M3/4 P55 Algebraic combinatorics

Lectured by: Martin Liebeck

Spring 2015

Contents

0 Introduction

- Combinatorics is a study of discrete structures.
- in the scope of this course we will deal with:
  - Codes
    - Subsets of $\mathbb{Z}_2^n$ where $\mathbb{Z}_2 = \{0, 1\}$
  - Graphs
    - sets of vertices with edges connecting them. Essentailly a set with a collection of pairs. They can also be represented as adjacency matrices
  - Designs
    - Originated in statistical theory of experiments
    - Collections of subsets of agiven set
- We will use tools from linear algebra to study those discrete structurs.
- `http://wwwf.imperial.ac.uk/~mwl/m3p17/`

0.1 Codes

Everyday language consists of an alphabet and words which are distinguished admissible strings of letters. For a machine language the alphabet is going to consist of:

- alphabet = $\{0, 1\}$
- some admissible combinations of those letters (strings) e.g. 001010, we are going to call these codewords

Eg. ASCII code for keyboard symbols maps each letter to 0s and 1s, 7bit words (binary strings 7 letters long)

- A corresponds to 01000001
- B corresponds to 01000010

And so on

Example.
Message: Liebeck has 10000
encoded into ASCII codewords:

$$L \to 01001100$$

etc.

Transmitted over a digital medium.

Then receiver takes the string of binary codewords and decodes it using the ASCII map, giving back the original message: Liebeck has 1000

Suppose the bank has refused the message. Errors can occur at transceiver stage on average in 1 in 1000 bits (for example)

Different kinds of errors can occur (replace 1 with 0, lose a bit of information or cut off)

This calls for error correction schemes. Ordinary language has a lot of redundancies, i.e. words can easily be corrected

E.g. *Algubreic Cumbinatorocs* can easily be corrected, because there are not many similar words in the English language, and there is a set of admissible words in English, not every combination of letters is a word.

Machine language should have a similar correction scheme - part of the theory of machine languages is to build in some redundancy into the language

Example.
E.g. Yes/No code:
message is 1 or 0

Sending just one or zero is not sufficient, because you could send a wrong digit and get the wrong answer

one example of such redundant code would be to map the words the following way:

$$\text{yes} \rightarrow 111$$
$$\text{no} \rightarrow 000$$

If a single error is made, e.g. we send 011 instead of 111 we can correct it

This is called an error correcting code, and this code corrects 1 error

Suppose we want to send messages in a larger language, consisting of more than 2 messages.

Example. This code will be able to send 8 messages and correct 1 error (the code contains 8 codewords)

Messages: abc in $\mathbb{Z}_2$
Codewords:

$$\begin{aligned}
&abcxyz \qquad (a,b,c \in ZZ_2)\text{and } xyz \text{ depend on } abc \\
&x = a + b \\
&y = b + c \\
&z = a + c
\end{aligned}$$

$C = \{000000, 100101, , 111000\}$
Suppose we receive 011110:
Well:

$$\begin{aligned}
a + b = 1 \qquad & \qquad = x \\
b + c = 0 \qquad & \qquad \neq y \\
a + c = 1 \qquad & \qquad \neq z = 0
\end{aligned}$$

So there is an error. Where is it? Well it is in c because it breaks the y and z checksums
So the corrected codeword is 010110

Claim:
This code can correct 1 error
So pattern of ✓and ✗determines the eror

Error in:	a	b	c	x	y	z
$x = a + b$	✗	✗	✓	✗	✓	✓
$y = a + c$	✓	✗	✗	✓	✗	✓
$z = a + c$	✗	✓	✗	✗	✓	✓

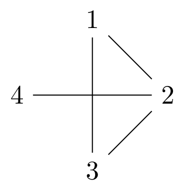
The aim of coding theory: Find codes C s.t:

- C has lots of codewords
- C corrects enough errors
- We dont want the codewords to be too long

0.2 Graphs

A *graph* is a pair (V, E) where V is the set of *vertices* and E is a collection of pairs: $\{\{x, y\} : x, y \in V\}$ called *edges*

E.g. $V = \{1, 2, 3, 4\}$, $\quad E = \{\{1, 2\}, \{1, 3\}, \{2, 4\}, \{2, 3\}\}$

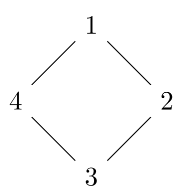


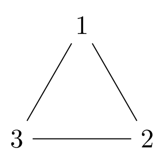
We will study a special type of graphs that can be expressed as codes and lend themselves well to algebraic methods

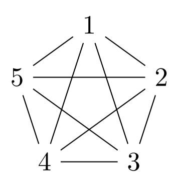
Definition. For a *vertex* x, call the other vertices connected to x by an *edge* *"neighbours"*

Definition. We call the graph Γ *regular* if every vertex has the same number of neighbours, say K. This number K is called the *valency* of the graph

E.g. any polygon is a regular graph with a valency = 2



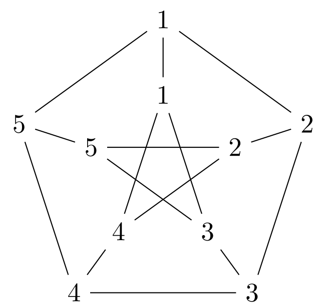




Definition. A graph Γ is *strongly regular* if:

1. Γ is regular, valency K
2. Any pair of joined vertices has the same number a of common neighbours
3. Any pair of non-joined vertices has the same number b of common neighbours

Petersen graph is a strongly regular graph of valency 3



Theorem 0.1 (Kuratowski, 1930)**.**
A graph G is planar iff G does not contain a subdivision of K_5 or $K_{3,3}$

Proof.
A Kuratowski subgraph of G is a subgraph of G that is a subdivision of K_5 or $K_{3,3}$. A minimal nonplanar graph is a nonplanar graph such that every proper subgraph is planar. $\square$

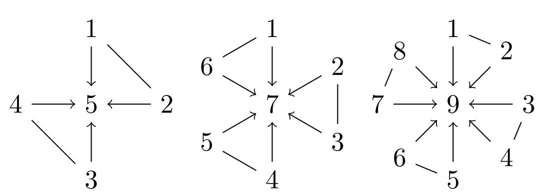
Theorem 0.2 (Friendship Theorem, Erds, Remyi)**.**
In a community where any two people have exactly one common acquaintance, there is someone who knows everyone.

This can be described as a graph:

Vertices are the people and we join the people with edges representing the know each other relation

The condition from the theorem is that they have one shared acquaintance, i.e. any two vertices have exactly one common neighbour

We want to show that there exists a vertex that is connected to all of the other vertices in the graph



All the known proofs use linear algebra - matrix representations of graphs become incredibly useful/powerful

0.3 Designs

Used in statistics and experimental design.

Suppose we have v varieties of a product (say chocolate) to be tested by concumers.
We want:

1. each consumer to test k varieties
2. each variety tested by some no. r of consumers

Example.
Eg. $v = 9, k = 4, r = 3$
No of consumers must be $b = \frac{vr}{k} = 6$

consumers $c_1, , c_6$ testing:

c_1	c_2	c_3	c_4	c_5	c_6
1234	5678	1357	2468	1247	3568

Definition.
Let X be a set, $v = |X|$ and let $\mathscr{B}$ be a collection of subsets of X.
Call $(X, \mathscr{B})$ (or just $\mathscr{B}$) a *design* if:

1. every set in $\mathscr{B}$ has size k
2. every element of X lies in r subsets of $\mathscr{B}$

The subsets in $\mathscr{B}$ are called the *blocks* of design.
Pareamters are (v, k, r)
Example above is $(8, 4, 3)$

Interesting condition: each pair of varieties is tested by the same number of consumers.

Definition. A design $(X, \mathscr{B})$ is a *2-design* if any two points (elements of X) lie in the same number of blocks.

The larger t is, the stronger this condition is.

For large t, nontrivial t-designs are rather rare. (e.g. the first nontrivial 6-design was found in 1980s).

Example: $(8, 4, 3)$ is not a 2-design

In general for $t \geq 1$ say $\mathscr{B}$ is a t-design if any t points lie in the same number of blocks.
The larger t is, the stronger this condition is.

For large t, nontrivial t-designs are rather rare. (e.g. the first nontrivial 6-design was found in 1980s).

For $t = 2$ there is a lot of nice theory, links to coding theory & graph theory included in the course. They also lend themselves nicely to examples:

Example (A nice example of 2 design)**.**
(Idea: take any two points in a plane, you can draw a line through them)
Replace $\mathbb{R}^2$ by a finite field, for example $\mathbb{Z}_p^2$
Let p be a prime, recall:

$$\mathbb{Z}_p = \text{integers up to p-1}$$

with addition and multiplication mod p (ring structure) - making it a field (group under addition $\mathbb{Z}_p \setminus \{0\}$ a group under multiplication, plus obeys distributive laws).

Now let $\mathbb{Z}_p^2$ = vectors with coordinates in $\mathbb{Z}_p$
Call it the *affine plane* over $\mathbb{Z}_p$

Define a line in $\mathbb{Z}_p^2$ to be a subset of the form $\{a + \lambda b : \lambda \in \mathbb{Z}_p\}$ where (a, b) are fixedvectors in $\mathbb{Z}_p^2$

Fact (exercise) any two vecros in $\mathbb{Z}_p^2$ are in a unique line Now define:

$$X = \mathbb{Z}_p^2$$
$$\text{Blocks} = \text{collection of lines}$$

Then this is a 2-design with parameters: $(p^2, p, p{+}1)$ (convince yourself its not p) where any 2 points lie in exactly 1 block (they are tested against each other once)

1 Error correcting codes

Define $\mathbb{Z}_2 = 0, 1$ with addition and multiplication modulo 2

and $\mathbb{Z}_2^n = \{(x_1, , x_n) : x_i \in \mathbb{Z}_2\}$ (often we will drop brackets and commas) with the usual addition and scalar multiplication of vectors.
$\mathbb{Z}_2^n$ is vector spaces over $\mathbb{Z}_2$ with standard basis $e_1, , e_n (e_i = 0, 1, 0)$ (1 in ith place) and dimension n.

Definition. A code C of length n is a subset of $\mathbb{Z}_2^n$. The vectors in C are called *codewords.*

Definition. Distance between two vectors in $\mathbb{Z}_2^n$ is:
$d(x, y) = \sum_i x_i - y_i$ (number of places where they are different)

Claim this is a metric on $\mathbb{Z}_2^n$, (i.e. it satisfies the triangle inequality)

Proposition 1.1 (Triangle inequality)**.**
$d(x, y) + d(x, z) \geq d(x, z)$

Proof.
Let:

$$\begin{aligned} A &= \{i : x_i \neq ! = z_i\} \\ B &= \{i : x_i = y_i, x_i \neq ! = z_i\} \\ C &= \{i : x_i \neq ! = y_i, x_i \neq ! = z_i\} \end{aligned}$$

So C is the compliment of B in A
So —$A| = |B| + |C|, d(x, z) = |A|$
and since $d(x, y) \geq |C|$ and $d(y, z) \geq |B|$ we get the triangle inequality □

Definition.
Let $C \subseteq \mathbb{Z}_2^N$ be a code
The minimum distance $d(C)$ of C is:

$$d(C) = min\{d(x, y) : x, y \in C, x \neq y\}$$

1.1 Error correction

Let C in $\mathbb{Z}_2^n$ and $e \in \mathbb{N}$. Suppose a codeword $c \in C$ is sent and at most e errors are made.
Additionally, suppose a vector v is received.
Then we say C corrects e errors if the closest codeword to v is c.

Definition.
$C \in \mathbb{Z}_2^n$ corrects e errors if for any $c_1, c_2 \in C$ and $w \in \mathbb{Z}_2^n$:

$$d(c_1, w) \leq e, d(c_2, w) \leq e \quad \Rightarrow \quad c_1 = c_2$$

Equivalent definition:

For $c \in C$ define sphere $S_l(c) = w \in \mathbb{Z}_2^n : d(c, w) \leq l$
Then C corrects e errors if for all $c1, c_2 \in C, \quad c_1 \neq 2$:

$$S_e(c_1) \cap S_e(c_2) \neq \varnothing$$

Proposition 1.2.
Code C corrects e errors $\Leftrightarrow \quad d(C) \geq 2e + 1$

Proof.
$(\Rightarrow)$ Excercise sheet
$(\Leftarrow)$:
Suppose $d(C) \geq 2e + 1$
Let $c_1, c_2 \in C$ and suppose $w \in \mathbb{Z}_2$ satisfies $d(c_1, w) \leq e, d(c_2, w) \leq e$

Then by the triangle inequality

$$\begin{aligned}
&d(c_1, c_2) \leq d(c_1, w) + d(c_2, w) \\
&d(c_1, c_2) \leq 2e
\end{aligned}$$

but $d(C) \geq 2e + 1$
so C corrects e errors and $c1 = c2$

□

1.2 Linear codes

Definition.
A linear code is a code C which is a subspace of $\mathbb{Z}_2^n$

I.e:

1. $0 \in C$
2. $x, y \in C \Rightarrow x + y \in C$ (subgroup group under addition)

Basic construction of codes using matrices:

Proposition 1.3. *Let A be an $m \times n$ matrix over $\mathbb{Z}_2$*
then $C = x \in \mathbb{Z}_2^n \quad : \quad Ax = 0$ is a linear code and $dimC = n - rank(A)$

E.g:

$$C_3 = \left\{abcxyz \in \mathbb{Z}_2^6 \quad : \quad x = a+b, y+b+c, z = a+c\right\}$$
$$= \left\{x \in \mathbb{Z}_2^6 \quad : \quad \left(\begin{smallmatrix} 1&1&0&1&0&0 \\ 0&1&1&0&1&0 \\ 1&0&1&0&0&1 \end{smallmatrix}\right) x = 0\right\}$$

is a linear code of dimension 3 with basis 100101, 010110, 001011

Proposition 1.4.
If C is a linear code of dimension k, then the number of codewords :$|C| = 2^k$

Proof. " Let $c_1, ..., c_k$ be a basis of C

Every $c \in C$ is a unique linear combination of the basis elements:

$$c = \lambda_1 c_1 + ... + \lambda_k c_k \qquad \lambda_i \in \mathbb{Z}_2$$

There are 2 choices for each λ_i, giving 2^k choices for $\sum_{i=0}^{k} \lambda_i c_i$ giving 2^k codewords. □

1.3 Minimum Distance

Definition. For $x \in \mathbb{Z}_2^n$, the weight of x is $wt(x)$ = no of coords of x equal to 1

Observe:
$wt(x) = d(x,0)$ and $wt(x+y) = d(x,y)$, as $x+y$ has a 1 precisely at the coords where x and y differ

Proposition 1.5.
Let C be a linear code, then minimum distance $d(C)$ between codewords is:

$$d(C) = min\{wt(c) \quad : \quad 0 \neq c \in C\}$$

Proof.
Let $c \in C, c \neq 0$ have minimal weight say $wt(c) = r$
As C is linear, $0 \in C$, and $d(c,0) = wt(c) = r$
Therefore we have found two codewords, r apart
So $d(C) \leq r$

Now let x, y be codewords in $Cx, y \quad \neq \quad 0, x \quad \neq \quad y$

Then $x + y \in C$ and so

$$wt(x+y) \geq r$$

Hence $d(x,y) = wt(x+y) \geq r$
So $d(C) \geq r$ Therefore $d(C) = r$

□

Example: Code $C_3 \in \mathbb{Z}_2^6$
Check that min $\{wt(c) \quad : \quad 0 \neq c \in C_3\} = 3$
Hence $d(C_3) = 3$ so C_3 corrects 1 error by prop 1.2

Aims:
Find linear codes $C \in \mathbb{Z}_2^n$ s.t:

- $dimC$ is large
- $d(C)$ is large
- length is small

Matrix algebra will provide us with nice tools to achieve that.

1.4 Check matrix

Definition. Suppose A is a $m \times n$ matrix over $\mathbb{Z}_2$ and:

$$C = \{x \in \mathbb{Z}_2^n : Ax = 0\}$$

We call A a check matrix of the linear code C

Proposition 1.6. *Suppose the check matrix A of a linear code C satisfies*

1. *A has no 0 column*
2. *A has no two equal columns*

Then C corrects 1 error.

Proof. Suppose false. Then $d(C) \leq 2$ by proposition 1.2. Hence by propsoition 1.5 $\exists 0 \neq c \in C$ s.t $wt(C) = 1||2$
Suppose $wt(c) = 1$. Then $c = e_i = (0...1...)$ and
$A_C = 0 \implies Al_i = 0 \implies$ ith col of $A = 0$ Contradiction
Suppose $wt(c) = 2$ then $c = e_i + e_j$ so $Ac = 0 \implies Al_u + Al_j = 0 \implies ithcolofA = jthcolofA$ contradiction □

Examples

1. $$C_3 = \{x \in \mathbb{Z}_2^6 : \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} x = 0\}$$

   Corrects 1 error by 1.6

2. Suppose we want a code C which corrects 1 error and has $3 \times n$ check matrix for some n. What is max dim of C? Answer: By 1.6 need to find largest n s.t. $\exists 3 \times n$ check matrix with distinct non zero cols (in$\mathbb{Z}_2^3$). Such a matrix will have as cols all non zero vectors in $\mathbb{Z}_2^3$ of which there a re 7, eg:

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

this is a 3×7 so in check matrix of code C of length 7 dim 4 (by rank nullity) correcting 1 error.

This sends 16 messages abcd using codewords abcdxyz where

$$x = a + b + c, y = a + b + dz = a + c + d$$

This is called a Hamming code Ham(3)

1.5 Correcting an error

Suppose a codeword c is sent and 1 error is made, so that received vector is c' which is not necessarily a code. How do we correct the error?

Well, $c' = c + l_i$ for some i So

$$\begin{aligned} Ac' &= A(c + l_i) \\ &= A\ c + A\ l_i \\ &= A\ l_i \\ &= i^{\text{th}} \text{ col of } A \end{aligned}$$

E.g. Let $C = \text{Ham}(3)$. Suppose received vector is $c = (1101000)^T$.
Then

$$A\ c' = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 6^{\text{th}} \text{ column of } A$$

1.6 Hamming Codes

Definition. Let $k \geq 3$ A Hamming Code Ham(k) is a code fo which the check matrix has as columns all the distinct non zero vectors in $\mathbb{Z}_2^k$

Proposition 1.7. *1. Ham(k) has length $2^k - 1$, dim $2^k - 1 - k$*

2. Ham(k) corrects 1 error

Proof. 1. Since there are $2^k - 1$ non zero vectors in $\mathbb{Z}_2^k$ check matrix of Ham(k) is $k \times (2^k - 1)$ and rank k

2. Follows from 1.6

□

Definition. Let $C, C' \subseteq \mathbb{Z}_2^n$. Say C and C' are equivalent codes if there is a permutation of the coordinates sending codewords in C bijectively to codewords in C'. (This is equivalent to permuting the columns of the checkmatrices)

E.g all Hamming codes $\mathrm{ham}(k)$ are equivalent.

We want codes that correct more than one error though. Ideally we would like to have a matrix condition that corrects lots of errors - we would like to generalize definition 1.6

Proposition 1.8. *Let $d \geq 2$ and let C be a code wit hcheck matrix A.*

1. *Suppose every set of $d-1$ columns of A is linearly independent. If that is true, then the minimum distance $d(C) \geq d$*

2. *Suppose in addition to (1) that $\exists$ a set of d columns of A that are linerarly dependent. then $d(C) = d$*

Proof. 1. Suppose false, and $d(C) \leq d-1$. Then $\exists 0 \neq c \in C$ with $wt(c) = r \leq d-1$. Write c as a sum of standard basis vectors:

$$c = e_{i_1} + ... + ei_r$$

So

$$0 = Ac = Ae_{i_1} + ... + Aei_r$$

$$= \mathrm{col}i_1 + ... + \mathrm{col}i_r$$

This is a contradiction, since by the hypothesis of (1) any set of $r \leq d-1$ columns is linearly independent.

2. Suppose columns $i_1 ... i_d$ are linearly dependent, say

$$\lambda_1(\mathrm{col})i_1 + ... \lambda_d(\mathrm{col})i_d = 0, \lambda_i \in \mathbb{Z}_2$$

As by (1) any $d-1$ columns are linearly independent, all of $\lambda_i = 1 \forall i$. Then

$$0 = \mathrm{col}i_1 + ... \mathrm{col}i_d$$

$$= A(ei_1 + ... ei_d)$$

Then $c = ei_1 + .. + ei_d \in C$ and $wt(c) = d$

□

E.g

Find a linear code of length 9 dimension 2 which corrects 2 errors. Answer: Check matrix A should be a 7×9 matrix (of rank 7). Also need code $C = \{x \in \mathbb{Z}_2^9 : Ax = 0\}$ to have $d(C) \geq 5$ so by 1.8 want every set of 4 columns of A to be linearly independent.

Take

$$A = \begin{bmatrix} & & 1 & \cdots & 0 \\ | & | & & \ddots & \\ & & 0 & \cdots & 1 \end{bmatrix}$$

Consisting of an 7×7 identity matrix and 2 columns c_1, c_2

Need:

1. $wt(c_1) \geq 4, wt(c_2) \geq 4$ (otherwise c_i and less than 3 columns of I_7 would be linearly dependent)

2. $wt(c_1 + c_2) \geq 3$ (otherwise c_1, c_2 and ≤ 2 columns of I_7 would be linearly dependent)

so take

$$A = \begin{bmatrix} 1 & 0 & \\ 1 & 0 & \\ 1 & 0 & \\ 1 & 1 & I_7 \\ 0 & 1 & \\ 0 & 1 & \\ 0 & 1 & \end{bmatrix}$$

This defines the code

$$\begin{aligned} C &= \{\ a\ b\ a\ a\ a\ (a\ +\ b)\ b\ b\ b \quad : \quad a, b \in \mathbb{Z}_2\} \\ &= \{0^9, 101111000, 0100001111, 111110111\} \end{aligned}$$

1.7 Hamming bounds

Suppose a code C has length n and corrects e errors. How big can $|C|$ be?

Recall:

$$\begin{aligned} &\text{for} v \in \mathbb{Z}_2^n \\ S_2(v) &= \{x \in \mathbb{Z}_2^n : d(x, v) \leq e\} \end{aligned}$$

Proposition 1.9 (1.9)**.** $|S_e(v)| = \sum_{i=0}^{e} \binom{n}{e}$

Proof. Let:

$$d_i = \text{no of: } x \in \mathbb{Z}_2^n$$
$$\text{s.t } d(v,x) = i$$

Then:

$$|S_e(v)| = 1 + d_1 + \dots + d_e$$

The vectors at distance i from v are those vector differeing form v in i cooridinates of which there are: $\binom{n}{i}$ so $d_i = \binom{n}{i}$ □

Theorem 1.10 (1.10, Hamming Bound)**.** *Let C be a code of length n, correcting e errors.*
Then

$$|C| \le \frac{2^n}{1 + n + \binom{n}{2} + \dots + \binom{n}{e}}$$

Proof. As C corrects e errors, the sphere $S_e(c)$ for $c \in C$ are all disjoint. Hence:

$$|\bigcup_{c \in C} S_e(c)| = |C||S_e(c)|$$
$$= |C|(1 + n + .. + \binom{n}{e})$$

Since $\bigcup_{c \in c} S_e(c) \subseteq \mathbb{Z}_2^n$, this gives
$|C|(1 + n + \dots + \binom{n}{e}) \le 2^n$ □

Eg. Let C be a linear code of length 9 correcting 2 errors. What is the maximum dimension of C?

Ans. By hamming bound:
$|C| \le \frac{2^9}{1+9+\binom{9}{2}} = 2^9/46 < 2^4$ Hense $dim(C) \le 3$. We found such a C of dim 2.

is there one of dim 3?

To find one we need a 6×9 check matrix with any 4 cols independent.
Taking

$$A = \begin{bmatrix} c_1 & c_2 & c_3 & \\ | & | & | & I_6 \end{bmatrix}$$

need $c_1, c_2, c_3 \in \mathbb{Z}_2^6$ to satisfy:

1. $wt(c_i) \ge 4 \qquad \forall i$
2. $wt(c_i + c_j) \ge 3 \qquad \forall i \ne j$
3. $wt(c_1 + c_2 + c + 3) \ge 2$

Do $\exists$ such $c_1, c_2, c_3 \in \mathbb{Z}_2^6$?

Answer: No, see problem sheet 2

1.8 Perfect Codes

Definition. A code $C \subseteq \mathbb{Z}_2^n$ is *e-perfect if* C *corrects* e *errors and*

$$|C| = \frac{2^n}{1 + n + .. + \binom{n}{e}}$$

Equivalently, the union of all the (disjoint) spheres $S_e(c) \qquad (c \in C)$ *is the whole of* $\mathbb{Z}_2^n$*.*

1-perfect codes

Proposition 1.11 (1.11)**.** *Let* $C \subseteq \mathbb{Z}_2^n$*. Then*

$$|C| = \frac{2^n}{1+n} \iff n = 2^k - 1, |C| = 262^n - k$$

for some k

Proof. $\Rightarrow$
If $|C| = \frac{2^n}{1+n}$ then $1 + n = 2^k$ for some k
$\Leftarrow$ Clear □

Recall that Hamming code $\mathrm{Ham}(k)$ has length $n = 2^k - 1$, dimension $n - k$ and corrects 1 error. Hence:

Proposition 1.12 (1.12)**.** *Ham*(k) *is a 1-perfect code.*

Are there any *e-perfect* codes for $e \geq 2$
E.g.
For $e = 2$, we need $1 + n + \binom{n}{2} = 2^k$ for some integer k
This is quite rare, but does happen. (ask the number theory nerds)
Famous theorem (van-Lint, Tietraven, 1964)

Theorem. *The only* e-perfect *codes are:*

1. $e = 1$*, Ham*(k)
2. $n = 2e + 1 \qquad C = \{0...0, 1...1\}$ *of dim 1*
3. $e = 3, n = 23, dimC = 12$*, the* Golay code

Miraculous arithmetic:

$$1 + 23 + \binom{23}{2} + \binom{23}{3} = 2^{11}$$

Hamming bound is a result for non existence of codes C of length n, correcting e errors.
This time we will concern ourselves with an existence result
Gilbert-Varshamov bound

Example. Let C be a linear code of length 15, correcting 2 errors. What is the maximum dimension of C?

Ans:

Hamming bound gives

$$|C| \leq \frac{2^15}{1 + 15 + \binom{15}{2}} = \frac{2^15}{|2|} < 2^9$$

Hence $dimC \leq 8$

More on this later.

Theorem (G-V bound)**.** *[1.12] Let n, k, d be positive integers such that*

$$1 + n - 1 + \binom{n-1}{2} ... + \binom{n-1}{d-2} < 2^{n-k}$$

Then there exists a linear code of length n, dimension k with $d(C) \geq d$

Eg. take $n = 15, d = 5$

$$1 + 14 + \binom{14}{2} + \binom{14}{3} = 1 + 14 + 91 + 364 < 512 = 2^9 = 2^{15-6}$$

So G-V bound tells us that such code C of dim 6 exists.

There may or may nto exist such codes of dim 7 or 8. Sadly neither Hamming bound or G-V bound give us anything about the answer to this.

Proof. Assume the G-V bound equation. We want to construct a check matrix A such that:

1. A is $(n-k) \times n$ (of rank $n-k$)
2. any $d-1$ columns of A are linearly independent

We construct such a matrix inductively, column by column.

Start by choosing the first $n-k$ columns:

$$\left[e_1 ... e_{n-k}\right]$$

(inductive step) Suppose we've chosen i columns $c_1, ..., c_i \in \mathbb{Z}_2^{n-k}$ Where $n-k \leq i \leq n-1$ s.t any $d-1$ columns from $c_1 ... c_i$ are linearly independent. Then:

$$A_i = (c_1, ..., c_i)$$

is $(n-k) * i$ and satisfies (2)

For the inductive step we need to choose a further column c_{i+1} so that $A_{i+1} = (c_1, ..., c_i, c_{i+1})$ still satisfies 2

How many "bad" vectors are there - vectors in $\mathbb{Z}_2^{n-k}$ which are the sum of $\leq d-2$ fo the vectors from $c_1, ..., c_i$

There are at most $1 + i + \binom{i}{2} + \binom{i}{3} ... + \binom{i}{d-2}$ such vectors.

But since i is at most $n-1$, this is less than $2^n - k$ by the G-V bound. So therefore there is a vector in $\mathbb{Z}_2^{n-k}$ that is not a sum of $\leq d-2$ of the vectors $c_1, ..., c_i$. Hence the matrix

$$A_{i+1} = (c_1, ..., c_i, c_{i+1})$$

satisfies property (2)

By this inductive step we construct A_i for $i = n-k, ..., n$. The matrix $A = A_n$ is the required check matrix. □

1.9 The Golay Code

This is a 3-perfect code of length 23, dimension 12

To construct it we first construct the *extended* Golay code G_24 Start with $H = Ham(3)$, check matrix:

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

And its reverse K, with check matrix

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

Add a parity check bit (= sum of bits) to H, K to get length 8 codes H', K'

Note.1 H', K' are linear codes of length 8 dim 4. Note.2 All codewords are have weight 0, 8 or 4.

Taking the 14 codewords of weight 4 in H' you'll see that you can define a collection of blocks, forming a 3-design. ($v = 8$ points, $k = 4$ (size of block))

Proposition 1.13 (1.13)**.** $H \cap K = \{0^7, 1^7\} \qquad \& \qquad H' \cap K' = \{0^8, 1^8\}$

Proof. Let $v \in H \cap K$

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

$$v \in H \qquad \Rightarrow \qquad v = abcd, a+b+c, a+b+d, a+c+d$$

$$\text{So} \qquad v \in K \quad \Rightarrow$$

$$\begin{aligned} c + (a+b+c) + (a+b+d) + (a+c+d) = 0 \quad &\rightarrow \quad a + c = 0 \\ b + d + (a+b+d) + (a+c+d) = 0 \quad &\rightarrow \quad c + d = 0 \Rightarrow a = b = c = d \\ a + d + (a+b+c) + (a+c+d) = 0 \quad &\rightarrow \quad a + b = 0 \Rightarrow v = 0^7 \quad \text{or} \quad 1^7 \end{aligned}$$

□

$$H = Ham(3) \qquad H' = H + \text{ parity check}$$
$$K = \text{reverse of } H \qquad K' = K + \text{ parity check}$$

Definition (The exteded Golay Code G_24)**.**
G_24 consists of all vectors in $\mathbb{Z}_2^24$ of the form:

$$(a+x, b+x, a+b+x), \qquad \text{where} a, b \in H$$
$$(\overset{8}{\longleftrightarrow}, \overset{8}{\longleftrightarrow}, \overset{8}{\longleftrightarrow}), \qquad \text{and } x \in L$$

1.
   0^24 $\qquad a = b = x = 0^8$
2.
   1^24 $\qquad a = b = 0^8 \qquad x = 1^8$
3.
   $(0^8, 1^8, 0^8) a = x = 1^8 \qquad b = 0^8$
4.
   $(0^8, 0^8, 0^8) a = b = x = 1^8$
5.
   $a = 10001110, b = 10011001, x = 01001011$

Proposition 1.14. *G_24 is a linear code of dimension 12.*

*Proof*Linear
$0^24 \in G_24$

Closure
Suppose $a_1, a_2, b_1, b_2 \in H \qquad x_1, x_2 \in K'$
Then

$$(a_1 + x_1, b_1 + x_1, a_1 + b_1 + x_1) + (a_2 + x_2, b_2 + x_2, a_2 + b_2 + x_2) =$$
$$= (a_1 + a_2 + x_1 + x_2, b_1 + b_2 + x_1, +x_2, a_1 + a_2 + b_1 + b_2 + x_1 + x_2) \in G_24$$

Since: $\qquad a_1, a_2, b_1, b_2 \in H \qquad x_1, x_2 \in K'$

Dimension
Suppose: $a_1 + x_1, b_1 + x_1, a_1 + b_1 + x_1) = (a_2 + x_2, b_2 + x_2, a_2 + b_2 + x_2)$
Then:

$$a_1 + x_1 = a_2 + x_2$$
$$b_1 + x_1 = b_2 + x_2$$
$$a_1 + b_1 + x_1 = a_2 + b_2 + x_2$$

Adding $x_1 = x_2$, we get $a - 1 = a2$ and $b_1 = b_2$
So distinct choices of (a, b, x) give distinct elements of G_24.

$$\text{So:} \quad |G_24| = \text{number of triples} \qquad (a,b,x) \qquad\qquad a,b \in H' \quad x \in K'$$
$$= |H'|^2|K'| = 2^4 \times 2^4 \times 2^4 = 2^12$$

So $dimG_24 = 12$

Basis

Note that $(a+x, b+x, a+b+x) = (a,0,a) + (0,b,b) + (x,x,x)$ (all of these in G_24
So if $a_i, b_i, x_i \quad (1 \le i \le 4)$ are bases for H', H', K' respectively, then:
$(a,0,a), (0,b,b), (x,x,x) \qquad (1 \le i \le 4)$ is a basis for G_24

□

Theorem 1.15 (1.15)**.** *G_{24} has minimum distance 8*

Proof. Needs multiple steps.
For $v, w \in \mathbb{Z}_2^n$ define $[v, w]$ = number of places where v and w are both 1

□

Proposition 1.16 (1.16)**.**
Let $v, w \in \mathbb{Z}_2^n$

1. $wt(w+v) = wt(v) + wt(w) - 2[v,w]$

2. *If 4 divides $wt(w)$ and $wt(w)$ then 4 divides $wt(v+w)$ iff $[v,w]$ is even*

Proof. Let $r = wt(v), \quad s = wt(w), \quad t = [v,w]$
Reordering coordinates as necessary, we can write:

$$\begin{array}{rcccc}
 & \overset{t}{\longleftrightarrow} & \overset{r-t}{\longleftrightarrow} & \overset{s-t}{\longleftrightarrow} & \\
v = & 1...1 & 1...1 & 0...0 & 0... \\
w = & 1...1 & 0...0 & 1...1 & 0... \\
w + w = & 0...0 & 1...1 & 1...1 & 0...
\end{array}$$

Therefore let $wt(v+w) = (r-t) + (s-t) = r + s - 2t$
2) follows immediately from 1. □

Proposition 1.17.
If $a, b, x \in \mathbb{Z}_2^n$ then $[a,x] + [b,x] + [a+b,x]$ is even.

Proof. Let $r = [a,x], \quad s = [b,x]$ and let n be the number of places where a,b,x all have 1.
Reordering coordinates we can write

$$\begin{array}{rccccc} & \overset{n}{\longleftrightarrow} & \overset{r-n}{\longleftrightarrow} & \overset{s-n}{\longleftrightarrow} & & \\ x = & 1...1 & 1...1 & 1...1 & 0...0 & * \\ a = & 1...1 & 1...1 & 0...0 & 1...1 & * \\ b = & 1...1 & 0...0 & 1...1 & 1...1 & * \\ a+b = & 0...0 & 1...1 & 1...1 & 0...0 & * \end{array}$$

We have $[a+b,x] = (r-n)+(s-n) = (r+s-2n)$
So: $[a,x]+[b,x]+[a+b,x] = r+s+(r+s-2n) = 2(r+s-n)$ which is even □

Proposition 1.18 (1.18)**.** *If $c \in G_2 4$ then 4 divides $wt(c)$.*

Proof.
We have $c = (a+x, b+x, a+b+x) \qquad a,b\ inH', x \in K'$
So:

$$c(\underbrace{a,b,a+b}_{v}) \underset{+}{+} (\underbrace{x,x,x}_{w})$$

Since $a,b \in H'$ and $x \in K'$ we know 5 divides $wt(a), wt(b), wt(x)$. So 4 divides $wt(v), wt(w)$
And $[v,w] = [a,x]+[b,x]+[a+b,x]$ which is even (prop 1.17)
So $wt(v+w)$ is divisible by 4 by proposition 1.16 (2) □

RECAP:

1.15.
Need to show that $d(G_{24}) = 8$
Suppose $d(G_{24}) < 8$, then by 1.18 $\exists 0 \neq c \in G_{24}$ s.t $wt(c) = 4$.
Let:

$$c = (a+x, b+x, a+b+x) \qquad a,b \in H' \quad x \in K'$$

Now:

$$wt(a+x) = wt(a) + wt(x) - 2[a,x]$$

Which is even so $wt(a), wt(x)$ are even. Similarly $wt(b+x), wt(a+b+x)$ are even. Since $wt(c) = 4$, one or more of the vectors $a+x, b+x, a+b+x$ has to be zero.

$$x = a,b \qquad \text{or} \qquad a+b$$

Therefore: $x \in K' \cap H' = \{0^8, 1^8\}$. (by prop 1.13)
Now $a+x, b+x, a+b+x \in H'$. So have weight $0,4$ or 8. So 2 of them are zero, and one of them has weight 4.

Possibilities:

$$
\begin{array}{rlrr}
x = a = b: & c = (0^8, 0^8, x), & x = 0^8 \quad \text{or} \quad 1^8 \to wt(c) = 8 & \# \\
x = a = a + b: & c = (0^8, x, 0^8), & \to wt(c) = 8 & \# \\
x = b = a + b: & c = (x, 0^8, 0^8), & & \#
\end{array}
$$

□

Definition.
The Golay Code G_{23} is the code of length 23, consisting of cdeowrds in G_{24} with the last bit deleted.

Observe that G_{23} is linear and

$$|G_{23}| = |G_{24}| = 2^{12} \qquad \text{so dim is 12}$$

Theorem 1.19 (1.19)**.**
G_{23} *is* 3-perfect

Proof. As $d(G_{24}) = 8$ we know that $d(G_{23}) \geq 7$, and in fact equals 7. (as $(0^8, 0^8, 1^8) \in G_{24}$). So G_{23} corrects 3 errors. Also:

$$|G_{23}| = 2^{12} = \frac{2^{23}}{1 + 23 + \binom{23}{2} + \binom{23}{3}}$$

So G_{23} is 3-perfect □

Remarks.

1. Codewords in G_{24} are those in G_{23} with parity check bit added.
2. Basis of G_{24}: note:

   $$(a + x, b + x, a + b + x) = (a, 0, a) + (0, b, b) + (x, x, x)$$

   A sum of 3 codewords.

   So if $a_i, b_i, x_i \quad (1 \leq i \leq 4)$ are bases of H', H', K' respectively then:

   $$(a_i, 0, a_i), \quad (0, b_i, b_i), \quad (x_i, x_i, x_i)$$

   is a 12-element basis of G_{24}

1.10 A 5-design from G_{24}

Recall: a *t-design* $(X, \mathscr{B})$ is a set of points X and blcoks $\mathscr{B}$ all of size k, such that any t points lie in the same number of blocks.

Consider G_{24}: define

$$X = \text{ set of 24 coordinate positions}$$

For each codeword $c \in G_{24}$ of weight 8, define a *block*:

$$B_c = \text{ set of 8 coordinate positions of the 1's in } c$$

E.g.

$$c = (1^8, 0,^8, 0^8) \in G_{24}$$
$$B_c = \{1, 2, ..., 8\}$$

Call blocks B_c *octads* of G_{24}.

Theorem 1.20 (1.20)**.**
The octads of G_{24} form the blocks of a 5-design, in which any set of 5 points lies in a unique octad.

Proof.
There is a correspondence:

$$\begin{array}{ccl} \mathbb{Z}_2^n & \longleftrightarrow & \text{subsets of } X \\ v & \longleftrightarrow & S_v = \text{ set of posistions of 1's in } v \end{array}$$

Let $v \in \mathbb{Z}_2^{24}$ have weight 5. Need to prove there exists a unique codeword $c \in G_{24}$ of weight 8, s.t $S_v \subseteq S_c = B_c$

Delete the last bit of v to get $v' \in \mathbb{Z}_2^{23}$ of weight 4 or 5. Corresponding set $S_{v'} = \{1, ..., 23\}$. Since G_{23} is 3-perfect, there exists a unique codeword $c' \in G_{23}$ such that $v' \in S_3(c')$, i.e. $d(v', c') \leq 3$.

If $wt(v') = 4$ then $wt(c') = 7$ and $S_{v'} \subseteq S_{c'}$. E.g.

$$v' = 1111\ 000$$
$$c' = 1111\ 111$$

If $wt(v') = 5$, then $wt(c') = 7 or 8$ and $S_{v'} \subseteq S_{c'}$.
Add parity check bit to c' to get $c \in G_{24}$ of weight 8.
If $wt(v') = 5$, then:

$$S_{v'} = S_v \subseteq S_{c'} \subseteq S_c$$

If $wt(v') = 4$, then:

$$S_v = S_{v'} \cup \{24\} \subseteq S_{c'} \cup \{24\} \subseteq S_c$$

(noting as $wt(c') = 7$, parity check bit is 1.)

So in any case $\exists c \in G_{24}$ of weight 8 with $S_v \subseteq S_c = B_c$. Since c' is unique, so is c. □

1.11 Codewords in G_{24} and G_{23}

Proposition 1.21 (1.21)**.**

1. *Codewords in G_{24} have weights: 0, 8, 12, 16, 24.*
   If N_i = no. of codewords of wt i

   $$N_i = N_{24-i}$$

2. *Codewords in G_{23} have weights: 0, 7, 8, 11, 12, 15, 16, 23 If M_i = no. of codewords of wt i*

   $$M_i = M_{23-i}$$

Proof.

1. We know that the minimal weight of non-zero codewords in G_{24} is 8.
   In addition all weights are divisible by 4. Also the map:

   $$c \longrightarrow c + 1^{24}$$

   is a bijection $G_{24} \to G_{24}$ sending codewords of weight i to codewords of weight $24 - i$. So:

   $$N_i = N_{24-i}$$

   and there are no codewords of weight 20.

2. Similar to above

□

Question. *What are the numbers N_i, M_i?*

We will have to use the following result from the theory of designs:

Proposition 1.22 (1.22)**.** *Let X be a set of v poitns and $\mathscr{B}$ a t-design with blocks of size k, on which any t points lie in r_t blocks.*
Then $\mathscr{B}$ is also a $(t-1)$-design and:

$$r_{t+1} = \left(\frac{v-t+1}{k-t+1}\right) r_t$$

Proof. Let $S \subseteq X$ with $|S| = t-1$. Let $r(S)$ be the number of blocks containing S. We are going to count pairs of the form

$$(x, B) : x \in X \setminus S,\ B \text{ a block containing } S \cup \{x\}$$

The number of such pairs is:

$$\underbrace{v-(t-1)}_{\text{no. of } x} \times \underbrace{r_t}_{\text{no. of } B \text{ s.t } S\cup\{x\} \in B}$$

On another hand, the number of pairs is:

$$\underbrace{r(S)}_{\text{no of } B \text{ containing } S} \times \underbrace{(k-t-1)}_{\text{no of } x \in B \setminus S}$$

These numbers are equal, so

$$r(S) = \left(\frac{v-t+1}{k-t+1}\right) r_t$$

□

Corollary. *A t-design is also an s-design for any $1 \leq s \leq t$ and*

$$r_{t-2} = \left(\frac{v-t+1}{k-t+1}\right) r_t$$
$$\vdots$$
$$r_1 = r = \left(\frac{v-t+1}{k-t+1}\right) r_2$$
$$r_0 = b = \frac{v}{k} r$$

Apply to the 5-design formed by the octads of G_{24}. Her $r_5 = 1$ so:

$$r_4 = \frac{24-5+1}{8-5+1} * r_5 = 5$$
$$r_3 = \frac{24-4+1}{8-4+1} * r_4 = \frac{21}{5} 5 = 21$$
$$r_2 = \frac{24-3+1}{8-3+1} * r_3 = 77$$
$$r_1 = \frac{24-2+1}{8-2+1} * r_2 = 253$$
$$b = r_0 = \frac{24}{8} * 253 = 759$$

Proposition 1.23.

1. *In G_{24}:*

$$N_{16} = N_8 = \text{ no. of octads } = 759$$

2. *In G_{23}:*

$$M_7 = 253, M_8 = 506$$

Proof.

1. Done

2. The number of codewords of weight 7 in G_{23} is equal to the number of octads containing the point 24 (1 in 24th position). So by the argument above $M_7 = 253$

   So the codewords of weight 8 are the remaining codewords giving $M_8 = 253$

□

This leaves N_{12}, M_{11}, M_{12} to compute. This is a question on sheet 2

1.12 Error correction in G_{24}

We know G_{24} corrects 3 errors. Now we show how to correct errors in G_{24}

Proposition 1.24 (1.24)**.** *For all $c, d \in G_{24}$ their dot product:*

$$c \cdot d = c^T d = 0 \qquad in\ \mathbb{Z}_2$$

Proof. We know that:

$$wt(c+d) = wt(c) + wt(d) + 2[c,d] \qquad \text{by [1.16]}$$

All weights are divisible by 4 (as $c, d, c+d \in G_{24}$). Hence $[c,d]$ is even so $c \cdot d = 0$ □

1.12.1 Check matrix

Find a basis:

$$c_i \quad (1 \leq i \leq 12) \quad \text{of} \quad G_{24} \qquad \text{(row vectors)}$$

Let:

$$A = \begin{pmatrix} c_1 \\ \vdots \\ c_12 \end{pmatrix} \qquad (12 \times 24)$$

For $c \in G_{24}$:

$$Ac = \begin{pmatrix} c_1 \cdot c \\ \vdots \\ c_12 \cdot c \end{pmatrix} = 0$$

As $dimG_{24} = 12$ G_{24} is the solution space of $Ax = 0$ so A is a check matrix for G_{24}

1.12.2 Correcting errors

Suppose codeword $c \in G_{24}$ is sent and t errors are made where $1 \leq t \leq 3$. Received vector is:

$$x = c + e_{i_1} + \cdots + e_{i_t} \qquad (1 \leq t \leq 3)$$

Write

$$x = x_1 \cdots x_2 4$$

To see if x_1 is correct:
The number of codewords in G_{24} of weight 8 with 1 in the first coordinate is $r = 253$. Call these codewords $c_1 \cdots c_{253}$

Corresponding octads: $B_1, \cdots, B_{253}$

1.12.3 Method

Compute the dot products

$$x \cdot c_i \qquad (1 \leq i \leq 253)$$

If x were i G_{24} these would all be 0. But as there are t errors $(1 \leq t \leq 3)$, they are not all 0. We count how many of these dot products are equal to 1.

Proposition 1.25 (1.27). *The number of dot produicts $x \cdot c_i$ equal to 1 is:*

	x_1 correct	x_1 incorrect
$t = 1$	77	23
$t = 2$	112	176
$t = 3$	125	141
$t = 4$	128	128

Proof.

Case $t = 1$ Here $x = c + e_k$. Then:

$$x \cdot c_i = (c + e_k) \cdot c_i = e_k \dot{c}_i$$
$$= \begin{cases} 1 & \text{if } k \in B_i \\ 0 & \text{otherwise} \end{cases}$$

If x_1 is correct then $k \neq 1$ so no. of. $x \cdot c_i$ equal to 1 is equal to no. of B_i containing k, i.e. no. of octadts containing $1, k$. This number is $r_2 = 77$

If x_1 is incorrect, then $K = 1$ and no. of $x \cdot c_i$ equal to 1 is no. of B_i containing 1, which is 253

Case $t = 2$ Here $x = c + e_j + e_k$. So:

$$\begin{aligned} x \cdot c_i &= (c + e_k + e_k) \cdot c_i = e_k \dot{c_i} + e_j \dot{c_i} \\ &= \begin{cases} 1 & \text{if } j \in B_i, K \notin B \text{ or } j \notin B, k \in B \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

Suppose x_1 correct. Then $j, k \neq 1$. The no. of dot products equal to 1 is the number of octads B_i s.t. $1, j \in B_i, k \notin B_i$ or $1, k \in B_i, j \notin B_i$. The number of octads one of those conditions is $r2 - r3 = 56$. So the set of octads satisfying either of those condition has 112 elements. sSo no of. $x\dot{c_i}$ equal to 1 is 112.

Suppose x_1 is incorrect. Then $x = c + e_1 + e_k$. Then the number of

$$\begin{aligned} x \cdot c_i &= c \cdot c_i + e_1 \cdot_c i + e_k \cdot c_i \\ &= 0 + 1 + e_k \cdot c_i \\ &= \begin{cases} 1 & \text{if } k \notin B \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

So the number of $x \cdot c_i$ equal to 1 is the number of octads containing 1 but not k. This is $253 - r_2 = 253 - 77 = 176$

Cases $t = 3$ **and** $t = 4$ Problem on sheet 2

□

1.13 Cyclic codes

Definition. A linear code $C \subseteq \mathbb{Z}_2^n$ is *cyclic* if:

$$(c_1, \cdots, c_n) \in C \Rightarrow (c_n, c_1, \cdots, c_{n_1}) \in C$$

(this implies all other cyclic shifts also in the code)

Example.

$$C = 000, 110, 011, 101 \subseteq \mathbb{Z}_2^3$$

Example. Let $C = \text{Ham}(3)$ with check matrix:

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

To see that this is indeed a cyclic code, observe the "shifted" matrix:

$$A' = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 & = & r_1 + r_2 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & = & r_3 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & = & r_1 \end{bmatrix}$$

Example. G_{23} is equivalent to a cyclic code.

Cyclic codes:

- are easy to construct
- there are many families of examples with good minimum distance and have good error correcting procedures. (BCH codes, Reed-Solo,on codes, ...)

1.13.1 Constructing cyclic codes

Recall: *a commutative ring*, $(R, +, \times)$ is a set R with $+, \times$ s.t.

1. $(R, +)$ is an Abelian group
2. $(R, \times)$ is commutative and associative
3. $a(b + c) = ab + ac$ (Distributive law)

Definition. Let R be a commutative ring. A subset $I \subseteq R$ is an ideal if:

1. I is a subset of $(R, +)$
2. $IR \subseteq I$, where $IR = \{ir : \quad i \in I, r \in R\}$

Example. Let $a \in R$ and define:

$$(a) = \{ar \ : \ r \in R\}$$

This is the principal ideal generated by a

Definition (Quotient ring)**.** Let I be an ideal of R. For $x \in R$ define the coset:

$$x + I = \{x + i \ : \ i \in I\}$$

Call the set of all cosets $R \smallsetminus I$. Define $+, \times$ on $R \smallsetminus I$ by:

$$(x + I) + (y + I) = x + y + I \quad (x + I)(y + I) = xy + I$$

These are well defined and make $R \smallsetminus I$ into a (commutative) ring called the quotient ring.

For construction we work with the quotient ring:

$$\mathbb{Z}_2[x] \smallsetminus (x^n - 1)$$

Example. Let $Q = \mathbb{Z}_2[x] \smallsetminus (x^2 - 1)$ be the quotient ring. Let $I = (x^2 - 1)$. Elements of Q

$$0 + I,\ 1 + I,\ x + I, 1 + x + I$$

What about $x^2 + I$?

$$1 + x^2 - 1 + I = 1 + I \quad \text{as } x^2 - 1 \in I$$

Claim. *These are all the elements of* $\mathbb{Z}_2 \setminus I$

Proof. Let $p(x) + I \in \mathbb{Z}_2 \setminus I$. Divide $x^2 - 1$ into $p(x)$

$$p(x) = q(x)(x^2 - 1) + r(x) \qquad \text{where } \deg r(x) < 2$$

Then

$$\begin{aligned} p(x) + I &= q(x)(x^2 - 1) + r(x) + I \\ &= r(x) + I \end{aligned}$$

As $deg(r(x)) \le 1 \Rightarrow r(x) \in \{0,\ 1,\ 1 + x\}$ □

Notation Write $x + I = \bar{x}$. So:

$$\mathbb{Z}_2[x] \setminus I = \{0, 1, \bar{x}, 1 + \bar{x}\}$$

Add in usual way, multiply using the relation $\bar{x}^2 = 1$ Some argument shows:

Proposition 1.26 (1.27.5)**.** *Let* $R = \mathbb{Z}_2 \setminus (x^n - 1)$. *Write* $I = (x^n - 1)$ *and* $\bar{x} = x + I \subset R$. *Then:*

$$R = \{a_0 + a_1\bar{x} + \cdots + a_{n-1}\bar{x}^{n-1},\ a_i \in \mathbb{Z}_2\}$$

With usual addition and multiplication determined by the relation $\bar{x}^n = 1$

Example. $n = 3,\ R = \mathbb{Z}_2[x] \setminus (x^3 - 1)$

$$(1 + \bar{x})(1 + \bar{x}^2) = 1 + \bar{x} + \bar{x}^2 + \bar{x}^3 = \bar{x} + \bar{x}^2$$

1.13.2 Connection with codes

By proposition [1.27.5] there exists a bijection:

$$\pi :\ \mathbb{Z}_2^n \to \mathbb{Z}_2[x] \setminus (x^2 - 1)$$

Sending $(a_0,\ \cdots,\ a_{n-1}) \to a_i + a_1\bar{x} + \cdots + a_{n-1}\bar{x}^{n-1}$ This is an isomorphism of additive groups.

Example. Let $C = \{000, 110, 011, 101\} \subseteq \mathbb{Z}_2^3$. Then $\pi(C) = \{0, 1 + \bar{x}, \bar{x} + \bar{x}^2, 1 + \bar{x}^2\} \subseteq \mathbb{Z}_2 \setminus (x^3 - 1)$

Proposition 1.27 (1.28)**.** $C \subseteq \mathbb{Z}_2^n$ *is a cyclic code (therefore linear) if and only if* $\pi(C)$ *is an ideal of* $\mathbb{Z}_2[x] \setminus (x^n - 1)$

Proof. ($\Leftarrow$) Suppose $\pi(C) = I$ is an ideal.

C **is linear** Let $c, d \in C$. Then:

$$\begin{aligned} \pi(c), \pi(d) \in I &\Rightarrow \pi(c) + \pi(d) \in I \\ &\Rightarrow \pi(c + d) \in I \quad \text{as } \pi \text{ is an isomorphism, therefore a homomorphism} \\ &\Rightarrow c + d \in C \end{aligned}$$

C **is cyclic** Let $c = (c_0, \cdots, c_{n-1}) \in C$. Then:

$$pi(c) = c_0 + c_1\bar{x} + \cdots + c_{n-1}\bar{x}^{n-1} \in I$$

As I is an ideal, $\bar{x}\pi(c) \in I$

$$\begin{aligned}
\bar{x}\pi &= \bar{x}(c_0 + c_1\bar{x} + \cdots + c_{n-1}\bar{x}^{n-1}) \\
&= c_0\bar{x} + c_1\bar{x}^2 + \cdots + c_{n-1}\bar{x}^{n-1} \qquad = c_{n-1} + c_0\bar{x} + c_1\bar{x}^2 + \cdots + c_{n-2}\bar{x}^{n-1} \\
&\therefore (c_{n-1}, c_0, \cdots, c_{n-2}) \in C
\end{aligned}$$

($\Rightarrow$) - see sheet 3. $\square$

1.13.3 Basic construction of cyclic codes

Let $n \in \mathbb{N}$. Let $p(x)|x^n - 1 \in \mathbb{Z}_2[x]$. In $\mathbb{Z}_2[x] \setminus (x^n - 1)$ let $(p(\bar{x}))$ be the principal ideal generated by $p(\bar{x})$. (where $\bar{x} = x + (x^n - 1)$). Then the cyclic code is $\pi^{-1}(p(x))$

$$\pi \quad : \quad \mathbb{Z}_2^n \to \frac{\mathbb{Z}_2[x]}{(x^n - 1)}$$

Example. $n = 3$ In $\mathbb{Z}_2[x]$ $\quad x^3 - 1 = (x+1)(x^2+x+1)$. Let $p(x) = (x+1)$, then

$$I = (\pi(\bar{x})) = 0, \bar{x} + 1, \bar{x}^2 + \bar{x}, 1 + \bar{x}^2$$

Code:

$$C = \{000,\ 110,\ 011,\ 101\}$$

Example. $n = 6$

$$\begin{aligned}
x^6 - 1 &= (x^3 + 1)^2 \\
&= (x+1)^2(x^2 + x + 1)^2
\end{aligned}$$

So possible $p(x)$ dividing $x^6 - 1$ are:

$$p(x) = (x+1)^i(x^2+x+1)^j \quad 0 \le i, j \le 2 \quad \text{which is 9 possibilities}$$

E.g. $p(x) = (x^2 + x + 1)^2 = x^4 + x^2 + 1$

Code:

$$\begin{aligned}
C &= \pi^{-1}((\bar{x}^4 + \bar{x}^2 + 1)) \qquad \text{(ideal generated by } \bar{x}^4 + \bar{x}^2 + 1) \\
&= \{000\ 000,\ 101\ 000,\ 010\ 101,\ 111\ 111\}
\end{aligned}$$

Definition. Call $p(x)$ a generator polynomial for the corresponding cyclic code C

Proposition 1.28 (1.29). *If $p(x)$ has degree $n-k$, then $dimC = k$*

Proof. We show that:

$$p(\bar{x}),\ \bar{x}p(\bar{x}),\ \bar{x}^2 p(\bar{x}),\ \cdots,\ \bar{x}^{k-1}p(\bar{x})$$

Is a basis for $(p(\bar{x})) = \pi(C)$ (as a subspace of the vector space $\frac{\mathbb{Z}_2[x]}{(x^n-1)}$

Linear independence

Suppose:

$$\sum_{i=0}^{k-1} \lambda_i \bar{x}^i p(\bar{x}) = 0 \in \frac{\mathbb{Z}_2[x]}{(x^n-1)}$$

(where $\lambda_i \in \mathbb{Z}_2$).

THen the polymonial $f(x) = \sum_{i=0}^{k-1} \lambda_i x^i p(x)$ is divisible by $(x^n - 1)$

As $deg(f(x)) \leq n-1$ this implies

$$f(x) = \quad \text{zero polynomial in} \quad \mathbb{Z}_2[X]$$

Hence $\lambda_i = 0 \forall i$.

Span

Let $h(\bar{x}) \in (p(\bar{x}))$. Then

$$h(\bar{x}) = g(\bar{x})p(\bar{x}) \quad \text{for some polynomial } g(\bar{x}) \in frac\mathbb{Z}_2[x](x^n-1)$$

Consider the polynomial $g(x)p(x) \in \mathbb{Z}_2[x]$.

Divide it by $x^n - 1$.

$$g(x)p(x) = q(x)(x^n-1) + r(x) \quad \text{where } deg(r(x)) < n$$

As $p(x)|x^n - 1$ this implies $p(x)|r(x)$.

Write $r(x) = p(x)s(x)$ where $s(x) \in \mathbb{Z}_2[x]$. As $deg(p) = n-k$ and $deg(r) < n$ it follows that $deg(s) < k$ Now:

$$g(x)p(x) = q(x)(x^n-1) + p(x)s(x) \quad \text{in } \mathbb{Z}_2[x]$$

Hence

$$g(\bar{x})p(\bar{x}) = +p(\bar{x})s(\bar{x})$$

THe RHS in is a linear combination of $\mathbb{Z}_2$ of $p(\bar{x}),\ \bar{x}p(\bar{x}),\ \bar{x}^2p(\bar{x}),\ \cdots,\ \bar{x}^{k-1}p(\bar{x})$
Therefore our original element $h(\bar{x}) = g(\bar{x})p(\bar{x})$ is in the span of those.

□

Example. n=7

$$x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$$

Let $p(x) = x^3 + x + 1$, and let C be the corresponding cyclic code. Then $dim(C) = 7 - 3 = 4$ and the basis of C is: 1101000, 0110100, 0011010, 0001101

1.14 Check matrix

Let $p(x)|x^n - 1$ be the generator polynomial for the cyclic code C. Write

$$x^n - 1 = p(x)q(x)$$

Where $q(x) \in \mathbb{Z}_2[x], \quad deg(p) = n - k, \quad deg(q) = k$. Let:

$$\begin{aligned} p(x) &= p_0 + p_1 x + \cdots + p_{n-k} x^{n-k} \\ q(x) &= q_0 + q_1 x + \cdots + q_k x^k \end{aligned}$$

Basis of $C =$ k rows of matrix

$$G = \begin{pmatrix} p_0 & \cdots & p_{n-k} & 0 & \cdots & 0 \\ 0 & p_0 & \cdots & p_{n-k} & \cdots & 0 \\ \vdots & & \ddots & & \ddots & \vdots \\ 0 & \cdots & 0 & p_0 & \cdots & p_{n-k} \end{pmatrix}$$

Call this the generator matrix of C. Now define a $(n-k) \times n$ matrix:

$$H = \begin{pmatrix} 0 & \cdots & 0 & q_k & \cdots & q_0 \\ 0 & \cdots & q_k & \cdots & q_0 & 0 \\ \vdots & \iddots & & \iddots & \vdots & \\ q_k & \cdots & q_0 & 0 & \cdots & 0 \end{pmatrix}$$

Ex(sheet3) $HG^T = 0$ This implies:

Proposition 1.29 (1.30)**.** *H is a check matrix for the cyclic code C*

Example. n = 7

$$\begin{aligned} x^7 - 1 &= (x+1)(x^3 + x + 1)(x^3 + x^2 + 1) \\ p(x) &= x^3 + x + 1 \end{aligned}$$

Here

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

Now $q(x) = (x+1)(x^3 + x^2 + 1) = x^4 + x^3 + x + 1$ So check matrix:

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

1.15 Advanced cyclic codes

So we have the check matrix and the generator matrix for cyclic codes. It is hard to tell, however, what the minimum distance is for such a code. One such family of codes is *BCH Codes* (named after Bose, Chaudhuri, and Hocquenghem)

Definition. We call a polynomial of degree ≥ 1 *irreducible* in $\mathbb{Z}_2[x]$ if it cannot be factorised as a product of two polynomials of a lower degree in $\mathbb{Z}_2[x]$.

Example. deg 1 $1,\ x,\ x+1$ are irreducible.

deg 2 $x^2+1=(x+1)^2$ is reducible, but:
x^2+x+1 is irreducible (has no root in $\mathbb{Z}_2$)

deg 3 The irreducible polynomials are: $x^3+x+1,\ x^3+x^2+1$

deg 4 The irreducible polynomials are:
$x^4+x+1,\ x^4+x^3+1$ (not $x^4+x^2+1=(x^2+1)^2$ (by the squaring principle))

Some facts

- Every polynomial in $\mathbb{Z}_2[x]$ is a unique product of irreducible polynomials. The proof is by Euclid's algorithm (or use rings - polynomial ring of a PID is a field, therefore all elements are a product of irreducibles). As a result we can define the hcf and lcm of polynomials in $\mathbb{Z}_2[x]$
- For each $k \geq 1$, $\exists$ finite field $\mathbb{F}_{2^k}$ of order 2^k. It is constructed as follows:

$$\text{let:}\quad p_k(x) \in \mathbb{Z}_2[x] \quad \text{be irreducible of degree } k$$

$$\text{then:}\quad \mathbb{F}_{2^k} = \frac{\mathbb{Z}_2[x]}{\underbrace{(p_k(x))}_{\text{ideal generated by } p_k(x)}}$$

E.g

$$\mathbb{F}_4 = \frac{\mathbb{Z}_2[x]}{(x^2+x+1)} = \frac{\mathbb{Z}_2[x]}{I}$$

Elements of this field are: $0+I,\ 1+I,\ x+I,\ x+1+I$
Write $\alpha = x+I$, then:

$$\mathbb{F}_4 = \{0,\ 1,\ \alpha,\ \alpha+1\}$$

With $\alpha^2+\alpha+1=0$. E.g. $\alpha(\alpha+1)=\alpha^2+\alpha=1,\ \alpha^3=\alpha^2+\alpha=1$
E.g.

$$\mathbb{F}_8 = \frac{\mathbb{Z}_2[x]}{(x^3+x+1)} \qquad \text{writing } \alpha = x+I$$

$$\mathbb{F}_8 = \left\{0,\ 1,\ \alpha,\ 1+\alpha,\ \alpha+\alpha^2,\ 1+\alpha^2,\ 1+\alpha+\alpha^2\right\}$$

- The multiplicative group:

$$\mathbb{F}_{2^k}^* = (\mathbb{F}_{2^k} \setminus 0, \times) \quad \text{is cyclic}$$

If $\mathbb{F}_{2^k}^* =< \beta >$ we call β a primitive element of $\mathbb{F}_{2^k}$ E.g.

$$\mathbb{F}_4^* =< \alpha >=< 1 + \alpha > \quad \text{has primitive elements } \alpha,\ 1 + \alpha$$

$\mathbb{F}_8^*$ has order 7 so all its elements apart from 1 are primitive (since it's a cyclic group of prime order)

$$\mathbb{F}_{16}^* = \frac{\mathbb{Z}_2[x]}{(x^4 + x + 1)} : \quad \text{let } \alpha = x + 1 \text{ so } \alpha^4 + \alpha + 1 = 0$$

Claim. *α is a primitive element*

Proof. The order of α in $\mathbb{F}_{16}^*$ divides 15.
Also:

$$\alpha^1 \neq 1$$
$$\alpha^5 = \alpha^2 + \alpha \neq 1$$

So α has order 15 and $\mathbb{F}_{16}^* = \alpha$
Non primitve elements are the powers of α □

- If $\gamma \in \mathbb{F}_{2^k}$ then γ has a minimal polynomial: $m(x) \in \mathbb{Z}_2[x]$. This is the unique irreducible polynomial that has γ as a root. Also:

$$deg(m(x)) \leq k$$
$$m(x) \text{ divides } x^{2^k - 1} - 1$$

E.g. in $\mathbb{F}_8$,

$$\alpha \text{ has min poly } x^3 + x + 1$$
$$\alpha^2 \text{ has min poly } x^3 + x + 1 \quad (\text{as } \alpha^6 + \alpha^2 + 1 = (\alpha^3 + \alpha + 1)^2 = 0)$$
$$\alpha^3 \text{ has min poly } x^3 + x^2 + 1 \quad \text{chec}$$

Definition (Definition of BCH codes)**.**
Let $k \geq 2$ and $d \geq 2$ be ingtegeres. In $\mathbb{F}_{2^k}$ let β be a primitive element. For each $i \geq 1$ let:

$$m_i(x) = \quad \text{the minimal polynomial of } \beta$$

Take the polynomials:

$$m_1(x),\ \cdots,\ m_{d-1}(x) \in \mathbb{Z}_2[x]$$

and let $p(x)$ be their lcm (i.e. the product of distinct $m_i(x)$ś).
Let $n = 2^k - 1$, so $p(x)$ divides $x^n - 1$. Then the cyclic code of length n and generative polynomial $p(x)$ is called the *BCH code* of length n and *designed distance d*

Example. $k = 3$, $\mathbb{F}_8$ with primitive element α.

$$\text{Take } d = 3: \quad \begin{aligned} m_1(x) &= \text{ min poly of } \alpha = x^3 + x + 1 \\ m_2(x) &= \text{ min poly of } \alpha^2 = x^3 + x + 1 \end{aligned}$$

Here $p(x) = x^3 + x + 1$
BCH code is Ham(3)

$$\text{Take d=4:} \quad m_3(x) = \text{ min poly of } \alpha^3 = x^3 + x^2 + 1$$

Here $p(x) = (x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + \cdots + 1$
BCH code is $\{0^6,\ 1^7\}$

Theorem 1.30. *Let $n = 2^k - 1$ and let C be BCH code of length n and designed distance d.*

1. *Then $d(C) \geq d$*
2. *Let $t = \frac{1}{2}d$ (so $d = 2t$ or $d = 2t + 1$ - take the integer part)*
   Then dim $C \geq n - tk$

Note Obvious $deg(p(x)) \leq deg(m_i(x) \cdots m(d - 1(x))) \leq (d - 1)k$

Example. $k = 4$ In $\mathbb{F}_{16}$, we have a primitive element α with minimal polynomial $x^4 + x + 1$
So:

$m_1(x) = x^4 + x + 1$

$m_2(x) =$ minimal polynomial of $\alpha^2 = x^4 + x + 1$

$m_3(x) =$ minimal polynomial of $\alpha^3 = x^4 + x^3 + x^2 + x + 1$

this divides $x^5 - 1$, as α^3 has order 5

$= (x + 1)(x^4 + x^3 + x^2 + x + 1)$ (this can be easily shown to be irreducible)

Example. $d = 5$

$$\begin{aligned} p(x) &= lcm(m_1,\ \cdots, m_4) \\ &= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \end{aligned}$$

So BCH code has dimension 7 and minimum distnace ≥ 5

Remark. Compare this with GV-Bound

$$1 + 14 + \binom{14}{2} + \binom{14}{3} \overset{??}{<} 2^{15-7}$$

This is false. GV-bound gives existence of code of length 15, minimum distance ≤ 5, dimension 6, but not dimension 7. So BCH beats GV here.

2 Strongly regular graphs

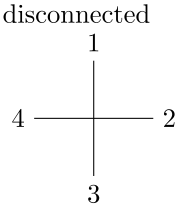
Recall: graph $\Gamma = (V, E)$ where:

$$\begin{aligned} V &= \text{ set of vertices} \\ E &= \text{ set of deges} \end{aligned}$$

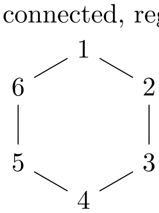
Γ is regular of valency k if every vertex in Γ has k neighbours.
A path in Γ is a sequence:
$v_0, \cdots, v_r$ s.t. v_i is joined to $v_{i+1}, \forall i$. Length of the path is then r.
Γ is connected if $\forall v, w \in V, \exists$ a path from v to w.
If Γ is connected and $v, w \in V$, the distance $d(v, w) =$ length of the shortest path from v to w.
Diameter $diam(\Gamma) = max\{d(v, w) : v, w \in V\}$ i.e. the length of the longest path in Γ.

Example.

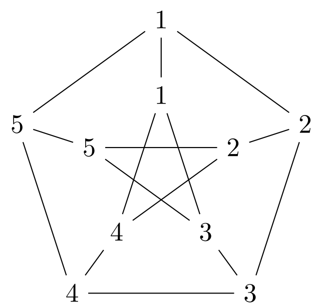
1. disconnected



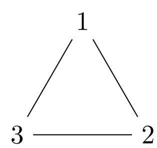
2. connected, regular, valency 2, diameter 3 (C_6)

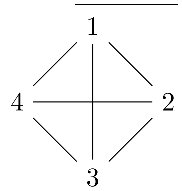


3. Petersen graph, regular, valency 3, connected, diameter 2

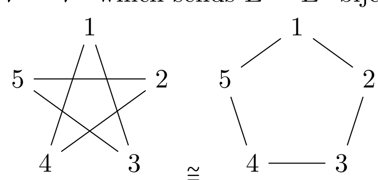


4. $diam(\Gamma) = 1 \Rightarrow$ any 2 vertices are joined by an edge. Such a graph with n vertices is called the complete graph K_n, e.g:





Two graphs are (V, E) and (V', E') are isomorphic if there exists a bijection $V \to V'$ which sends $E \to E'$ bijectively. Eg:



Sometimes we write $V = V(\Gamma), E = E(\Gamma)$.

Proposition 2.1. *Suppose Γ is a connected graph that is regular of valency k, diameter d. Then* $|V(\Gamma)| \le N(k, d) = 1 + k + k(k-1) + k(k-1)^2 + \cdots + k(k-1)^{d-1}$

Proof. Let $x \in V(\Gamma)$
For $i \ge 1$ let

$$D_i = \{y \in V(\Gamma) : d(x, y) = i\}$$

Then

$$|D_1| = k$$
$$|D_2| \le k(k-1)$$
$$|D_3| \le |D_2|(k-1) \le k(k-1)^2$$

and so on

As $diam(\Gamma) = d$

$$displaystyle \sum_{i=1}^{d} |D_i| V(\Gamma) = x \cup D_1 \cup D_2 \cdots \cup D_d$$

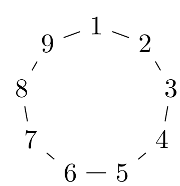
So:
$$|V(\Gamma)| \leq 1 + \sum_{i=1}^{d} |D_i| \leq 1 + \sum_{i=1}^{d} k(k-1)^{i-1}$$

$\square$

Question. *When does the equality occur?*

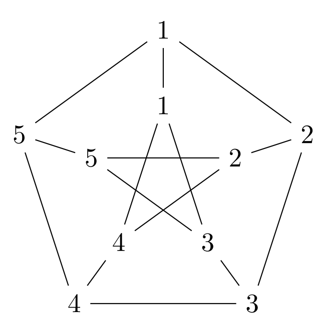
Definition. Call Γ a Moore graph if Γ is connected, regular of valency k, diameter d and
$$|V(\Gamma)| = N(k,d)$$

Example. 1. $k = 2, N(2,d) = 1 + 2d$



Any *n-gon* is a *Moore Graph*

2. $k = 3, d = 2, N(3,2) = 1 + 3 + 6 = 10$



The Petersen graph is the only Moore graph wit these k, d up to isomorphism. (excercise)

3. $k = 3, d = 3$ and higher it gets much harder.

4. $k = 4, d = 2$ Note that:
$$N(k,2) = 1 + k + k(k-1) = k^2 + 1$$
So we need a graph with 17 vertices. There is no such Moore graph with $k = 4, d = 2$.

Proof. (a) IN a moore graph with $diam(2)$ there are no triangles or squares

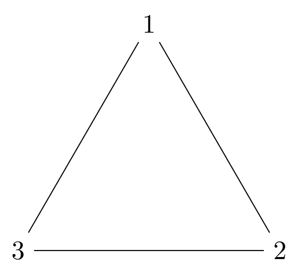
(b) Now let $k = 4$. Start with an edge $0, \infty$. Let a, b, c and x, y, z be the other neighbours of 0 and ∞.

As diameter is 2, $\exists$ a common neighnour of a, x. By (1) it's a new vertex, $callit(a, x)$.
Similarly there are new vertices $(a, x), (a, y), (a, z), \cdots, (c, z)$ (9 in total). These together with $a, b, c, x, y, z, 0, \infty$ are 17 vertices.

There are 2 neighbourso f(a, x) among the 9 new vertices, not $(a, \cdot)$ or $(\cdot, x)$ so possibilities are among

$$(b, x), (b, z), (c, y), (c, z)$$

Say
Then (a, x) not joined to $(b, z), (c, y)$ (no squares)
So (a, x) joined to $(b, y), (c, z)$.
<u>Neighbours of (b, y):</u>
$(b, y), (a, x)$ and 1 other. not $(a, \cdot), (\cdot, x), (b, \cdot), (\cdot, y)$. So the only possibility is (c, z)



<u>contradiction</u>

$\square$

Question. *For which k is there a Moore graph of dimension 2, valency k? So far we have seen examples for $k = 2, k = 3$, but impossible for $k = 4$. We need more theory.*

Answer: Only for $k = 2, 3, 7, 57$ $\square$

Definition. A graph Γ is <u>*strongly regular*</u> with parameters (v, k, a, b) if:

1. Γ has v vertices and is <u>regular</u> of valency k.
2. Any two joined vertices have exactly a common neighbours.
3. any two non-joined vertices have b common neighbours.

Proposition 2.2. *Suppose Γ is strongly regular.*

1. *if $b > 0$ then Γ is connected and $diam(\Gamma) = 2$*
2. *if $b = 0$ then Γ is a disjoint union of complete graphs K_{k+1}*

Proof.

1. If $b > 0$ then any 2 non-joined vertices can be joined by a path of length 2.
2. Suppose $b = 0$. Let vertex x have neighbours $v_1, \cdots, v_k$. As $b = 0$, v_i is joined to v_j, $\forall i \neq j$. So $x, v_1, \cdots, v_k$ form a complete graph K_{k+1}. Any further vertex is not joined to x and is not joined to any vertices v_i as $b = 0$.
   As above y and its neighbours form another K_{k+1}

□

Examples.

1. Moore graphs of diameter 2 are strongly regular with parameters $(v, k, 0, 1)$ $\quad (v = k^2 + 1)$ (since there are no triangles or squares).
2. <u>Triangular graphs $T(n)$</u> $(n \geq 4)$

$$\begin{aligned} \text{Vertices: } &= \binom{n}{2} \text{ pairs from } \{1, \cdots, n\} \\ \text{Edges: } &= \text{join } ij, kl \text{ iff } |ij \cap kl| = 1 \end{aligned}$$

   This is a strongly regular graph with parameters

$$\begin{aligned} v &= \binom{n}{2} \\ k &= 2n - 1 \\ a &= n - 2 \\ b &= 4 \end{aligned}$$

3. <u>Lattice graphs $L(n)$</u>

$$\begin{aligned} \text{Vertices: } &= \text{ ordered pairs } (i, j), \text{ where } i, j \in \{1, \cdots, n\} \\ \text{Edges: } &= \text{join } (i, j), (k, l) \text{ if } i = k \text{ or } j = l \end{aligned}$$

   Params:

$$\begin{aligned} v &= n^2 \\ k &= 2n - 2 \\ a &= n - 2 \\ b &= 2 \end{aligned}$$

4. Payley graphs
   Let $n > 2$ be prime. Recall $\mathbb{Z}_p = \{0, 1, \cdots, p-1\}$ with $(+, \times)$ modulo p is a field.

   Define:

$$Q = \{x^2 : x \in \mathbb{Z}_p^*\}$$

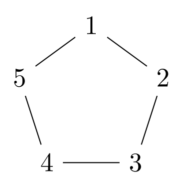
   a subgroup of $(\mathbb{Z}_p^*, \times)$
   Map $\phi : x \to x^2 \qquad (\mathbb{Z}_p^* \to Q)$ is a homomorphism with kernel:

$$ker(\phi) = \{x : x^2 = 1\} = \{x : (x-1)(x+1) = 0\} = \pm 1$$

   Therefore $|Q| = |im\ \phi| = \frac{|\mathbb{Z}_p^*|}{|ker\ Q|} = \frac{p-1}{2}$ assume $p \equiv 1 mod 4$
   Then $|Q|$ is even, so (by Lagrange theorem), Q has an element of order 2, whicb y above must be -1. Hence $-1 \in Q$.

   Definition. Payley graph $P(p)$, (p prime $\equiv 1 mod 4$)

$$\begin{aligned} \text{Vertices: } &= \text{ elements of } \mathbb{Z}_p\ (i,j), \text{ where } i,j \in \{1, \cdots, n\} \\ \text{Edges: } &= \text{join } (x,y) \text{ iff } (x,y) \in Q \end{aligned}$$



   is the smallest Payley graph

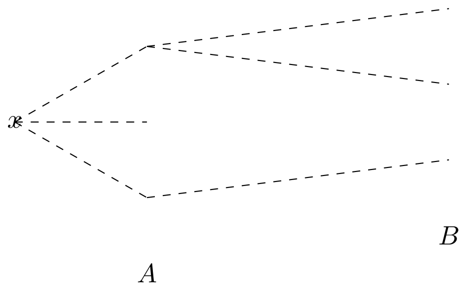
Proposition 2.3. *$P(p)$ is strongly regular, params:*

$$v = p, \quad k = \frac{p-2}{2}, \quad a = \frac{p-5}{4}, \quad b = \frac{p-1}{4}$$

Proof. See sheet 4 □

2.1 Theory

Proposition 2.4. *If Γ is strongly regular, params (v,k,a,b) then Γ^C is also strongly regular, params $(v, v-k-1, v-2l+b-2, v-2k+1)$.[$\Gamma^C$, the complement of Γ is the graph with the same vertex set and all edges (non-edges) replaced with non-edges (edges), Eg. $P(5)$ is the complement of $K_5 - P(5)$].*



Proof. Γ^C is regular of valency $v - k - 1$ (as we are connecting each vertex to $v - 1 - k$ vertices that were previously disconnected).

In Γ^C, b becomes:

$$v - 2(k - a - 1) - a - 2 = v - 2k + a$$

Since we are removing $2(k-a-1)$ common neighbours and we are disconnecting an extra pair $a - 2$
Param a is $v - 2(k - b) - b - 2 = v - 2k + b - 2$ □

Proposition 2.5. *Balloon equation If Γ is strongly regular graph with params (v, k, a, b), then:*

$$k(k - a - 1) = b(v - k - 1)$$

Proof. Let $x \in V(\Gamma)$, let A be the set of k neighbours of x, and B be the remaining vertices. So $|B| = v - k - 1$.
Count the number of edges between A and B. Each vertex in A is joined to $k - a - 1$ vertices in B, so:

$$\begin{aligned}|N| &= |A| \times (k - a - 1)\\ &= k(k - a - 1)\end{aligned}$$

Each vertex in B is joined to b vertices in A. So:

$$|N| = |B| \times b = (v - k - 1)b$$

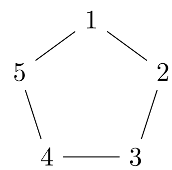
. Hence $k(k - a - 1) = b(v - k - 1)$ □

Remark. "Balloon picture" of Γ e.g. Moore graphs of diameter 2 are strongly regular with parameters $(v, k, 0, 1)$. Picture So the "baloon equation" is $k(k - 1) = v - k - 1$. So $v = k^2 + 1$

2.2 Adjacency matrices

Let Γ be a graph with vertex set $\{e_1, \cdots, e_r\}$. Define a $r \times r$ matrix $A = (a_{ij})$ by:

$$a_{ij} = \begin{cases} 1 & \text{if } e_i \text{ joined to } ej \\ 0 & \text{otherwise} \end{cases}$$



Example.

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

Basic properties of A:

1. A is symmetric with all entries 0 or 1
2. A has zeroes on the diagonal

Definition. A is the adjacecny matrix of Γ

For strongly regular graph, A has nice properties.

Proposition 2.6. *Let Γ be strongly regular, params (v, ka, a, b) with the adjacency matrix A. Let J be the $v \times v$ matrix with all entries 1.*

1. $AJ = kJ$

2. $A^2 = (a-b)A + (k-b)I + bJ$

Proof. 1. As Γ is regular of valency k, each row of A has k 1s so $AJ = kJ$

2. Since A is symmetric, $A^2 = AA^T$ So:

$$\begin{aligned} ij\text{th entry of } A^2 &= ij\text{th entry of } AA^T \\ &= (\text{row } i \text{ of } A)(\text{col } j \text{ of } A^T) \\ &= (\text{row } i \text{ of } A)(\text{row } j \text{ of } A) \\ &= \text{no. of common neighbours of } e_i \text{ and } e_j \\ &= \begin{cases} k & \text{if } i = j \\ a & \text{if } i \neq j \text{ and } e_i \text{ and } e_j \text{ are joined in } \Gamma \\ b & \text{if } i \neq j \text{ and } e_i \text{ and } e_j \text{ are not joined in } \Gamma \end{cases} \end{aligned}$$

So A^2 has ks on the diagonal, $a's$ where A has a one (i.e. where A describes edges that are joined), $b's$ elsewhere.
Therefore:

$$\begin{aligned} A^2 = kI &= aA + b(J - I - A) \\ &= (a-b)A + (k-b)I + bJ \end{aligned}$$

□

Eigenvalues Let v is the number of vertices. Adjacency matrix of a graph Γ is real and symmetric, so it has real eigenvalues and is diagonalizable, i.e.:

$$\exists P \quad \text{s.t.} \quad P^{-1}AP = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_v \end{pmatrix}$$

The multiplicity of an eigenvalue λ_i is the number of times it appears on the diagonal.

Theorem 2.7 (2.7)**.** *Let Γ be a strongly regular graph with (v,k,a,b) $\quad b > 0, \quad v > 2k$.*

1. *A has 3 eigenvalues $k, r_1, r_2 :$ $\quad r_1, r_2$ are roots of:*

$$x^2 - (a-b)x - (k-b) = 0$$

2. *r_1, r_2 have multiplicities m_1, m_2, where:*

$$m_1 + m_2 = v - 1$$
$$m_1 r_1 + m_2 r_2 = 0k$$

3. *$r_1, r_2 \in \mathbb{Z}$, unless parameters $(4b+1, 2b, b-1, b)$*

Remark. Concerning the 2nd assumption: $v > 2k$
If $2k \geq v$ then Γ^C is strongly regular (proven last time) with params $(v, v-k-1, \cdots)$ adn $v \leq 2k \Rightarrow v > 2(v-k-1)$ where $v-k-1$ is the valency of Γ^C So Theorem 2.7 applies to Γ^C provided Γ^C is connected (i.e. $b > 0$). If Γ^C is not connected we know from (2.3) that Γ^C is a disjoin union of complete graphs, so we know what Γ is.

Proof later

Applications

Moore graphs : Recall Moore graph of diameter 2 is strongly regular, parameters $(v, k, 0, 1), v = k^2 + 1$

Theorem 2.8 (2.8)**.** *If $\exists$ a Moore graph of valency k diameter 2, then:*

$$k = 2, 3, 5, 6 \; or \; 57$$

Proof. Let Γ be sucha Moore graph, so Γ is strongly regular, params $(k^2+1, k, 0, 1)$. Note $b = 1 > 0$ and $k^2 + 1 > 2k$ (as$k > 1$). So Theorem 2.7 applies. Let A be the adjacency matrix of Γ. By 2.7 A has 3 eigven values k, r_1, r_2 where r_1, r_2 are the roots of:

$$x^2 + x - (k-1) = 0$$

So:

$$r_1, r_2, = \frac{1}{2}\left(-1 \pm \sqrt{4k-3}\right)$$

By 2.7 (2) the results m_1, m_2 of r_1, r_2 satisfy:

$$m_1 + m_2 = k^2$$
$$m_1 r_1 + m_2 r_2 = -k$$

From the second equation we get:

$$\frac{1}{2}(-m_1 - m_2) + \frac{1}{2}\sqrt{4k-3}\,(m_1 - m_2) = -k$$

So:

$$\sqrt{4k-3}\,(m_1 - m_2) = k^2 - 2k$$

But we also know that the square root term is an integer, which gives us a lot of information about k

By 2.7(3) $r_1, r_2 \in \mathbb{Z}$ unless the parameters are $(5,2,0,1)$, in which case Γ is C_5 (a pentagon). Therefore $r_1, r_2 \in \mathbb{Z}$. This implies $\sqrt{4k-3} \in \mathbb{Z}$ Write:

$$n = \sqrt{4k-3}$$

Then $n^2 = 4k - 3$, so $k = \frac{n^2+3}{4}$. Then use it in the previous equations:

$$\begin{aligned} n(m_1 - m_2) &= k(k-2) \\ &= \frac{n^2+3}{4} \times \frac{n^2-5}{4} \end{aligned}$$

Conclude that $m_1 - m_2 = \frac{(n^2+3)}{(n^2-5)} 16n$.

Key point: this is an integer. So n divides $(n^2+3)(n^2-5)$. Now:

$$hcf(n, n^2+3) | 5$$
$$hcf(n, n^2-5) | 5$$

Therefore n divides 15. Possibilities:

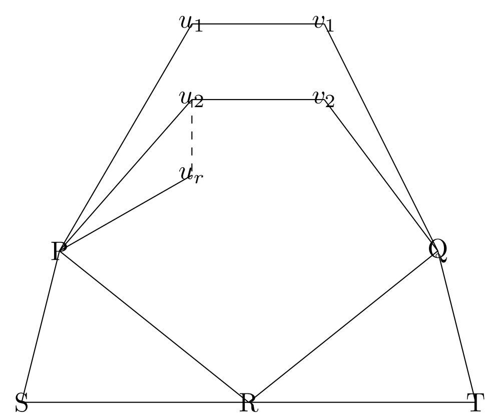
$n = 1$ then $1 = \sqrt{4k-3} \Rightarrow k = 1$ <u>contradiction</u>

$n = 3$ then $4k - 3 = 9 \Rightarrow k = 3$

$n = 5$ then $4k - 3 = 25 \Rightarrow k = 7$

$n = 15$ then $4k - 3 = 225 \Rightarrow k = 57$

□



Frendship theorem

Theorem 2.9. *Suppose* Γ *is a graph in which any 2 vertices have exactly 1 common neighbour. Then* $\exists$ *a vertex that is joined to all of the other verices.*

Proof. Assume false, i.e. there is <u>no vertex</u> that is joined to all the others. Aim for contradiction.

Claim. Γ *is a regular graph*

Proof. First we show, if P, Q are non-joined vertices, then $v(P) = v(Q)$ (where $v(P)$ = no. of the neighbours of P).

To see this, let R be the common neighbour of P and Q. Let S be the common neighbour of P, R and T a common neighbour of Q, R. Note that $S \neq T$ (otherwise P, Q would have 2 common nieghbours). Let the remaining neighbours of P be $u_1, u_2, \cdots, u_r$. Consider the common neighbour of u_1 and Q. It is not T (otherwise P, T have 2 common neighbours) and it is not R, (otherwise P, R have 2 common nieghbours). So it is a new vertex v_1. Now consider the common neighbour of u_2, Q. It's not v_1 (otherwise u_1, u_2 have 2 common neighbours). So it is a new vertex v_2. Carrying on for each u_i, its common neighbour with Q is a new vertex v_i Hence:

$$v(P) = r + 2 \leq v(Q)$$

Similarly $v(Q) \leq v(P)$, hence $v(P) = v(Q)$ proving the claim.

First note that non-joined P, Q exist (by the assumption that $\exists$ a vertex joined to all others). So $v(P) = v(Q)$. Let R be a common neighbour of P, Q. If S is a futher vertex it is not joined to both P, Q by the previous claim. Moreover

$$v(S) = v(P) = v(Q)$$

Finally by assumption $\exists$ vertex S not joined to R, so $v(R) = v(S)$. Therefore Γ is regular. $\square$

Claim. *last part* Γ *is strongly regular with params* $(v, k, 1, 1)$

Claim. *There is no such strongly regular graph*

Proof. So:

$$k(k-2) = v - k - 1$$

Hence:

$$v = k^2 - k + 1$$

Now apply Theorem 2.7. Note:

- $b = 1 > 0$
- $v = k^2 - k + 1 > 2k \Leftrightarrow k \geq 3$

If $k = 2$ then $v = 3$ and Γ is C_3. <u>contradiction</u>
Hence $v > 2k$, so Theorem 2.7 applies to Γ Let A be the adjacency matrix of Γ. By 2.7(1), A has 3 eigenvalues k, r_1, r_2, wher r_1, r_2 are the roots of:

$$x^2 - k(-1) = 0$$

So $r_1 = \sqrt{(k-1)}, \quad r_2 = -\sqrt{(k-1)}$ By 2.7 (2), multiplicities m_1, m_2 of r_1, r_2 satisfy:

1. $m_1 + m_2 = k^2 - k$
2. $r_1 m_1 + r_2 m_2 = -k$

From (2):

$$\sqrt{k-1}(m_1 - m_2) = -k$$

Hence:

$$(k-1)(m_1 - m_2)^2 = k^2$$

Since $m_1 - m_2 \in \mathbb{Z}$, this means $k - 1$ divides k^2. But $hcf(k-1, k) = 1$, so there is no such strongly regular graph unless $k = 2$. $\square$

$\square$

Strongly regular graphs with small v

Question. *What are the possible parameters of strongly regualr graphs with* $v = 15$

Examples.

1. Triangular graph $T(6)$: vertices are pairs from $\{1, \cdots, 6\}$, join ij with kl if $|ij \cap kl| = 1$. Params of $T(6)$ are $(15, 8, 4, 4)$
2. $T(6)^C$: params $(16, 6, 1, 3)$
3. Examples with $b = 0$: $(K_3)^5$ and $(K_5)^3$. Parameters are $(15, 2, 1, 0)$, $15, 4, 3, 0$ respectively.
   Complements of these are also strongly regular with $v = 15$, paramters are: $(15, 12, 9, 12)$, $(15, 10, 5, 10)$ respectively.

Proposition 2.10. *If Γ is strongly regular with $v = 15$ then Γ is isomorphic one of the graphs listed above. I.e. the parameters of Γ are those of $T(6), (K_5)^3, (K_3)^5$ or of the complements of those.*

Proof. Let Γ have parameters$(15, k, a, b)$ If $15 \leq 2k$, replace Γ by complement Γ^C so can assume:

$$15 > 2k$$

If $b = 0$ then Γ is $(K_5)^3$ or $(K_3)^5$ by (2.2) So assume now that $b > 0$. Hence Theorem 2.7 applies to Γ
Consider each possible k, with $2 \leq k \leq 7$

$k = 2$ Γ is a 15-gon, which not strongly regular <u>contradiction</u>

$k = 3$ Balloon: By balloon equation

$$\begin{aligned} 3(2-a) = 11b &\Rightarrow 11 | 3(2-a) \\ &\Rightarrow 11 | 2-a \\ &\Rightarrow a = 2 \end{aligned}$$

<u>contradiction</u>

$k = 4$ Balloon: By balloon equation

$$\begin{aligned} 4(3-a) = 10b &\Rightarrow 10 | 4(3-a) \\ &\Rightarrow 5 | 3-a \\ &\Rightarrow a = 3 \end{aligned}$$

<u>contradiction</u>

$k = 3$ Balloon: By balloon equation

$$\begin{aligned} 5(4-a) = 9b &\Rightarrow 9 | 4-a \\ &\Rightarrow a = 4, b = 0 \end{aligned}$$

<u>contradiction</u>

$k = 6$

$$6(5-a) = 8b \Rightarrow a = 1, b = 3$$

These are the parameters $(15, 6, 1, 3)$ so, $\Gamma \cong T(6)^C$

$k = 7$ Here $7(6-a) = 7b \Rightarrow b = 6 - a$
Apply Theorem 2.7: The eigenvalues are $7, r_1, r_2$, roots of:

$$x^2 - (a-b)x - (k-6) = 0$$
$$x^2 - (2a-6)x - (a+1) = 0$$

So $r_1, r_2 = (a-3) \pm \sqrt{(}a^2 - 5a + 10)$. Use part 3 of Theorem 2.7. These are integers, since $15 \neq 4b + 1$. $r_1, r_2 \in \mathbb{Z}$ hence: $a^2 - 5a + 10$ is a square. We know that $0 \leq a \leq 5$. Possible such a are: $2, 3$.

$a = 2$ Then $r_1 = 1, r_2 = -3$, so 2.7(2) gives $m_1 + m_2 = 14$ and $m_1 - 3m_2 = -7$
So $4m_2 = 21$, But $m_2 \in \mathbb{Z}$contradiction

$a = 3$ Then $r_1 = 2, r_2 = -2$. And $m_1 + m_2 = 14$, $2_m 1 - 2m_2 = -7$ contradiction

So $k = 7$ does not occur.

□

Proof of Theorem 2.7 We are going to need:

Lemma 2.11. *Let A be a $v \times v$ real matrix (a_{ij}). and let $\lambda_1, \cdots, \lambda_v$ be the eigenvalues of A. Then $Tr(A) = \sum_{i=1}^{v} \lambda_i$*

Proof. By definition, λ_i are the roots of the characteristic polynomial of A:

$$\begin{aligned}
|xI - A| &= det\left(\begin{bmatrix} x - a_{11} & -a_{12} & \cdots & x - a_{1v} \\ -a_{21} & x - a_{22} & \cdots & x - a_{2v} \\ & & \vdots & \\ -a_{v1} & \cdots & \cdots & x - a_{vv} \end{bmatrix}\right) \\
&= x^v + x^{v-1}(-a11 - \cdots - a_{vv}) \\
&= x^v - Tr(A)x^{v-1} + \cdots
\end{aligned}$$

Therefore the sum of the roots is $Tr(A)$ □

Let's clear up a point:
The complete graph K_n, K_n^C do not count as strongly regular graphs.

2.3 Two-weight codes and strongly regular graphs

Definition. A linear code $C \subseteq \mathbb{Z}_2^n$ is a two-weight code if $\exists$ positive integers $w_1, w_2, w_1 \neq w_2$ such that every non zero codeword in C has a weight w_1 or w_2 and both weights occur.

Examples.

1. Extended $Ham(3) \subseteq \mathbb{Z}_2^8$ weights 4, 8
2. $C = \left\{v \in \mathbb{Z}_2^5 : wt(v) \text{ is even}\right\}$ weights 2,4
3. $C = \{x \in G_{24} : x_{16} = \cdots = x_{24} = 0\}$ weights 8, 12

Recall: a generator matrix for a linear code is a matrix whose rows form a basis for the code.

Definition. A linear code is *projective* if it has a generator matrix with all columns distinct and nonzero

Example. H' is a projective generator matrix:

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

Theorem 2.12 (2.12)**.** *Let $C \subseteq \mathbb{Z}_2^n$ be a linear code and assume:*

- *C is projective*
- *C is a two-weight, with weights $w_1 < w_2$*

Define a graph Γ as follows:

- *vertices of Γ : codewords in C*
- *join vertices a, b : if and only if $d(a,b) = wt(a+b) = min(w_1, w_2)$*

Then Γ is a strongly regular graph.

Example. $C = H'$ (extended Hamming(3) code), $w_1 = 4, w_2 = 8$.
What is Γ?
Well in Γ^C we join codewords a, b if and only if $d(a,b) = 8$, i.e. $a = b + 1^8$. So a is joined to only one other vector. So valency of Γ^C is 1 and it is K_2^8

Proof.
Let $k = dim(C)$ and let b_1, b_2 be the number of codewords in C of weight w_1, w_2 respectively.
Note $b_1 + b_2 = |C| - 1 = 2^k - 1$ (ommitting the zero vector)
For $i = 1, 2$ let:

$$A_i = b_i \times n \text{ matrix whose rows are the codewords of wt } w_i$$

Define:

$$A = \left(\frac{A_1}{A_2} \right) \quad (b_1 + b_2) \times n$$

Claim. *Each column of A hs weight 2^{k-1}*

Proof. Define $\phi_i : C \to \mathbb{Z}_2$ by:

$$\phi_i(x_1, \cdots, x_n) = x_i$$

$\forall i$ the i^{th} column of A is non zero (as C is projective), so ϕ_i is surjective. Therefore $ker\phi_i$ has dimension $k-1$
Hence the i^{th} column of A has $2^{k-1} - 1$ zeros and the rest of the entries are 2^{k-1} ones.

∎

Now we have equations:

$$b_1 + b_2 = 2^k - 1$$

$$b_1 w_1 + b_2 w_2 = n 2^{k-1}$$

Hence we can work out b_1, b_2.

Next step Consider column j of A. Let r_1 be the number of 0's in col j of A_1 and r_2 the number if 0's in col j of A_2. Codewords in C with 0 in j^{th} position form a subcode of C which is two-weight, with weights w_1-1, w_2-1. Its generator matrix has no zero column. (we are dropping the j^{th} column however) Otherwise A would have another column identical to j, but C is assumed to be projective, so it can't have two identical columns.

Hence we can work out r_1, r_2 as for b_1, b_2. r_1, r_2 are independent of the choice of column j. So every column of A_i has r_i 0's.

Bring back the graph Let us label the rows of A_1 as $a_1, \cdots, a_{b_1}$. (recall $b_1 + b_2 = k$ and b_1 is number of rows in A_1) We can calculate:

$$\sum_{i=1}^{b_1} d(a_i, a_1) = D$$

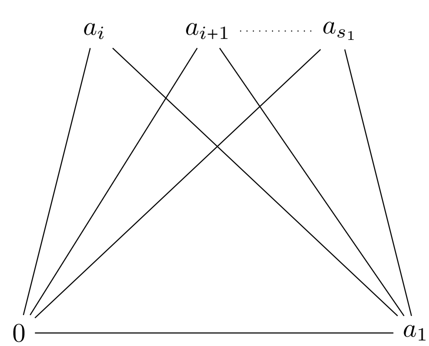
Let:

$$\begin{aligned} s_1 &= \text{ number of } a_i\text{'s such that } d(a_1, a_i) = w_1 \\ s_2 &= \text{ number of } a_i\text{'s such that } d(a_1, a_i) = w_2 \end{aligned}$$

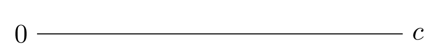
Then:

$$\begin{aligned} s_1 + s_2 &= b_1 - 1 \\ s_1 w_1 + s_2 w_2 &= D \end{aligned}$$

So can calculate s_1, s_2. Now in the graph Γ :



SO for any edge such that the corresponding codeword c has weight $w_1 = wt(c)$



The vertices $0, c$ have s_1 common neighbours.

For a general edge $x \longleftrightarrow y, wt(x+y) = w_1$ there is a bijective correspondence between common neighbours of x, y and those of $0, x+y$

So any joined pair x, y have s_1 common neighbours. Similarly working with A_2 see that any non-joined pair has constant number of common neighbours, Finally note Γ is regular of valency b_1. Hence Γ is strongly regular. □

3 t-designs

3.1 Symmetric 2-designs

Definition. A 2-design is symmetric if it has $b = v$. Equivalently $k = r$

Example. $X = \mathbb{Z}_2^3 \setminus 0, |X| = 7$ Block one sets $\{x, y, x+y\}$ This is a 2-design params $(7, 3, 1)$ For this design

$$\lambda(v-1) = r(k-1) \Rightarrow b = r \Rightarrow r = 3$$

So $b = \frac{vr}{k} = 7$. So this is symmetric

This is called a Fano plane.

This is the smallest projective plane symmetric 2-design with $\lambda = 1$

Theorem 3.1. *Suppose there exists a symmetric 2-design with params (v, k, λ), and v is even. Then $k - \lambda$ is a square.*

Example. Is there a 2-design with params $(22, 7, 2)$?

Answer: Well:

$$\lambda(v-1) = r(k-1) \implies 2 \times 21 = r \times 6 \implies r = 7 = k$$

But $v = 22$ is even and and $k - \lambda = 7 - 2 = 5$ is not a square. So no such design exists

Proof. As $b = v$, the incidence matrix for A is square $v \times v$. So $det(A)$ exists and moreover, since A is square, $det(A) \in \mathbb{Z}$.

Now $det(A^T) = det(A)$, so $det(AA^T) = det(A)^2$. By Proposition (3.5)

$$det(A)^2 = (r-\lambda)^2(\lambda(v-1)+r)$$

Now noting that $r = k$

$$\lambda(v-1) = r(k-1) = k(k-1)$$

So

$$\lambda(v-1) + r = k(k-1) + k = k^2$$

Hence

$$det(A)^2 = (k-\lambda)^{v-1}k^2$$

Both sides are squares in $\mathbb{Z}$, hence $(k-\lambda)^{v-1}$ is a square. As v is even, $v-1$ is odd, so $k-\lambda$ is a square. □

Remark. If v is odd, the Bruch-Ryser-Charla theorem says: if a symmetric 2-design exists with parameters (v,k,λ) then the equation:

$$z^2 = (k-\lambda)x^2 + (-1)^{\frac{v-1}{2}}\lambda y^2$$

has a solution with $x,y,z \in \mathbb{Z}$ (not all $x,y,z = 0$)

Theorem 3.2. *(3.10) If $\mathcal{B}$ is a symmetric 2-design with parameters (v,k,λ), then any 2 blocks of $\mathcal{B}$ intersect in exactly λ points.*

Proof. Let A be the $v \times v$ incidence matrix. Consider $A^T A$:

$$\begin{aligned} ij\text{-entry} &= (\text{row } i \text{ of } A^T) \cdot (\text{col } j \text{ of } A) \\ &= (\text{col } i \text{ of } A) \cdot (\text{col } j \text{ of } A) \\ &= |B_i \cap B_j| \end{aligned}$$

Where $\mathcal{B} = \{B_1, \cdots, B_v\}$ ON the other hand by 3.5

$$AA^T = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & & \ddots & \\ \lambda & & & r \end{pmatrix} = \lambda J + (r-\lambda) I$$

So we are done if we prove $A^T A = AA^T$. Now $AJ = kJ = JA$ and $AI = IA$ hence A commuts with $AA^T = \lambda J + (r-\lambda)I$. So

$$AAA^T = AA^T A$$

We know that $det(AA^T) = det(A)^2 = (k-\lambda)^{v-1}k^2 \neq 0$. So $det(A) \neq 0$. So A is invertible and we can cancel out A on the left in the equality above, so $AA^T = A^T A$. □

Projective planes A symmetric 2-design with $\lambda = 1$ is called a projective plane. By 3.10 any two blocks will meet in 1 point.

Definition. (Equivalent definition of a projective plane)
A set of points and lines (lines are the blocks, or subsets of points) satisfying 3 axioms:

1. Any 2 points lie on a unique line
2. Any 2 lines meet in a unique point
3. There exists a collection of 4 points such that no 3 are on the same line

Remark. Follows from the axioms that all lines have the same number of points. So a projective plane is indeed a 2-design with $\lambda = 1$ - can show that it is also symmetric.

Remark. There is a converse to theorem 3.9 - namely, if there exists a 2-design with (v,k,λ) in which any 2 blocks intersect in λ points, then it is automatically symmetric.

3.2 Examples of symmetric 2-designs

Difference sets

Example. Let $X = \mathbb{Z}_7 = \{0, 1,$ $, 6\}$ and let $B_0 = 0, 1, 3 \subset X$ Define 7 subsets of X:

$$B_0 + i = \{b + i \;:\; b \in B_0\} \quad (0 \le i \le 6)$$

These subsets are:

$$\{0,1,3\}, \quad \{1,2,4\}, \quad \{2,3,5\}, \quad \cdots \quad \{6,0,2\}$$

Claim. *The subsets $B_0 + i$, $(0 \le i \le 6)$ are the blocks of a symmetric 2-design, params $(7, 3, 1)$*

Proof. Consider the differences $b_1 - b_2$ for $b_1, b_2 \in B_0$, $b_1 \ne b_2$. Easy inspection shows that each non zero element of $\mathbb{Z}_7$ occurs exactly once as a difference. The claim holds by proposition below □

Definition. Let λ and v be positivive integers and let $B_0 \subseteq \mathbb{Z}_v = \{0, 1, \cdots, v-1\}$. We say B_0 is a λ-difference set, if for any $d \in \mathbb{Z}_v \setminus 0$ there are exactly λ pairs $(b_1, B-2), b_i \in B_0$ such that $b_1 - b_2 = d$

Proposition 3.3. *(3.11) Suppose B_0 is a λ-difference set in $\mathbb{Z}_v$. For $i \in \mathbb{Z}_v$ Define:*

$$B_0 + i = \{b + i \;:\; b \in B_0\}$$

Let $k = |B_0|$. Then the subsets $B_i + i$ are the blocks of a symmetric 2-design with parameters (v, k, λ)

Proof. All the subsets $B_0 + i$ have size k, and there are v of them.
So need to show that any 2 points in $\mathbb{Z}_v$ are in λ blocks.

Pick $r, s \in \mathbb{Z}_v$, $(r \ne s)$. Then:

$$r, s \in B_0 + i \iff r - i, s - i \in B_0$$

Number of such i's is exactly the number of pairs $(b_1, b_2), b_1, b_2 \in B_0$ such that $b_1 - b_2 = r - s$. By definition of a λ-difference set, there are λ of them. □

Example. $v = 11, B_0 = \{1, 4, 9, 5, 3\}$. By proposition below B_0 is a 2-difference set, and therefore we get a symmetric 2-design with parameters $(11, 5, 2)$

Example. $v = 13$, $B_0 = \{0, 1, 3, 9\}$. Check that this is a 1-differnce set. And we get a symmetric 2-design with parameters $(13, 4, 1)$ so this is a projective plane!

An inifnite family
Let p be prime and define:

$$Q = \{x^2 \ : \ x \in \mathbb{Z}_p \setminus 0\}$$

Recall that Q is a subgroup of the C_p^* of order $\frac{p-1}{2}$

Proposition 3.4. *Suppose $p \cong 3mod4$. Then $Q \subseteq \mathbb{Z}_p$ is a λ-difference set with $\lambda = \frac{p-3}{4}$. The corresponding symmetric 2-design has parameters $(p, \frac{p-1}{2}, \frac{p-3}{4})$*

Example. See the examples with $p = 7, 11$ above.

Proof. Observe that as $p \cong 3mod4$, $|Q| = \frac{p-1}{2}$ so $-1 \notin Q$. Therefore:

$$Q \cup (-Q) = \mathbb{Z}_p^*$$

For an element of $q \in Q$ define:

$$S_q = \{(x_1, x_2) \ : \ x_1 - x_2 = q, x_1, x_2 \in Q\}$$

If $r \in Q$ then $qr \in Q$ and:

$$x_1 - x_2 = q \iff rx_1 - rx_2 = qr$$

So:

$$(x_1, x_2) \in S_q \iff (rx_1, rx_2) \in S_{qr}$$

Hence $|S_q|$ is constant for all $q \in Q$. Also, $-q \in -Q$ and:

$$(x_1, x_2) \in S_q \iff (x_2, x_1) \in S_{-q}$$

So $|S_{-q}| = S_q$. So $|S_x|$ is constant for $x \in Q \cup -Q = \mathbb{Z}_p^*$. Therefore Q is a difference set in $\mathbb{Z}_p$. The number of differences λ is:

$$|Q|(|Q| - 1)$$

So:

$$\lambda = \frac{|Q|(|Q| - 1)}{p - 1} = \frac{\frac{p-1}{2}\frac{p-3}{2}}{p - 1} = \frac{p - 3}{4}$$

□

Affine planes

These are like points and lines in $\mathbb{R}^2$ replacing $\mathbb{R}$ by a finite field.
Let $\mathbb{F}$ be a finite field, (e.g. $\mathbb{Z}_p$). Define

$$\mathbb{F}^2 = \{(x_1, x_2) : x_i \in \mathbb{F}\}$$

This is a 2-dimensional vector space over $\mathbb{F}$. Define:

points = vectors in $\mathbb{F}^2$

lines = subsets of form $\{v + \lambda w : \lambda \in \mathbb{F}\}$ for fixed v, w $(= v + span(W))$

Note:

1. Number of poitns is q^2
2. Lines are solution sets of linear equations:

$$(m,c) \in F \qquad y = mx + c \leftrightarrow (0,c) + span(1,m)$$
$$x = c \leftrightarrow (c,0) + span(0,1)$$

So the number of lines is $q^2 + q$

Definition. This collection of points and lines is called the affine plane over $\mathbb{F}$, denoted $\mathrm{AG}(2,\mathbb{F})$

Proposition 3.5 (3.13)**.**

1. *Every line has q points*
2. *Any two points lie on a unique line*

Hence $AG(2,\mathbb{F})$ is a 2-design with parameters $(q^2, q, 1)$

Proof.

1. A line $v + span(w) = \{v + \lambda w \quad : \quad \lambda in \mathbb{F}\}$ so there are q points
2. Let $a, b \in \mathbb{F}^2$. Then $a, b \in L$ where L:

$$L = \{a + \lambda(b-a) \quad : \quad \lambda \in \mathbb{F}\}$$

Suppose a, b lie on a line $L' = v + span(w)$ so:

$$a = v + \lambda_1 w, \quad b = v + \lambda_2 w$$

Then $b - a = (\lambda_2 - \lambda_1)w$ so:

$$L = a + span(b-a) = a + span(w) = v + \lambda_1 w + span(w) = v + span(w) = L'$$

□

In $\mathrm{AG}(2,\mathbb{F})$, two lines L_1, L_2 meet in 1 or 0 points (by 3.13(2)). If they meet in 0 points, L_1, L_2 are parallel lines

Proposition 3.6 (3.14)**.** *$AG(2,\mathbb{F})$ has q^2+q lines. They fall into $q+1$ disjoint sets, each containing q parallel lines.*

Proof. The $q+1$ disjoint sets are:

$$m \in \mathbb{F}, \quad \mathcal{L}_m = \text{set of lines } y = mx + c \quad (c \in \mathbb{F})$$
$$\mathcal{L}_\infty = \text{set of lines } x = c$$

Cakk the two sets $\mathcal{L}_m, \mathcal{L}_\infty$ parallel classes of lines. □

Proposition 3.7. *Each point in $\mathbb{F}^2$ lies in exacly one line in each parallel class.*

Proof. Each parallel class has q disjoint lines with q points □

Projective planes

Recall the definition of a projective plane (symmetric 2-design with $\lambda = 1$:
Here we are going to construct some examples of projective planes:

Example. $AG(2, \mathbb{Z}_3)$: lines fall into 4 parallel classes: $\mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_\infty$. To turn it into a projective plane, add new points p_0, p_1, p_2, p_∞ to each line and define a new line l_∞ through them: $l_\infty = \{p_0, p_1, p_2, p_\infty\}$

General case

$\mathbb{F}$ finite field $|\mathbb{F}| = q$. Start with an affine plane $AG(2, \mathbb{F})$. Add $q + 1$ new points $p_m \quad (m \in \mathbb{F}), p_\infty$.

New lines: to each line in $\mathcal{L}_m$ add the point p_m. Same for $\mathcal{L}_\infty$ and p_∞.

One more line: $l_\infty = \{p_m, p_\infty \quad : \quad m \in \mathbb{F}\}$

Proposition 3.8 (3.16)**.** *The points* $\mathbb{F}^2 \cup \{p_m, p_\infty \quad : \quad m \in \mathbb{F}\}$ *and the new lines, form a projective plane.*

Definition. Call this $PG(2, \mathbb{F})$, the projective plane over the field $\mathbb{F}$. (by definition there's only one)

Proof. We prove that the points and lines form a symmetric 2-design with $\lambda = 1$ (this is equivalent to the definition of a projective plane).

$$\begin{aligned} \text{no. of points} &= q^2 + q + 1 \\ \text{no. of lines} &= \text{no of lines in } AG(2, \mathbb{F}) + 1 \quad (\text{for } l_\infty) \\ &= q^2 + q + 1 \end{aligned}$$

So the number of lines is the same the same as the number of points, so the design is symmetric.

Next we prove the size of each line: each line in $AG(2, \mathbb{F})$ has q points, so each line has $q + 1$ points in $PG(2, \mathbb{F})$ (since we add p_m to each line). l_∞ also has $q + 1$ points by construction, so each line in $PG(2, \mathbb{F})$ has the same number of points.

Finally, need to show that any two points lie on a unique line. Pick $a, b \in PG(2, \mathbb{F})$.

1. If $a, b \in \mathbb{F}^2$ then they lie on a unique line in $AG(2, \mathbb{F})$. So it lies on a unique new line in $PG(2, \mathbb{F})$
2. If $a \in \mathbb{F}^2, b = p_m$ for some m (one of the new points). WLOG can swap a, b. Clearly $p_m \in \mathcal{L}_m$ and by (3.15) a lies on a unique line in the parallel class $l \in \mathcal{L}_m$. So the unique unique line containing a, b is the line $l \cup p_m$. Exact same argument follows for p_∞

3. If a, b are both new points, then by construction the unique line containing them is l_∞

$\square$

Remark. $\mathrm{PG}(2, \mathbb{F})$ is a symmetric 2-design parameters $(q^2 + q + 1, q + 1, 1)$