Invariance for weight enumerators of evaluation codes and counting $\mathbb{F}_q$-rational points on hypersurfaces.

Master of Science (M. Sc.) Project

Olivier Mila

Supervised by

Prof. Eva Bayer-Fluckiger and Dr. Martino Borello

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Spring Semester 2015
## Contents

**Introduction** ................................................. 4

**Notations** .................................................. 13

1 Background ................................................... 14

1.1 Coding Theory .............................................. 14

1.1.1 Basics .................................................. 14

1.1.2 MacWilliams' Theorem .................................... 18

1.2 Invariant Theory ............................................ 25

1.2.1 Basics .................................................. 25

1.2.2 Molien series .......................................... 27

1.2.3 An application to self-dual doubly-even codes ......... 29

1.3 Algebraic Geometry ......................................... 33

1.3.1 Basic definitions ...................................... 33

1.3.2 Regular maps, morphisms and rational maps .......... 37

2 Evaluation Codes ............................................. 42

2.1 Affine Reed-Muller Codes ................................. 42

2.1.1 The dimension of $\mathcal{R}_M$-codes .................. 43

2.1.2 The dual of $\mathcal{R}_M$-codes .......................... 48

2.1.3 Other properties ...................................... 50
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.4</td>
<td>Examples</td>
<td>51</td>
</tr>
<tr>
<td>2.2</td>
<td>Projective Reed-Muller Codes</td>
<td>52</td>
</tr>
<tr>
<td>2.2.1</td>
<td>Properties of $PRM$-codes</td>
<td>53</td>
</tr>
<tr>
<td>3</td>
<td>Divisibility</td>
<td>56</td>
</tr>
<tr>
<td>3.1</td>
<td>The divisibility of Reed-Muller codes</td>
<td>57</td>
</tr>
<tr>
<td>3.1.1</td>
<td>Affine Reed-Muller codes</td>
<td>57</td>
</tr>
<tr>
<td>3.1.2</td>
<td>Borissov’s Proof</td>
<td>60</td>
</tr>
<tr>
<td>3.1.3</td>
<td>Projective Reed-Muller codes</td>
<td>63</td>
</tr>
<tr>
<td>3.2</td>
<td>Weil’s Method: a geometrical point of view</td>
<td>65</td>
</tr>
<tr>
<td>3.2.1</td>
<td>The Picard group</td>
<td>66</td>
</tr>
<tr>
<td>3.2.2</td>
<td>The Frobenius map</td>
<td>69</td>
</tr>
<tr>
<td>3.2.3</td>
<td>Example of use</td>
<td>71</td>
</tr>
<tr>
<td>4</td>
<td>Invariants and weight enumerators of particular Reed-Muller codes</td>
<td>77</td>
</tr>
<tr>
<td>4.1</td>
<td>Invariants of Reed-Muller codes</td>
<td>77</td>
</tr>
<tr>
<td>4.2</td>
<td>Computations in the self-dual case</td>
<td>79</td>
</tr>
<tr>
<td>4.3</td>
<td>The action of $PGL_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$</td>
<td>81</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Cross-Ratios</td>
<td>82</td>
</tr>
<tr>
<td>4.4</td>
<td>Finiteness of Stabilizers</td>
<td>84</td>
</tr>
<tr>
<td>4.5</td>
<td>A weight enumerator with trivial stabilizer</td>
<td>87</td>
</tr>
<tr>
<td>4.5.1</td>
<td>An algorithm to find the stabilizer</td>
<td>92</td>
</tr>
</tbody>
</table>
Introduction

The problem of counting rational points on curves and varieties over finite fields is one of the classical problems of algebraic geometry. Already in 1801, in his *Disquisitiones Arithmeticae*, Gauss counted the number of solutions of the cubic Fermat equation

\[ x^3 + y^3 + z^3 \equiv 0 \pmod{p} \]

for a prime \( p > 3 \). Rephrasing his result in modern language, he proved that the curve \( C \) defined by this equation in the projective plane over the prime field \( \mathbb{F}_p \) has \( p + 1 \) \( \mathbb{F}_p \)-rational points if \( p \not\equiv 1 \pmod{3} \), and \( p + 1 + a \) points if \( p \equiv 1 \pmod{3} \), where \( a \) is the unique integer with \( a \equiv 1 \pmod{3} \) such that one can write \( 4p = a^2 + 27b^2 \) for some integer \( b \).

The concept of finite field was introduced in 1830 by Galois, and during the 19th century, algebraic curves were already an important subject in mathematics. However, it was only in the 20th century that mathematicians started to consider systematically algebraic curves over finite fields, and that this topic became a subject of intense research.

One of the main discovery in this area is the famous Hasse-Weil bound. It was Artin in his 1924 Ph.D. thesis who indirectly set the problem back in the front of the scene. He constructed a function similar to the Riemann zeta function for function fields of hyperelliptic curves over finite fields, and conjectured the analogue of the well known Riemann hypothesis for this function. A few years later, Schmidt reformulated the problem and wrote the zeta function for a smooth absolutely irreducible projective curve \( C \) over some finite field \( \mathbb{F}_q \) as the generating function for the values \( c(n) := \#C(\mathbb{F}_{q^n}) \), the number of rational points of \( C \) in an extension of \( \mathbb{F}_q \) of degree \( n \):

\[
Z_C(t) := \exp \left( \sum_{n=1}^{\infty} c(n) \frac{t^n}{n} \right). 
\]
This function turns out to be a rational function of $t$:

$$Z_C(t) = \frac{P(t)}{(1-t)(1-qt)},$$

for some polynomial $P \in \mathbb{Z}[t]$ of degree $2g$, where $g$ is the genus of the curve. Artin’s conjecture then states that all zeroes of this function have modulus $q^{-1/2}$.

In 1934, Hasse proved this conjecture for elliptic curves, and observed that this implies the following bound: if $X$ is an elliptic curve over some finite field $\mathbb{F}_q$, then

$$|\#X(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}.$$ 

It was only 4 years later in 1940 that Weil generalized this to the case of arbitrary genus. This is the so-called Hasse-Weil bound: any smooth projective curve $X$ over $\mathbb{F}_q$ of genus $g$ satisfies

$$|\#X(\mathbb{F}_q) - (q + 1)| \leq 2g\sqrt{q}.$$ 

Besides this bound, Weil also did remarkable foundational work on algebraic geometry itself. He generalized Artin’s conjecture to other types of zeta functions: the famous Weil conjectures were born. After that, the tendency shifted away from the actual counting of rational points of curves to the resolution of these conjectures and related problems. Grothendieck’s revolution with the introduction of étale cohomology was the most important step towards proving this theorem. The complete proof of Weil’s conjectures was carried out by Deligne in 1974.

It was Goppa’s work which attracted attention again on the counting of points in curves. His idea was to construct codes coming from the evaluation of rational functions on a subset of points of a projective curve. He remarked that the “quality” of those codes depends on how many rational points a curve contains, and that if this number is large enough, the codes constructed that way are “optimal” in the sense that they attain the so-called Gilbert-Varshamov bound. The problem of finding explicitly the number of those points was brought back to the front of the scene.

Many mathematicians worked on this subject. For example, Schoof (in [Sch95]) gave an explicit algorithm to compute the number of rational points of an elliptic curve over a prime field $\mathbb{F}_p$. With his algorithm (and some improvements from Atkin and Elkies) he was able to compute the number of $\mathbb{F}_p$-rational points of the elliptic curve $Y^2 = X^3 + 105X + 78153$ for the prime $p = 10^{200} + 153$.

In another paper ([Sch87]), Schoof explicitly gives the point counts for cubics plane curves over finite fields. Along the same lines, in an unpublished paper, Elkies used
Coding Theory to give the point counts of cubic surfaces in $\mathbb{P}^3(\mathbb{F}_q)$. This idea was generalized by Kaplan in his Ph.D. thesis (Kap13) to other types of surfaces such as del Pezzo surfaces. The work of Elkies an Kaplan was very inspirational for the present thesis.

Before explaining their method, we give some basic definitions.

A linear code $C$ is a subspace of $\mathbb{F}_q^n$ for some integer $n$, which is called the \textit{length} of the code. Elements of $C$ are usually called \textit{codewords}. The dual code $C^\perp$ is then the vector space of elements $x \in \mathbb{F}_q^n$ which satisfy $\langle x, y \rangle := \sum_{i=1}^n x_i y_i = 0$ for any $y \in C$ ($\langle \cdot, \cdot \rangle$ is the usual Euclidean product of $\mathbb{F}_q^n$). If $c \in C$, the \textit{weight} of $c$ (denoted $\text{wt}(c)$) is simply the number of non-zero coordinates of $c$. The \textit{weight enumerator} of $C$ is the polynomial

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

Examples of linear codes coming from algebraic geometry are the so called Reed-Muller codes. The affine Reed-Muller code on $m$ variables of degree $r$ over the finite field $\mathbb{F}_q$, denoted $\mathcal{RM}_{\mathbb{F}_q}(r, m)$, is simply the code coming from the evaluation at each point of $\mathbb{A}^m(\mathbb{F}_q)$ of the polynomials $f \in \mathbb{F}_q[X_1, \ldots, X_m]$ on $m$ variables, of degree not exceeding $r$. Explicitly,

$$\mathcal{RM}_{\mathbb{F}_q}(r, m) = \{(f(x))_{x \in \mathbb{A}^m(\mathbb{F}_q)} \mid f \in \mathbb{F}_q[X_1, \ldots, X_m] \text{ of degree } \leq r\}.$$ 

The projective Reed-Muller codes are defined similarly, except that only homogeneous polynomials of degree exactly $r$ (together with the 0 polynomial) are considered, and evaluation is on a fixed set of representatives of the projective space $\mathbb{P}^m(\mathbb{F}_q)$. Observe that the code obtained in that way depends on the choice of representatives, but a change in these representatives results in an equivalent code, in a sense that we will define later on. We denote by $\mathcal{PRM}_{\mathbb{F}_q}(r, m)$ the projective Reed-Muller code of degree $r$ on $m$ variables over $\mathbb{F}_q$.

Observe that while these codes have interesting geometric properties, their interest also lies in practical applications in communication systems. For example, in 1972 during a spacial expedition to acquire pictures of the planet Mars, the spacecraft Mariner 9 used the Reed-Muller code $\mathcal{RM}_{\mathbb{F}_2}(1, 3)$ (the code coming from lines in $\mathbb{A}^3(\mathbb{F}_2)$) to encode the data sent over space.

A very important formula relating the weight enumerator of a code to the one of its dual is MacWilliams’ Theorem. This theorem states that if $C$ is a linear code over $\mathbb{F}_q$,
then the weight enumerator of the dual code $C^\perp$ is given by
\begin{equation*}
W_{C^\perp}(X, Y) = \frac{1}{|C|} \cdot W_C(X + (q - 1)Y, X - Y).
\end{equation*}

The idea of Elkies can be roughly summarized as follows. He used existing knowledge on the point counts of some cubic surfaces as a starting point. He considered a projective Reed-Muller code $(\mathcal{PRM}_{F_q}(3, 3))$, by evaluating cubics at all points of the projective space. He then used MacWilliams’ Theorem to get conditions on the dual of such a code. As he observed, the codewords of this code correspond to points failing to impose independent conditions on cubics. This can be understood as the sets of points $S$ such that the vector space of those cubics passing through all points of $S$ has dimension greater than the expected dimension $d := \dim C - \#S$, where $C$ is the (finite-dimensional) vector space of all cubics over $\mathbb{F}_q$. By geometrical arguments, he was able to determine some counts for these specific points. A close analysis of these cases then gives linear equations which allowed him to solve the problem of counting points of cubics in $\mathbb{P}^3(\mathbb{F}_q)$.

These ideas lead us to wonder what we could say on the weight enumerator of these types of codes. Of course, this is not an easy problem since the determination of the polynomial is equivalent to giving the point count of hypersurfaces. However, we wanted to use the very geometric definition of those codes on one side, and combine these informations with a powerful tool: Invariant Theory over a polynomial algebra.

Let us recall some basic notions. The general linear group $GL_2(\mathbb{C})$ acts on the polynomial ring $\mathbb{C}[X, Y]$ by linear combination of the variables: a matrix $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C})$ sends $f \in \mathbb{C}[X, Y]$ to $f^g$, where $f^g(X, Y) := f(aX + bY, cX + dY)$. An interesting way of studying the weight enumerator is to the is to compute the group of matrices of $GL_2(\mathbb{C})$ which leaves it invariant.

One of the main applications of this theory is Gleason’s Theorem on classification of self-dual doubly-even codes. This theorem states that if a code is self-dual (the dual of itself) and doubly-even (the weight of all codewords are divisible by 4) then its weight enumerator is in the ring $\mathbb{C}[f, g]$, where
\begin{equation*}
f = X^8 + 14X^4Y^4 + Y^8 \quad \text{and} \quad g = X^4Y^4(X^4 - Y^4)^4.
\end{equation*}

The crucial argument in the proof of this theorem is to observe the two properties we consider give interesting invariants for the weight enumerator of these codes. The
doubly-even condition is equivalent to the fact that the weight enumerator of such a code $C$ is invariant under the transformation

$$W_C(X, Y) = W_C(X, iY).$$

In terms of matrices acting on polynomials, this is the same as saying that $W_C$ is invariant under the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

If a code $C$ is self-dual, MacWilliams’ Theorem states that $W_C$ satisfies the following equation:

$$W_C(X, Y) = \frac{1}{|C|} W_C(X + (q - 1)Y, X - Y).$$

Since $C$ is the dual of itself, it implies that $\dim C = n/2$, and so $|C| = q^{n/2}$. Therefore, since $W_C$ is a homogeneous polynomial of degree $n$, this equation is the same as saying that $W_C$ is invariant under the matrix

$$\frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q - 1 \\ 1 & -1 \end{pmatrix}.$$

Gleason’s Theorem has many interesting consequences. For example, it implies that any self-dual doubly-even code must have a length which is divisible by 8. Furthermore, it gives some important bounds on the minimum distance of such codes. It is with these considerations in mind that we set ourselves to find such invariants for Reed-Muller codes.

As we have already mentioned, the proof of Gleason’s Theorem uses two types of invariants. The first one is the one coming from the doubly-even property. To find such invariants one needs to investigate the so-called divisibility of codes: a code is divisible by some integer $\Delta \geq 1$ if the weight of every codeword is divisible by $\Delta$.

For Reed-Muller codes, the main result concerning divisibility is Ax’s Theorem. This is a general theorem about the number of zeroes of polynomials over finite fields which translates as follows in the language of coding theory.

**Theorem** (Ax, [Ax64]). For any integers $r, m$ and prime power $q = p^r$, the affine Reed-Muller code $R_{n}(r, m)$ is divisible by $q^{\lfloor (m-1)/r \rfloor}$ and this is the largest power of the prime $p$ with this property.
It follows from an easy argument relating the projective and affine zeroes of a homogeneous polynomial that the projective Reed-Muller code $\mathcal{PRM}_{F_q}(r, m)$ is divisible $q^{m/r}$. This implies that the number $N$ of projective zeroes of any homogeneous degree $r$ polynomial $F$ in $m$ variables is of the form

$$N = \#\mathbb{P}^m(F_q) - aq^{m/r} = (q^m + q^{m-1} + \cdots + q + 1) - aq^{m/r},$$

for some integer $a$.

Now, what is this integer $a$? This is a hard question in general. Actually, there is a quite deep geometrical interpretation of this number. For example, in the case of smooth rational surfaces in $\mathbb{P}^3(F_q)$, Weil's trace formula affirms that the number of zeroes of such a surface $X$ in $F_q$ is given by

$$\#X(F_q) = q^2 + q\text{Tr}(\varphi) + 1,$$

where $\text{Tr}(\varphi)$ is the trace of the Frobenius automorphism $\varphi : F_q \to F_q$, $x \mapsto x^q$ seen as a linear endomorphism of the Picard group of $X$, the surface $X$ seen as a variety over $\overline{F_q}$.

Since we are in $\mathbb{P}^3(F_q)$, we can think of a surface as the set of zeroes of a single homogeneous polynomial $f$. This result then implies that the weight of the codeword $c_f$ coming from this polynomial is of the form

$$\text{wt}(c_f) = q^3 + q(1 - \text{Tr}(\varphi)).$$

In conclusion, the weight enumerator of an affine Reed-Muller code $\mathcal{RM}_{F_q}(r, m + 1)$ or of a projective Reed-Muller code $\mathcal{PRM}_{F_q}(r, m)$ is fixed by the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix}, \quad \text{where} \quad \zeta^{q^{m/r}} = 1.$$

The second type of invariants is the one coming from self-duality. Before looking for such invariants in the general case, we give some results about the dual of affine and projective Reed-Muller codes.

A standard property of Reed-Muller codes is the following.

**Theorem.** If $q$ is a prime power and $r, m$ are integers such that $r < m(q - 1)$, then the dual of $\mathcal{RM}_{F_q}(r, m)$ is

$$\mathcal{RM}_{F_q}(r, m)^\perp = \mathcal{RM}_{F_q}(r, m(q - 1) - r - 1).$$
A similar result holds for projective Reed-Muller codes (see Proposition 2.2.3). From this it follows that $\mathcal{RM}_{F_q}(r, m)$ is self dual if and only if $m(q-1) - r - 1 = r$. This can happen only if $q = 2^\nu$ is a power of $2$, if $m$ is odd, and if $r = \frac{m(q-1)-1}{2}$. In the case where $q = 2$, all the self-dual Reed-Muller codes are of the form $\mathcal{RM}_{F_2}(r, 2r + 1)$ and by Ax’s Theorem, all such codes are divisible by $4$, i.e. doubly-even. Hence we can use Gleason’s classification to obtain the weight enumerators. For example, the weight enumerator of $\mathcal{RM}_{F_2}(3, 7)$ is given in Table 1.

<table>
<thead>
<tr>
<th>Weight</th>
<th>Number of codewords</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>128</td>
</tr>
<tr>
<td>16</td>
<td>112</td>
</tr>
<tr>
<td>24</td>
<td>104</td>
</tr>
<tr>
<td>28</td>
<td>100</td>
</tr>
<tr>
<td>32</td>
<td>96</td>
</tr>
<tr>
<td>36</td>
<td>92</td>
</tr>
<tr>
<td>40</td>
<td>88</td>
</tr>
<tr>
<td>44</td>
<td>84</td>
</tr>
<tr>
<td>48</td>
<td>80</td>
</tr>
<tr>
<td>52</td>
<td>76</td>
</tr>
<tr>
<td>56</td>
<td>72</td>
</tr>
<tr>
<td>60</td>
<td>68</td>
</tr>
<tr>
<td>64</td>
<td>5193595576952890822</td>
</tr>
</tbody>
</table>

Table 1: Weight Distribution for $\mathcal{RM}_{F_2}(3, 7)$

For non self-dual Reed-Muller codes, the situation is a little more complicated. Indeed, the goal is to find non-diagonal invariants such as the one given by MacWilliams’ Theorem, and there is no obvious indication on how to proceed. Our approach was to try to find some non-trivial invariants of already known weight enumerators, and see if these can be generalized for other codes. We found the following ones.

**Theorem.** 1. The weight enumerator of $\mathcal{RM}(m-1, m)$ is invariant under the following matrix:

$$
\begin{pmatrix}
  u & u-1 \\
  u-1 & u
\end{pmatrix}, \quad u = \frac{\zeta + 1}{2}, \quad \zeta \text{ is a } 2^m \text{ th root of unity}.
$$
2. The weight enumerator of $\mathcal{RM}(m-2,m)$ is invariant under the following matrix:

$$
\begin{pmatrix}
  u & u-1 \\
  u-1 & u \\
\end{pmatrix}, \quad u = \frac{\zeta + 1}{2}, \quad \zeta \text{ is a } 2^{m-1} \text{'th root of unity.}
$$

The proof of these facts is not so interesting: simple algebraic manipulations on the known weight enumerators give the result. However, in order to find those invariants, one has to look for possible matrix entries which will leave the polynomial invariant. In principle, this can be restated as a finite number of equations and so this problem has a solution. In practice, this is not so easy, and computational times may be long. It is for this reason that we looked for simpler methods.

Since the weight enumerators are homogeneous polynomials in two variables, they cut out a projective variety in $\mathbb{P}^1(\mathbb{C})$. The group $PGL_2(\mathbb{C})$ acts sharply 3-transitively on $\mathbb{P}^1(\mathbb{C})$. In other words, describing an element of $PGL_2(\mathbb{C})$ is the same as picking 3 projective points of $\mathbb{P}^1(\mathbb{C})$ and describing where you want them to go. Since any $g \in GL_2(\mathbb{C})$ leaving a polynomial $f$ invariant induces a $\bar{g} \in PGL_2(\mathbb{C})$ which must leave the projective roots of $f$ globally invariant, this trick reduces a lot the number of potential elements $g \in GL_2(\mathbb{C})$ with this property. Furthermore, this is one of the main steps which allowed us to prove the following theorem on finiteness of stabilizers.

**Theorem.** The stabilizer in $GL_2(\mathbb{C})$ of all weight enumerators $W$ such that $W(X,1)$ has at least 3 roots is finite.

This procedure also gives a way of studying the stabilizer group of some specific polynomials. Using an approximation of the roots given by the software Magma, and an upper bound on the error described in Section 4.5, we get the following theorem.

**Theorem.** The following Reed-Muller codes have trivial stabilizer:

- $\mathcal{RM}_{\mathbb{F}_4}(2,2)$,
- $\mathcal{RM}_{\mathbb{F}_4}(3,2)$,
- $\mathcal{RM}_{\mathbb{F}_5}(2,2)$,
- $\mathcal{PRM}_{\mathbb{F}_5}(3,2)$,
- $\mathcal{PRM}_{\mathbb{F}_5}(5,2)$.

The thesis is divided into four chapters. The first introduces the necessary background. The second chapter explores Evaluation codes and Reed-Muller codes, and gives their main properties. The third chapter is devoted to the study of divisibility of Reed-Muller codes and to the geometrical point of view given by Weil’s trace formula. Finally, in the fourth section we expose the main results about the stabilizer of weight enumerators.
I would like to thank Eva Bayer-Fluckiger for giving me the opportunity to do my project in her group. Also, I would like to thank all members of the group, who were helpful and nice to me.

I warmly thank Martino Borello without whom this project would not be as it is. His unbounded help and support undoubtedly were the key to my salvation.

Finally, I would like to thank Lucie Giesbrecht for her support, my family and friends for their presence, and all my friends from the MA building and beyond for the (coffees) fruitful discussions we shared.
In general, $q$ is a positive power of some prime $p$. The finite field with $q$ elements is denoted $\mathbb{F}_q$. The letter $k$ usually denotes a field, except in Section 1.1 where it is used for the dimension. We write $k[X_1, \ldots, X_m]$ for the polynomial algebra on $m$ variables over $k$. A monomial of $k[X_1, \ldots, X_m]$ is an element of the form $X_1^{e_1} \cdots X_m^{e_m}$, where $e_1, \ldots, e_m$ are non-negative integers (the leading coefficient is one). Except in Section 1.1 where we explicitly use line vectors, we identify any $n$-tuple of elements $(a_1, \ldots, a_n)$ (of some ring, field) with its notation as a column vector

$$a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

so that if $M$ is an $n \times n$ matrix, the notation $Ma$ is well defined.
Chapter 1

Background

1.1 Coding Theory

In this section we introduce basics of Coding Theory and prove MacWilliams’ Theorem, which is a fundamental result for our purposes. For the whole section $q$ is a power of a prime $p$ and $\mathbb{F}_q$ denotes the finite field with $q$ elements. If not specified, $n, k, d$ are positive integers. Since it is common in coding theory to consider line vectors instead of column vectors, we will do so during this section, unless specified otherwise.

1.1.1 Basics

Definition 1.1.1. Let $n$ be a positive integer. A subspace $C$ of the vector space $\mathbb{F}_q^n$ is called a linear code over $\mathbb{F}_q$. The integer $n$ is called the length of the code and the $\mathbb{F}_q$-dimension of $C$ is the dimension of the code. An element of $C$ is called a codeword. If $c \in C$, the weight of $c$ is the value

$$\text{wt}(c) = \#\{j \mid c_j \neq 0\}.$$ 

If $c, c' \in C$ are two codewords, their Hamming distance is the value

$$d(c, c') = \text{wt}(c - c') = \#\{j \mid c_j \neq c'_j\}.$$ 

Finally, the minimum distance, or minimum weight (usually written $d$) is

$$d := \min_{\substack{c \in C \setminus \{0\}}} \text{wt}(c) = \min_{\substack{c, c' \in C \setminus \{0\}}} d(c, c'),$$

the rightmost equality following from the linearity of the code.
Notation 1.1.2. A linear code over $\mathbb{F}_q$ of length $n$, dimension $k$ and minimum distance $d$ is called an $[n, k, d]_q$ code. If the field is clear from the context, the subscript $q$ is omitted.

Remark 1.1.1.1. From the point of view of communication systems, these three parameters are very important to determine how efficient a given code is. Let $C$ be an $[n, k, d]_2$ binary code; think of the codewords as bits which will be sent over a noisy channel, such as an ethernet cable or radio waves. Each time you want to send a piece of information, you will send $n$ bits of data. However, not all these bits carry the information: some redundancy can be added, for example to be able to correct some errors which could have been introduced during transmission.

A good way to understand this quantity is to look at the ratio of the dimension over length: $k/n$. This is called the transmission rate of the code. If this value is close to one, then we are sending a good proportion of useful information in our codewords. Therefore, this value should be made as large as possible.

The other important parameter for error decoding is the minimum distance. If you receive a vector which has potential errors in it, a natural decoding algorithm can be to check all distances to all other codewords and choose the closest codeword as the correct value. This is why a high minimum distance is important: if it is too small then few errors can corrupt the codeword to a point where the redundancy which has been added is no longer enough to fully recover the message. If it is large however, then a lot of errors can occur and the message can still be reconstructed. Since this value also depends on the length, it is common to divide by the length to normalize. The value $d/n$ is then called the relative distance.

Finally, it is important to say that these two values are not independent. For fixed $n$, we have for example the Singleton bound: if $C$ is an $[n, k, d]_q$ code, then

$$k \leq n - d + 1.$$ 

See [MS77, Theorem 11, Chapter 1] for a proof.

Linear codes are quite used in communication systems, because of their algebraic properties. In particular, since they are vector spaces, they can be described by giving a basis, which is usually encoded in a matrix.

Definition 1.1.3. If $C \subset \mathbb{F}_q^n$ is a code, a generator matrix for $C$ is a matrix $G$ with coefficients in $\mathbb{F}_q$ such that its rows form a basis for $C$. 
If $G$ is a generator matrix for $\mathcal{C}$, we simply have

$$\mathcal{C} = \{xG \mid x = (x_1, \ldots, x_k) \in \mathbb{F}_q^k\}.$$ 

We now explore various transformations which can be applied to linear codes. We want these transformations to preserve the basic properties of the code (length, dimension) but also its weight distribution. This leads to the following definition.

**Definition 1.1.4.** The symmetric group $S_n$ on $n$ elements acts on $\mathbb{F}_q^n$ by permuting the coordinates. Such a transformation is called a **permutation** of $\mathbb{F}_q^n$.

A **monomial transformation** of $\mathbb{F}_q^n$ is a permutation composed by a transformation of the following form:

$$\mathbb{F}_q^n \to \mathbb{F}_q^n$$

$$(x_1, \ldots, x_n) \mapsto (\lambda_1 x_1, \ldots, \lambda_n x_n)$$

for $\lambda_1, \ldots, \lambda_j \in \mathbb{F}_q^\times$. In other words, it is a permutation together with a multiplication by a non-zero scalar in each coordinate.

Let $\mathcal{C}, \mathcal{C}' \subset \mathbb{F}_q^n$ be linear codes. We say that $\mathcal{C}$ and $\mathcal{C}'$ are **permutation equivalent** (resp. **monomially equivalent**) if $\mathcal{C}'$ can be obtained by applying a permutation (resp. monomial transformation) to $\mathcal{C}$.

The **permutation** (resp. **monomial** automorphism group) of a linear code $\mathcal{C}$, denoted $\text{PAut}(\mathcal{C})$ (resp. $\text{MAut}(\mathcal{C})$) is the group of all permutations (resp. monomial transformations) which send $\mathcal{C}$ into itself.

It is easy to check that these notions of equivalences are indeed equivalence relations and that they preserve the weight of each codewords. In fact, we even have the following counterpart:

**Theorem 1.1.5.** Let $\mathcal{C}, \mathcal{C}'$ be linear codes, and let $g \in GL_n(\mathbb{F}_q)$ be a linear transformation such that $\mathcal{C}g := \{cg \mid c \in \mathcal{C}\} = \mathcal{C}'$. Suppose that for any $c \in \mathcal{C}$, $\text{wt}(cg) = \text{wt}(c)$. Then there exists a monomial transformation $M$ such that

$$M(c) = cg \quad \forall c \in \mathcal{C}.$$ 

See [HP03, Theorem 7.9.4] for a proof.
The vector space \( \mathbb{F}_q^n \) can be endowed with the following scalar product:

\[
\langle \cdot, \cdot \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q \\
(x, y) \longmapsto \sum_{j=1}^n x_j y_j.
\]

This allows us to make the following definition.

**Definition 1.1.6.** Let \( C \subseteq \mathbb{F}_q^n \) be a linear code. The **dual** of \( C \), written \( C^\perp \) is the linear code

\[
C^\perp := \{ x \in \mathbb{F}_q^n \mid \langle x, y \rangle = 0 \ \forall y \in C \}.
\]

The code \( C \) is **self-orthogonal** if \( C \subseteq C^\perp \) and **self-dual** if \( C = C^\perp \).

Observe that by easy Linear Algebra, if \( C \) is an \([n, k, d]_q\) code, then

\[
\dim C^\perp = n - k.
\]

In particular, if \( C \) is self-dual, then \( k = \dim C = \dim C^\perp = n/2 \).

Besides the dimension, length and minimum distance, there is another very important object associated to a code.

**Definition 1.1.7.** If \( C \subset \mathbb{F}_q^n \) is a code, the **weight enumerator** of \( C \) is the homogeneous polynomial

\[
W_C(X, Y) = \sum_{c \in C} X^{n - \mathrm{wt}(c)} Y^{\mathrm{wt}(c)} = \sum_{i=0}^n A_i X^{n-i} Y^i,
\]

where

\[
A_i := \# \{ c \in C \mid \mathrm{wt}(c) = i \}.
\]

This polynomial is a convenient way to encode all weights of a given code. Since the weight of the codewords are preserved under equivalence of codes, two equivalent code have the same weight enumerator.

We now discuss cyclicity.

**Definition 1.1.8.** A linear code \( C \) is **cyclic** if \( \text{PAut}(C) \) contains a cycle of order \( n \).

With this definition, it is clear that cyclicity is preserved under permutation equivalence. Hence, upon permuting the coefficients, a code \( C \subset \mathbb{F}_q^n \) is cyclic if and only if for any codeword \( c = (c_0, \ldots, c_{n-1}) \in C \), the codeword

\[
c' := (c_{n-1}, c_1, \ldots, c_{n-1})
\]
is also in $C$. This justifies the terminology.

Now there is a third way of seeing cyclicity, which is the most important. Observe that there is an isomorphism of vector spaces

$$F_q^n \rightarrow F_q[X]/(X^n - 1)$$

$$(a_0, \ldots, a_{n-1}) \mapsto \sum_{j=0}^{n-1} a_j X^j.$$

Thus we can see any linear code $C$ as a subspace of $F_q[X]/(X^n - 1)$.

This gives an equivalent formulation of cyclicity: a linear code $C$ is cyclic if and only if, upon permuting the coordinates, the code $C$ is an ideal of $F_q[X]/(X^n - 1)$. This assertion follows easily from the fact that $C$ is an ideal of $F_q[X]/(X^n - 1)$ if and only if $X^C \subset C$.

Now since $F_q[X]$ is a P.I.D., so is $F_q[X]/(X^n - 1)$ and thus all its ideals are generated by a single element.

**Definition 1.1.9.** Let $C \subset F_q^n$ be a linear cyclic code. Then a **generator polynomial** for $C$ is a polynomial $g \in F_q[X]$ such that the image of $g$ in the quotient $F_q[X]/(X^n - 1)$ generates $C$ as an ideal.

Observe that since cyclicity is only defined upon permutation of the coefficients, there might be more than one generator polynomial if there is more than one permutation which make $C$ into an ideal of $F_q[X]/(X^n - 1)$.

However, for each such permutation, there is a unique choice of generator polynomial which is monic and of degree $\leq n - 1$.

Finally, we present the notion of divisibility which will be useful in Chapter 3.

**Definition 1.1.10.** A linear code $C$ is said to be **divisible** by some integer $\Delta \geq 1$ if all its weights are divisible by $\Delta$. A code is **even** if it is divisible by 2 and **doubly-even** if it is divisible by 4.

### 1.1.2 MacWilliams’ Theorem

Let $C$ be an $[n, k, d]_q$ code. From a theoretical point of view, the dual code $C^\perp$ is completely determined by $C$. More precisely, if we know $C$, we can compute $C^\perp$ and all its properties. However, if we don’t know $C$ explicitly, but only some limited informations
about it (for example: the dimension, the minimum distance) it is interesting to ask which properties we can deduce from the dual.

Suppose that only the parameters \([n, k, d]\) of the code \(C\) are known. Then it is clear that the length of \(C^\perp\) is still \(n\), and that

\[
\dim C^\perp = n - k.
\]

However for the minimum distance, this knowledge is not enough: there are codes with same length, dimension and minimum distance, but which have duals with different minimum distances. An easy example is the following: Let \(C_1, C_2\) be the two \([3, 2, 1]\) codes given by the generator matrices \(G_1, G_2\) defined as

\[
G_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}.
\]

Their duals \(C_1^\perp\) and \(C_2^\perp\) are simply

\[
C_1^\perp = \{(0, 0, 0), (0, 0, 1)\} \quad C_2^\perp = \{(0, 0, 0), (0, 1, 1)\},
\]

and as one readily sees, \(C_1^\perp\) is a \([3, 1, 1]\) code, while \(C_2^\perp\) is a \([3, 1, 2]\) code. Thus it is not possible to determine the minimum distance of the dual of a code, only by knowing its parameters.

The same question holds for the weight enumerator of a code: if the weight enumerator of some code \(C\) is known, is it enough to fully determine the weight enumerator of \(C^\perp\)? The beautiful theorem of MacWilliams gives a positive answer to this question.

**Theorem 1.1.11** (MacWilliams, [MS77, Chap. 5, §6, Theorem 13]). Let \(C\) be a code over \(\mathbb{F}_q\) and let \(C^\perp\) denote its dual. Let \(W_C\) and \(W_{C^\perp}\) denote the weight enumerator of \(C\) and \(C^\perp\), respectively. Then

\[
W_{C^\perp}(X, Y) = \frac{1}{|C^\perp|} \cdot W_C(X + (q - 1)Y, X - Y).
\]

An important corollary is the following.

**Corollary 1.1.12.** If \(C\) is a self-dual code, then \(W_C\) is invariant under the transformation

\[
X \mapsto \frac{X + (q - 1)Y}{\sqrt{q}}, \quad Y \mapsto \frac{X - Y}{\sqrt{q}}.
\]
Proof. Since \( W_C \) is a homogeneous polynomial of degree \( n \), and since \( |C| = q^{n/2} \), we have

\[
\frac{1}{|C|} \cdot W_C(X + (q - 1)Y, X - Y) = W_C\left(\frac{X + (q - 1)Y}{\sqrt{q}}, \frac{X - Y}{\sqrt{q}}\right).
\]

This corollary will be useful in the following sections. The rest of this section is devoted to the proof of MacWilliams' Theorem.

First, we need a general lemma about characters.

**Lemma 1.1.13.** Let \( G \) be a finite group, \([G,G]\) its commutator subgroup and let \( \hat{G} \) denote its character group \( \hat{G} := \text{Hom}(G, \mathbb{C}^\times) \).

Then

\( \hat{G} \cong G/[G,G] \).

In particular, if \( G \) is abelian then \( \hat{G} \cong G \).

Proof. Suppose first that \( G \) is cyclic, say of order \( n \). If \( \zeta := e^{2\pi i/n} \) and \( Z := \langle \zeta \rangle \leq \mathbb{C}^\times \), then \( G \cong Z \) so it is enough to show that \( \hat{G} \cong Z \).

Let \( g \) be a generator of \( G \), and let \( \text{ev}_g : \hat{G} \to \mathbb{C}^\times \) denote the evaluation at \( g \). Any homomorphism \( f \in \hat{G} \) sends \( g \) to an element \( \alpha \in \mathbb{C}^\times \) of order dividing \( n \). These elements are exactly the solutions to the equation

\[
X^n = 1
\]

in \( \mathbb{C} \), which are given by \( \{1, \zeta, \ldots, \zeta^{n-1}\} \). Therefore \( \alpha = \zeta^s \) for some power \( s \), and \( \text{ev}_g \) corestricts to \( Z \). We claim that \( \text{ev}_g | Z \) is an isomorphism.

Clearly, for any integer \( s \), we can define a homomorphism \( f \in \hat{G} \) which sends \( g \) to \( \zeta^s \), and hence any power \( g^t \) to \( \zeta^{st} \). This shows that \( \text{ev}_g | Z \) is surjective. Moreover, if \( f, f' \in \hat{G} \) have the same value at \( g \), then, since any \( g' \in G \) can be written as \( g' = g^t \) (for some \( t \geq 0 \)) we have

\[
f(g') = f(g^t) = f(g)^t = f'(g)^t = f'(g'),
\]

so \( f \) and \( f' \) are equal. Hence \( \text{ev}_g | Z \) is injective, whence bijective, as desired.

Now suppose that \( G \) is finite abelian. Then \( G \) is isomorphic to a product of cyclic groups, say \( G \cong C_{n_1} \times \cdots \times C_{n_r} \). Thus

\[
\hat{G} \cong \text{Hom}\left(\prod_{j=1}^{r} C_{n_j}, \mathbb{C}^\times\right) \cong \prod_{j=1}^{r} \text{Hom}(C_{n_j}, \mathbb{C}^\times) \cong \prod_{j=1}^{r} C_{n_j} \cong G
\]
by the previous case.

Finally suppose $G$ is arbitrary and let $f \in \hat{G}$. Since $\text{im } f$ is abelian, $f([G,G]) = 1$ so $f$ induces a homomorphism

$$
\bar{f} : G/[G,G] \to \mathbb{C}^\times.
$$

Now the map sending $f \in \hat{G}$ to $\bar{f} \in \text{Hom}(G/[G,G],\mathbb{C}^\times)$ is clearly an isomorphism of groups (its inverse is given by precomposing $\bar{f}$ with the projection $G \twoheadrightarrow G/[G,G]$). Therefore,

$$
\hat{G} \cong \text{Hom}(G/[G,G],\mathbb{C}^\times) \cong G/[G,G]
$$

as desired. \hfill \square

The key idea of the proof of MacWilliams’ Theorem is to see the code simply as a subgroup of the group $\mathbb{F}_q^n$, and to apply the so-called technique of Discrete Poisson Summation.

**Lemma 1.1.14** (Discrete Poisson Summation). Let $G$ be a finite abelian group, $H \leq G$. Let $\hat{G} := \text{Hom}(G,\mathbb{C}^\times)$ be the character group, and $H^* := \{ f \in \hat{G} \mid \ker f \subset H \}$. If $\varphi : G \to V$ is a function to an arbitrary $\mathbb{C}$-vector space $V$, write $\hat{\varphi} : \hat{G} \to V$ for its Fourier transform given by

$$
\hat{\varphi}(f) = \sum_{g \in G} f(g) \varphi(g)
$$

for $f \in \hat{G}$. Then the following formula holds:

$$
[G : H] \sum_{h \in H} \varphi(h) = \sum_{f \in H^*} \hat{\varphi}(f).
$$

**Proof.** Since

$$
\sum_{f \in H^*} \hat{\varphi}(f) = \sum_{f \in H^*} \sum_{g \in G} f(g) \varphi(g) = \sum_{g \in G} \varphi(g) \sum_{f \in H^*} f(g),
$$

it is enough to show that for any $g \in G$

$$
\sum_{f \in H^*} f(g) = \begin{cases} [G : H] & g \in H \\ 0 & g \notin H. \end{cases}
$$

Suppose first that $H = \{1\}$. Then we need to show that for any $g \in G$

$$
\sum_{f \in \hat{G}} f(g) = \begin{cases} |G| & g = 1 \\ 0 & g \neq 1. \end{cases}
$$
If \( g = 1 \), then
\[
\sum_{f \in \hat{G}} f(g) = \sum_{f \in \hat{G}} f(1) = |\hat{G}|.
\]

By Lemma 1.1.13, \( \hat{G} \cong G \), so \(|\hat{G}| = |G|\).

Now if \( g \neq 1 \), let \( \text{ev}_g : \hat{G} \to \mathbb{C}^\times \) be the evaluation at \( g \). It is a group homomorphism, so it induces an isomorphism
\[
\hat{G} / \ker(\text{ev}_g) \cong \text{im}(\text{ev}_g).
\]

This implies
\[
\sum_{f \in \hat{G}} f(g) = \sum_{f \in \hat{G}} \text{ev}_g(f) = |\ker(\text{ev}_g)| \sum_{f \in \hat{G} / \ker(\text{ev}_g)} \text{ev}_g(f) = |\ker(\text{ev}_g)| \sum_{\alpha \in \text{im}(\text{ev}_g)} \alpha.
\]

But \( \text{im}(\text{ev}_g) \) is a finite subgroup of \( \mathbb{C}^\times \) so it is cyclic.

We claim that this is not the trivial group. To show this, we must construct a homomorphism \( f : G \to \mathbb{C}^\times \) which is different from 1 on \( g \). Let \( G \cong C_{n_1} \times \cdots \times C_{n_r} \) be the decomposition of \( G \) into cyclic groups. If \( g \) corresponds to \( (g_1, \ldots, g_r) \), then since \( g \) is non-zero, there is some \( g_j \) which is non-zero. Let \( h_j \) be a generator of \( C_{n_j} \), and define \( f \) to be the composite
\[
\begin{align*}
f : G & \xrightarrow{\cong} C_{n_1} \times \cdots \times C_{n_r} \xrightarrow{\text{projection}} C_{n_j} \xrightarrow{\cong} \langle e^{2\pi i/n_j} \rangle \xrightarrow{\cong} \mathbb{C}^\times, 
\end{align*}
\]

where the rightmost isomorphism sends \( h_j \) to \( e^{2\pi i/n_j} \). If \( g_j = h_j^\alpha \), then it is clear that \( f(g) = e^{2\pi i \cdot (\alpha/n_j)} \neq 0 \). Thus \( f \) is not trivial on \( g \), and \( \text{im}(\text{ev}_g) \) is not trivial.

But if \( \text{im}(\text{ev}_g) \) is not trivial, it is generated by some \( z \in \mathbb{C} \) of module 1, with \( z \neq 1 \). Thus,
\[
\sum_{\alpha \in \text{im}(\text{ev}_g)} \alpha = \sum_{j=0}^{\lfloor \text{im}(\text{ev}_g) \rfloor - 1} z^j = \frac{z^{\lfloor \text{im}(\text{ev}_g) \rfloor} - 1}{z - 1} = 0,
\]

and the special case \( H = \{1\} \) is proved.

Now if \( H \neq \{1\} \), observe that any \( f \in H^* \) contains \( H \) in its kernel, and therefore induces a homomorphism \( \bar{f} : G/H \to \mathbb{C}^\times \). Conversely, any homomorphism \( \tilde{f} : G/H \to \mathbb{C}^\times \) can be precomposed with the projection \( G \to G/H \) to give a homomorphism \( f : G \to \mathbb{C}^\times \).

It is easy to see that these maps are inverses and induce an isomorphism
\[
H^* \cong \text{Hom}(G/H, \mathbb{C}^\times).
\]
Applying the previous case to $G/H$, we see that for any $g \in G$, if $\bar{g}$ denotes the image of $g$ in $G/H$,

$$\sum_{f \in H^*} \overline{f(g)} = \sum_{f \in \text{Hom}(G/H, \mathbb{C}^\times)} \overline{f(\bar{g})} = \begin{cases} |\text{Hom}(G/H, \mathbb{C}^\times)| & \bar{g} = 1 \\ 0 & \bar{g} \neq 1 \end{cases} = \begin{cases} [G : H] & g \in H \\ 0 & g \notin H \end{cases},$$

as desired. \qed

Now we are ready to prove MacWilliams’ Theorem.

**Proof of Theorem 1.1.11.** Since the dual of the dual of a code is the code itself, it is enough to show that

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

Assume $C \subset \mathbb{F}_q^n$. We apply Discrete Poisson Summation to the following data. We take $G = \mathbb{F}_q^n$, $H = C \leq G$, and $\varphi : G \to \mathbb{C}[X, Y]$ as

$$\varphi(g) = X^{n-\text{wt}(g)}Y^{\text{wt}(g)}.$$

We construct a special isomorphism between $G$ and $\hat{G}$. Let $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be any fixed non-trivial character. We define $\Psi : G \to \hat{G}$ by the formula

$$\Psi(g)(h) := \psi(\langle g, h \rangle) \quad \forall g, h \in G.$$

This map is injective: suppose $\Psi(g) \in \hat{G}$ is the trivial map. Since $\psi$ is non-trivial, there is some $a \in \mathbb{F}_q$ with $\psi(a) \neq 1$. If $g \neq 0$, $g_i \neq 0$ for some $i$ and we have

$$\langle g, (0, \ldots, 0, \underbrace{g_i^{-1}a}_{i}, 0, \ldots, 0) \rangle = g_i g_i^{-1}a = a,$$

so applying $\psi$ to this expression is different from 1. Therefore $g = 0$ and $\Psi$ is injective. But we proved in Lemma 1.1.13 that the two groups are isomorphic, and hence in particular they have the same number of elements. So $\Psi$ must be an isomorphism; in what follows we identify $G$ with $\hat{G}$ by means of this.

With this notation, we have

$$H^* = \{ g \in G \mid \forall h \in C, \psi(\langle g, h \rangle) = 1 \} = \{ g \in G \mid \forall h \in C, \langle g, h \rangle = 0 \} = C^\perp,$$

and hence $[G : H] = |\mathbb{F}_q^n/C| = |C^\perp|$. 

Observe that for \( h \in H^* = C^\perp \), if \( \textbf{1} \) denotes the indicator function, we have

\[
\hat{\varphi}(h) = \sum_{g \in G} \varphi(g) \psi(\langle g, h \rangle) = \sum_{g_1, \ldots, g_n \in \mathbb{F}_q} \prod_{i=1}^n X^{1-\textbf{1}(g_i \neq 0)} \psi(g_i h_i)
\]

\[
= \prod_{i=1}^n \sum_{a \in \mathbb{F}_q^*} X^{1(a=0)} Y^{1(a \neq 0)} \psi(g_i h_i)
\]

\[
= \prod_{i=1}^n \left( X + Y \sum_{a \in \mathbb{F}_q^*} \psi(ah_i) \right).
\]

If \( h_i \neq 0 \) on the sum on the right, then a change of variable gives

\[
\sum_{a \in \mathbb{F}_q^*} \psi(ah_i) = \sum_{b \in \mathbb{F}_q^*} \psi(b) = \sum_{b \in \mathbb{F}_q^*} \psi(b) - 1.
\]

As before, the sum \( \sum_{b \in \mathbb{F}_q^*} \psi(b) \) is the sum of all elements in \( \text{im}(\psi) \), each taken with multiplicity \( |\ker(\psi)| \). But since \( \psi \) is non-trivial, \( \text{im}(\psi) \) is a non-trivial subgroup of \( C^\times \), and is therefore cyclic and generated by some \( z \neq 1 \). Thus, we get

\[
\sum_{b \in \mathbb{F}_q^*} \psi(b) = |\ker(\psi)| \sum_{\alpha \in \text{im}(\psi)} \alpha = |\ker(\psi)| \sum_{i=0}^{\text{im}(\psi)-1} z^i = |\ker(\psi)| \frac{z^{\text{im}(\psi)} - 1}{z - 1} = 0,
\]

and hence

\[
\sum_{a \in \mathbb{F}_q^*} \psi(ah_i) = -1.
\]

If \( h_i = 0 \) however, the sum is simply \( \sum_{\mathbb{F}_q^*} 1 = |\mathbb{F}_q^*| = (q - 1) \). Defining \( \theta : G \to C \) by

\[
\theta(g) = \begin{cases} 
  q - 1 & g = 0 \\
  -1 & g \neq 0,
\end{cases}
\]

we get

\[
\hat{\varphi}(h) = \prod_{i=1}^n \left( X + \theta(h_i) Y \right)
\]

\[
= \prod_{h_i = 0} \left( X + (q - 1) Y \right) \cdot \prod_{h_i \neq 0} \left( X + (-1) Y \right)
\]

\[
= \left( X + (q - 1) Y \right)^{n-\text{wt}(h)} \left( X - Y \right)^{\text{wt}(h)}.
\]

Finally, replacing \( \varphi \) and \( \hat{\varphi} \) in the formula for Discrete Poisson Summation, we get

\[
|C^\perp| \sum_{c \in C} X^{n-\text{wt}(c)} Y^{\text{wt}(c)} = \sum_{c' \in C^\perp} \left( X + (q - 1) Y \right)^{n-\text{wt}(c')} \left( X - Y \right)^{\text{wt}(c')}
\]

and the result follows.
1.2 Invariant Theory

1.2.1 Basics

In this section, we introduce some notions of Invariant Theory over a polynomial algebra. Let $k$ be any field and let $k[X_1, \ldots, X_m]$ denote the polynomial ring over $k$ in $m$ variables. As before, we identify any $n$-tuple $(a_1, \ldots, a_n)$ with its column notation, to be able to multiply on the left with an $n \times n$ matrix.

The group $GL_m(k)$ acts on $k[X_1, \ldots, X_m]$ by linear combination on the unknowns:

$$f^g(X_1, \ldots, X_m) := f(g(X_1, \ldots, X_m)), \quad \forall f \in k[X_1, \ldots, X_m], g \in GL_m(k).$$

Thus, so does every subgroup $G \leq GL_m(k)$.

**Definition 1.2.1.** If $G \leq GL_m(k)$ is a group, then the invariant ring of $G$, denoted $k[X_1, \ldots, X_m]^G$, is the ring of elements in $k[X_1, \ldots, X_m]$ fixed by $G$:

$$k[X_1, \ldots, X_m]^G := \{ f \in k[X_1, \ldots, X_m] \mid f^g = f \ \forall g \in G \}.$$

It follows from the definition of the action that this is indeed a ring, and even a $K$-algebra. Conversely, if $S \subset k[X_1, \ldots, X_m]$ is a set of polynomials, the stabilizer of $S$ in $G$ is

$$\text{Stab}_G(S) := \{ g \in G \mid f^g = f \ \forall f \in S \}.$$

There are two natural questions to ask.

1. For fixed $G \leq GL_m(k)$, what is the shape of $k[X_1, \ldots, X_m]^G$?

2. For fixed $S \subset k[X_1, \ldots, X_m]$, what is the shape of $\text{Stab}_G(S)$?

In what follows, we will give some theorems which tend to answer the first question. For the second one, we will show in section Section 4.5 that $\text{Stab}_G(S)$ may be trivial, even if $S$ consists of one polynomial.

The first main theorem tells valuable information about the invariant ring of a finite group over $\mathbb{C}$.

**Theorem 1.2.2 (Noether).** Let $G \leq GL_m(\mathbb{C})$ be a finite group, of order $n$. Then the invariant ring $\mathbb{C}[X_1, \ldots, X_m]^G$ is generated as a $\mathbb{C}$-algebra by $\leq \binom{n+m}{m}$ homogeneous
elements of degree \( \leq n \). In other words, there exist homogeneous elements \( f_1, \ldots, f_r \) in \( \mathbb{C}[X_1, \ldots, X_m]^G \) of degree at most \( n \), with \( r \leq \binom{n+m}{m} \) such that

\[
\mathbb{C}[X_1, \ldots, X_m]^G = \mathbb{C}[f_1, \ldots, f_r].
\]

A proof can be found in [RS98].

Now we know that over \( \mathbb{C} \), the invariants of a finite group form a finitely generated algebra. In fact, we can be more precise about the shape of these invariants. For this we need a definition.

**Definition 1.2.3.** Polynomials \( f_1, \ldots, f_s \) in \( m \) variables over a field \( k \) are said to be **algebraically dependent** if there is a polynomial \( p \) in \( s \) variables such that

\[
p(f_1, \ldots, f_s) = 0.
\]

The polynomials are said to be **algebraically independent** otherwise.

We set ourselves again in the situation of a finite group acting on polynomials over \( \mathbb{C} \).

**Theorem 1.2.4.** Let \( G \leq GL_m(\mathbb{C}) \) be a group. Then there exists \( m \) but not \( m+1 \) algebraically independent elements of \( \mathbb{C}[X_1, \ldots, X_m]^G \). In other words, the transcendence degree over \( \mathbb{C} \) of the field of fractions of \( \mathbb{C}[X_1, \ldots, X_m]^G \) is \( m \).

**Proof.** See [RS98] Theorem 18. \( \square \)

The second theorem has an interesting corollary.

**Theorem 1.2.5** (Noether Normalization Theorem). Let \( R \) be a finitely generated entire \( k \)-algebra (\( k \) a field). Suppose that the field of fractions of \( R \) has transcendence degree \( r \) over \( k \). Then there are \( r \) elements \( f_1, \ldots, f_r \) in \( R \) such that \( R \) is integral over \( k[f_1, \ldots, f_r] \).

**Proof.** See [Lan02] Chap. VIII, §2. \( \square \)

**Corollary 1.2.6.** Let \( G \leq GL_m(\mathbb{C}) \) be a finite group and let \( R = \mathbb{C}[X_1, \ldots, X_m]^G \). Then there exist elements \( f_1, \ldots, f_m \in R \).
such that $R$ is a finitely generated $\mathbb{C}[f_1, \ldots, f_m]$-module. In other words, there exists polynomials $g_1, \ldots, g_t \in R$ such that every $h \in R$ can be written

$$h = \sum_{i=1}^{t} g_ip_i(f_1, \ldots, f_m)$$

for some polynomials $p_1, \ldots, p_t$ of $m$ variables over $\mathbb{C}$.

**Proof.** By Theorem 1.2.2, $R$ is a finitely generated $\mathbb{C}$-algebra. Moreover, by Theorem 1.2.4 the fraction field of $R$ has transcendence degree $m$ over $\mathbb{C}$. Therefore, the theorem applies and $R$ is integral over $\mathbb{C}[f_1, \ldots, f_m]$ for some $f_1, \ldots, f_m \in R$. Since $R$ is a finitely generated $\mathbb{C}[f_1, \ldots, f_m]$-algebra, this implies that $R$ is finitely generated as a $\mathbb{C}[f_1, \ldots, f_m]$-module (see [Lan02, Proposition 1.2]).

**Definition 1.2.7.** Let $G \leq GL_m(k)$ be a group. A maximal subset of algebraically independent polynomials in $k[X_1, \ldots, X_m]^G$ is called a set of **primary invariants**. If \{f_1, \ldots, f_s\} are primary invariants, a set \{g_1, \ldots, g_t\} of polynomials in $k[X_1, \ldots, X_m]^G$ is called a set of **secondary invariants** if any $h \in k[X_1, \ldots, X_m]^G$ can be written

$$h = \sum_{i=1}^{t} g_ip_i(f_1, \ldots, f_m)$$

for some polynomials $p_1, \ldots, p_t$ of $r$ variables.

In the case of a finite group $G$ acting on polynomials over the field $k = \mathbb{C}$, the existence of primary and secondary invariants is assured by Corollary 1.2.6. This is a very useful description of the invariants of the group.

**1.2.2 Molien series**

Let $G \leq GL_m(\mathbb{C})$ be a finite group and let $R = \mathbb{C}[X_1, \ldots, X_m]^G$. We have just seen in the previous section that the ring of invariants $R$ admits primary and secondary invariants, which permit us to completely determine its structure. We expose a convenient way to quantify the “number” of elements in the invariant ring.

By Theorem 1.2.2 we know that there are homogeneous polynomials $f_1, \ldots, f_r$ such that

$$R = \mathbb{C}[f_1, \ldots, f_r].$$
Now for a fixed degree $d$, we let $\Lambda_d$ be the vector space of homogeneous degree $d$ polynomials which are invariant under $G$:

$$\Lambda_d := \{ f \in R \mid f \text{ homogeneous of degree } d \}.$$ 

It is clear that $\Lambda_d$ is spanned over $\mathbb{C}$ by the finite set

$$\{ f^{e_1} \cdots f^{e_r} \mid \sum e_j \deg(f_j) = d \}.$$ 

Hence all $\Lambda_d$ are finite dimensional; let $a_d := \dim \Lambda_d$.

**Definition 1.2.8.** The series

$$\Phi_G(\lambda) = \sum_{d=0}^{\infty} a_d \lambda^d$$

is called the **Molien series** of the group $G$.

This can be seen as a formal series (which is equivalent to seeing it as a sequence of integers $a_d$), but in our case we can prove that it is absolutely convergent for all complex $\lambda$ with sufficiently small module. This will not be useful in what follows, but it justifies the notation of the infinite sum.

Very crude approximation assure absolute convergence for all $\lambda$ with $|\lambda| < 1/e$. Indeed, since $\Lambda_d$ is a subspace of all polynomials of degree $d$, standard bounds on binomial coefficients give

$$a_d = \dim \Lambda_d \leq \# \{ \text{monomials of degree } d \} \leq \binom{m+d}{d} \leq \left( \frac{(m+d)e}{d} \right)^d.$$ 

Now since $\Phi_G$ is a power series, it admits a radius of convergence defined as

$$\rho := \liminf_{d \to \infty} |a_d|^{-1/d},$$

which ensures that for any $\lambda$ with $|\lambda| < \rho$, the series $\Phi_G(\lambda)$ will converge.

But clearly,

$$\liminf_{d \to \infty} |a_d|^{-1/d} \leq \liminf_{d \to \infty} \left( \frac{(m+d)e}{d} \right)^{-d/d} = \liminf_{d \to \infty} \frac{d}{(m+d)e} = 1/e.$$ 

The main application of this series is the following.

**Theorem 1.2.9** (Molien). Let $G \leq GL_m(\mathbb{C})$ be a finite group of order $n$. Then

$$\Phi_G(\lambda) = \frac{1}{n} \sum_{g \in G} \frac{1}{\det(I - \lambda g)}$$

*Proof.* See [RS98, Theorem 10].
1.2.3 An application to self-dual doubly-even codes

We show how Molien’s Theorem can be applied to determine the shape of some weight enumerator. Let \( \mathcal{C} \subseteq \mathbb{F}_2^n \) be a linear code over \( \mathbb{F}_2 \). We assume that \( \mathcal{C} \) is self-dual (i.e. \( \mathcal{C}^\perp = \mathcal{C} \)) and doubly-even (i.e. all weights of \( \mathcal{C} \) are divisible by 4).

Let \( W_\mathcal{C}(X, Y) \) denote the weight enumerator of \( \mathcal{C} \). Since \( \mathcal{C} \) is self-dual, MacWilliams’ Theorem gives

\[
W_{\mathcal{C}}(X, Y) = W_{\mathcal{C}^\perp}(X, Y) = 2^{-n/2} \cdot W_{\mathcal{C}}(X + Y, X - Y) = W_{\mathcal{C}} \left( \frac{X + Y}{\sqrt{2}}, \frac{X - Y}{\sqrt{2}} \right),
\]

since \( W_{\mathcal{C}} \) is a homogeneous polynomial of degree \( n \). In terms of invariants, this is the same that saying that \( W_{\mathcal{C}} \) is invariant under the transformation

\[
g = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.
\]

Moreover, the condition on the weights translates easily as an invariant of the weight enumerator: it is equivalent to say that all powers of \( W_{\mathcal{C}} \) are divisible by 4. In other words, \( W_{\mathcal{C}} \) is invariant under the transformation

\[
h = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.
\]

Set \( G = \langle g, h \rangle \). Then this implies that

\[
W_{\mathcal{C}} \in \mathbb{C}[X, Y]^G.
\]

We study \( G \) in order to compute its associated Molien series.

**Lemma 1.2.10.** The group \( G \) has order 192, and consists of matrices of the form

\[
M_1(\eta, \alpha) := \eta \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}, \quad M_2(\eta, \alpha) := \eta \begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix},
\]

and \( M_3(\eta, \alpha, \beta) := 2^{-1/2} \eta \begin{pmatrix} 1 & \beta \\ \alpha & -\alpha \beta \end{pmatrix} \)

for complex numbers satisfying \( \alpha^4 = 1, \beta^4 = 1, \eta^8 = 1 \).
Proof. This is section 6.2 in [RS98]. We prove only the fact that the order is 192, a proof which comes from [BE72].

First, observe that

\[(gh)^3 = \eta \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \eta = \frac{i+1}{\sqrt{2}} \text{ an 8th root of unity.}\]

Thus, the subgroup \(\langle (gh)^3 \rangle\) is normal in \(G\).

Let \(S_n\) denote the symmetric group on \(n\) elements; set \(\sigma = (12)\) and \(\tau = (1 \ldots n)\). Then \(S_n\) has the following presentation:

\[S_n = \langle \sigma, \tau \mid \tau^n = (\sigma \tau)^{n-1}, \sigma^2 = (\sigma \tau^{-j} \sigma \tau)^2 = 1 \ (2 \leq j \leq n/2) \rangle.\]

In the case of \(S_4\) we claim that this reduces to

\[S_4 = \langle \sigma^2 = \tau^4 = (\sigma \tau)^3 = 1 \rangle.\]

Indeed, from the first relations, we get \(\sigma^2 = 1\) and \(\tau^4 = (\sigma \tau)^3\). But we know that \(\tau^4 = 1\), so the first presentation implies the second. To show the converse, since \(\tau^2 = \tau^{-2}\), we only need to show that \((\sigma \tau^2 \sigma \tau^2)^2 = 1\) starting from our presentation. We have

\[\sigma \tau^2 = (\sigma \tau) \tau = \tau^{-1} \sigma \tau^{-1} \sigma \tau\]

which is a conjugate of \(\tau^{-1}\). Thus their order are equal and we have

\[(\sigma \tau^2 \sigma \tau^2)^2 = (\sigma \tau^2)^4 = 1\]

as desired.

Now observe that neither \(h\), \(h^2\) nor \(g\) are in \(\langle (gh)^3 \rangle\). Therefore, the images of \(g\) and \(h\) in \(G/\langle (gh)^3 \rangle\) have order 2 and 4 respectively, and their product is of order 3. But this quotient is clearly generated by those two images, and they have the exact same shape as our presentation of \(S_4\). Thus

\[G/\langle (gh)^3 \rangle \cong S_4,\]

and this group is of order 24. But since \((gh)^3 = \eta \text{id}\) and \(\eta^8 = 1\), the group \(\langle (gh)^3 \rangle\) is of order 8 and thus \(|G| = 8 \cdot 24 = 192.\]

We now compute the Molien series of \(G\) using Molien’s Theorem. We first compute the determinant of matrices of the form \(M_1, M_2, M_3\). Fix \(\eta, \alpha, \beta\) as in the lemma. We have
CHAPTER 1. BACKGROUND

1. \( \det(I - \lambda M_1(\eta, \alpha)) = \begin{vmatrix} 1 - \eta \lambda & 0 \\ 0 & 1 - \eta \alpha \lambda \end{vmatrix} = (1 - \eta \lambda)(1 - \eta \alpha \lambda). \)

2. \( \det(I - \lambda M_2(\eta, \alpha)) = \begin{vmatrix} 1 & -\eta \lambda \\ -\eta \alpha \lambda & 0 \end{vmatrix} = 1 - \eta^2 \alpha \lambda^2 \)

3. \( \det(I - \lambda M_2(\eta, \alpha, \beta)) = \begin{vmatrix} 1 - (\eta/\sqrt{2}) \lambda & (\eta/\sqrt{2}) \beta \lambda \\ (\eta/\sqrt{2}) \alpha \lambda & 1 + (\eta/\sqrt{2}) \alpha \beta \lambda \end{vmatrix} = 1 + (\eta/\sqrt{2}) \lambda (\alpha \beta - 1) + (\eta^2/2) \alpha \beta \lambda^2. \)

Calculations using a computer software finally give
\[
\Phi_G(\lambda) = \frac{1}{(1 - \lambda^8)(1 - \lambda^{24})} = (1 + \lambda^8 + \lambda^{16} + \cdots)(1 + \lambda^{24} + \lambda^{48} + \cdots).
\]

Now assume that there exist homogeneous polynomials \( f_8 \) and \( f_{24} \) of degree 8 and 24 respectively, such that \( f_8 \) and \( f_{24} \) are primary invariants of \( \mathbb{C}[X, Y]^G \). This is equivalent to saying that \( f_8 \) and \( f_{24} \) are in \( \mathbb{C}[X, Y]^G \), and that they are algebraically independent. This implies that all products \( f_8^i f_{24}^j \) \((i, j \geq 1)\) are linearly independent and hence that the coefficients \( a_d \) of the Molien series satisfy
\[
a_d \geq \#\{ f = f_8^i f_{24}^j \mid \deg(f) = d \} = \#\{(i, j) \mid 8i + 24j = d \}.
\]

But expanding the terms in the Molien series of \( G \) give exactly this formula:
\[
a_d = \#\{(i, j) \mid 8i + 24j = d \}.
\]

Thus, all homogeneous polynomials of degree \( d \) which are in \( \mathbb{C}[X, Y]^G \) are linear combinations of \( \{ f_8^i f_{24}^j \mid \deg(f) = d \} \) from which it follows that
\[
\mathbb{C}[X, Y]^G = \mathbb{C}[f_8, f_{24}].
\]

Now it remains only to find such polynomials \( f_8 \) and \( f_{24} \). We claim that the following choices of polynomials fulfill the criterion:

1. \( f_8 \) is the weight enumerator of the \([8, 4, 4]\) \_2 Reed-Muller code \( \mathcal{R}_M_{F_2}(1, 3) \):
\[
f_8 = X^8 + 14X^4Y^4 + Y^8.
\]

We will see in Proposition 2.1.5 that this code is self-dual.
2. \( f_{24} \) is the weight enumerator of the \([24, 12, 8]_2\) Golay code:

\[
f_{24} = X^{24} + 759X^{16}Y^{8} + 2576X^{12}Y^{12} + 759X^{8}Y^{16} + Y^{24}.
\]

The definition of this code, as well as a proof of its self-duality can be found in \cite{MS77, Chap. 2, § 6].

Since they come from self-dual doubly-even codes (as seen in their weight-enumerator), these two polynomials are in \( \mathbb{C}[X, Y]^G \). It remains to be shown that they are algebraically independent. This is equivalent to asking that the matrix

\[
\begin{pmatrix}
\frac{\partial f_8}{\partial X} & \frac{\partial f_8}{\partial Y} \\
\frac{\partial f_{24}}{\partial X} & \frac{\partial f_{24}}{\partial Y}
\end{pmatrix}
\]

has non-zero determinant (as shown in \cite{ER93, Theorem 2.2}). The monomial with highest degree (in \( X \)) of this determinant is easily seen to be

\[-(24 \cdot 64)X^{23} \cdot X^4 \cdot Y^3 = -1536X^{27}Y^4 \neq 0\]

and hence these polynomials are algebraically independent.

Finally, noting that

\[
f'_{24} := \frac{f_8^3 - f_{24}}{42} = X^4Y^4 (X^4 - Y^4)^4
\]

and \( f_8 \) are still algebraically independent, we arrive to the following beautiful theorem:

**Theorem 1.2.11 (Gleason).** The invariants of \( G \) in \( \mathbb{C}[X, Y] \) are given by polynomials in \( f_8 \) and \( f'_{24} \). In other words,

\[
\mathbb{C}[X, Y]^G = \mathbb{C}[f_8, f'_{24}],
\]

where

\[
f_8 = X^8 + 14X^4Y^4 + Y^8 \quad \text{and} \quad f'_{24} = X^4Y^4 (X^4 - Y^4)^4.
\]

There are various important consequences of this theorem. The easiest is maybe the following.

**Corollary 1.2.12.** The length of every self-dual doubly-even code is divisible by 8.

**Proof.** Both 8 and 24 are divisible by 8. Therefore the weight enumerator of such a code has degree divisible by 8, and so the length must be too. \( \square \)
Furthermore, this construction gives an upper bound on the minimal distance of these codes.

**Theorem 1.2.13** (Mallows-Sloane, [MS73]). Let $C$ be a self-dual doubly-even code over $\mathbb{F}_2$ of length $n$ and minimum distance $d$. Then

$$d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4.$$ 

**Definition 1.2.14.** A self-dual doubly-even code over $\mathbb{F}_2$ with minimum distance attaining this bound is called an **extremal** code.

Actually, the extremal condition is quite restrictive. The following theorem implies that the family of extremal self dual codes is finite.

**Theorem 1.2.15** (Zhang, [Zha99]). Let $C$ be a self-dual doubly-even code over $\mathbb{F}_2$ of length $n$. Then

$$n \leq 3928.$$ 

A longstanding open problem asked by Sloane (in [Slo73]) is the question of existence of a self-dual doubly-even $[72,36,16]_2$ code. Using these bounds and MacWilliams' Theorem, it is possible to completely determine the weight-enumerator of a $[72,36,16]_2$ code, without knowing or not if it exists. This question has not been answered yet. A survey of the recent results can be found in [Bor15].

### 1.3 Algebraic Geometry

In this section, we review some basic algebraic geometry needed to understand evaluation codes (Chapter 2), and Weil’s trace formula (Section 3.2). Throughout the whole section, $k$ is an algebraically closed field of arbitrary characteristic.

#### 1.3.1 Basic definitions

**Definition 1.3.1.** The **affine $n$-space** $\mathbb{A}^n(k)$ is the vector space $k^n$. A **point in** $\mathbb{A}^n(k)$ is simply a $n$-tuple of elements of $k$.

The **projective $n$-space** $\mathbb{P}^n(k)$ is the space of lines in $\mathbb{A}^{n+1}(k)$. Explicitly, a **point in** $\mathbb{P}^n(k)$ is an equivalence classes of points of $\mathbb{A}^{n+1}(k)$, where two points $P, P' \in \mathbb{A}^{n+1}(k)$
are identified if \( P = \lambda P' \) for some \( \lambda \in k^\times \). We often write \( P = (P_0 : \cdots : P_n) \) to say that \( P \) is represented by the point \((P_0, \ldots, P_n) \in \mathbb{A}^{n+1}(k)\). We say that \((P_0 : \cdots : P_n)\) are \textbf{homogeneous coordinates} for \( P \).

Now that the main objects have been defined, we will study a particular class of subsets called algebraic sets. These will later help us to put a topological structure on \( \mathbb{A}^n(k) \) and \( \mathbb{P}^n(k) \). Observe that every polynomial \( f \in k[X_1, \ldots, X_n] \) can be seen as a function \( \mathbb{A}^n(k) \to k \) by polynomial evaluation. The same is not true for \( \mathbb{P}^n(k) \): an arbitrary polynomial \( f \in k[X_0, \ldots, X_n] \) is in general not well defined as a function \( \mathbb{P}^n(k) \to k \), since its values may depend on the choice of homogeneous coordinates for the point.

\textbf{Definition 1.3.2.} A polynomial \( f \in k[X_0, \ldots, X_n] \) is called \textbf{homogeneous} of degree \( d \) if it is a linear combination of degree \( d \) monomials. The set of homogeneous polynomials of degree \( d \) is denoted by \( k[X_0, \ldots, X_n]_d \). We write \( k[X_0, \ldots, X_n]_{\text{hom}} \) for the set of all homogeneous polynomials.

While the value of a polynomial \( f \in k[X_0, \ldots, X_m]_{\text{hom}} \) at a point \( P \in \mathbb{P}^n(k) \) is still not well defined, the equation
\[
f(\lambda P_0, \ldots \lambda P_n) = \lambda^{\text{deg}(f)} f(P_0, \ldots, P_n) \quad \forall \lambda \in k, \ \forall P_i \in k
\]
tells us that the property of being zero at \( P \in \mathbb{P}^n \) is well defined and does not depend on the choice of the representative of \( P \).

We now define algebraic sets.

\textbf{Definition 1.3.3.} If \( S \subseteq k[X_1, \ldots, X_n] \) is a set of polynomials, the \textbf{affine algebraic set} defined by \( S \) is
\[
V_{\mathbb{A}^n(k)}(S) := \{ P \in \mathbb{A}^n(k) \mid f(P) = 0 \ \forall f \in S \}.
\]
If \( S \subseteq k[X_0, \ldots, X_n]_{\text{hom}} \) is a set of homogeneous polynomials, the \textbf{projective algebraic set} defined by \( S \) is
\[
V_{\mathbb{P}^n(k)}(S) := \{ P \in \mathbb{P}^n(k) \mid f(P) = 0 \ \forall f \in S \}.
\]
If the context is clear, we will omit the subscripts and write \( V(S) \).

The algebraic sets on \( \mathbb{A}^n(k) \) or \( \mathbb{P}^n(k) \) can be seen as closed sets of a topology on these spaces. It is called the \textbf{Zariski topology}. All algebraic sets are seen as topological spaces using this topology (or the corresponding subspace topology).
A **principal open subset** is a subset $D(f)$ of $\mathbb{A}^n(k)$ or $\mathbb{P}^n(k)$ defined as the complement of $V(f)$ for some polynomial $f$ (homogeneous, if the space is $\mathbb{P}^n(k)$). Principal open subsets form a basis for the Zariski topology.

An algebraic set is **irreducible** if it is as a topological space, i.e. if it is not the union of two non-empty distinct closed subsets. An equivalent condition is that two non-empty open sets always intersect. This implies that in an irreducible topological space, *every (non-empty) open set is dense.*

An **affine** (resp. **projective**) variety is an algebraic set which is irreducible. A **quasi-affine** (resp. **quasi-projective**) variety is an open subset of an affine (resp. projective) variety.

We will simply write **variety** when we do not want to specify its type (affine, projective, quasi-affine or quasi-projective).

The **dimension** of a variety $Y$ is defined as:

$$\dim(Y) = \sup\{n \in \mathbb{N} \mid \exists \text{ chain } Z_0 \subseteq \cdots \subseteq Z_n \subseteq Y \text{ of distinct irreducible subsets}\}.$$  

If $Z$ is a closed subset of some variety $Y$, then its **codimension** in $Z$ is

$$\operatorname{codim}_Z(Y) = \dim(Y) - \dim(Z)$$

$$= \sup \left\{ n \in \mathbb{N} \mid \exists \text{ chain } Z_0 \subseteq \cdots \subseteq Z_n = Y \text{ of distinct irreducible subsets} \right\}.$$  

A variety of dimension 1 is called a **curve** and one of dimension 2 is called a **surface**.

Next we investigate the very important link between algebraic sets and ideals of the ring $k[X_1, \ldots, X_n]$ (or $k[X_0, \ldots, X_n]$, in the projective case).

**Definition 1.3.4.** If $Y \subset \mathbb{A}^n(k)$ is a set of affine points, the **ideal** of these points is

$$I(Y) := \{f \in k[X_1, \ldots, X_n] \mid f(P) = 0 \ \forall P \in Y\}.$$  

If $Y \subset \mathbb{P}^n(k)$ is a set of projective points, the **ideal** of these points is

$$I(Y) := \langle\{f \in k[X_0, \ldots, X_n]_{\text{hom}} \mid f(P) = 0 \ \forall P \in Y\}\rangle,$$

i.e. it is the ideal generated by this set.

We regroup these links into two propositions, one about the affine case, and its projective analogue.
**Proposition 1.3.5** (Affine case).

1. If \( S \subset k[X_1, \ldots, X_n] \) is any subset, then \( I(V(S)) = \sqrt{\langle S \rangle} \), the radical of the ideal generated by \( S \). If \( Y \subset \mathbb{A}^n(k) \), then \( V(I(Y)) = \bar{Y} \), the closure of \( Y \) with respect to the Zariski Topology.

2. The applications \( I \) and \( V \) induce a bijection

\[
\{ \text{algebraic subsets of } \mathbb{A}^n(k) \} \leftrightarrow \{ \text{radical ideals of } k[X_1, \ldots, X_n] \}.
\]

This bijection sends irreducible subvarieties to prime ideals, and vice-versa.

The projective analogue is then the following.

**Proposition 1.3.6** (Projective case).

1. If \( S \subset k[X_0, \ldots, X_n] \) is any subset, then \( I(V(S)) = \sqrt{\langle S \rangle} \), the radical of the homogeneous ideal generated by \( S \). If \( Y \subset \mathbb{A}^n(k) \), then \( V(I(Y)) = \bar{Y} \), the closure of \( Y \) with respect to the Zariski Topology.

2. The applications \( I \) and \( V \) induce a bijection

\[
\{ \text{algebraic subsets of } \mathbb{P}^n(k) \} \leftrightarrow \left\{ \text{homogeneous radical ideals of } k[X_0, \ldots, X_n] \right\},
\]

where \( k[X_0, \ldots, X_n]_+ \) is the ideal of \( k[X_0, \ldots, X_n] \) which is the direct sum of vector spaces

\[
k[X_0, \ldots, X_n]_+ = \bigoplus_{d \geq 1} k[X_0, \ldots, X_n]_d.
\]

This bijection sends irreducible subvarieties to homogeneous prime ideals, and vice-versa.

These two proposition have an important consequence, valid in the affine and projective case:

**Proposition 1.3.7.** Each algebraic set \( V \) admits a unique decomposition into a finite number of irreducible closed subsets

\[
V = V_1 \cup \cdots \cup V_r, \quad V_i \text{ irreducible.}
\]
We refer to [Har77, Chap.1, §1 and §2] for the proofs of these three propositions.

Finally, we introduce a definition in the case when we consider subfields of \( k \).

**Definition 1.3.8.** Let \( k_0 \) be a subfield of \( k \). An affine (resp. projective) variety \( X \) is **defined over** \( k_0 \) if \( X = V(S) \) for some subset \( S \subseteq k_0[X_1, \ldots, X_n] \) (respectively \( S \subseteq k_0[X_0, \ldots, X_n]_{\text{hom}} \) in the projective case). The \( k_0 \)-**rational points**, denoted \( X(k_0) \) are the points of \( \mathbb{A}^n(k) \) (resp. \( \mathbb{P}^n(k) \)) which have all coordinates in \( k_0 \) (resp. which admit a set of homogeneous coordinates in \( k_0 \)).

### 1.3.2 Regular maps, morphisms and rational maps

Apart from its topology, there is another important object associated to a variety: its ring of regular functions. As before, polynomials play an important role in this definition, except that quotients will also be allowed.

Let \( f, g \in k[X_1, \ldots, X_n] \) be two polynomials. We can see \( f/g \) as a function from the subset \( D(g) \subseteq \mathbb{A}^n(k) \) with values in \( k \); we say that \( f/g \) is defined at a point \( P \in \mathbb{A}^n(k) \) if \( g(P) \neq 0 \). Its value is then simply \( f(P)/g(P) \). Similarly, if \( f, g \) are two homogeneous polynomials of the same degree in \( k_0[X_0, \ldots, X_n]_d \), then \( f/g \) also defines a function from the subset \( D(g) \subseteq \mathbb{P}^n(k) \) to \( k \) (it is easy to check that the value does not depend on the choice of homogeneous coordinates), and \( f/g \) is defined at \( P \in \mathbb{P}^n(k) \) if \( g(P) \neq 0 \). This motivates the following definition.

**Definition 1.3.9.** Let \( Y \) be a variety, and let \( k_0 \) be a subfield of \( k \).

1. If \( Y \) is (quasi)-affine, then a **regular** function \( f : Y \to k \) is a function which is locally a quotient of polynomials. More precisely, we require that for any point \( P \in Y \), there exists an open neighborhood \( U \subseteq Y \) of \( P \) and polynomials \( g, h \in k[X_1, \ldots, X_n] \) with \( h \) nowhere zero on \( U \) and \( f|_U = g/h \).

2. If \( Y \) is (quasi)-projective, then a **regular** function \( f : Y \to k \) is a function which is locally a quotient of homogeneous polynomials of the same degree. More precisely, we require that for any point \( P \in Y \), there exists an open neighborhood \( U \subseteq Y \) of \( P \) and polynomials \( g, h \in k[X_0, \ldots, X_n]_d \) for some \( d \geq 0 \), with \( h \) nowhere zero on \( U \) and \( f|_U = g/h \).

3. If \( Y \) is defined over \( k_0 \), then a **\( k_0 \)-regular** function is a function \( f : Y \to k_0 \) which is regular in the previous sense, but where the corresponding polynomials can be chosen to have coefficients in \( k_0 \).
If \( Z \) is another variety, a **morphism** \( \varphi : Y \to Z \) is a continuous function preserving regular maps, i.e. such that for any regular function \( f : Z \to k \), \( f \circ \varphi : Y \to k \) is regular. An isomorphism is a morphism with a two sided inverse: it is a bijective map \( \varphi : Y \to Z \) such that both \( \varphi \) and \( \varphi^{-1} \) are morphisms.

Finally, if both \( Y \) and \( Z \) are defined over \( k_0 \), a \( k_0 \)-**morphism** \( \varphi : Y \to Z \) is a morphism which preserves \( k_0 \)-regular maps. If \( \varphi \) is an isomorphism, we say that \( Y \) and \( Z \) are **isomorphic over** \( k_0 \).

If \( Y, Z \) are varieties defined over some subfield \( k_0 \subset k \), then a \( k_0 \)-**morphism** \( \varphi : Y \to Z \) preserves \( k_0 \)-rational points (easy to verify). Consequently, if \( Y \) and \( Z \) are isomorphic over \( k_0 \), then the isomorphism induces a bijection between their \( k_0 \)-rational points.

In Section 3.2.3 we will see an example of varieties defined over some \( k_0 \subset k \), which are isomorphic over \( k \) but not over \( k_0 \), and which do not have the same number of \( k_0 \)-rational points.

Next we look at some interesting rings associated to a variety.

**Definition 1.3.10.** Let \( Y \) be a variety.

1. \( \mathcal{O}(Y) \) is the **ring of regular functions on** \( Y \).

2. \( K(Y) \) is the **function field** of \( Y \): it is the set of equivalence classes \( \langle U, f \rangle \) where \( U \) is a non-empty open of \( X \), \( f : U \to k \) is regular function on \( U \) and where \( \langle U, f \rangle \) and \( \langle V, g \rangle \) are identified if \( f|_{U \cap V} = g|_{U \cap V} \). It is easy to check that this is a field (using the fact that all non-empty open sets are dense in \( Y \)).

3. If \( Z \subset Y \) is a subvariety, the **local ring of** \( Z \) **on** \( Y \) is the subset \( \mathcal{O}_{Z,Y} \) of \( K(Y) \) of pairs \( \langle U, f \rangle \) where \( U \cap Z \neq \emptyset \). In particular, if \( Z \) is a point \( P \in Y \), the **local ring of** \( P \) **on** \( Y \) is simply the subset \( \mathcal{O}_{P,Y} \) of \( K(Y) \) of functions which are defined at \( P \).

**Remark 1.3.2.1.** First, it is easy to see that \( \mathcal{O}_{Z,Y} \) is indeed a local ring, with maximal ideal \( m := \{ \langle U, f \rangle \in \mathcal{O}_{Z,Y} \mid f|_{U \cap Z} = 0 \} \). Second, note that for \( Y \) a variety, and \( P \in Y \), we have inclusions

\[
\mathcal{O}(Y) \hookrightarrow \mathcal{O}_{P,Y} \hookrightarrow K(Y).
\]

Finally, observe that if \( Y \) is a closed variety and \( U \) a non-empty open subset of \( Y \), then \( K(U) = K(Y) \) and \( \mathcal{O}_{Z,U} = \mathcal{O}_{Z,Y} \) for any subvariety \( Z \subset Y \) which intersects \( U \). However, in general, \( \mathcal{O}(U) \neq \mathcal{O}(Y) \) (for example, \( \mathcal{O}(\mathbb{A}^1(k)) = k[X] \), while \( \mathcal{O}(D(X)) \) contains \( 1/X \) which is not regular on the whole \( \mathbb{A}^1(k) \)).
Finally, we define a weaker notion of maps between varieties.

**Definition 1.3.11.** Let $Y, Z$ be varieties. A *rational map* $\varphi : Y \to Z$ is an equivalence class $\langle U, \varphi_U \rangle$ where $U \subset Y$ is a non-empty open set, $\varphi_U : U \to Z$ is a morphism and where $\langle U, \varphi_U \rangle$ and $\langle V, \psi_V \rangle$ are identified if $\varphi_U|_{U \cap V} = \psi_V|_{U \cap V}$. It is *dominant* if for some (or equivalently, every) open $U$, $\varphi_U(U)$ is dense in $Y$. A rational map which admits an inverse rational map is called *birational*. Two varieties with a birational between them are *birationally equivalent*.

The main theorem concerning birational equivalence:

**Theorem 1.3.12.** Let $Y, Z$ be varieties. The following are equivalent:

1. $Y$ and $Z$ are birationally equivalent.
2. There are non-empty open-sets $U \subset Y$, $V \subset Z$ with $U$ isomorphic to $V$ as varieties.
3. The function fields $K(Y)$ and $K(Z)$ are isomorphic as $k$-algebras.

*Proof.* See [Har77, Chap.1, §4, Corollary 4.5].

We now discuss smoothness and singularities.

**Definition 1.3.13.** A commutative ring $A$ is a *regular local ring* if it is Noetherian, local and if $\dim A = \dim_{A/m}(m/m^2)$ (the first is the Krull dimension, and the second is the dimension as an $A/m$-vector space).

A variety $Y$ is *nonsingular* or *smooth* at $P \in Y$ if $\mathcal{O}_{P,Y}$ is a regular local ring, i.e. if

$$\dim \mathcal{O}_{P,Y} = \dim_k m/m^2,$$

where $m := \{ f \in K(Y) \mid f(P) = 0 \}$ is the maximal ideal of $\mathcal{O}_{P,Y}$. (Observe that $\mathcal{O}_{P,Y}/m = k$, so this coincides with the previous definition). $Y$ is *singular* at $P$ if $Y$ it not smooth at $P$. $Y$ is *smooth* if it is smooth at all points.

** Remark 1.3.2.2.** If $Y$ is affine, then $Y$ is smooth at $P$ if and only if the rank of the matrix $(\partial f_i/\partial x_j(P))_{i,j}$ is $n - \dim Y$, for some generators $f_1, \ldots, f_n$ of $I(Y)$ ([Har77, Chap 1, Theorem 5.1]). This corresponds to the intuition that the tangent space at $P$ is *nice*, i.e. non-degenerate.
A useful proposition is the following:

**Proposition 1.3.14.** Let $Y$ be a (quasi-projective) variety, and $Z$ a subvariety, both irreducible. Then

$$\dim \mathcal{O}_{Z,Y} = \operatorname{codim}_Y Z$$

**Sketch of proof.** By Remark 1.3.2.1 and observing that if $U \subset Y$ is open and if $Z \subset U$, then $\operatorname{codim}_Y Z = \operatorname{codim}_U Z$, we can assume that $Y$ is closed.

First, assume $Y$ affine. Let $A = k[X_1, \ldots, X_n]/I(Y)$, and let $p$ be the image of $I(Z)$ in $A$ (it is a prime ideal). A chain of subvarieties $Z = Z_0 \subset \cdots \subset Z_n = Y$ corresponds to a chain of prime ideals $p = p_0 \supset \cdots \supset p_n = (0)$. In turn, this chain of ideals corresponds to a chain of prime ideals in the localization: $pA_p = p_0A_p \supset \cdots \supset p_nA_p = (0)$. But $\mathcal{O}_{Z,Y} = A_p$, so we get a chain of prime ideals in $\mathcal{O}_{Z,Y}$. It is easy to see that this construction works the other way around, i.e. that for a chain of prime ideals in $\mathcal{O}_{Z,Y}$ one constructs a chain of primes in $A$ and hence a chain of subvarieties of $Y$ containing $Z$. The conclusion then follows from the definition of Krull dimension and codimension of subvarieties.

If $Y$ is projective, pick an affine open $U \subset Y$ with $U \cap Z \neq \emptyset$. Then $\mathcal{O}_{U \cap Z,U \cap Y} = \mathcal{O}_{Z,Y}$, and a chain of irreducible subvarieties $Z = Z_0 \subset \cdots \subset Z_n = Y$ corresponds to a chain of irreducible subvarieties $Z \cap U = Z_0 \cap U \subset \cdots \subset Z_n \cap U = Y \cap U$. Thus we are reduced to a problem with affine varieties.

To state the next proposition, we need a definition.

**Definition 1.3.15.** A Noetherian local domain $R$ which is not a field is called a **discrete valuation ring** if the two equivalent conditions are satisfied:

1. The maximal ideal of $R$ is principal.

2. There is some $t \in R$ such that any $f \in R$ can be written uniquely as

$$f = ut^n \quad n \in \mathbb{N}, u \in R^\times.$$

The $t$ in the second condition is called a **uniformizer** of $R$, and it is easily verified that it is unique up to multiplication by a unit.
If $R$ is a discrete valuation ring, we can define a function $v : R \setminus \{0\} \to \mathbb{N}_{\geq 0}$ as follows: For any $x \in R$, we can write $x = ut^n$, with $u \in R^\times$ and $t$ a uniformizer. This decomposition is unique up to multiplication by a unit, so we can define

$$v(x) = v(ut^n) := n.$$ 

Thus $v(x)$ is the largest integer $n$ so that $x \in m^n$ ($m$ is the maximal ideal of $R$, and where we say that $m^0 = R$).

If $K$ is the fraction field of $R$, $v$ extends to $v : K \setminus \{0\} \to \mathbb{Z}$ as follows:

$$v(a/b) = v(a) - v(b).$$

This proposition will be very important in Section 3.2.

**Proposition 1.3.16.** Let $Y$ be a smooth (projective) variety, and $Z$ a codimension one subvariety. Then $\mathcal{O}_{Z,Y}$ is a discrete valuation ring.

**Proof.** The proposition follows from Proposition 1.3.14 and the two following facts:

- Any regular local domain of dimension one is a discrete valuation ring ([AM69, Prop. 9.2]).
- Any local ring of a smooth variety $Y$ at an irreducible subvariety $Z$ is regular. To see this, observe that if $P$ is a point of $Z$, and if $m$ is the maximal ideal of $\mathcal{O}_{Y,Z}$, then

$$\mathcal{O}_{Y,Z} = (\mathcal{O}_{P,Z})_m \mathcal{O}_{P,Z}.$$ 

Now $\mathcal{O}_{P,Z}$ is a regular local ring, and hence so is every localization ([Ser65, Chap. IV, Prop. 23]). Therefore $\mathcal{O}_{Y,Z}$ is a regular local ring. □
Chapter 2

Evaluation Codes

When one speaks of algebraic geometry codes or evaluation codes, there are two main families which can be considered. The first one, the family of Goppa codes, are the codes obtained by evaluating rational functions at some particular sets of points of a smooth projective curves. These codes usually have very good properties and are well studied.

The second one is the family of generalized Reed-Muller codes, and these are the ones we will study in this section. They are much simpler to define: they simply come from the evaluation of polynomials over the affine or projective space. We consider the affine case first.

2.1 Affine Reed-Muller Codes

Let $q$ be a power of a prime $p$, $\mathbb{F}_q$ the field with $q$ elements, $r$ and $m$ integers. We denote by $\mathbb{A}^m(\mathbb{F}_q)$ the affine space over $\mathbb{F}_q$ of dimension $m$ (i.e., $\mathbb{A}^m(\mathbb{F}_q) = \mathbb{F}_q^m$). We will write $\mathbb{A}^m$ for $\mathbb{A}^m(\mathbb{F}_q)$ for simplicity. Let $\mathbb{F}_q[X_1, \ldots, X_m]_{\leq r}$ denote the set of polynomials in $m$ variables of total degree $\leq r$. We denote by $\mathbb{F}_q^{\mathbb{A}^m}$ the vector space $\mathbb{F}_q^{\mathbb{A}^m}$ indexed by $\mathbb{A}^m = \mathbb{F}_q^m$; we can also see this vector space as the set of all functions

$$\mathbb{A}^m \rightarrow \mathbb{F}_q$$

with usual scalar multiplication and addition of functions.

Definition 2.1.1. The Reed-Muller code $\mathcal{R}\mathcal{M}_{\mathbb{F}_q}(r, m)$ on $m$ variables, of degree $r$
and defined over $\mathbb{F}_q$ is the code in $\mathbb{F}^\mathbb{A}_m$ given by

$$\mathcal{RM}_{\mathbb{F}_q}(r, m) := \{ \tilde{f} = (f(x))_{x \in \mathbb{A}_m} \mid f \in \mathbb{F}_q[X_1, \ldots, X_m]_{\leq r} \}.$$ 

If the field is $\mathbb{F}_2$, we often omit it from the notation and write $\mathcal{RM}(r, m)$ for $\mathcal{RM}_{\mathbb{F}_2}(r, m)$.

In other words, $\mathcal{RM}_{\mathbb{F}_q}(r, m)$ is the set of polynomial functions $\mathbb{F}_q^m \to \mathbb{F}_q$ with degree at most $r$. Observe that $\mathcal{RM}_{\mathbb{F}_q}(r, m)$ contains fewer elements than $\mathbb{F}_q[X_1, \ldots, X_m]$: for example, the two polynomials $X_1$ and $X_1^q$ define the same function $\mathbb{F}_q^m \to \mathbb{F}_q$, since any element in $\mathbb{F}_q$ is a root of $X^q - X$.

By definition, the length of the code $\mathcal{RM}_{\mathbb{F}_q}(r, m)$ is simply

$$\# \mathbb{A}_m(\mathbb{F}_q) = q^m.$$ 

In the following subsections we investigate the other properties of Reed-Muller codes ($\mathcal{RM}$-codes in what follows).

### 2.1.1 The dimension of $\mathcal{RM}$-codes

Let $\Phi_m$ denote the following map:

$$\Phi_m : \mathbb{F}_q[X_1, \ldots, X_m] \to \mathbb{F}_q^\mathbb{A}_m$$

$$f \mapsto (f(x))_{x \in \mathbb{A}_m}.$$ 

In other words, $\Phi_m$ is the map which evaluates a polynomial of $m$ variables at each point of $\mathbb{A}_m$, or equivalently it is the map which sends a polynomial to its corresponding function $\mathbb{A}_m \to \mathbb{F}_q$. It is clearly a ring homomorphism, and we have

$$\Phi_m(\mathbb{F}_q[X_1, \ldots, X_m]_{\leq r}) = \mathcal{RM}_{\mathbb{F}_q}(r, m).$$

**Lemma 2.1.2.** The map $\Phi_m$ is surjective, and its kernel is

$$\ker(\Phi_m) = (X_1^q - X_1, \ldots, X_m^q - X_m).$$

**Proof.** For surjectivity, it is enough to show that for all $a \in \mathbb{A}_m$ the element

$$\delta_a : \mathbb{A}_m \to \mathbb{F}_q$$

$$x \mapsto \begin{cases} 1 & x = a \\ 0 & \text{otherwise} \end{cases}$$

is a codeword of $\mathcal{RM}_{\mathbb{F}_q}(r, m)$. This is immediate from the definition of $\Phi_m$.
is attained (every element in $F_A^m$ is a sum of $\delta_a$’s). Consider the polynomial

$$f_a = \frac{X_1^q - X_1}{X_1 - a_1} \cdots \frac{X_m^q - X_m}{X_m - a_m}.$$  

Its value at $x \in A^m$ is non-zero precisely when $x = a$. Hence

$$\delta_a = (f_a(a)^{-1}) f_a,$$

proving surjectivity.

We compute the kernel by induction on $m$. If $m = 1$, it follows from the identity $X_1^q - X_1 = \prod_{a \in F_q} (X_1 - a)$, that for any $f \in F_q[X_1]$, we have

$$\Phi_1(f) = 0 \iff f(a) = 0 \quad \forall a \in A^1 = F_q$$

$$\iff (X_1 - a) \text{ divides } f \quad \forall a \in F_q$$

$$\iff X_1^q - X_1 \text{ divides } f$$

proving the result.

Assume $m \geq 2$. Let $I_{m-1}$ denote the ideal of $F_q[X_1, \ldots, X_{m-1}]$ generated by

$$\{X_1^q - X_1, \ldots, X_{m-1}^q - X_{m-1}\},$$

and let $I_m$ denote the ideal generated by the same set of polynomials, but in the ring $F_q[X_1, \ldots, X_m]$.

Let $\text{ev}^q_{X_m} : F_q[X_1, \ldots, X_m] \to F_q[X_1, \ldots, X_{m-1}]$ denote the polynomial evaluation at $a$ of the variable $X_m$. If $i^a_m : A^{m-1} \hookrightarrow A^m$ is the map sending $(a_1, \ldots, a_{m-1})$ to

$$i^a_m(a_1, \ldots, a_{m-1}) = (a_1, \ldots, a_{m-1}, a),$$

let $\pi^a_m : F_A^m \to F_A^{m-1}$ denote precomposition by $i^a_m$.

It is clear that the two following diagrams are commutative (the second one is induced by the first on quotients)

$$\begin{array}{ccc}
F_q[X_1, \ldots, X_{m-1}, X_m] & \xrightarrow{\Phi_m} & F_A^m \\
\downarrow_{\text{ev}^a_{X_m}} & & \downarrow_{\pi^a_m} \\
F_q[X_1, \ldots, X_{m-1}] & \xrightarrow{\Phi_{m-1}} & F_A^{m-1}
\end{array}$$

$$\begin{array}{ccc}
F_q[X_1, \ldots, X_{m-1}, X_m]/I_m & \xrightarrow{\Phi_m} & F_A^m \\
\downarrow_{\text{ev}^a_{X_m}} & & \downarrow_{\pi^a_m} \\
F_q[X_1, \ldots, X_{m-1}]/I_{m-1} & \xrightarrow{\Phi_{m-1}} & F_A^{m-1}
\end{array}.$$
CHAPTER 2. EVALUATION CODES

By induction, $\Phi_{m-1}$ is an isomorphism. Therefore

$$\ker(\Phi_m) = \bigcap_{a \in \mathbb{F}_q} \ker \left( \pi_m^a \circ \Phi_m \right) \overset{(*)}{=} \bigcap_{a \in \mathbb{F}_q} \ker \left( \Phi_{m-1} \circ \text{ev}_{X_m}^a \right)$$

$$\overset{(**)}{=} \bigcap_{a \in \mathbb{F}_q} \ker \left( \text{ev}_{X_m}^a \right) = \bigcap_{a \in \mathbb{F}_q} (X_n - \bar{a}) = (X_m^q - X_m)$$

(in (*) we use the commutativity of the diagram, and in (**), the fact that $\Phi_{m-1}$ is injective). Thus,

$$\ker(\Phi_m) = I_m + (X_m^q - X_m) = (X_1^q - X_1, \ldots, X_m^q - X_m)$$

as desired. \(\square\)

**Remark 2.1.1.1.** The argument for surjectivity actually gives a condition for the code $\mathcal{RM}_{\mathbb{F}_q}(r, m)$ to be trivial. Indeed, this happens exactly when

$$\mathcal{RM}_{\mathbb{F}_q}(r, m) = \Phi_m(\mathbb{F}_q[X_1, \ldots, X_m]_{< r}) = \mathbb{F}_q^k,$$

or equivalently when $\mathcal{RM}_{\mathbb{F}_q}(r, m)$ contains all the $\delta_a$ constructed in the proof, for any $a \in \mathbb{A}^m$. But observe that for any $a \in \mathbb{A}^m$, the polynomial $f_a$ constructed in the proof has degree $m(q-1)$. Therefore, as soon as $r \geq m(q-1)$, $f_a \in \mathbb{F}_q[X_1, \ldots, X_m]_{\leq r}$ and hence $\delta_a \in \mathcal{RM}_{\mathbb{F}_q}(r, m)$.

Using this lemma, we can compute the dimension of $\mathcal{RM}_{\mathbb{F}_q}(r, m)$. Let $V$ denote the vector space

$$V := \mathbb{F}_q[X_1, \ldots, X_m]_{\leq r} \cap \ker(\Phi_m).$$

By our previous considerations, we have an exact sequence

$$0 \to V \to \mathbb{F}_q[X_1, \ldots, X_m]_{\leq r} \xrightarrow{\Phi_m} \mathcal{RM}_{\mathbb{F}_q}(r, m) \to 0.$$

**Definition 2.1.3.** A polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_m]$ is said to be **reduced** (or $q$-reduced if we want to precise the $q$) if all individual degrees of $f$ are not greater than $q - 1$. Explicitly, $f$ is reduced if

$$\forall 1 \leq j \leq m, \quad \deg_{X_j}(f) \leq q - 1.$$

We claim that $\Phi_m$ induces an isomorphism between $\mathcal{RM}_{\mathbb{F}_q}(r, m)$ and the subspace $W$ of $\mathbb{F}_q[X_1, \ldots, X_m]_{\leq r}$ generated by the set $M$ of reduced monomials of total degree $\leq r$. Explicitly,

$$M := \left\{ X_1^{e_1} \cdots X_m^{e_m} \mid \sum_j e_j \leq r \text{ and } e_j \leq q - 1 \forall j \right\}.$$
We prove that $\Phi_m|_W$ is injective. If $f \in W$ is so that $\Phi_m(f) = 0$, then $f \in V \subset \ker(\Phi_m)$. But it is clear that all non-zero elements of $\ker(\Phi_m)$ have $\deg X_j \geq q$ for some $j$ (any non-zero polynomial with all individual degrees $\leq q - 1$ is non-zero at some element of $\mathbb{F}_q^m$). Thus $f$ can only be 0 and $\Phi_m|_W$ is injective.

To show surjectivity, since $\mathcal{R}\mathcal{M}_{\mathbb{F}_q}(r, m)$ is generated by the image of all monomials of total degree $\leq r$, it is enough to show that $\Phi_m|_W$ attains all such monomials. Let $\tilde{f} := \Phi_m(X_1^{f_1} \cdots X_m^{f_m})$ and let $f = X_1^{e_1} \cdots X_m^{e_m}$ be a monomial in $\Phi_m^{-1}(\tilde{f})$ with minimal individual degrees. Suppose some $e_j \geq q$ (we assume that $j = 1$, the other cases are similar). Then

$$\tilde{f} = \Phi_m(X_1^{e_1} \cdots X_m^{e_m}) = \Phi_m((X_1^q - X_1)(X_1^{e_1-q} \cdots X_m^{e_m}) + X_1^{e_1-q} \cdots X_m^{e_m})$$

$$= \Phi_m(X_1^{e_1-q} \cdots X_m^{e_m}),$$

contradicting the choice of $f$. Thus $f$ is reduced and $\Phi_m|_W$ is surjective.

We have reduced the problem of computing the dimension of $\mathcal{R}\mathcal{M}_{\mathbb{F}_q}(r, m)$ to the one of computing the number of elements in the set $M$. Let

$$A_s := \{s\text{-subsets of } \{X_1, \ldots, X_m\}\} \times \{\text{monomials of total degree } \leq r - sq\}.$$ 

If $\tilde{M}$ denotes the set of monomials of degree $\leq r$, then we have a map

$$\pi_s : A_s \longrightarrow \tilde{M}$$

$$((\{X_{n_1}, \ldots, X_{n_s}\}, f)) \longmapsto X_{n_1}^q \cdots X_{n_s}^q \cdot f.$$ 

For $f \in \tilde{M}$, let $n_s(f) := |\pi_s^{-1}\{\{f\}\}|$. If $f$ has $t$ exponents (say the exponents of $X_1, \ldots, X_t$) greater or equal to $q$, then the number of pre-images of $f$ in $A_s$ is the number of decompositions

$$f = X_{n_1}^q \cdots X_{n_s}^q \cdot g,$$

with $1 \leq n_1 < \cdots < n_s \leq t$ and $g$ an arbitrary monomial. It is clear that there are exactly $\binom{t}{s}$ such decompositions, so we get

$$n_s(f) = \begin{cases} 
\binom{t}{s} & 0 \leq s \leq t \\
0 & \text{otherwise.} 
\end{cases}$$

Since for any $t \geq 1$,

$$\sum_{j=0}^{t} (-1)^j \binom{t}{j} = 0,$$
and since this formula gives $1$ for $t = 0$ (making the convention that $\binom{0}{0} = 1$), we see that
\[
\sum_{s=0}^{m} (-1)^s n_s(f) = \begin{cases} 
1 & \text{if all exponents } \leq q - 1 \\
0 & \text{otherwise}
\end{cases}
\]
Therefore, we have
\[
\# M = \sum_{f \in M} 1 = \sum_{f \in M} \left( \sum_{s=0}^{m} (-1)^s n_s(f) \right) \\
= \sum_{s=0}^{m} (-1)^s \sum_{f \in M} n_s(f) \\
\overset{(*)}{=} \sum_{s=0}^{m} (-1)^s \# A_s
\]
(where in $(*)$ we used that $A_s = \bigcup_{f \in M} \pi_s^{-1}(\{f\})$).

The cardinality of $A_s$ is easy to compute. There are $\binom{m}{s}$ ways to choose the powers which are equal to $q$ or less, and the remaining powers is simply the number of monomials of total degree $r - sq$ or less. Therefore,
\[
\# A_s = \binom{m}{s} \left( \begin{array}{c} r - sq + m \\ r - sq \end{array} \right),
\]
and thus we have shown:

**Proposition 2.1.4.** The dimension of the Reed-Muller code $\mathcal{RM}_{F_q}(r, m)$ is
\[
\dim \mathcal{RM}_{F_q}(r, m) = \sum_{s=0}^{m} (-1)^s \binom{m}{s} \left( \begin{array}{c} r - sq + m \\ r - sq \end{array} \right).
\]

**Remark 2.1.1.2.** This formula is simpler than the one given in [AK92], or in [Lac88] for example. Their formula is the following:
\[
\dim \mathcal{RM}_{F_q}(r, m) = \sum_{i=0}^{r} \sum_{s=0}^{m} (-1)^s \binom{m}{s} \left( \begin{array}{c} i - sq + m - 1 \\ i - sq \end{array} \right).
\]
It is obtained by noting that:

- The number of monomials on $m$ variables of degree $i - sq$ is $\binom{i - sq + m - 1}{i - sq}$.
- An inclusion exclusion argument gives that the inner sum is the number of monomials of degree $i$ with no exponent $\geq q$.
- Summing on all the possible degrees gives the result.
2.1.2 The dual of $\mathcal{RM}$-codes

In this section we compute the dual codes of Reed Muller codes. By Remark 2.1.1.1, $\mathcal{RM}_{\mathbb{F}_q}(r, m)$ is trivial if $r \geq m(q - 1)$. However, if $r < m(q - 1)$ we have an interesting property about duals.

**Proposition 2.1.5.** Let $0 \leq r < m(q - 1)$. Then

$$\mathcal{RM}_{\mathbb{F}_q}(r, m) = \mathcal{RM}_{\mathbb{F}_q}(m(q - 1) - r - 1, m).$$

In particular, $\mathcal{RM}_{\mathbb{F}_q}(r, m)$ is self-orthogonal if and only if

$$2r < m(q - 1).$$

To prove this statement, we need a lemma and an easy corollary.

**Lemma 2.1.6.** Let $q$ be a prime power and $r$ a nonnegative integer.

$$\sum_{a \in \mathbb{F}_q} a^r = \begin{cases} -1 & \text{if } r \neq 0 \text{ and } r \equiv 0 \pmod{q - 1} \\ 0 & \text{otherwise.} \end{cases}$$

**Proof.** If $r = 0$, then

$$\sum_{a \in \mathbb{F}_q} a^0 = |\mathbb{F}_q| = q = 0.$$

Suppose $r \neq 0$. Then $0^r = 0$ so we have

$$\sum_{a \in \mathbb{F}_q} a^r = \sum_{a \in \mathbb{F}_q^*} a^r.$$

Now suppose $r = m(q - 1)$ for $m \neq 0$. We have

$$\sum_{a \in \mathbb{F}_q^*} a^r = \sum_{a \in \mathbb{F}_q^*} (a^{q-1})^m = \sum_{a \in \mathbb{F}_q^*} 1 = q - 1 = -1$$

as desired.

Finally, assume $r \equiv 0 \pmod{q - 1}$. Let $g$ be a generator of the cyclic group $\mathbb{F}_q^*$; observe that this implies that $g^r \neq 1$. The sum becomes

$$\sum_{a \in \mathbb{F}_q^*} a^r = \sum_{i=0}^{q-2} (g^i)^r = \sum_{i=0}^{q-2} (g^r)^i = \frac{(g^r)^{q-1} - 1}{g^r - 1} = 0$$

as desired. \qed
Corollary 2.1.7. Let \( f \in \mathbb{F}_q[X_1, \ldots, X_m] \). If \( \deg(f) < m(q - 1) \) then

\[
\sum_{x \in \mathbb{A}^m} f(x) = 0.
\]

Proof. Since every polynomial \( f \) is a linear combination of monomials, it is enough to prove it for \( f = X_1^{e_1} \cdots X_m^{e_m} \) with \( e_1 + \cdots + e_m < m(q - 1) \). Write

\[
\sum_{x \in \mathbb{A}^m} f(x) = \sum_{x_1, \ldots, x_m \in \mathbb{F}_q} x_1^{e_1} \cdots x_m^{e_m} = \left( \sum_{x_1 \in \mathbb{F}_q} x_1^{e_1} \right) \cdots \left( \sum_{x_m \in \mathbb{F}_q} x_m^{e_m} \right).
\]

If all \( e_i \) are \( \geq (q - 1) \) we contradict the restriction on the degree, so some \( e_i \) is less than \( q - 1 \). By the previous lemma, \( \sum_{x_i \in \mathbb{F}_q} x_i^{e_i} = 0 \) and the conclusion follows. \( \square \)

We are ready to prove the proposition.

Proof of Proposition 2.1.5. Let \( f \in \mathbb{F}_q[X_1, \ldots, X_m] \leq_r \), \( g \in \mathbb{F}_q[X_1, \ldots, X_m] \leq_{m(q - 1) - r - 1} \) and let \( \bar{f} \in \mathcal{R}\mathcal{M}_{\mathbb{F}_q}(r, m) \), \( \bar{g} \in \mathcal{R}\mathcal{M}_{\mathbb{F}_q}(m(q - 1) - r - 1, m) \) be their corresponding codewords.

Then \( \deg(fg) = \deg(f) + \deg(g) \leq m(q - 1) - 1 \), so by the previous corollary,

\[
\langle \bar{f}, \bar{g} \rangle = \sum_{x \in \mathbb{A}^m} f(x)g(x) = 0.
\]

Thus \( \mathcal{R}\mathcal{M}_{\mathbb{F}_q}(m(q - 1) - r - 1, m) \subset \mathcal{R}\mathcal{M}_{\mathbb{F}_q}(r, m)^\perp \).

To see that this is an equality, it is enough to count dimensions. Observe that there is a bijection

\[
\begin{align*}
\{ \text{reduced monomials} \\ \text{of degree} \leq r \} & \quad \longleftrightarrow \quad \{ \text{reduced monomials} \\ \text{of degree} \geq m(q - 1) - r \} \\
X_1^{e_1} \cdots X_m^{e_m} & \quad \longleftrightarrow \quad X_1^{(q-1)-e_1} \cdots X_m^{(q-1)-e_m}.
\end{align*}
\]

By Section 2.1.1 we get

\[
\dim \mathcal{R}\mathcal{M}_{\mathbb{F}_q}(r, m) = \# \left\{ \text{reduced monomials} \right. \\ \left. \text{of degree} \geq m(q - 1) - r \right\} = q^m - \# \left\{ \text{reduced monomials} \right. \\ \left. \text{of degree} \leq m(q - 1) - r - 1 \right\} = q^m - \dim \mathcal{R}\mathcal{M}_{\mathbb{F}_q}(m(q - 1) - r - 1, m).
\]
Therefore
\[ \dim \mathcal{R} \mathcal{M}_{F_q}(r, m)^\perp = q^m - \dim \mathcal{R} \mathcal{M}_{F_q}(r, m) = \dim \mathcal{R} \mathcal{M}_{F_q}(m(q - 1) - r - 1, m), \]
whence
\[ \mathcal{R} \mathcal{M}_{F_q}(r, m)^\perp = \mathcal{R} \mathcal{M}_{F_q}(m(q - 1) - r - 1, m). \]

### 2.1.3 Other properties

We briefly discuss other properties of these codes.

**Definition 2.1.8.** The punctured Reed-Muller code \( \mathcal{R} \mathcal{M}_{F_q}(r, m)^* \) is the code obtained from \( \mathcal{R} \mathcal{M}_{F_q}(r, m) \) by “removing coordinate zero”. Explicitly, if \( i \) is the inclusion \( \mathbb{A}^m \setminus \{0\} \hookrightarrow \mathbb{A}^m \), then \( \mathcal{R} \mathcal{M}_{F_q}(r, m)^* \) is the code in \( F_q^\mathbb{A}^m \) given by
\[ \mathcal{R} \mathcal{M}_{F_q}(r, m)^* := i^*(\mathcal{R} \mathcal{M}_{F_q}(r, m)) = \{ \bar{f} \circ i \mid \bar{f} \in \mathcal{R} \mathcal{M}_{F_q}(r, m) \}. \]

**Proposition 2.1.9.** Let \( 0 \leq r < m(q - 1) \). Then \( \mathcal{R} \mathcal{M}_{F_q}(r, m)^* \) is a cyclic code with generator polynomial
\[ g(X) = \prod (X - \omega^u), \]
where \( \omega \) is a primitive element of \( F_q^m \) (i.e. a generator of the cyclic group \((F_q^m)^*\)) and where the product is taken over all integers \( u \) satisfying
\[ 0 < u < q^m - 1 \text{ and } \sum_{i=0}^{\infty} u_i \leq m(q - 1) - r - 1, \]
with \( u = \sum_{i=0}^{\infty} u_i q^i \) the \( q \)-ary representation of \( u \).

**Proof.** Corollary 5.5.1 of [AK92]. \( \square \)

Using this cyclicity, we can get the minimal distance of \( \mathcal{R} \mathcal{M}_{F_q}(r, m) \).

**Proposition 2.1.10.** Let \( 0 \leq r < m(q - 1) \) and write \( r = u(q - 1) + v \) such that \( 0 \leq v < (q - 1) \). Then the minimum distance of \( \mathcal{R} \mathcal{M}_{F_q}(r, m) \) is
\[ d := (q - v)q^{m-u-1}. \]

**Proof.** Corollary 5.5.4 of [AK92]. \( \square \)

The fact that this distance is a multiple of \( q \) is not a surprise, as we will see in section Section 3.1 when we study divisibility of codes.
2.1.4 Examples

We end this section with a few examples of various Reed-Muller codes.

Example 2.1.4.1. Let us look at the code $\mathcal{RM}_{F_q}(0, m)$. This is the code coming from the evaluation of constant polynomials, at all points of $A^m(F_q)$. Therefore, this code is not very interesting: it is an $[q^m, 1, q^m]_q$ code, with generator matrix

$$G := \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix} \quad (1 \times q^m \text{ matrix}).$$

Its weight enumerator is simply

$$W_{\mathcal{RM}_{F_q}(0, m)}(X, Y) = X^{q^m} + (q - 1)Y^{q^m}.$$

Its dual is $\mathcal{RM}_{F_q}(m(q - 1) - 1, m)$, whose weight enumerator is thus (by MacWilliams' Theorem, Theorem 1.1.11)

$$W_{\mathcal{RM}_{F_q}(m(q-1)-1, m)}(X, Y) = q^{-1}W_{\mathcal{RM}_{F_q}(0, m)}(X + (q - 1)Y, X - Y).$$

Example 2.1.4.2. Let us now consider the code $\mathcal{RM}_{F_q}(1, m)$. It is the code coming from the evaluation of linear polynomials (and constant polynomials). Using Proposition 2.1.4 and Proposition 2.1.10, we see that this code is of type $[q^m, m + 1, q^{m-1}]_2$.

A basis for it is given by the all one vector and the evaluations of all the monomials $X_1, \ldots, X_m$.

Let us compute its weight enumerator. Let $f = \sum_{i=1}^{m} \lambda_i X_i + \mu$ be a linear polynomial. If $f$ is constant, then either $f$ is zero and gives the all zero vector in $\mathcal{RM}_{F_q}(1, m)$, or $f$ is non-zero and $f$ has only non-zero values. Thus, the $Y^{q^m}$ coefficient of the weight enumerator is $(q - 1)$ and the $X^{q^m}$ coefficient is one.

In the case where at least one $\lambda_i$ is non-zero, we claim that $V(f)$ is isomorphic to $V(X_1)$ over $F_q$, and hence these two sets have the same number of $F_q$-rational points. Observe that there are exactly $q^{m+1} - q$ such polynomials. First, we can assume (upon permuting the coordinates) that $\lambda_1 \neq 0$. Second, the translation

$$A^m(F_q) \rightarrow A^m(F_q)$$

$$x \mapsto x - (\lambda_1^{-1} \mu, 0, \ldots, 0)$$
sends $V(f)$ to $V(f - \mu)$, and since it is an $F_q$-isomorphism, these two algebraic sets have the same number of $F_q$-rational points, so we may assume $\mu = 0$.

Finally, we have the following $F_q$-linear map:

$$\mathbb{A}^m(F_q) \longrightarrow \mathbb{A}^m(F_q)$$

$$x \longmapsto Ax,$$

where

$$A = \begin{pmatrix}
\lambda_1 & \lambda_2 & \cdots & \lambda_m \\
0 & & & \\
\vdots & I_{m-1} & \\
0 & & & \\
\end{pmatrix}$$

and $I_{m-1}$ is the $(m-1) \times (m-1)$ identity matrix. This is a $F_q$-isomorphism which sends $V(f)$ to $V(X_1)$, and so these two sets have the same number of $F_q$-rational points.

Now it suffices to compute the number of $F_q$-rational points of $V(X_1)$. This is the number of points in $\mathbb{A}^m(F_q)$ which have the first coordinate zero. It is clear that there are $q^{m-1}$ such points.

Putting all this information together, we get:

$$W_{RM_q(1,m)}(X,Y) = X^{q^m} + q(q^m - 1)X^{q^{m-1}}Y^{(q-1)q^{m-1}} + (q - 1)Y^{q^m}.$$

### 2.2 Projective Reed-Muller Codes

As before, let $q = p^r$ denote a prime power, $F_q$ the field with $q$-elements. The projective space on $m$ variables over $F_q$ is denoted $\mathbb{P}^m(F_q)$ and will often be denoted simply by $\mathbb{P}^m$, in this section. Let $F_q[X_0, \ldots, X_m]^r$ denote the set of homogeneous polynomials of degree $r$ in the $m + 1$ variables $X_0, \ldots, X_m$, together with $0$.

Whereas it makes sense to speak of a projective zero of a homogeneous polynomial, we cannot speak of its value since it is not invariant under scalar multiplication. Therefore, to define projective Reed-Muller codes, we need to fix a system of representatives of the projective space $\mathbb{P}^m$.

**Definition 2.2.1.** Let $x \in \mathbb{P}^m$ be a projective point. Then $x$ has a unique representative in homogeneous coordinates of the form

$$x = (0 : \cdots : 0 : 1 : x_j : \cdots : x_m),$$
i.e. a representative in which the leftmost non-zero coordinate is chosen to be one. This will be called the *standard representative* of \( x \in \mathbb{P}^m \). If \( f \in \mathbb{F}_q[X_0, \ldots, X_m]^h \), we can define its **value** at \( x \) by

\[
f(x) := f(0, \ldots, 0, 1, x_j, \ldots, x_m),
\]
i.e. its value at the standard representative of \( x \).

Let \( \mathbb{F}_q^m \) denote the vector space of dimension \( \#\mathbb{P}^m = (q^{m+1} - 1)/(q - 1) \) indexed by the set of projective points \( \mathbb{P}^m \). As before, this can also be seen as the vector space of functions \( \mathbb{P}^m \to \mathbb{F}_q \). With this notation we can define projective Reed-Muller codes easily.

**Definition 2.2.2.** The *projective Reed-Muller* code \( \mathcal{PRM}_{\mathbb{F}_q}(r, m) \) on \( m \) variables of degree \( r \) defined over \( \mathbb{F}_q \) is the code in \( \mathbb{F}_q^m \) given by

\[
\mathcal{PRM}_{\mathbb{F}_q}(r, m) := \{ \bar{f} = (f(x))_{x \in \mathbb{P}^m} \mid f \in \mathbb{F}_q[X_0, \ldots, X_m]^h \}.
\]

It is clear that if we change the representatives of \( \mathbb{P}^m \), we get a code which is monomially equivalent to this one (cf. Definition [1.1.4]). An important consequence is that the weight enumerator is independent of the representatives chosen.

### 2.2.1 Properties of \( \mathcal{PRM} \)-codes

As before, the length of the a \( \mathcal{PRM}_{\mathbb{F}_q}(r, m) \) code is

\[
\#\mathbb{P}^m(\mathbb{F}_q) = \frac{q^{m+1} - 1}{q - 1}.
\]

We compute the dimension of \( \mathcal{PRM} \)-codes. It is clear that \( \mathcal{PRM}_{\mathbb{F}_q}(r, m) \) is generated by the images of the monomials of total degree \( r \). Moreover, for any homogeneous polynomial \( f \in \mathbb{F}_q[X_0, \ldots, X_m]^h \), we have

\[
f(\mathbb{P}^m(\mathbb{F}_q)) = 0 \iff f(\mathbb{A}^{m+1}(\mathbb{F}_q)) = 0
\]

and it follows that two homogeneous polynomials give the same image in \( \mathcal{PRM}_{\mathbb{F}_q}(r, m) \) if and only if the reduced form of \( f - g \) is zero.

Following the same argument as in \( \mathcal{RM} \)-codes, one is tempted to say that a basis of a \( \mathcal{PRM} \)-code is given by

\[
M := \{ X_0^{e_0} \cdots X_m^{e_m} \mid \sum_{j=0}^m e_j = r, \ \forall j, e_j \leq q - 1 \}.
\]
Chapter 2. Evaluation Codes

But a non-reduced polynomial monomial $f$ may have a reduced image which is not of total degree $r$ anymore: for example, if $r = q$, then the polynomial $X_0^q$ is in $\mathbb{F}_q[X_0, \ldots, X_m]^h$, but no monomial in $M$ takes the same values as $X_0^q$ on $\mathbb{P}^m(\mathbb{F}_q)$.

Thus we must refine $M$ as follows: we let

$$M' := \left\{ f := X_0^{e_0} \cdots X_m^{e_m} \mid f \neq 0, \forall j, e_j \leq q - 1 \text{ and } f \text{ is the reduced form of some monomial of total degree } r \right\}.$$ 

In that way, the images of $M'$ form a basis of $\mathcal{PRM}_{\mathbb{F}_q}(r, m)$.

Let $f$ be a monomial of degree $r$, and suppose its reduced form has degree $t$. Then it is clear that

$$t \equiv r \pmod{q - 1}$$

since replacing powers of $X_j^q$ by $X_j$ always lowers the degree by $(q - 1)$. Therefore, all monomials in $M'$ have degree congruent to $r$, mod $(q - 1)$.

But if $t \equiv r \pmod{q - 1}$, then all the reduced monomials of degree $t$ are in $M'$: if $X_0^{e_0} \cdots X_m^{e_m}$ is such a monomial, with say $e_j \neq 0$, then

$$X_0^{e_0} \cdots X_j^{e_j + r - t} \cdots X_m^{e_m}$$

is a monomial of degree $r$ which reduces to the given monomial in $M'$. Therefore

$$\dim \mathcal{PRM}_{\mathbb{F}_q}(r, m) = \#M'$$

$$= \sum_{t \equiv r \pmod{q - 1}} \#\{\text{monomials of degree } t \text{ with no exponent } \geq q\}$$

$$= \sum_{t \equiv r \pmod{q - 1}} \sum_{s = 0}^{m} (-1)^s \binom{m}{s} \binom{t - sq + m - 1}{t - sq},$$

the last equality following from Remark 2.1.1.2.

The minimal length of $\mathcal{PRM}_{\mathbb{F}_q}(r, m)$ is

$$d = (q - s)q^{m-r-1},$$

where $s$ is the rest of the euclidean division of $(r - 1)$ by $(q - 1)$, i.e.

$$r - 1 = l(q - 1) + s, \quad 0 \leq s < q - 1.$$ 

We refer to [Sor91, Theorem 1] for the proof of this fact.

Finally, we discuss the dual of Projective Reed-Muller codes. The situation is very similar than the one of affine Reed-Muller codes.
Proposition 2.2.3. The dual of $\mathcal{PRM}_{\mathbb{F}_q}(r, m)$ is

$$
\mathcal{PRM}_{\mathbb{F}_q}(r, m)^\perp = \begin{cases} 
\mathcal{PRM}_{\mathbb{F}_q}(m(q - 1) - r, m) & \text{if } r \neq 0 \pmod{q - 1} \\
\mathcal{PRM}_{\mathbb{F}_q}(m(q - 1) - r, m) \oplus \mathbb{F}_q \mathbf{1} & \text{if } r \equiv 0 \pmod{q - 1},
\end{cases}
$$

where $\mathbf{1} = (1, \ldots, 1)$ is the all-one vector.

This is [Sør91, Theorem 2]. The proof is similar to the one of the affine case. One first computes that $\mathcal{PRM}_{\mathbb{F}_q}(r, m(q - 1) - r) \subseteq \mathcal{PRM}_{\mathbb{F}_q}(r, m)^\perp$ using properties similar to Corollary 2.1.7 and then one uses a dimension argument for the reverse inclusion.
Chapter 3

Divisibility

As shown in Section 1.2, Invariant Theory can be a very powerful tool to determine weight enumerators. It is towards finding such invariants that we look at divisibility.

As previously, $p$ denotes a prime number, $q$ a power of $p$ and $\mathbb{F}_q$ denotes the finite field with $q$ elements. If $F$ is a polynomial over $\mathbb{F}_q$, then we let $N(F)$ denote its number of zeroes (in $\mathbb{F}_q$). To shorten notations, we will write $\mathcal{R}\mathcal{M}(r, m)$ for the Reed-Muller code $\mathcal{R}\mathcal{M}_{\mathbb{F}_2}(r, m)$.

We recall (cf. Definition 1.1.10) that a linear code $C$ is divisible by some integer $\Delta \geq 1$ if all its weights are divisible by $\Delta$.

For example, a doubly-even code is divisible by 4. In terms of invariants, this translates as follows: a linear code $C$ is divisible by $\Delta$ if and only if its weight enumerator is invariant under the transformation

$$\begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix} \in GL_2(\mathbb{C}),$$

where $\zeta$ is a primitive $\Delta$’th root of unity in $\mathbb{C}$.

The divisibility of a given code can contain some useful information on the code itself. We cite two standard results about such codes which are interesting by themselves, but which will not be used in what follows.

Theorem 3.0.4 (Ward). Let $C$ be a non-zero linear code over $\mathbb{F}_q$. Suppose $C$ is divisible by $\Delta$, and that $\Delta$ is relatively prime to $q$. There exists a code $C'$ such that $C$ is equivalent to the code obtained by repeating each coordinate $\Delta$ times, and adding enough zero coordinates to match the length of $C$.  

56
The proof can be found in [War81].

Another information we can get is an upper bound on the dimension. For an integer $m$ let $v_p(m)$ denote the $p$-adic valuation of $m$, where $p$ is the characteristic of $\mathbb{F}_q$.

**Theorem 3.0.5** (Ward). Let $C$ be an $[n, k, d]_q$ code, with $p | q$. Suppose $C$ is divisible by $\Delta$ and that its non-zero codeword weights are among the $m$ values $\{ (b-m+1)\Delta, \ldots, b\Delta \}$ (for some integer $b$). Then the dimension $k$ of $C$ satisfies

$$kp \leq m(v_p(\Delta) + p) + v_p\left(\binom{m}{b}\right).$$

This is proved in [War01a].

In what follows we study the divisibility properties of Reed-Muller and Projective Reed-Muller codes.

### 3.1 The divisibility of Reed-Muller codes

#### 3.1.1 Affine Reed-Muller codes

We consider affine Reed-Muller codes. Since for $r = 0$, the code $\mathcal{RM}_{\mathbb{F}_q}(r, m)$ is trivially seen to be divisible by $q^m$, we will generally assume the degree of the defining polynomials is $r \geq 1$. We first give the proof of a result of Chevalley and Warning which, despite being much weaker than the main theorem of this section (Theorem 3.1.3), serves as a good explanation of the main idea used in its proof.

**Theorem 3.1.1** (Chevalley-Warning). Let $F$ be a polynomial in $\mathbb{F}_q[X_1, \ldots, X_m]$ with degree less than $m$. Then

$$N(F) \equiv 0 \pmod{p}.$$  

**Proof.** The essential fact is the following: since $F$ takes values in $\mathbb{F}_q$, we have for any $x \in \mathbb{A}^m(\mathbb{F}_q)$

$$F(x)^{q-1} = \begin{cases} 0 & F(x) = 0 \\ 1 & F(x) \neq 0. \end{cases}$$

Consequently, in $\mathbb{F}_q$ we get

$$N(F) = q^m - \sum_{x \in \mathbb{A}^m(\mathbb{F}_q)} F(x)^{q-1} \equiv - \sum_{x \in \mathbb{A}^m(\mathbb{F}_q)} F(x)^{q-1} \pmod{p}. $$
Now since the degree of $F$ is less than $m$, $F^{q-1}$ is a linear combination of monomials of degree $< m(q - 1)$. Thus our conclusion follows from Corollary 2.1.7.

We explain what this Theorem means in terms of divisibility. Recall that Reed-Muller codes come from evaluation of degree $\leq r$ polynomials over the whole affine space $\mathbb{A}^m(\mathbb{F}_q)$. Let $F \in \mathbb{F}_q[X_1, \ldots, X_m]_{\leq r}$, and let $f$ be its image in $\mathcal{R.M}_{\mathbb{F}_q}(r, m)$. If $N(F)$ denotes the number of zeroes in $\mathbb{A}^m(\mathbb{F}_q)$ of $F$, and $wt(f)$ the weight of the codeword $f$, then it is clear that

$$\text{wt}(f) = \#\mathbb{A}^m(\mathbb{F}_q) - N(F) = q^m - N(F).$$

In particular, for any $a$ such that $p^a | q^m$, we have that

$$p^a | \text{wt}(f) \quad \text{if and only if} \quad p^a | N(F).$$

Hence, in terms of divisibility of Reed-Muller codes, we have:

**Corollary 3.1.2.** The code $\mathcal{R.M}_{\mathbb{F}_q}(r, m)$ is divisible by $p$ if $r < m$.

In fact, a much stronger result holds. It is the following theorem of Ax.

**Theorem 3.1.3** (Ax, [Ax64]). Let $F = F(X_1, \ldots, X_m)$ be a polynomial of total degree $r \geq 1$ over $\mathbb{F}_q$. If $b$ is the largest integer strictly less than $m/r$, then $q^b$ divides the number of zeroes of $F$. In other words, the number of solutions of $F$ in $\mathbb{F}_q$ is divisible by

$$q^{\lfloor m/r \rfloor - 1} = q^{\lfloor (m-1)/r \rfloor}.$$

**Remark 3.1.1.1.** The equality $\lfloor m/r \rfloor - 1 = \lfloor (m-1)/r \rfloor$ follows from the fact that $r \geq 1$. Indeed, in that case, there is a unique integer $j$ so that $jr \leq m - 1 < m \leq (j+1)r$. From this, it follows that $\lfloor (m-1)/r \rfloor = j$ while $\lfloor m/r \rfloor - 1 = (j+1) - 1 = j$.

As before, this statement translates easily in terms of coding theory.

**Corollary 3.1.4.** For $r \geq 1$, the code $\mathcal{R.M}_{\mathbb{F}_q}(r, m)$ is divisible by $q^{\lfloor m/r \rfloor - 1} = q^{\lfloor (m-1)/r \rfloor}$.

The complete proof of this theorem is quite technical and will not be exposed here. It can be found in [Ax64]. In what follows we will give Borissov’s proof of the special case $q = 2$. In that case, Ax’s Theorem is sometimes called McEliece’s Theorem.

It is natural to ask if that is the best possible divisibility of this code. In terms of power of $p$, the answer is yes and comes from an example at the end of Ax’s paper [Ax64].
CHAPTER 3. DIVISIBILITY

To show this, it is enough to exhibit a polynomial with degree \( \leq r \) and with a number of zeroes which does not divide a higher power of \( p \). Suppose first that the number of variables is \( m = ar \) for some integer \( a \). We claim that the following polynomial satisfies our criterion:

\[
G_{a,r} := X_1 \cdots X_r + X_{r+1} \cdots X_{2r} + \cdots + X_{(a-1)r+1} \cdots X_{ar}.
\]

We prove by induction on \( a, r \) that the highest power of \( p \) dividing \( N(G_{a,r}) \) is \( q^{a-1} \). If \( a = r = 1 \), \( G_{1,1} = X_1 \) and has only the trivial zero, so the assertion is true. For general \( a, r \) observe that \( N(p)^{G_{a,r}} \) is:

\[
N(G_{a+1,r}) = N(G_{a,r})N(G_{1,r}) + (q^{ar} - N(G_{a,r})(q-1)^{r-1})
\]

\[
= qN(G_{a,r})(q^{r-1} - (q-1)^{r-1}) + q^{ar}(q-1)^{r-1}
\]

from which the desired conclusion follows.

Now for general \( m \), write \( m = br + h \) where \( 0 < h \leq r \). In that way, \( b \) is the largest integer strictly less than \( m/r \). Define

\[
F(X_1, \ldots, X_m) = G_{b,r}(X_1, \ldots, X_{br}) + (X_{br+1} \cdots X_m)1_{h>1}
\]

(\( 1_{h>1} \) is the indicator function, whose value is one if \( h > 1 \) and zero otherwise). We claim that the highest power of \( p \) dividing \( N(F) \) is \( q^h \). If \( h = 1 \), then it is clear that \( N(F) = qN(G_{b,r}) \) and we are done. If \( h > 1 \), we have, as before

\[
N(F) = \#\{\text{zeroes of } G_{b,r} \text{ and } X_{br+1} \cdots X_m\}
\]

\[
+ \#\{(x_1, \ldots, x_m) \mid G_{b,r}(x_1, \ldots, x_{br}) = x_{br+1} \cdots x_m\}
\]

\[
= N(G_{b,r})N(X_1 \cdots X_h) + (q^{br} - N(G_{b,r})(q-1)^{h-1})
\]

\[
= qN(G_{b,r})(q^{h-1} - (q-1)^{h-1}) + q^{br}(q-1)^{h-1}.
\]

and our conclusion follows easily from this.
3.1.2 Borissov’s Proof

In this section we prove the special case of Ax’s Theorem when \( q = 2 \), i.e. for standard Reed-Muller codes over \( \mathbb{F}_2 \). The proof is inspired from Borissov’s proof in [Bor13]. We extend the notion of weight to any function \( f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2 \) naturally, i.e. as

\[
\text{wt}(f) = \# \{(x_1, \ldots, x_m) \in \mathbb{F}_2^m \mid f(x_1, \ldots, x_m) \neq 0\}.
\]

If \( f \) comes from a polynomial of degree \( r \), this coincides with the weight of its corresponding codeword in \( \mathcal{R}\mathcal{M}(r, m) \).

We restate the special case of Theorem 3.1.3 when \( q = 2 \).

**Theorem 3.1.5.** For \( r \geq 1 \), \( \mathcal{R}\mathcal{M}(r, m) \) is divisible by \( 2^{\lceil (m-1)/r \rceil} \).

The main ingredient of the proof is the following relation on the weight of a sum.

**Lemma 3.1.6.** Let \( g_1, \ldots g_n : \mathbb{F}_2^m \rightarrow \mathbb{F}_2 \) be arbitrary functions. Then

\[
\text{wt} \left( \sum_{i=1}^{n} g_i \right) = \sum_{l=1}^{n} (-2)^{l-1} \sum_{1 \leq i_1 < i_2 < \cdots < i_l \leq n} \text{wt}(g_{i_1} \cdots g_{i_l})
\]

*Proof.* Induction on \( n \). If \( n = 1 \), it is trivial. If \( n = 2 \), we have

\[
\begin{align*}
\text{wt}(g_1 + g_2) &= \# \{ x \mid g_1(x) + g_2(x) = 1 \} \\
&= \# \{ x \mid g_1(x) = 1, g_2(x) = 0 \} + \# \{ x \mid g_1(x) = 0, g_2(x) = 1 \} \\
&= \text{wt}(g_1) - \# \{ x \mid g_1(x) = 1 = g_2(x) \} + \text{wt}(g_2) - \# \{ x \mid g_1(x) = 1 = g_2(x) \} \\
&\equiv \text{wt}(g_1) + \text{wt}(g_2) - 2 \text{wt}(g_1g_2)
\end{align*}
\]

(in \( * \) we used that \( g_1(x)g_2(x) = 1 \iff g_1(x) = 1 = g_2(x) \)).

Suppose \( n \geq 3 \). Writing \( \sum_{i=1}^{n} g_i = (\sum_{i=1}^{n-1} g_i) + g_n \) and applying the case \( n = 2 \) to these two functions, we get

\[
\text{wt} \left( \sum_{i=1}^{n} g_i \right) = \text{wt} \left( \sum_{i=1}^{n-1} g_i \right) + \text{wt}(g_n) - 2 \text{wt} \left( \sum_{i=1}^{n-1} g_i g_n \right).
\] (3.1)

By induction, the term on the right is

\[
-2 \text{wt} \left( \sum_{i=1}^{n-1} g_i g_n \right) = \sum_{k=1}^{n-1} (-2)^{k} \sum_{1 \leq j_1 < \cdots < j_k \leq n-1} \text{wt}(g_{j_1} \cdots g_{j_k} g_n).
\]
CHAPTER 3. DIVISIBILITY

Writing \( A \) as

\[
\sum_{1 \leq j_1 < \cdots < j_{k+1} \leq n} \text{wt}(g_{j_1} \cdots g_{j_k} g_{j_{k+1}}) - \sum_{1 \leq j_1 < \cdots < j_k \leq n-1} \text{wt}(g_{j_1} \cdots g_{j_k}) \text{wt}(g_{j_{k+1}}),
\]

and making the change of variables \( l = k + 1 \), we get

\[
-2 \text{wt} \left( \sum_{i=1}^{n-1} g_{il} g_{in} \right) = \left( \sum_{l=2}^{n} (-2)^{l-1} \right) \cdot \left( \sum_{1 \leq j_1 < \cdots < j_l \leq n} \text{wt}(g_{j_1} \cdots g_{j_l}) - \sum_{1 \leq j_1 < \cdots < j_l \leq n-1} \text{wt}(g_{j_1} \cdots g_{j_l}) \right).
\]

Substituting in (3.1) and applying induction again to \( \text{wt} \left( \sum_{i=1}^{n-1} g_i \right) \), we get

\[
\text{wt} \left( \sum_{i=1}^{n} g_i \right) = \sum_{l=1}^{n-1} (-2)^{l-1} \sum_{1 \leq i_1 < \cdots < i_l \leq n-1} \text{wt}(g_{i_1} \cdots g_{i_l}) + \text{wt}(g_n) + \sum_{l=2}^{n} (-2)^{l-1} \sum_{1 \leq i_1 < \cdots < i_l \leq n} \text{wt}(g_{i_1} \cdots g_{i_l})
\]

proving the desired result. \( \square \)

Before proving Theorem 3.1.5, we make a few considerations on how this lemma can be applied. Let \( f \in \mathcal{RM}(r, m) \). Since the base field is \( \mathbb{F}_2 \), we can write

\[
f = \sum_{i=1}^{n} g_i \]

where all the \( g_i \) are monomials of degree \( \leq r \) (recall that we mean monic monomials).

Since any \( x \in \mathbb{F}_2 \) satisfies \( x^2 = x \), the monomial \( X_1^2 \) gives rise to the same function \( \mathbb{F}_2^m \to \mathbb{F}_2 \) as the monomial \( X_1 \). Similarly, we see that any monomial \( X_1^{e_1} \cdots X_m^{e_m} \), when seen as a function \( \mathbb{F}_2^m \to \mathbb{F}_2 \), is the same as the monomial \( X_1^{\min(e_1, 1)} \cdots X_m^{\min(e_m, 1)} \). Thus we can assume that the exponent of any variable \( X_j \) is at most 1 in all the monomials \( g_i \). Observe that in that case, saying that \( \text{deg}(g_i) \leq r \) is equivalent to saying that no more than \( r \) variables appear in the monomial \( g_i \).

We now get to the proof of the main theorem.
**Proof of Theorem 3.1.5** Let \( f \in \mathcal{RM}(r, m) \) be written as \( f = \sum_{i=1}^{n} g_i \), with \( g_i \) monomials of degree \( \leq r \). By our previous considerations, we can assume that all the \( g_i \) are monomials with all exponents \( \leq 1 \), and in which no more than \( r \) variables occur.

Applying the weight formula gives

\[
\text{wt}(f) = \sum_{l=1}^{n} 2^{l-1} \left( \sum_{1 \leq i_1 < \cdots < i_l \leq n} \text{wt}(g_{i_1} \cdots g_{i_l}) \right)
= \sum_{l=1}^{\left\lfloor \frac{m-1}{r} \right\rfloor} 2^{l-1} S_l + 2^{\left\lfloor \frac{m-1}{r} \right\rfloor - 1} \left( \sum_{l=1}^{n} 2^{l-1-\left\lfloor \frac{m-1}{r} \right\rfloor} S_l \right).
\]

Hence, for our divisibility conclusions, it is enough to focus on the first sum \( S \).

We analyze the structure of \( S_l \). Suppose given \( l \) integers \( 1 \leq i_1 < \cdots < i_l \leq n \). Then the monomial \( g := g_{i_1} \cdots g_{i_l} \) has \( \leq lr \) variables. We want to compute \( \text{wt}(g) \). Upon permuting the variables, we can assume that only \( X_1, \ldots, X_s \) occur with positive power in \( g \), with \( s \leq lr \). Since we assumed that all exponents in the \( g_i \) are not greater than 1, we can write

\[
g = X_1 \cdots X_s.
\]

It is clear that \( g(x_1, \ldots, x_m) \neq 0 \) if and only if \( x_1 = \cdots = x_s = 1 \). Thus

\[
\text{wt}(g) = \# \{ x \mid x_1 = \cdots = x_s = 1 \} = 2^{m-s}.
\]

If we now assume that \( l \leq \frac{m-1}{r} \), \( 2^{m-lr} \) is an integer and since \( s \leq lr \) we get that

\[
\text{wt}(g) = 2^{m-lr} a(g)
\]

where \( a(g) = 2^{lr-s} \) is an integer.

This conclusion holds for every choice of integers \( 1 \leq i_1 < \cdots < i_l \leq n \), with \( l \leq \left\lfloor \frac{m-1}{r} \right\rfloor \), so for such \( l \) we can write

\[
S_l = (-1)^{l-1} \sum_{1 \leq i_1 < \cdots < i_l \leq n} \text{wt}(g_{i_1} \cdots g_{i_l}) = 2^{m-lr} (-1)^{l-1} \sum_{1 \leq i_1 < \cdots < i_l \leq n} a(g_{i_1} \cdots g_{i_l}).
\]

Substituting in \( S \), we get

\[
S = \sum_{l=1}^{\left\lfloor \frac{m-1}{r} \right\rfloor} 2^{l-1} S_l = \sum_{l=1}^{\left\lfloor \frac{m-1}{r} \right\rfloor} 2^{l-1+m-lr} T_l.
\]
But for $l \leq \frac{m-1}{r}$, we have
\[
l - 1 + m - lr = l(1 - r) + m - 1
\]
\[
\geq \frac{m - 1}{r} \cdot (1 - r) + m - 1
\]
\[
= \frac{m - 1}{r},
\]
(in $(*),$ we use that $r \geq 1$) and so $2^{l - 1 + m - lr}$ is divisible by $2^{\frac{m - 1}{r}}$.
Thus $S$ is also divisible by $2^{\frac{m - 1}{r}}$, which is what we wanted to prove. 

3.1.3 Projective Reed-Muller codes

We finally discuss projective Reed-Muller codes. Projective Reed-Muller codes are similar in many points to standard Reed-Muller codes. Their dimension is computed similarly, and their minimal distance is the same. It is therefore not a surprise to learn that their divisibilities are equal. However, some care must be taken.

In the case of $\mathcal{RM}$-codes, we showed that the weight of a codeword $f$ coming from a polynomial $F \in k[X_1, \ldots, X_m]$ is simply
\[
\text{wt}(f) = \#A^m(k) - \#(\text{affine zeroes of } F)
\]
\[
= q^m - \#(\text{affine zeroes of } F)
\]
Therefore we could conclude that if some power of $p$ divides the number of zeroes of $F$, then the same power of $p$ divides the weight of $f$.

In the projective space, a similar formula holds, but with different conclusions: If $F \in k[X_0, \ldots, X_m]^h$ is a homogeneous polynomial, we can now consider its projective zeroes. Let $f$ denotes its associated codeword; we have
\[
\text{wt}(f) = \#P^m(k) - \#(\text{projective zeroes of } F)
\]
\[
= q^m + q^{m-1} + \cdots + q + 1 - \#(\text{projective zeroes of } F).
\]
Thus the number of zeroes of $F$ and the weight of $f$ are never divisible by the same power of $p$ (except the trivial power $p^0 = 1$). However, it turns out that in our case the powers of $p$ tend to divide more the weight of $f$ than the number of zeroes of $F$, which is to our advantage.

We compute the divisibility of these codes. As for the affine case, the divisibility of a $\mathcal{PRM}_{F_q}(r, m)$ code is uninteresting for $r = 0$: it is clearly seen to be $q^m$. This very simple argument comes from [Bon01].
Proposition 3.1.7. For \( r \geq 1 \), \( \mathcal{P \mathcal{R} \mathcal{M}}_q(r, m) \) is divisible by \( q^{[(m+1)/r]-1} = q^{[m/r]} \).

Proof. Let \( F \in k[X_0, \ldots, X_m]^h \) be a homogeneous polynomial of degree \( r \). We can consider its zeroes both in \( \mathbb{P}^m(\mathbb{F}_q) \) (call those the projective zeroes) and in \( \mathbb{A}^{m+1}(\mathbb{F}_q) \) (call those the affine zeroes). It is clear that each of its projective zeroes correspond to \((q-1)\) affine zeroes. Moreover, since \( F \) is homogeneous, the affine point \((0, \ldots, 0) \in \mathbb{A}^{m+1}(\mathbb{F}_q) \) is also a zero of \( F \). Therefore, we have

\[
\#\{\text{projective zeroes of } F\} = \frac{\#\{\text{affine zeroes of } F\} - 1}{q-1}.
\]

Now by Ax’s Theorem, the number of zeroes of \( F \) in \( \mathbb{A}^{m+1}(\mathbb{F}_q) \) is divisible by \( q^{[m/r]} \):

\[
\#\{\text{affine zeroes of } F\} = q^{[m/r]}u, \quad u \in \mathbb{N}.
\]

Therefore,

\[
\text{wt}(f) = \#\mathbb{P}^m(\mathbb{F}_q) - \#\{\text{projective zeroes of } F\}
= \frac{q^{m+1} - 1}{q-1} - \frac{\#\{\text{affine zeroes of } F\} - 1}{q-1}
= \frac{q^{m+1} + q^{[m/r]}u}{q-1}.
\]

Now this is value is clearly an integer, and since \( q \) and \( q-1 \) are coprime, \( q^{[m/r]} \) divides this fraction if and only if it divides the numerator. But this is trivially verified, and the proposition is proved. \( \square \)

An obvious but interesting corollary is the following:

Corollary 3.1.8. Let \( F \in k[X_0, \ldots, X_m]^h \) be a homogeneous degree \( r \) polynomial. If \( r \leq m \), then

\[
\#\{\text{projective zeroes of } F\} \equiv 1 \pmod{q}.
\]

In particular, \( F \) has at least one zero in \( \mathbb{P}^m(\mathbb{F}_q) \).

In the next section, we will analyze more in detail this number of zeroes, using a geometrical approach.
3.2 Weil’s Method: a geometrical point of view

In the previous section, we presented a theorem which solves the question of divisibility of affine and projective Reed-Muller codes (at least up to powers of the characteristic of the base field). In particular, we ended it with a theorem on the zeroes of homogeneous polynomials in the projective space.

The goal of this section is to present a more geometrical approach to counting the various zeroes of polynomials. Indeed, we know that the number of zeroes must be coprime to $q$ but this does not help us determine the actual number of these zeroes. The goal of this section is to present a theorem of Weil, which we then illustrate by an example.

**Theorem 3.2.1** (Weil). Let $X$ be a smooth projective surface defined over $\mathbb{F}_q$, and let $\bar{X}$ be the surface obtained by extending the scalars to $\overline{\mathbb{F}_q}$, the algebraic closure of $\mathbb{F}_q$. If the surface $\bar{X}$ is birational to $\mathbb{P}^2$, then the number $\#X(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points is

$$\#X(\mathbb{F}_q) = q^2 + q \text{Tr}(\varphi) + 1,$$

where $\varphi : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$ is the Frobenius automorphism (sending $x \mapsto x^q$), and $\text{Tr}(\varphi)$ denotes its trace in the representation of $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ on $\text{Pic}(\bar{X})$.

The proof can be found in [Man86, Chap. IV, §27].

In the case when the surface $X$ can be embedded in $\mathbb{P}^3$, then it can be given by a single polynomial equation, say $X = V(F)$. Then this theorem gives us explicitly the number of zeroes of this polynomial $F$, and if $f$ denotes the associated projective codeword, then it is clear that

$$\text{wt}(f) = q^3 + q^2 + q + 1 - \#X(\mathbb{F}_q) = q^3 + q(1 - \text{Tr}(\varphi)).$$

Comparing this expression with the divisibility factor of $q^{3/r}$ assured by Proposition 3.1.7 (where $r$ is the degree of $F$), we see that $\text{Tr}(\varphi)$ must be one if $r = 1$ and that it can be $\leq 1$ in the other cases.

The first two parts of this section are devoted to the understanding of this formula. They are mainly inspired from [Bri08]. In the third part we give an example of its use to compute the number of $\mathbb{F}_q$-rational points of a surface.
3.2.1 The Picard group

Let $X$ be a smooth irreducible quasi-projective variety over a field $k$.

**Definition 3.2.2.** A **prime divisor** on $X$ is an irreducible closed subvariety $Z \subset X$ of codimension one, defined over $k$. A **divisor** is an element of the free abelian group with the set of all prime divisors as basis. Explicitly, a divisor is an element of the form

$$D = \sum_Z n_Z \cdot Z$$

where the sum ranges over all prime divisors of $X$, and almost all $n_Z$ are zero (i.e. all but a finite number of $n_Z$). The set of divisors is denoted $\text{Div}(X)$.

Among all divisors, there are some which arise from rational functions on $X$. We explain their construction.

Let $Z$ be a subvariety of $X$ of codimension one. By Proposition 1.3.16, $\mathcal{O}_{Z,X}$ is a discrete valuation ring. If $v_Z$ denotes this valuation, then it can be extended to the field of fractions of $\mathcal{O}_{Z,X}$ which is identified with $K(X)$, so we get a valuation $v_Z : K(X) \to \mathbb{Z}$, for all prime divisors $Z$.

Now let $f \in K(X)$ be fixed. We claim that $v_Z(f)$ is zero for all but finitely many prime divisors $Z$. Suppose $f$ is defined on an open set $U \subset X$ as a quotient of homogeneous polynomials $g/h$, with $h$ nowhere zero on $U$, and consider the closed algebraic set $V(g) \cup V(h) = V(gh)$. Let $Z$ be a prime divisor of $X$, and assume first that it intersects the open set $U := X \cap D(gh) = X \setminus V(gh)$. Then $f$ is non-zero on a non-empty open set of $Z$, namely $U \cap Z$. Thus it has an inverse in $\mathcal{O}_{Z,X}$: it is the function represented by $h/g$ on $U$. This implies that its valuation at $Z$ is zero.

Now if a prime divisor $Z$ does not intersect $U$, then it must be contained in $V(gh)$. This is a closed subset, and hence it admits a unique decomposition into closed irreducible subsets:

$$V(gh) = Z_1 \cup \cdots \cup Z_n.$$

Among those $Z_j$, some may be of codimension one, and some may be of codimension 2 or more. However, in any case, there are finitely many codimension one irreducible closed subsets of $V(gh)$, and thus finitely many $Z$ for which $v_Z(f)$ can be non-zero.

Therefore we can make the following definition.
**Definition 3.2.3.** Let $f \in K(X)$ be a rational function on $X$. The **divisor of** $f$ is

$$\text{div } f = (f) = \sum_{Z} v_Z(f) \cdot Z.$$  

Divisors of this form are called **principal divisors**; the set of principal divisors is denoted $\text{PDiv}(X)$. Two divisors $D, D' \in \text{Div}(X)$ are **linearly equivalent** if

$$D - D' = (f)$$

for some $f \in K(X)$. We denote it by $D \equiv D'$. The **Picard group** of $X$ is the quotient

$$\text{Pic}(X) = \text{Div}(X)/\text{PDiv}(X).$$

There are other definitions of the Picard group, but for a projective variety all are equivalent to this one. See [Har77, Chap. 2, Section 6] for precisions.

We will make use of the following exact sequence, which is easily proven.

**Proposition 3.2.4.** Let $X$ be a smooth quasi-projective variety, and let $Z$ be a prime divisor on $X$. There is an exact sequence

$$Z \to \text{Pic}(X) \to \text{Pic}(X \setminus Z) \to 0,$$

where the first map sends $1 \mapsto Z$ and the second one sends a prime divisor $Y \subset X$ to $Y \cap (X \setminus Z)$ if this intersection is non-empty, and zero otherwise.

**Proof.** Let $U = X \setminus Z$. If $Y$ is a prime divisor of $U$, then it is clear that its closure $\bar{Y}$ in $X$ is also irreducible, and that $\bar{Y} \cap U = Y$. Thus $\text{Pic}(X) \to \text{Pic}(U)$ is surjective. For the part $Z \to \text{Pic}(X) \to \text{Pic}(U)$, the composition is clearly zero, so the kernel of the second map is in the image of the first. Conversely, suppose that some divisor $D$ has trivial image in $\text{Pic}(U)$. This implies that the support of $D$ is contained in $\{Z\}$, whence that $D = aZ$ for some $a \in Z$. Therefore the sequence is exact. \[\square\]

Using this proposition, we can show an interesting result on the generation of $\text{Pic}(X)$ (which will be useful in what follows).

**Corollary 3.2.5.** Let $X$ be a smooth quasi-projective variety, and $Y \subset X$ a closed subset of codimension 1. Suppose $\text{Pic}(X \setminus Y)$ is trivial. Then $\text{Pic}(X)$ is generated by the irreducible components of $Y$. In particular, $\text{Pic}(X)$ is finitely generated.
Proof. Induction on the number of irreducible components of $Y$. If $Y$ is irreducible, then the conclusion follows from the exact sequence of the proposition, which becomes

$$ZY \to \text{Pic}(X) \to 0 \to 0.$$  

Assume $Y = Y_1 \cup \cdots \cup Y_n$ with the $Y_j$ irreducible. Since $X \setminus Y = (X \setminus Y_n) \setminus (Y_1 \cup \cdots \cup Y_{n-1})$, the induction hypothesis gives that $\text{Pic}(X \setminus Y_n)$ is generated by $Y_1, \ldots, Y_{n-1}$. Thus we have a commutative diagram

$$\begin{array}{ccc}
ZY_1 \oplus \cdots \oplus ZY_{n-1} & ZY_1 \oplus \cdots \oplus ZY_{n-1} \\
\downarrow & \downarrow \\
ZY_n \longrightarrow \text{Pic}(X) \longrightarrow \text{Pic}(X \setminus Y_n) \longrightarrow 0 \\
\downarrow & \\
0.
\end{array}$$

A diagram chase gives that for any $D \in \text{Pic}(X)$, there exists a $D' \in ZY_1 \oplus \cdots \oplus ZY_{n-1}$ such that $D - D'$ has zero image in $\text{Pic}(X \setminus Y_n)$. But then, there is some $aY_n \in ZY_n$ with $D - D' = aY_n$ by exactness of the middle row. The conclusion follows. \qed

Finally, one last element will be needed in what follows. It is the notion of intersection number. We will define it only for surfaces (varieties of dimension 2). In that particular case, codimension one subvarieties are also of dimension one, and are hence curves.

**Definition 3.2.6.** Let $X$ be a smooth projective surface. Two curves $C, C'$ of $X$ are said to intersect transversally if for every point $P \in C \cap C'$, there are two elements $f, f'$ in the local ring $\mathcal{O}_{P,X}$ such that:

1. The maximal ideal of $\mathcal{O}_{P,X}$ is generated by $f$ and $f'$.
2. There exists a neighborhood $U$ of $P$ such that $f$ can be written as a quotient of homogeneous polynomials of the same degree $f = g/h$, with $h$ nowhere zero on $U$ and such that $U \cap C = U \cap V(f) = U \cap V(g)$.
3. The same holds for $C'$ and $f'$.

If that is the case, their intersection number is

$$C \cdot C' := #(C \cap C').$$

The most interesting application of this intersection number is the following:
Theorem 3.2.7. Let $X$ be a smooth projective surface. There is a unique symmetric bilinear form

$$\operatorname{Div}(X) \times \operatorname{Div}(X) \rightarrow \mathbb{Z}$$

$$(D, D') \mapsto D \cdot D'$$

such that

1. If $C, C'$ are nonsingular curves intersecting transversally, then $C \cdot C'$ is simply the intersection number of $C$ and $C'$ defined before.

2. If two divisors $D, D'$ are linearly equivalent, then

$$D \cdot D_0 = D' \cdot D_0$$

for any divisor $D_0$.

Proof. Theorem V.1.1 of [Har77].

Definition 3.2.8. The induced symmetric bilinear form $\operatorname{Pic}(X) \times \operatorname{Pic}(X) \rightarrow \mathbb{Z}$ is called the intersection number of the divisors.

Now that we defined enough background in algebraic geometry, we proceed to the definition of the Frobenius map on the Picard group of a smooth surface.

### 3.2.2 The Frobenius map

In this subsection we assume that $k = \mathbb{F}_q$ for $q$ a power of the prime $p$. We denote by $\bar{k}$ the algebraic closure of $k$.

Definition 3.2.9. The Frobenius automorphism $\varphi$ is the generator of the cyclic Galois group $\operatorname{Gal}(\bar{k}/k)$ given by the map

$$\varphi : \bar{k} \rightarrow \bar{k}$$

$$x \mapsto x^q.$$

If $F \in \bar{k}[X_1, \ldots, X_m]$ is a polynomial with coefficients in $\bar{k}$, we define $\varphi(F)$ to be simply the polynomial obtained by applying $\varphi$ to each coefficient of $F$. 
CHAPTER 3. DIVISIBILITY

Because it is an automorphism, it is clear that $\varphi$ is linear. Thus it acts on $\mathbb{P}^n(\bar{k})$ as follows:

\[
\varphi : \mathbb{P}^n(\bar{k}) \longrightarrow \mathbb{P}^n(\bar{k})
\]

\[
(x_0 : \cdots : x_n) \longmapsto (x_0^q : \cdots : x_n^q).
\]

Let $X$ be a projective variety over $k$, and let $\bar{X}$ denote the variety obtained by extending scalars to $\bar{k}$. Since $X$ is defined over $k$, we can find homogeneous polynomials $f_1, \ldots, f_r$ in $k[X_0, \ldots, X_m]$ with $X = V_{\mathbb{P}^m(\bar{k})}(f_1, \ldots, f_r)$, and consequently $\bar{X} = V_{\mathbb{P}^m(\bar{k})}(f_1, \ldots, f_r)$. Now since these polynomials have coefficients in $k$, they are fixed by $\varphi$ and so

\[
\varphi(\bar{X}) = \varphi(V_{\mathbb{P}^m(\bar{k})}(f_1, \ldots, f_r)) = V_{\mathbb{P}^m(\bar{k})}(\varphi(f_1), \ldots, \varphi(f_r)) = V_{\mathbb{P}^m(\bar{k})}(f_1, \ldots, f_r) = \bar{X}.
\]

Therefore, $\varphi$ acts on $\bar{X}$.

Moreover, if $Z$ is a prime divisor of $\bar{X}$, then $\varphi(Z)$ is still irreducible, and of codimension one. Thus $\varphi(Z)$ is another prime divisor of $\bar{X}$ (observe that we may not have $\varphi(Z) = Z$ since $Z$ is not defined over $k$). Extending by $\mathbb{Z}$-linearity, we get a linear action of $\text{Gal}(\bar{k}/k)$ on the group $\text{Div}(\bar{X})$ of divisors of $\bar{X}$.

Finally, if $D, D' \in \text{Div}(\bar{X})$ and $D = D' + (f)$ for some $f \in K(\bar{X})$, then we trivially have

\[
\varphi(D) = \varphi(D') + (\varphi(f)),
\]

so $\varphi$ preserves linear equivalence of divisors and thus, $\text{Gal}(\bar{k}/k)$ acts linearly on $\text{Pic}(\bar{X})$.

Now that we have defined the action of the Galois group, we need to define the trace. On a finite dimensional vector space, the trace of a linear map is the sum of the diagonal coefficients of its matrix form, after choosing a basis (and this value is independent of the choice of the basis). This definition extends to any free module of finite rank.

In our case however, there are two problems:

1. $\text{Pic}(\bar{X})$ is not necessarily a free module.

2. $\text{Pic}(\bar{X})$ is not necessarily finitely generated.

The first problem can easily be solved, either by quotienting out the torsion elements to get a free $\mathbb{Z}$-module, or by taking the tensor product over $\mathbb{Z}$ with $\mathbb{Q}$. It is clear that a $\mathbb{Z}$-basis of the first construction corresponds to a $\mathbb{Q}$-basis of the second, so the trace is the same.
In general, the second problem cannot be solved, in the sense that it may well happen that \( \text{Pic}(\tilde{X}) \) is not finitely generated. However, if \( X \) is smooth, projective and defined over \( k = \mathbb{F}_q \), we have the following non-trivial result.

**Theorem 3.2.10.** Let \( X \) be a smooth projective surface over \( \mathbb{F}_q \). Then \( \text{Pic}(\tilde{X}) \) is finitely generated.

**Proof.** This is Corollaire 2 of [Kah06]. Observe that \( X \) smooth \( \implies \) \( X \) normal, \( X \) projective \( \implies \) \( X \) of finite type over \( \text{Spec} \mathbb{F}_q \).

However, in our case we can get away with a simple argument, since the surface considered in Weil’s Theorem are birationally trivial (once seen as varieties over the algebraic closure). Indeed, if a surface \( X \) is birational to \( \mathbb{P}^2 \), then there is a non-empty open set \( U \subset X \) which is isomorphic to an open set of \( \mathbb{P}^2 \). Upon restricting this open set, we may assume that \( U \) is isomorphic to an open set \( V \subset \mathbb{A}^2 \). Using the exact sequence of Proposition 3.2.4, we see that \( \text{Pic}(\mathbb{A}^2) \) surjects onto \( \text{Pic}(V) \cong \text{Pic}(U) \). But \( \text{Pic}(\mathbb{A}^2) \) is trivial ([Har77, Proposition II.6.2] applied to \( A = k[X_1, X_2] \) which is a U.F.D.) and hence \( \text{Pic}(U) = 0 \). Now if \( X \setminus U \) is of codimension 1, then we can apply Corollary 3.2.5 to see that \( \text{Pic}(X) \) is finitely generated. If \( X \setminus U \) is of codimension \( \geq 2 \), then a prime divisor \( Z \) of \( X \) corresponds to a prime divisor \( Z \cap U \) of \( U \) (this intersection is non-empty since \( \text{codim}_X(X \setminus U) \geq 2 \)). Thus \( Z \cap U = (f) \) for some \( f \in K(U) = K(X) \), and it is easy to see that \( Z = (f) \). Therefore, any such \( Z \) is equivalent to zero and \( \text{Pic}(X) \) is simply zero.

### 3.2.3 Example of use

We will give an example of this formula by computing explicitly first the Picard group, and then the trace of the Frobenius map on it. We consider smooth quadrics in \( \mathbb{P}^3 \) defined over \( \mathbb{F}_q \). Suppose the variables of the homogeneous polynomials are \( x, y, z, w \).

As shown in [Hir85] (and also in [CD13]), there are only two types of smooth quadrics up to \( \mathbb{F}_q \) isomorphism:

1. The **elliptic** quadrics, isomorphic over \( \mathbb{F}_q \) to the variety \( V(xy - zw) \subset \mathbb{P}^3 \).
2. The **hyperbolic** quadrics, isomorphic over \( \mathbb{F}_q \) to the variety \( V(f(x, y) - zw) \subset \mathbb{P}^3 \).
where \( f \in \mathbb{F}_q[x, y] \) is an irreducible homogeneous polynomial over \( \mathbb{F}_q \) of degree 2.

We first study the elliptic quadric. Let \( E = V(xy - zw) \subset \mathbb{P}^3(\mathbb{F}_q) \), and let \( \tilde{E} \) be the same variety seen in \( \mathbb{P}^3(\overline{\mathbb{F}_q}) \). \( E \) is then a smooth surface (as is easily shown by computing the partial derivatives), and we claim that it is birational to \( \mathbb{P}^2 \).

If \( U = D(w) \cap \tilde{E} \) is the open subset of \( \tilde{E} \) given by \( w \neq 0 \), then we claim that \( U \cong \mathbb{A}^2 \).

We define the morphisms

\[
U \longrightarrow \mathbb{A}^2 \quad (x : y : z : w) \longmapsto (x/w, y/w) \quad \text{and} \quad \mathbb{A}^2 \longrightarrow U \quad (x', y') \longmapsto (x' : y' : x'y' : 1).
\]

It is clear that these two maps are regular on their domain of definition, and that they are inverses to each other, so \( U \cong \mathbb{A}^2 \) (observe that in particular, \( \text{Pic}(U) = 0 \)). Therefore, this surface is birational to \( \mathbb{P}^2 \), and Weil's Theorem can be applied to it.

Now observe that \( \tilde{E}\backslash U = V(w) \subset \tilde{E} \) is composed of two lines

\[
l_x = V(x, w) \subset \tilde{E} \quad \text{and} \quad l_y = V(y, w) \subset \tilde{E}.
\]

Therefore, Corollary 3.2.5 tells us that \( \text{Pic}(\tilde{E}) \) is generated by these two lines, i.e. the sequence

\[
\mathbb{Z}l_x \oplus \mathbb{Z}l_y \rightarrow \text{Pic}(\tilde{E}) \rightarrow 0
\]

is exact (the first map is the inclusion modulo linear equivalence). We claim that this map is an isomorphism.

**Proposition 3.2.11.** The inclusion modulo linear equivalence

\[
\mathbb{Z}l_x \oplus \mathbb{Z}l_y \rightarrow \text{Pic}(\tilde{E})
\]

is an isomorphism.

The following lemma is the key.

**Lemma 3.2.12.** \( l_x \cdot l_y = 1, l_x \cdot l_x = 0 = l_y \cdot l_y \). (The intersection numbers are taken in the sense of divisors).

**Proof.** First, we show that \( l_x \cdot l_y = 1 \). Clearly, \( l_x \cap l_y = \{(0 : 0 : 1 : 0)\} \), so we must show that \( l_x \) and \( l_y \) intersect transversally at \( P = (0 : 0 : 1 : 0) \). In the neighborhood \( D(z) \) of \( P \), we have that \( x \) is a local equation for \( l_x \) (any point \( Q := (a : b : c : d) \in \tilde{E} \cap D(z) \) satisfies \( ab = cd \) and \( c \neq 0 \), whence \( d = c^{-1}ab \), so \( a = 0 \) is a necessary and sufficient
condition for $Q$ to be in $l_x$), and similarly, $y$ is one for $l_y$. Now let $f \in \mathcal{O}_{P,E}$ and suppose that $f$ is regular on $U$. Then, $f$ can be written as a quotient $f = g/h$ on $U$, where $g, h$ are homogeneous polynomials of the same degree (say $d$), and $h$ is nowhere zero on $U$. Thus, $f(P) = 0$ if and only if $g$ has no term $z^d$. But this implies that $f$ is in the ideal of $\mathcal{O}_{P,E}$ generated by $x$ and $y$. We have therefore shown that $l_x$ and $l_y$ intersect transversally at $P$ and so $l_x \cdot l_y = 1$.

For the other part, we prove that $l_x \cdot l_x = 0$, the case for $l_y$ being similar.

Observe first that it is important to speak of intersection number between divisors. The reason for that is that $l_x$ does not intersect transversally with itself, so taking intersection between $l_x$ and $l_x$ as curves is not defined. However, as divisors, it is defined as the intersection number $l_x \cdot C$ with $C$ is another curve linearly equivalent to $l_x$, but intersecting transversally with it.

Therefore, to show that $l_x \cdot l_x = 0$, it is enough to find a curve $C$ which is linearly equivalent to $l_x$, but does not intersect it. We claim that $C := V(y, z)$ is such a curve.

First, it is clear that $l_x \cap C = \emptyset$, so that $l_x \cdot C$ is well defined and zero. Consider the function $f \in K(X)$ given by the quotient of homogeneous polynomials

$$f = \frac{yz}{xw}.$$ 

We claim that the associated divisor is

$$\text{div } f = C - l_x.$$ 

First, it is clear that $v_C(f) = 1$. Indeed, on the open set $U = D(xw) \cap C \subset C$, $f$ is identically zero, so $v_C(f) \geq 1$. Moreover, if $m$ denotes the maximal ideal of $\mathcal{O}_{C,X}$ (recall that $m = \{f \in K(X) \mid f$ is zero on a non-empty open set of $C\}$), then $f \notin m^2$ since $f$ cannot be decomposed as a product of elements in $m$. Hence $v_C(f) = 1$ and similarly, $v_{l_x}(f) = -1$.

Now it remains to show that for any closed codimension one subvariety $Z \subset X$ which is not $C$ or $l_x$, we have

$$v_Z(f) = 0.$$ 

This is equivalent to finding an open set $U \subset X$ with $U \cap X \neq \emptyset$ so that $f$ is non-zero on $U$.

Observe that on the open set $U = D(xyzw) \cap X$, the function $f$ is non-zero. Thus, this shows that $v_Z(f) = 0$ for any closed codimension one subvariety $Z$ of $X$ which has
non-empty intersection with $U$. Now the only subvarieties that remain are the ones which are contained in $X \setminus U = V(xyzw) \cap X = V(xyzw, xy - zw)$.

It is clear that this closed set admits the following decomposition into irreducibles:

$$V(xyzw, xy - zw) = V(x, z) \cup V(x, w) \cup V(y, z) \cup V(y, w).$$

But such a decomposition is unique! Hence these are the only closed codimension one subvarieties of $X$ which are in this closed set. The second and the third are respectively $l_x$ and $C$. Thus it remains to prove that there exists an open set $U \subset X$ so that $f$ is non-zero (and defined) on $U$ and with $U \cap V(x, z) \neq \emptyset$ (and the same for $V(y, w)$).

Define $U = D(y, w) \cap X$. Then $U \cap V(x, z) \neq \emptyset$, and on $U$, we can write $f$ as

$$f = \frac{yz}{xw} \ast \frac{y(\frac{zw}{xw})}{xw} = \frac{xy^2}{xw} = \frac{y^2}{w} \neq 0,$$

where in (asterisk), we use that in $K(X)$, the two functions $z$ and $xy/w$ are identified. Thus $f$ is non-zero on $U \cap V(x, z)$ and hence $v_{V(x,z)}(f) = 0$.

A similar argument with $U = D(x, z) \cap X$ works for $V(y, w)$, and so $v_{V(y,w)} = 0$.

Therefore, $\text{div } f = C - l_x$ and thus $l_x \equiv C$ since

$$l_x = C + \text{div } f.$$

We can now prove our proposition.

Proof of Proposition 3.2.11. We have already proven surjectivity of the map. We show injectivity.

Suppose that $al_x + bl_y \in \mathbb{Z}l_x \oplus \mathbb{Z}l_y$ is mapped to zero in $\text{Pic}(\bar{E})$. This implies that the divisor $al_x + bl_y \equiv 0$, and hence that

$$al_x \equiv -bl_y.$$

Using Lemma 3.2.12 and the linearity of intersection numbers (Theorem 3.2.7), we get the following relations:

$$0 = a(l_x \cdot l_x) = (-bl_y) \cdot l_y = -b, \quad 0 = -b(l_y \cdot l_y) = (al_x) \cdot l_y = a,$$

which imply that $a, b = 0$. Thus the kernel of the map $\mathbb{Z}l_x \oplus \mathbb{Z}l_y \rightarrow \text{Pic}(\bar{E})$ is trivial, and this is an isomorphism.
But both varieties $l_x$ and $l_y$ are defined over $\mathbb{F}_q$ (and even over any base field), so they are fixed by the Frobenius automorphism. Thus $\varphi$ induces the identity on $\text{Pic}(\overline{E})$, and therefore its trace is

$$\text{Tr}(\varphi) = \text{Tr} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 2.$$ 

Hence we conclude that the number of $\mathbb{F}_q$-rational points of the variety is

$$\#E(\mathbb{F}_q) = q^2 + 2q + 1 = (q + 1)^2.$$ 

Now for the case of hyperbolic quadrics, it seems more complicated. However, there is a very nice argument which simplifies the computations drastically. Consider a hyperbolic quadric $H = V(f(x, y) - zw) \subset \mathbb{P}^3(\mathbb{F}_q)$, with $f$ homogeneous of degree two. This implies that $f(x, 1)$ splits in the extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$, so we can write $f(x, 1) = (x - \alpha)(x - \alpha')$ for some $\alpha, \alpha' \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. But the Frobenius automorphism $\varphi$ permutes the roots of $f(x, 1)$; since it clearly does not fix $\alpha$, we must have

$$\alpha' = \varphi(\alpha) = \alpha^q.$$ 

Homogenizing, we see that $f(x, y) = (x - \alpha y)(x - \alpha^q y)$ in $\mathbb{F}_{q^2}[x, y]$. Now the key observation is that $H$ is nothing but a twist of $E$, in the sense that, while they are not isomorphic over $\mathbb{F}_q$, they become isomorphic when seen over $\mathbb{F}_{q^2}$. The isomorphism is given by

$$H \rightarrow E \quad \text{where} \quad A = \begin{pmatrix} 1 & \alpha & 0 & 0 \\ 1 & \alpha^q & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$ 

The idea of this isomorphism comes from [CD13].

Write $\overline{H}$ for $H$ seen as a variety over $\mathbb{F}_{q^2}$. This isomorphism implies that $\overline{H}$ is smooth, birational to $\mathbb{P}^2$, and that

$$\text{Pic}(\overline{H}) \cong \text{Pic}(\overline{E}),$$

the generators of $\text{Pic}(\overline{H})$ being given by the image under the isomorphism of the ones of $\text{Pic}(\overline{E})$.

Explicitly, the inverse of $A$ is

$$A^{-1} = B^{-1} \begin{pmatrix} \alpha^q & -\alpha & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}.$$
where $\beta = (\alpha^q - \alpha)$, and so the isomorphism in the Picard group is

$$\text{Pic}(\mathcal{E}) \longrightarrow \text{Pic}(\mathcal{H})$$

$$l_x \mapsto A^{-1}l_x = \{(\beta^{-1}\alpha b, \beta^{-1}b, c, 0) \mid a, b, c, d \in \mathbb{F}_q\} = V(w, \alpha x + y)$$

$$l_x \mapsto A^{-1}l_x = \{(\beta^{-1}\alpha^q a, -\beta^{-1}a, c, 0) \mid a, b, c, d \in \mathbb{F}_q\} = V(w, \alpha^q x + y),$$

and $\{A^{-1}l_x, A^{-1}l_y\}$ is a basis for $\text{Pic}(\mathcal{H})$. Now it is clear that the Frobenius map sends $V(w, \alpha x + y)$ to $V(w, \alpha^q x + y)$, and vice versa, whence

$$\varphi(A^{-1}l_x) = A^{-1}l_y, \quad \varphi(A^{-1}l_y) = A^{-1}l_x.$$ 

Hence $\varphi$ acts on $\text{Pic}(\mathcal{H})$ as a permutation of the basis elements, i.e as the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus, its trace is zero and we get

$$#H(\mathbb{F}_q) = q^2 + 1.$$
Chapter 4

Invariants and weight enumerators of particular Reed-Muller codes

In this final chapter, we expose our results concerning the application of Invariant Theory to the determination of weight enumerators of Reed-Muller codes. We first give some simple examples of invariants that we found on particular Reed-Muller codes. We then expose some computations in the self-dual case and we prove a finiteness criterion on the stabilizer. We finally give some examples of weight enumerators with trivial stabilizer, and explain how this procedure can be used to get approximations on the stabilizer.

4.1 Invariants of Reed-Muller codes

We first give some general invariants of two simple cases of Reed-Muller Codes.

Proposition 4.1.1. Let \( \zeta \) be a \( 2^m \)'th root of unity, for \( m \geq 2 \), and let \( u := \frac{\zeta + 1}{2} \). Then

\[
T := \begin{pmatrix}
u & u - 1 \\
u - 1 & u
\end{pmatrix} \in \text{Stab}(W_{R_M(m-1,m)}).
\]

Proof. By Proposition 2.1.5, \( R_M(m - 1, m) \) is the dual of \( R_M(0, m) \). Hence (cf. Example 2.1.4.1), its weight enumerator is

\[
W_{R_M(m-1,m)}(X,Y) = \frac{1}{2} \left((X + Y)^{2m} + (X - Y)^{2m}\right).
\]
Now we get
\[
W_{\mathcal{R},\mathcal{M}_{(m-1,m)}}^T(X, Y) = W_{\mathcal{R},\mathcal{M}_{(m-1,m)}}(uX + (u-1)Y, (u-1)X + uY) \\
= \frac{1}{2} \left( ((2u-1)(X+Y))^{2m} + (X-Y)^{2m} \right) \\
= \frac{1}{2} \left( \zeta^{2m}(X+Y)^{2m} + (X-Y)^{2m} \right) \\
= W_{\mathcal{R},\mathcal{M}_{(m-1,m)}}(X, Y). \qedhere
\]

This immediately generalizes to the following.

**Proposition 4.1.2.** Let \( \zeta \) be a \( 2^{m-1} \)th root of unity, for \( m \geq 3 \), and let \( u := \frac{\zeta + 1}{2} \).

Then
\[
T := \begin{pmatrix} u & u-1 \\ u-1 & u \end{pmatrix} \in \text{Stab}(W_{\mathcal{R},\mathcal{M}_{(m-2,m)}}).
\]

**Proof.** By Example 2.1.4.2 the weight enumerator of \( \mathcal{R}.M(1,m) \) is:
\[
W_{\mathcal{R},\mathcal{M}_{(1,m)}}(X, Y) = X^{2m} + 2 \cdot (2^m - 1)X^{2m-1}Y^{2m-1} + Y^{2m}.
\]

Now since \( \mathcal{R}.M(m-2,m) = \mathcal{R}.M(1,m) \), an application of MacWilliams’ Theorem gives
\[
W_{\mathcal{R},\mathcal{M}_{(m-2,m)}}(X, Y) = \\
= \frac{1}{2m+1} \left( (X-Y)^{2m} + 2 \cdot (2^m - 1)(X-Y)^{2m-1}(X+Y)^{2m-1} + (X+Y)^{2m} \right) \\
= \frac{1}{2m} W_{\mathcal{R},\mathcal{M}_{(m-1,m)}}(X, Y) + \frac{1}{2m+1} (2^{m+1} - 2)(X^2 - Y^2)^{2m-1}.
\]

Consider the polynomial \( A := X^2 - Y^2 \). We have
\[
A^T(X,Y) = (uX + (u-1)Y)^2 - ((u-1)X + uY)^2 \\
= u^2X^2 + 2u(u-1)XY + (u-1)^2Y^2 - (u-1)^2X^2 \\
- 2u(u-1)XY - u^2Y^2 \\
= u^2X^2 + (u^2 - 2u + 1)Y^2 - (u^2 - 2u + 1)X^2 - u^2Y^2 \\
= (1 - 2u)(Y^2 - X^2) \\
= -\zeta A(X,Y).
\]
Thus, applying $T$ to $W_{RM(m-2,m)}$ gives
\[
W_{RM(m-2,m)}^T(X, Y) = \frac{1}{2^m} W_{RM(m-1,m)}^T(X, Y) + \frac{1}{2^{m+1}} (2^{m+1} - 2)(A^T(X, Y))^{2^{m-1}}
\]
\[
= \frac{1}{2^m} W_{RM(m-1,m)}(X, Y) + \frac{1}{2^{m+1}} (2^{m+1} - 2)\zeta^{2^{m-1}}(X^2 - Y^2)^{2^{m-1}}
\]
\[
= W_{RM(m-2,m)}(X, Y),
\]
as desired.

\section*{4.2 Computation in the self-dual case}

In the particular case of self-dual codes, MacWilliams' Theorem (Theorem 1.1.11) gives us a very nice invariant of the weight enumerator. For Reed-Muller codes, we can use Proposition 2.1.5 to get conditions for the code to be self-dual. We put them in a proposition.

\begin{proposition}
A Reed-Muller code $RM_{F_q}(r, m)$ is self-dual if and only if $q = 2^t$ is a power of 2, $m$ is odd and $r = \frac{m(q-1)-1}{2}$.
\end{proposition}

\begin{proof}
Let $C = RM_{F_q}(r, m)$ be a Reed-Muller code, assuming $r < m(q-1)$. Then its dual is simply (see Proposition 2.1.5)
\[
C^\perp = RM_{F_q}(m(q-1) - r - 1, m).
\]
Thus $C$ is self-dual if and only if
\[
r = m(q-1) - r - 1 \iff 2r = m(q-1) - 1.
\]
The left-hand side is even, so $m(q-1)$ must be odd. This happens if and only if both $m$ and $(q-1)$ are odd. But $q$ is a power of a prime $p$, and so $q$ must be a power of 2. Therefore, we have $C$ is self-dual if and only if
\[
q = 2^t, \quad m \text{ is odd and } r = \frac{m(q-1)-1}{2}.
\]
We consider the special case $q = 2$. In that case, the only self-dual Reed-Muller codes are the codes of the form
\[
RM_{F_2}(r, 2r + 1), \quad r \in \mathbb{N}.
\]
Using our divisibility criterion for Reed-Muller codes (Theorem 3.1.3), we see that such codes are divisible by

\[ 2^{\frac{(2r+1)-1}{2}} = 2^2 = 4, \]

in other words, all such codes are doubly-even.

Therefore, we can apply Gleason’s Theorem to find that for any degree \( r \in \mathbb{N} \), the weight enumerator of \( R.M_{\mathbb{F}_2}(r, 2r+1) \) is in \( \mathbb{C}[f_8, f_{24}'] \), where \( f_8 \) and \( f_{24}' \) come from Theorem 1.2.11.

Using these considerations, we are able to compute some weight enumerators. We briefly explain how.

Observe that if some \( f \in \mathbb{C}[f_8, f_{24}'] \) has degree \( n \) (Corollary 1.2.12 implies that \( n \) is divisible by 8), then \( f \) is a linear combination of

\[ \{(f_8)^a \cdot (f_{24}')^b \mid 8a + 24b = n\} = \{(f_8)^{j-3l} \cdot (f_{24}')^l \mid 0 \leq l \leq \lfloor j/3 \rfloor\}, \]

where \( j = n/8 \). Now since \( f_{24}' \) has no term \( X^{24} \), we see that the highest power of \( X \) in \( (f_8)^{j-3l} \cdot (f_{24}')^l \) is \( X^{8(j-3l)+20l} = X^{8j-4l} \). Thus, if we write

\[ f = \sum_{l=0}^{\lfloor j/3 \rfloor} a_l f_8^{j-3l} \cdot f_{24}'^l, \]

then equating the coefficient in front of \( X^{8j-4l} \) gives a linear equation in which the only unknowns are \( \{a_1, \ldots, a_l\} \). Therefore, if we know some of the first coefficients of \( f \) (i.e. some low weights of the considered code), we can compute the values \( a_l \) one after the other, provided we have enough coefficients.

Kasami et. al. were able to compute the weights of Reed-Muller codes over \( \mathbb{F}_2 \) which are strictly less than \( 2.5d \), where \( d \) is the minimum distance of the codes. Their results can be found in [MS77, Chap. 15, §3, Theorem 11] for the weights up to \( 2d \), and [KTA76] for the weights strictly less than \( 2.5d \).

Using this technique, we are able to compute the following distribution.

**Proposition 4.2.2.** The weight distribution of \( R.M_{\mathbb{F}_2}(3, 7) \) is given in Table 4.1.

Moreover, again using this argument, we are almost able to compute the weights of the code \( R.M_{\mathbb{F}_2}(4, 9) \), in the sense that two degree of freedom remain. This is because to apply our technique the weights 80 and 84 are necessary to fully determine the weight enumerator. But the minimum distance of this code is \( d = 32 \), so \( 2.5d = 80 \) and we cannot use Kasami’s results.
<table>
<thead>
<tr>
<th>Weight</th>
<th>Number of codewords</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 128</td>
<td>1</td>
</tr>
<tr>
<td>16 112</td>
<td>94488</td>
</tr>
<tr>
<td>24 104</td>
<td>74078592</td>
</tr>
<tr>
<td>28 100</td>
<td>312843688</td>
</tr>
<tr>
<td>32 96</td>
<td>312335197020</td>
</tr>
<tr>
<td>36 92</td>
<td>18125860315136</td>
</tr>
<tr>
<td>40 88</td>
<td>552366841342848</td>
</tr>
<tr>
<td>44 84</td>
<td>9491208609103872</td>
</tr>
<tr>
<td>48 80</td>
<td>94117043084875944</td>
</tr>
<tr>
<td>52 76</td>
<td>549823502398291968</td>
</tr>
<tr>
<td>56 72</td>
<td>192060477925721574</td>
</tr>
<tr>
<td>60 68</td>
<td>405196690678938096</td>
</tr>
<tr>
<td>64 51</td>
<td>5193595576952890822</td>
</tr>
</tbody>
</table>

Table 4.1: Weight Distribution for $\mathcal{R}_M_{\mathbb{F}_2}(3, 7)$

### 4.3 The action of $PGL_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$

Our key ingredient to analyze stabilizers of homogeneous polynomials is the action of $PGL_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$. We briefly recall its construction. As previously, $n$-tuples are seen as column vectors, so that multiplication by matrices on the left is well defined.

It is clear that $GL_2(\mathbb{C})$ acts on $\mathbb{A}^2(\mathbb{C}) = \mathbb{C}^2$ by matrix multiplication. Moreover, for any $\lambda \in \mathbb{C}$, $(x, y) \in \mathbb{A}^2(\mathbb{C})$ and $g \in GL_2(\mathbb{C})$,

$$g(\lambda x, \lambda y) = \lambda g(x, y),$$

so $GL_2(\mathbb{C})$ also acts on $\mathbb{P}^1(\mathbb{C})$. If we identify $\mathbb{C}$ with the subgroup $\{\lambda I \mid \lambda \in \mathbb{C}\}$ of $GL_2(\mathbb{C})$ (where $I$ is the identity matrix in $GL_2(\mathbb{C})$), this action factors by $\mathbb{C}$, so we actually have an action of

$$PGL_2(\mathbb{C}) := GL_2(\mathbb{C})/\mathbb{C}$$

on $\mathbb{P}^1(\mathbb{C})$.

A very useful property of this action is the following.

**Proposition 4.3.1.** The action of $PGL_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$ is sharply 3-transitive. In other words, for any 3 distinct points $a_0, b_0, c_0$, and 3 distinct points $a, b, c$ (not necessarily
different from \(a_0, b_0, c_0\) there is a unique \(\bar{g} \in \text{PGL}_2(\mathbb{C})\) which maps \(a_0\) to \(a\), \(b_0\) to \(b\) and \(c_0\) to \(c\).

**Proof.** It is clearly enough to show it for \(a_0 = (1 : 0), b_0 = (0 : 1), c_0 = (1 : 1)\). Suppose \(a = (a_1 : a_2), b = (b_1 : b_2), c = (c_1 : c_2)\). Let \(g \in \text{GL}_2(\mathbb{C})\) be such that the image of \(g\) in \(\text{PGL}_2(\mathbb{C})\) sends \(a_0, b_0, c_0\) to \(a, b, c\). Then \(g(1, 0) = \lambda(a_1, a_2)\) and \(g(0, 1) = \mu(b_1, b_2)\), for some \(\lambda, \mu \in \mathbb{C}^\times\), so \(g\) is of the form

\[
g = \begin{pmatrix}
\lambda a_1 & \mu b_1 \\
\lambda a_2 & \mu b_2
\end{pmatrix}.
\]

Now since \(g(1, 1) = \eta(c_1, c_2)\) for \(\eta \in \mathbb{C}^\times\),

\[
\begin{pmatrix}
\eta c_1 \\
\eta c_2
\end{pmatrix} = g \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix}
\lambda a_1 + \mu b_1 \\
\lambda a_2 + \mu b_2
\end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \end{pmatrix}.
\]

But since \(a' \neq b'\), we have

\[
\begin{vmatrix}
a_1 & b_1 \\
a_2 & b_2
\end{vmatrix} = a_1 b_2 - a_2 b_1 \neq 0.
\]

Thus this matrix is invertible, and we get

\[
\begin{pmatrix}
\lambda \\
\mu
\end{pmatrix} = \eta \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}^{-1} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}.
\]

In other words,

\[
g = \eta \begin{pmatrix}
\lambda' a_1 & \mu' b_1 \\
\lambda' a_2 & \mu' b_2
\end{pmatrix}, \quad \text{where} \quad \begin{pmatrix}
\lambda' \\
\mu'
\end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}^{-1} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}.
\]

Now it is easy to check that any \(g\) of this form indeed permutes the points in the expected way. All matrices of this form have the same image in \(\text{PGL}_2(\mathbb{C})\), whence \(\bar{g} \in \text{PGL}_2(\mathbb{C})\) is uniquely determined by the choice of \(a, b, c\). \(\square\)

### 4.3.1 Cross-Ratios

We introduce the main tool for Section 4.5 where we explicit a polynomial with a trivial stabilizer.
**Definition 4.3.2.** Let \( x_1 = (\lambda_1 : \mu_1), \ldots, x_4 = (\lambda_4 : \mu_4) \) be four distinct points in \( \mathbb{P}^1(\mathbb{C}) \). The **cross-ratio** between the points \( x_1, x_2, x_3, x_4 \) is the ratio

\[
[x_1, x_2, x_3, x_4] = \frac{(\lambda_1 \mu_3 - \lambda_3 \mu_1)(\lambda_2 \mu_4 - \lambda_4 \mu_2)}{(\lambda_1 \mu_4 - \lambda_4 \mu_1)(\lambda_2 \mu_3 - \lambda_3 \mu_2)}.
\]

If \( z_1, \ldots, z_4 \) are four distinct complex numbers, their cross ratio is simply the cross-ratio of their homogenizations \((z_1 : 1), \ldots, (z_4 : 1)\) in \( \mathbb{P}^1(\mathbb{C}) \). In other words

\[
[z_1, z_2, z_3, z_4] = \frac{(z_1 - z_3)(z_2 - z_4)}{(z_1 - z_4)(z_2 - z_3)}.
\]

This definition is easily seen to be independent of the homogeneous coordinates chosen. The reason why we study these cross-ratios is the following.

**Proposition 4.3.3.** The action of \( PGL_2(\mathbb{C}) \) on \( \mathbb{P}^1(\mathbb{C}) \) preserves the cross-ratio of any four points. Explicitly, if \( \tilde{g} \in PGL_2(\mathbb{C}) \) and \( x_1, x_2, x_3, x_4 \) are four distinct points in \( \mathbb{P}^1(\mathbb{C}) \), then

\[
\tilde{g}x_1, \tilde{g}x_2, \tilde{g}x_3, \tilde{g}x_4 = [x_1, x_2, x_3, x_4].
\]

**Proof.** Let \( g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C}) \) represent \( \tilde{g} \). Write \( x_1 = (\lambda_1 : \mu_1), \ldots, x_4 = (\lambda_4 : \mu_4) \) and define \( \lambda'_i = a\lambda_i + b\mu_i \) and \( \mu'_i = c\lambda_i + d\mu_i \) so that

\[
\tilde{g}x_i = (a\lambda_i + b\mu_i : c\lambda_i + d\mu_i) = (\lambda'_i : \mu'_i).
\]

We compute the cross ratio \([\tilde{g}x_1, \tilde{g}x_2, \tilde{g}x_3, \tilde{g}x_4]\). Algebraic manipulations give

\[
(\lambda'_i \mu'_j - \lambda'_j \mu'_i) = (ad - bc)(\lambda_i \mu_j - \lambda_j \mu_i)
\]

for \( i \neq j \) (observe that \( ad - bc \neq 0 \) since the matrix \( g \) is invertible). We get

\[
[\tilde{g}x_1, \tilde{g}x_2, \tilde{g}x_3, \tilde{g}x_4] = \frac{(\lambda'_i \mu'_3 - \lambda'_3 \mu'_i)(\lambda'_j \mu'_4 - \lambda'_4 \mu'_j)}{(\lambda'_i \mu'_4 - \lambda'_4 \mu'_i)(\lambda'_j \mu'_3 - \lambda'_3 \mu'_j)} = \frac{(ad - bc)^2}{(ad - bc)^2}[x_1, x_2, x_3, x_4]
\]

as desired. \( \Box \)

**Remark 4.3.1.1.** We finish this subsection by an observation. Consider four distinct points \( x_1 = (\lambda_1 : \mu_1), \ldots, x_4 = (\lambda_4 : \mu_4) \), and let \( \sigma \in S_4 \) be a permutation. If \( \sigma = \text{id} \), it is clear that

\[
[x_1, x_2, x_3, x_4] = [x_1, x_2, x_3, x_4]
\]

for any permutation \( \sigma \).
A natural question to ask is: for which $\sigma \in S_4$ does this hold? An easy computation shows that, for arbitrarily chosen points $x_1, x_2, x_3, x_4$, there are always at least four permutations which fix the cross-ratio: These form the Klein four-group

$$V = \{\text{id}, (12)(34), (13)(24), (14)(23)\}.$$ 

We will say that these are the **Klein-four permutations** of $(x_1, x_2, x_3, x_4)$. As we will show in Section 4.5, there are choices of points for which these are the only permutations which fix the cross-ratio.

### 4.4 Finiteness of Stabilizers

Now that we defined the important action of $PGL_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$, we use it to show a finiteness result on stabilizers. This is essential if we want to apply the technique of computing the Molien series. Indeed, this series is only defined when the considered group is finite (see Theorem 1.2.9).

If $f \in \mathbb{C}[X,Y]$, we let

$$\text{Stab}(f) := \{g \in GL_2(\mathbb{C}) \mid f^g = f\}$$

de note the stabilizer of $f$ in $GL_2(\mathbb{C})$.

**Proposition 4.4.1.** Let $f = \sum_{i=0}^{d} a_i X^{d-i} Y^i \in \mathbb{C}[X,Y]$ be a homogeneous degree $d$ polynomial. Suppose that $a_0 \neq 0$ and that $f(X,1)$ has at least 3 distinct roots. Then $\text{Stab}(f)$ is finite.

**Proof.** Let $V := V_{\mathbb{P}^1(\mathbb{C})}(f)$ denote the complex projective variety defined by $f$. Observe that if $(x : y) \in V$, then $y \neq 0$ since otherwise we would have

$$0 = f(x, y) = f(x, 0) = a_0 x^d$$

implying that $x = 0 = y$, which is impossible. Thus

$$V = \{(x : 1) \mid x \text{ root of } f(X,1)\}$$

and consequently, $V$ has at least 3 points.

Consider the action of $PGL_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$ defined in Section 4.3. By Proposition 4.3.1 we know that this group acts **sharply 3-transitively** on $\mathbb{P}^1(\mathbb{C})$, i.e. that given 3 distinct
We want to show that \( \rho \) is finite. Since \( S_n \) is a finite group and \( G = \pi^{-1}(\rho^{-1}(S_n)) \), it is enough to show that the fibers of the maps \( \pi \) and \( \rho \) are finite.

Let \( \sigma \in S_n \) be a permutation of \( V \). Then, \( \sigma \) sends \( v_1, v_2 \) and \( v_3 \) to three fixed distinct points (since it is injective). Thus, there is exactly one element \( \bar{g} \in PGL_2(\mathbb{C}) \) which sends \( v_1 \) to \( \sigma(v_1) \), \( v_2 \) to \( \sigma(v_2) \) and \( v_3 \) to \( \sigma(v_3) \). Note that we do not necessarily have \( \rho(\bar{g}) = \sigma \) since, for example, \( \bar{g} \) could send \( v_4 \) to a point different from \( \sigma(v_4) \). However, if \( \rho(\bar{g}) = \sigma \), then \( \bar{g} \) is unique with this property. We have shown that for any permutation \( \sigma \), there is at most one \( \bar{g} \in PGL_2(\mathbb{C}) \) which induces it, i.e. one pre-image in \( \rho^{-1}(\sigma) \). Thus \( \rho \) has finite fibers.

Now if \( \bar{g} \in \bar{G} \), and if \( g \) is a fixed pre-image of \( \bar{g} \) under the map \( GL_2(\mathbb{C}) \rightarrow PGL_2(\mathbb{C}) \), then for any \( \lambda \in \mathbb{C}^\times \), \( \lambda g \) is also a pre-image of \( \bar{g} \). So in principle, \( \bar{g} \) has infinitely many pre-images in \( GL_2(\mathbb{C}) \).

But we are considering only pre-images \( g \in G \), i.e. those which fix \( f \). If there are no \( g \in G \) with \( \pi(g) = \bar{g} \), then we are done: the fiber of \( \bar{g} \) under \( \pi \) is empty whence finite. Suppose that \( g \in G \) fixes \( f \), and that \( \pi(g) = \bar{g} \).

If \( \lambda g \) (for \( \lambda \in \mathbb{C} \)) also fixes \( f \), the \( X^d \) coefficient of \( f(\lambda g) \) and that of \( f \) must be equal. Observing that

\[
\begin{align*}
 f((\lambda g))(X, Y) &= f^g(\lambda X, \lambda Y) = \lambda^d f^g(X, Y) = \lambda^d f(X, Y),
\end{align*}
\]
we see that $\lambda$ must satisfy the equation

$$\lambda^d a_0 = a_0 \iff \lambda^d = 1.$$ 

Hence, if $\lambda g$ fixes $f$, then $\lambda$ is a $d$’th root of unity. But there are only finitely many $d$’th roots of unity, and hence finitely many $\lambda$ which fulfill this condition. Since any pre-image under $\pi$ of $\bar{g}$ is of the form $\lambda g$, we see that there are only finitely many $g \in G$ having $\pi(g) = \bar{g}$, i.e. the fibers of $\pi$ in $G$ are finite. \hfill \Box

**Corollary 4.4.2.** The stabilizer of any weight enumerator $W(X, Y)$ is finite, provided $W(X, 1)$ has at least 3 complex roots.

**Remark 4.4.0.2.** This condition of at least two roots is clearly necessary. Indeed, if $f(X, 1)$ has only one root, then $f(X, Y) = \lambda(X + \alpha Y)^n$ and $f$ is invariant under the transformation

$$\begin{pmatrix} 1 & \eta \\ 0 & 1 - \alpha^{-1}\eta \end{pmatrix},$$

and this for any $\eta \in \mathbb{C}$. Thus the stabilizer of $f$ is infinite. If $f(X, 1)$ has two distinct roots, then $f(X, Y) = \lambda(X + \alpha Y)^{e_1}(X + \beta Y)^{e_2}$. Computations show that the matrix

$$\frac{1}{\alpha - \beta} \begin{pmatrix} \alpha \gamma - \beta \eta & \alpha \beta \gamma - \alpha \beta \eta \\ -\gamma + \eta & -\beta \gamma + \alpha \eta \end{pmatrix}$$

sends $f$ to $\lambda \eta^{e_1}(X + \alpha Y)^{e_1} \cdot \gamma^{e_2}(X + \beta Y)^{e_2}$. Hence, for any choice of $\eta, \gamma \in \mathbb{C}$ such that $\eta^{e_1} \gamma^{e_2} = 1$,

this matrix fixes the polynomial $f$. In particular, there are infinitely many choices.

In terms of weight enumerators, the intuition behind this proposition is that almost all weight enumerators have finite stabilizer, in the sense that the only ones with infinite stabilizer are the ones with 2 roots or less.

This can happen in some cases: for example, the full code $\mathbb{F}_q^n$ has weight enumerator $W(X, Y) = (X + (q - 1)Y)^n$, and so $W(X, 1)$ has only one root.

It is not known in general if a given polynomial can be realized as the weight enumerator of some linear code. A classical example is the existence of a self-dual [72, 36, 16]_2 code: although we are able to completely determine the weight enumerator of a self-dual doubly-even binary code with these parameters (see at the end of Section 1.2.3 for references), it is a longstanding open question to know if such a code exists or not.
We will conclude this section by stating a few necessary conditions for a polynomial to be realizable as the weight enumerator of a code.

**Definition 4.4.3.** Let \( q \) be a prime power. A polynomial \( f = \sum_{i=0}^{n} a_i X^{n-i} Y^i \) is called **weakly admissible** if

1. \( a_0 = 1 \).
2. \( \sum_{i=1}^{n} a_i = q^k - 1 \) for some \( k \geq 1 \).
3. All the \( a_i \) are non-negative integers.
4. For \( 1 \leq i \leq n \), \( a_i \) is divisible by \( q - 1 \).

It is called **admissible** if the dual polynomial \( f^\perp(X, Y) := q^{-k} f(X + (q - 1)Y, X - Y) \) is also weakly admissible (\( k \) is the integer of part 2 of the definition of weakly admissible for \( C \)).

It is clear that a polynomial can be realized as a weight enumerator only if it is admissible. However, as said before, it is in general an unsolved problem to know if some polynomial can be realized as such or not. See [Ken94] for more details and results.

### 4.5 A weight enumerator with trivial stabilizer

In this section we exhibit a Reed-Muller code whose weight enumerator has trivial stabilizer.

Let \( F \) be the weight enumerator of \( \mathcal{R}_2 \mathcal{M}_{2} (2, 2) \). A calculation shows that

\[
F(X, Y) = \begin{align*}
1 \quad &X^{16} \\
+ 90 \quad &X^{8} Y^{8} \\
+ 480 \quad &X^{7} Y^{9} \\
+ 864 \quad &X^{5} Y^{11} \\
+ 840 \quad &X^{4} Y^{12} \\
+ 1440 \quad &X^{3} Y^{13} \\
+ 288 \quad &X Y^{15} \\
+ 93 \quad &Y^{16} .
\end{align*}
\]
Let $f = F(X, 1)$. Eisenstein’s criterion with prime $p = 3$ shows that this polynomial is irreducible over $\mathbb{Q}$. Therefore, all its roots are distinct and by Proposition 4.4.1, $\text{Stab}(F)$ is finite.

Because $F$ is a homogeneous polynomial of degree 16, it is invariant under the matrices

$$\zeta I = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta \end{pmatrix}$$

where $\zeta$ is a 16’th root of unity. Moreover, these are the only scalar matrices (matrices of the form $\lambda I$) which stabilize $F$. We claim that these are actually the only matrices of $GL_2(\mathbb{C})$ with this property:

**Proposition 4.5.1.** If $F$ denotes the weight enumerator of $\mathcal{R} M_{8,4}(2, 2)$, then

$$\text{Stab}(F) = \{ \zeta I \mid \zeta \in \mathbb{C}, \zeta^{16} = 1 \}.$$ 

This is equivalent to saying that all $g \in \text{Stab}(F)$ have trivial image in $PGL_2(\mathbb{C})$. Now since any $g \in \text{Stab}(F)$ induces $\bar{g}$ in $PGL_2(\mathbb{C})$ which permutes the points of the projective variety $V := V_{p_1(\mathbb{C})}(F)$, it is enough to show that no non-trivial element of $PGL_2(\mathbb{C})$ sends $V$ into itself. The following lemma will help us.

**Lemma 4.5.2.** There exist 5 distinct roots $z_1, \ldots, z_5$ of $f$ such that the only 4-tuples of distinct roots $(y_1, y_2, y_3, y_4)$ satisfying

$$[z_1, z_2, z_3, z_j] = [y_1, y_2, y_3, y_4]$$

are the Klein-four permutations of $(z_1, z_2, z_3, z_j)$, for $j \in \{4, 5\}$.

Assume the lemma for the moment, and let $g \in GL_2(\mathbb{C})$ be such that $F^g = F$. Then the image $\bar{g} \in PGL_2(\mathbb{C})$ of $g$ permutes the roots of $f$ in a way which preserves cross-ratios. Therefore, the lemma implies that it must send $(z_1, z_2, z_3, z_4)$ to a Klein-four permutation of $(z_1, z_2, z_3, z_4)$, and the same for $(z_1, z_2, z_3, z_5)$.

Suppose $\bar{g} z_4 = z_l$ with $l \in \{1, 2, 3, 4\}$. If $l \in \{1, 2, 3\}$, then since $\bar{g}$ sends $\{z_1, z_2, z_3, z_5\}$ into itself, one of those elements is also sent to $z_l$. But this is impossible since $\bar{g}$ is invertible, whence injective. Thus $\bar{g} z_4 = z_4$.

But the only Klein-four permutation of $(z_1, z_2, z_3, z_4)$ which sends $z_4$ to $z_4$ is the identity. Thus $\bar{g}$ fixes $z_1, z_2, z_3, z_4$. Since the action of $PGL_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$ is sharply transitive, we must have $\bar{g} = \text{id}$, as desired. This proves Proposition 4.5.1.
It remains to prove Lemma 4.5.2. If we had access to the exact values of the roots of $f$, the task would be easy: we could simply use a computer software to compute all cross-ratios $[y_1, y_2, y_3, y_4]$ to show that only the trivial ones are equal to $[z_1, z_2, z_3, z_j]$ ($j \in \{4, 5\}$). However, computations show that the Galois group of this polynomial is the symmetric group $S_{16}$. Thus $f$ is not solvable, and there are no closed formulas involving only algebraic operations (addition, multiplication and $n$'th root).

Hence we can only work on approximated values of the roots of $f$, and we need to keep track of our approximation errors to ensure that they are not too large to make our calculations false.

We need a general lemma about approximations.

**Lemma 4.5.3.** Let $a_1, a_2, a_3, a_4$ be complex numbers, and $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be complex numbers with module less than some fixed $\delta < 1$. Then

$$|(a_1 + \alpha_1)(a_2 + \alpha_2)(a_3 + \alpha_3)(a_4 + \alpha_4) - a_1a_2a_3a_4| \leq 15M^3\delta,$$

where $M = \max(|a_1|, |a_2|, |a_3|, |a_4|)$.

**Proof.** Expand the expression. The term $a_1a_2a_3a_4$ cancels out, so we are left with 15 terms, all of which contain at least one of the $\alpha_i$, and at most three $a_i$’s. Explicitly, all remaining terms are of the form

$$\prod a_i \cdot \prod \alpha_j$$

where the first product ranges over at most 3 indices $i$, and the second ranges over at least 1 index $j$. Since $\delta < 1$, all these terms are less than $M^3\delta$ in module, whence the conclusion.

This lemma has a very useful corollary.

**Corollary 4.5.4.** Let $x_1, \ldots, x_8$ be 8 complex numbers, and let $\tilde{x}_1, \ldots, \tilde{x}_8$ be approximations so that

$$\max_j |x_j - \tilde{x}_j| \leq \epsilon < 1/2$$

for a fixed $\epsilon$. Let $N$ be a number larger then $\max_j |x_j|$. Then:

1. $\max_{i,j} |(x_i - x_j) - (\tilde{x}_i - \tilde{x}_j)| \leq 2\epsilon$

2. $|(x_1 - x_3)(x_2 - x_4)(x_5 - x_8)(x_6 - x_7) - (\tilde{x}_1 - \tilde{x}_3)(\tilde{x}_2 - \tilde{x}_4)(\tilde{x}_5 - \tilde{x}_8)(\tilde{x}_6 - \tilde{x}_7)| \leq 60N^3\epsilon.$
3. Let \( a = (x_1 - x_3)(x_2 - x_4)(x_5 - x_8)(x_6 - x_7) \), \( b = (x_1 - x_4)(x_2 - x_3)(x_5 - x_7)(x_6 - x_8) \), and let \( \tilde{a}, \tilde{b} \) denote the same expressions where the \( x \)'s have been replaced by their approximations. If \(|\tilde{a} - \tilde{b}| \geq 120N^3\epsilon\), then \(|a - b| > 0\).

**Proof.** Part 1 is just the triangle inequality. Part 2 follows from the lemma applied to the various differences \((x_i - x_j)\) in place of the \(a\)'s and the approximations \((\tilde{x}_i - \tilde{x}_j)\) in place of the \(\alpha\)'s, and noting that the \(M\) from the lemma is less than twice the \(N\) from the corollary, and that the maximal module of the \(\alpha\)'s is less than \(2\epsilon\).

Finally, for Part 3 it suffices to observe that

\[
|\tilde{a} - \tilde{b}| \leq |\tilde{a} - a| + |a - b| + |b - \tilde{b}| \iff |\tilde{a} - \tilde{b}| - |a - b| - |b - \tilde{b}| \leq 60N^3\epsilon,
\]

Now the previous part applied to different permutations of \(x_1, \ldots, x_8\) certainly imply that

\[|\tilde{a} - a|, |b - \tilde{b}| \leq 60N^3\epsilon,\]

and the result follows. \(\square\)

We now prove the main lemma.

**Proof of Lemma 4.5.2.** We use the software Magma to get an approximation of the roots of \(f\). As described in their technical informations about the algorithm for finding roots (see [CBFS08, 25.4.10]) an optional precision argument can be given to the algorithm to ensure that the approximations are arbitrarily close to the original ones. The following table gives approximations up to \(10^{-10}\):

| \(\hat{z}_1\) | \(-0.25173341452\) | \(\hat{z}_2\) | \(-1.9972538511\) |
| \(\hat{z}_3\) | \(0.19413768033 + 0.46883334035i\) | \(\hat{z}_4\) | \(\overline{\hat{z}_3}\) |
| \(\hat{z}_5\) | \(0.81160811592 + 1.3370476389i\) | \(\hat{z}_6\) | \(\overline{\hat{z}_5}\) |
| \(\hat{z}_7\) | \(0.88714124700 + 1.6221174517i\) | \(\hat{z}_8\) | \(\overline{\hat{z}_7}\) |
| \(\hat{z}_9\) | \(2.0184761959 + 0.67929901507i\) | \(\hat{z}_{10}\) | \(\overline{\hat{z}_9}\) |
| \(\hat{z}_{11}\) | \(-0.48473639852 + 1.9179700645i\) | \(\hat{z}_{12}\) | \(\overline{\hat{z}_{11}}\) |
| \(\hat{z}_{13}\) | \(-1.5946294096 + 1.1560742429i\) | \(\hat{z}_{14}\) | \(\overline{\hat{z}_{13}}\) |
| \(\hat{z}_{15}\) | \(-0.70750379821 + 0.86423556346i\) | \(\hat{z}_{16}\) | \(\overline{\hat{z}_{15}}\) |
Let \( z_1, \ldots, z_{16} \) denote the roots of \( f \), listed so that \( z_j \) is approximated by \( \tilde{z}_j \) in the above table.

We claim that \( z_1, \ldots, z_5 \) satisfy the proposition of the lemma. We want to show that for any choice \( y_1, \ldots, y_4 \) of distinct roots of \( f \) which are not a Klein-four permutation of \( (z_1, z_2, z_3, z_j) \) (for \( j = 4 \) or \( 5 \)) we have

\[
[z_1, z_2, z_3, z_j] \neq [y_1, y_2, y_3, y_4].
\]

This is equivalent to showing that

\[
\frac{(z_1 - z_3)(z_2 - z_j)}{(z_1 - z_j)(z_2 - z_3)} \neq \frac{(y_1 - y_3)(y_2 - y_4)}{(y_1 - y_4)(y_2 - y_3)}
\]

which is again equivalent to

\[
|(z_1 - z_3)(z_2 - z_j)(y_1 - y_4)(y_2 - y_3) - (z_1 - z_j)(z_2 - z_3)(y_1 - y_3)(y_2 - y_4)| > 0 \quad (4.1)
\]

for any non-trivial choice of points.

By looking at our approximations, we see that if we set \( N = 3 \), and \( \epsilon = 10^{-6} \), then we certainly have

\[
N \geq \max_j |z_j| \quad \text{and} \quad \max_j |z_j - \tilde{z}_j| \leq \epsilon < 1/2.
\]

Therefore, Corollary 4.5.4 applied to

\[
x_1 = z_1, \ x_2 = z_2, \ x_3 = z_3, \ x_4 = z_j, \ x_5 = y_1, \ x_6 = y_2, \ x_7 = y_3, \ x_8 = y_4
\]

tells us that, for (4.1) to be satisfied, it is enough to check that

\[
|(\tilde{z}_1 - \tilde{z}_3)(\tilde{z}_2 - \tilde{z}_j)(\tilde{y}_1 - \tilde{y}_4)(\tilde{y}_2 - \tilde{y}_3) - (\tilde{z}_1 - \tilde{z}_j)(\tilde{z}_2 - \tilde{z}_3)(\tilde{y}_1 - \tilde{y}_3)(\tilde{y}_2 - \tilde{y}_4)| > 120 \cdot 9^3 \cdot 10^{-6},
\]

where \( \tilde{y}_j \) denotes the corresponding approximation of \( y_j \). But this can now easily be checked for all possible choices of \( y_1, \ldots, y_4 \), since we took our original approximations small enough. Hence the lemma is proved.

Using the same idea, we were able to prove that other Reed-Muller codes have trivial stabilizer. In the end, we get:

**Proposition 4.5.5.** The following affine and projective Reed-Muller codes have trivial stabilizer.

\[
\begin{align*}
\mathcal{RM}_{F_4}(2, 2), & \quad \mathcal{RM}_{F_4}(3, 2), \quad \mathcal{RM}_{F_4}(2, 2), \\
\mathcal{PRM}_{F_5}(3, 2), & \quad \mathcal{PRM}_{F_5}(3, 2)^\perp = \mathcal{PRM}_{F_5}(5, 2).
\end{align*}
\]
4.5.1 An algorithm to find the stabilizer

This procedure actually gives an algorithm to approximate the stabilizer of a homogeneous polynomial $F \in \mathbb{C}[X, Y]$ with non-zero $X^{\deg(F)}$ coefficient and such that $F(X, 1)$ has at least three complex roots. Its description is the following.

1. Find approximations for all the zeroes of $F(X, 1)$. These zeroes correspond to the projective zeroes of $F$.

2. Compute all the possible cross ratios between those points. This is quite a fast procedure, since there are about $n^4$ simple operations to be made, where $n$ is the degree of $F$.

3. Find the cross ratios which are close to each other (in the sense described in Corollary 4.5.4), and compute the (unique) element of $PGL_2(\mathbb{C})$ which permutes the roots in the appropriate way.

4. Apply this transformation to the weight enumerator, and see if it remains almost invariant (by again using an upper bound on the error term, as in Corollary 4.5.4). This gives an approximation of the invariants of this polynomial.

In conclusion, our methods showed that there is no general invariant which works for all Reed-Muller codes. This does not imply that this theory cannot be used to determine weight enumerators, but suggests that the very geometric definition of these codes is not enough to ensure the presence of invariants of the weight enumerator. However, observe that this method can be applied to other types of codes, either to find invariants, or to show that none exist.
Bibliography


