous theorem and the relation between the weight enumerator and the Tutte polynomial from Theorem 8.4, we find

$$\begin{aligned} & U^{-k} W_C(X+(U-1)Y, X-Y, U) \\ &= U^{-k}(UY)^k (X-Y)^{n-k}\, t_C\left(\frac{X}{Y}, \frac{X+(U-1)Y}{X-Y}\right) \\ &= Y^k (X-Y)^{n-k}\, t_{C^\perp}\left(\frac{X+(U-1)Y}{X-Y}, \frac{X}{Y}\right) \\ &= W_{C^\perp}(X,Y,U). \end{aligned}$$

Note in the last step that $\dim C^{\perp} = n - k$, and $n - (n - k) = k$. □

We can use the relations in Theorems 2.23 and 2.25 to prove the MacWilliams identities for the generalized weight enumerator.

Theorem 8.8. *Let C be a code and let $C^{\perp}$ be its dual. Then the generalized weight enumerators of C completely determine the generalized weight enumerators of $C^{\perp}$ and vice versa, via the following formula:*

$$W_{C^{\perp}}^{(r)}(X,Y) = \sum_{j=0}^{r}\sum_{l=0}^{j}(-1)^{r-j}\frac{q^{\binom{r-j}{2}-j(r-j)-l(j-l)-jk}}{\langle r-j\rangle_q\langle j-l\rangle_q}W_C^{(l)}(X+(q^j-1)Y,X-Y).$$

Proof. We write the generalized weight enumerator in terms of the extended weight enumerator, use the MacWilliams identities for the extended weight enumerator, and convert back to the generalized weight enumerator.

$$\begin{aligned}
W_{C^{\perp}}^{(r)}(X,Y) &= \frac{1}{\langle r\rangle_q}\sum_{j=0}^{r}\begin{bmatrix} r \\ j \end{bmatrix}_q (-1)^{r-j}q^{\binom{r-j}{2}}\,W_{C^{\perp}}(X,Y,q^i) \\
&= \sum_{j=0}^{r}(-1)^{r-j}\frac{q^{\binom{r-j}{2}-j(r-j)}}{\langle j\rangle_q\langle r-j\rangle_q}q^{-jk}\,W_c(X+(q^j-1)Y,X-Y,q^j) \\
&= \sum_{j=0}^{r}(-1)^{r-j}\frac{q^{\binom{r-j}{2}-j(r-j)-jk}}{\langle j\rangle_q\langle r-j\rangle_q} \\
&\qquad \times\sum_{l=0}^{j}\frac{\langle j\rangle_q}{q^{l(j-l)}\langle j-l\rangle_q}\,W_C^{(l)}(X+(q^j-1)Y,X-Y) \\
&= \sum_{j=0}^{r}\sum_{l=0}^{j}(-1)^{r-j}\frac{q^{\binom{r-j}{2}-j(r-j)-l(j-l)-jk}}{\langle r-j\rangle_q\langle j-l\rangle_q} \\
&\qquad \times W_C^{(l)}(X+(q^j-1)Y,X-Y).
\end{aligned}$$

□

This theorem was proved by Kløve [62]. This proof uses only half of the relations between the generalized weight enumerator and the extended weight enumerator: using both makes the proof much shorter.

9

Introduction to geometric lattices

In matroid theory, an interesting structure associated to a matroid is its *lattice of flats*: it is at the basis of many enumeration problems in matroid theory. This lattice is a geometric lattice. There are, roughly speaking, two ways to define a geometric lattice: as the lattice of flats of a matroid, or via the combinatorics of posets, lattices and the Möbius function. Since we already introduced matroids, the first approach is fairly short: see Section 9.7.
It requires some work to define a geometric lattice via lattices. However, the theory of lattices is very useful when studying hyperplane arrangements, as we will see in the next chapter. Therefore, we consider in this chapter the theory of posets, lattices and the Möbius function. Geometric lattices are defined and their connection with matroids are given. We will give several examples of the theory. For more background on the combinatorics in this chapter, see Aigner [1], Rota [81], or Stanley [87]. The connection with hyperplane arrangements can be found in Cartier [29], Orlik and Terao [76], or Stanley [88].

9.1 Posets

Definition 9.1. Let P be a set and $\leq$ a relation on P such that for all $x, y, z \in P$:

(PO.1) $x \leq x$ *(reflexive)*.

(PO.2) If $x \leq y$ and $y \leq x$, then $x = y$ *(anti-symmetric)*.

(PO.3) If $x \leq y$ and $y \leq z$, then $x \leq z$ *(transitive)*.

The pair $(P, \leq)$, or just P, is called a *poset* with *partial order* $\leq$ on the set P.

The elements x and y in P are called *comparable* if $x \leq y$ or $y \leq x$. If $x \leq y$ and $x \neq y$, we say $x < y$. We use the following notation for some parts of a poset we often refer to.

$$\begin{array}{rcl} P_x & = & \{y \in P : x \leq y\} \\ P^x & = & \{y \in P : y \leq x\} \\ [x, y] & = & \{z \in P : x \leq z \leq y\} \end{array}$$

We call $[x, y]$ the *interval* between x and y. Note that $[x, y] = P_x \cap P^y$.

Let P be a poset. If P has an element 0_P such that 0_P is the unique minimal element of P, then 0_P is called the *minimum* of P. Similarly 1_P is called the *maximum* of P if 1_P is the unique maximal element of L. If $x, y \in P$ and $x \leq y$, then the interval $[x, y]$ has minimum x and maximum y. Suppose that P has 0_P and 1_P as minimum and maximum, also denoted by 0 and 1, respectively. Then $0 \leq x \leq 1$ for all $x \in P$.
Let $x, y \in P$. We call y a *cover* of x if $x < y$ and there is no z such that $x < z < y$. We denote this by $x \lessdot y$. The elements x and y have a *least upper bound* if there is a $z \in P$ such that $x \leq z$ and $y \leq z$, and if $x \leq w$ and $y \leq w$, then $z \leq w$ for all $w \in P$. If x and y have a least upper bound, then such an element is unique and it is called the *join* of x and y and is denoted by $x \vee y$. Similarly the *greatest lower bound* of x and y is defined. If it exists, then it is unique and it is called the *meet* of x and y and denoted by $x \wedge y$. We summarize this in the following definition.

DEFINITION 9.2. For every poset P and elements $x, y \in P$, we can define the following.

0_P	The minimum of P.
1_P	The maximum of P.
$x \lessdot y$	y is a cover of x.
$x \vee y$	The least upper bound, or join, of x and y.
$x \wedge y$	The greatest lower bound, or meet, of x and y.

A poset L is called a *lattice* if $x \vee y$ and $x \wedge y$ exist for all $x, y \in L$.

REMARK 9.3. Let $(P, \leq)$ be a finite poset with maximum 1 such that $x \wedge y$ exists for all $x, y \in P$. The collection $\{z : x \leq z, y \leq z\}$ is finite and not empty, since it contains 1. The meet of all the elements in this collection is well defined and is given by

$$x \vee y = \bigwedge \{z : x \leq z, y \leq z\}.$$

Hence P is a lattice. Similarly, P is a lattice if P is a finite poset with minimum 0 such that $x \vee y$ exists for all $x, y \in P$, since $x \wedge y = \bigvee \{z : z \leq x, z \leq y\}$.

9.2 Chains and the Möbius function

A *chain* is a (subset of a) poset in which any two elements are comparable. We call a chain *finite* (or *infinite*) when the cardinality of the chain is finite (or infinite). Let $r \geq 0$ be an integer and let $x, y \in P$. If a chain is finite, we can write it as $x = x_0 < x_1 < \cdots < x_r = y$ and we say this is a chain from x to y of length r. We denote by $c_r(x, y)$ the number of chains of length r from x to y. The number $c_r(x, y)$ is finite if the poset P is finite. The poset is called *locally finite* if $c_r(x, y)$ is finite for all $x, y \in P$ and every integer $r \geq 0$. A poset P is locally finite if and only if $[x, y]$ is finite for all $x \leq y$ in P. Note that a poset can be locally finite and still have infinite chains.

PROPOSITION 9.4. *Let P be a locally finite poset and let $x \leq y$ in P. Then*

(N.1) $c_0(x,y) = 0$ *if* x *and* y *are not comparable.*

(N.2) $c_0(x,x) = 1$ *and* $c_r(x,x) = 0$ *for all* $r > 0$*, and* $c_0(x,y) = 0$ *if* $x < y$*.*

(N.3) $c_{r+1}(x,y) = \sum_{x \leq z < y} c_r(x,z) = \sum_{x < z \leq y} c_r(z,y)$*.*

Proof. Statements (N.1) and (N.2) are trivial. Let $z < y$ and let $x = x_0 < x_1 < \cdots < x_r = z$ be a chain of length r from x to z. Then $x = x_0 < x_1 < \cdots < x_r < x_{r+1} = y$ is a chain of length $r+1$ from x to y and every chain of length $r+1$ from x to y is obtained uniquely in this way. Hence $c_{r+1}(x,y) = \sum_{x \leq z < y} c_r(x,z)$. The last equality is proved similarly. □

The chain $x = y_0 < y_1 < \cdots < y_s = y$ from x to y is called an *extension* of the chain $x = x_0 < x_1 < \cdots < x_r = y$ if $\{x_0, x_1, \ldots, x_r\}$ is a subset of $\{y_0, y_1, \ldots, y_s\}$. A chain from x to y is called *maximal* if there is no extension to a longer chain from x to y. In a maximal chain, we have that $x = x_0 \lessdot x_1 \lessdot \cdots \lessdot x_r = y$.

Definition 9.5. The *Möbius function* of a locally finite poset P, denoted by μ_P or μ, is defined by

$$\mu(x,y) = \sum_{r=0}^{\infty} (-1)^r c_r(x,y).$$

We write $\mu(x) = \mu(0,x)$ and $\mu(P) = \mu(0,1)$ if P is finite.

Proposition 9.6. *Let* P *be a locally finite poset. Then for all* $x, y \in P$*:*

(M.1) $\mu(x,y) = 0$ *if* x *and* y *are not comparable.*

(M.2) $\mu(x,x) = 1$*.*

(M.3) If $x < y$*, then* $\sum_{x \leq z \leq y} \mu(x,z) = \sum_{x \leq z \leq y} \mu(z,y) = 0$*.*

(M.4) If $x < y$*, then* $\mu(x,y) = -\sum_{x \leq z < y} \mu(x,z) = -\sum_{x < z \leq y} \mu(z,y)$*.*

Proof. (M.1) and (M.2) follow from (N.1) and (N.2), respectively, of Proposition 9.4. (M.3) is clearly equivalent to (M.4). If $x < y$, then $c_0(x,y) = 0$. So

$$\begin{aligned}
\mu(x,y) &= \sum_{r=1}^{\infty} (-1)^r c_r(x,y) \\
&= \sum_{r=0}^{\infty} (-1)^{r+1} c_{r+1}(x,y) \\
&= -\sum_{r=0}^{\infty} (-1)^r \sum_{x \leq z < y} c_r(x,z) \\
&= -\sum_{x \leq z < y} \sum_{r=0}^{\infty} (-1)^r c_r(x,z) \\
&= -\sum_{x \leq z < y} \mu(x,z).
\end{aligned}$$

The first and last equality use the definition of μ. The second equality starts counting at $r = 0$ instead of $r = 1$, the third uses (N.3) of Proposition 9.4 and in the fourth the order of summation is interchanged. □

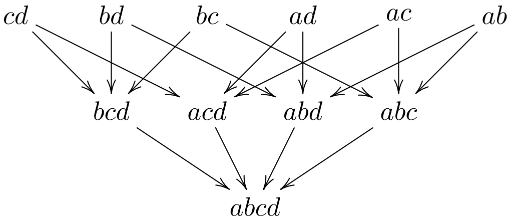


FIGURE 9.1: The Hasse diagram of a poset. The elements are the subsets of $\{a, b, c, d\}$ of size at least 2 and the partial order is given by inverse inclusion.

REMARK 9.7. (M.2) and (M.4) of Proposition 9.6 can be used as an alternative way to compute $\mu(x, y)$ by induction.

9.3 More on posets and lattices

DEFINITION 9.8. A poset can be visualized by a *Hasse diagram*. The Hasse diagram of a poset P is a directed graph that has the elements of P as vertices, and there is a directed edge from y to x if and only if y is a cover of x.

See Figure 9.1 for an example of a poset with a minimum but without a maximum. If we "turn upside down" the Hasse diagram of a poset, we get the inverse poset.

DEFINITION 9.9. Let P be a poset. The *inverse poset* $i(P)$ of P contains the same elements as P, but the order is reversed: $x \geq_i y$ in the inverse poset if and only if $x \leq y$ in the original poset.

If P is a finite poset, then the Möbius function $\mu_P(y, x)$ is well-defined and $\mu_{i(P)}(x, y) = \mu_P(y, x)$. If the poset has a minimum and maximum, then the inverse poset has a maximum and minimum: $0_P = 1_{i(P)}$ and $1_P = 0_{i(P)}$. The Hasse diagram of $i(P)$ is obtained by reversing all arrows in the Hasse diagram of P. Sometimes the inverse poset is called the *dual* poset. We will not use this terminology, because it does not coincide with the notion of "dual" that we use for codes and matroids.

DEFINITION 9.10. Let $(P_1, \leq_1)$ and $(P_2, \leq_2)$ be posets. A map $\varphi : P_1 \to P_2$ is called *monotone* if $\varphi(x) \leq_2 \varphi(y)$ for all $x \leq_1 y$ in P_1. The map φ is called *strictly monotone* if $\varphi(x) <_2 \varphi(y)$ for all $x <_1 y$ in P_1. The map is called an *isomorphism of posets* if it is strictly monotone and there exists a strictly monotone map $\psi : P_2 \to P_1$ that is the inverse of φ. The posets are called *isomorphic* if there is an isomorphism of posets between them.

If $\varphi : P_1 \to P_2$ is an isomorphism between locally finite posets with a minimum, then $\mu_{P_2}(\varphi(x), \varphi(y)) = \mu_{P_1}(x, y)$ for all x, y in P_1. If $(L_1, \leq_1)$ and $(L_2, \leq_2)$ are isomorphic posets and L_1 is a lattice, then L_2 is also a lattice.

9.4 Applications and examples

In this section we will see some examples to motivate the study of posets, lattices and the Möbius function.

Definition 9.11. Let P be a locally finite poset with a minimum element. Let A be an abelian group and $f : P \to A$ a map from P to A. The *sum function* $\hat{f}$ of f is defined by

$$\hat{f}(x) = \sum_{y \leq x} f(y).$$

Define similarly the sum function $\check{f}$ of f by $\check{f}(x) = \sum_{x \leq y} f(y)$ if P is a locally finite poset with a maximum element.

Note that the sum function is well-defined, because in a locally finite poset all intervals are finite, and in particular $[0, x]$ and $[x, 1]$, if the poset has a minimum and maximum element, respectively.

Theorem 9.12 (Möbius inversion formula). *Let P be a locally finite poset with a minimum element. Then*

$$f(x) = \sum_{y \leq x} \mu(y, x)\hat{f}(y).$$

Similarly, $f(x) = \sum_{x \leq y} \mu(x, y)\check{f}(y)$ if P is a locally finite poset with a maximum element.

Proof. Let x be an element of P. Then

$$\begin{aligned}
\sum_{y \leq x} \mu(y, x)\hat{f}(y) &= \sum_{y \leq x} \sum_{z \leq y} \mu(y, x) f(z) \\
&= \sum_{z \leq x} f(z) \sum_{z \leq y \leq x} \mu(y, x) \\
&= f(x)\mu(x, x) + \sum_{z < x} f(z) \sum_{z \leq y \leq x} \mu(y, x) \\
&= f(x).
\end{aligned}$$

The first equality uses the definition of $\hat{f}(y)$. In the second equality the order of summation is interchanged. In the third equality the first summation is split in the parts $z = x$ and $z < x$, respectively. Finally $\mu(x, x) = 1$ and the second summation is zero for all $z < x$, by Proposition 9.6. The proof of the second equality is similar. □

Example 9.13. Let L be the collection of all finite subsets of a given set $\mathcal{X}$. Let $\leq$ be defined by the inclusion, that means $I \leq J$ if and only if $I \subseteq J$. Then $0_L = \emptyset$, and L has a maximum if and only if $\mathcal{X}$ is finite in which case $1_L = \mathcal{X}$. For $\mathcal{X} = \{a, b, c, d\}$ the Hasse diagram of the lattice is given in Figure 9.2.
Let $I, J \in L$ and $I \leq J$. Then $|I| \leq |J| < \infty$. Let $m = |J| - |I|$. Then

$$c_r(I, J) = \sum_{m_1 < m_2 < \ldots < m_{r-1} < m} \binom{m_2}{m_1} \binom{m_3}{m_2} \cdots \binom{m}{m_{r-1}}.$$

Hence L is locally finite. L is finite if and only if $\mathcal{X}$ is finite. Furthermore, $I \vee J = I \cup J$ and $I \wedge J = I \cap J$, so L is a lattice. Using Remark 9.7 we see that $\mu(I, J) = (-1)^{|J|-|I|}$ if $I \leq J$. This is much easier than computing $\mu(I, J)$ by means of Definition 9.5.

Example 9.14. Let $\mathcal{X} = [n]$ and let k be an integer between 0 and n. Let $L_k = \{\mathcal{X}\}$ and L_i be the collection of all subsets of $\mathcal{X}$ of size i for all $i < k$. Let the partial order be given by the inclusion. Then L is a poset and $\mu(I, J) = (-1)^{|J|-|I|}$ if $I \leq J$ and $|J| < k$ as in Example 9.13, and $\mu(I, \mathcal{X}) = -\sum_{I \leq J < \mathcal{X}} (-1)^{|J|-|I|}$ for all $I < \mathcal{X}$ by Proposition 9.6.

Example 9.15. Now suppose again that $\mathcal{X} = [n]$. Let L be the poset of subsets of $\mathcal{X}$. Let $A_1, \ldots, A_n$ be a collection of subsets of a finite set A. Define for a subset J of $\mathcal{X}$

$$A_J = \bigcap_{j \in J} A_j \quad \text{and} \quad f(J) = \left| A_J \setminus \left(\bigcup_{I<J} A_I \right) \right| .$$

Then A_J is the disjoint union of the subsets $A_I \setminus (\bigcup_{K<I} A_K)$ for all $I \leq J$. Hence the sum function is equal to

$$\hat{f}(J) = \sum_{I \leq J} f(I) = \sum_{I \leq J} \left| A_I \setminus \left(\bigcup_{K<I} A_K \right) \right| = |A_J|.$$

Möbius inversion gives that

$$\left| A_J \setminus \left(\bigcup_{I<J} A_I \right) \right| = \sum_{I \leq J} (-1)^{|J|-|I|} |A_I|,$$

which is called the *principle of inclusion/exclusion*.

Example 9.16. A variant of the principle of inclusion/exclusion is given as follows. Let $H_1, \ldots, H_n$ be a collection of subsets of a finite set H. Let L be the poset of all intersections of the H_j with the reverse inclusion as partial order. Then H is the minimum of L and $H_1 \cap \cdots \cap H_n$ is the maximum of L. Let $x \in L$. Define

$$f(x) = \left| x \setminus \left(\bigcup_{x<y} y \right) \right| .$$

Then

$$\check{f}(x) = \sum_{x \leq y} f(y) = \sum_{x \leq y} \left| y \setminus \left(\bigcup_{y<z} z \right) \right| = |x|.$$

Hence

$$\left| x \setminus \left(\bigcup_{x<y} y \right) \right| = \sum_{x \leq y} \mu(x, y) |y|.$$

9.5 Geometric lattices

Definition 9.17. A poset P satisfies the *Jordan-Dedekind property* if all maximal chains between the same elements have the same finite length. If moreover all maximal chains with endpoint x have the same length, this length is called the *rank* of x. We denote it by $r_P(x)$ or simply $r(x)$.

The following proposition follows directly from the definition:

Proposition 9.18. *Let P be a poset with minimum 0. Then P satisfies the Jordan-Dedekind property if and only if it admits a rank function $r : P \to \mathbb{N}_0$ that satisfies the following:*

- $r(0) = 0$*;*
- $x \lessdot y \Rightarrow r(y) = r(x) + 1$*.*

We will define some more properties posets and lattices can have.

Definition 9.19. Let P be a poset with minimum 0. An *atom* is an element $a \in P$ that covers 0. The poset is said to be *atomic* if every element except 0 is the join of atoms.

Definition 9.20. Let L be a lattice. It is called *semimodular* if for all $x, y \in L$

$$x \wedge y \lessdot x \Rightarrow y \lessdot x \vee y.$$

The notion of semimodularity is often encountered in the context of a function. For lattices, we can prove that the same holds.

Lemma 9.21. *A semimodular lattice satisfies the Jordan-Dedekind property.*

Theorem 9.22. *Let L be a lattice with minimum 0. The lattice is semimodular if and only if it has a rank function r such that for all $x, y \in L$*

$$r(x \wedge y) + r(x \vee y) \leq r(x) + r(y).$$

We can now define the notion of a geometric lattice.

Definition 9.23. A lattice is called *geometric* if it is

(GL.1) atomic;

(GL.2) semimodular;

(GL.3) without infinite chains.

Let L be a geometric lattice. We call the set $L_j = \{x \in L : r(x) = j\}$ the j-th *level* of L. The *Hasse diagram* of L is a graph that has the elements of L as vertices. If $x, y \in L$ and $x \lessdot y$, then x and y are connected by an edge. So, only elements between two consecutive levels L_j and L_{j+1} are connected by an edge. See Figure 9.2 for an example. The Hasse diagram of P considered as a poset as in Definition 9.8 is the directed graph with an arrow from y to x if $x, y \in L$ and $x \lessdot y$.

9.6 Some examples of geometric lattices

Example 9.24. Let L be the collection of all finite subsets of a given set $\mathcal{X}$ as in Example 9.13. For $\mathcal{X} = \{a, b, c, d\}$ the Hasse diagram is drawn in Figure 9.2. The atoms are the singleton sets, i.e., the subsets consisting of exactly one element of $\mathcal{X}$. Every $x \in L$ is the finite union of its singleton subsets, so L is atomic and $r(x) = |x|$. Now y covers x

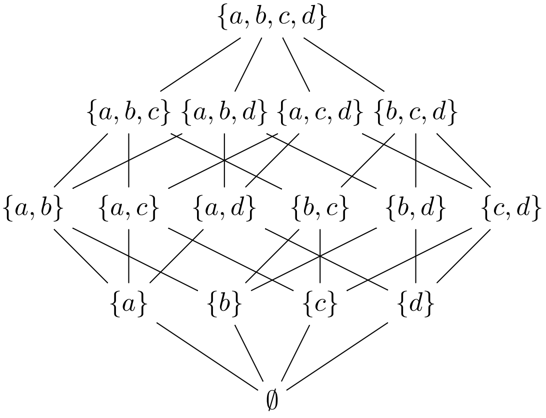

{a, b, c, d}
{a, b, c} {a, b, d} {a, c, d} {b, c, d}
{a, b} {a, c} {a, d} {b, c} {b, d} {c, d}
{a} {b} {c} {d}
∅

FIGURE 9.2: The Hasse diagram of the geometric lattice of all subsets of $\{a, b, c, d\}$

if and only if there is an element Q not in x such that $y = x \cup \{Q\}$. If $x \neq y$ and x and y both cover z, then there is an element P not in z such that $x = z \cup \{P\}$, and there is an element Q not in z such that $y = z \cup \{Q\}$. Now $P \neq Q$, since $x \neq y$. Hence $x \vee y = z \cup \{P, Q\}$ covers x and y. Hence L is semimodular. Furthermore, L is locally finite, and L is a geometric lattice if and only if $\mathcal{X}$ is finite.

EXAMPLE 9.25. Let $\mathbb{F}$ be a field and let $\mathcal{V} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be an n-tuple of nonzero vectors in $\mathbb{F}^k$. Let $L = L(\mathcal{V})$ be the collection of all linear subspaces of $\mathbb{F}^k$ that are generated by subsets of $\mathcal{V}$, with inclusion as partial order. Therefore, L is finite and a fortiori locally finite. By definition $\{\mathbf{0}\}$ is the linear subspace space generated by the empty set. Then $0_L = \{\mathbf{0}\}$ and 1_L is the subspace generated by all $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Furthermore L is a lattice with $x \vee y = x + y$ and

$$x \wedge y = \bigvee\{z : z \leq x, z \leq y\}$$

by Remark 9.3. Let a_j be the linear subspace generated by $\mathbf{v}_j$. Then $a_1, \ldots, a_n$ are the atoms of L. Let x be the subspace generated by $\{\mathbf{v}_j : j \in J\}$. Then $x = \bigvee_{j \in J} a_j$. If x has dimension r, then there exists a subset I of J such that $|I| = r$ and $x = \bigvee i \in I a_i$. Hence L is atomic and $r(x) = \dim(x)$. Now $x \wedge y \subseteq x \cap y$, so

$$r(x \vee y) + r(x \wedge y) \leq \dim(x + y) + \dim(x \cap y) = r(x) + r(y).$$

Hence the semimodular inequality holds and L is a geometric lattice.

EXAMPLE 9.26. Let $\mathbb{F}$ be a field and let $\mathcal{A} = (H_1, \ldots, H_n)$ be an arrangement over $\mathbb{F}$ of hyperplanes in the vector space $V = \mathbb{F}^k$. Let $L = L(\mathcal{A})$ be the collection of all nonempty intersections of elements of $\mathcal{A}$. By definition $\mathbb{F}^k$ is the empty intersection. Define the partial order $\leq$ by

$$x \leq y \quad \text{if and only if} \quad y \subseteq x.$$

Then V is the minimum element and $\{\mathbf{0}\}$ is the maximum element. Furthermore

$$x \vee y = x \cap y \ \text{ if } \ x \cap y \neq \emptyset, \quad \text{and} \quad x \wedge y = \bigcap\{z : x \cup y \subseteq z\}.$$

Suppose that $\mathcal{A}$ is a central arrangement. Then $x \cap y$ is nonempty for all $x, y \in L$, so $x \vee y$ and $x \wedge y$ exist for all $x, y \in L$ and L is a lattice. Let $\mathbf{v}_j = (v_{1j}, \ldots, v_{kj})$ be a nonzero vector such that $\sum_{i=1}^{k} v_{ij} X_i = 0$ is a homogeneous equation of H_j. Let $\mathcal{V} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$. Consider the map $\varphi : L(\mathcal{V}) \to L(\mathcal{A})$ defined by

$$\varphi(x) = \bigcap_{j \in J} H_j \text{ if } x \text{ is the subspace generated by } \{\mathbf{v}_j : j \in J\}.$$

Now $x \subset y$ if and only if $\varphi(y) \subset \varphi(x)$ for all $x, y \in L(\mathcal{V})$. Therefore, φ is a strictly monotone map. Furthermore φ is a bijection and its inverse map is also strictly monotone. Hence $L(\mathcal{V})$ and $L(\mathcal{A})$ are isomorphic lattices. Therefore $L(\mathcal{A})$ is also a geometric lattice.

9.7 Geometric lattices and matroids

The notion of a geometric lattice is *cryptomorphic* to the concept of a matroid: that is, almost equivalent. See [13, 27, 29, 32, 77, 88] for proofs of the statements in this section. First, we see that we can associate a matroid with every geometric lattice.

Proposition 9.27. *Let L be a finite geometric lattice and let $M(L)$ be the set of all atoms of L. Let $\mathcal{I}(L)$ be the collection of all subsets $I = \{a_1, \ldots, a_r\}$ of atoms of $M(L)$ such that $r(a_1 \vee \ldots \vee a_r) = r$. Then $(M(L), \mathcal{I}(L))$ is a matroid.*

On the other hand, we can associate a lattice to every matroid.

Proposition 9.28. *Let M be a matroid and let $L(M)$ be the set of all flats of M. Then $L(M)$ with the inclusion as partial order is a lattice with*

$$F_1 \wedge F_2 = F_1 \cap F_2, \qquad F_1 \vee F_2 = \overline{F_1 \cup F_2}.$$

We call $L(M)$ the lattice of flats *of M.*

This lattice is actually a geometric lattice, but the correspondence between matroids and geometric lattices is in general not one-to-one.

Proposition 9.29. *Let M be a matroid. Then $L(M)$ with the inclusion as partial order is a geometric lattice and $L(M)$ is isomorphic with $L(\overline{M})$.*

The inverse of the first statement also holds, leading to the next theorem.

Theorem 9.30. *A lattice is geometric if and only if it is the lattice of flats of a matroid.*

If we start with a geometric lattice L, then $M(L)$ is a simple matroid and thus $L(M(L)) = L$. If we start with a matroid M, we find that $M(L(M)) = \overline{M}$. We conclude that there is a one-to-one correspondence between simple matroids and geometric lattices.

Example 9.31. The geometric lattice of the matroid $U_{n,k}$, see Definition 7.3, is isomorphic with the lattice consisting of $[n]$ and all its subsets of size at most $k-1$. We will refer to this geometric lattice as the *uniform lattice*. See Figure 9.2 for the geometric lattice of the free matroid of size 4.

Let G be a generator matrix of a code C. The *simplified matrix* $\overline{G}$ is the matrix obtained from G by deleting all zero columns from G and all columns that are a scalar multiple of a previous column. The *simplified code* $\overline{C}$ of C is the code with generator matrix $\overline{G}$. Every simplified code is projective. Note that this definition of $\overline{C}$ does not depend on the choice of the generator matrix G of C. Therefore the matroids $\overline{M}_G$ and $M_{\overline{G}}$ are isomorphic.

10

Characteristic polynomials and their generalizations

In this chapter we treat the characteristic polynomial of a geometric lattice. This is generalized in two variable polynomials in two ways: the *coboundary polynomial* and the *Möbius polynomial.*

The coboundary polynomial was originally studied by Crapo [31] in connection with graph coloring. For simple matroids and codes the coboundary polynomial is equivalent to the Tutte polynomial and the extended weight enumerator.

The Möbius polynomial (also known as "Whitney polynomial") was originally defined by Zaslavsky for hyperplanes [110] and signed graphs [111]. An important property is that it determines the Whitney numbers. We will show that the Möbius function also contains information on the number of minimal subcodes and codewords.

For both polynomials, we show how to calculate them in the specific case of an arrangement and code. The coboundary and Möbius polynomial do, in general, not determine each other. This will be shown by examples of three dimensional codes. More relations between the two polynomials can be found in the next chapter.

10.1 The characteristic and coboundary polynomial

Definition 10.1. Let L be a finite geometric lattice. The *characteristic polynomial* of L is defined by

$$\chi_L(U) = \sum_{x \in L} \mu_L(x) U^{r(L)-r(x)}.$$

The *two-variable characteristic polynomial* or *coboundary polynomial* is defined by

$$\chi_L(S,U) = \sum_{x \in L} \sum_{x \leq y \in L} \mu(x,y) S^{a(x)} U^{r(L)-r(y)}$$

where $a(x)$ is the number of atoms a in L such that $a \leq x$.

Note that $\mu(L) = \mu(0,1) = \chi_L(0)$ and $\chi_L(0,U) = \chi_L(U)$, because for $S = 0$ the only nonzero term has $a(x) = 0$, so $x = 0_L$. Also, the number $a(x)$ is equal to $|x|$ in $M(L)$.

Remark 10.2. Let n be the number of atoms of L. Then the following relation holds for the coboundary polynomial in terms of characteristic polynomials:

$$\chi_L(S,U)=\sum_{i=0}^{n} S^i\chi_i(U) \quad \text{with} \quad \chi_i(U)=\sum_{\substack{x\in L\\ a(x)=i}}\chi_{L_x}(U).$$

The polynomial $\chi_i(U)$ is called the i-*defect* polynomial. See [31, 27].

Example 10.3. Let L be the lattice of all subsets of a given finite set of r elements as in Examples 9.13 and 9.24. Then $r(x)=a(x)$ and $\mu(x,y)=(-1)^{a(y)-a(x)}$ if $x\le y$. Hence

$$\chi_L(U)=\sum_{j=0}^{r}\binom{r}{j}(-1)^jU^{r-j}=(U-1)^r \quad \text{and} \quad \chi_i(U)=\binom{r}{i}(U-1)^{r-i}.$$

Therefore $\chi_L(S,U)=(S+U-1)^r$.

An important property of the coboundary polynomial is that is it is determined by the rank generating function.

Theorem 10.4. *The coboundary polynomial $\chi_L(S,U)$ of a finite geometric lattice L is related to the Whitney rank generating function of $M(L)$ by the formula*

$$\chi_L(S,U)=(S-1)^{r(L)}R_{M(L)}\left(\frac{U}{S-1},S-1\right).$$

Proof. In [30, p. 605], Crapo proved that the coboundary polynomial is equal to

$$\chi_L(S,U)=\sum_{x\subseteq M(L)}(S-1)^{|x|}U^{r(L)-r(x)}.$$

The proof uses a generalization to matroids of the Möbius inversion formula in Theorem 9.12. Crapo used this result in [31, Theorem II] to prove the relation to the rank generating function. In our notation, the proof is as follows.

$$\begin{aligned}\chi_L(S,U) &= \frac{(S-1)^{r(L)-r(x)}}{(S-1)^{r(L)-r(x)}}\sum_{x\subseteq M(L)}(S-1)^{|x|}U^{r(L)-r(x)}\\ &= (S-1)^{r(L)}\sum_{x\subseteq M(L)}(S-1)^{|x|-r(x)}\left(\frac{U}{S-1}\right)^{r(L)-r(x)}\\ &= (S-1)^{r(L)}R_{M(L)}\left(\frac{U}{S-1},S-1\right)\end{aligned}$$

We use that $r(M)=r(M(L))$. □

Corollary 10.5. *We have the following relations between $t_{M(L)}(X,Y)$ and $\chi_L(S,U)$:*

$$\chi_L(S,U)=(S-1)^{r(L)}t_{M(L)}\left(\frac{S+U-1}{S-1},S\right)$$

and, vice versa,

$$t_{M(L)}(X,Y)=(Y-1)^{-r(L)}\chi_L(Y,(X-1)(Y-1)).$$

Therefore the polynomials $\chi_L(S,U)$ and $t_{M(L)}(X,Y)$ completely determine each other.

Starting with an arbitrary matroid M one has the associated geometric lattice $L(M)$, but $M(L(M))$ is isomorphic with M if and only if M is simple by Proposition 9.29. Therefore, $t_M(X,Y)$ and $\chi_{L(M)}(S,U)$ completely determine each other if M is simple, but $t_M(X,Y)$ is a stronger invariant than $\chi_{L(M)}(S,U)$ if M is not simple. We will see a counterexample in Example 10.34. The relation between $t_{M(L)}(X,Y)$ and $\chi_L(S,U)$ shows great similarity with the formula in Theorem 8.5. Combining the relations gives the next theorem.

Theorem 10.6. *For projective codes, the coboundary polynomial of the geometric lattice associated to the code is the reciprocal inhomogeneous form of the extended weight enumerator of the code:*

$$\chi_{L(M_C)}(S,U) = S^n W_C(1,S^{-1},U).$$

This means $\chi_i(U) = A_{n-i}(U)$.

Example 10.7. Consider the uniform lattice $U_{n,k}$. Determining its coboundary polynomial is now quite easy: use Theorem 10.6 and the extended weight enumerator of an MDS code we found in Theorem 2.27.

10.2 The Möbius polynomial and Whitney numbers

Definition 10.8. Let P be a poset that satisfies the Jordan-Dedekind property. Then P has a rank function by Proposition 9.18. The *Möbius polynomial* of P is defined by

$$\mu_P(S,U) = \sum_{x\in P}\sum_{x\leq y\in P} \mu(x,y)S^{r(x)}U^{r(P)-r(y)}.$$

Note that for a geometric lattice L we have $\mu_L(0,U) = \chi_L(0,U) = \chi_L(U)$.

Remark 10.9. Let r be the rank of the geometric lattice L. Then the following relation holds for the Möbius polynomial in terms of characteristic polynomials:

$$\mu_L(S,U) = \sum_{i=0}^{r} S^i \mu_i(U) \quad \text{with} \quad \mu_i(U) = \sum_{x\in L_i} \chi_{L_x}(U).$$

Example 10.10. In Examples 9.24 and 10.3 we considered the lattice L of all subsets of a given finite set of r elements. Since $r(x) = a(x)$ for all $x \in L$, the Möbius polynomial of L is equal to the coboundary polynomial of L, so $\mu_L(S,U) = (S+U-1)^r$.

Remark 10.11. Let L be a geometric lattice. Then

$$\begin{aligned}\sum_{i=0}^{r(L)} \mu_i(U) &= \mu_L(1,U)\\ &= \sum_{y\in L}\sum_{0\leq x\leq y} \mu(x,y)U^{r(L)-r(y)}\\ &= U^{r(L)}\end{aligned}$$

since $\sum_{0\leq x\leq y}\mu(x,y)=0$ for all $0<y$ in L by Proposition 9.6. Similarly $\sum_{i=0}^{n}\chi_i(U)=\chi_L(1,U)=U^{r(L)}$. Also $\sum_{w=0}^{n}A_w(U)=U^k$ for the extended weights of a code of dimension k by Propositions 2.14 and 2.16 for $t=0$.

Example 10.12. Let L be the uniform lattice $U_{n,k}$. Then $\mu_i(U)$ and $\chi_i(U)$ are both equal to $\binom{n}{i}(U-1)^{n-i}$ for all $i<k$ as in Example 10.3, and $\chi_i(U)=0$ for all $k\leq i<n$, since $a(1_L)=n$, $r(1_L)=k$ and $a(x)=r(x)$ for all x in L_i and $i<k$. Remark 10.11 implies

$$\mu_k(U)=U^k-\sum_{i<k}\binom{n}{i}(U-1)^{n-i} \text{ and } \chi_n(U)=U^k-\sum_{i<k}\binom{n}{i}(U-1)^{n-i}.$$

An important reason to study the Möbius polynomial is because it determines the Whitney numbers. See [44], [27, §6.6.D], [77, Chapter 15], and [87, §3.11].

Definition 10.13. Let L be a finite geometric lattice. The *Whitney numbers* w_i and W_i of the *first and second kind*, respectively, are defined by

$$w_i=\sum_{x\in L_i}\mu(x) \quad \text{and} \quad W_i=|L_i|.$$

The *doubly indexed Whitney numbers* w_{ij} and W_{ij} of the *first and second kind*, respectively, are defined by

$$w_{ij}=\sum_{x\in L_i}\sum_{y\in L_j}\mu(x,y) \quad \text{and} \quad W_{ij}=|\{(x,y):x\in L_i,y\in L_j,x\leq y\}|.$$

In particular, $w_j=w_{0j}$ and $W_j=W_{0j}$.

Remark 10.14. We have that

$$\chi_L(U)=\sum_{i=0}^{r(L)}w_iU^{r(L)-i} \quad \text{and} \quad \mu_L(S,U)=\sum_{i=0}^{r(L)}\sum_{j=0}^{r(L)}w_{ij}S^iU^{r(L)-j}.$$

Hence the (doubly indexed) Whitney numbers of the first kind are determined by $\mu_L(S,U)$. The leading coefficient of

$$\mu_i(U)=\sum_{x\in L_i}\sum_{x\leq y}\mu(x,y)U^{r(L_x)-r_{L_x}(y)}$$

is equal to $\sum_{x\in L_i}\mu(x,x)=|L_i|=W_i$. Hence the Whitney numbers of the second kind W_i are also determined by $\mu_L(S,U)$. We will see in Example 10.35 that the Whitney numbers are not determined by $\chi_L(S,U)$. Finally, let $r=r(L)$. Then

$$\mu_{r-1}(U)=(U-1)\cdot W_{r-1}.$$

There are a lot of open conjectures about the sequences of Whitney numbers. A sequence of real numbers $(v_0,v_,\ldots,v_r)$ is called *unimodal* if

$$v_i\geq\min\{v_{i-1},v_{i+1}\} \text{ for all } 0<i<r.$$

The sequence is called *logarithmically concave* or *log-concave* if

$$v_i^2 \geq v_{i-1}v_{i+1} \text{ for all } 0 < i < r.$$

The Whitney numbers of the first kind are alternating in sign. That is:

$$w_i^+ := (-1)^i w_i > 0 \text{ for all } i.$$

It was conjectured by Rota [82] that the Whitney numbers w_i^+ are unimodal. See [102, Problem 12]. Welsh [103] conjectured that the Whitney numbers w_i^+ are log-concave by generalizing a conjecture of Read [80] on graphs. It was shown that the following weaker version of the unimodal property is true for a matroid M of rank r:

$$w_i^+ < w_j^+ \text{ for all } 0 \leq i \leq r/2 \text{ and } i < j \leq r - i.$$

See [2, Corollary 8.4.2]. For a recent overview of all conjectures, see [77, §15.2].

10.3 Minimal codewords and subcodes

Definition 10.15. A *minimal codeword* of a code C is a codeword whose support does not properly contain the support of another codeword.

The zero word is a minimal codeword. Note that a nonzero scalar multiple of a minimal codeword is again a minimal codeword. Nonzero minimal codewords play a role in minimum distance decoding [4, 9, 10], in secret sharing schemes, and in access structures [72, 89]. We can generalize this notion to subcodes instead of words.

Definition 10.16. A *minimal subcode of dimension* r of a code C is an r-dimensional subcode whose support is not properly contained in the support of another r-dimensional subcode.

A minimal codeword generates a minimal subcode of dimension one, and all the elements of a minimal subcode of dimension one are minimal codewords. A codeword of minimal weight is a nonzero minimal codeword, but the converse is not always the case.

In Example 10.35 we will see two codes that have the same Tutte polynomial, but a different number of minimal codewords. Hence the number of minimal codewords and subcodes is not determined by the Tutte polynomial. However, the number of minimal codewords and the number of minimal subcodes of a given dimension are given by the Möbius polynomial.

Theorem 10.17. *Let C be a code of dimension k and let $0 \leq r \leq k$. Then the number of minimal subcodes of dimension r is equal to W_{k-r}, the $(r-k)$-th Whitney number of the second kind, and it is determined by the Möbius polynomial.*

Proof. Let D be a subcode of C of dimension r and let J be the complement in $[n]$ of the support of D. If $\mathbf{d} \in D$ and $d_j \neq 0$, then $j \in \mathrm{supp}(D)$ and $j \notin J$. Hence $D \subseteq C(J)$. Now suppose moreover that D is a minimal subcode of C. Without loss of generality we may assume that D is systematic at the first r positions, i.e., that D has a generator matrix of the form $(I_r|A)$. Denote the i-th row of this matrix by $\mathbf{d}_i$. Let $\mathbf{c} \in C(J)$. If $\mathbf{c} - \sum_{i=1}^r c_i\mathbf{d}_i$

is not the zero word, then the subcode D' of C generated by $\mathbf{c}, \mathbf{d}_2, \ldots, \mathbf{d}_r$ has dimension r and its support is contained in $\mathrm{supp}(D) \setminus \{1\}$ and $1 \in \mathrm{supp}(D)$. This contradicts the minimality of D. Hence $\mathbf{c} - \sum_{i=1}^{r} c_i \mathbf{d}_i = 0$ and $\mathbf{c} \in D$. Therefore, $D = C(J)$.
To find a minimal subcode of dimension r, we fix $l(J) = r$ and minimize the support of $C(J)$ with respect to inclusion. Because J is contained in the complement in $[n]$ of the support of $C(J)$, this is equivalent to maximizing J with respect to inclusion. In matroid terms this means we are maximizing J for $r(J) = k - l(J) = k - r$. This means $J = \overline{J}$ is a flat of rank $k - r$. The flats of a matroid are the elements in the geometric lattice $L = L(M)$. The number of $(k-r)$-dimensional elements in $L(M)$ is equal to $|L_{k-r}|$, which is equal to the Whitney number of the second kind W_{k-r} and thus equal to the leading coefficient of $\mu_{k-r}(U)$ by Remark 10.14. Hence the Möbius polynomial determines all the numbers of minimal subcodes of dimension r for $0 \leq r \leq k$. □

Note that the flats of dimension $k-r$ in a matroid are exactly the hyperplanes (i.e., flats of rank $r(M) - 1$) in the $(r-1)$-th truncated matroid $\tau^{r-1}(M)$ (see also Chapter 13). This gives another proof of the result of Britz [21, Theorem 3] that the minimal supports of dimension r are the cocircuits of the $(r-1)$-th truncated matroid. For $r = 1$, this gives the well-known equivalence between nonzero minimal codewords and cocircuits. See [77, Proposition 9.2.4] and [96, 1.21].

The number of minimal subcodes of dimension r does not change after extending the code under a finite field extension, since this number is determined by the Möbius polynomial of the lattice of the code, and this lattice does not change under a finite field extension.

10.4 The characteristic polynomial of an arrangement

Let $\mathcal{X}$ be an *affine variety* in $\mathbb{A}^k$ defined over $\mathbb{F}_q$, that is, the zeroset of a collection of polynomials in $\mathbb{F}_q[X_1, \ldots, X_k]$. Then $\mathcal{X}(\mathbb{F}_{q^m})$ is the set of all points $\mathcal{X}$ with coordinates in $\mathbb{F}_{q^m}$, also called the set of $\mathbb{F}_{q^m}$*-rational points* of $\mathcal{X}$. Note the similarity with extension codes.

A central arrangement $\mathcal{A}$ gives rise to a geometric lattice $L(\mathcal{A})$ and characteristic polynomial $\chi_{L(\mathcal{A})}$ that will be denoted by $\chi_{\mathcal{A}}$. Zaslavsky [110] showed that if $\mathcal{A}$ is an arrangement over the real numbers, then $|\chi_{\mathcal{A}}(-1)|$ counts the number of connected components of the complement of the arrangement. Something similar can be said about arrangements over finite fields.

Proposition 10.18. *Let q be a prime power, and let $\mathcal{A} = (H_1, \ldots, H_n)$ be a simple and central arrangement in $\mathbb{F}_q^k$. Then*

$$\chi_{\mathcal{A}}(q^m) = |\mathbb{F}_{q^m}^k \setminus (H_1 \cup \ldots \cup H_n)|.$$

Proof. Let $A = \mathbb{F}_{q^m}^k$ and $A_j = H_j(\mathbb{F}_{q^m})$. Let L be the poset of all intersections of the A_j with the reverse inclusion as partial order. The principle of inclusion/exclusion as formulated in Example 9.16 gives that

$$|\mathbb{F}_{q^m}^k \setminus (H_1 \cup \cdots \cup H_n)| = \sum_{x \in L} \mu(x)|x| = \sum_{x \in L} \mu(x) q^{m \dim(x)}.$$

The expression on the right hand side is equal to $\chi_{\mathcal{A}}(q^m)$, since L is isomorphic with the geometric lattice $L(\mathcal{A})$ of the arrangement $\mathcal{A} = (H_1, \ldots, H_n)$ with rank function $r = r_L$, so $\dim(x) = r(L) - r(x)$. See also [7, Theorem 2.2], [15, Proposition 3.2], [32, Sect. 16] and [76, Theorem 2.69]. □

Definition 10.19. Let $\mathcal{A} = (H_1, \ldots, H_n)$ be a central simple arrangement over the field $\mathbb{F}$ in $\mathbb{F}^k$ and let $J \subseteq [n]$. Define $H_J = \cap_{j \in J} H_j$. Consider the decreasing sequence

$$\mathcal{N}_k \subset \mathcal{N}_{k-1} \subset \cdots \subset \mathcal{N}_1 \subset \mathcal{N}_0$$

of algebraic subsets of the affine space $\mathbb{A}^k$, defined by

$$\mathcal{N}_i = \bigcup_{\substack{J \subseteq [n] \\ r(H_J) = i}} H_J.$$

Define $\mathcal{M}_i = \mathcal{N}_i \setminus \mathcal{N}_{i+1}$.

Note that $\mathcal{N}_0 = \mathbb{A}^k$, $\mathcal{N}_1 = \cup_{j=1}^n H_j$, $\mathcal{N}_k = \{0\}$ and $\mathcal{N}_{k+1} = \emptyset$. Furthermore, $\mathcal{N}_i$ is a union of linear subspaces of $\mathbb{A}^k$ all of dimension $k - i$. Remember from Remark 4.3 that H_J is isomorphic with $C(J)$ in case $\mathcal{A}$ is the arrangement of the generator matrix G of the code C.

Proposition 10.20. *Let $\mathcal{A} = (H_1, \ldots, H_n)$ be a central simple arrangement over the field $\mathbb{F}$ in $\mathbb{F}^k$. Let $z(\mathbf{x}) = \{j \in [n] : \mathbf{x} \in H_j\}$ and $r(\mathbf{x}) = r(H_{z(\mathbf{x})})$ the* rank *of $\mathbf{x}$ for $\mathbf{x} \in \mathbb{A}^k$. Then*

$$\mathcal{N}_i = \{\mathbf{x} \in \mathbb{A}^k : r(\mathbf{x}) \geq i\} \quad \textit{and} \quad \mathcal{M}_i = \{\mathbf{x} \in \mathbb{A}^k : r(\mathbf{x}) = i\}.$$

Proof. Let $\mathbf{x} \in \mathbb{A}^k$ and $\mathbf{c} = \mathbf{x}G$. Let $\mathbf{x} \in \mathcal{N}_i$. Then there exists a $J \subseteq [n]$ such that $r(H_J) = i$ and $\mathbf{x} \in H_J$. So, $c_j = 0$ for all $j \in J$ and $J \subseteq z(\mathbf{x})$. Hence $H_{z(\mathbf{x})} \subseteq H_J$ and therefore $r(\mathbf{x}) = r(H_{z(\mathbf{x})}) \geq r(H_J) = i$. The converse implication is proved similarly. The statement about $\mathcal{M}_i$ is a direct consequence of the one about $\mathcal{N}_i$. □

Proposition 10.21. *Let $\mathcal{A}$ be a central simple arrangement over $\mathbb{F}_q$ and let $L = L(\mathcal{A})$ be the geometric lattice of $\mathcal{A}$. Then*

$$\mu_i(q^m) = |\mathcal{M}_i(\mathbb{F}_{q^m})|.$$

Proof. Remember from Remark 10.9 that $\mu_i(U) = \sum_{r(x)=i} \chi_{L_x}(U)$. Let $L = L(\mathcal{A})$ and $x \in L$. Then x is an intersection of hyperplanes of $\mathcal{A}$, i.e., $x = \cup_{i \in I} H_i$. Let l be the dimension of x. We define the arrangement $\mathcal{A}_x$ to be the arrangement in $\mathbb{F}_q^l$ of all hyperplanes $x \cup H_j$ in x such that $x \cup H_j \neq \emptyset$ and $x \cup H_J \neq x$, for a chosen isomorphism of x with $\mathbb{F}_q^l$. Then $L(\mathcal{A}_x) = L_x$.
Let $\cup\mathcal{A}_x$ be the union of the hyperplanes of $\mathcal{A}_x$. Then $|(x \setminus (\cup\mathcal{A}_x))(\mathbb{F}_{q^m})| = \chi_{L_x}(q^m)$ by Proposition 10.18. Now $\mathcal{M}_i$ is the disjoint union of complements of the arrangements of $\mathcal{A}_x$ for all $x \in L$ such that $r(x) = i$ by Proposition 10.20. Hence

$$\begin{aligned} |\mathcal{M}_i(\mathbb{F}_{q^m})| &= \sum_{\substack{x \in L \\ r(x)=i}} |(x \setminus (\cup\mathcal{A}_x))(\mathbb{F}_{q^m})| \\ &= \sum_{\substack{x \in L \\ r(x)=i}} \chi_{L_x}(q^m). \end{aligned}$$

See also [7, Theorem 6.3]. □

10.5 The characteristic polynomial of a code

PROPOSITION 10.22. *Let C be a nondegenerate linear code over $\mathbb{F}_q$. Then*

$$A_n(U) = \chi_C(U).$$

PROOF. The short proof is given by $\chi_C(U) = \chi_C(0, U) = \chi_0(U) = A_n(U)$. The geometric interpretation is as follows.
The elements in $\mathbb{F}_{q^m}^k \setminus (H_1 \cup \cdots \cup H_n)$ correspond one-to-one to codewords of weight n in $C \otimes \mathbb{F}_{q^m}$ by Proposition 4.2 and because the arrangements corresponding to C and to $C \otimes \mathbb{F}_{q^m}$ are the same. Therefore, $A_n(q^m) = \chi_C(q^m)$ for all positive integers m by Proposition 10.18. Hence $A_n(U) = \chi_C(U)$. □

DEFINITION 10.23. Let G be a generator matrix of an $[n, k]$ code C over $\mathbb{F}_q$. Define

$$\mathcal{Y}_i = \{\mathbf{x} \in \mathbb{A}^k : \mathrm{wt}(\mathbf{x}G) \leq n - i\} \quad \text{and} \quad \mathcal{X}_i = \{\mathbf{x} \in \mathbb{A}^k : \mathrm{wt}(\mathbf{x}G) = n - i\}.$$

The $\mathcal{Y}_i$ form a decreasing sequence

$$\mathcal{Y}_n \subseteq \mathcal{Y}_{n-1} \subseteq \ldots \subseteq \mathcal{Y}_1 \subseteq \mathcal{Y}_0$$

of algebraic subsets of $\mathbb{A}^k$, and $\mathcal{X}_i = \mathcal{Y}_i \setminus \mathcal{Y}_{i+1}$. Suppose that G has no zero column and let $\mathcal{A}_G$ be the arrangement of G. Then

$$\mathcal{X}_i = \{\mathbf{x} \in \mathbb{A}^k : \mathbf{x} \text{ is in exactly } i \text{ hyperplanes of } \mathcal{A}_G\}.$$

PROPOSITION 10.24. *Let C be a projective code of length n. Then*

$$\chi_i(q^m) = |\mathcal{X}_i(\mathbb{F}_{q^m})| = A_{n-i}(q^m).$$

PROOF. Every $\mathbf{x} \in \mathbb{F}_{q^m}^k$ corresponds one-to-one to a codeword in $C \otimes \mathbb{F}_{q^m}$ via the map $\mathbf{x} \mapsto \mathbf{x}G$. Therefore, $|\mathcal{X}_i(\mathbb{F}_{q^m})| = A_{n-i}(q^m)$. Also, $A_{n-i}(q^m) = \chi_i(q^m)$ for all i, by Theorem 10.6. See also [3, Theorem 3.3]. □

Note that the statement $|\mathcal{X}_i(\mathbb{F}_{q^m})| = A_{n-i}(q^m)$ and its proof are the the affine versions of Proposition 4.2 and its proof.

REMARK 10.25. Another way to define $\mathcal{X}_i$ is the collection of all points $P \in \mathbb{A}^k$ such that P is on exactly i distinct hyperplanes of the arrangement $\mathcal{A}_G$. Denote the arrangement of hyperplanes in $\mathbb{P}^{k-1}$ also by $\mathcal{A}_G$ and let $\overline{P}$ be the point in $\mathbb{P}^{k-1}$ corresponding to $P \in \mathbb{A}^k$. Define

$$\overline{\mathcal{X}}_i = \{\overline{P} \in \mathbb{P}^{k-1} : \overline{P} \text{ is on exactly } i \text{ hyperplanes of } \mathcal{A}_G\}.$$

For all $i < n$ the polynomial $\chi_i(U)$ is divisible by $U - 1$. Define $\overline{\chi}_i(U) = \chi_i(U)/(U - 1)$. Then $\overline{\chi}_i(q^m) = |\overline{\mathcal{X}}_i(\mathbb{F}_{q^m})|$ for all $i < n$ by Proposition 10.24.

Theorem 10.26. *Let G be a generator matrix of a nondegenerate code C. Let $\mathcal{A}_G$ be the associated central arrangement. Let $d^\perp = d(C^\perp)$. Then $\mathcal{N}_i \subseteq \mathcal{Y}_i$ for all i and equality holds for all $i < d^\perp$. Also, $\mathcal{M}_i = \mathcal{X}_i$ for all $i < d^\perp - 1$. If furthermore C is projective, then*

$$\mu_i(U) = \chi_i(U) = A_{n-i}(U) \text{ for all } i < d^\perp - 1.$$

Proof. A more general version of this statement will be proven in Theorem 11.4, using matroids. Here we give the proof for codes and arrangements.
Let $\mathbf{x} \in \mathcal{N}_i$. Then $\mathbf{x} \in H_J$ for some $J \subseteq [n]$ such that $r(H_J) = i$. This means $|J| \geq i$ and $\mathrm{wt}(\mathbf{x}G) \leq n - i$ by Proposition 4.2. Hence $\mathbf{x} \in \mathcal{Y}_i$ and therefore $\mathcal{N}_i \subseteq \mathcal{Y}_i$.
Let $i < d^\perp$ and $\mathbf{x} \in \mathcal{Y}_i$. Then $\mathrm{wt}(\mathbf{x}G) \leq n - i$. Let $J = \mathrm{supp}(\mathbf{x}G)$. Then $|J| \geq i$. Take a subset I of J such that $|I| = i$. Then $\mathbf{x} \in H_I$ and $r(I) = |I| = i$ by Lemma 2.7, since $i < d^\perp$. Hence $\mathbf{x} \in \mathcal{N}_i$ and therefore $\mathcal{Y}_i \subseteq \mathcal{N}_i$, $\mathcal{Y}_i = \mathcal{N}_i$ for all $i < d^\perp$, and $\mathcal{M}_i = \mathcal{X}_i$ for all $i < d^\perp - 1$.
The code is nondegenerate, so $d^\perp \geq 2$. Suppose furthermore that C is projective. Then $\mu_i(U) = \chi_i(U) = A_{n-i}(U)$ for all $i < d^\perp - 1$, by Theorem 10.6 and Propositions 10.24 and 10.21. □

Remember that the extended and generalized weight enumerators are determined by the pair (n, k) for an $[n, k]$ MDS code by Theorem 2.27. If C is an $[n, k]$ code, then $d^\perp$ is at most $k + 1$ by the Singleton bound. Furthermore $d^\perp = k + 1$ if and only if C is MDS if and only if $C^\perp$ is MDS.

Definition 10.27. An $[n, k, d]$ code is called *almost MDS* if $d = n - k$. The code C is called *near MDS* if both C and $C^\perp$ are almost MDS.

So $d^\perp = k$ if and only if $C^\perp$ is almost MDS. If C is almost MDS, then $C^\perp$ is not necessarily almost MDS. See [33] for more on near-MDS codes.

Proposition 10.28. *Let C be an $[n, k, d]$ code such that $C^\perp$ is MDS or almost MDS and $k \geq 3$. Then both $\chi_C(S, U)$ and $W_C(X, Y, U)$ determine $\mu_C(S, U)$. In particular:*

$$\mu_i(U) = \chi_i(U) = A_{n-i}(U) \text{ for all } i < k - 1,$$

$$\mu_{k-1}(U) = \sum_{i=k-1}^{n-1} \chi_i(U) = \sum_{i=k-1}^{n-1} A_{n-i}(U),$$

and $\mu_k(U) = 1$.

Proof. Let C be a code such that $d(C^\perp) \geq k \geq 3$. Then C is projective and $\mu_i(U) = \chi_i(U) = A_{n-i}(U)$ for all $i < k - 1$ by Theorem 10.26. Furthermore, $\mu_k(U) = \chi_n(U) = A_0(U) = 1$.
Finally let $L = L(C)$. Then $\sum_{i=0}^{k} \mu_i(U) = U^k$, $\sum_{i=0}^{n} \chi_i(U) = U^k$ and $\sum_{i=0}^{n} A_i(U) = U^k$ by Remark 10.11. Hence the formula for $\mu_{k-1}(U)$ holds. Therefore, $\mu_C(S, U)$ is determined both by $W_C(X, Y, U)$ and $\chi_C(S, U)$. □

Projective codes of dimension 3 are examples of codes C such that $C^\perp$ is almost MDS. In the following we will give explicit formulas for $\mu_C(S, U)$ for such codes.

Let C be a projective code of length n and dimension 3 over $\mathbb{F}_q$ with generator matrix G. The arrangement $\mathcal{A}_G = (H_1, \dots, H_n)$ of planes in $\mathbb{F}_q^3$ is simple and essential, and the corresponding arrangement of lines in $\mathbb{P}^2(\mathbb{F}_q)$ is also denoted by $\mathcal{A}_G$. We defined in Remark 10.25 that

$$\overline{\mathcal{X}}_i(\mathbb{F}_{q^m}) = \{\overline{P} \in \mathbb{P}^2(\mathbb{F}_{q^m}) : \overline{P} \text{ is on exactly } i \text{ lines of } \mathcal{A}_G\}$$

and $\overline{\chi}_i(q^m) = |\overline{\mathcal{X}}_i(\mathbb{F}_{q^m})|$ for all $i < n$.
Note that for projective codes of dimension 3 we have $\overline{\mathcal{X}}_i(\mathbb{F}_{q^m}) = \overline{\mathcal{X}}_i(\mathbb{F}_q)$ for all positive integers m and $2 \leq i < n$. Abbreviate in this case $\overline{\chi}_i(q^m) = \overline{\chi}_i$ for $2 \leq i < n$.

PROPOSITION 10.29. *Let C be a projective code of length n and dimension 3 over $\mathbb{F}_q$. Then*

$$\begin{cases} \mu_0(U) &= (U-1)\left(U^2 - (n-1)U + \sum_{i=2}^{n-1}(i-1)\overline{\chi}_i - n + 1\right), \\ \mu_1(U) &= (U-1)\left(nU + n - \sum_{i=2}^{n-1} i\overline{\chi}_i\right), \\ \mu_2(U) &= (U-1)\left(\sum_{i=2}^{n-1} \overline{\chi}_i\right), \\ \mu_3(U) &= 0. \end{cases}$$

PROOF. A more general statement and proof is possible for $[n,k]$ codes C such that $d^\perp \geq k$, using Proposition 10.28, the fact that $B_t(U) = U^{k-t} - 1$ for all $t < d^\perp$ by Lemma 2.7, and the expression of $B_t(U)$ in terms of $A_w(U)$ by Proposition 2.16. We will give a second geometric proof for the special case of projective codes of dimension 3.
By Lagrange interpolation it is enough to show this proposition with $U = q^m$ for all m. Note that $\mu_i(q^m)$ is the number of elements of $\mathcal{M}_i(\mathbb{F}_{q^m})$ by Proposition 10.21. Let $\overline{P}$ be the corresponding point in $\mathbb{P}^2(\mathbb{F}_{q^m})$ for $P \in \mathbb{F}_{q^m}^3$ and $P \neq 0$. Abbreviate $\mathcal{M}_i(\mathbb{F}_{q^m})$ by $\mathcal{M}_i$ and define $\overline{\mathcal{M}}_i = \{\overline{P} : P \in \mathcal{M}_i\}$. So, $|\mathcal{M}_i| = (q^m - 1)|\overline{\mathcal{M}}_i|$ for all $i < 3$.
When $\overline{P} \in \overline{\mathcal{M}}_2$, we have $\overline{P} \in H_j \cap H_k$ for some $j \neq k$. Hence $\overline{P} \in \overline{\mathcal{X}}_i(\mathbb{F}_q)$ for some $i \geq 2$, since the code is projective. This means $\overline{\mathcal{M}}_2$ is the disjoint union of the $\overline{\mathcal{X}}_i(\mathbb{F}_q)$ for $2 \leq i < n$. Therefore, $|\overline{\mathcal{M}}_2| = \sum_{i=2}^{n-1} \overline{\chi}_i$.
We have $\overline{P} \in \overline{\mathcal{M}}_1$ if and only if $\overline{P}$ is on exactly one line H_j. There are n lines, and every line has $q^m + 1$ points that are defined over $\mathbb{F}_{q^m}$. If $i \geq 2$, then every $\overline{P} \in \overline{\mathcal{X}}_i(\mathbb{F}_q)$ is on i lines H_j. Hence $|\overline{\mathcal{M}}_1| = n(q^m + 1) - \sum_{i=2}^{n-1} i\overline{\chi}_i$.
Finally, $\mathbb{P}^2(\mathbb{F}_{q^m})$ is the disjoint union of $\overline{\mathcal{M}}_0$, $\overline{\mathcal{M}}_1$ and $\overline{\mathcal{M}}_2$. The numbers $|\overline{\mathcal{M}}_2|$ and $|\overline{\mathcal{M}}_1|$ are already computed, and $|\mathbb{P}^2(\mathbb{F}_{q^m})| = q^{2m} + q^m + 1$. From this we derive the number of elements of $\overline{\mathcal{M}}_0$. □

Note that $\mu_i(U)$ is divisible by $U - 1$ for all $0 \leq i < k$. Define $\overline{\mu}_i = \mu_i(U)/(U-1)$. Define similarly $\overline{A}_w = A_w(U)/(U-1)$ for all $0 < w \leq n$.

10.6 Examples and counterexamples

EXAMPLE 10.30. Consider the matrix G given by

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

Let C be the code over $\mathbb{F}_q$ with generator matrix G. For $q = 2$, this is the simplex code $\mathcal{S}_2(2)$. The columns of G represent also the coefficients of the lines of $\mathcal{A}_G$. The projective picture of $\mathcal{A}_G$ is given in Figure 10.1.

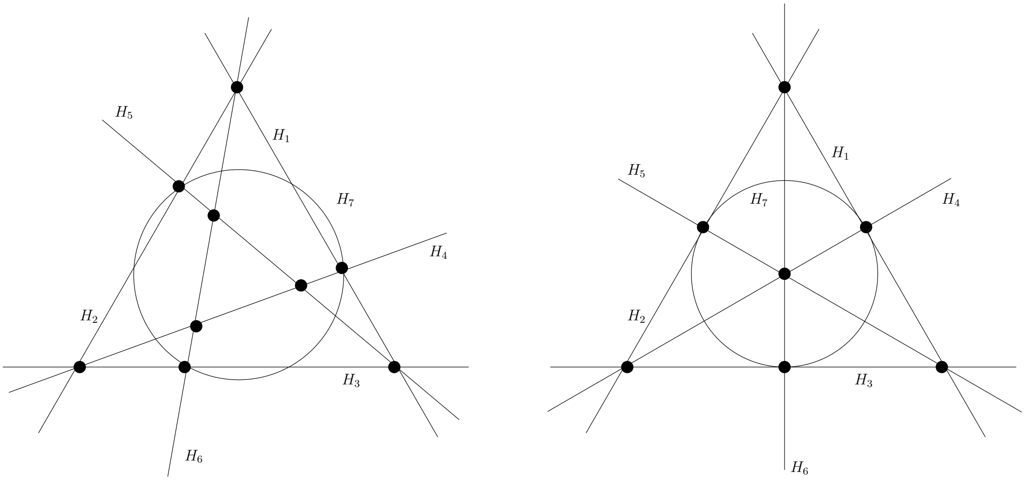


Figure 10.1: The arrangement of G for q odd and q even

If q is odd, then there are 3 points on two lines and 6 points on three lines, so $\overline{\chi}_2 = 3$ and $\overline{\chi}_3 = 6$. The number of points that are on one line is equal to the number of points on each of the seven lines, minus the points we already counted, with multiplicity: $7(U+1) - 3 \cdot 2 - 6 \cdot 3 = 7U - 17$. There are no points on more than three lines, so $\overline{\chi}_i = 0$ for $i > 3$. We calculate $\overline{\chi}_0$ via $\overline{\chi}_0 + \overline{\chi}_1 + \overline{\chi}_2 + \overline{\chi}_3 = U^2 + U + 1$.
If q is even, we can do the same kind of calculation. The values of $\overline{\mu}_i$ can be calculated using Proposition 10.29, but they follow more directly from Proposition 10.28. The results are in the next table:

	i	0	1	2	3	4	5	6	7
q odd	$\overline{\chi}_i$	$U^2 - 6U + 9$	$7U - 17$	3	6	0	0	0	
	$\overline{A}_i$		0	0	0	6	3	$7U - 17$	$U^2 - 6U + 9$
	$\overline{\mu}_i$	$U^2 - 6U + 9$	$7U - 17$	9	1				
q even	$\overline{\chi}_i$	$U^2 - 6U + 8$	$7U - 14$	0	7	0	0	0	
	$\overline{A}_i$		0	0	0	7	0	$7U - 14$	$U^2 - 6U + 8$
	$\overline{\mu}_i$	$U^2 - 6U + 8$	$7U - 14$	7	1				

Note that there is a codeword of weight 7 in case q is even and $q > 4$ or q is odd and $q > 3$, since $\overline{A}_7 = (U-2)(U-4)$ or $\overline{A}_7 = (U-3)^2$, respectively.

Example 10.31. Let G be a $3 \times n$ generator matrix of an MDS code. As mentioned in Example 2.28, the lines of the arrangement $\mathcal{A}_G$ are in general position. That means that every two distinct lines meet in one point and every three mutually distinct lines have an empty intersection, so $\overline{\chi}_2 = \binom{n}{2}$ and $\overline{\chi}_i = 0$ for all $i > 2$. By Proposition 10.29 we have $\overline{\mu}_2 = \binom{n}{2}$ and $\overline{\mu}_1 = nU + 2n - n^2$ and $\overline{\mu}_0 = U^2 - (n-1)U + \binom{n-1}{2}$. By Proposition 10.21

we find $A_i = 0$ for $0 < i < n-2$, $\overline{A}_{n-2} = \overline{\chi}_2$ and $\overline{A}_{n-1} = \overline{\chi}_1 = \overline{\mu}_1$ and $\overline{A}_n = \overline{\chi}_0 = \overline{\mu}_0$. The values found for the extended weight enumerator are in agreement with Theorem 2.27.

Example 10.32. Let a and b be positive integers such that $2 < a < b$ and let $n = a + b$. Let G be a $3 \times n$ generator matrix of a nondegenerate code. Suppose that there are two points P and Q in the projective plane over $\mathbb{F}_q$ such that the $a + b$ lines of the projective arrangement of $\mathcal{A}_G$ consists of a distinct lines incident with P, and b distinct lines incident with Q and there is no line incident with P and Q. Then $\overline{\chi}_2 = \overline{A}_{n-2} = ab$, $\overline{\chi}_a = \overline{A}_b = 1$ and $\overline{\chi}_b = \overline{A}_a = 1$. Hence $\overline{\mu}_2(U) = ab + 2$. Furthermore

$$\overline{\mu}_1 = \overline{A}_{n-1} = (a+b)U - 2ab,$$

$$\overline{\mu}_0 = \overline{A}_n = U^2 - (a+b-1)U + ab - 1$$

and $\overline{A}_i = 0$ for all $i \notin \{a, b, n-2, n-1, n\}$.

Example 10.33. Let a, b and c be positive integers such that $2 < a < b < c$. Let $n = a + b + c$. Let G be a $3 \times n$ generator matrix of a nondegenerate code $C(a, b, c)$. Suppose that there are three points P, Q and R in the projective plane over $\mathbb{F}_q$ such that the lines of the projective arrangement of $\mathcal{A}_G$ consist of a distinct lines incident with P and not with Q and R, b distinct lines incident with Q and not with P and R, and c distinct lines incident with R and not with P and Q. The a lines through P intersect the b lines through Q in ab points. Similar statements hold for the lines through P and R intersecting in ac points, and the lines through Q and R intersecting in bc points. Suppose that all these $ab + bc + ac$ intersection points are mutually distinct, so every intersection point lies on exactly two lines of the arrangement. If q is large enough, then such a configuration exists.

The number of points on two lines of the arrangement is $\overline{\chi}_2 = ab + bc + ca$. Since P is the unique point on exactly a lines of the arrangement, we have $\overline{\chi}_a = 1$. Similarly $\overline{\chi}_b = \overline{\chi}_c = 1$. Finally, $\overline{\chi}_i = 0$ for all $2 \leq i < n$ and $i \notin \{2, a, b, c\}$. Propositions 10.28 and 10.29 imply that $\overline{A}_{n-a} = \overline{A}_{n-b} = \overline{A}_{n-c} = 1$ and $\overline{A}_{n-2} = ab+bc+ca$ and $\overline{\mu}_2 = ab+bc+ca+3$. Furthermore

$$\overline{\mu}_1 = \overline{\chi}_1 = \overline{A}_{n-1} = nU - 2(ab + bc + ca),$$

$$\overline{\mu}_0 = \overline{\chi}_0 = \overline{A}_n = U^2 - (n-1)U + ab + bc + ca - 2$$

and $\overline{A}_i(U) = 0$ for all $i \notin \{0, n-c, n-b, n-a, n-2, n-1, n\}$.

Therefore, $W_{C(a,b,c)}(X, Y, U) = W_{C(a',b',c')}(X, Y, U)$ if and only if $(a, b, c) = (a', b', c')$, and $\mu_{C(a,b,c)}(S, U) = \mu_{C(a',b',c')}(S, U)$ if and only if $a + b + c = a' + b' + c'$ and $ab + bc + ca = a'b' + b'c' + c'a'$. In particular, let $C_1 = C(3, 9, 14)$ and $C_2 = C(5, 6, 15)$. Then C_1 and C_2 are two projective codes with the same Möbius polynomial $\mu_C(S, U)$ but distinct extended weight enumerators and coboundary polynomial $\chi_C(S, U)$.

Now $d(C(a, b, c)) = n - c$. Hence $d(C_1) = 12$ and $d(C_2) = 11$. Therefore, $\mu_C(S, U)$ does not determine the minimum distance, although it gives the number of minimal codewords.

Example 10.34. Consider the codes C_3 and C_4 over $\mathbb{F}_q$ with $q > 2$ and generator matrices G_3 and G_4 given by

$$G_3 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad G_4 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & a & 0 & 0 & 1 \end{pmatrix},$$

where $a \in \mathbb{F}_q \setminus \{0,1\}$. It was shown by Brylawsky [27, Exercise 6.96] that the duals of these codes have the same Tutte polynomial. Therefore, the codes C_3 and C_4 have the same Tutte polynomial

$$t_C(X,Y) = 2X + 2Y + 3X^2 + 5XY + 4Y^2 + X^3 + X^2Y + 2XY^2 + 3Y^3 + Y^4.$$

Hence C_3 and C_4 have the extended weight enumerator given by

$$X^7 + (2U-2)X^4Y^3 + (3U-3)X^3Y^4 + (U^2-U)X^2Y^5 + \\ + (5U^2 - 15U + 10)XY^6 + (U^3 - 6U^2 + 11U - 6)Y^7.$$

The codes C_3 and C_4 are not projective and their simplifications $\overline{C}_3$ and $\overline{C}_4$, respectively, have generator matrices given by

$$\overline{G}_3 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \overline{G}_4 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & a & 0 & 1 \end{pmatrix},$$

where $a \in \mathbb{F}_q \setminus \{0,1\}$. From the arrangements $\mathcal{A}(\overline{C}_3)$ and $\mathcal{A}(\overline{C}_4)$ in Figure 10.2 we deduce the $\overline{\chi}_i$ that are given in the following table.

code \ i	0	1	2	3	4	5
C_3	$U^2 - 5U + 6$	$6U - 12$	3	4	0	0
C_4	$U^2 - 5U + 6$	$6U - 13$	6	1	1	0

Therefore, $t_{C_3}(X,Y) = t_{C_4}(X,Y)$, but $\chi_{C_3}(S,U) \neq \chi_{C_4}(S,U)$ and $t_{\overline{C}_3}(X,Y) \neq t_{\overline{C}_4}(X,Y)$.

Example 10.35. Let $C_5 = C_3^\perp$ and $C_6 = C_4^\perp$. Their generator matrices are

$$G_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad G_6 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & a \end{pmatrix},$$

where $a \in \mathbb{F}_q \setminus \{0,1\}$. Then C_5 and C_6 have the same Tutte polynomial $t_{C^\perp}(X,Y) = t_C(Y,X)$ as given by Example 10.34:

$$2X + 2Y + 4X^2 + 5XY + 3Y^2 + 3X^3 + 2X^2Y + XY^2 + Y^3 + 3X^4.$$

Hence C_5 and C_6 have the same extended weight enumerator given by

$$X^7 + (U-1)X^5Y^2 \\ + (6U-6)X^4Y^3 + (2U^2 - U - 1)X^3Y^4 + (15U^2 - 43U + 28)X^2Y^5 \\ + (7U^3 - 36U^2 + 60U - 31)XY^6 + (U^4 - 7U^3 + 19U^2 - 23U + 10)Y^7.$$

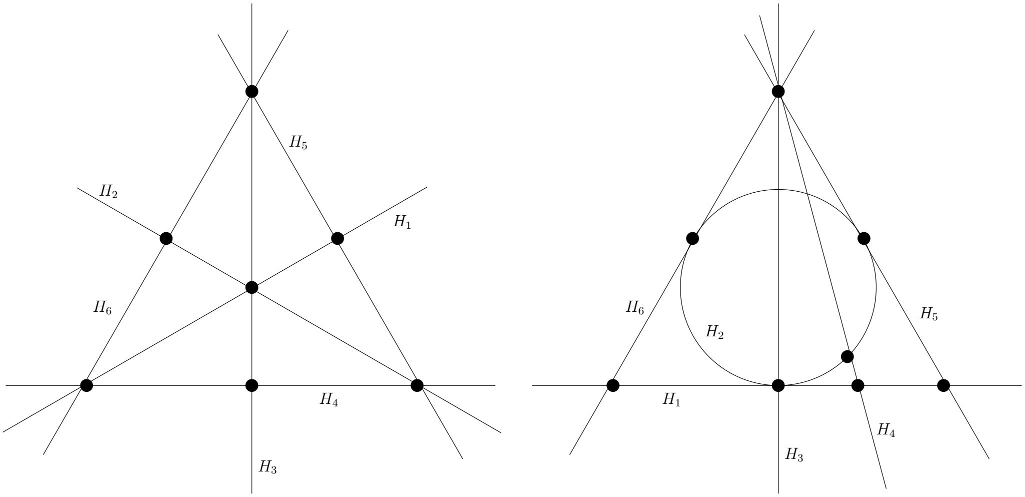


Figure 10.2: The arrangements of $\overline{G}_3$ and $\overline{G}_4$

The geometric lattice $L(C_5)$ has atoms a, b, c, d, e, f, g corresponding to the first, second, etc. column of G_5. The second level of $L(C_5)$ consists of the following 17 elements:

$$abe,\ ac,\ ad,\ af,\ ag,\ bc,\ bd,\ bf,\ bg,\ cd,\ ce,\ cf,\ cg,\ de,\ df,\ dg,\ efg.$$

The third level consists of the following 12 elements:

$$abce,\ abde,\ abefg,\ acdg,\ acf,\ adf,\ bcdf,\ bcg,\ bdg,\ cde,\ cefg,\ defg.$$

Similarly, the geometric lattice $L(C_6)$ has atoms a, b, c, d, e, f, g corresponding to the first, second, etc. column of G_6. The second level of $L(C_6)$ consists of the following 17 elements:

$$abe,\ ac,\ ad,\ af,\ ag,\ bc,\ bd,\ bf,\ bg,\ cd,\ ce,\ cf,\ cg,\ de,\ dfg,\ ef,\ eg.$$

The third level consists of the following 13 elements:

$$abce,\ abde,\ abef,\ abeg,\ acd,\ acf,\ acg,\ adfg,\ bcdfg,\ cde,\ cef,\ ceg,\ defg.$$

Theorem 10.26 implies that $\mu_0(U)$ and $\mu_1(U)$ are the same for both codes and equal to

$$\mu_0(U) = \chi_0(U) = A_7(U) = (U-1)(U-2)(U^2-4U+5)$$

$$\mu_1(U) = \chi_1(U) = A_6(U) = (U-1)(7U^2-29U+31).$$

The polynomials $\mu_3(U)$ and $\mu_2(U)$ are given in the following table using Remarks 10.14 and 10.11.

	C_5	C_6
$\mu_2(U)$	$17U^2-49U+32$	$17U^2-50U+33$
$\mu_3(U)$	$12U-12$	$13U-13$

This example shows that for projective codes the Möbius polynomial $\mu_C(S,U)$ is not determined by the coboundary polynomial $\chi_C(S,U)$.

11

Relations between the Möbius and coboundary polynomials

When studying polynomial invariants of matroids, much attention is given to the Tutte polynomial, see Chapter 8. Many other polynomials associated to graphs, arrangements, linear codes and matroids turn out to be an evaluation of the Tutte polynomial, or define the Tutte polynomial. Sometimes the polynomials and the Tutte polynomial determine each other.

In Chapter 10 we discussed two other polynomial invariants of matroids: the coboundary polynomial and the Möbius polynomial. The former is, for simple matroids, equivalent to the Tutte polynomial, see Corollary 10.5. The latter, however, is not, as we showed by the examples in Section 10.6.

It follows that, in general, the coboundary polynomial and the Möbius polynomial do not determine each other. Less is known about more specific cases. In this chapter we will investigate if it is possible that the Möbius polynomial of a matroid, together with the Möbius polynomial of the dual matroid, define the coboundary polynomial of the matroid. In some cases, the answer is affirmative, and we will give two constructions to determine the coboundary polynomial in these cases.

This chapter is a copy of [54].

11.1 Connections

For a matroid M with rank function r and dual matroid M^*, we will study the following parameters:

- n, the number of elements of M and M^*;
- k, the rank of M;
- d, the size of the smallest cocircuit in M (i.e., circuit in M^*);
- d^*, the size of the smallest circuit in M (i.e., cocircuit in M^*).

Note that if a matroid is representable over a finite field, then there is a linear code associated to it with length n, dimension k, minimum distance d and dual minimum distance d^*.

Throughout this chapter, we will restrict ourselves to simple matroids. Also the dual of a matroid is assumed to be simple. This implies $d > 2$ and $d^* > 2$. In this case, there is a two-way equivalence between matroids and geometric lattices: we will freely change between these objects when necessary.

Some natural questions arise about the dependencies between the coboundary polynomial and Möbius polynomial of a matroid and its dual. First of all, do the coboundary and Möbius polynomial determine each other? The answer is "no", even if both the matroid and its dual are simple. We have seen counterexamples in Examples 10.33 and 10.35.

In Corollary 10.5 we saw that the coboundary polynomial is equivalent to the Tutte polynomial. The Tutte polynomial of a matroid is determined by the Tutte polynomial of the dual matroid, as we saw in Theorem 8.7. Therefore, the same holds for the coboundary polynomials of a matroid and its dual.

THEOREM 11.1. *Let $\chi_M(S,U)$ be the coboundary polynomial of a simple matroid M with simple dual M^*. Let $\chi_{M^*}(S,U)$ be the coboundary polynomial of M^*. Then*

$$\chi_{M^*}(S,U) = (S-1)^n U^{-k} \chi_M \left(\frac{S+U-1}{S-1}, U \right).$$

PROOF. The rewriting is analogous to the proof of Theorem 2.19 in Section 8.2. We use Corollary 10.5 and Theorem 8.7.

$$\begin{aligned} & (S-1)^n U^{-k} \chi_M \left(\frac{S+U-1}{S-1}, U \right) \\ = \quad & (S-1)^n U^{-k} \left(\frac{U}{S-1} \right)^k t_M \left(S, \frac{S+U-1}{S-1} \right) \\ = \quad & (S-1)^{n-k} t_{M^*} \left(\frac{S+U-1}{S-1}, S \right) \\ = \quad & \chi_{M^*}(S,U). \end{aligned}$$

Note that in the last step we use that the rank of M^* is equal to $n-k$. □

One might notice the resemblance between this theorem and the MacWilliams relations for the extended weight enumerator in 2.19. This is because of the relation in Theorem 10.6.

The question comes up if such a duality relation also exists for the Möbius polynomial. To answer this, we need some more theory.

LEMMA 11.2. *Let M be a matroid. Then for all elements $x \in M$ with $r(x) < d^* - 1$, we have $|x| = r(x)$. Furthermore, if M is simple, we have $a(x) = r(x)$ in the corresponding geometric lattice.*

PROOF. By definition, d^* is the size of the smallest circuit in M and thus the size of the smallest dependent set in M. It has rank $d^* - 1$. This means all elements $x \in M$ of rank $r(x) < d^* - 1$ are independent and have $|x| = r(x)$. For simple matroids, $|x| = a(x)$ in the corresponding geometric lattice. □

PROPOSITION 11.3. *Given the Möbius polynomial $\mu_M(S, U)$ of a matroid. Then we can determine the parameter d^* of the matroid M.*

PROOF. The coefficient of the term $S^i U^{k-j}$ in the Möbius polynomial is given by

$$\sum_{\substack{x \in L \\ r(x)=i}} \sum_{\substack{y \in L \\ r(y)=j}} \mu(x, y).$$

These numbers are the doubly-indexed Whitney numbers of the first kind, see Section 10.2. In the case $j = i$, we just count the number of elements in L of rank i, i.e., the number of flats of rank i in M. These are the Whitney numbers of the second kind. From Lemma 11.2 it now follows that for $i < d^* - 1$ all elements of rank i are flats, so there are $\binom{n}{i}$ of them. For $i \geq d^* - 1$, the number of flats is strictly smaller then $\binom{n}{i}$. Therefore we can determine d^* from the Möbius polynomial of M. □

In the previously mentioned Example 10.33, we have two matroids with the same Möbius polynomial but with different d. By Proposition 11.3, this means that their duals cannot have the same Möbius polynomial. This gives a negative answer to the question in [58, §10.5] if the Möbius polynomial of a matroid and its dual are determined by each other.

To summarize, together with Theorem 11.1 we know the following about the coboundary and Möbius polynomials of a matroid and its dual:

- The coboundary polynomial $\chi_M(S, U)$ of a matroid and the coboundary polynomial $\chi_{M^*}(S, U)$ of the dual matroid completely determine each other.
- The Möbius polynomial $\mu_M(S, U)$ of a matroid does not determine the Möbius polynomial $\mu_{M^*}(S, U)$ of the dual matroid.
- The coboundary polynomial $\chi_M(S, U)$ does not determine the Möbius polynomial $\mu_M(S, U)$. The same holds in the dual case.
- The Möbius polynomial $\mu_M(S, U)$ does not determine the coboundary polynomial $\chi_M(S, U)$.

The last three statements also hold in case M and/or M^* are not simple. In this chapter, we will address another question between dependencies:

> Given the Möbius polynomials $\mu_M(S, U)$ and $\mu_{M^*}(S, U)$ of a matroid and its dual. Do they determine $\chi_M(S, U)$?

We will see that, in some cases, the answer is "yes". Proposition 11.3 tells us that the Möbius polynomial gives us information about the dual of the matroid. This is the reason to ask if the Möbius polynomial of the matroid, together with the Möbius polynomial of its dual, determine the coboundary polynomial.

For completeness, note that $\mu_M(S, U)$ and $\mu_{M^*}(S, U)$ define not only d^* and d, respectively, but also n and k: the degree of $\mu_M(S, U)$ in S is $r(M) = k$, and the degree of $\mu_{M^*}(S, U)$ in S is $r^*(M^*) = n - k$.

Theorem 11.4. *Let M be a matroid, and let the Möbius polynomial $\mu_M(S,U)$ be given. Then part of the coboundary polynomial $\chi_M(S,U)$ is determined from this:*

$$\chi_i(U) = \begin{cases} \mu_i(U), & \text{for } i < d^* - 1, \\ 0, & \text{for } n-d < i < n, \\ 1, & \text{for } i = n. \end{cases}$$

Proof. The first equality follows from Proposition 11.3, the definition of the Möbius and coboundary polynomial, and Lemma 11.2. We proved this statement for codes and arrangements in Theorem 10.26. If d is the smallest size of a cocircuit in M, then $n-d$ is the biggest size of a hyperplane in M and thus the biggest size of a flat with rank smaller then k in M. This implies the second equality. The third equality is obvious from the definition of the coboundary polynomial. □

Using this theorem, we can determine the value of $\chi_i(U)$ for $(d^*-1)+(d-1)+1 = d^*+d-1$ values of i. This leaves $n+1-(d^*+d-1) = n-d-d^*+2$ of the $\chi_i(U)$ unknown. We can say the same about the coefficients $\chi_i^*(U)$ of the coboundary polynomial $\chi_{M^*}(S,U)$ of the dual matroid. The idea is to use Theorem 11.1 to calculate the missing values of $\chi_i(U)$ and $\chi_i^*(U)$. We first rewrite Theorem 11.1 to a more convenient form.

Proposition 11.5. *Let $\chi_i(U)$ be the coefficients of the coboundary polynomial of a simple matroid M with simple dual M^*. Let $\chi_i^*(U)$ be the coefficients of the coboundary polynomial of M^*. Then*

$$U^{v-k}\sum_{i=v}^{n}\binom{i}{v}\chi_i(U) = \sum_{i=n-v}^{n}\binom{i}{n-v}\chi_i^*(U), \qquad v = 0,\ldots,n.$$

Proof. This is obtained by rewriting the formula in Theorem 11.1. This is analogous to the rewriting of the MacWilliams relations from coding theory, see for example [70, §5.2]. Replacing S by $S+1$, binomial expanding and reversing the order of summation gives:

$$\begin{aligned}
\sum_{i=0}^{n}\chi_i^*(U)S^i &= (S-1)^nU^{-k}\sum_{i=0}^{n}\chi_i(U)\left(\frac{S+U-1}{S-1}\right)^i \\
\sum_{i=0}^{n}\chi_i^*(U)(S+1)^i &= S^nU^{-k}\sum_{i=0}^{n}\chi_i(U)\left(\frac{S+U}{S}\right)^i \\
\sum_{i=0}^{n}\chi_i^*(U)\sum_{v=0}^{i}\binom{i}{v}S^v &= U^{-k}\sum_{i=0}^{n}S^{n-i}\chi_i(U)\sum_{v=0}^{i}\binom{i}{v}S^{i-v}U^v \\
\sum_{v=0}^{n}S^v\sum_{i=v}^{n}\binom{i}{v}\chi_i^*(U) &= \sum_{v=0}^{n}S^{n-v}U^{v-k}\sum_{i=v}^{n}\binom{i}{v}\chi_i(U) \\
\sum_{v=0}^{n}S^{n-v}\sum_{i=n-v}^{n}\binom{i}{n-v}\chi_i^*(U) &= \sum_{v=0}^{n}S^{n-v}U^{v-k}\sum_{i=v}^{n}\binom{i}{v}\chi_i(U).
\end{aligned}$$

Comparing the coefficients of S^{n-v} leads to the given formula. □

In some cases, the relations from Theorem 11.4 and Propositions 11.5 are enough to completely determine the coboundary polynomial $\chi_M(S,U)$ from the polynomials $\mu_M(S,U)$ and $\mu_{M^*}(S,U)$.

Theorem 11.6. *Let M be a matroid with $2(d+d^*) \geq n+3$. Then the Möbius polynomials $\mu_M(S,U)$ and $\mu_{M^*}(S,U)$ determine $\chi_M(S,U)$.*

We give three ways to prove this theorem, exploiting various techniques in matroid theory. The first two proofs show that the proposed construction, using the duality relations in Proposition 11.5, indeed works. For the third proof, we use the theory of zeta polynomials.

11.2 Independence of duality relations

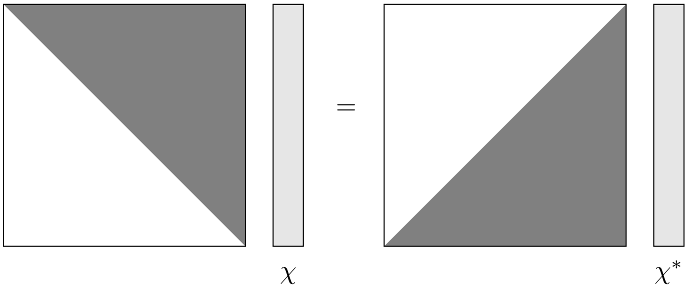
Proof (Theorem 11.6). We try to determine the coboundary polynomials of M and M^* simultaneously. First we use Theorem 11.4 for M and M^*. This gives us the value of $\chi_i(U)$ for $i < d^*-1$ and $i > n-d$, and the value of $\chi_i^*(U)$ for $i < d-1$ and $i > n-d^*$. So we are left with the unknowns

$$\chi_{d^*-1}(U), \chi_{d^*}(U), \ldots, \chi_{n-d}(U), \chi_{d-1}^*(U), \chi_d^*(U), \ldots, \chi_{n-d^*}^*(U).$$

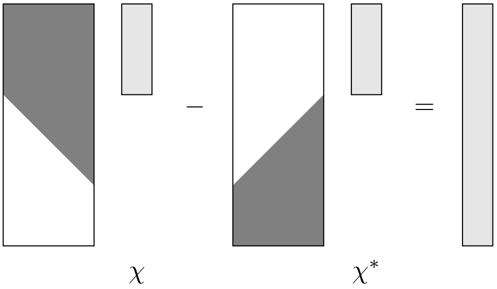
This are $2(n-d-d^*+2)$ variables. Proposition 11.5 gives us $n+1$ equations. In order for this system to be solvable, we need at least as may equations as unknowns. This means

$$\begin{array}{rcl} n+1 & \geq & 2(n-d-d^*+2) \\ n+1 & \geq & 2n+4-2(d+d^*) \\ 2(d+d^*) & \geq & n+3. \end{array}$$

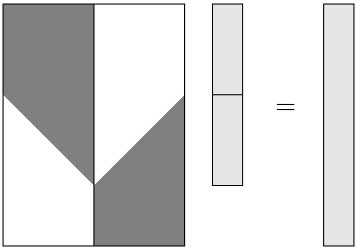
We now need to show that, given $2(d+d^*) \geq n+3$, we have enough independent equations. Since all the coefficients of the equations are known, it is possible to do this directly, but that gives lengthy calculations. We will give a more graphical approach. First, we visualize how Proposition 11.5 looks like in matrix form. The grey areas of the matrices are filled with nonzero entries, the white areas contain only zeros. The vectors are filled with light grey, because it does not matter if the entries are zero or not.



From the triangular shape of the matrices, it is clear that they both have full rank – something we could have also concluded from the fact that the relation in Theorem 11.1 is a two way equivalence. We order the system now in a way that all unknowns are on the left hand side. This means for the first matrix we “cut off” d^*-1 columns at the right of the matrix, and $d-1$ at the left, since they correspond to values of i for which $\chi_i(U)$ is known. For the second matrix, it is the other way around. Since we assumed $2(d+d^*) \geq n+3$, we are cutting off at least half of the rows. The new system looks like this:



The vector on the right hand side is known and depends on d, d^* and the two Möbius polynomials. The matrices both have full rank $n-d-d^*+2$, as is clear from their shape. We can write this as one system by "glueing together" the matrices on the left hand side.



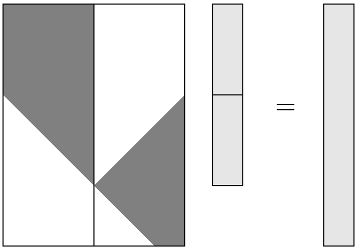
We need to show that this matrix has full rank. Have a look at the bottom d rows of this matrix. The complete left side is zero, so we ignore that for a moment. The right side has all entries nonzero, and from Proposition 11.5 we know the entries are binomial coefficients:

$$\begin{pmatrix} \binom{d-1}{d-1} & \binom{d}{d-1} & \cdots & \binom{n-d^*}{d-1} \\ \vdots & \vdots & & \vdots \\ \binom{d-1}{1} & \binom{d}{1} & \cdots & \binom{n-d^*}{1} \\ \binom{d-1}{0} & \binom{d}{0} & \cdots & \binom{n-d^*}{0} \end{pmatrix}.$$

By the inductive relations between binomial coefficients, we can perform row operations on this matrix to obtain

$$\begin{pmatrix} 0 & 0 & \cdots & \binom{n-d-d^*+1}{d-1} \\ \vdots & \vdots & & \vdots \\ 0 & \binom{1}{1} & \cdots & \binom{n-d-d^*+1}{1} \\ \binom{0}{0} & \binom{1}{0} & \cdots & \binom{n-d-d^*+1}{0} \end{pmatrix}.$$

Flipping the matrix upside down, we have obtained the following picture:



In this picture, we show the case for $d < n-d-d^*+2$. If we had $d \geq n-d-d^*+2$, we would have obtained a matrix that was of full rank and we were done. If $d^* \geq n-d-d^*+2$, we can change M and M^* and we are also done. So from now on, assume $d, d^* < n-d-d^*+2$. Call the left and the right half of the matrix L and R. Suppose a linear combination of the columns of the matrix is zero. Since all columns inside L and inside R are independent, this means we can make a linear combination $\mathbf{l}$ of columns of L and a linear combination $\mathbf{r}$ of columns of R that are both nonzero and a nonzero multiple of each other.
By the shape of L and R, the first d^* and the last d entries of $\mathbf{l}$ and $\mathbf{r}$ have to be zero. We will show that the remaining $n-d-d^*+1$ entries of $\mathbf{l}$ and $\mathbf{r}$ cannot be multiples of each other.
Crucial in the proof is that all rows of L are multiplied with a different power of U, whereas R is completely filled with integers. Therefore, any linear combination of columns of R will have the same powers of U involved in every nonzero entry, even if we take the coefficients of the linear combination to be polynomials in U and U^{-1}. On the other hand, the entries of $\mathbf{l}$ will all have different powers of U involved. The only possibility to cancel this out, is if we can have only one nonzero entry in $\mathbf{l}$ and $\mathbf{r}$, at the same place.
We focus now on the matrix L. It has maximal (column) rank $n-d-d^*+2$. From Proposition 11.5 we know the entries are binomial coefficients, with every row multiplied with another (possibly negative) power of U. The first d^* rows form a matrix with rank d^*, from the same reasoning we used for the last d rows of R. So if we make a linear combination of the columns of L where the first d^* entries are zero, there are $n-d-d^*+2-d^* = n-d-2d^*+2$ free variables involved. Note we assumed $d^* < n-d-d^*+2$, so this number is positive. We can use those free variables to make more entries of $\mathbf{l}$ zero: add one of the middle $n-d-d^*+1$ rows of L as an extra constraint, and choose one of the free variables in a way that the corresponding entry in $\mathbf{l}$ becomes zero. We are left with

$$n-d-d^*+1-(n-d-2d^*+2) = d^*-1 \geq 2$$

entries of $\mathbf{l}$ that are not zero. They also cannot be zero "by accident" since the middle $n-d-d^*+1$ rows of L form a matrix of full rank. So $\mathbf{l}$ cannot have only one nonzero entry, as was to be shown.
To summarize, we have shown that we can use Theorem 11.4 and some of the equations in Proposition 11.5 to find $\chi_M(S,U)$ from $\mu_M(S,U)$ and $\mu_{M^*}(S,U)$ if $2(d+d^*) \geq n+3$. □

11.3 Divisibility arguments

In the previous section, we directly showed that the construction to determine $\chi_M(S,U)$, given $\mu_M(S,U)$ and $\mu_{M^*}(S,U)$ and using Theorem 11.4 and Proposition 11.5, indeed works. In this paragraph, we will give a direct proof that if two matroids have the same Möbius polynomials, and their duals too, then the matroids have the same coboundary polynomial. Although the proof itself is not constructive, it is a much shorter proof for Theorem 11.6 and it also shows why the proposed construction works. The proofs in this section are similar to the proof of the Mallows-Sloane bound given in [38] and are thanks to an anonymous referee for [54].

Proof (Theorem 11.6). Let two matroids M_1 and M_2 have coboundary polynomials χ_{M_1} and χ_{M_2} (we omit the (S,U) part for clarity). Let the Möbius polynomials of the matroids coincide, just as the matroid polynomials of their duals: so, let $\mu_{M_1} = \mu_{M_2}$ and $\mu_{M_1^*} = \mu_{M_2^*}$. We will show that if $2(d+d^*) \geq n+3$, then $\chi_{M_1} = \chi_{M_2}$.
Using Theorem 11.4, we see that the coefficients of χ_{M_1} and χ_{M_2} coincide for $i < d^*-1$ and $i > n-d$. It follows that

$$S^{d^*-1} \mid \chi_{M_1} - \chi_{M_2} \quad \text{and} \quad \deg_S(\chi_{M_1} - \chi_{M_2}) \leq n-d.$$

Combining this with Theorem 11.1, we find that

$$(S+U-1)^{d^*-1} \mid \chi_{M_1^*} - \chi_{M_2^*} \quad \text{and} \quad (S-1)^d \mid \chi_{M_1^*} - \chi_{M_2^*}.$$

If we apply Theorem 11.4 to the dual matroids, we find that

$$S^{d-1} \mid \chi_{M_1^*} - \chi_{M_2^*} \quad \text{and} \quad \deg_S(\chi_{M_1^*} - \chi_{M_2^*}) \leq n-d^*.$$

Combining all the divisibilities, we have

$$(S+U-1)^{d^*-1}(S-1)^d S^{d-1} \mid \chi_{M_1^*} - \chi_{M_2^*},$$

where the degree of $\chi_{M_1^*} - \chi_{M_2^*}$ in S is at most $n-d^*$. For $(d^*-1)+d+(d-1) > n-d^*$, i.e., for $2(d+d^*) \geq n+3$, this implies $\chi_{M_1^*} = \chi_{M_2^*}$ and thus $\chi_{M_1} = \chi_{M_2}$. □

This proof is a matroid generalization of the following result for codes, that we include here to illustrate the application of Theorem 11.6 for codes.

Theorem 11.7. *Let C_1 and C_2 be two codes with the same length and let d and d^* be two integers such that $0 < d, d^* < n$. Suppose C_1 and C_2 have the same number of words of weight w for $w < d$ and $w > n-d^*+1$, and suppose the dual codes $C_1^\perp$ and $C_2^\perp$ have the same number of words for $w < d^*$ and $w > n-d+1$. If $2(d+d^*) \geq n+3$, then C_1 and C_2 have the same weight distribution.*

Proof. Write the weight enumerator of a code as

$$W_C = \sum_{w=0}^{n} A_w X^{n-w} Y^w.$$

Also here we omit the (X,Y) part for clarity. Because the weight distributions of the two codes coincide for $w < d$ and $n-w < d^*-1$, we have

$$X^{d^*-1} Y^d \mid W_{C_1} - W_{C_2}.$$

Applying the MacWilliams relations gives

$$(X+(q-1)Y)^{d^*-1} \mid W_{C_1^*} - W_{C_2^*} \quad \text{and} \quad (X-Y)^d \mid W_{C_1^*} - W_{C_2^*}.$$

Because the weight distributions of the dual codes coincide for $w < d^*$ and $n-w < d-1$, we have

$$X^{d-1}Y^{d^*} \mid W_{C_1^*} - W_{C_2^*}.$$

Combining the divisibilities, we find that

$$(X+(q-1)Y)^{d^*-1}(X-Y)^d X^{d-1}Y^{d^*} \mid W_{C_1^*} - W_{C_2^*}.$$

The total degree of all terms in $W_{C_1^*} - W_{C_2^*}$ is n. So, for $(d^*-1)+d+(d+1)+d^* > n$, i.e., for $2(d+d^*) \geq n+3$, this implies $W_{C_1^*} = W_{C_2^*}$ and thus $W_{C_1} = W_{C_2}$. □

Note that in this theorem d and d^* do not necessarily have to be the minimum distance and dual minimum distance of the code. As long as the total length of the four intervals on which the weights agree is big enough, the theorem holds.

11.4 Zeta polynomials

In Chapter 3 we discussed the zeta polynomial of a code. We will extend this theory to matroids, and use it to give another construction to prove Theorem 11.6. Just as with the other polynomials, we often refer to the zeta polynomial in the following form:

$$P_C(T,U) = \sum_{i=0}^{r} P_i(U)\, T^i.$$

Duursma [39] extended the definition of the zeta polynomial to matroids. We choose a similar approach and use that we can talk about the extended weight enumerator of a matroid, via its equivalence with the Tutte polynomial (see Theorems 8.4 and 8.5).

Theorem 11.8. *Let M be a matroid with coboundary polynomial $\chi_M(S,U)$. The two-variable zeta polynomial $P_M(T,U)$ of this matroid is the unique polynomial in $\mathbb{Q}[T,U]$ of degree at most $n-d$ in T such that if we expand the generating function*

$$\frac{P_M(T,U)}{(1-T)(1-TU)}(1+(S-1)U)^n$$

as a power series in the variable T, we get

$$\ldots + \ldots T^{n-d-1} + \frac{\chi_M(S,U) - S^n}{U-1} T^{n-d} + \ldots T^{n-d+1} + \ldots .$$

Proof. Apply $X = 1$ and $Y = S^{-1}$ in the definition of the zeta function and multiply the whole equation with S^n.

$$\begin{aligned} Z(T,U)\cdot(Y(1-T)+XT)^n &= \ldots + \frac{W_C(X,Y,U) - X^n}{U-1} T^{n-d} + \ldots \\ Z(T,U)\cdot S^n \cdot (S^{-1}(1-T)+T)^n &= \ldots + \frac{W_C(1,S^{-1},U) - 1}{U-1} S^n T^{n-d} \\ Z(T,U)\cdot(1+(S-1)T)^n &= \ldots + \frac{\chi_M(S,U) - S^n}{U-1} T^{n-d} + \ldots \end{aligned}$$

□

Propositions 3.2, 3.4, and 3.5 and Theorem 3.3 have a direct analogue for matroids. Let $X_{n,d}$ be the coboundary polynomial of the uniform matroid on n elements with rank $n-d+1$.

PROPOSITION 11.9. *A matroid is uniform if and only if* $P_M(T,U)=1$.

THEOREM 11.10. *The zeta polynomial gives us a way to write the coboundary polynomial with respect to a basis of coboundary polynomials of uniform matroids:*

$$\chi_M(S,U)=P_0(U)\,X_{n,d}+P_1(U)\,X_{n,d+1}+\ldots+P_r(U)\,X_{n,d+r}.$$

PROPOSITION 11.11. *The degree of* $P_M(T,U)$ *in* T *is* $n-d-d^*+2$.

PROPOSITION 11.12. *For the two-variable zeta polynomial of a matroid* M *and dual* M^* *we have*

$$P_{M^*}(T,U)=P_M\left(\frac{1}{TU},U\right)\,U^{n-k+1-d}T^{n-d-d^*+2}.$$

We are now ready to give an alternative proof of Theorem 11.6 using the two-variable zeta polynomial.

PROOF (THEOREM 11.6). Our goal is to determine all the coefficients $P_j(U)$ of the two-variable zeta polynomial, and thus the coboundary polynomial $\chi_M(S,U)$. Denote the coefficient of S^j in $X_{n,d}$ by $X_{n,d,j}$. We know the exact value of these coefficients, just like we know the extended weight enumerator of MDS codes, see Theorem 2.27. So, we can split up Theorem 11.10 in $n+1$ equations:

$$\chi_j(U)=\sum_{i=0}^{n-d-d^*+2}P_i(U)\,X_{n,d+i,j},\qquad j=0,\ldots,n.$$

Not all of these equations are helpful in determining the $P_i(U)$. For $j<d^*-1$ and $j>n-d$ the $\chi_j(U)$ are known by Theorem 11.4. In the case $n-d<j<n$ we have $\chi_j(U)=0$ and also $X_{n,d+i,j}=0$ for all i, so the corresponding equations just state $0=0$. For $d^*-1\leq j\leq n-d$ we don't know $\chi_j(U)$, so these equations are also not helpful. We are left with the equations for $j<d^*-1$ and $j=n$, so d^* equations in the $n-d-d^*+3$ unknown $P_i(U)$.
We can do the same for the dual matroid, leading to d equations in the $n-d-d^*+3$ unknown $P_i^*(U)$. From Proposition 11.12 it follows that

$$P_i^*(U)=U^{i-k-1+d^*}P_{n-d-d^*+2-i}(U),$$

so we can replace the $P_i^*(U)$ one-to-one by the appropriate $P_i(U)$. So all together, we have $d+d^*$ equations in $n-d-d^*+3$ unknown $P_i(U)$. To get at least as many equations as unknowns, we need

$$\begin{array}{rcl} d+d^* & \geq & n-d-d^*+3 \\ 2(d+d^*) & \geq & n+3. \end{array}$$

This is the same bound we already obtained in Theorem 11.6. □

11.5 Open questions

We have seen two methods to determine the coboundary polynomial $\chi_M(S,U)$ of a matroid from the Möbius polynomials $\mu_M(S,U)$ and $\mu_{M^*}(S,U)$ of a matroid and its dual. Both methods rely on duality relations for, respectively, the coboundary and Tutte polynomial.

Theorem 11.6 is valid for matroids that are "close" to the uniform matroid. Stated in terms of codes, this means codes with a minimum distance and dual minimum distance that is high, so the code is "close to MDS". Examples of such codes are MDS codes itself (but this is a trivial example, since there is only one uniform matroid given length and rank) and near-MDS codes, these are codes with $d = n - k$ and $d^{\perp} = k$ (see Definition 10.27). Also almost-MDS codes with $k \leq n/2$ are in this category. See Boer [33] for more on almost-MDS codes and Faldum and Willems [41] for more on codes that are close to MDS. Other specific codes that have $2(d + d^*) \geq n + 3$ are the q-ary Hamming codes (and their duals, the simplex codes) and the first order q-ary Reed-Muller codes. These codes were treated in Chapter 5.

A logical question is now: how sharp is the bound in Theorem 11.6? To look for an example to show the bound is tight, we need two matroids with the same parameters and $2(d + d^*) < n + 3$ that have equal Möbius polynomials $\mu_M(S,U)$ and $\mu_{M^*}(S,U)$ but different coboundary polynomial $\chi_M(S,U)$. The smallest case is $d = d^* = 3$ (because otherwise the matroid is not simple) and thus $n = 10$.
An exhaustive computer search on 260 random matrices with the desired parameters and $k = 5$ did not lead to such an example, so there is room for improvement on the bound in Theorem 11.6.

In Proposition 6.3 of [24] the issue is addressed how many Tutte polynomials there are, given the size and rank of a matroid. This is done by looking at the affine space generated by the coefficients of the Tutte polynomial, and determining its dimension. See also [25]. It would be interesting to see if we can do the same thing for the Möbius polynomial, given n, k, d and d^*. If we determine the dimension of the affine space generated by the coefficients of the Möbius polynomial of a matroid and its dual, we can compare it to the dimension for the Tutte polynomial. This could give us more information about the relations between the Möbius and coboundary polynomials in general.

12

The spectrum polynomial

The spectrum polynomial of a matroid M without loops was introduced by Kook, Reiner and Stanton to show that the spectra of the combinatorial Laplace operators on the independent complex $IN(M)$ are nonnegative and integral [65]. The spectrum polynomial contains the same information as these spectra, hence the name *spectrum polynomial.* The main results concerning the spectrum polynomial are the recurrence relations by Kook [64] and the generalization of Denham [34] to an invariant that specializes to both the Tutte polynomial and to the spectrum polynomial. Since it is a matroid invariant, it is tempting to compare the spectrum polynomial to the Tutte polynomial. Kook et al. [65] showed that the Tutte polynomial does not determine the spectrum polynomial. The opposite problem is still open.
In this chapter we calculate the spectrum polynomial of the uniform matroid M of rank k on n elements. We give two different methods, using equivalent definitions of the spectrum polynomial.

12.1 Calculations using combinatorics

The spectrum polynomial has the following combinatorial definition.

Definition 12.1. Let $M = (E, \mathcal{I})$ be a matroid and $L(M)$ the associated geometric lattice. Then the *spectrum polynomial* of M is defined by

$$\mathrm{Spec}_M(S,U) = \sum_{x,y \in L(M)} |\tilde{\chi}(IN(x))|\, |\mu_{L(M)}(x,y)|\, U^{r(y)} S^{|x|},$$

where $|x|$ is the number of elements of M that are in the flat x and $\tilde{\chi}(IN(x))$ is the *reduced Euler characteristic* of the independence complex of x.

The value of $|x|$ is equal to $a(x)$ for all flats x if M is a simple matroid. The following formula holds by [14, p. 238]:

$$|\tilde{\chi}(IN(M))| = R_M(-1,0) = \sum_{I \in \mathcal{I}} (-1)^{r(M)-|I|}.$$

We will start by calculating the Möbius function of the uniform lattice.

LEMMA 12.2. *The Möbius function of the uniform lattice $U_{n,k}$ is given by*

$$\mu(x,y)=\begin{cases}0, & \textit{if} \quad x\not\leq y,\\ (-1)^{|y|-|x|}, & \textit{if} \quad y\neq\hat{1},\\ \sum_{i=1}^{k-|x|}(-1)^i\binom{n-|x|}{i-1}, & \textit{if} \quad y=\hat{1}.\end{cases}$$

PROOF. We know $\mu(x,x)=1$ and $\mu(x,y)=0$ if x and y are not comparable. If $x\leq y$, we get an alternating sum of binomial coefficients. For $y\neq\hat{1}$ the corresponding lattice is the full powerset, so $\mu(x,y)=(-1)^{|y|-|x|}$, see for example [29]. □

THEOREM 12.3. *The spectrum polynomial of the uniform matroid $U_{n,k}$ is equal to*

$$\operatorname{Spec}_{U_{n,k}}(S,U)=\sum_{r=0}^{k-1}\binom{n}{r}U^r+\binom{n-1}{k-1}U^k+\binom{n-1}{k}S^nU^k.$$

PROOF. The Möbius function of the uniform lattice was calculated in Lemma 12.2. We continue with the calculation of the Euler characteristic $\chi(IN(x))$. We first look at the case $x\neq\hat{1}$. Then all subsets of x are independent: summing over their rank, the Euler characteristic becomes

$$\sum_{i=0}^{|x|}(-1)^{|x|-i}\binom{|x|}{i}.$$

This expression is zero, except for $x=\hat{0}$, the empty set: then $\chi=1$. If $x=\hat{1}$ the Euler characteristic is equal to

$$\sum_{i=0}^{k}(-1)^{k-i}\binom{n}{i}.$$

We have enough information now to calculate the spectrum polynomial. We only have to look at three cases, since for the others the Euler characteristic is zero:

1. $y\neq\hat{1}$ and $x=\hat{0}$,

2. $y=\hat{1}$ and $x=\hat{0}$,

3. $y=x=\hat{1}$.

For the first one, the value in the inner summation of the spectrum polynomial is 1, so we just have to count the number of elements on each level of L. The second and third case are just filling in the right values in the Möbius function and Euler characteristic. So, we have

1. $\binom{n}{r}U^r$ for all $r<k$,

2. $U^k\cdot\left|\sum_{i=0}^{k}(-1)^{k-i}\binom{n}{i}\right|\cdot 1\cdot S^n$,

3. $U^k\cdot 1\cdot\left|\sum_{i=1}^{k}(-1)^i\binom{n}{i-1}\right|\cdot S^0$.

The summation in the second case can be rewritten as

$$\sum_{i=0}^{k}(-1)^{k-i}\binom{n}{i} = (-1)^k\sum_{i=0}^{k}(-1)^i\binom{n}{i} = (-1)^{2k}\binom{n-1}{k},$$

so the absolute value of this is $\binom{n-1}{k}$. The summation in the third case can be rewritten similarly:

$$\sum_{i=1}^{k}(-1)^i\binom{n}{i-1} = (-1)\sum_{i=0}^{k-1}(-1)^i\binom{n}{i} = (-1)^k\binom{n-1}{k-1},$$

which has absolute value $\binom{n-1}{k-1}$. Note that these two binomials add up to $\binom{n}{k}$, the number of bases of M. Filling in the calculated expressions for the Euler characteristic and the Möbius function, we find that the spectrum polynomial of the uniform matroid $U_{n,k}$ is equal to the given formula. □

12.2 Calculations using ordered matroids

Another way of defining the spectrum polynomial is based on the next theorem, see [65, Theorem 1].

Theorem 12.4. *Let $M = (E, \omega, \mathcal{I})$ be an ordered matroid. Then we can decompose each independent set I into two disjoint sets $I = I_1 \cup I_2$ such that I_1 is a base of internal activity 0 for the flat $|\overline{I_1}|$ and I_2 is a base of external activity 0 for the contracted matroid $\overline{I} \backslash \overline{I_1}$.*

Proof. The desired decomposition can be obtained by the following algorithm:

1. Start with $I_1 = I$ and let $V = \overline{I_1}$.

2. Pick the smallest element $e \in I_1$ with respect to ω.

3. Find the fundamental cocircuit of e with respect to I_1 in V, i.e. the unique cocircuit in $V - I_1 + e$.

4. If e is the smallest element in this cocircuit (i.e. internally active in I_1), remove it from I_1 and redefine $V = \overline{I_1}$.

5. Take the next $e \in I_1$ with respect to ω and return to Step 3. If there are no elements left in V, we are done.

See [65] for a proof that this construction indeed gives the decomposition from the theorem. □

Definition 12.5. Let $M = (E, \omega, \mathcal{I})$ be an ordered matroid. Then the *spectrum polynomial* of M is defined by

$$\mathrm{Spec}_M(S, U) = \sum_{I \in \mathcal{I}} S^{|\overline{I_1}|} U^{r(I)}.$$

We can now give a proof of Theorem 12.3 that uses an ordering of the matroid.

Proof (Theorem 12.3). We use the algorithm in the proof of Theorem 12.4. For an independent set $I \in \mathcal{I}$ with $|I| < k$, this algorithm gives $I_1 = \emptyset$, as we show by induction. For $I = \emptyset$ we obviously get $I_1 = \emptyset$. Now assume $I_1 = \emptyset$ for all I with $|I| < r$ and $0 < r < k$, and pick an independent set I with $|I| = r$. The closure of this set is the set itself, so we start with $V = I_1 = I$. Let e be the smallest element in I. (Actually, the following works for any element in I.) Then $V - I_1 + e = \{e\}$, so the fundamental cocircuit of e consists of just the element e. Therefore, e is the smallest element in its fundamental cocircuit and we remove it from I_1. Now $|I_1| = r - 1$ and according to the induction hypothesis this reduces further to $I_1 = \emptyset$.
The number of independent sets of size r is equal to $\binom{n}{r}$, so we get terms $\binom{n}{r}U^r$ for $0 \leq r < k$.

Now we look at the bases of $U_{n,k}$ and see how the algorithm applies. Since $\overline{B} = E$ we start with $V = E$ and $I_1 = B$. For any element $e \in B$, its fundamental cocircuit is the whole of $E - B + e$ because a set of smaller size is independent in $U^*_{n,k}$. Let e be the smallest element of E. We distinguish between $e \in B$ and $e \notin B$.
In the first case, when e is internally active, we remove e from I_1 to get $|I_1| = k - 1$ and by the above we end up with $I_1 = \emptyset$. The number of bases which contain e is equal to $\binom{n-1}{k-1}$, so we get the term $\binom{n-1}{k-1}U^k$.
If $e \notin B$ there are no internally active elements in B, since all fundamental cocircuits contain e. There are $\binom{n-1}{k}$ bases which do not contain e, so we get the term $\binom{n-1}{k}S^nU^k$.

Altogether we get the result we already know: the spectrum polynomial of the uniform matroid $U_{n,k}$ is equal to

$$\mathrm{Spec}_{U_{n,k}}(S, U) = \sum_{r=0}^{k-1} \binom{n}{r} U^r + \binom{n-1}{k-1} U^k + \binom{n-1}{k} S^n U^k.$$

□

13

Truncation formulas

The mathematical meaning of *truncation* is just as it is in every day life: cutting something off. In the situation of this chapter, we will be “cutting off” matroids and geometric lattices by ‘removing’ their hyperplanes and bases, respectively. An overview of more possible constructions on matroids and geometric lattices can be found in [26].
Britz [21] showed that the rank generating function of a truncated matroid is defined by the rank generating function of the matroid itself. It is a natural question to ask if there are similar truncation formulas for other polynomials. We will give truncation formulas for the coboundary, Möbius and spectrum polynomial. The outline of the combinatorial proof for these formulas is the same for all three polynomials.
This chapter is a copy of [57].

13.1 Truncation of matroids and geometric lattices

We can define the truncation of a matroid in several equivalent ways, just as we can define a matroid in terms of its independent sets, bases, rank function, flats, circuits, etcetera. We will give some equivalent definitions that are most suitable for our purposes. For a more extensive list, see [26].

Definition 13.1. The *truncation* of a matroid M of rank $r(M) = r \geq 1$ is denoted by $\tau(M)$. It has the same set of elements as M and it has the following equivalent definitions:

- The independent sets of $\tau(M)$ are all the independent sets of M, except those of rank r.
- The rank function of $\tau(M)$ is given by $r_{\tau(M)}(A) = \min\{r_M(A), r-1\}$.
- The bases of $\tau(M)$ are the independent sets of rank $r-1$ in M.

The truncation of a matroid is again a matroid.

Example 13.2. Consider the uniform matroid $M = U_{n,r}$ on n elements of rank $r \geq 1$. Then $\tau(M) = U_{n,r-1}$.

For a geometric lattice, the definition is more straightforward.

Definition 13.3. The *truncation* of a geometric lattice L of rank $r(L) = r \geq 1$ with partial ordering $\leq$ has as elements all the elements of L except those of rank $r-1$, with the same partial ordering $\leq$. It is denoted by $\tau(L)$.

The truncation of a geometric lattice is again a geometric lattice. Note that the truncations of a matroid and a geometric lattice each have rank $r-1$. For a matroid M, we denote by $L(M)$ its associated geometric lattice of flats. Conversely, for a geometric lattice L, we denote by $M(L)$ its associated matroid. Then $\tau(M(L)) = M(\tau(L))$ and $\tau(L(M)) = L(\tau(M))$.

Instead of removing all elements of rank $r-1$ from a geometric lattice, one might ask what happens if we remove all elements of rank 1, the *atoms*, from the geometric lattice. Unfortunately, the resulting structure is no longer a geometric lattice. We therefore loosen our definitions to get a class of objects that is closed under this “truncation from below”. If we start with a geometric lattice and drop the requirements that it is atomic and that its rank function is semimodular, we get a poset with rank function, see Proposition 9.18.

Definition 13.4. The *upper truncation* of a poset with rank function P of rank $r(P) = r \geq 1$ with partial ordering $\leq$ has as elements all the elements of P except those of rank $r-1$, with the same partial ordering $\leq$. It is denoted by $\tau_+(P)$. The *lower truncation* of P has as elements all the elements of P except those of rank 1, with the same partial ordering $\leq$. It is denoted by $\tau_-(P)$.

Again, truncating lowers the rank by 1, so $\tau_+(P)$ and $\tau_-(P)$ both have rank $r-1$.

Lower truncation can be described in terms of upper truncation and inversion (see Definition 9.9): the lower truncation of a poset can be obtained by first inverting the poset, then taking upper truncation, and then inverting back again. On the other hand, we can obtain upper truncation by first inverting, then taking lower truncation, and then inverting back again.

Let L be a geometric lattice of rank r, and $P(L)$ its associated poset with rank function. Then $P(\tau(L)) = \tau_+(P(L))$. But it is not true that $\tau_-(P(L))$ is the poset of some sort of truncation of the geometric lattice L, since it is not always the case that the rank function on $\tau_-(P(L))$ is semimodular.

Example 13.5. Consider $M = U_{4,4}$, the uniform matroid on 4 elements of rank 4. Let L be the lattice of flats of M, and P the associated poset of L with rank function. Consider $x = \{1,2\}$ and $y = \{3,4\}$ in $\tau_-(P)$. The meet and join of x and y in $\tau_-(P)$ are given by $x \wedge y = \emptyset$ and $x \vee y = \{1,2,3,4\}$, respectively. Then $r_{\tau_-(P)}(x) = r_{\tau_-(P)}(y) = 1$ and $r_{\tau_-(P)}(x \wedge y) = 0$ and $r_{\tau_-(P)}(x \vee y) = 3$. Hence $\tau_-(P)$ is not a geometric lattice.

There is a natural way to extend the lattice $\tau_-(L)$ to a geometric lattice, called *Dilworth completion*. See [26, §7.7], [35], [67], and [104, §12]. The result of this completion is referred to as the *Dilworth truncation* of a lattice. It can be viewed as the smallest geometric lattice that contains $\tau_-(L)$. Since our techniques for finding truncation formulas do not apply to the Dilworth truncation, we will not go into the details of its definition.

13.2 Representation of a truncated matroid

It was shown by Mason [71, §2.4] that if a matroid is representable over a field, then its Dilworth truncation is representable over an extension of that field. For ordinary truncation this question is addressed in [26, Prop. 7.4.10]: if M is a matroid that is representable over the field $\mathbb{F}$, then $\tau(M)$ is a representable matroid over a transcendental extension of $\mathbb{F}$. We will give a stronger version of this result.

Example 13.6. Consider the simplex code C of dimension 3 over the finite field with q elements. This code has length $n = q^2 + q + 1$ and minimum distance q^2. The associated matroid $M = M_C$ is by definition representable. The truncation $\tau(M)$ is the uniform matroid $U_{n,2}$. Now $U_{n,2}$ is representable over $\mathbb{F}_q$ if and only if n is at most $q+1$. Therefore $\tau(M)$ is representable over any extension of $\mathbb{F}_{q^3}$ but it is not representable over $\mathbb{F}_q$ itself.

Theorem 13.7. *Let M be a matroid of rank k on n elements that is representable over a field $\mathbb{F}$.*

1. *If $\mathbb{F}$ is infinite, then $\tau(M)$ is representable over $\mathbb{F}$.*
2. *If $\mathbb{F}$ is finite consisting of q elements and $m \geq \lceil \log_q(\binom{n}{k-1}) \rceil + 1$, then $\tau(M)$ is representable over $\mathbb{F}_{q^m}$.*

Proof. Suppose that M is a matroid of rank k on the set $E = \{1, \ldots, n\}$ and M is represented by a $k \times n$ matrix G of rank k over $\mathbb{F}$. A subset I of E is an independent set of M if and only if the columns of G enumerated by I are independent. Let C be the subspace of $\mathbb{F}^n$ generated by the rows of G. Then C has dimension k, since G has rank k. The idea of the proof is to show that a "generic" subspace of C of dimension $k-1$ represents $\tau(M)$. In order to have enough space one has to extend the field $\mathbb{F}$ in case it is finite, since a finite union of hyperplanes in $\mathbb{F}^n$ might be equal to $\mathbb{F}^n$. The details are similar as given in the proof of Proposition 5.1 of [79].

The space C is the null space of a $(n-k) \times n$ matrix H of rank $n-k$ over $\mathbb{F}$. Let $|I| = k$. Then I is a basis of M if and only if the columns of H enumerated by $J = E \setminus I$ are independent. Let $t = n - k$ and let $H(j_1, \ldots, j_t)$ be the $t \times t$ matrix obtained from H by taking the columns numbered by $j_1, \ldots, j_t \in J$, where $1 \leq j_1 < \ldots < j_t \leq n$. Let $\Delta(j_1, \ldots, j_t)$ be the determinant of $H(j_1, \ldots, j_t)$.

Now let I be a basis of $\tau(M)$ and let $J = E \setminus I$. Then $|I| = k-1$ and there exists an i in J such that $I \cup \{i\}$ is a basis of M. Hence the columns of H enumerated by $J \setminus \{i\}$ are independent. Let $J = \{j_1, \ldots, j_{t+1}\}$ for some $1 \leq j_1 < \ldots < j_{t+1} \leq n$. Consider the linear function given by

$$f_I(X_1, \ldots, X_n) = \sum_{s=1}^{t+1} (-1)^s \Delta(j_1, \ldots, \hat{j}_s, \ldots, j_{t+1}) X_{j_s},$$

where $(j_1, \ldots, \hat{j}_s, \ldots, j_{t+1})$ is the t-tuple obtained from $(j_1, \ldots, j_s, \ldots, j_{t+1})$ by deleting the s-th element. There exists an s such that $j_s = i$ and the corresponding determinant $\Delta(j_1, \ldots, \hat{j}_s, \ldots, j_{t+1})$ is not zero. Hence the above equation is not identically zero and defines a hyperplane $\mathcal{H}_I$ in $\mathbb{F}^n$ with equation $f_I(X_1, \ldots, X_n) = 0$ for every basis I of $\tau(M)$. Consider the product

$$f(X_1, \ldots, X_n) = \prod_{I \text{ basis of } M} f_I(X_1, \ldots, X_n).$$

So, $f(X_1, \dots, X_n)$ is a nonzero polynomial. If $\mathbb{F}$ is infinite, then this polynomial is not everywhere zero on $\mathbb{F}^n$ by [69, V §4 Corollary 3]. Therefore there exists an element $\mathbf{x} \in \mathbb{F}^n$ such that $f(x_1, \dots, x_n)$ is not zero.
If $\mathbb{F}$ is finite, then $\mathbb{F} = \mathbb{F}_q$ and we assumed $m \geq \lceil \log_q(\binom{n}{k-1}) \rceil + 1$. So $q^m > \binom{n}{k-1}$. Hence

$$(q^m)^n > \binom{n}{k-1}(q^m)^{n-1}.$$

The number of basis of $\tau(M)$ is at most $\binom{n}{k-1}$. Therefore, $\mathbb{F}_{q^m}^n$ has more elements than the union of all hyperplanes $\mathcal{H}_I$ with I a basis of $\tau(M)$. So there exists an element $\mathbf{x} \in \mathbb{F}_{q^m}^n$ that does not lie in this union.
In both cases an n-tuple $\mathbf{x}$ is found, possibly over an extension of $\mathbb{F}$ such that $f_I(x_1, \dots, x_n)$ is not zero for every basis I of $\tau(M)$. Let $\tilde{H}$ be the $(t+1) \times n$ matrix obtained by adding to H the row $\mathbf{x}$. Then for every basis I of $\tau(M)$ the columns of $\tilde{H}$ enumerated by the complement of I are independent, because the determinant of the corresponding square matrix of size $t+1$ is equal to $f_I(\mathbf{x}) \neq 0$.
The conclusion is that the null space of $\tilde{H}$ is a subspace of C of dimension $k-1$ that represents $\tau(M)$. □

13.3 Truncation and the coboundary polynomial

For polynomials associated with matroids and geometric lattices, one might ask if we can find the polynomial of their truncation from the polynomial of the original structure. The answer is positive for the characteristic polynomial, see [26, p. 149]. For the rank generating function $R_M(X, Y)$ of a matroid we have the following theorem, proved by Britz [21, Prop. 15].

Theorem 13.8 (Truncation formula). *Let M be a matroid. Then*

$$X \cdot R_{\tau(M)}(X, Y) = R_M(X, Y) + (XY - 1) \cdot R_M(0, Y).$$

In this section, we will consider the same question for the coboundary polynomial.

Theorem 13.9. *Let L be a geometric lattice of rank $r \geq 3$. Then*

$$U \cdot \chi_{\tau(L)}(S, U) = \chi_L(S, U) + (U - 1) \cdot \chi_L(S, 0).$$

Proof. The identity is a direct consequence of Theorem 13.8 using the relation between the rank generating and coboundary polynomial from Theorem 10.4. □

Since the coboundary polynomial is equivalent to the rank generating function, it is clear that a truncation formula for the coboundary polynomial should exist. However, the definition of the coboundary polynomial makes it possible to find a more general idea behind this truncation formula, that can also be applied to other polynomial invariants that are not equivalent to (or determined by) the rank generating function.

Theorem 13.10. *Let $f(S, U)$ be a polynomial invariant of a matroid, geometric lattice, or poset with rank function that has rank r and can be written as*

$$f(S, U) = \sum_{i=0}^{r} f_j(S) U^{r-j}.$$

Let f' be the corresponding polynomial invariant of the truncation of the matroid, geometric lattice, or poset with rank function. So, we can write

$$f'(S,U) = \sum_{i=0}^{r-1} f'_j(S) U^{r-1-j}.$$

If the coefficients $f_j(S)$ and $f'(S)$ are related via

$$\begin{cases} f'_j(S) &= f_j(S), & \text{for } j \leq r-2, \\ f'_j(S) &= f_j(S) + f_{j+1}(S), & \text{for } j = r-1. \end{cases}$$

then the following truncation formula holds:

$$U \cdot f'(S,U) = f(S,U) + (U-1) \cdot f(S,0).$$

PROOF. The proof is given by rewriting.

$$\begin{aligned} U \cdot f'(S,U) &= \sum_{i=0}^{r-1} f'_j(S) U^{r-j} \\ &= \sum_{i=0}^{r-2} f_j(S) U^{r-j} + U \cdot (f_{r-1}(S) + f_r(S)) \\ &= \sum_{i=0}^{r-1} f_j(S) U^{r-j} + U \cdot f_r(S) \\ &= \sum_{i=0}^{r} f_j(S) U^{r-j} - f_r(S) + U \cdot f_r(S) \\ &= f(S,U) + (U-1) \cdot f(S,0). \end{aligned}$$

□

We can use this formula to give a different proof of Theorem 13.9.

PROOF (THEOREM 13.9). We can not directly apply Theorem 13.10 to the coboundary polynomial: we will use the following reduced form, where we delete the highest degree terms in S. Let m be the number of atoms of L and let

$$\overline{\chi}_L(S,U) = \chi_L(S,U) - S^m = \sum_{j=0}^{r} \overline{\chi}_j(S) U^{r-j},$$

where

$$\overline{\chi}_j(S) = \sum_{\substack{a_L(x)=i \\ i<m}} \sum_{\substack{x \leq y \\ r_L(y)=j}} \mu_L(x,y)\, S^i.$$

Let the reduced coboundary polynomial of the truncated geometric lattice be given by

$$\overline{\chi}'(S,U) = \sum_{i=0}^{r-1} \overline{\chi}'_j(S) U^{r-1-j}.$$

We need to show the relations of Theorem 13.10. Note that if $r_L(x) \leq r-2$, then $r_L(x) = r_{\tau(L)}(x)$ and $a_L(x) = a_{\tau(L)}(x)$. Also, if $r(x), r(y) \leq r-2$, then $\mu_L(x,y) = \mu_{\tau(L)}(x,y)$. Therefore, $\overline{\chi}'_j(S) = \overline{\chi}_j(S)$ for $j \leq r-2$.
It is left to show that $\overline{\chi}_{r-1}(S) + \overline{\chi}_r(S) = \overline{\chi}'_{r-1}(S)$, that is,

$$\sum_{\substack{a_L(x)=i \\ i<m}} \sum_{\substack{x\leq y \\ r_L(y)=r-1}} \mu_L(x,y)\, S^i + \sum_{\substack{a_L(x)=i \\ i<m}} \mu_L(x,1_L)\, S^i = \sum_{\substack{a_{\tau(L)}(x)=i \\ i<m}} \mu_{\tau(L)}(x, y_{\tau(L)})\, S^i.$$

Since $a_L(x) < m$, we have $r_L(x) < r$ in every summation. We split into two parts. If $r_L(x) = r-1 = r_{\tau(L)}(x)$, then $a_{\tau(L)}(x) = m$, so the right hand side of the summation is 0. The left hand side of the summation is then equal to

$$\sum_{\substack{a_L(x)=i \\ i<m}} S^i\,(1-1) = 0,$$

so this cancels out. Now suppose $r_L(x) = r_{\tau(L)}(x) \leq r-2$. We can drop the first summation and the factor S^i, because they are the same on both sides. So, we need to show that

$$\sum_{\substack{x\leq y \\ r_L(y)=r-1}} \mu_L(x,y) + \mu_L(x,1_L) = \mu_{\tau(L)}(x, y_{\tau(L)}).$$

We will use the induction formula for the Möbius function: for $x < y$, it holds that

$$\sum_{x\leq z\leq y} \mu_L(x,z) = \sum_{x\leq z\leq y} \mu_L(z,y) = 0.$$

If we use this on the left hand side, we get

$$\begin{aligned}
\sum_{\substack{x\leq y \\ r_L(y)=r-1}} \mu_L(x,y) + \mu_L(x,1_L) &= \sum_{\substack{x\leq y \\ r_L(y)=r-1}} \mu_L(x,y) - \sum_{x\leq z<1_L} \mu_L(x,z) \\
&= -\sum_{\substack{x\leq z \\ r_L(z)\leq r-2}} \mu_L(x,z).
\end{aligned}$$

The right hand side is equal to

$$\begin{aligned}
\mu_{\tau(L)}(x, 1_{\tau(L)}) &= -\sum_{x\leq z<1_{\tau(L)}} \mu_{\tau(L)}(x,z) \\
&= -\sum_{\substack{x\leq z \\ r_{\tau(L)}(z)\leq r-2}} \mu_{\tau(L)}(x,z) \\
&= -\sum_{\substack{x\leq z \\ r_L(z)\leq r-2}} \mu_L(x,z)
\end{aligned}$$

We conclude that $\overline{\chi}_{r-1}(S) + \overline{\chi}_r(S) = \overline{\chi}'_{r-1}(S)$, so the reduced coboundary polynomial satisfies the conditions in Theorem 13.10 and therefore has a truncation formula. Since the term S^m that we omitted does not change under truncation, we get the truncation formula as is Theorem 13.9. □

Example 13.11. The uniform matroid $U_{n,r}$ has rank generating function

$$R_{U_{n,r}}(X,Y)=\sum_{i=0}^{r-1}\binom{n}{i}X^{r-i}+\sum_{i=r}^{n}\binom{n}{i}Y^{i-r},$$

as follows directly from the definitions. Since the coboundary polynomial is defined by the rank generating function (see Theorem 10.4), we can find the coboundary polynomial of the uniform geometric lattice:

$$\chi_{U_{n,r}}(S,U)=\sum_{i=0}^{r-1}\binom{n}{i}(S-1)^iU^{r-i}+\sum_{i=r}^{n}\binom{n}{i}(S-1)^i.$$

In this form many terms cancel each other. For example, $U_{7,3}$ has coboundary polynomial

$$\chi_{U_{7,3}}(S,U)=S^7+21S^2(U-1)+7S(U^2-6U+5)+(U^3-7U^2+21U-15).$$

In the form as above, it is straightforward to verify the truncation formula for the coboundary polynomial for arbitrary uniform geometric lattices. In case of the lattice $U_{7,3}$, its truncation $U_{7,2}$ has coboundary polynomial

$$\chi_{U_{7,2}}(S,U)=S^7+7S(U-1)+(U^2-7U+6).$$

13.4 Truncation and the Möbius polynomial

The combinatorial proof for the truncation formula in Theorem 13.9 is also applicable to other polynomials. In this section we treat the Möbius polynomial. We loosen to the case of posets with rank functions, so we can also address the lower truncation.

Theorem 13.12. *Let P be a poset with rank function of rank r. Then*

$$U\cdot\mu_{\tau_+(P)}(S,U)=\mu_P(S,U)+(U-1)\cdot\mu_P(S,0)+S^{r-1}U-S^rU.$$

Proof. Just as in the case of the coboundary polynomial, we will use a reduced form of the polynomial to work with. Let

$$\overline{\mu}_P(S,U)=\mu_P(S,U)-S^r=\sum_{j=0}^{r}\overline{\mu}_j(S)U^{r-j},$$

where

$$\overline{\mu}_j(S)=\sum_{\substack{r_P(x)=i\\ i<r}}\ \sum_{\substack{x\leq y\\ r_P(y)=j}}\mu_P(x,y)\,S^i.$$

Note that the sets $\{x\in L:a_L(x)<m\}$ and $\{x\in L:r_L(x)<r\}$ are the same, so the proof that the reduced Möbius polynomial obeys the constrains in Theorem 13.10 is exactly the same as in the case of the reduced coboundary polynomial. Hence the reduced Möbius polynomial has a truncation formula as in Theorem 13.10. To switch to the non-reduced Möbius polynomial, $-US^{r-1}$ gets added at the left hand side of the formula, and $-S^r-(U-1)S^r$ at the right hand side. This gives the term $+S^{r-1}U-S^rU$ in the formula. □

Example 13.13. We consider again the uniform geometric lattice $L = U_{n,r}$. For all elements $x \in U_{n,r}$ with $r_L(x) < r(L)$, we have that $a_L(x) = r_L(x)$. Therefore the coboundary polynomial and the Möbius polynomial differ only in the leading term: for the coboundary polynomial this is S^n, while for the Möbius polynomial it is $S^{r(L)}$. For example, the Möbius polynomial of the geometric lattice $U_{7,3}$ is equal to

$$\mu_{U_{7,3}}(S,U) = S^3 + 21S^2(U-1) + 7S(U^2 - 6U + 5) + (U^3 - 7U^2 + 21U - 15).$$

The Möbius polynomial of its truncation $U_{7,2}$ is equal to

$$\mu_{U_{7,2}}(S,U) = S^2 + 7S(U-1) + (U^2 - 7U + 6).$$

Comparing with Example 13.11, we see why the term $S^{r-1}U - S^rU$ is needed in the truncation formula of the Möbius polynomial.
We would like to mention that it is possible to give a general formula for the Möbius polynomial of a uniform geometric lattice, see Example 10.12. Checking the truncation formula directly in the case of a general uniform geometric lattice is therefore possible, but we leave the rather lengthy calculation to the reader.

For posets, we can find a similar truncation formula for the lower truncation.

Theorem 13.14. *Let P be a poset with rank function of rank r. Then*

$$S \cdot \mu_{\tau_-(P)}(S,U) = \mu_P(S,U) + (S-1) \cdot \mu_P(0,U) + SU^{r-1} - SU^r.$$

Proof. We prove this formula by using the inverse poset, see Definition 9.9. The Möbius polynomial of the inverse poset $i(P)$ is found by interchanging the variables in the Möbius polynomial of the original poset P:

$$\begin{aligned}
\mu_{i(P)}(S,U) &= \sum_{x\in i(P)} \sum_{y \in i(P)} \mu_{i(P)}(x,y)\, S^{r_{i(P)}(x)} U^{r(i(P)) - r_{i(P)}(y)} \\
&= \sum_{x\in P} \sum_{y\in P} \mu_P(y,x)\, S^{r - r_P(x)} U^{r-(r-r_P(y))} \\
&= \sum_{x\in P} \sum_{y\in P} \mu_P(x,y)\, U^{r_P(x)} S^{r - r_P(y)} \\
&= \mu_P(U,S).
\end{aligned}$$

This makes it possible to derive the formula for lower truncation directly from the formula for upper truncation. We start with the formula for upper truncation in Theorem 13.12:

$$U \cdot \mu_{\tau_+(P)}(S,U) = \mu_P(S,U) + (U-1) \cdot \mu_P(S,0) + S^{r-1}U - S^rU.$$

For the inverse of P, the same formula holds:

$$U \cdot \mu_{\tau_+(i(P))}(S,U) = \mu_{i(P)}(S,U) + (U-1) \cdot \mu_{i(P)}(S,0) + S^{r-1}U - S^rU.$$

Now we use that $\tau_+(i(P)) = i(\tau_-(P))$ and $\mu_{i(P)}(S,U) = \mu_P(U,S)$:

$$U \cdot \mu_{\tau_-(P)}(U,S) = \mu_P(U,S) + (U-1) \cdot \mu_P(0,S) + S^{r-1}U - S^rU.$$

Interchanging S and U gives the formula for lower truncation. □

13.5 Truncation and the spectrum polynomial

We discussed the spectrum polynomial in Chapter 12. By a slight change of variables, we get a polynomial on which we can apply the same technique as before to prove a truncation formula.

DEFINITION 13.15. Let M be a matroid and $L = L(M)$ its associated geometric lattice. Let

$$\nu_M(x,y) = (-1)^{r_M(x)}\mu_L(x,y)\,|\tilde{\chi}(IN(x))|$$

and define the *reciprocal alternating spectrum polynomial* of M by

$$\mathrm{Rasp}_M(S,U) = \sum_{x\in L}\ \sum_{x\le y\in L} \nu_M(x,y)\,S^{|x|}U^{r(L)-r_L(y)}.$$

Note the similarity to the definition of the coboundary polynomial. The polynomial $\mathrm{Rasp}_M(S,U)$ is equivalent to the spectrum polynomial.

THEOREM 13.16. *The polynomial* $\mathrm{Rasp}_M(S,U)$ *is the reciprocal alternating polynomial of* $\mathrm{Spec}_M(S,U)$ *in* U*:*

$$\mathrm{Rasp}_M(S,U) = U^{r(M)}\,\mathrm{Spec}_M(S,-\frac{1}{U}).$$

PROOF. Let $L = L(M)$. Using the fact that $|\mu(x,y)| = (-1)^{r(y)-r(x)}\mu(x,y)$ and rewriting gives:

$$\begin{aligned}
&U^{r(M)}\,\mathrm{Spec}_M(S,-\frac{1}{U})\\
&= U^{r(M)}\sum_{x\in L}\ \sum_{x\le y\in L} |\mu_L(x,y)|\,|\tilde{\chi}(IN(x))|\,S^{|x|}(-U^{-1})^{r(y)}\\
&= U^{r(M)}\sum_{x\in L}\ \sum_{x\le y\in L} (-1)^{r(y)-r(x)}\mu_L(x,y)\,|\tilde{\chi}(IN(x))|\,S^{|x|}(-U^{-1})^{r(y)}\\
&= U^{r(M)}\sum_{x\in L}\ \sum_{x\le y\in L} (-1)^{r(x)}\mu_L(x,y)\,|\tilde{\chi}(IN(x))|\,S^{|x|}(U^{-1})^{r(y)}\\
&= \sum_{x\in L}\ \sum_{x\le y\in L} \nu_M(x,y)\,S^{|x|}U^{r(M)-r(y)}\\
&= \mathrm{Rasp}_M(S,U).
\end{aligned}$$

We omit the subscripts L and M by the rank function to emphasize the cryptomorphism between $L(M)$ and M. □

We need the following computational lemmas about Rasp_M and ν_M.

LEMMA 13.17. *Let* $\mathcal{B}_M$ *be the collection of all bases of a matroid* M*. Then*

$$\mathrm{Rasp}_M(1,0) = (-1)^{r(M)}|\mathcal{B}_M|.$$

PROOF. Let $\mathcal{I}$ be the set of independent sets of M, and let $L = L(M)$.

$$\begin{aligned}
\mathrm{Rasp}_M(1,0) &= \sum_{x\in L} \nu_M(x, 1_L) \\
&= \sum_{x\in L} (-1)^{r(x)} \mu_L(x, 1_L) \sum_{\substack{I\subseteq x \\ I\in\mathcal{I}}} (-1)^{r(x)-|I|} \\
&= \sum_{I\in\mathcal{I}} (-1)^{-|I|} \sum_{\bar{I}\leq x\leq 1_L} \mu_L(x, 1_L) \\
&= \sum_{B\in\mathcal{B}} (-1)^{-r(M)} \\
&= (-1)^{-r(M)} |\mathcal{B}_M|.
\end{aligned}$$

□

LEMMA 13.18. *Let M be a matroid and $x < y$ elements of $L = L(M)$. Then $\nu_M(x,y)$ has the following induction formula:*

$$\sum_{x\leq z\leq y} \nu_M(x,z) = \sum_{x\leq z\leq y} \nu_M(z,y) = 0.$$

PROOF. For $x < y$ we have

$$\begin{aligned}
\nu_M(x,y) &= (-1)^{r_M(x)} |\tilde{\chi}(IN(x))|\, \mu_L(x,y) \\
&= (-1)^{r_M(x)} |\tilde{\chi}(IN(x))| \sum_{x\leq z<y} -\mu_L(x,z) \\
&= -\sum_{x\leq z<y} \nu_M(x,z).
\end{aligned}$$

This implies the given induction fomula. □

We can now prove a truncation formula for the polynomial $\mathrm{Rasp}_M(S,U)$.

THEOREM 13.19. *Let M be a matroid of rank r on a set of m elements. Then*

$$U \cdot \mathrm{Rasp}_{\tau(M)}(S,U) = \mathrm{Rasp}_M(S,U) + (U-1)\cdot \mathrm{Rasp}_M(S,0) - S^m U \cdot \mathrm{Rasp}_M(1,0).$$

PROOF. Just as in the previous cases, we will use a reduced form of the polynomial to work with. Let

$$\overline{\mathrm{Rasp}}_M(S,U) = \mathrm{Rasp}_M(S,U) - \nu_M(1_M,1_M)S^m = \sum_{j=0}^{r} \overline{\mathrm{Rasp}}_j(S) U^{r-j},$$

where

$$\overline{\mathrm{Rasp}}_j(S) = \sum_{\substack{|x|=i \\ i<m}} \sum_{\substack{x\leq y \\ r_M(y)=j}} \nu_M(x,y) S^i.$$

Note that the sets $\{x \in M : |x| < m\}$ and $\{x \in M : r_M(x) < r\}$ are the same and that Lemma 13.18 gives the same induction formula for $\nu(x,y)$ as we have for $\mu(x,y)$ so again we can copy the previous proofs to show that the reduced Rasp polynomial obeys the constrains in Theorem 13.10. Hence the reduced Rasp polynomial has a truncation formula as in Theorem 13.10. To switch to the non-reduced Rasp polynomial, $-\nu_{\tau(M)}(1_{\tau(M)}, 1_{\tau(M)})S^m U$ gets added at the left hand side of the formula, and $-\nu_M(1_M, 1_M)S^m - (U-1)\nu_M(1_M, 1_M)$ at the right hand side. In total, we have to add $-S^m U$ times the following:

$$\begin{aligned}
&\nu_M(1_M, 1_M) - \nu_{\tau(M)}(1_{\tau(M)}, 1_{\tau(M)})\\
&= (-1)^r \cdot 1 \cdot \sum_{I \in \mathcal{I}_M} (-1)^{r-|I|} - (-1)^{r-1} \cdot 1 \cdot \sum_{I \in \mathcal{I}_{\tau(M)}} (-1)^{r-1-|I|}\\
&= (-1)^r \left(\sum_{I \in \mathcal{I}_M \setminus \mathcal{B}_M} (-1)^{r-|I|} + \sum_{I \in \mathcal{B}_M} (-1)^{r-r} + \sum_{I \in \mathcal{I}_M \setminus \mathcal{B}_M} (-1)^{r-1-|I|} \right)\\
&= (-1)^r \sum_{I \in \mathcal{B}_M} 1\\
&= (-1)^r |\mathcal{B}_M|.
\end{aligned}$$

Combining with Lemma 13.17, the theorem follows. □

The truncation formula for $\mathrm{Rasp}_M(S,U)$ also makes it possible to determine the spectrum polynomial of a truncated matroid from the spectrum polynomial of the matroid itself. However, if we try to apply Theorem 13.16 directly to the truncation formula for $\mathrm{Rasp}_M(S,U)$, we run into trouble with the terms that have $U = 0$. To avoid this, notice that the term $\mathrm{Rasp}_M(S,0)$ actually means "write $\mathrm{Rasp}_M(S,U)$ as a polynomial in U and take the coefficient of U^0". In terms of the spectrum polynomial, this is "write $\mathrm{Spec}_M(S,U)$ as a polynomial in U, take the coefficient of $U^{r(M)}$ and multiply by $(-1)^{r(M)}$". This motivates the following definition.

Definition 13.20. The polynomials $S_i(S)$ are the coefficients of the spectrum polynomial, written as a polynomial in U:

$$\mathrm{Spec}_M(S,U) = \sum_{i=0}^{r(M)} S_i(S)\, U^i.$$

From this definition, it follows that we can write

$$\mathrm{Rasp}_M(S,U) = \sum_{i=0}^{r(M)} (-1)^i S_i(S)\, U^{r(M)-i}.$$

We use this to prove the truncation formula for the spectrum polynomial.

Theorem 13.21. *Let M be a matroid of rank r on a set of m elements. Then*

$$\mathrm{Spec}_{\tau(M)}(S,U) = \mathrm{Spec}_M(S,U) - U^{r-1}(U+1) \cdot S_r(S) + S^m U^{r-1} \cdot S_r(1).$$

PROOF. The truncation formula for $\mathrm{Rasp}_M(S,U)$ can be written as

$$U \cdot \mathrm{Rasp}_{\tau(M)}(S,U) = \mathrm{Rasp}_M(S,U) + (-1)^r(U-1)\cdot S_r(S) - (-1)^r S^m U \cdot S_r(1).$$

Using the equivalence in Theorem 13.16, we get

$$U \cdot U^{r-1} \cdot \mathrm{Spec}_{\tau(M)}(-\frac{1}{U},S) = U^r \cdot \mathrm{Spec}_M(-\frac{1}{U},S) + (-1)^r(U-1)\cdot S_r(S) - (-1)^r S^m U \cdot S_r(1).$$

Applying the transformation $U \to -\frac{1}{U}$ and multiplying by $(-U)^r$ gives the desired truncation formula for the spectrum polynomial. □

EXAMPLE 13.22. In Chapter 12, we calculated the spectrum polynomial of the uniform matroid. It is not difficult to see that this polynomial obeys the truncation formula for the spectrum polynomial. For example, we have

$$\begin{aligned} \mathrm{Rasp}_{U_{3,7}}(S,U) &= U^3 - 7U^2 + 21U - 15 - 20S^7 \\ \mathrm{Spec}_{U_{3,7}}(S,U) &= 20U^3S^7 + 15U^3 + 21U^2 + 7U + 1 \end{aligned}$$

and for the truncation

$$\begin{aligned} \mathrm{Rasp}_{U_{2,7}}(S,U) &= U^2 - 7U + 6 + 15S^7 \\ \mathrm{Spec}_{U_{2,7}}(S,U) &= 15U^2S^7 + 6U^2 + 7U + 1. \end{aligned}$$

13.6 Applications and generalizations

There are several constructions on matroids closely related to the ordinary truncation, for example the previously mentioned Dilworth truncation, the principal truncation, and weak and strong maps, see [26, 35, 67, 68]. It would be interesting to see whether truncation-like formulas also exist for these constructions.

We showed that the truncation of a matroid M that is representable over a finite field is representable over a finite extension of the same finite field. We gave an upper bound for the extension degree that is needed. However, in practice it is possible that $\tau(M)$ is already representable over a much smaller extension field. We might be able to achieve better bounds if we use the extended weight enumerator. If M is representable over a finite field, then all codes associated to it have the same extended weight enumerator, which we denote by $W_M(X,Y,U)$. Using the relations with the rank generating function and the coboundary polynomial, we find that

$$U \cdot W_{\tau(M)}(X,Y,U) = W_M(X,Y,U) + (U-1)\cdot W_M(X,Y,0).$$

Thus we can determine the extended weight enumerator of the truncated matroid. If the truncated matroid is representable over a field of size q, the polynomial $W_{\tau(M)}(X,Y,q)$ should have only nonnegative coefficients. It is often not difficult to see for which values of q this happens, as we illustrate by an example.

Example 13.23. Let M be the matroid represented over $\mathbb{F}_q$ with $q > 2$ by

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & \alpha \end{pmatrix}.$$

The extended weight enumerator of this matroid is given by

$$X^7 + 2(U-1)X^4Y^3 + 3(U-1)X^3Y^4 + U(U-1)X^2Y^5 + (U-1)(U-2)(U-3)Y^7.$$

The extended weight enumerator of the truncated matroid is thus

$$W_{\tau(M)}(X,Y,U) = X^7 + (U-1)X^2Y^5 + 5(U-1)XY^6 + (U-1)(U-5)Y^7.$$

We see that if U is at least 5, then all coefficients are positive. Hence $\tau(M)$ is representable over $\mathbb{F}_5$, for example by

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 2 & 3 & 4 \end{pmatrix}.$$

If we represent M over $\mathbb{F}_3$, then the bound in Theorem 13.7 gives that $\tau(M)$ is representable over the field of size $3^4 = 81$. If we start with a field of larger size, the bound becomes even bigger.

The truncation formula for the Möbius polynomial gives relations between the Whitney numbers of a poset with rank function P and the Whitney numbers of its truncations $\tau_-(P)$ and $\tau_+(P)$. This gives an approach to a proof by induction of the several unimodal conjectures considering Whitney numbers, see Section 10.2.

We saw that the lower truncation of a geometric lattice does not need to be a geometric lattice. Also, the unimodal conjectures are not true for posets with rank function in general. So the challenge is to find a class of objects that is "in between" posets with rank function and geometric lattices: this class needs to be closed under lower truncation, while still the unimodal property holds. Also, for the induction to work, the smallest cases in this class need to be proved unimodal.

The spectrum polynomial is in general not determined by the rank generating function of a matroid. In order to find counterexamples for the implication in the other direction, we see from the truncation formulas for the coboundary and Rasp polynomial that it is sufficient to find a counterexample with respect to the one variable polynomials in S, setting $T = 0$.

14

Overview of polynomial relations

In this thesis we have established various links between polynomial invariants of codes, arrangements and matroids. In this chapter, we give an overview of the relations between these polynomials.

We started in Chapter 2 with the relation between the extended weight enumerator and the set of generalized weight enumerators. One may wonder if the method of generalizing and extending the weight enumerator can be continued, creating the generalized extended weight enumerator, in order to get a stronger invariant. The answer is no: the generalized extended weight enumerator can be defined, but does not contain more information than the two underlying polynomials. The original weight enumerator $W_C(X,Y)$ contains less information and therefore does not determine $W_C(X,Y,U)$ or $\{W_C^{(r)}(X,Y)\}_{r=0}^k$. See Simonis [85].

In Chapter 3 we studied two generalizations of the zeta polynomial. The relations are summarized in Figure 14.1. The generalized polynomials on the right represent the generalized polynomials for all dimensions $r=0,\dots,k$. The relations labeled with a D can be found in Duursma [39]. We see there are no arrows from the weight enumerator to the zeta polynomial: this is because the relation the other way around is not a linear transformation, like for example between the sets $A_w(U)$ and $B_t(U)$. However, we can link a normalized version of the weight enumerator to the zeta polynomial, see [37, 39].

$$\begin{tikzcd}
 & P_C(T,U) \arrow[r, leftrightarrow, "\text{D.}"] \arrow[dl, leftrightarrow, "\text{D.}"'] \arrow[d, "\text{Df.}3.1"] & P_C^{(r)}(T) \arrow[d, "\text{Th.}3.9"'] \arrow[dr, shift right, "\text{D.}"'] & \\
\{B_t(U)\}_{t=0}^n \arrow[r, shift left, "\text{Th.}2.15"] & W_C(X,Y,U) \arrow[l, shift left, "\text{Pr.}2.16"] \arrow[r, shift left, "\text{Th.}2.25"] & W_C^{(r)}(X,Y) \arrow[l, shift left, "\text{Th.}2.23"] \arrow[r, shift left, "\text{Pr.}2.10"] & \{B_t^{(r)}\}_{t=0}^n \arrow[l, shift left, "\text{Th.}2.11"] \arrow[ul, shift right, "\text{Th.}3.8"']
\end{tikzcd}$$

Figure 14.1: Relations between the weight enumerator and zeta polynomial

In Chapter 6 we investigated relations between the extended weight enumerator, the extended coset leader weight enumerator, the extended list weight enumerator and the same polynomials of the dual code. In Figure 14.2 we see an overview. The arrows ending in × mean that the polynomial at the start does not define the polynomial at the end point. If an arrow is labeled by a question mark, it means it is unknown if the polynomial at the start defines the polynomial at the end point. The figure is symmetric in the vertical axis because of duality.

$$\begin{tikzcd}
 & \alpha_C(X,Y,U) \arrow[r, dash, "\text{Ex.}6.13", "\times"{marking, very near start}, "\times"{marking, very near end}] \arrow[dl, shift left, "\text{Ex.}6.13"] \arrow[d, shift left, "\text{Ex.}6.13"] & \alpha_{C^\perp}(X,Y,U) \arrow[dr, shift left, "\text{Ex.}6.13"] \arrow[d, shift left, "\text{Ex.}6.13"] & \\
W_C(X,Y,U) \arrow[ur, dash, shift left, "\text{Rem.}6.3", "\times"{marking, very near end}] \arrow[dr, dash, shift left, "\text{Rem.}6.3", "\times"{marking, very near end}] \arrow[rrr, leftrightarrow, bend left=5, "\text{Th.}2.19"] & & & W_{C^\perp}(X,Y,U) \arrow[ul, dash, shift left, "\text{Rem.}6.3", "\times"{marking, very near end}] \arrow[dl, dash, shift left, "\text{Rem.}6.3", "\times"{marking, very near end}] \\
 & \lambda_C(X,Y,U) \arrow[ul, shift left, "?"] \arrow[u, shift left, "?"] \arrow[r, leftrightarrow, "?"] & \lambda_{C^\perp}(X,Y,U) \arrow[ur, shift left, "?"] \arrow[u, shift left, "?"] &
\end{tikzcd}$$

Figure 14.2: Relations between the extended weight enumerator and the extended list- and coset weight enumerator

We have established relations between the generalized weight enumerators for $0 \leq r \leq k$, the extended weight enumerator and the Tutte polynomial in Chapter 8. We summarize this in Figure 14.3. We see that the Tutte polynomial, the extended weight enumerator and the collection of generalized weight enumerators all contain the same amount of information about a code, because they completely define each other.

$$\begin{tikzcd}
 & W_C(X,Y,U) \arrow[dl, shift left, "\text{Th.}2.25"] \arrow[d, shift left, "\text{Th.}8.5"] \\
\{W_C^{(r)}(X,Y)\}_{r=0}^{k} \arrow[ur, shift left, "\text{Th.}2.23"] \arrow[r, leftrightarrow, "\text{Th.}8.6"] & t_C(X,Y) \arrow[u, shift left, "\text{Th.}8.4"]
\end{tikzcd}$$

Figure 14.3: Relations between the weight enumerator and Tutte polynomial

The polynomials $t_C(X,Y)$, $R_{M_C}(X,Y)$ and $\chi_C(S,U)$ determine each other on the class of projective codes by Theorem 10.4. This is summarized in Figure 14.4. The dotted arrows only apply if the matroid is simple or, equivalently, if the code is projective.

The polynomials $\chi_C(S,U)$ and $\mu_C(S,U)$ do not determine each other in general by Examples 10.33 and 10.35. However, in Chapter 11 we saw that sometimes the pair $\mu_M(S,U)$ and $\mu_{M^*}(S,U)$ does define $\chi_M(S,U)$.

$$\begin{tikzcd}
W_C(X,Y,U) \arrow[rr, shift left, "\text{Th.}8.5"] \arrow[dd, dotted, shift left, "\text{Th.}10.6"] & & t_C(X,Y) \arrow[ll, shift left, "\text{Th.}8.4"] \arrow[dl, shift left, "\text{Df.}8.1"] \arrow[dd, dotted, shift left] \\
 & R_{M_C}(X,Y) \arrow[ur, shift left, "\text{Df.}8.1"] \arrow[dl, dotted, shift left, "\text{Th.}10.4"] & \\
\chi_C(S,U) \arrow[rr, shift left, "\text{Co.}10.5"] \arrow[uu, dotted, shift left, "\text{Th.}10.6"] \arrow[ur, dotted, shift left, "\text{Th.}10.4"] & & t_{\overline{C}}(X,Y) \arrow[ll, shift left, "\text{Co.}10.5"] \arrow[uu, dotted, shift left]
\end{tikzcd}$$

FIGURE 14.4: Relations between the weight enumerator, characteristic and Tutte polynomial

Bibliography

[1] M. Aigner. *Combinatorial theory.* Springer, New York, 1979.

[2] M. Aigner. Whitney numbers. In N. White, editor, *Combinatorial geometries*, pages 139–160. Cambridge University Press, Cambridge, 1987.

[3] F. Ardila. Computing the Tutte polynomial of a hyperplane arrangement. *Pacific J. Math.*, 230:1–26, 2007.

[4] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Trans. Inform. Theory*, 44:2010–2017, 1998.

[5] E. F. Assmus, Jr. On the Reed-Muller codes. *Discrete Math.*, 106/107:25–33, 1992.

[6] E. F. Assmus, Jr. and J. D. Key. *Designs and their codes.* Cambridge University Press, 1992.

[7] C. A. Athanasiadis. Characteristic polynomials of subspace arrangements and finite fields. *Adv. Math.*, 122:193–233, 1996.

[8] T. Baicheva, I. Bouyukliev, S. Dodunekov, and W. Willems. Teaching linear codes. In *International Congress MASSEE*, 2003.

[9] A. Barg. The matroid of supports of a linear code. *AAECC*, 8:165–172, 1997.

[10] A. Barg. Complexity issues in coding theory. In V. S. Pless, W. Huffman, and R. Brualdi, editors, *Handbook of coding theory*, volume 1, pages 649–754. North-Holland, Amsterdam, 1998.

[11] E. R. Berlekamp. *Algebraic coding theory.* Aegon Park Press, Laguna Hills, 1984.

[12] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Inform. Theory*, 24:384–386, 1978.

[13] G. Birkhoff. Abstract linear dependence and lattices. *Amer. J. Math.*, 56:800–804, 1935.

[14] A. Björner. The homology and shallability of matroids and geometric lattices. In N. White, editor, *Matroid applications*, pages 226–280. Cambridge University Press, Cambridge, 1992.

[15] A. Björner and T. Ekedahl. Subarrangments over finite fields: Chomological and enumerative aspects. *Adv. Math.*, 129:159–187, 1997.

[16] R. E. Blahut. *Theory and practice of error control codes.* Addison-Wesley, Reading, 1983.

[17] D. Britz, T. Britz, K. Shiromoto, and H. Sørensen. The higher weight enumerators of the doubly-even, self-dual $[48, 24, 12]$ code. *IEEE Trans. Inform. Theory*, 53: 2567–2571, 2007.

[18] T. Britz. *Relations, matroids and codes.* PhD thesis, Univ. Aarhus, 2002.

[19] T. Britz. MacWilliams identities and matroid polynomials. *Electron. J. Combin.*, 9, 2002.

[20] T. Britz. Extensions of the critical theorem. *Discrete Math.*, 305:55–73, 2005.

[21] T. Britz. Higher support matroids. *Discrete Math.*, 307:2300–2308, 2007.

[22] T. Britz and C. G. Rutherford. Covering radii are not matroid invariants. *Discrete Math.*, 296:117–120, 2005.

[23] T. Britz and K. Shiromoto. A MacWillimas type identity for matroids. *Discrete Math.*, 308:4551–4559, 2008.

[24] T. H. Brylawski. The Tutte polynomial. I. General theory. In *C.I.M.E. Summer Schools*, 1980.

[25] T. H. Brylawski. The affine dimension of the space of intersection matrices. *Rend. Mat. (6)*, 13(1):59–68, 1980.

[26] T. H. Brylawski. Constructions. In N. White, editor, *Theory of matroids*, pages 127–223. Cambridge University Press, Cambridge, 1986.

[27] T. H. Brylawski and J. G. Oxley. The Tutte polynomial and its applications. In N. White, editor, *Matroid Applications*, pages 173–226. Cambridge University Press, Cambridge, 1992.

[28] R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bull. Lond. Math. Soc.*, 18:97–122, 1986.

[29] P. Cartier. Les arrangements d'hyperplans: un chapitre de géométrie combinatoire. *Seminaire N. Bourbaki*, 561:1–22, 1981.

[30] H. Crapo. Möbius inversion in lattices. *Arch. Math.*, 19:595–607, 1968.

[31] H. Crapo. The Tutte polynomial. *Aequationes Math.*, 3:211–229, 1969.

[32] H. Crapo and G. C. Rota. *On the foundations of combinatorial theory: Combinatorial geometries.* MIT Press, Cambridge MA, 1970.

[33] M. A. de Boer. Almost MDS codes. *Des. Codes Cryptogr.*, 9:143–155, 1996.

[34] G. Denham. The combinatorial Laplacian of the Tutte complex. *J. Algebra*, 242: 160–175, 2001.

[35] R. P. Dilworth. Dependence relations in a semimodular lattice. *Duke Math. J.*, 11: 575–587, 1944.

[36] I. M. Duursma. Weight distributions of geometric Goppa codes. *Trans. Amer. Math. Soc.*, 351:3609–3639, 1999.

[37] I. M. Duursma. From weight enumerators to zeta functions. *Discrete Appl. Math.*, 111:55–73, 2001.

[38] I. M. Duursma. Extremal weight enumerators and ultraspherical polynomials. *Discrete Math.*, 268:103–127, 2003.

[39] I. M. Duursma. Combinatorics of the two-variable zeta function. In G. L. Mullen, A. Poli, and H. Stichtenoth, editors, *International Conference on Finite Fields and Applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, pages 109–136. Springer, 2003.

[40] G. Etienne and M. Las Vergnas. External and internal elements of a matroid basis. *Discrete Math.*, 179:111–119, 1995.

[41] A. Faldum and W. Willems. Codes of small defect. *Des. Codes Cryptogr.*, 10(3): 341–350, 1997.

[42] G. D. Forney. Dimension/length profiles and trellis complexity of linear block codes. *IEEE Trans. Inform. Theory*, 40:1741–1752, 1994.

[43] C. Greene. Weight enumeration and the geometry of linear codes. *Stud. Appl. Math.*, 55:119–128, 1976.

[44] C. Greene and T. Zaslavsky. On the interpretation of Whitney numbers through arrangements of hyperplanes, zonotopes, non-Radon partitions and orientations of graphs. *Trans. Amer. Math. Soc.*, 280:97–126, 1983.

[45] R. W. Hamming. Error detecting and error correcting codes. *Bell System Tech. J.*, 29:147–160, 1950.

[46] P. Heijnen and R. Pellikaan. Generalized Hamming weights of q-ary Reed-Muller codes. *IEEE Trans. Inform. Theory*, 44:181–196, 1998.

[47] T. Helleseth. The weight distribution of the coset leaders of some classes of codes with related parity-check matrices. *Discrete Math.*, 28:161–171, 1979.

[48] T. Helleseth and T. Kløve. The Newton radius of codes. *IEEE Trans. Inform. Theory*, 43(6):1820–1831, 1997.

[49] T. Helleseth, T. Kløve, and J. Mykkeltveit. The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/n)$. *Discrete Math.*, 18:179–211, 1977.

[50] D. Jungnickel and V. D. Tonchev. A Hamada type characterization of the classical geometric designs. *Des. Codes Cryptogr.*, DOI: 10.1007/s10623-011-9580-3, 2011.

[51] D. Jungnickel and V. D. Tonchev. New invariants for incidence structures. *Des. Codes Cryptogr.*, DOI: 10.1007/s10623-012-9636-z, 2012.

[52] R. P. M. J. Jurrius. Classifying polynomials of linear codes. Master's thesis, Leiden University, 2008.

[53] R. P. M. J. Jurrius. Weight enumeration of codes from finite spaces. *Des. Codes Cryptogr.*, 63(3):321–330, 2012.

[54] R. P. M. J. Jurrius. Relations between Möbius and coboundary polynomials. *Math. Comput. Sci.*, DOI: 10.1007/s11786-012-0117-6, 2012. To appear.

[55] R. P. M. J. Jurrius and R. Pellikaan. Extended and generalized weight enumerators. In T. Helleseth and Ø. Ytrehus, editors, *Proc. Int. Workshop on Coding and Cryptography WCC-2009*, pages 76–91. Selmer Center, Bergen, 2009.

[56] R. P. M. J. Jurrius and R. Pellikaan. The extended coset leader weight enumerator. In F. Willems and T. Tjalkens, editors, *Proc. 30th Symposium 2009 on Information Theory in the Benelux*, pages 217–224, 2009.

[57] R. P. M. J. Jurrius and R. Pellikaan. Truncation formulas for invariant polynomials of matroids and geometric lattices. *Math. Comput. Sci.*, 2011. To appear.

[58] R. P. M. J. Jurrius and R. Pellikaan. *Codes, arrangements and matroids.* Ser. Coding Theory Cryptol. World Scientific Publishing, To appear, 2012.

[59] J. Justesen and T. Høholdt. Bounds on list decoding of MDS codes. *IEEE Trans. Inform. Theory*, 47:1604–1609, 2001.

[60] G. L. Katsman and M. A. Tsfasman. Spectra of algebraic-geometric codes. *Probl. Inf. Transm.*, 23:19–34, 1987.

[61] T. Kløve. The weight distribution of linear codes over GF(q^l) having generator matrix over GF(q). *Discrete Math.*, 23:159–168, 1978.

[62] T. Kløve. Support weight distribution of linear codes. *Discrete Math.*, 106/107: 311–316, 1992.

[63] T. Kløve. *Codes for error detection*, volume 2 of *Series on Coding Theory and Cryptology.* World Scientific Publishing, 2007.

[64] W. Kook. Recurrence relations for the spectrum polynomial of a matroid. *Discrete Applied Mathematics*, 143:312–317, 2004.

[65] W. Kook, V. Reiner, and D. Stanton. Combinatorial Laplacians of matroid complexes. *J. Amer. Math. Soc.*, 13:129–148, 2000.

[66] J. P. S. Kung. *A source book in matroid theory.* Birkhäuser, Boston, 1986.

[67] J. P. S. Kung. Strong maps. In N. White, editor, *Theory of matroids*, pages 224–253. Cambridge University Press, Cambridge, 1986.

[68] J. P. S. Kung and H. Q. Nguyen. Weak maps. In N. White, editor, *Theory of matroids*, pages 254–271. Cambridge University Press, Cambridge, 1986.

[69] S. Lang. *Algebra.* Addison-Wesley, Reading, 1965.

[70] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes.* North-Holland Mathematical Library, Amsterdam, 1977.

[71] J. H. Mason. Matroids as the study of geometrical configurations. In M. Aigner, editor, *Higher combinatorics*, pages 133–176. Reidel Publ. Comp., Dordrecht, 1977.

[72] J. L. Massey. Minimal codewords and secret sharing. In *Proc. Sixth Joint Swedish-Russian Workshop on Information Theory, Molle, Sweden*, pages 276–279, 1993.

[73] E. G. Mphako. Tutte polynomials of perfect matroid designs. *Combin. Probab. Comput.*, 9:363–367, 2000.

[74] M. Munuera. Steganography and error-correcting codes. *Signal Processing*, 87(6): 1528–1533, 2007.

[75] M. Munuera. *Steganography from a coding theory point of view.* Series on Coding Theory and Cryptology. World Scientific Publishing, To appear, 2012.

[76] P. Orlik and H. Terao. *Arrangements of hyperplanes*, volume 300. Springer-Verlag, Berlin, 1992.

[77] J. G. Oxley. *Matroid theory.* Oxford University Press, Oxford, second edition, 2011.

[78] L. H. Ozarev and A. D. Wyner. Wire-tap channel II. *AT&T Bell Labs Tech. J.*, 63:2135–2157, 1984.

[79] R. Pellikaan. On the existence of error-correcting pairs. *J. Statist. Plann. Inference*, 51:229–242, 1996.

[80] R. C. Read. An introduction to chromatic polynomials. *J. Combin. Theory Ser. A*, 4:52–71, 1968.

[81] G. C. Rota. On the foundations of combinatorial theory I: Theory of Möbius functions. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 2:340–368, 1964.

[82] G. C. Rota. Combinatorial theory, old and new. In *Proc. Int. Congress Math. 1970 (Nice)*, volume 3, pages 229–233, Paris, 1971. Gauthier-Villars.

[83] C. G. Rutherford. *Matroids, codes and their polynomial links.* PhD thesis, Queen Mary University of London, 2001.

[84] A. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27: 379–423 and 623–656, 1948.

[85] J. Simonis. The effective length of subcodes. *AAECC*, 5:371–377, 1993.

[86] A. N. Skorobogatov. Linear codes, strata of Grassmannians, and the problems of Segre. In H. Stichtenoth and M. A. Tsfasman, editors, *Coding Theory and Algebraic Geometry*, volume 1518 of *Lecture Notes in Math.*, pages 210–223. Springer-Verlag, Berlin, 1992.

[87] R. P. Stanley. *Enumerative combinatorics*, volume 1. Cambridge University Press, Cambridge, 1997.

[88] R. P. Stanley. An introduction to hyperplane arrangements. In *Geometric combinatorics*, number 13 in IAS/Park City Math. Ser., pages 389–496. Amer. Math. Soc., Providence, RI, 2007.

[89] D. R. Stinson. *Cryptography, theory and practice.* CRC Press, Boca Raton, 1995.

[90] M. Sudan. Decoding of Reed-Solomon codes beyond the error-correction bound. *J. Complexity*, 13:180–193, 1997.

[91] V. D. Tonchev. Linear perfect codes and a characterization of the classical designs. *Des. Codes Cryptogr.*, 17:121–128, 1999.

[92] M. A. Tsfasman and S. G. Vlădut. *Algebraic-geometric codes.* Kluwer Academic Publishers, Dordrecht, 1991.

[93] M. A. Tsfasman and S. G. Vlădut. Geometric approach to higher weights. *IEEE Trans. Inform. Theory*, 41:1564–1588, 1995.

[94] W. T. Tutte. A ring in graph theory. *Proc. Amer. Math. Soc.*, 43:26–40, 1947.

[95] W. T. Tutte. A contribution to the theory of chromatic polynomials. *Canad. J. Math.*, 6:80–91, 1954.

[96] W. T. Tutte. Lectures on matroids. *Journal of Research of the National Bureau of Standards, Sect. B*, 69:1–47, 1965.

[97] B. L. van der Waerden. *Modern Algebra*, volume 1. Springer Verlag, Berlin, second edition, 1937.

[98] J. H. van Lint. *Introduction to coding theory*, volume 86 of *Graduate Texts in Math.* Springer, Berlin, third edition, 1999.

[99] J. H. van Lint and R. M. Wilson. *A course in combinatorics.* Cambridge University Press, Cambridge, 1992.

[100] A. Vardy. The intractability of computing the minimum distance of a code. *IEEE Trans. Inform. Theory*, 43:1757–1766, 1997.

[101] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37:1412–1418, 1991.

[102] D. J. A. Welsh. Combinatorial problems in matroid theory. In D. Welsh, editor, *Combinatorial mathematics and its applications*, pages 291–306. Academic Press, London, 1972.

[103] D. J. A. Welsh. *Matroid theory.* Academic Press, London, 1976.

[104] D. J. A. Welsh. Matroids: Fundamental concepts. In R. L. Graham, M. Grötschel, and L. Lovász, editors, *Handbook of combinatorics*, volume 1, pages 483–526. Elsevier Scientific Publishers, Amsterdam, 1995.

[105] N. White. *Theory of matroids*, volume 26 of *Encyclopedia Math. Appl.* Cambridge University Press, Cambridge, 1986.

[106] N. White. *Matroid applications*, volume 40 of *Encyclopedia Math. Appl.* Cambridge University Press, Cambridge, 1992.

[107] H. Whitney. On the abstract properties of linear dependence. *Amer. J. Math.*, 57: 509–533, 1935.

[108] G. Whittle. A charactrization of the matroids representable over GF(3) and the rationals. *J. Combin. Theory Ser. B*, 65:222–261, 1995.

[109] G. Whittle. On matroids representable over GF(3) and other fields. *Trans. Amer. Math. Soc.*, 349:579–603, 1997.

[110] T. Zaslavsky. *Facing up to arrangements: Face-count formulas for partitions of space by hyperplanes*, volume 1. Amer. Math. Soc., Providence, RI, 1975.

[111] T. Zaslavsky. Signed graph colouring. *Discrete Math.*, 39:215–228, 1982.

Notations

Part I: Codes

A_w	number of codewords of weight w
$A_{C\otimes\mathbb{F}_{q^m},w}$	number of codewords in $C\otimes\mathbb{F}_{q^m}$ of weight w
$A_w^{(r)}$	number of subcodes of dimension r and weight w
$A_w(U)$	coefficient of $X^{n-w}Y^w$ in the extended weight enumerator
$b_i^{(r)}$	generalized binomial moment
$B_J^{(r)}$	number of r-dimensional subspaces of $C(J)$
$B_J(U)$	$U^{l(J)}-1$
$B_t^{(r)}$	sum of all $B_J^{(r)}$ with $\|J\|=t$
$B_t(U)$	sum of all $B_J(U)$ with $\|J\|=t$
$\mathbf{c}$	codeword
C	linear code
$C^\perp$	dual code of C
$C\otimes\mathbb{F}_{q^m}$	extension code of C over $\mathbb{F}_{q^m}$
$C(J)$	all codewords of C with $c_j=0$ for all $j\in J$
C^m	linear subspace of all $m\times n$ matrices whose rows are words of C
d	minimum distance of a code
$d^\perp$	minimum distance of the dual code
$d(C,\mathbf{x})$	distance between the vector $\mathbf{x}$ and the code C
d_r	r-th generalized Hamming weight of a code
$d(\mathbf{x},\mathbf{y})$	Hamming distance between the vectors $\mathbf{x}$ and $\mathbf{y}$
$\mathbb{F}_q$	finite field with q elements
G	generator matrix of a code
G_J	submatrix of G formed by the columns of G indexed by J

H	parity check matrix of a code
J	subset of $[n]$
$\begin{bmatrix} k \\ r \end{bmatrix}_q$	Gaussian binomial
$l(J)$	dimension of $C(J)$
$M_{n,d}$	weight enumerator of MDS code of length n and minimum distance d
$M_{n,d_r}^{(r)}$	generalized weight enumerator of an MDS code of length n and generalized Hamming weight d_r
$[m,r]_q$	number of $m \times r$ matrices of rank r over $\mathbb{F}_q$
$[n]$	set of integers $\{1,2,\dots,n\}$
$[n,k]$	parameters of a (linear) code: length n and dimension k
$P_C(T,U)$	two-variable zeta polynomial of the code C
$P_C^{(r)}(T)$	r-th generalized zeta polynomial of the code C
$P_i(U)$	coefficient of T^i in the two-variable zeta polynomial
$P_i^{(r)}$	coefficient of T^i in the generalized zeta polynomial
$\rho(C)$	covering radius of the code C
$r(J)$	rank of G_J
$\langle r \rangle_q$	number of bases of $\mathbb{F}_q^r$
$\mathbf{s}$	syndrome of a vector
$\text{supp}(\mathbf{x})$	support of a vector $\mathbf{x}$
$\text{supp}(D)$	support of a subcode D
t	size of the set J
w	weight of a codeword
$W_C(X,Y)$	weight enumerator of the code C
$W_C^{(r)}(X,Y)$	r-th generalized weight enumerator of the code C
$W_C(X,Y,U)$	extended weight enumerator of the code C
$\text{wt}(\mathbf{x})$	weight of a vector $\mathbf{x}$
$\text{wt}(D)$	weight of a subcode D
$\mathbf{x}+C$	coset of $\mathbf{x}$ with respect to C
$\mathbf{x},\mathbf{y}$	vectors in $\mathbb{F}_q^n$
$Z_C(T,U)$	two-variable zeta function of the code C
$Z_C^{(r)}(T)$	generalized zeta function of the code C

Part II: Codes and arrangements

$\mathcal{A}$	arrangement of hyperplanes
$\mathcal{A}_G$	arrangement of hyperplanes associated to a (generator) matrix G
$\alpha_C(X,Y)$	coset leader weight enumerator of the code C
$\alpha_C(X,Y,U)$	extended coset leader weight enumerator of the code C
α_i	number of cosets of weight i
$\alpha_i(U)$	coefficient of $X^{n-i}Y^i$ in the extended coset leader weight enumerator
$\mathbb{F}$	field, not necessarily finite
$G_{\mathcal{P}}$	matrix associated to the projective system $\mathcal{P}$
$\mathbf{h}_j$	j-th column of a parity check matrix H
H_j	hyperplane in an arrangement
$\lambda_C(X,Y)$	list weight enumerator of the code C
$\lambda_C(X,Y,U)$	extended list weight enumerator of the code C
λ_i	number of vectors in $\mathbb{F}_q^n$ that are of minimal weight i in their coset
$\lambda_i(U)$	coefficient of $X^{n-i}Y^i$ in the extended list weight enumerator
$\mathcal{P}$	projective system
$\mathcal{P}_G$	projective system associated to a (generator) matrix G
P_j	point in a projective system
Π	subspace of $\mathbb{P}^{k-1}(\mathbb{F}_q)$
$\mathbb{P}^r(\mathbb{F})$	projective space of dimension r over the field $\mathbb{F}$
$\mathcal{RM}_q(1,s-1)$	first order q-ary Reed-Muller code of dimension s
$\mathcal{S}_q(s)$	q-ary Simplex code of dimension s
V_J	subspace of $\mathbb{F}_q^{n-k}$ generated by the vectors $\mathbf{h}_j^T$ with $j \in J$
$\mathcal{V}_t$	union of all V_J with $\lvert J\rvert = t$
$\mathrm{wt}_H(\mathbf{s})$	syndrome weight of $\mathbf{s}$ with respect to H
$\mathrm{wt}(\mathbf{y}+C)$	weight of the coset $\mathbf{y}+C$

Part III: Codes, arrangements and matroids

0_P	minimum of the poset P
1_P	maximum of the poset P
$\leq$	partial order
$\overline{A}_w(U)$	$A_w(U)/(U-1)$
$a(x)$	number of atoms a of a geometric lattice such that $a \leq x$

$\mathcal{B}$	collection of bases of a matorid
B	basis of a matroid
$\mathcal{B}^*$	collection of bases of the dual matroid
$\mathcal{C}$	collection of circuits of a matorid
C	circuit of a matroid
$\chi_{\mathcal{A}}(U)$	characteristic polynomial of the arrangement $\mathcal{A}$
$\tilde{\chi}(IN(x))$	reduced Euler characteristic of the independence complex of x
$\chi_i(U)$	coefficient of S^i in the coboundary polynomial
$\overline{\chi}_i(U)$	$\chi_i(U)/(U-1)$
$\chi_i^*(U)$	coefficient of S^i in the coboundary polynomial of the dual matroid
$\chi_L(S,U)$	coboundary polynomial of the geometric lattice L
$\chi_L(U)$	characteristic polynomial of the geometric lattice L
$\chi_M(S,U)$	coboundary polynomial of the simple matroid M
$c_r(x,y)$	number of chains of length r from x to y in a poset
$\overline{C}$	simplification of the code C
$\mathcal{D}$	collection of dependent sets of a matorid
D	dependent set of a matroid
d	size of the smallest cocircuit in a matroid
d^*	size of the smallest circuit of a matroid
E	finite set, ground set of a matroid
e,f	elements of a matroid
$\epsilon(B)$	external activity of the basis B
$\mathcal{F}$	collection of flats of a matorid
F	flat of a matroid
$f:P\to A$	map from the poset P to the abelian group A
$\check{f}$	sum function of f
$\hat{f}$	sum function of f
$\overline{G}$	simplification of the (generator) matrix G
H_J	intersection of all hyperplanes H_j with $j\in J$
$\mathcal{I}$	collection of independent sets of a matroid
I	independent set of a matorid
$\mathcal{I}_C$	collection of independent sets associated to the code C

$\mathcal{I}_G$	collection of independent sets associated to the (generator) matrix G
$\mathcal{I}(L)$	collection of independent sets associated to the geometric lattice L
$\iota(B)$	internal activity of the basis B
$i(P)$	inverse poset of the poset P
$\overline{J}$	closure of the subset J in a matroid
k	rank of a matroid
L	lattice
$L(\mathcal{A})$	geometric lattice associated to the arrangement $\mathcal{A}$
L_j	j-th level of the geometric lattice L
$L(M)$	lattice of flats of the matroid M
M	matroid
M^*	dual of the matroid M
M_C	matroid associated to the code C
M_G	matroid associated to the (generator) matrix G
$\mathcal{M}_i$	$\mathcal{N}_i \setminus \mathcal{N}_{i+1}$
$M(L)$	matroid associated to the geometric lattice L
$\overline{M}$	simplification of the matroid M
$\mu(x)$	$\mu(0,x)$
$\mu_i(U)$	coefficient of S^i in the Möbius polynomial
$\overline{\mu}_i(U)$	$\mu_i(U)/(U-1)$
$\mu_M(S,U)$	Möbius polynomial of the simple matroid M
$\mu(P)$	$\mu(0,1)$ in a finite poset P
$\mu_P(S,U)$	Möbius polynomial of the poset P with rank function
$\mu_P(x,y)$	Möbius function of the poset P
n	number of elements of a matroid
$\mathcal{N}_i$	union of all H_J with $J \subseteq [n]$ and $r(H_J) = i$
$\nu_M(x,y)$	$(-1)^{r_M(x)}\mu_L(x,y)\,\lvert\tilde{\chi}(IN(x))\rvert$, with $x,y \in L(M)$
ω	linear ordering on the ground set of a matroid
P	poset
$P_i(U)$	coefficient of T^i in the two-variable zeta polynomial
$P_i^*(U)$	coefficient of T^i in the two-variable zeta polynomial of the dual matroid
$P_M(T,U)$	two-variable zeta polynomial of the matroid M

P^x	all elements y in a poset with $y \leq x$
P_x	all elements y in a poset with $x \leq y$
$\mathrm{Rasp}_M(S,U)$	reciprocal alternating spectrum polynomial
$r(M)$	rank of the matroid M
$r(J)$	rank of the subset J of a matroid
$r^*(J)$	rank of the subset J in the dual matroid
$R_M(X,Y)$	Whitney rank generating function of the matroid M
$r(x)$	rank of the element x of a poset
$\mathrm{Spec}_M(S,U)$	spectrum polynomial of the matroid M
$\tau_+(P)$	upper truncation of the poset with rank function P
$\tau_-(P)$	lower truncation of the poset with rank function P
$\tau(L)$	truncation of the geometric lattice L
$\tau(M)$	truncation of the matroid M
$t_C(X,Y)$	Tutte polynomial of the matroid associated to the code C
$t_M(X,Y)$	Tutte polynomial of the matroid M
$U_{n,k}$	uniform matroid on n elements of rank k
w_i	Whitney number of the first kind
W_i	Whitney number of the second kind
w_{ij}	doubly indexed Whitney number of the first kind
W_{ij}	doubly indexed Whitney number of the second kind
$\mathcal{X}$	affine variety
$\mathcal{X}(\mathbb{F}_{q^m})$	set of $\mathbb{F}_{q^m}$-rational points of the affine variety $\mathcal{X}$
$\mathcal{X}_i$	set of all $\mathbf{x} \in \mathbb{A}^k$ such that $\mathrm{wt}(\mathbf{x}G) = n - i$
x, y, z	elements of a poset or lattice
$x \lessdot y$	y is a cover of x
$[x, y]$	interval between x and y
$x \vee y$	join of x and y
$x \wedge y$	meet of x and y
$\mathcal{Y}_i$	set of all $\mathbf{x} \in \mathbb{A}^k$ such that $\mathrm{wt}(\mathbf{x}G) \leq n - i$

Index

Samenvatting in het Nederlands

Deze samenvatting is bedoeld voor iedereen die denkt niets van dit proefschrift te zullen begrijpen, maar wel graag wil weten waar het over gaat. Er is geen wiskundige voorkennis nodig om de volgende pagina's te lezen. Als je die wel hebt, lees dan ook de samenvatting voorin dit proefschrift en probeer daarna de hoofdstukken die beginnen met "Introduction to..." te lezen.

Talen om de wereld om je heen te beschrijven

Om de wereld om ons heen te beschrijven, gebruiken mensen taal. Er zijn een heleboel talen op de wereld om de wereld mee te beschrijven, maar ze zijn niet allemaal hetzelfde. Zo heeft het Nederlands een heleboel woorden om verschillende soorten regen te beschrijven, omdat het zo vaak regent in Nederland. Kijk je naar een meer Mediterrane taal zoals Italiaans, dan zal je veel minder verschillende woorden voor "regen" tegenkomen, vanwege het droge klimaat. Niet alle Nederlandse woorden voor verschillende soorten regen kan je dus letterlijk naar het Italiaans vertalen. Als je een verhaal schrijft over regen, dan is het Nederlands dus een goede keus. Maar als je een verhaal over sneeuw gaat schrijven, kan je beter de taal van de Eskimo's nemen: volgens de legende hebben die meer dan veertig verschillende woorden voor verschillende varianten van sneeuw.

In de wiskunde is hetzelfde aan de hand. Als je bepaalde eigenschappen van wiskundige objecten bestudeert, dan zoek je naar de beste manier om "tegen de zaak aan te kijken". Met andere woorden, je zoekt het beste *model* voor het probleem. Het is erg handig om verschillende manieren te hebben om tegen hetzelfde wiskundige object aan te kijken. Door je probleem te "vertalen" naar een ander model, heb je opeens een stuk meer kennis ter beschikking om het probleem op te lossen. Vraagstukken die ingewikkeld lijken, hebben misschien wel een eenvoudige oplossing als je ze naar een ander wiskundig model vertaalt.

Om te kunnen wisselen tussen verschillende talen, heb je goede woordenboeken nodig. Dit proefschrift is een soort wiskundig woordenboek. Het beschrijft hoe je kan vertalen tussen drie wiskundige objecten: *codes*, *arrangementen*, en *matroïden*. In het bijzonder behandelt dit "woordenboek" hoe je bepaalde informatie over de drie objecten die gevangen is in *polynomen* kan vertalen. Ook worden stellingen over een van de drie objecten bewezen met behulp van vertalingen tussen de verschillende objecten en polynomen. In deze samenvatting vind je een uitleg over de drie objecten en de polynomen die erbij horen.

Polynomen

In dit proefschrift bestuderen we eigenschappen van wiskundige objecten die we kunnen weergeven als een rij getallen. We kijken hoe dit werkt met behulp van een voorbeeld. Stel, een leraar geeft een proefwerk, waarbij de leerlingen een cijfer tussen de 1 en de 10 kunnen scoren. Om bij te houden hoeveel leerlingen welk cijfer hebben gehaald, schrijft de leraar de volgende rijt op:

$$(1, 0, 0, 3, 3, 7, 8, 5, 2, 1).$$

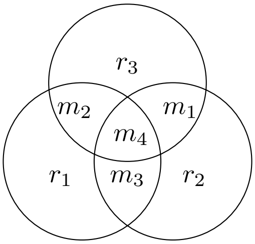
De getallen staan voor aantallen leerlingen. De plaats in de rij waarop een getal staat, geeft het cijfer aan. Er is dus één leerling met een 1, geen leerlingen met een 2 of 3, drie leerlingen met een 4, etcetera. Uit deze rij kan je snel informatie halen. Zo zie je dat er 30 leerlingen in de klas zitten. Om te kijken hoeveel leerlingen een voldoende hebben gehaald, tellen we de cijfers vanaf plaats 6 bij elkaar op: dit zijn 23 leerlingen.
In deze rij van tien cijfers kunnen we nog wel makkelijk zien waar de zesde plaats is. Maar als we lange rijtjes bekijken, wordt dat lastiger. We kunnen de rij getallen daarom als volgt opschrijven:

$$X + 3X^4 + 3X^5 + 7X^6 + 8X^7 + 5X^8 + 2X^9 + X^{10}.$$

Deze manier van schrijven noemen we een *polynoom*. In dit polynoom is X de *variabele*, die schrijven we meestal met een hoofdletter. De getallen rechts van de X zijn de *exponenten*, de getallen links de *coëfficiënten*. In ons voorbeeld worden de cijfers dus weergegeven door de exponenten. Het aantal leerlingen dat een bepaald cijfer haalt, vind je in de bijbehorende coëfficiënt. We gaan nu bekijken wat de polynomen zijn die horen bij codes, arrangementen en matroïden.

Foutverbeterende codes

Je kent vast wel de stukken tekst die op internet rondzwerven waarbij van alle woorden de letters door elkaar zijn gehusseld, behalve de eerste en de laatste letter. Het blijkt vaak dat je, met een beetje moeite, die tekst nog gewoon kan lezen. Dat komt doordat onze taal *redundante informatie* bevat. Dit betekent dat onze woorden veel korter geweest zouden zijn, als we simpelweg alle mogelijke rijtjes van letters een betekenis hadden gegeven. Dat heeft natuurlijk allerlei praktische nadelen, bijvoorbeeld de uitspraak. Een



FIGUUR 1: Schematische weergave van de Hamming code

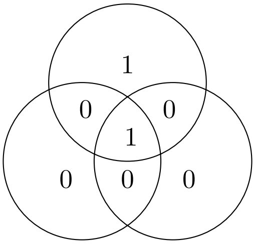
belangrijk voordeel van van woorden met redundante informatie is het volgende: als je een typefout maakt, of even je spellingsregels bent vergeten, dan kan je dat gemakkelijk corrigeren. Je lees dan een rij letters die geen bestaand woord is, maar wel op een bestaand woord lijkt. Dus corrigeer je naar het bestaande woord.

Computers werken, net als andere digitale apparaten zoals je mobiele telefoon of cd-speler, met nullen en enen. Toen computers net waren uitgevonden en nog met ponskaarten werkten, werden alle opdrachten voor de computer vertaald naar nullen en enen. Alle rijtjes van nullen en enen betekenden iets anders. Maar naar mate computers vaker gebruikt werden, merkten de mensen die ermee werkten dat dit nogal eens voor fouten zorgde. Als de computer ergens een 0 in een 1 veranderde, of andersom, liep direct het hele programma vast. Naar verluidt was ene Richard Hamming zo gefrustreerd over deze fouten, dat hij de code bedacht die later naar hem vernoemd is.
Het idee van Hamming was dat een computer een leesfout moest kunnen corrigeren, net als dat wij spelfouten in woorden kunnen corrigeren. Dat deed hij door redundante informatie toe te voegen aan de commando's voor de computer. De commando's die Hamming aan de computer gaf, bestonden uit vier *bits*: het waren rijen van vier getallen die elk 0 of 1 zijn, bijvoorbeeld 1101. De bits noemen we m_1, m_2, m_3, en m_4. Hamming zette de bits in drie cirkels, zoals je ziet in Figuur 1. Vervolgens berekende hij drie bits redundante informatie: r_1, r_2 en r_3. Hij deed dat op zo'n manier, dat in elke cirkel een even aantal (dus 0, 2 of 4) enen kwam te staan. Deze bits plakte hij achter het oorspronkelijke commando.

In plaats van de gebruikelijke 4 bits, bestonden de commando's die Hamming aan de computer gaf nu uit 7 bits. Maar niet elke rij van 7 enen of nullen kan voorkomen. Er kan bijvoorbeeld nooit maar één 1 voorkomen in de rij. (Zie je waarom?) De toegestane rijtjes noemen we *codewoorden*. Het aantal bits in een codewoord noemen we de *lengte* van de code en de bits noemen we ook wel *coördinaten*.

Stel, het bericht dat we door willen sturen heeft $m_1 = 1$, $m_2 = 1$, $m_3 = 0$ en $m_4 = 1$. De redundante bits zijn dan $r_1 = 0$, $r_2 = 0$ en $r_3 = 1$. Het codewoord dat bij dit bericht hoort, is dus 1101001. Stel nu dat er iets mis gaat bij het inlezen van dit codewoord: de tweede coördinaat verandert in een 0, dus de computer leest 1001001. Om te kijken welk bericht hierbij hoort, maakt de computer gebruik van het cirkeldiagram uit Figuur 1 en vult het ontvangen woord hier in. Je zit dit in Figuur 2. De computer controleert of in iedere cirkel een even aantal enen staat. Dat is niet het geval in de bovenste cirkel en in de linker cirkel. In de rechter cirkel staat wel het juiste aantal enen. De computer concludeert nu dat de fout is gemaakt in de coördinaat die zowel in de linker cirkel als in de bovenste cirkel staat: dat is de coördinaat m_2. Op die manier kan de computer de ontvangen rij corrigeren naar het codewoord 1101001.

Hoe "goed" een code is, hangt af van hoeveel fouten verbeterd kunnen worden en hoeveel redundante informatie je daarvoor nodig hebt. Van meer redundantie wordt je computer trager, dus je wil er niet teveel van hebben. Maar je wil ook het risico op fouten beperken. Informatie die kan helpen deze afweging te maken, is het *gewicht* van de codewoorden in de code. Het gewicht van een codewoord is het aantal coördinaten dat niet nul is. Het gewicht van het codewoord 1101001 is dus vier. Hoeveel codewoorden er zijn met welk



FIGUUR 2: Een ontvangen bericht in de Hamming code

gewicht, kunnen we opschrijven in een polynoom dat het *gewichtsverdelingspolynoom* heet (in het Engels: weight enumerator). Het gewichtsverdelingspolynoom van de Hamming code is

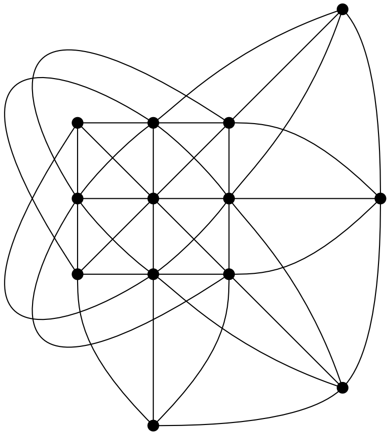
$$1 + 7X^3 + 7X^4 + X^7.$$

Dit betekent dat er één woord is van gewicht nul (namelijk 0000000), één woord van gewicht zeven (namelijk 1111111), zeven woorden van gewicht drie, en zeven woorden van gewicht vier. Probeer maar eens of je alle zestien woorden van de Hamming code op kan schrijven! (Tip: gebruik het schema uit Figuur 1. Hoeveel mogelijkheden zijn er voor m_1, m_2, m_3 en m_4?)

Arrangementen van lijnen in een vlak

Een *arrangement* is eigenlijk heel simpel een verzameling van lijnen in een vlak. Niet zoveel aan, zou je zeggen. Maar je kan er aardig wat aan rekenen. Iets dat voor de hand ligt is het volgende: stel dat we een bepaalde hoeveelheid lijnen in het vlak hebben getekend. (We gaan er meestal vanuit dat ons papier oneindig groot is en dat de lijnen oneindig lang doorlopen.) In hoeveel verschillende gebieden heb je het vlak dan verdeeld? Als je één lijn in het vlak tekent, dan deelt deze lijn het vlak in twee stukken. Als je er een tweede lijn bij tekent, dan zul je meestal vier stukken krijgen. Tenzij de lijnen toevallig precies evenwijdig lopen: dan hebben we het vlak in drie stukken gedeeld. Bij drie lijnen in een driehoek deel je het vlak in zeven stukken. Als de drie lijnen toevallig alledrie door hetzelfde punt gaan, dan verdelen we het vlak in zes "taartpunten". Ook als twee van de drie lijnen evenwijdig lopen, krijgen we zes stukken. Als alle drie de lijnen evenwijdig zijn, hebben we maar vier stukken. Je ziet: alleen het aantal lijnen geeft niet genoeg informatie over het aantal stukken waarin ze het vlak verdelen. Je moet ook iets weten over parallelle lijnen en over punten waar meer dan twee lijnen samenkomen.

Nu is het in de vlakke meetkunde zoals we die gewend zijn, een vrij unieke gebeurtenis als twee lijnen evenwijdig lopen of als drie lijnen door één punt gaan. Als je twee willekeurige lijnen tekent, zullen ze elkaar vrijwel altijd snijden. Maar in de wiskunde die we in dit proefschrift gebruiken, is de meetkunde *eindig* en *projectief*. Deze twee woorden hebben enige uitleg nodig. Met *eindig* bedoelen we niet het eindig zijn zoals een bladzijde in dit proefschrift. We spreken af dat maar eindig veel lijnen en eindig veel punten bij onze meetkunde horen. Dan heeft elke lijn maar eindig veel punten en gaan er maar eindig veel



Figuur 3: Een projectief vlak van 13 punten en 13 lijnen

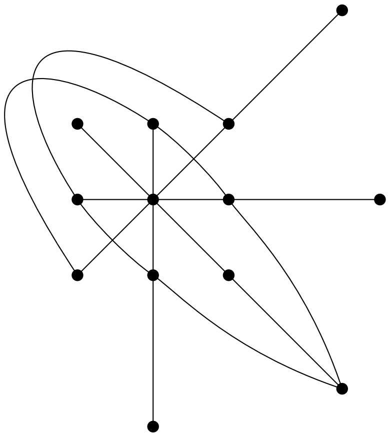
lijnen door elk punt – in tegenstelling tot de gewone vlakke meetkunde met oneindig veel punten op een lijn en oneindig veel lijnen door een punt. Dat een meetkunde *projectief* is, betekent het volgende:

- Door ieder tweetal punten gaat precies één lijn.
- Ieder tweetal lijnen snijdt elkaar in precies één punt.
- (Er is ook nog een eis die bepaalde extreme situaties uitsluit, die zullen we hier niet behandelen.)

De eerste eis zal je niet zoveel verbazen: dat is in de gewone vlakke meetkunde ook het geval. Maar de tweede eis heeft een belangrijk gevolg: parallelle lijnen bestaan niet in de projectieve meetkunde!
Omdat zo'n eindige projectieve meetkunde nogal abstract klinkt, staat in Figuur 3 een voorbeeld. Er zijn projectieve vlakken met verschillende aantallen punten en lijnen: we speren af dat dit eindige projectieve vlak uit 13 punten en 13 lijnen bestaat. Iedere lijn bevat 4 punten en door ieder punt gaan 4 lijnen – dat kan niet anders als je 13 punten en 13 lijnen hebt, maar het gaat wat ver om hier uit te leggen waarom. In de figuur lopen de lijnen niet helemaal recht en lopen soms over elkaar heen terwijl ze geen snijpunt hebben, maar dat komt omdat het papier waarop ze gedrukt zijn, niet een eindig projectief vlak is.

We gaan nu kijken naar een arrangement in dit projectieve vlak. Je ziet het in Figuur 4. Het arrangement bestaat uit zes lijnen. Zoals gezegd, komen er geen parallelle lijnen voor. Maar je ziet dat er best veel punten zijn waar meer dan twee lijnen doorheen gaan: doordat er maar eindig veel lijnen zijn, zullen veel vaker drie of meer lijnen door hetzelfde punt gaan.

Wat gaan we nu tellen aan een arrangement? Het aantal gebieden waarin het vlak verdeeld wordt, heeft niet echt een betekenis in het projectieve vlak. We tellen daarom hoeveel punten er zijn waar een bepaald aantal lijnen doorheen gaat. Die informatie vatten we



Figuur 4: Een arrangement van zes lijnen in het projectieve vlak van Figuur 3

samen in het *coboundary polynoom* (er is niet echt een mooie Nederlandse vertaling voor *coboundary*). Voor het arrangement uit Figuur 4 is het coboundary polynoom gelijk aan

$$5X + 6X^2 + X^3 + X^4.$$

Dit betekent dat er vijf punten zijn die op één lijn liggen, zes punten die op twee lijnen liggen, één punt dat op drie lijnen ligt, en één punt dat op vier lijnen ligt. Er zijn geen punten die op nul, vijf of zes lijnen liggen.

We weten nu genoeg over arrangementen om de vertaling naar codes en gewichten te maken. De woorden van een code vetalen we naar de punten in het eindige projectieve vlak. De lijnen van het arrangement stellen de verschillende coördinaten van de codewoorden voor. Wanneer een lijn van het arrangement door een punt heen gaat, dan betekent dit dat het bijbehorende codewoord een 0 heeft in de coördinaat die bij de lijn hoort.
Het arrangement in Figuur 4 vertalen we dus naar een code met 13 codewoorden en lengte 6. Het gewicht van de codewoorden kunnen we aflezen uit het aantal lijnen dat door het bijbehorende punt gaat: het punt waar vier lijnen doorheen gaan, correspondeert bijvoorbeeld met een codewoord dat vier nullen heeft. Dit codewoord heeft dus gewicht twee, omdat de code lengte zes heeft.

Doordat we codes naar arrangementen kunnen vertalen en andersom, kunnen we ook de bijbehorende polynomen vertalen. Als je het gewichtsverdelingspolynoom weet en je zet de coëfficiënten in de omgekeerde volgorde, dan vind je het coboundary polynoom. Heel eenvoudig eigenlijk! Zo vinden we dat het gewichtsverdelingspolynoom dat hoort bij het arrangement uit Figuur 4 gelijk is aan

$$X^2 + X^3 + 6X^4 + 5X^5.$$

Andersom kan je ook de volgorde van de coëfficiënten van het coboundary polynoom omkeren om het gewichtsverdelingspolynoom te krijgen.

Matroïden

Stel, we hebben een arrangement, zoals in de vorige sectie beschreven. Wanneer we maar naar een aantal lijnen uit het arrangement kijken, noemen we dit een *deelverzameling*. We spreken af dat een deelverzameling alle lijnen van het arrangement mag bevatten, of helemaal geen. We gaan nu aan elke deelverzameling een getal toekennen: de *rang*. In het geval van het arrangement uit Figuur 4 is de rang minimaal 0 en maximaal 3. De rang is 0 als de deelverzameling uit nul lijnen bestaat, 1 als de deelverzameling uit één lijn bestaat, en 2 als de deelverzameling uit twee lijnen bestaat. Bij een deelverzameling van drie of meer lijnen, moeten we een beetje opletten: als alle lijnen door hetzelfde punt gaan, is de rang 2; als dat niet het geval is, is de rang 3.
Het zal je niet verbazen dat we deze informatie ook weer kunnen samenvatten in een polynoom: het *Whitney rang-polynoom*, genoemd naar de wiskundige Whitney die het als eerste opschreef. Dit polynoom heeft niet één, maar twee variabelen. De exponent van X geeft de grootte van de deelverzameling aan, de exponent van Y de rang van die deelverzameling. De coëfficiënt geeft aan hoeveel deelverzamelingen er zijn van een bepaalde grootte en rang. Voor het voorbeeld uit Figuur 4 is het Whitney rang-polynoom gelijk aan

$$1 + 6XY + 15X^2Y^2 + 5X^3Y^2 + X^4Y^2 + 15X^3Y^3 + 14X^4Y^3 + 6X^5Y^3 + X^6Y^3.$$

Hier betekent $5X^3Y^2$ dat er vijf deelverzamelingen zijn die uit drie lijnen bestaan die door hetzelfde punt gaan. Als we alle coëfficiënten bij elkaar optellen, zie je dat er in totaal 64 deelverzamelingen zijn. De coëfficiënten van het Whitney-polynoom vertellen iets over wanneer meerdere lijnen door hetzelfde punt gaan. Door een slimme combinatie van deze coëfficiënten te nemen, kunnen we dan ook zowel het gewichtsverdelingspolynoom als het coboundary polynoom bepalen.

De rang van de deelverzamelingen van een arrangement voldoet aan een aantal eisen. De eerste twee kan je zelf controleren voor ons voorbeeld.

- De rang van een deelverzameling is altijd minstens 0 en maximaal het aantal lijnen in de deelverzameling.
- Als je een lijn toevoegt aan een deelverzameling, dan blijft de rang van de deelverzameling gelijk of gaat met één omhoog.
- (Er is ook nog een eis over wat er gebeurt met de rang als je twee deelverzamelingen samenvoegt, maar die is te ingewikkeld om hier uit te leggen.)

Het blijkt dat deze eisen niet alleen gelden voor de rang van deelverzamelingen van arrangementen. Je kan ook deelverzamelingen nemen van andere wiskundige structuren en daar een rang voor definiëren. Je kan zelfs helemaal niet vastleggen waarvan je deelverzamelingen neemt. Je zou bij wijze van spreken vijftien verschillende soorten fruit kunnen nemen en alle deelverzamelingen een rang geven die aan de eisen voldoet. Het wiskundige object dat hoort bij een aantal “dingen” en een rang voor elke deelverzameling die aan bovenstaande eisen voldoet, heet een *matroïde*. De “dingen” heten *elementen*, bijvoorbeeld de lijnen van een arrangement. Voor iedere matroïde kan je het Whitney rang-polynoom opschrijven.

Alle arrangementen en codes zijn te vertalen naar matroïden, maar niet alle matroïden zijn ook een arrangement of een code. Er zijn veel meer matroïden dan dat er codes en arrangementen zijn. De matroïde is dan ook de meest "algemene" en abstracte structuur die in dit proefschrift aan de orde komt. Toch blijkt het handig te zijn om juist een algemenere structuur te onderzoeken. De dingen die je kan laten zien over matroïden, kan je toepassen naar een heleboel verschillende voorbeelden. Net zoals dat onderzoek naar zoogdieren toepassingen heeft voor koeien, paarden, walvissen en mensen.

Tenslotte

Ik hoop dat het lezen van deze samenvatting het een beetje duidelijker maakt waar ik me de afgelopen vier jaar mee bezig heb gehouden. Ik hoop in elk geval mijn enthousiasme voor mijn onderzoek over te brengen.

Tijdens het schrijven heb ik mij enkele wiskundige vrijheden veroorloofd, met name bij de definitie van het Whitney rang-polynoom (zie Definition 8.1 in dit proefschrift) en de gewichtsverdeling van het arrangement uit Figuur 4 (zie Example 10.34 in dit proefschrift). Ook heb ik voor het gemak alleen arrangementen van lijnen in het vlak behandeld, in plaats van arrangementen van hypervlakken in ruimtes van willekeurige dimensie. De wiskundigen die toch deze samenvatting zijn gaan lezen, zijn bij deze uitgedaagd deze vrijheden te corrigeren.

Curriculum Vitae

Relinde Jurrius was born on February 25, 1984 in Haarlem, The Netherlands. In 2002 she obtained her gymnasium diploma from the Coornhert Lyceum in Haarlem. In the same year she started studying both mathematics and astronomy at Leiden University. After completing the first year (propedeuse) in the two subjects, she continued in mathematics.

Relinde wrote her bachelor thesis *Algebraïsche topology en de fixpuntstelling van Lefshetz* (Algebraic topology and the Lefshetz fixed point theorem) under supervision of dr. Robin de Jong. After obtaining her bachelors degree in 2005, she was in the board of the students rowing club Asopos de Vliet for the academic year 2005–2006. When she continued with her master studies, she learned about coding theory via a course in the national MasterMath program. It gained her interest, and she wrote her master thesis *Classifying polynomials of linear codes* under joint supervision of dr. Robin de Jong from Leiden University and dr. Ruud Pellikaan from Eindhoven University of Technology. Relinde obtained her masters degree in 2008.

In October 2008, Relinde started as a PhD student at Eindhoven University of Technology under supervision of dr. Ruud Pellikaan. She continued the work from her master thesis and extended her area of interest to arrangements and matroids. This thesis is the result of her research from 2008 to 2012.

Relinde likes sharing her enthusiasm for mathematics with others. Every summer she spends a week at math camp with Vierkant voor Wiskunde. She helps organizing the camp and writing the material. Furthermore, she was involved in organizing the Dutch Mathematical Olympiad and setting up a new round in the contest. To show high school girls that science is not just something for boys, she is a ‘role-model’ for VHTO.

During the day, as a break from work, Relinde likes to play the violin. She started playing long time ago and was in various orchestras. Currently, she plays in the Philips Symphony Orchestra, where she is also in the board as treasurer.

Acknowledgments

Although this thesis contains hours and hours of work by myself, it would not have existed without the help of many people in my working environment.

Het is onder promovendi niet ongebruikelijk af en toe te zeuren over je begeleider. Ik begon dan altijd op te scheppen: dat ik de vrijheid kreeg weken niets van me te laten horen, maar wel altijd langs kon komen. Dat we er allebei niet van houden een uur voor de deadline pas een artikel af te hebben. Dat ik er vaak pas achteraf achter kwam dat ik toch weer subtiel de goede (onderzoeks)richting in was gestuurd. En bovenal, dat ik de fijne kneepjes van het vak kon afkijken van een goede wetenschapper. Beste hr. Pellikaan, beste Ruud, heel erg veel dank.

Henk, ik hoop dat ik later net zo'n goede professor word als jij.

I would like to express my gratitude also to the other members of my defense committee: Aart Blokhuis, Andries Brouwer, Tom Høhold, Dieter Jungnickel, Tanja Lange and Jack van Wijk. Thank you for traveling to Eindhoven for my defense, reading my thesis and suggesting further improvements.

During my time as a PhD student I had multiple interesting and inspiring discussions with other mathematicians around the world. In particular I wish to thank Vladimir Tonchev for asking the question that led to Chapter 5 of this thesis, as well as to many ideas for further research.

Sebastiaan, bedankt voor het inkleuren van de cover van dit boekje. Vanessa en Sietse, heel fijn dat jullie de Nederlandse samenvatting wilden lezen en vragen stelden die ik zelf niet had kunnen bedenken.

My colleagues at the Security and the Discrete Mathematics group provided an excellent working atmosphere. In particular my fellow PhD students: thank you Reza, Peter, Michael, José, other Peter, Jing, Christiane, Gaëtan, Bruno, Ruben, Daniel, jet another Peter, Sebastiaan, Mayla, Antonino, Elisa, Dion, Jan-Jaap, Meilof, Thijs, Sokratis, and our visitor Irene. It was a pleasure having coffee with you.

Tenslotte een warm woord van dank voor onze secretaresses Anita, Jolande, en Rianne. Er zouden heel veel praktische zaken mis gaan zonder jullie – en het zou ook een stuk minder gezellig zijn.