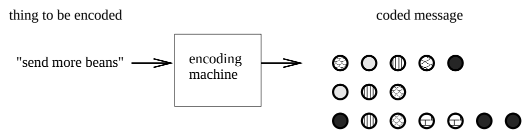


FIGURE 1. Sending a message

Lattices and Codes

1. Notation

A code will be given by a subspace C of $\mathbb{F}_2^n$ of allowed words.

The distance between two code words is the number of places they differ in.

The minimum distance of a code, d, is the minimum distance between two words of the code. A code can correct $\lceil (d-2)/n \rceil$ errors.

We call this an $[n, k, d]-$code. We want d big, and also k big.

The weight of a code word, $w(c)$ is its distance from $(0, 0, \ldots, 0)$.

The **weight enumerator** is a function that bundles up all the weights of the code into a polynomial, given by

$$W_c(X, Y) := \sum_{u \in C} X^{n-w(u)} Y^{w(u)}$$

$$= \sum_{u \in C} A_i X^{n-i} Y^i$$

where A_i is the number of codes of weight i

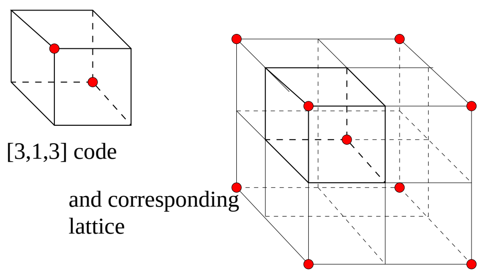


FIGURE 2. Part of lattice from a very simple code

Lattice	Code
Integral	$C \subset C^{\perp}$
Even	doubly even
Unimodular	self dual

TABLE 1. correspondence of properties in lattices and codes

For the Hamming code, we've got

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

for the extended Hamming code, we get:

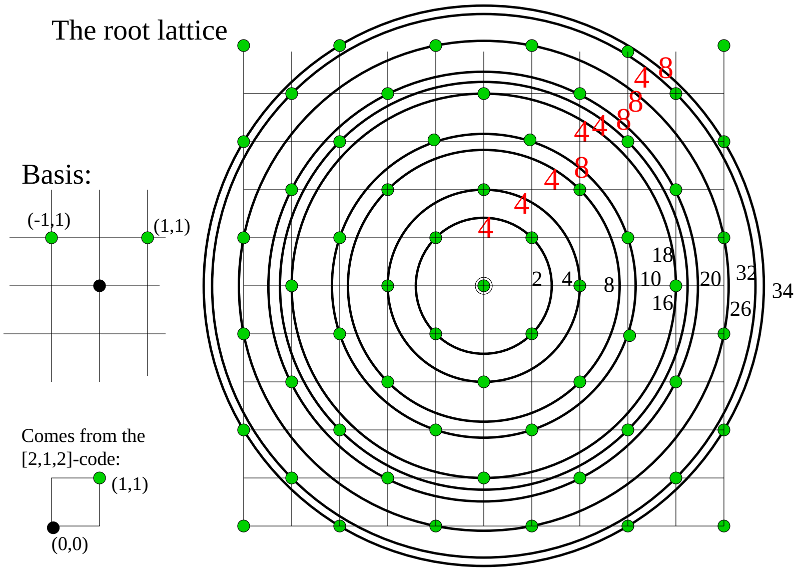
$$W_{\tilde{H}}(X,Y) = X^8 + 14X^4Y^4 + Y^8$$

2. How to get a lattice from a code

Define

$$\rho : \mathbb{Z}^n \to \mathbb{F}_2^n$$

$$\Gamma_C := \frac{1}{\sqrt{2}}\rho^{-1}(C)$$



$$\vartheta_\Gamma(q) = 1 + 4q^2 + 4q^4 + 4q^8 + 8q^{10} + 4q^{16} + 4q^{18} + 8q^{20} + 8q^{26} + 4q^{32} + 8q^{34} + ...$$

FIGURE 3. Example of a theta function

3. Theta functions

The theta function of a lattice is given by:

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

Where $q = exp(2\pi i\tau)$, $\tau \in \mathbb{H}$, the upper half plane.

This function is analogous to the weight enumeration polynomial.

For an even integral lattice,

$$\vartheta_\Gamma(\tau) = \sum_{x\in\Gamma} a_r q^r$$

where a_r is the number of vectors of length $2r$, so we're counting lattice points on a sphere radius $\sqrt{2r}$. So this tells us about the growth of the a_r, and that the sequence converges. See Figure 3.

THEOREM 3.1. *If Γ is an even unimodular lattice in $\mathbb{R}^n$, then $n \equiv 0$ mod(8), and the theta function $\vartheta_\Gamma(\tau)$ is a modular form of weight $\frac{n}{2}$.*

The Weight ennumerator tells us about the minimum distance of vectors in the code.

THEOREM 3.2. *if our code is in $\mathbb{F}^{24}$, then*
(1) $A_i = 0$ if $i \not\equiv 0(mod\ 4)$
(2) $A_8 = 759 - 4A_4$.

THEOREM 3.3. *(Mac Williams Identity) For a binary $[n, k, d]-$code $C \subset \mathbb{F}_2^n$,*

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

COROLLARY 3.4. *For a self dual code,*

$$W_C(X, Y) = W_C(\frac{X + Y}{\sqrt{2}}, \frac{X - Y}{\sqrt{2}}).$$

THEOREM 3.5. *(Gleason) If $C \subset \mathbb{F}_2^n$ is a doubly even self dual code, then $W_C(X, Y)$ is a polynomial in*

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

and

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

Now, if we want to get a big minimum distance, we would like to make $A_4 = 0$.

3.1. sketch proofs.

THEOREM 3.6. *The algebra of modular forms is isomorphic to the polynomial algebra*

$$\mathbb{C}[E_4, E_6]$$

Here E_4 is a modular form of weight 4 given by:

$$E_4(\tau) := \frac{1}{2\zeta(k)} \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(m\tau+n)^4}$$

and E_6 is a modular form of weight 6 given by:

$$E_6(\tau) := \frac{1}{2\zeta(k)} \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(m\tau+n)^6}$$

Another important modular form is the weight 12 modular form Δ, which is given by

$$\Delta(\tau) = 1728q\prod_{r=0}^{\infty}(1-q^r)^{24}.$$

Now we get going on the theorems about codes....
Theorem 3.1

PROOF. Assume that n is not divisible by 8. wlog $n \equiv 4 \mod 8$.

The idea is to show that

$$\vartheta(TS\tau) = -\tau^{n/2}\vartheta(\tau),$$

which gives

$$\vartheta((TS)^3\tau) = -\vartheta(\tau),$$

but $(TS)^3 = 1$, which gives a contradiction. $\square$

THEOREM 3.7. *ϑ is a modular form of weight 12; the space of modular forms of weight 12 is spanned by E_4^3 and E_6^2.*

COROLLARY 3.8. *for a weight 12 modular form $\sum a_i q^i$, we have*

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

Since the theta function for a unimodular lattice is a modular form of weight $n/2$, which is 12 in our case, and the coefficient of q^0 is 1, we have

$$a_2 = 196560 - 24a_1$$

for the theta function.

LEMMA 3.9. *For a self dual doubly even code,*

$$a_1 = 24.2 + 16A_4$$

and

$$a_2 = 2^8 + 16A_4.20.2 + \begin{pmatrix} 24 \\ 2 \end{pmatrix}.4$$

PROOF.

$$a_1 = \text{number of elements } x \in \Gamma_C \text{with} x.x = 2$$

$$a_2 = \text{number of elements } x \in \Gamma_C \text{with} x.x = 4$$

Figure 4 shows how the code gets repeated throughout $\mathbb{Z}^{24}/\sqrt{2}$ to give a lattice and shows how we get the above numbers □

From this we deduce Theorem 3.1
Next for Theorem 3.5

THEOREM 3.10. *The algebra of modular forms of weight divisible by 4 is generated by E_4 and Δ.*

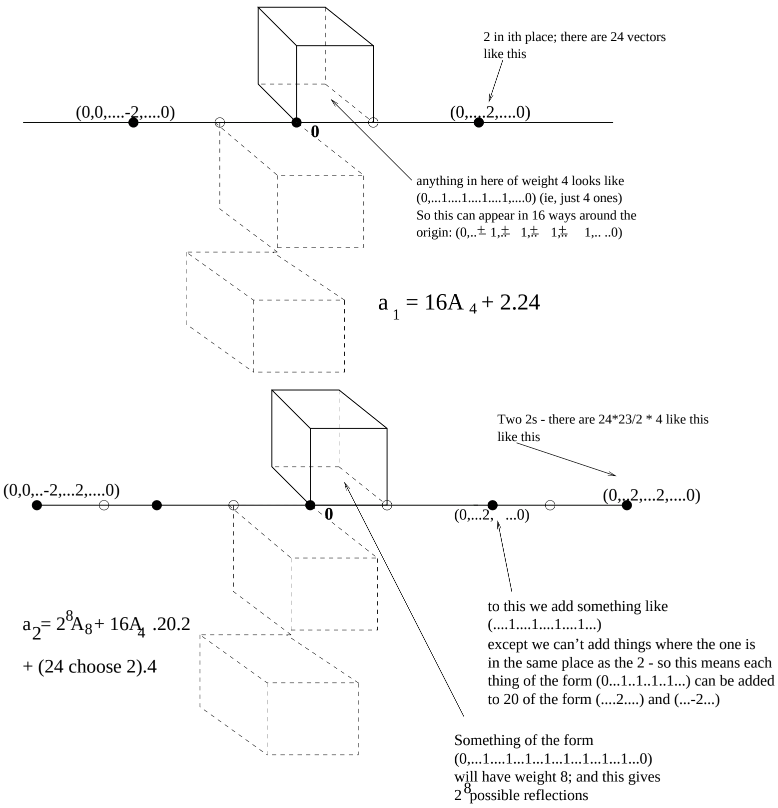


FIGURE 4. Where relations between a_i and A_i come from

The idea of the proof of Theorem 3.5 is to take some functions $A(\tau)$ and $B(\tau)$, and look at $W_C(A(\tau), B(\tau))$, and show that this function must be a modular form; but A and B have been chosen so that

$$E_4 = A^8 + 14A^4B^4 + B^8$$

and

$$\Delta = 172816A^4B^4(A^4 - B^4)^4.$$

From this we have the result.

A and B are given by

$$A(\tau) := \sum_{x \in \mathbb{Z}} q^{(x.x)}$$

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

I won't go through the proof that $W_C(A, B)$ is a modular form; I will go over a useful lemma that's important in the proof, and gives you an idea of how things go:

LEMMA 3.11. *We have*

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

PROOF. We have a map

$$\rho : \mathbb{Z}^n \to \mathbb{F}_2^n$$

remember that the lattice Γ_C is defined to be

$$\Gamma_C := \frac{1}{\sqrt{2}} \rho^{-1}(C)$$

and

$$\vartheta_{\Gamma_C}(\tau) = \sum_{x \in \Gamma_C} q^{\frac{1}{2} x.x}$$

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

Now we also have

$$\sum_{x \in \frac{1}{\sqrt{2}} \rho^{-1}(c)} q^{\frac{1}{2} x.x} = \sum_{x \in \rho^{-1}(c)} q^{\frac{1}{4} x.x} = \sum_{x \in \rho^{-1}(c)} q^{\frac{1}{4} x.x} = \sum_{x = (x_1, x_2, x_3, \ldots x_n) \in \rho^{-1}(c)} q^{\frac{1}{4} x.x}$$

$$= \sum_{x = (a_1 + 2N_1, a_2 + 2N_2, \ldots a_n + 2N_n), (a_1, a_2, a_3, \ldots a_n) \in (c)} q^{\frac{1}{4} x.x}$$

$$= \sum_{x = (a_1 + 2N_1, a_2 + 2N_2, \ldots a_n + 2N_n), (a_1, a_2, a_3, \ldots a_n) \in (c)} q^{\frac{1}{4}((a_1 + 2N_1)^2 + \cdots (a_n + 2N_n)^2}$$

$$= \sum_{N_i \in \mathbb{Z}, (a_1, a_2, a_3, \ldots a_n) \in (c)} \prod q^{\frac{1}{4}((a_i + 2N_i)^2}$$

$$= \prod_{a_i = 0} \sum_{N_i \in \mathbb{Z}} \prod q^{\frac{1}{4}((a_i + 2N_i)^2} \prod_{a_i \neq 0} \sum_{N_i \in \mathbb{Z}} \prod q^{\frac{1}{4}((a_i + 2N_i)^2}$$

$$= A^{n - w(c)} B^{w(c)}$$

$\square$

Now, if we want to get a big minimum distance, we would like to make $A_4 = 0$.

So, now we might set about looking for such a code... It turns out there is a unique doubly even linear code with $A_4 = 0$. This is called the Golay code. It's automorphism group is the finite simple group M_{24}. Wow! This group is a Mattieu group.

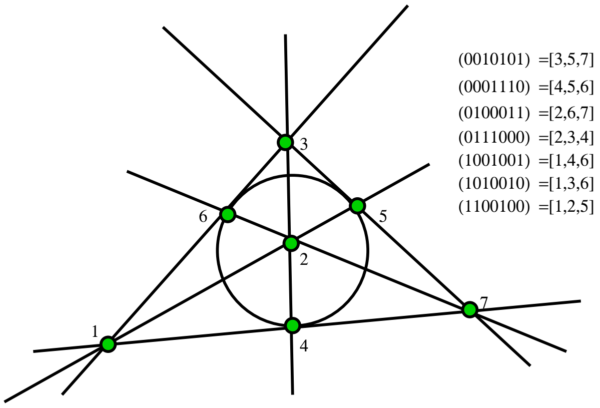


FIGURE 5. Steiner $S(2,3,7)$ system

4. Stiener Systems

After the above results about coding theory and number theory, we will go on to look at the automorphism groups of some of the very nicest codes; these are the automorphism groups of certain Stiener systems, and turn out to be examples of finite simple sporadic groups.

A Steiner system $S(l,m,n)$ is a collection of subets of size m in a set of size n such that any subset of size l is in exactly one of them.

The vectors of weight 4 in the extended Hamming code form a Steiner $S(2,3,7)$ system. See Figure 5.

THEOREM 4.1. *For a self dual doubly even code $\tilde{G}$ in $\mathbb{F}_2^{24}$, with $A_4 = 0$, the code words of weight* 8 *form a Steiner $S(5,8,24)$ system.*

PROOF. By the above theorem about th A_i, we know there are 759 vectors of weight 8; these can be veiwed as subsets of size 8 from a set of size 24.

Take a subset of size 5, eg, represented by

$$(1,1,1,1,1,\overbrace{0,0,\cdots,0,0}^{19 zeros}).$$

Suppose there are two codewords of weight 8 containing this subsequence:

$$c_1 = (1, 1, 1, 1, 1, \overbrace{0, 0, \cdots, 0, 0}^{16 zeros and 3 ones}).$$

$$c_2 = (1, 1, 1, 1, 1, \overbrace{0, 0, \cdots, 0, 0}^{16 zeros and 3 ones}).$$

Add these together to get

$$(0, 0, 0, 0, 0, *)$$

Here $*$ either could be something like

$$\begin{array}{rcccccc} & 0 & 0 & 0 & 1 & 1 & 1 \\ + & 1 & 1 & 1 & 0 & 0 & 0 \\ \hline & 1 & 1 & 1 & 1 & 1 & 1 \end{array}$$

$$\begin{array}{rccccc} & 0 & 0 & 1 & 1 & 1 \\ + & 1 & 1 & 1 & 0 & 0 \\ \hline & 1 & 1 & 0 & 1 & 1 \end{array}$$

$$\begin{array}{rcccc} & 0 & 1 & 1 & 1 \\ + & 1 & 1 & 1 & 0 \\ \hline & 1 & 0 & 0 & 1 \end{array}$$

$$\begin{array}{rccc} & 1 & 1 & 1 \\ + & 1 & 1 & 1 \\ \hline & 0 & 0 & 0 \end{array}$$

but none of these is weight divisible by 4, which is a constradiction.

So every subset of size 5 is in at most one of the code words.

But there are $\begin{pmatrix} 8 \\ 5 \end{pmatrix} = 56$ subsets of size 5 in a code of weight 8. This means that altogether $759 * 56$ different subsets of size 5 are contained in these weight 8 codes; but there are only $\begin{pmatrix} 24 \\ 5 \end{pmatrix} = 56 * 759 = 8 * 7 * 11 * 3 * 23$ subsets of size 5 altogether, so this is all of them. $\square$

The Mathieu group M_{24} is the automorphism group of $S(5,8,24)$. It has order $244,823,040$.

I'll just prove one result about this group:

Proposition 4.2. *The automorphism group of* $S(5,8,24)$ *acts transitively on the* 24 *co-ordinate positions.*

5. Glossary

Finite simple group: a group G with no normal subgroup

Normal subgroup: $H \leq G$, s.t $\forall g \in G$, $g^{-1}Hg \leq H$.

Lattice, Γ: $\Gamma = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \cdots \oplus \mathbb{Z}e_n \subset \mathbb{R}^n$, $\{e_i\}$ a basis of $\mathbb{R}^n$.

Integral lattice, Γ: $\forall x, y \in \Gamma$, $x.y \in \mathbb{Z}$.

Dual lattice, Γ: $\Gamma^* = \{x \in \mathbb{R}^n | x.y \in \mathbb{Z} \forall y \in \Gamma\}$

Unimodular lattice Γ: $\Gamma = \Gamma^*$.

even lattice Γ: $\forall x \in \Gamma, 2|x.x$.

Root vector $x \in \Gamma$: $x.x = 2$.

Root Lattice Γ: Γ is generated by it's roots.

Code of lenght n: $C \subset \mathbb{F}_q^n$.

Binary code of length n: $C \subset \mathbb{F}_2^n$. (We just cover this case today.)

distance between code words: number of places they differ.

Weight of a code word: Number of non zero entries.

Linear code: Linear subspace of ${\mathbb{F}_q}^n$

(n,M,d)-code: $C \subset \mathbb{F}_2^n$, $|C| = M$, min distance between code words is d.

[n,k,d]-code: $C \cong \mathbb{F}_2^k \subset \mathbb{F}_2^n$, minimum distance between code words is d.

Information rate: $R := \frac{log_2(M)}{n}$

modular form of weight k: A function $f(\tau)$, $\tau \in \mathbb{H}$, the upper half plane, with $f(\gamma\tau) = (c(\gamma, \tau))^k f(\tau)$, and $f(\tau)$ has an expansion in terms of $q = exp(2\pi i\tau)$. Here $c(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tau) = (c\tau + d)$.

Theta function of a lattice Γ, $\vartheta_\Gamma(\tau)$: $\vartheta_\Gamma(\tau) = \sum_{x \in \Gamma} q^{\frac{1}{2}x.x}, q = e^{2\pi i\tau}$

Steiner system, S(n,m,l): $(X, \mathcal{B})$, X a set, $|X| = n$, $\mathcal{B} \subset \mathcal{P}(X)$, $\forall U \in \mathcal{B}$, $|U| = m$; $\forall O \subset X, |O| = l \Rightarrow \exists! U \in \mathcal{B} \ni O \subset U$.