Weight Enumerator of binary self-dual codes

Panwei Hu

Contents

This report is largely based on the book [1] from chapter 2.7 to 2.9 and will deal with the *hamming weight enumerator* of a binary code. We will first draw a conclusion about the specific case when the code is of length 24 and self-dual doubly even. We will also consider the relationship between the *theta function* of the corresponding lattice and the *hamming weight enumerator* of the code. Next we will give a specific example of the binary self-dual doubly even code of length 24 and a lattice with certain property. In the end, we will prove the famous *MacWilliams Identity Theorem* and *Gleason's Theorem* using what we have learnt about *modular form*.

1 Introduction

We have dealt mainly with lattices in the previous two lectures. Now we will discuss the relationship between lattices and codes. So the first step is to construct a bridge between these two. Throughout the report, we will only discuss the binary case.
Before discussing further the codes, let us recall some results from the *theta function* and *modular form*, which we simply state without proof.
Let $\Gamma \subset \mathbb{R}^n$ be a lattice. We define $q = e^{2\pi i \tau}$, for $\tau \in \mathbb{H}$.
The theta function ϑ_Γ of the lattice Γ is defined as

$$\vartheta_\Gamma(\tau) := \sum_{x\in\Gamma} q^{\frac{1}{2}(x\cdot x)}$$

We recall the main theorem on even unimodular lattice

Theorem 1.1. Let Γ be an even unimodular lattice in $\mathbb{R}^n$. Then

1. n $\equiv$ 0 (mod 8)

2. ϑ_Γ is a modular form of weight $\frac{n}{2}$

Proposition 1.2. Let $\Gamma \subset \mathbb{R}^n$ be a lattice, then $\vartheta_\Gamma(-\frac{1}{\tau}) = (\frac{\tau}{i})^{\frac{n}{2}} \frac{1}{\mathrm{vol}(\mathbb{R}^n/\Gamma)} \vartheta_{\Gamma^*}(\tau)$

Definition 1.3. Let $k \in \mathbb{Z}$, k even, $k > 2$. The series

$$G_k(\tau) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(m\tau+n)^k}$$

is called the *Eisenstein series of index k*. The *normalized Eisenstein series* is defined as

$$E_k(\tau) := \frac{1}{2\zeta(k)} G_k(\tau)$$

where $\zeta(k)$ is the *Riemann ζ-function*

We define

$$\Delta := \frac{1}{1728}(E_4^3 - E_6^2)$$

The Δ function has the following form:

Proposition 1.4.

$$\Delta = q \prod_{r=1}^{\infty} (1-q^r)^{24}$$

Definition 1.5. The set of modular forms of weight k is a $\mathbb{C}$-vector space, and is denoted as M_k. M_k^0 denotes the $\mathbb{C}$-vector space of cusp forms of weight k.

Theorem 1.6.

1. $M_k = 0$ for k odd, for $k < 0$ and for k = 2
2. $M_0 = \mathbb{C}$, $M_0^0 = 0$ and for k = 4, 6, 8, 10, $M_k^0 = 0$, $M_k = \mathbb{C} \cdot E_k$
3. Multiplication by $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$ defines an isomorphism of M_{k-12} onto M_k^0

Corollary 1.7. The algebra M of mdular forms is isomorphic to the polynomial algebra $\mathbb{C}[E_4, E_6]$.

Proposition 1.8. Let Γ be an even unimodular lattice in $\mathbb{R}^8$. Then Γ is isomorphic to E_8. And the theta function

$$\vartheta_\Gamma = E_4$$

We consider first the standard $\mathbb{Z}^n$ lattices and define the canonical projection onto $\mathbb{F}_2^n$

$$\rho : \mathbb{Z}^n \to \mathbb{F}_2^n, x \mapsto \bar{x}$$

For a binary (n,k,d)*-code* C. Since $|\frac{\mathbb{F}_2^n}{\mathrm{C}} = 2^{n-k}|$, we have $|\frac{\mathbb{Z}^n}{\rho^{-1}(\mathrm{C})} = 2^{n-k}|$. In particular $\rho^{-1}(\mathrm{C})$ is a lattice in $\mathbb{R}^n$. By defining $\Gamma_\mathrm{C} := \frac{1}{\sqrt{2}}\rho^{-1}(\mathrm{C})$. We will state the following proposition without proof.

Proposition 1.9. Let C be a linear code.

1. $\mathrm{C} \subset \mathrm{C}^\perp$, if and only if Γ_C is an integral Lattice

2. C is doubly even if and only if Γ_{C} is an even Lattice.

3. C is self-dual if and only if Γ_{C} is a unimodular Lattice.

Lemma 1.10. Let $\mathrm{C} \subset \mathbb{F}_2^n$ be a binary linear code.Then

$$\Gamma_{\mathrm{C}}^* = \Gamma_{\mathrm{C}^\perp}$$

We recall some definitions from the coding theory

Definition 1.11. Let $\mathrm{C} \subset \mathbb{F}_2^n$ a $(\boldsymbol{n,k,d})$-*code*.

1. Let $c \in \mathrm{C}$, the Hamming weight is defined as $\mathrm{wt}(c) := |\{i|c(i) = 1\}|$.

2. The *Hamming weight enumerator* of C is a polynomial of $\mathbb{Z}[X,Y]$ defined as:

$$\begin{aligned} W_{\mathrm{C}}(X,Y) &:= \sum_{c \in \mathrm{C}} X^{n-\mathrm{wt}(c)} Y^{\mathrm{wt}(c)} \\ &= \sum_{i=0}^{i=n} A_i X^{n-i} Y^i \end{aligned}$$

where A_i denotes the number of codewords of weight i in C

Remark 1.12. i) We recognize $\langle , \rangle$ as the inner product of vectors. For simplicity of notation, we will denote $\langle u,v \rangle$ as $u \cdot v$, if it is clear in context that we are having a scalar product of two vectors. For the latter case, if we have two identical vectors u, we will abuse the notation u^2.

ii) For the brevity, we will simply call the *hamming weight enumerator* as *weight enumerator* in the following discussion.

Example 1.13. For the Hamming code $\mathrm{H} \subset \mathbb{F}_2^7$ with the generator matrix:

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

and the weight enumerator:

$$W_H(X,Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7$$

By considering the control matrix, we can see that the minimum distance is 3. So $A_2 = 0$. We could see that $1^7 \in H$, where 1^7 denotes the all-one vector. Consequently, the complement of every codeword is also a codeword in H. So $A_i = A_{7-i}$. Thus $A_5 = 0$. Given $A_0 = A_7 = 1, A_3 = A_4$, and $\sum_{i=0}^{i=7} = |H| = 16$, we obtainn that $A_3 = A_4 = 7$
In this case, it's also convenient to find the generator matrix of its dual code.

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

And we can find that the weight enumerator is

$$W_{H^{\perp}}(X,Y) = X^7 + 7X^3Y^4 + Y^7$$

By adding an extra parity bit in the generator matrix of H, we obtained the extended Hamming code $\widetilde{H}$.
The weight enumerator is

$$W_{\widetilde{H}}(X,Y) = X^8 + 14X^4Y^4 + Y^8$$

Based on the lecture of theta series and modular forms, we have learned the following proposition.

Proposition 1.14. Let $\mathrm{C} \subset \mathbb{F}_2^n$ be a self-dual doubly even code. Then $\mathrm{n} \equiv 0 \pmod 8$

Proof. Using the theorem 1.1 and proposition 1.9 □

We now want to prove a relationship between A_8 and A_4 for the special case $n = 24$ and C self-dual and doubly even.

Proposition 1.15. Let $n = 24$. $\mathrm{C} \subset \mathbb{F}_2^{24}$ a self-dual doubly even code, and let $W_{\mathrm{C}}(X,Y)$ be the Hamming weight enumerator. Then we obtain $A_i = 0$, if $i \not\equiv 0 \pmod 4$ and $A_8 = 759 - 4A_4$

Proof. Since C is self-dual doubly even, it follows that the theta function of Γ_{C} is a modular form of weight $\frac{n}{2}$.

$$\vartheta_{\Gamma_{\mathrm{C}}} = \sum_{r=0}^{\infty} a_r q^r$$

where a_r denotes the number of elements $x = \frac{1}{\sqrt{2}}(c + 2y) \in \Gamma_{\mathrm{C}}$, $c \in \mathrm{C}$, $y \in \mathbb{Z}^{24}$, with $x^2 = 2r$.
The proof comprises of three part:

1. express a_1, a_2 as polynomial in A_4, A_8 respectively
2. By using the following lemma 1.16, 1.17, find an equation of a_1 and a_2
3. substituting the equation we derived in 1 into the equation derived in 2.

In this proof, we perform the first step, i.e. find the relationship between a_1, a_2 and A_4, A_8.
For further analysis, it's helpful to note that:

$$x^2 = \frac{1}{2}(c + 2y)^2 = \sum_{i=1}^{24}(c_i + 2y_i)^2 \tag{1.15.1}$$

For a_1, we deduce that

$$a_1 = 24 \cdot 2 + A_4 \cdot 16 \tag{1.15.2}$$

It can be understood as following:
Note firstly that from (1.15.1), we need solve:

$$\sum_{i=1}^{24}(c_i + 2y_i)^2 \overset{!}{=} 4 \tag{1.15.3}$$

The possible cases are following: a) if $c = 0^{24}$, where 0^{24} denotes the zero vector in $\mathbb{F}_2^{24}$, then since $(\pm 2)^2 = 4$. We can choose one position to fill ± 2 and 0 elsewhere. This gives $24 \cdot 2$ choices
b) if $\mathrm{wt}(c) = 4$, then at the support (see definition 2.8) of c, y can be chosen -1 or 0 and 0 elsewhere. This gives $2^4 \cdot A_4$ choices. Since for other cases, (1.15.3) would be impossible. These are the only two possible cases. Combining the result, we prove consequently (1.15.2).
For a_2, we perform the similar analysis. First, we know that

$$\sum_{i=1}^{24} (c_i + 2y_i)^2 \overset{!}{=} 8 \tag{1.15.4}$$

There are three cases:
a) $c = 0^{24}$, then since $(\pm 2)^2 + (\pm 2)^2 = 8$, we have $\binom{24}{2} \cdot 2^2$ choices for the y_i.
b) $\mathrm{wt}(c) = 4$, then y could choose 1 or 0 at the support of c and choose ± 1 at another position where c is 0, since $(\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 + (\pm 2)^2 = 8$. This gives $A_4 \cdot 2^4 \cdot 20 \cdot 2$.
c) $\mathrm{wt}(c) = 8$, then y could only choose -1 or 0 at the support of c. This gives $A_8 \cdot 2^8$.
These are the only possible cases. Combining these results, it follows that

$$a_2 = 2^8 A_8 + 16 A_4 \cdot 20 \cdot 2 + \begin{pmatrix} 24 \\ 2 \end{pmatrix} \cdot 4 \tag{1.15.5}$$

□

We state the following lemma without proof.

Lemma 1.16. Let f be a modular form of weight 12 and

$$f(\tau) = \sum_{r=0}^{\infty} a_r q^r$$

its power series expansion in q. Then

$$a_2 = -24 a_1 + 196560 a_0$$

Proposition 1.17. Let $\Gamma \subset \mathbb{R}^2 4$ be an even unimodular lattice. Then

$$a_2 = 196560 - 24 a_1$$

Proof. We know that from theorem 1.1, the theta function ϑ_Γ is a modular form of weight 12. We now use lemma 1.16 combining the fact that $a_0 = 1$ for ϑ_Γ □

We now combine the proposition 1.17 to complete the proof of proposition 1.15.

Example 1.18. 1. We consider the direct sum of extended Hamming code $\mathrm{C} = \widetilde{H} \bigoplus \widetilde{H} \bigoplus \widetilde{H} \subset \mathbb{F}_2^{24}$. Since $\widetilde{H}$ is self-dual, so is the direct sum. Hence C is self-dual doubly even code with dimension 12.

$$\begin{aligned} W_{\mathrm{C}}(X,Y) &= (X^8 + 14X^4Y^4 + Y^8)^3 \\ &= X^{24} + 42X^{20}Y^4 + 591X^{16}Y^8 + \dots \end{aligned}$$

Since 591 = 759 - 168. It conforms with what proposition 1.15 asserts.

2. consider the extended Golay code $\widetilde{\mathrm{G}}$ (see section 2 and 3). $\widetilde{\mathrm{G}}$ is a self-dual doubly even code with minimum distance 8. It follows that

$$A_8 = 759$$

which we will see in section 2

Proposition 1.15 and 1.17 raises the question whether there exists code C with $A_4 = 0$ and lattice where $a_1 = 0$. We will answer that question in the next section.

2 The Golay Code and the Leech Lattice

In this section, we will discuss a particular type of codes, the golay codes. We will show that there exists a unique doubly even linear code $\widetilde{G} \subset \mathbb{F}_2^{24}$ with $A_4 = 0$. The following discussion on designs is largely based on chapter 4, section 3 of [2].
We shall first introduce some definitions.

Definition 2.1.

1. A set with t elements is called a **t-set**, a subset of a given set with t elements is called a **t-subset**

2. Let V be a **v-set** and each element is called a **point**. Let $\mathscr{D}$ be a collection of distinct **k-subset**. Every such **k-subset** is called a **block**. If for any **t-subset** T, there are exactly λ **k-subsets** B from S, s.t, $T \subset B$ then $\mathscr{D}$ is called a $\boldsymbol{t}$**-**$(\boldsymbol{v},\boldsymbol{k},\boldsymbol{\lambda})$ ***design***. We sometimes simply call it a $\boldsymbol{t}$-design.

3. A $\boldsymbol{t}$**-**$(\boldsymbol{v},\boldsymbol{k},1)$ design is called a *Steiner System*, denoted as $\boldsymbol{S}(\boldsymbol{t},\boldsymbol{k},\boldsymbol{v})$

Example 2.2. The projective plane of order 2 is a **2-**$(7,3,1)$ design, hence a $\boldsymbol{S}(2,3,7)$ *Steiner System*

Before we begin with the proofs, let us discuss some properties of the $\boldsymbol{t}$-design.

Lemma 2.3. If $\mathscr{D}$ be a $\boldsymbol{t}$***-design***. Then $\mathscr{D}$ is also a $\boldsymbol{s}$***-design***, for $0 \le s \le t$

Proof. Let $\mathscr{D}$ be a $\boldsymbol{t}$**-**$(\boldsymbol{v},\boldsymbol{k},\boldsymbol{\lambda})$ ***design***. Let S be a s-subset, we count the pairs (T,B) with the property, that $S \subset T \subset B$, with T a t-subset and B a block of $\mathscr{D}$. We denote λ_s as the number of blocks in $\mathscr{D}$ which contains S. We want to show that λ_s is independent of the set S, but only depends on the size of the set. For each $\binom{v-s}{t-s}$ choices of T that contains S, we have λ blocks B which contains T. In another way, for each of the λ_s $\boldsymbol{block}$ that contains S, there are $\binom{k-s}{t-s}$ choices for T. So we obtain:

$$\lambda_s \binom{k-s}{t-s} = \lambda \binom{v-s}{t-s}$$

$$\Rightarrow \quad \lambda_s = \frac{\lambda \binom{v-s}{t-s}}{\binom{k-s}{t-s}} \tag{2.3.1}$$

In particular λ_s is only dependent on the size of the subsets. So that $\mathscr{D}$ is a $\boldsymbol{s}$***-design*** □

Corollary 2.4. Let $\mathscr{D}$ be a $\boldsymbol{t}$-$(\boldsymbol{v},\boldsymbol{k},\boldsymbol{\lambda})$ ***design***. Then $\mathscr{D}$ has b blocks, where

$$b = \frac{\lambda\binom{v}{t}}{\binom{k}{t}}$$

Let us denote λ_0 as b (total number of blocks) and λ_1 as r (total number of blocks containg a given point)
Before proving the next lemma, we need a another fact from linear algebra.

Lemma 2.5. Let I be the identity matrix in $M := \mathbb{R}^{n\times n}$ Let $J \in M$ be the matrix with all entries equal to 1, and $k \in \mathbb{R}^* \backslash \{-\frac{1}{n}\}$, then $A := I + kJ$ is invertible.

Proof. Since $(kJ)^2 = k^2nJ$ we can conclude that the minimal polynomial of A is:

$$\mu_A(x) := (x-1)(x-1-(kn))$$

In particular $\mu_A(0) \neq 0$, so A is invertible. □

Lemma 2.6. In a $\mathbf{2}$-$(\boldsymbol{v},\boldsymbol{k},\boldsymbol{\lambda})$ ***design*** with $b = v$, $k = r$, any two blocks have exactly λ common points.

Proof. Let I, J have the same meaning as in the previous lemma for $n = v$.
We first note that $\lambda \neq r$, since λ denotes the number of blocks that contain two given points and r denotes the number of blocks that contain one given point. In particular $r > \lambda$
We define the characteristic vectors of the blocks as the rows of a $b \times v$ matrix M. That is

$$M_{i,j} = \begin{cases} 1, & \text{if block } i \text{ contains the point } j \\ 0, & \text{otherwise} \end{cases}$$

Denote the i-th block as B_i, and the j-th point as v_j, $1 \leq i \leq b, 1 \leq j \leq v$ Now we have the two equations:

$$\sum_{j=1}^{v} M_{i,j} = |\{v \mid v \in B_i\}| \tag{2.6.1}$$

$$\sum_{i=1}^{b} M_{i,j} = \left|\{i \mid v_j \in B_i\}\right| \tag{2.6.2}$$

Based on these two equations, we can translate the condition that any block contains k points and that any point lies in r blocks in view of $k = r$ into following:

$$MJ = kJ = rJ = JM$$

Meanwhile, if we denote $M = (w_1|w_2|\ldots|w_v)$, it follows that:

$$\begin{aligned} w_j^t w_i &= \left|\{i \mid v_j \in B_i \wedge v_i \in B_i\}\right| \qquad (2.6.3) \\ &\overset{\wedge}{=} \text{“Number of blocks that contain both } v_i \text{ and } v_j\text{”} \end{aligned}$$

If we denote

$$M = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_b \end{pmatrix}$$

Then it follows that:

$$\begin{aligned} u_i u_j^t &= \left|\{v_i \mid v_i \in B_i \wedge v_i \in B_j\}\right| \qquad (2.6.4) \\ &\triangleq \text{“Number of points that both block } B_i \text{ and } B_j \text{ contains”} \end{aligned}$$

The condition that we have a **2-(v,k,λ) *design***, i.e. any pair of points lies in λ blocks can be expressed based on (2.6.3) as follows:

$$M^t M = (r-\lambda)I + \lambda J$$

We see that $r - \lambda > 0$ so that we can apply (Lemma 2.5). In particular M is invertible.
Since M commutes with J and $M^t = ((r-\lambda)I + \lambda J)M^{-1}$, M also commutes with M^t and thus:

$$MM^t = (r-\lambda)I + \lambda J$$

Based on (2.6.4) we see that any two blocks have exactly λ points in common. □

Proposition 2.7. There is only one **2-$(11,5,2)$ *design***

Proof. We conclude in this case according to (2.3.1):

$$b = \frac{2\binom{11}{2}}{\binom{5}{2}} = 11 = v$$

$$r = \frac{2\binom{11-1}{2-1}}{\binom{5-1}{2-1}} = 5$$

Therefore, we can apply Lemma 2.6 and it follows that any two blocks have 2 common points.
w.l.o.g we choose the characteristic vector of the first block as (11111000000). The remaining blocks correspond to the 2-$subset$s of the first five points.
we can choose the second row as (11000111000) and the following 4 rows can be chosen in the similar way. For the 6-th row, there are two choices, namely (01100010011) or (01100001101). And the rest are uniquely determined.
We obtain for the first choice the matrix:

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

For the second choice of the matrix, we just interchange the column 4 and 5 , 7 and 8, and 9 and 10 and the corresponding rows. In other words, it's just the same matrix, when we renumerate the points appropriately. □

Now let us come back to codes and discuss the relationship between design and codes.
Let $\widetilde{\mathrm{G}}$ be a binary code of length n.
First we define $S_d := \{c \,|\, wt(c) = d, c \in \widetilde{\mathrm{G}}\}$ as the set of codes of $\widetilde{\mathrm{G}}$, s.t the weight of the codes equals d

Definition 2.8. Let x, y two binary words of length n

1. The sphere around x with radius r is denoted as $B(x,r)$ with respect to the usual hamming distance.

2. The **support** of x is the set of positions in which x has no zero entries.

3. We say that x **covers** y, if the support y is a subset of x

4. We say that S_d **holds a** ***t*-(n,d,λ) *design***, if the support of the codewords of S_d form the blocks of a ***t*-(n,d,λ) *design***. In other words, for any ***t-set*** T, there are exactly λ words in S_d s.t the codes has 1 in position given by T

Lemma 2.9. Let $\widetilde{\mathrm{G}}$ be a perfect binary (n,M,d)-*code*. Then the set S_d of all codewords of minimum distances d holds a *Steiner system* $S(t+1,d,n)$, where $d = 2t+1$

Proof. Since $\widetilde{\mathrm{G}}$ is perfect, so all the spheres $B(c,t)$ are disjoint with one another. So given a binary word x of length $t+1$, it must be included exclusively in one sphere, say $B(c,t)$. Now, since $wt(c) \leq wt(x) + d(c,x) = t+1+t = d$, so we deduce that $c \in S_d$. The cardinality of the intersection of support of these two words is thus:

$$\begin{aligned} & 2wt(x \cap c) = wt(x) + wt(c) - d(x,c) \geq 2t+2 \\ \Rightarrow \quad & wt(x \cap c) \geq t+1 \end{aligned}$$

So c **covers** x.
Now if there is another $\tilde{c} \in S_d$ that also **covers** x. Then the weight must satisfy:

$$wt(\tilde{c}) \geq wt(x \cap \tilde{c}) + d(x,\tilde{c}) \geq 2t+2 = d+1$$

which is impossible.
So S_d is a ***t*** **1-$(n,d,1)$** ***design***, hence $S(t+1,d,n)$ *Steiner System* □

Corollary 2.10. Let $\widetilde{\mathrm{G}}$ be a perfect binary (n,M,d)-*code*. Let A_d denotes the number of words of $\widetilde{\mathrm{G}}$ with weight d. Then

$$A_d = \frac{\binom{n}{t+1}}{\binom{d}{t+1}}$$

Proof. Using Collary 2.4 and Lemma 2.9 □

Example 2.11. For hamming $(7,4,3)$-*code*. We obtain

$$A_3 = \frac{\binom{7}{2}}{\binom{3}{2}} = 7$$

Before we discuss the main theorem, it's helpful to recall that for two vectors u,v in $\mathbb{F}_2^n$:

$$\mathrm{d}(u,v) = \mathrm{wt}(u) + \mathrm{wt}(v) - 2\langle u,v\rangle \tag{2.11.1}$$

We come to the main theorem in this section.

Theorem 2.12. Let $\widetilde{\mathrm{G}}$ be a binary $(24,2^{12},8)$-*code* containing 0. Then $\widetilde{\mathrm{G}}$ is a up to equivalence the only one doubly even self-dual linear $(24,12,8)$-*code*. We call $\widetilde{\mathrm{G}}$ the *extended Golay code*

Proof. Let $\widetilde{\mathrm{G}}$ be such a code. We first punctuate a position of each code word and denote the resulted code as G. This code has minimum distance 7 or 8. So it is a $(23,2^{12},7)$-*code* or $(23,2^{12},8)$-*code*. No matter the minimum distance is 7 or 8, the sphere $B(c,3)$ are disjoint from each other for all codes $c \in \mathrm{G}$.
We show that the minimum distance is 7. Indeed:

$$2^{12} \cdot (1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}) = 2^{23}$$

In particular, this argument shows that the spheres $B(c,3)$ covers the space $\mathbb{F}_2^{23}$ and it follows that the minimum distance is 7. (otherwise, there are “leak points” at the middle of the distance between these two points and these points are not covered, contradictory to the full packing) and G is perfect.
Since $0 \in \mathrm{G}$, $A_0 = 1$, using Collary 2.10, we obtain $A_7 = \frac{\binom{23}{4}}{\binom{7}{4}}$.
To calculate A_8, we know that the number of vectors of weight 5 in $\mathbb{F}_2^{23}$ are given by $\binom{23}{5}$ and they may lie in the spheres of codes with weights 7 or 8. So we conclude that:

$$A_8 = \frac{\binom{23}{5} - A_7\binom{7}{5}}{\binom{8}{5}} = 506$$

Using the same idea, we could easily infer that

$$A_k = \frac{B}{\binom{k}{k-3}} \quad , \text{for } 8 \le k \le 23 \tag{2.12.1}$$

where B stands for

$$\begin{aligned} B := \binom{23}{k-3} - \{ & A_{k-6} \cdot \binom{23-(k-6)}{3} + A_{k-5} \cdot \binom{23-(k-5)}{2} \\ & + A_{k-4} \cdot \left[(k-4) \cdot \binom{23-(k-4)}{2} + (23-(k-4)) \right] \\ & + A_{k-3} \cdot [(k-3)\cdot(23-(k-3))] + A_{k-2} \cdot \left[(k-2) + \binom{k-2}{2} \cdot (23-(k-2)) \right] \\ & + A_{k-1} \cdot \binom{k-1}{2} \} \end{aligned}$$

we obtain thus the following weight counts:

$$
\begin{aligned}
A_9 &= \frac{\binom{23}{6} - (A_7 \cdot (7 + 16 \cdot \binom{7}{5}) + A_8 \cdot \binom{8}{6})}{\binom{9}{6}} = 0\\
A_{10} &= \frac{\binom{23}{7} - (A_7 \cdot (1 + 7 \cdot 16) + A_8 \cdot (8 + 15 \cdot \binom{8}{2}))}{\binom{10}{7}} = 0\\
A_{11} &= \frac{\binom{23}{8} - (A_7 \cdot (16 + 7 \cdot \binom{16}{2}) + A_8 \cdot (1 + 8 * 15))}{\binom{11}{8}} = 1288\\
A_{12} &= \frac{\binom{23}{9} - (A_7 \cdot \binom{16}{2} + A_8 \cdot (15 + 8 \cdot \binom{15}{2}) + A_{11} \cdot \binom{11}{2})}{\binom{12}{9}} = 1288\\
A_{13} &= \frac{\binom{23}{10} - (A_7 \cdot \binom{16}{3} + A_8 \cdot \binom{15}{2} + A_{11} \cdot (11 + \binom{11}{2} \cdot 12) + A_{12} \cdot \binom{12}{2})}{\binom{13}{10}} = 0\\
A_{14} &= \frac{\binom{23}{11} - (A_8 \cdot \binom{15}{3} + A_{11} \cdot (1 + 11 \cdot 12) + A_{12} \cdot (12 + \binom{12}{2} \cdot 11))}{\binom{14}{11}} = 0\\
A_{15} &= \frac{\binom{23}{12} - (A_{11}(12 + 11 \cdot \binom{12}{2}) + A_{12} \cdot (1 + 12 \cdot 11))}{\binom{15}{12}} = 506\\
A_{16} &= \frac{\binom{23}{13} - (A_{11} \cdot \binom{12}{2} + A_{12} \cdot (11 + 12 \cdot \binom{11}{2}))}{\binom{16}{13}} = 253\\
A_{17} &= \ldots = 0\\
&\vdots\\
A_{22} &= \ldots = 0\\
A_{23} &= \frac{\binom{23}{20}}{\binom{23}{20}} = 1
\end{aligned}
$$

Now if $\widetilde{\mathrm{G}}$ contains a codeword of weight w which is not divisible by 4, then by puncturing the $\widetilde{\mathrm{G}}$ appropriately, we will obtain codeword of weight w or $w-1$ not equal to 0 or -1 (mod 4), which contradicts the weight enumerator coefficients calculated above. So we conclude that $\widetilde{\mathrm{G}}$ is doubly even and we infer that the weight enumerator coefficients for $\widetilde{\mathrm{G}}$

$$A_0 = A_{24} = 1, A_8 = A_{16} = 759, A_{12} = 2576$$

In particular all the distances between two codewords are divisible by 4. We deduce from 2.11.1 that for all $u, v \in \widetilde{\mathrm{G}}$, $\langle u, v \rangle \in 2\mathbb{Z}$, and it follows in this case that $\widetilde{\mathrm{G}} \subset \widetilde{\mathrm{G}}^{\perp}$. But since $\widetilde{\mathrm{G}}^{\perp}$ is a linear subspace of dimensions 24 - $\dim\langle\widetilde{\mathrm{G}}\rangle \leq 12$. It follows that $\langle\widetilde{\mathrm{G}}\rangle$ has less than 2^{12} elements. Since $\widetilde{\mathrm{G}} \subset \langle\widetilde{\mathrm{G}}\rangle$ we follow from the cardinality of $\widetilde{\mathrm{G}}$ that $\widetilde{\mathrm{G}} = \widetilde{\mathrm{G}}^{\perp}$ and $\widetilde{\mathrm{G}}$ is linear.

Now we prove the uniqueness of such codes.

Consider a codeword u of weight 12 in $\widetilde{\mathrm{G}}$ and since $A_{24} = 1$, we have another codeword $\bar{u}$ s.t $u + \bar{u} = 1^{24}$ where 1^{24} stands for the all-one vector in $\mathbb{F}_2^{24}$. Let us denote $\widetilde{\mathrm{G}}_u$ as the subspace when we puncture all the positions of $\widetilde{\mathrm{G}}$ given by the support of u. Define the function π_u as the canonical projection. We deduce that for $c \in \widetilde{\mathrm{G}}$, both c and $c+u$ will be projected to the same image. Since c is arbitrarily chosen, it follow that $|\widetilde{\mathrm{G}}_u| \leq \frac{2^{12}}{2} = 2^{11}$. Now if there are two different codewords $x, y \in \widetilde{\mathrm{G}}$ s.t $\pi_u(c) = \pi_u(y)$ and $x - y = v \neq u$. Then we know that u covers v and $v \in \widetilde{\mathrm{G}}$ so $\mathrm{wt}(v) \geq 8$. It follows that $\mathrm{d}(u,v) \leq 4$, contradicting the fact that the minimum distance is 8. So $\widetilde{\mathrm{G}}_u$ has exactly 2^{11} elements hence a linear subspace of dimension 11.

For all the codes $v \in \widetilde{\mathrm{G}}_u$, Let $x \in \widetilde{\mathrm{G}}$ s.t $\pi_u(x) = v$. It follows that $\mathrm{wt}(v) = x \cdot \bar{u} \in 2\mathbb{Z}$ since $x, \bar{u} \in \widetilde{\mathrm{G}}$ and $\widetilde{\mathrm{G}}$ is doubly even. It follows that $\widetilde{\mathrm{G}}_u$ is of word length 12, dimension 11, and every codeword is of even length. So by arranging the columns of the codeword appropriately, the generator matrix of $\widetilde{\mathrm{G}}$is of the form:

$$G := \left[\begin{array}{c|c|c|c} 1^{11} & 1 & 0 & 0^{11} \\ \hline A & (0^{11})^t & (1^{11})^t & I_{11} \end{array}\right]$$

where I_{11} is the 11×11 identity matrix and a^k denotes a row vector of length k and every entry is a. Since $\widetilde{\mathrm{G}}$ has minimum distance 8, we deduce that each row of the matrix G has weight ≥ 8. The matrix A has consequently two properties:

1. each row has weight ≥ 6

2. every two rows have distance ≥ 6

We claim that actually in both properties the equality holds.

First equality: take for example, $G_{1,-}$ and $G_{2,-}$. It follows that $\mathrm{d}(G_{1,-}, G_{2,-}) = \mathrm{d}(1^{11}, A_{1,-}) + 3 \geq 8$. So $\mathrm{wt}(A_{1,-}) \leq 6$. Combining the property 1, $\mathrm{wt}(A_{1,-}) = 6$. Similarly, all the row of A must have weight 6.

Second equality: since $\widetilde{\mathrm{G}}$ is doubly even and linear, $4 \mid \mathrm{d}(G_{i,-}, G_{j,-})$, for $1 \leq i,j \leq 12$. Using the equality in property 1, it follows that $\mathrm{d}(A_{i,-}, A_{j,-}) \in \{6, 10\}$. If $\mathrm{d}(A_{i,-}, A_{j,-}) = 10$, then it follows that $\mathrm{d}(1^{11}, A_{i,-} - A_{j,-}) = 1$, and hence $\mathrm{d}(G_{1,-}, G_{i,-} - G_{j,-}) = 4$, contradicting the fact that $\widetilde{\mathrm{G}}$ has minimum weight 8. So equality holds.

Now, we only need to prove the uniqueness. We resort to proposition 2.7.

The idea is to prove that the submatrix A in G is up to column and corresponding row permutation unique. We define $B := J_{11} - A$, where J is the 11×11 matrix with all entries 1. Then $\mathrm{wt}(B_{i,-}) = 5$, for all $1 \leq i \leq 11$. And $\mathrm{d}(B_{i,-}, B_{j,-}) = 6$. Using 2.11.1, it follows $\mathrm{wt}(B_{i,-} \cap B_{j,-}) = 2$. We define a set of eleven elements P and a collection $\mathscr{D}$ of eleven 5-*subset* of P. For clarity, we denote each element of P as point, and each element of $\mathscr{D}$ as block. Note it is not a coincidence with the definition 2.1, since we will see $\mathscr{D}$ is actually a design. We identify B as the incidence matrix of the collection $\mathscr{D}$. It follows that $BJ = 5J$. Since every two blocks of $\mathscr{D}$ has exactly two points in common and $|P| = |\mathscr{D}|$, there is a bijection between $M := \{D | D \subset \mathscr{D}, |D| = 2\}$ and $N := \{T | T \subset P, |T| = 2\}$ by defining

$$\phi : M \to N, \quad \{B_1, B_2\} \mapsto B_1 \bigcap B_2$$

So it follows that every 2-*subset* of points is contained in exactly two blocks. So $\mathscr{D}$ is a
2-(11,5,2) *design*.

Applying proposition 2.7, we find that B is unique up to renumbering of points. Hence the code $\widetilde{\mathrm{G}}$ is unique up to equivalence. □

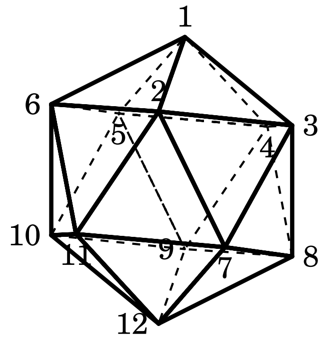

Figure 2.12.1: icosahedron

We now want to construct such a code. For that purpose, let us consider the regular icosahedron as a graph. Let A be the adjacency matrix of this graph. By numbering the 12 vertices as shown in the figure 2.12.1. We define the entry of A as:

$$A_{i,j} = \begin{cases} 1, & \text{if there is an edge between point } i \text{ and point } j \\ 0, & \text{otherwise} \end{cases}$$

It follows that A has the form:

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

More over, define $B := J_{12} - A$. Then it follows that

$$B^t B = I_{12} \in \mathbb{F}_2^{12\times 12}. \tag{2.12.2}$$

It follows that the column vector $B_{-,i} = u + v_i$,where $u = J_{12-,i}$ and $v = A_{-,i}$:

$$\begin{aligned} (u+v_i)^t(u+v_j) &= u^t u + u^t(v_i + v_j) + v_i^t v_j \\ &= 12 + a + b \end{aligned}$$

Now by observing the figure 2.12.1, it follows that $v_i + v_j \in \{10, 6\}$, $v_i^t v_j \in \{2, 0\} \in \mathbb{Z}$, in particular, all the three terms above are 0 in $\mathbb{F}_2$. So the row of the matrix $G := (I_{12}B)$ generate the the **(24,12,8)-*code*** $\widetilde{\mathrm{G}}$.

Proof. The generated code is certainly linear, of length 24 and has dimension 12. The only thing to prove is the minimum distance.
By observing the matrix of G we find that each row of G has weight 8, in particular divisable by 4. So using (2.11.1), we deduce that $\widetilde{\mathrm{G}}$ is doubly even.
Observing that $G^tG = I_{24}$, it follows that $\widetilde{\mathrm{G}}$ is self-dual.
For the linear combination of more than three rows of G we will see at least four 1s on the first 12 position. By using (2.12.2) it is impossible that all the entries on the right half of the 12 position of codeword are complete 0. (otherwise B would have nontrivial kernel which contradicts the fact that B is invertible). In particular every such combination creates codeword with codeword ≥ 5, hence at least 8. So the only case to consider is the linear combination of two or three vectors.
On reconsidering the icosahedron, from which the adjacency matrix A is derived, we could make a similar interpretation of B, that is

$$B_{i,j} = \begin{cases} 0, & \text{there is an edge between point } i \text{ and point } j \\ 1, & \text{otherwise} \end{cases}$$

And for the sum $c_{i,j} := B_{i,-} + B_{j,-}$ of two row vectors of B

$$c_{i,j}(k) = \begin{cases} 1, & \text{there is an edge from point } i \text{ or } j \text{ to } k\text{, but not both} \\ 0, & \text{otherwise} \end{cases}$$

The possible results are $\{6,10\}$. With two 1s on the left 12 positions, the weights are $\{8,12\}$.
Similarly, for the sum of three vectors v_i ,v_j and v_k, there is a 1 at position l if vertice l is connected to exactly two of the three or none of the three. the possible results are $\{5,9\}$. With three 1s on the left 12 poisitions, the weights are $\{8,12\}$. □

Now we want to construct an even unimodular lattice with $a_1 = 0$, i.e., does not contains roots, using the extended golay code $\widetilde{\mathrm{G}}$. We recall that $\rho : \mathbb{Z}^{24} \to \mathbb{F}_2^{24}$ defines a canonical projection and the corresponding lattice of the $\widetilde{\mathrm{G}}$ is $\Gamma_{\widetilde{\mathrm{G}}} := \frac{1}{\sqrt{2}}\rho^{-1}(\widetilde{\mathrm{G}})$. We denote $\Gamma := \rho^{-1}(\widetilde{\mathrm{G}})$.
The goal is to construct a lattice which contains no roots based on Γ. We recall that an element x in a lattice is called a root if and only if $x^2 = 2$. We want to construct a lattice of the form $\frac{1}{\sqrt{2}}\Gamma_1$, for some sublattice Γ_1 of Γ, so we want to find a lattice which contains no elements of squared length 4, i.e. $x^2 = 4$.
For every element x of Γ, $x = c + 2y$, for $c \in \widetilde{\mathrm{G}}, y \in \mathbb{Z}^{24}$.
It's instructive to consider a_1 of the theta function for $\Gamma_{\widetilde{\mathrm{G}}}$ first. We know according to (1.15.2) that:

$$a_1 = 48$$

We know from the proof of proposition 1.15, that all the vectors which contribute to a_1 is of the form $(\pm 2)^1 0^{23}$, where the notation $a^k b^j$ means a vector in whose entry a appears k times and b j times. We want to get rid of these 48 vectors, so that we could have no roots in the lattice.
We define

$$\begin{aligned} \alpha : \Gamma &\to \mathbb{F}_2 \\ x &\mapsto \frac{1}{2}\sum x_i \pmod 2 \end{aligned}$$

We note that since all the codewords in $\widetilde{\mathrm{G}}$ has weight divisable by 4:

$$\frac{1}{2}\sum x_i \equiv \sum y_i \pmod 2$$

In particular all the roots in $\Gamma_{\widetilde{\mathrm{G}}}$ will be mapped to 1.
So by defining $A := \alpha^{-1}(0)$, we obtain a sublattice which contains no roots of $\Gamma_{\widetilde{\mathrm{G}}}$.
We define $N := \alpha^{-1}(1)$ and $O := A \bigcup (\frac{1}{2}1^{24} + N)$.

Proposition 2.13. *O is a lattice and every element has squared length divisable by 4*

Proof. For simplicity of notation, we define $M = \frac{1}{2}1^{24} + N$
Note first that M is symmetric, since given $v \in M$, then $v = \frac{1}{2}1^{24} + c + 2y$, $c \in \widetilde{\mathrm{G}}$, $y \in \mathbb{Z}^{24}$ with $\sum y_i$ odd.

$$\begin{aligned} -v &= -\frac{1}{2}1^{24} - c - 2y \\ &= -\frac{1}{2}1^{24} - c - 2(y + 1^{24}) + 2^{24} \\ &= \frac{1}{2}1^{24} + \underbrace{(1^{24} - c)}_{\substack{\in \widetilde{\mathrm{G}}, \\ \text{since } 1^{24} \in \widetilde{\mathrm{G}}}} - 2\tilde{y} \in M \end{aligned}$$

To prove that O is a lattice, we only need to prove that O is closed under addition. Since A is as kernel of a homomorphism automatically a additive group, we only need to check the following two cases:

i) $u \in A$, $v \in M$, then $u = e + 2r$, $e \in \widetilde{\mathrm{G}}$, $r \in \mathbb{Z}^{24}$ with $\sum r_i$ even and $v = \frac{1}{2}1^{24} + c + 2y$, $c \in \widetilde{\mathrm{G}}$, $y \in \mathbb{Z}^{24}$ with $\sum y_i$ odd. Then $u + v = \frac{1}{2}1^{24} + \tilde{c} + 2\tilde{y}$, for some $\tilde{c} \in \widetilde{\mathrm{G}}$ and $\tilde{y} \in \mathbb{Z}^{24}$ with $\sum \tilde{y}_i$ odd. So $u + v \in M$

ii) $u \in M$, $v \in M$, then $u = \frac{1}{2}1^{24} + e + 2r$, $e \in \widetilde{\mathrm{G}}$, $r \in \mathbb{Z}^{24}$ with $\sum r_i$ odd and $v = \frac{1}{2}1^{24} + c + 2y$, $c \in \widetilde{\mathrm{G}}$, $y \in \mathbb{Z}^{24}$ with $\sum y_i$ odd. Then

$$\begin{aligned} u + v &= \overbrace{1^{24} + c + e}^{\in \widetilde{\mathrm{G}}} + 2(r + y) \\ &= \tilde{c} + 2\tilde{y} \in A \end{aligned}$$

for some $\tilde{c} \in \widetilde{\mathrm{G}}$ and $\tilde{y} \in \mathbb{Z}^{24}$ with $\sum \tilde{y}_i$ even. So $u + v \in A$,

To prove the property of squared length. We consider first the vector in A.
Let $v = c + 2y \in A$, $c \in \widetilde{\mathrm{G}}$, $y \in \mathbb{Z}^{24}$ with $\sum y_i$ even.

$$\begin{aligned} v^2 &= \sum (c_i + 2y_i)^2 \\ &\equiv \sum c_i \pmod 4 \\ &\equiv \mathrm{wt}(c) \pmod 4 \\ &\equiv 0 \pmod 4 \end{aligned}$$

Now let $v = \frac{1}{2}1^{24} + c + 2y \in M$, $c \in \widetilde{\mathrm{G}}$, $y \in \mathbb{Z}^{24}$ with $\sum y_i$ odd.

$$\begin{aligned} v^2 &= \sum(\frac{1}{2} + c_i + 2y_i)^2 \\ &\equiv \sum(1/4 + c_i + c_i + 2y_i) \pmod 4 \\ &\equiv 6 + 2\mathrm{wt}(c) + 2\sum y_i \pmod 4 \\ &\equiv 0 \pmod 4 \end{aligned}$$

□

Remark 2.14. We know from theorem of homomorphism that A has index 2 in Γ and it follows that A also has index 2 in O

We are now able to construct the *Leech lattice*

Definition 2.15. The *Leech lattice* is defined as

$$\Lambda_{24} := \frac{1}{\sqrt{2}}\left(A \bigcup (\frac{1}{2}1^{24} + N)\right)$$

Lemma 2.16. The lattice Λ_{24} is well-defined and is an even unimodular lattice, which contains no roots.

Proof. It follows from proposition 2.13, that Λ_{24} is a indeed a lattice (so well-defined) and it's even.
To prove unimodularity:
We know from remark 2.14, that A has index 2 in O, so $A_1 := \frac{1}{\sqrt{2}}A$ is a sublattice with index 2 in $\Gamma_{\widetilde{\mathrm{G}}}$. Note that A_1 also has index 2 in Λ_{24}.

$$\mathrm{vol}(\mathbb{R}^{24}/\Lambda_{24}) \cdot |\Lambda_{24}/A_1| \;=\; \mathrm{vol}(\mathbb{R}^{24}/A_1) \;=\; \mathrm{vol}(\mathbb{R}^{24}/\Gamma_{\widetilde{\mathrm{G}}}) \cdot |\Gamma_{\widetilde{\mathrm{G}}}/A_1|$$

it follows that

$$\mathrm{vol}(\mathbb{R}^{24}/\Lambda_{24}) \;=\; \mathrm{vol}(\mathbb{R}^{24}/\Gamma_{\widetilde{\mathrm{G}}}) \;=\; 1$$

So Λ_{24} is unimodular. □

3 The MacWilliams Identity and Gleason's Theorem

We have till now studied the theta function of the lattices and the weight enumerator of the binary codes. In addition, we have learned there is a relationship between the binary codes and the corresponding lattices. We will study in this section first the relevance between the theta function and the weight enumerator, then we will prove the *MacWilliams Identity* and *Gleason's Theorem* using the properties of theta functions.

We consider first two functions: Let $A(\tau)$ denote the theta function of the lattice $\Gamma = \sqrt{2}\mathbb{Z}$, i.e.

$$\begin{aligned} A(\tau) &= \sum_{x\in\Gamma} q^{\frac{1}{2}x\cdot x} \\ &= \sum_{x\in\mathbb{Z}} q^{x\cdot x} \\ &= \sum_{x\in 2\mathbb{Z}} q^{\frac{1}{4}(x\cdot x)} \qquad (3.0.1) \\ &= 1+2q+2q^4+2q^9+\dots \end{aligned}$$

Consider another function:

$$B(\tau) := \sum_{x\in 2\mathbb{Z}+1} q^{\frac{1}{4}(x\cdot x)} \qquad (3.0.2)$$

Note that $B(\tau)$ is not a theta function of a lattice, since the constant term is not 0. By adding the two functions together, it follows that

$$A(\tau)+B(\tau) = \sum_{x\in\mathbb{Z}} q^{\frac{1}{4}(x\cdot x)} = \sum_{x\in\frac{1}{\sqrt{2}}\mathbb{Z}} q^{\frac{1}{2}x\cdot x} = \sum_{x\in\Gamma^*} q^{\frac{1}{2}(x\cdot x)} \qquad (3.0.3)$$

So the sum of the two functions is the theta function of the dual lattice of Γ. Using proposition 1.2, it follows :

$$A(-\frac{1}{\tau}) = (\frac{\tau}{i})^{1/2}\frac{1}{\sqrt{2}}(A(\tau)+B(\tau)). \qquad (3.0.4)$$

By replacing the τ into $-\frac{1}{\tau}$, we obtain from (3.0.4)

$$\begin{aligned} A(\tau) &= [A(-\frac{1}{\tau})+B(-\frac{1}{\tau})]\frac{1}{\sqrt{2}}(\frac{1}{-\tau i})^{\frac{1}{2}} \\ \Rightarrow \quad B(-\frac{1}{\tau}) &= \frac{\sqrt{2}}{(-\frac{1}{\tau i})^{\frac{1}{2}}}A(\tau) - (\frac{\tau}{i})^{1/2}\frac{1}{\sqrt{2}}(A(\tau)+B(\tau)) \\ &= (\frac{\tau}{i})^{\frac{1}{2}}\frac{1}{\sqrt{2}}(A(\tau)-B(\tau)) \qquad (3.0.5) \end{aligned}$$

When we consider A and B as two variables, and consider now the “rotation by 45° followed by a reflection”,i.e.

$$Q := \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

in the (A,B)-plane. For simplicity of notation we identify A as $(A,0)^t$ and B as $(0,B)^t$, then it follows that:

$$QA = \frac{1}{\sqrt{2}}(A+B)$$

$$QB = \frac{1}{\sqrt{2}}(A-B)$$

We can find that the following homogeneous polynomial in A and B of degree 24 is invariant under such transformation by elementary algebra.

$$A^4B^4(A^2-B^2)^4(A^2+B^2)^4 \; = \; A^4B^4(A^4-B^4)^4$$

For simplicity, we define $g := A^4B^4(A^4-B^4)^4$ and $p := X^4Y^4(X^4-Y^4)^4 \in \mathbb{C}[X,Y]_{hom,24}$

Proposition 3.1. $g(-\frac{1}{\tau}) = \tau^{12} g(\tau)$

Proof. We deduce that:

$$g(-\frac{1}{\tau}) = A(-\frac{1}{\tau})^4 B(-\frac{1}{\tau})^4 (A(-\frac{1}{\tau})^4 - B(-\frac{1}{\tau})^4)^4$$

$$= ((\frac{\tau}{i})^{\frac{1}{2}} QA)^4 ((\frac{\tau}{i})^{\frac{1}{2}} QB)^4 (((\frac{\tau}{i})^{\frac{1}{2}} QA)^4 - ((\frac{\tau}{i})^{\frac{1}{2}} QB)^4)^4$$
$$= (\frac{\tau}{i})^{12} p(QA,QB)$$
$$= \tau^{12} p(A,B) = \tau^{12} g(\tau)$$

□

Since A is invariant under the transformation $\tau \mapsto \tau+1$ and so does B^4, it follows that $A^4 B^4 (A^4 - B^4)^4$ is invariant under this transformation.
Combining these two results, we deduce that $A^4 B^4 (A^4 - B^4)^4$ is a modular form of weight 12.

Proposition 3.2.

$$g := A^4 B^4 (A^4 - B^4)^4 \; = \; 16\Delta \; = \; 16q \prod_{n=1}^{\infty} (1-q^n)^{24}$$

Proof. Since the constant term of B is zero, so is the constant term of g. It follows that g is a cusp form of weight 12.
According to theorem 1.6, $g = k\Delta$ for a $k \in \mathbb{C}$. We could determine k by looking at the coefficient of the term of the first order.
Since

$$B(\tau) = 2q^{\frac{1}{4}} + 2q^{\frac{9}{4}} + 2q^{\frac{25}{4}} + \dots$$

So, it follows that

$$B(\tau)^4 = 16q + \text{high order terms}$$

As a result

$$A^4 B^4 (A^4 - B^4)^4 = 16q + \text{high order terms}$$

So, we deduce that $A^4 B^4 (A^4 - B^4)^4 = 16\Delta$ □

Proposition 3.3. Let $\mathrm{C} \subset \mathbb{F}_2^n$ be a binary linear code with Hamming weight enumerator $W_{\mathrm{C}}(X,Y)$. Then

$$\vartheta_{\Gamma_{\mathrm{C}}} = W_{\mathrm{C}}(A,B)$$

Proof. Let $c \in \mathrm{C}$, and let $\rho : \mathbb{Z}^n \to \mathbb{F}_2^n$ be the canonical reduction modulo 2 projection. Then

$$\sum_{x \in \frac{1}{\sqrt{2}}\rho^{-1}(c)} q^{\frac{1}{2}(x\cdot x)} = \sum_{x \in \rho^{-1}(c)} q^{\frac{1}{4}(x\cdot x)}$$

$$= \sum_{(y_1,y_2,\dots,y_n)\in\mathbb{Z}^n} q^{\frac{1}{4}\sum_{i=1}^{n}(c_i+2y_i)^2}$$

$$= \prod_{i=1}^{n} (\sum_{y\in\mathbb{Z}} q^{\frac{1}{4}(c_i+2y)^2})$$

Since

$$\sum_{y\in\mathbb{Z}} q^{\frac{1}{4}(c_i+2y)^2}) = \begin{cases} \sum_{y\in\mathbb{Z}} q^{y^2}, & \text{if } c_i = 0 \\ \sum_{y\in\mathbb{Z}} q^{\frac{1}{4}(1+2y)^2}, & \text{if } c_i = 1 \end{cases}$$
$$= \begin{cases} A, & \text{if } c_i = 0 \\ B, & \text{if } c_i = 1 \end{cases}$$

It follows that

$$\sum_{x\in\frac{1}{\sqrt{2}}\rho^{-1}(c)} q^{\frac{1}{2}(x\cdot x)} = A^{n-\mathrm{wt}(c)} B^{\mathrm{wt}(c)}$$

The rest follows by summing over all the codewords in C □

Example 3.4. For the extended Hamming code $\widetilde{H}$ the weight enumerator is of the form:

$$W_{\widetilde{H}}(X,Y) = X^8 + 14X^4Y^4 + Y^8$$

We know that the corresponding lattice $\Gamma_{\widetilde{H}}$ is E_8 . Thus it follows in consideration of proposition 1.8

$$\vartheta_{\Gamma_{\widetilde{H}}} = E_4 = A^8 + 14A^4B^4 + B^8$$

We are now able to prove the *MacWilliams identity*.

Theorem 3.5. Let $\mathrm{C} \subset \mathbb{F}_2^n$ be a binary (n,k,d)***-code*** . Then

$$W_{\mathrm{C}^\perp}(X,Y) = \frac{1}{2^k} W_{\mathrm{C}}(X+Y, X-Y)$$

Proof. We observe first that

$$\begin{aligned} W_{\mathrm{C}}(A(-\frac{1}{\tau}), B(-\frac{1}{\tau})) &= \vartheta_{\Gamma_{\mathrm{C}}}(-\frac{1}{\tau}) && \text{(by proposition 3.3)} \\ &= (\frac{\tau}{i})^{\frac{n}{2}} \frac{1}{2^{\frac{n}{2}-k}} \vartheta_{\Gamma^*_{\mathrm{C}}}(\tau) && \text{(by proposition 1.2)} \\ &= (\frac{\tau}{i})^{\frac{n}{2}} \frac{1}{2^{\frac{n}{2}-k}} \vartheta_{\Gamma_{\mathrm{C}^\perp}}(\tau) && \text{(by Lemma 1.10)} \\ &= (\frac{\tau}{i})^{\frac{n}{2}} \frac{1}{2^{\frac{n}{2}-k}} W_{\mathrm{C}^\perp}(A(\tau), B(\tau)) && \text{(by proposition 3.3)} \end{aligned}$$

Since the weight enumerator is a homogeneous polynomial, and by the transformation formula (3.0.4), (3.0.5). We obtain

$$W_{\mathrm{C}}(A(-\frac{1}{\tau}), B(-\frac{1}{\tau})) = (\frac{\tau}{i})^{\frac{n}{2}} \frac{1}{2^{\frac{n}{2}}} W_{\mathrm{C}}(A(\tau)+B(\tau), A(\tau)-B(\tau))$$

Thus

$$W_{\mathrm{C}^\perp}(A,B) = \frac{1}{2^k} W_{\mathrm{C}}(A+B, A-B)$$

We only need to prove that A and B are algebraically independent. But recall that from corollary 1.7, all the modular forms is generated by the E_4 and E_6 (as algebra). This implies that the modular form with weight divisable by 4 is generated by E_4 and Δ . But recall example 3.4 and proposition 3.2:

$$\begin{aligned} E_4 &= A^8 + 14A^4B^4 + B^8 \\ \Delta &= \frac{1}{16}A^4B^4(A^4 - B^4)^4 \end{aligned}$$

It follows that A and B are algebraically independent and we are done. □

Example 3.6. Let's now reexamine the example 1.13. We obtain the weight enumerator of H

$$W_H(X,Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + 1$$

Now we use *MacWilliams Identity* to caculate the weight enumerator of the dual code. We obtain

$$\begin{aligned} W_{H^\perp}(X,Y) &= \frac{1}{2^4}W_H(X+Y,X-Y) \\ &= X^7 + 7X^3Y^4 + Y^7 \end{aligned}$$

which is the exact result we obtained in the previous example

Corollary 3.7. If $\mathrm{C} \subset \mathbb{F}_2^n$ is a self-dual code, then

$$W_{\mathrm{C}}(X,Y) = W_{\mathrm{C}}(\frac{X+Y}{\sqrt{2}}, \frac{X-Y}{\sqrt{2}})$$

Proof. Since C is self-dual, it is a $(n, \frac{n}{2}, d)$***-code*** . Since C = $\mathrm{C}^\perp$, it follows by using *MacWilliams Identity*

$$\begin{aligned} W_{\mathrm{C}}(X,Y) &= \frac{1}{2^{\frac{n}{2}}} W_{\mathrm{C}}(X+Y,X-Y) \\ &= W_{\mathrm{C}}(\frac{X+Y}{\sqrt{2}}, \frac{X-Y}{\sqrt{2}}) \qquad (W_{\mathrm{C}}(X,Y) \text{ is homogen of degree n}) \end{aligned}$$

□

Another important theorem is the *Gleason Theorem*, which characterizes the *hamming weight enumerator* of a binary doubly self-dual even code.

Theorem 3.8. Let $\mathrm{C} \subset \mathbb{F}_2^n$ be a doubly even self-dual code. Then the *Hamming weight enumerator* $W_{\mathrm{C}}(X,Y)$ is a polynomial in

$$\phi := W_{\tilde{H}}(X,Y) = X^8 + 14X^4Y^4 + Y^8$$

and

$$\xi := X^4Y^4(X^4 - Y^4)^4$$

Proof. We consider the function $W_C(A,B)$, where A and B are defined in (3.0.1) and (3.0.2). We have seen in proposition 3.3, that

$$\vartheta_{\Gamma_C} = W_C(A,B)$$

Since C is doubly even and self-dual, it follows from proposition 1.9, that Γ_C is even and unimodular. The theorem 1.1 can be applied. We deduce that $W_C(A,B)$ is a modular form of weight $\frac{n}{2}$ and $\frac{n}{2} \equiv 0 \pmod 4$.
We have seen in the proof of theorem 3.5, that the algebra of modular form of weight divisable by 4 is generated as algebra by E_4 and Δ. Hence, $W_C(A,B)$ is generated by $A^4B^4\,(A^4-B^4)^4$ and $A^8+14A^4B^4+B^8$. Replace A and B as X and Y. □

Example 3.9. As an application of *Gleason Theorem*, we would like to calculate the *hamming weight enumerator* of the extended Golay code $\widetilde{\text{G}}$.
We have known from section 2, that $\widetilde{\text{G}}$ is self-dual and doubly even. So according to *Gleason Theorem*, $W_{\widetilde{G}}(X,Y) \in \mathbb{Z}[\phi,\rho]$ (since all the coefficients must be integer).
Since $W_{\widetilde{G}}(X,Y)$ is homogeneous of degree 24, and the leading coefficient of X^{24} is 1, it follows that:

$$W_{\widetilde{G}}(X,Y) = \phi^3 + k\cdot\xi, \qquad \text{for some k} \in \mathbb{Z}$$

To determine the value of k, we can make use of the fact that $A_4 = 0$ in $\widetilde{\text{G}}$. So it follows that

$$14\cdot 3 + k = 0 \quad \Rightarrow \quad k = -42$$

Thus, the *hamming weight enumerator* of $\widetilde{\text{G}}$ is

$$W_{\widetilde{G}}(X,Y) = (X^8 + 14X^4Y^4 + Y^8)^3 - 42X^4Y^4(X^4-Y^4)^4$$

4 Outlook

Now we want to pose the question that given a certain $n = 24m+8k$, $k = 0,1,2$ how much can we achieve such that given $C \subset \mathbb{F}_2^n$ be a doubly even self-dual code, the minimum distance is as large as possible.
With the help of theorem 3.8, the weight enumerator of C is given by

$$W_C = \sum_{j=0}^{m} b_j\,\phi^{3(m-j)+k}\,\xi^j, \qquad b_j \in \mathbb{C}$$

Now we can choose the coefficients of b_j, such that $A_{4l} = 0$, for $l = 1,\dots,m$ (it's possible, by solving m equations in m variables). Then the possibly non-zero coefficient A_{4m+4} is uniquely determined by b_j, which we denote by A^*_{4m+4} . The code with such property is called an *extremal code*. An extremal code has thus minimum distance at least $4m+4$. It can be shown that the minimum distance is $4m+4$ by showing that $A^*_{4m+4} \neq 0$ for all $m \geq 1$, details see chapter 19, section 5 of [3]
But this m cannot be large, since it is shown by Mallows, that for m sufficiently large, $n = 24m$

$$A^*_{4m+8} < 0$$

One knows that for $n \leq 64$, and some $n > 72$, there exists extremal doubly even self-dual code. It is still unknown whether this is true for $n = 72$.
There are also similar results for lattices. Let Γ be an even unimodular lattice in $\mathbb{R}^n$, $n = 24 + 8k$, $k = 0, 1, 2$. We know from the proof of theorem 3.5, that we can write the theta function of Γ as:

$$\vartheta_\Gamma = \sum_{j=0}^{m} b_j E_4^{3(m-j)+k} \Delta^j, \qquad b_j \in \mathbb{C}$$

With the analog argument, we can find coefficients, such that we can cancel all the first $2m + 1$ term up to the constant term, i.e.

$$\vartheta_\Gamma(\tau) = 1 + a^*_{2m+2} q^{2m+2} + \dots$$

Such lattice is called an *extremal lattice*. One can also show that m can not be too large. It is worth noting that our dear Prof. Nebe has proven in 2010 the existence of an extremal even unimodular lattice in $\mathbb{R}^{72}$

References

[1] W. Ebeling, “Lattices and codes,” in *Lattices and Codes*, pp. 53–66, Springer, 2013.

[2] S. Roman, *Coding and information theory*, vol. 134. Springer Science & Business Media, 1992.

[3] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, vol. 16. Elsevier, 1977.