The binary Golay code and the Leech lattice

Recall from previous talks:

Def 1: (linear code)

A code C over a field *F* is called linear if the code contains any linear combinations of its codewords

A *k*-dimensional linear code of length *n* with minimal Hamming distance *d* is said to be an [n, k, d]-code.

Why are linear codes interesting?

- Error-correcting codes have a wide range of applications in telecommunication.
- A field where transmissions are particularly important is space probes, due to a combination of a harsh environment and cost restrictions.
- Linear codes were used for space-probes because they allowed for just-in-time encoding, as memory was error-prone and heavy.

Space-probe example

The Hamming weight enumerator

Def 2: (weight of a codeword)

The weight w(**u**) of a codeword **u** is the number of its nonzero coordinates.

Def 3: (Hamming weight enumerator)

The Hamming weight enumerator of C is the polynomial:

$$W_C(X,Y)=\sum_{i=0}^{n} A_i X^{n-i} Y^i$$

where A_i is the number of codeword of weight i.

Example (Example 2.1, [8])

For the binary Hamming code of length 7 the weight enumerator is given by:

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

Dual and doubly even codes

Def 4: (dual code)

For a code C we define the dual code C° to be the linear code of codewords orthogonal to all of C.

Def 5: (doubly even code)

A binary code C is called doubly even if the weights of all its codewords are divisible by 4.

The lattice $\Gamma_{\underline{C}}$

To any linear code C we can associate a lattice

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

where

$$\rho : \mathbb{Z}^n \longrightarrow (\mathbb{Z}/2\mathbb{Z})^n = \mathbb{F}_2^n.$$

is the canonical projection.

We can relate properties of a code to properties of its lattice:

Lemma 1: (Prop 1.3, [8])

Let C be a linear code.

- C is doubly even iff Γ_C is an even lattice.
- C is self-dual iff Γ_C is unimodular.

Lemma 2: (Theorem 2.1, [8])

Let Γ be an even unimodular lattice.

Then the dimension of Γ is divisible by 8.

Prop 1: (Prop 2.6, [8])

Let C be a self-dual doubly even code.

Then the length of C is divisible by 8.

Prop 2: (Prop 2.7, [8])

Let C be a self-dual doubly even code.

Then the weights of its Hamming weight enumerator satisfy

$$A_8 = 759 - 4A_4$$

A code satisfying these assumptions is the extended Golay code which we will construct later.

Cyclic codes

Def 6: (cyclic code)

A code C is called cyclic if for every codeword

$$\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$$

its cyclic shift

$$\mathbf{u_s} = (u_{n-1}, u_0, \ldots, u_{n-2})$$

is also a codeword in C.

It is useful to represent such a code C using polynomials in $F_n[x]$ (= $F[x]/(x^n - 1)$), i.e.

$\mathbf{u} = (u_0, u_1, \ldots, u_{n-1}) \rightarrow f(x) = u_0 + u_1 x + \ldots + u_{n-1} x^{n-1}$

A cyclic shift of the polynomial associated with the word **u** is then given by $xf(x)$.

Prop 2: (Theorem 46, [14])

A set of elements S in $F_n[x]$ corresponds to a cyclic code iff S is an ideal in $F_n[x]$

Theorem 1: (Theorem 47, [14])

Let C be an ideal in $F_n[x]$, and $g(x)$ the monic polynomial of smallest degree in C.

Then $g(x)$ is unique and C is generated by $g(x)$.

Prop 3: (Theorem 48, [14])

There is a 1 to 1 correspondence between divisors of $x^n - 1$ and ideals of $F_n[x]$.

Prop 4: (Theorem 49, [14])

If the degree of $g(x)$ is n – k, then the dimension of its corresponding code is k and the generator matrix of C is given by all the cyclic shifts of $g(x)$.

Example for n = 7

Factoring $x^n - 1$

Prop 5: (Theorem 45, [14])

Let α be a root of $x^n - 1$ in the smallest finite field *F* of characteristic p that contains α, and let *m(x)* be its minimal polynomial. Let β be a primitive nth root of unity in *F*, and let $\alpha = \beta^s$.

If u is the smallest element in the cyclotomic coset of n containing s, then

$$m(x) = \prod_{i \in C_u} (x - \beta^i)$$

Cyclotomic cosets for n = 23

Quadratic Residue Codes

For p, n primes and p a square mod n we can generate a cyclotomic coset by

$$J = \{ j : j \neq 0 \ is\ a\ square\ modulo\ n \}$$

We call the corresponding code a quadratic residue code.

Golay Codes

Def 6: (binary Golay code G_{23})

We call the binary quadratic residue code of length 23 the binary Golay code.

Def 7: (extended binary Golay code G_{24})

Based on G_{23} we define the extended binary Golay code as

$$G_{24}=\left\{\left(u_1,u_2,\ldots,u_{24}\right):\left(u_1,u_2,\ldots,u_{23}\right)\in G_{23},\ \sum_{i=1}^{24}u_i=0\right\}$$

Theorem 2: (Theorem 2.6 [8])

Let C be a binary (24,2^{12},8)-code containing 0.

Then C is a unique self-dual, doubly even code.

Def 8: (perfect code)

A (2,n,d)-code with d = 2e + 1 is called a perfect code if one of the following equivalent conditions holds:

1) Every x in F^n has distance ≤ e to exactly one codeword
2) $|C|(1+\binom{n}{1}+\ldots+\binom{n}{e})=2^n$

Proof **Theorem 2**

Proof **Theorem 2**

Proof **Theorem 2**

Proof **Theorem 2**

Recall:

Prop 2: (Prop 2.7, [8])

Let C be a self-dual doubly even code.

Then the weights of its Hamming weight enumerator satisfy

$$A_8 = 759 - 4A_4$$

The Golay code satisfies these assumptions and, since its minimum distance is 7, $A_4 = 0$.

Recall:

Def 9: A Steiner system S(t,k,v) is an assignment of a set S with v elements to blocks of size k s.t. each t-subset of S is contained in exactly one block.

Using the extended binary Golay code we can generate an S(5,8,24) Steiner system.

S(5,8,24)

The Leech lattice

Recall from “Construction B”: (Theorem 5.2, [8])

$$X = \left\{ x \in \mathbb{R}^n : x \pmod 2 \in C, \sum_{i=1}^{n} x_i \in 4\mathbb{Z} \right\}$$

Def 10: The Leech lattice is defined as the set

$$\Lambda_{24} = \frac{1}{\sqrt{2}} X \bigcup \left(\mathbf{u} + \frac{1}{\sqrt{2}} X \right)$$

where X is the set constructed above using G_{24} and

$$\mathbf{u} = \frac{1}{\sqrt{8}}(1,\ 1,\ \ldots,\ 1,\ -3)$$