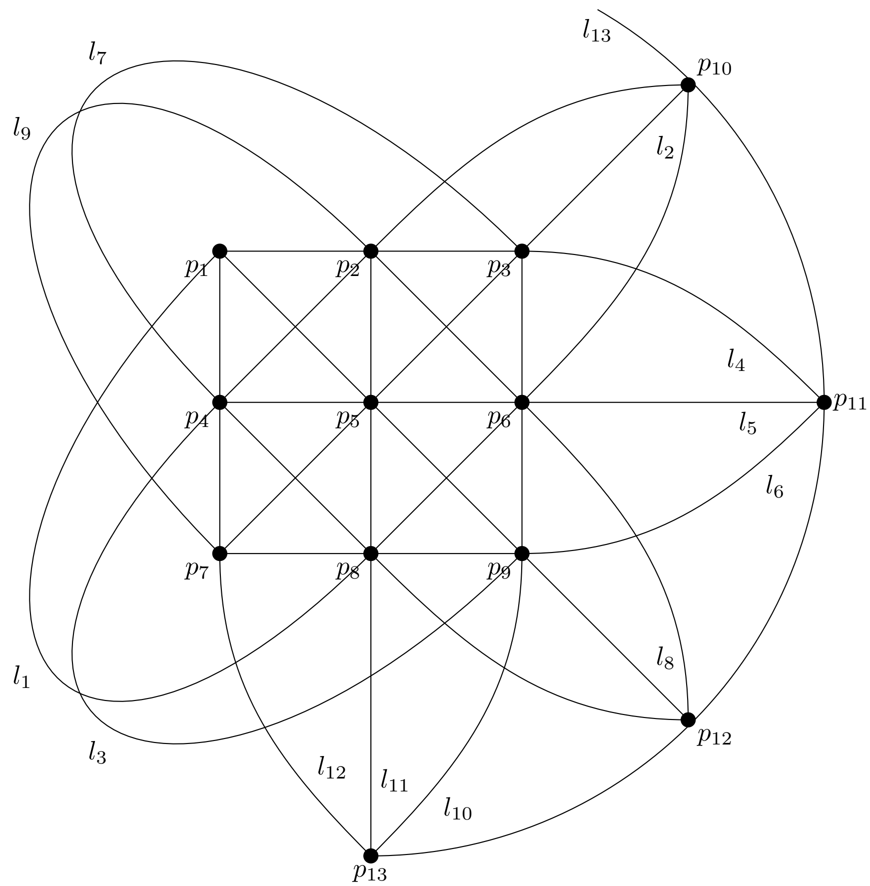
M3P17 Algebraic Combinatorics

Lectured by Dr Joanna Fawcett
Typed by David Kurniadi Angdinata

Autumn 2018



$\mathrm{PG}(2, \mathbb{F}_3)$

Syllabus

Error-correcting codes. Linear codes. Hamming codes. The Golay code. Cyclic codes. BCH codes. Automorphism group of a code. Strongly regular graphs. Adjacency matrices. Strongly regular graphs from two weight codes. Automorphism group of a graph. t-designs. Incidence matrices. Automorphism group of a design. Construction of 2-designs. Designs and strongly regular graphs.

Contents

0 Introduction

Lecture 1
Tuesday
09/10/18

Combinatorics is the study of discrete structures. We will study

1. codes, which are subsets of $\mathbb{Z}_2^n$,
2. graphs, which are vertices and edges, and
3. designs, which are collections of subsets of sets.

Algebra is linear algebra, which are matrices and vector spaces, groups, rings, and fields. We use methods from linear algebra to study $1, 2, 3$. Prerequisites are first and second year algebra. The following are recommended books.

- O Pretzel, Error-correcting codes and finite fields, 1992
- J van Lint, Introduction to coding theory, 1976
- D Hughes and F Piper, Design theory, 1985
- N Biggs, Algebraic graph theory, 1974
- C Godsil and G Royle, Algebraic graph theory, 2001
- P Cameron and J van Lint, Designs, graphs, codes, and their links, 1991
- N Biggs, Discrete mathematics, 1985

0.1 Codes

If the language is the alphabets $a, b, \dots$, the words are certain strings of alphabets. A code is a language for machines. The language is $0, 1 \in \mathbb{Z}_2$ and the words are certain strings in 0 and 1.

Example. The ASCII code of keyboard symbols is $A \mapsto 1000001$ to $9 \mapsto 0111001$. There are ~ 80 symbols, so need length seven as $2^7 > 80$.

The following is the communication process.

$$\text{message} \xrightarrow{\text{encode}} \text{codewords} \xrightarrow{\text{transmit}} \text{received message} \xrightarrow{\text{decode}} \text{decoded message}.$$

Errors in communication occur. What do we do? Language has lots of redundancies. Errors are easily corrected because no other words are close to received ones. The same idea for codes.

Example.

- Two messages yes and no or 1 and 0. The codewords are $1 \mapsto 111$ and $0 \mapsto 000$. To decode, if the received string is not a codeword, such as 101, then we take majority 111. This code corrects one error.
- Eight messages abc for $a, b, c \in \mathbb{Z}_2$. For each abc, define codeword $abcxyz$, where $x = a+b, y = a+c, z = b + c$. So the code is

  $$C = \{000000, 100110, 010101, 110011, 001011, 101101, 011110, 111000\} \subseteq \mathbb{Z}_2^6.$$

  Suppose the received string is 010110. Then $abx = 011, acy = 001, bcz = 100$. The error has to be with c. The correct codeword is 011110. Claim that this code corrects one error, since

  $$\begin{array}{c|cccccc} & a & b & c & x & y & z \\ \hline abx & \times & \times & \checkmark & \times & \checkmark & \checkmark \\ acy & \times & \checkmark & \times & \checkmark & \times & \checkmark \\ bcz & \checkmark & \times & \times & \checkmark & \checkmark & \times \end{array}.$$

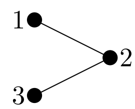
The aims of coding theory are to find $C \subseteq \mathbb{Z}_2^n$ such that

- C has lots of codewords,
- C corrects as many errors as possible, and
- the length n of C is as small as possible.

0.2 Graphs

A graph is (V, E) where V is a set of vertices, and E is a collection of unordered pairs from V called edges, or 2-subsets of V.

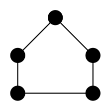
Example. Let $V = \{1, 2, 3\}$ and $E = \{\{1, 2\}, \{2, 3\}\}$. Then



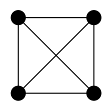
.

We will study certain types of graphs. If $\{i, j\} \in E$, say i is adjacent to j, or i is joined to j, or i and j are neighbours. A graph is regular if every vertex has the same number k of neighbours. The valency, or degree, is k.

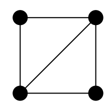
Example.



regular
$k = 2$



regular
$k = 3$

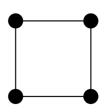


not regular

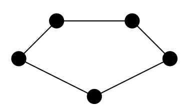
A graph is strongly regular if

- it is regular of valency k,
- any two adjacent vertices have the same number λ of common neighbours, and
- any two non-adjacent vertices have the same number μ of common neighbours.

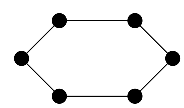
Example.



strongly regular
$k = 2$
$\lambda = 0$
$\mu = 2$

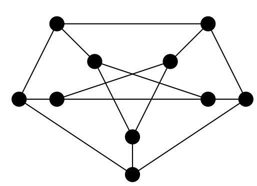


strongly regular
$k = 2$
$\lambda = 0$
$\mu = 1$



not strongly regular
$k = 2$
$\lambda = 0$

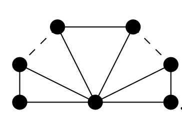
Example. The **Petersen graph**



is strongly regular of $k = 3, \lambda = 0, \mu = 1$.

Here is a famous friendship theorem. In a community where any two people have exactly one common acquaintance, there is someone who knows everyone. For the graph, vertices are people and join two people if they know each other. Theorem says that if any two vertices have exactly one common neighbour, then the graph is a windmill

Lecture 2
Tuesday
09/10/18



.

Many proofs, all use linear algebra.

0.3 Designs

Let v be varieties of cereal to be tested by consumers such that each consumer tests the same number k of varieties, and each variety is tested by the same number r of consumers.

Example. Let $v = 7, k = 3, r = 3$, and seven consumers $c_1, \dots, c_7$. Then

	c_1	c_2	c_3	c_4	c_5	c_6	c_7
varieties	123	145	356	167	257	347	246

is a design.

Let X be a set such that $|X| = v$ and $\mathcal{B}$ be a collection of subsets of X. Say $\mathcal{B}$ is a design with parameters v, k, r if each set in $\mathcal{B}$ has k elements, and each element of X lies in exactly r elements of $\mathcal{B}$. The elements of $\mathcal{B}$ are called blocks.

Example. The above

$$X = \{1, 2, 3, 4, 5, 6, 7\}, \qquad \mathcal{B} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{3, 5, 6\}, \{1, 6, 7\}, \{2, 5, 7\}, \{3, 4, 7\}, \{2, 4, 6\}\}$$

is a design with parameters $7, 3, 3$.

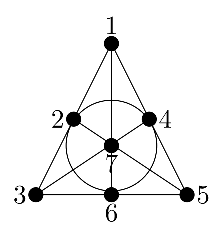
Designs are too common to be interesting. More interesting is each pair of varieties lies in the same number λ of blocks. A design $\mathcal{B}$ is a 2-design if every pair of points lies in the same number λ of blocks.

Example. The above design is a 2-design with $\lambda = 1$.

More generally, $\mathcal{B}$ is a t-design if every set of t elements is in the same number λ of blocks. 2-designs are common, and $t \geq 3$ less so. The first non-trivial 6-design, so not all k-sets are blocks, was only found in 1982.

Example. 2-designs from geometry.

- The **Fano plane**



  is the projective plane of order two. Projective planes exist for all powers of p for p prime.

- Let p be prime. Then $\mathbb{Z}_p = \{0, \dots, p-1\}$ is a field, since $(\mathbb{Z}_p, +)$ is a group, $\left(\mathbb{Z}_p^\times, \times\right)$ is a group, and $a(b+c) = ab + ac$. Define
$$\mathbb{Z}_p^2 = \{(x_1, x_2) \mid x_i \in \mathbb{Z}_p\},$$
  a plane with p^2 points. Define a line in $\mathbb{Z}_p^2$ to be the solutions of an equation $ax + by + c = 0$ for $a, b, c \in \mathbb{Z}_p$. Any two points are on a unique line. Let $X = \mathbb{Z}_p^2$ and $\mathcal{B}$ be lines. This is a 2-design with parameters
$$v = p^2, \qquad k = p, \qquad r = p + 1, \qquad \lambda = 1.$$

We will study

- constructions of t-designs,
- conditions on parameters, such as
  - if design parameters are v, k, r then easily $b = vr/k$, so $k \mid vr$ and $vr/k \leq \binom{v}{k}$,
  - in non-trivial 2-design, $b \geq v$, so $r \geq k$, by linear algebra, and
- links to codes and graphs.

1 Codes

1.1 Error-correcting codes

$\mathbb{Z}_2 = \{0, 1\}$ is a field, and

$$\mathbb{Z}_2^n = \{(x_1, \dots, x_n) \mid x_i \in \mathbb{Z}_2\}$$

is a vector space over $\mathbb{Z}_2$ with

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n), \qquad \lambda (x_1, \dots, x_n) = (\lambda x_1, \dots, \lambda x_n).$$

Example. In $\mathbb{Z}_2^4$, $0010 + 1010 = 1000$.

Definition. A **code** C of **length** n is a subset of $\mathbb{Z}_2^n$. The elements of C are called **codewords**. The **distance** between $x, y \in \mathbb{Z}_2^n$ is $\mathrm{d}(x, y)$, the number of places where x and y differ.

Example. $\mathrm{d}(01101, 10111) = 3$.

Proposition 1.1 (Triangle inequality)**.**

$$\mathrm{d}(x, y) + \mathrm{d}(y, z) \ge \mathrm{d}(x, z).$$

Proof. Let

$$A = \{i \mid x_i \ne z_i\}, \qquad B = \{i \mid x_i = y_i,\ x_i \ne z_i\}, \qquad C = \{i \mid x_i \ne y_i,\ x_i \ne z_i\}.$$

Then

$$\mathrm{d}(x, z) = |A|, \qquad |B| + |C| = |A|, \qquad |C| \le \mathrm{d}(x, y), \qquad |B| \le \mathrm{d}(y, z).$$

□

Lecture 3 Wednesday 10/10/18

Definition. The **minimum distance** of a code $C \subseteq \mathbb{Z}_2^n$ is

$$\mathrm{d}(C) = \min\{\mathrm{d}(x, y) \mid x, y \in C,\ x \ne y\}.$$

Say a code C corrects e errors if when $c \in C$ is sent and $w \in \mathbb{Z}_2^n$ is received, then c is the nearest codeword to w.

Definition. Let $e \ge 1$. Then C **corrects** e **errors** if for any $c_1, c_2 \in C$ and $w \in \mathbb{Z}_2^n$, $\mathrm{d}(c_1, w) \le e$ and $\mathrm{d}(c_2, w) \le e$ implies that $c_1 = c_2$. For an equivalent definition, let

$$\mathrm{S}_e(c) = \{w \in \mathbb{Z}_2^n \mid \mathrm{d}(c, w) \le e\}.$$

Then C corrects e errors if $\mathrm{S}_e(c) \cap \mathrm{S}_e(d) = \emptyset$ for any $c, d \in C$ such that $c \ne d$.

Proposition 1.2. *C corrects e errors if and only if* $\mathrm{d}(C) \ge 2e + 1$.

Proof.

$\implies$ Sheet 1. [1]

$\impliedby$ Suppose $\mathrm{d}(C) \ge 2e + 1$. Suppose $c_1, c_2 \in C$ and $w \in \mathbb{Z}_2^n$ where $\mathrm{d}(c_1, w) \le e$ and $\mathrm{d}(c_2, w) \le e$. Then $\mathrm{d}(c_1, c_2) \le 2e$ by 1.1, so $c_1 = c_2$. Thus C corrects e errors.

□

[1] Exercise

1.2 Linear codes

1.2.1 Linear codes

Definition. A code $C \subseteq \mathbb{Z}_2^n$ is **linear** if it is a subspace of $\mathbb{Z}_2^n$. That is

- $0 \in C$, and
- $x, y \in C$ implies that $x + y \in C$.

Proposition 1.3. *Let A be an $m \times n$ matrix over $\mathbb{Z}_2$. Then*

$$C = \{x \in \mathbb{Z}_2^n \mid Ax^{\mathsf{T}} = 0\}$$

is a linear code of dimension $n - \operatorname{rk} A$.

Proof. By first year linear algebra. ☐

Example. The code

$$\mathrm{C}_3 = \{abcxyz \mid x = a + b,\ y = a + c,\ z = b + c\} = \left\{ x \in \mathbb{Z}_2^6 \;\middle|\; \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} x^{\mathsf{T}} = 0 \right\} \subseteq \mathbb{Z}_2^6$$

is linear. This is the **triple check code**, where messages are a, b, c and check bits are x, y, z. Then $\dim \mathrm{C}_3 = 3$ and a basis is

$$100110, \qquad 010101, \qquad 001011.$$

Proposition 1.4. *Let $C \subseteq \mathbb{Z}_2^n$ be a linear code. If $k = \dim C$, then $|C| = 2^k$.*

Proof. A basis for C is $c_1, \dots, c_k$. Every $c \in C$ has the form $\lambda_1 c_1 + \dots + \lambda_k c_k$ for some $\lambda_i = 0, 1$. There are 2^k such expressions. ☐

1.2.2 Minimum distance

Definition. For $x \in \mathbb{Z}_2^n$, the **weight** of x is the number of non-zero entries of x. Denote it by $\operatorname{wt} x$.

Note. $\operatorname{wt} x = \mathrm{d}(x, 0)$.

Example. 1101 has weight three.

Proposition 1.5. *If C is a linear code, then*

$$\mathrm{d}(C) = \min \{\operatorname{wt} c \mid c \in C,\ c \neq 0\}.$$

Proof. Let $0 \neq c \in C$ be of minimum weight. Say $\operatorname{wt} c = r$. Then $0, c \in C$, so $\mathrm{d}(c, 0) = \operatorname{wt} c = r$, so $\mathrm{d}(C) \leq r$. For $x, y \in C$ with $x \neq y$, $\mathrm{d}(x, y) = \operatorname{wt}(x + y) \geq r$, since $x + y \in C$. Thus $\mathrm{d}(C) \geq r$. Thus $\mathrm{d}(C) = r$. ☐

Example. Let $\mathrm{C}_3 = \{abcxyz\}$. Then

$$\mathrm{d}(\mathrm{C}_3) = \min \{\operatorname{wt} c \mid c \in \mathrm{C}_3,\ c \neq 0\} = 3.$$

Thus C_3 corrects one error by 1.2.

The aims are to find linear codes C with

- large $\dim C$, so lots of codewords,
- large $\mathrm{d}(C)$, so corrects lots of errors, and
- small length of C, so save space.

1.2.3 Check matrix and error correction

Definition. If A is an $m \times n$ matrix over $\mathbb{Z}_2$ and C is the linear code $C = \{x \in \mathbb{Z}_2^n \mid Ax^\intercal = 0\}$, then we call A the **check matrix** of code C.

Remark. A check matrix always exists for a linear code.

Proposition 1.6. *Suppose a check matrix A for a linear code C has no zero column and no two columns are equal. Then C corrects one error.*

Proof. By 1.2, need to show $\mathrm{d}(C) \geq 3$. By 1.5, equivalent to show that the minimum weight is at least 3. Suppose for a contradiction that there exists $0 \neq c \in C$ such that $\mathrm{wt}\, c \leq 2$. If $\mathrm{wt}\, c = 1$, then

$$c = e_i = \begin{pmatrix} 0 \dots 0 & 1 & 0 \dots 0 \end{pmatrix},$$

so $0 = Ac^\intercal = Ae_i^\intercal = \mathrm{col}\, i$, a contradiction. If $\mathrm{wt}\, c = 2$, then $c = e_i + e_j$, so

$$0 = A\left(e_i^\intercal + e_j^\intercal\right) = Ae_i^\intercal + Ae_j^\intercal = \mathrm{col}\, i + \mathrm{col}\, j,$$

so $\mathrm{col}\, i = \mathrm{col}\, j$, a contradiction. $\square$

Example.

- The triple check code is

$$\mathrm{C}_3 = \left\{ x \in \mathbb{Z}_2^6 \;\middle|\; \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} x^\intercal = 0 \right\}.$$

  Thus C_3 corrects one error.

- Suppose we want a linear code with a $3 \times n$ check matrix A correcting one error. What is $\max(\dim C)$? By 1.6, take A to have all distinct columns in $\mathbb{Z}_2^3$,

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

  So $C \subseteq \mathbb{Z}_2^7$, $\dim C = 4, |C| = 16$, and

$$C = \{x_1 \dots x_7 \mid x_5 = x_1 + x_2 + x_3,\ x_6 = x_1 + x_2 + x_4,\ x_7 = x_1 + x_3 + x_4\}.$$

  Uses three check bits to encode messages x_1, x_2, x_3, x_4. A basis is

$$1000111, \qquad 0100110, \qquad 0010101, \qquad 0001011.$$

1.3 Hamming codes

1.3.1 Hamming codes

These are the best codes correcting one error. Lecture 4 Tuesday 16/10/18

Definition. Let $k \geq 2$. A **Hamming code** $\mathrm{Ham}\, k$ is a linear code whose check matrix has as columns all distinct non-zero vectors in $\mathbb{Z}_2^k$.

Example.

- $\mathrm{Ham}\, 3$ is the example before.
- $\mathrm{Ham}\, 4$ has check matrix

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

  Length is 15, dimension is 11, and four check bits for messages $x_1, \dots, x_{11}$.

Definition. Two linear codes are **equivalent** if one is obtained from the other by permuting coordinates, that is by permuting the columns of check matrix.

So all $\operatorname{Ham} k$'s are equivalent, and we say the Hamming code.

Proposition 1.7.

1. $\operatorname{Ham} k$ *corrects one error.*
2. $\operatorname{Ham} k$ *has length* $2^k - 1$ *and dimension* $2^k - k - 1$.

Proof.

1. Holds by 1.6.
2. The number of columns in $\mathbb{Z}_2^k \setminus \{0\}$ is $2^k - 1$, so check matrix A_k is $k \times \left(2^k - 1\right)$. Thus length is $2^k - 1$ and dimension is $2^k - 1 - \operatorname{rk} A_k = 2^k - 1 - k$.

□

1.3.2 Correcting one error

Suppose we have a linear code C with check matrix A, correcting one error. How do we correct one error? Suppose $c \in C$ is sent, obtain an error, say in i-th coordinate. So received vector is $c' = c + e_i$. Then

$$Ac'^{\intercal} = Ac^{\intercal} + Ae_i^{\intercal} = 0 + \operatorname{col} i.$$

So we correct i-th bit of c', where $Ac'^{\intercal} = \operatorname{col} i$.

Example. The triple check code has check matrix

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

Receive $c' = 100010$. Then $Ac'^{\intercal} = 100^{\intercal}$, so the fourth coordinate is wrong. Thus the correct codeword is $c = 100110$.

1.3.3 Correcting more than one error

Proposition 1.8. *Let* $d \in \mathbb{Z}_{\geq 2}$. *Let* C *be a linear code with check matrix* A. *Suppose that any* $d - 1$ *columns of* A *are linearly independent. Then*

1. $\mathrm{d}(C) \geq d$, *and*
2. *if there exists* d *linearly dependent columns, then* $\mathrm{d}(C) = d$.

Note. Agrees with 1.6.

Proof.

1. Suppose $\mathrm{d}(C) \leq d - 1$. By 1.5, there exists $0 \neq c \in C$ with $\operatorname{wt} c = r \leq d - 1$. So $c = e_{i_1} + \dots + e_{i_r}$. Then
$$0 = Ac^{\intercal} = Ae_{i_1}^{\intercal} + \dots + Ae_{i_r}^{\intercal} = \operatorname{col} i_1 + \dots + \operatorname{col} i_r.$$
By assumption, these r columns are linearly independent, a contradiction. Thus $\mathrm{d}(C) \geq d$.
2. Say columns $i_1, \dots, i_d$ are linearly dependent. By assumption, no fewer columns are dependent. Hence
$$0 = \operatorname{col} i_1 + \dots + \operatorname{col} i_d = A\left(e_{i_1} + \dots + e_{i_d}\right)^{\intercal}.$$
So $c = e_{i_1} + \dots + e_{i_d} \in C$ and $\operatorname{wt} c = d$.

□

Example. Find a linear code C of length nine, dimension two, correcting two errors. Want 7×9 check matrix A, of rank seven. Can do row operations and permute columns to put A in the form

$$A = \begin{pmatrix} & & 1 & & 0 \\ c_1 & c_2 & & \ddots & \\ & & 0 & & 1 \end{pmatrix}.$$

Need $\mathrm{d}(C) \geq 5$ to correct two errors. Need any four columns of A to be linearly independent. Need

1. $\mathrm{wt}\, c_1 \geq 4$, else c_1 is the sum of at most three e_i's, a contradiction, and
2. $\mathrm{wt}\,(c_1 + c_2) \geq 3$, else c_1 is the sum of at most two e_i's, a contradiction.

Given 1 and 2, any four columns will be linearly independent. Thus

$$c_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}^\intercal, \qquad c_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}^\intercal,$$

so

$$C = \{abaaa\,(a+b)\,bbb \mid a, b \in \mathbb{Z}_2\} = \{000000000, 101111000, 010001111, 111110111\}$$

has dimension two, length nine, and corrects two errors.

1.3.4 Hamming bound

Recall that for $v \in \mathbb{Z}_2^n$ and $e \geq 1$, $\mathrm{S}_e(v) = \{w \in \mathbb{Z}_2^n \mid \mathrm{d}(w, v) \leq e\}$.

Proposition 1.9.

$$|\mathrm{S}_e(v)| = \binom{n}{0} + \cdots + \binom{n}{e}.$$

Proof. $|\mathrm{S}_e(v)| = d_0 + \cdots + d_e$, where d_i is the number of vectors $w \in \mathbb{Z}_2^n$ such that $\mathrm{d}(v, w) = i$. The vector distance i from v are those where we change i of the coordinates. Thus $d_i = \binom{n}{i}$. ☐

Theorem 1.10 (Hamming bound)**.** *If $C \in \mathbb{Z}_2^n$ corrects e errors, then*

$$|C| \leq \frac{2^n}{\binom{n}{0} + \cdots + \binom{n}{e}}.$$

Lecture 5 Tuesday 16/10/18

Proof. By definition, the spheres $\mathrm{S}_e(c)$ for $c \in C$ are disjoint. So

$$\left| \bigcup_{c \in C} \mathrm{S}_e(c) \right| = |C| |\mathrm{S}_e(c)| = |C| \left(\binom{n}{0} + \cdots + \binom{n}{e} \right),$$

by 1.9. Of course, $\left| \bigcup_{c \in C} \mathrm{S}_e(c) \right| \leq 2^n$. Thus $|C| \left(\binom{n}{0} + \cdots + \binom{n}{e} \right) \leq 2^n$. ☐

Example. Let C be a linear code of length nine correcting two errors. What is $\max(\dim C)$? By 1.10,

$$|C| \leq \frac{2^9}{\binom{9}{0} + \binom{9}{1} + \binom{9}{2}} = \frac{512}{46} < 12.$$

Then $|C| = 2^{\dim C}$, since C is linear. So $\dim C \leq 3$.

The previous example is that there exists C of dimension two. Does there exist C of dimension three? Need 6×9 check matrix, of rank six. Then

$$A = \begin{pmatrix} & & & 1 & & 0 \\ c_1 & c_2 & c_3 & & \ddots & \\ & & & 0 & & 1 \end{pmatrix},$$

with any four columns linearly independent. So need

- $\operatorname{wt} c_i \geq 4$,
- $\operatorname{wt}(c_i + c_j) \geq 3$, and
- $\operatorname{wt}(c_1 + c_2 + c_3) \geq 2$.

Do such codewords exist?

1.3.5 Perfect codes

If $C \subseteq \mathbb{Z}_2^n$ corrects e errors, then spheres $\mathrm{S}_e(c)$ for $c \in C$ are disjoint and $\bigcup_{c \in C} \subseteq \mathbb{Z}_2^n$. Equality is interesting.

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

$$|C| = \frac{2^n}{\binom{n}{0} + \dots + \binom{n}{e}}.$$

Equivalently, $\mathbb{Z}_2^n$ is a disjoint union of spheres $\mathrm{S}_e(c)$ for $c \in C$.

Proposition 1.11. *Let $C \subseteq \mathbb{Z}_2^n$. Then $|C| = 2^n / (n+1)$ if and only if $n = 2^k - 1$ and $|C| = 2^{n-k}$ for some k.*

Proof.

$\Longrightarrow$ Suppose $|C| = 2^n / (n+1)$. Then $n + 1 = 2^k$ for some k. Then $|C| = 2^{n-k}$ and $n = 2^k - 1$.

$\Longleftarrow$ Suppose $n = 2^k - 1$ and $|C| = 2^{n-k}$ for some k. Then $|C| = 2^n/2^k = 2^n / (n+1)$.

∎

Example. $\operatorname{Ham} k$ is 1-perfect by 1.7, since length is $2^k - 1$ and dimension is $2^k - k - 1 = (2^k - 1) - k$.

Are there any more perfect codes? If C is e-perfect then

$$\binom{n}{0} + \dots + \binom{n}{e} = 2^k,$$

which is rare.

Example. Let $e = 2$. Then

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} = 2^k,$$

so $n^2 + n + 2 = 2^{k+1}$, which is rare.

The following is a famous theorem, by van Lint-Tietavainen in 1973. The only e-perfect codes C for $e \geq 1$ and $|c| > 1$ are

- $e = 1$ and $C = \operatorname{Ham} k$,
- $n = 2e + 1$, $\dim C = 1$, and $C = \{0 \dots 0, 1 \dots 1\}$, and
- $e = 3$, $n = 23$, and $\dim C = 12$ is the Golay code, which is a miracle, since

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2048 = 2^{11}.$$

1.3.6 Gilbert-Varshamov bound

Example. Let C be a linear code of length 15 correcting two errors. What is the largest possible $\dim C$? By the Hamming bound,

$$|C| \le \frac{2^{15}}{\binom{15}{0}+\binom{15}{1}+\binom{15}{2}} = \frac{2^{15}}{121} < 2^9.$$

So $\dim C \le 8$. This is a negative result. There are no such codes of dimension at least nine. What about positive results?

Theorem 1.12 (G-V bound)**.** *Let $n, k, d \in \mathbb{Z}$, where $2 \le d \le n$ and $1 \le k \le n$, such that*

$$\binom{n-1}{0} + \dots + \binom{n-1}{d-2} < 2^{n-k}. \qquad (1)$$

Then there exists a linear code C of length n and dimension l with $\mathrm{d}(C) \ge d$.

Example. Let $C \subseteq \mathbb{Z}_2^{15}$ correcting two errors. Want $\mathrm{d}(C) \ge 5$. Putting $n = 15$ and $d = 5$ into (1),

$$\binom{14}{0} + \binom{14}{1} + \binom{14}{2} + \binom{14}{3} = 1 + 14 + 91 + 364 < 512 = 2^9 = 2^{15-6}.$$

So by 1.12, there exists such a C with $\dim C = 6$. Does there exist C of dimension seven or eight? 1.12 says nothing.

A warning is do not use the G-V bound to prove non-existence.

Proof. Need to find check matrix A satisfying

1. A is $(n-k) \times n$ matrix of rank $n-k$, and
2. any $d-1$ columns of A are linearly independent, using 1.8.

We construct A inductively, adding one column at a time, satisfying 2 at each step. Start with $n-k$ columns $e_1, \dots, e_{n-k} \in \mathbb{Z}_2^{n-k}$. Write $c_i = e_i$. Now suppose we have i columns $c_1, \dots, c_i$, where $n-k \le i \le n-1$. Let $A_1 = \begin{pmatrix} c_1 & \dots & c_i \end{pmatrix}$ be $(n-k) \times i$, with any $d-1$ columns linearly independent. The number of vectors in $\mathbb{Z}_2^{n-k}$ in the span of at most $d-2$ of $c_1, \dots, c_i$ is at most $N_i = \binom{i}{0} + \dots + \binom{i}{d-2}$. Since $i \le n-1$, $N_i < 2^{n-k}$ by hypothesis (1). Hence there exists a vector $c_{i+1} \in \mathbb{Z}_2^{n-k}$ that is not in the span of at most $d-2$ of $c_1, \dots, c_i$. Let $A_{i+1} = \begin{pmatrix} c_1 & \dots & c_{i+1} \end{pmatrix}$. Then any $d-1$ columns of A_{i+1} are linearly independent. This process constructs $A_{n-k}, \dots, A_n$. So $A = A_n$ satisfies 1 and 2, as required. $\square$

1.4 The Golay code

Lecture 6 Wednesday 17/10/18

This is the famous 3-perfect code of length 23 and dimension 12. First we will construct the extended Golay code $\mathrm{G}_{24} \subseteq \mathbb{Z}_2^{24}$.

1.4.1 Construction of G_{24}

Start with $H = \mathrm{Ham}\, 3$, so check matrix is

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

Form **reverse** code K, with check matrix

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

Add parity check to H and K, so sum of bits, to get length eight codes H' and K',

$$H' = \left\{ \begin{array}{c} 00000000, 10001110, 10110010, 11010100, 11101000, 01011010, 01100110, 00111100 \\ 11111111, 01110001, 01001101, 00101011, 00010111, 10100101, 10011001, 11000011 \end{array} \right\},$$

$$K' = \left\{ \begin{array}{c} 00000000, 11100010, 10011010, 01010110, 00101110, 10110100, 11001100, 01111000 \\ 11111111, 00011101, 01100101, 10101001, 11010001, 01001011, 00110011, 10000111 \end{array} \right\}.$$

Note.

- H' and K' are linear of length eight and dimension four.
- All codewords of H' and K' have weight zero, four, or eight.
- The 14 weight four codewords in H' form a 3-design.

Proposition 1.13.

$$H \cap K = \{0000000, 1111111\}, \qquad H' \cap K' = \{00000000, 11111111\}.$$

Proof. Let $v \in H \cap K$. Then $v \in H$, so

$$v = abcd\,(a+b+c)\,(a+b+d)\,(a+c+d), \qquad a, b, c, d \in \mathbb{Z}_2.$$

So $v \in K$, so

- $c + (a+b+c) + (a+b+d) + (a+c+d) = 0$, so $a + c = 0$,
- $b + d + (a+b+d) + (a+c+d) = 0$, so $c + d = 0$, and
- $a + d + (a+b+c) + (a+c+d) = 0$, so $a + b = 0$.

Thus $a = b = c = d$, so $v = 0000000$ or $v = 1111111$. ☐

Definition. The **extended Golay code** G_{24} consists of all vectors in $\mathbb{Z}_2^{24}$ of the form

$$(a+x)\,(b+x)\,(a+b+x), \qquad a, b \in H', \qquad x \in K'.$$

Example. Some codewords in G_{24}.

- $0^{24} \in \mathrm{G}_{24}$.
- $a = b = 0^8$ and $x = 1^8$, so $1^{24} \in \mathrm{G}_{24}$.
- $a = x = 1^8$ and $b = 0^8$, so $0^8 1^8 0^8 \in \mathrm{G}_{24}$.
- $a = 10001110, b = 10011001, x = 01001011$, so $110001011101001001011100 \in \mathrm{G}_{24}$.

Proposition 1.14. G_{24} *is a linear code of dimension* 12.

Proof. Linear, since $0^{24} \in \mathrm{G}_{24}$ and

$$\begin{aligned} &(a_1+x_1)\,(b_1+x_1)\,(a_1+b_1+x_1) + (a_2+x_2)\,(b_2+x_2)\,(a_2+b_2+x_2) \qquad a_i, b_i \in H', \qquad x_i \in K' \\ &= (a_1+a_2+x_1+x_2)\,(b_1+b_2+x_1+x_2)\,(a_1+a_2+b_1+b_2+x_1+x_2) \in \mathrm{G}_{24}, \end{aligned}$$

since $a_1 + a_2, b_1 + b_2 \in H'$ and $x_1 + x_2 \in K'$. For dimension, suppose

$$(a_1+x_1)\,(b_1+x_1)\,(a_1+b_1+x_1) = (a_2+x_2)\,(b_2+x_2)\,(a_2+b_2+x_2), \qquad a_i, b_i \in H', \qquad x_i \in K'.$$

Then

1. $a_1 + x_1 = a_2 + x_2$,
2. $b_1 + x_1 = b_2 + x_2$, and
3. $a_1 + b_1 + x_1 = a_2 + b_2 + x_2$.

1 and 2 implies that $a_1 + b_1 = a_2 + b_2$. Substituting in 3, $x_1 = x_2$, so 1 and 2 implies that $a_1 = a_2$ and $b_1 = b_2$. Thus distinct choices of triple abx give distinct codewords in G_{24}. Thus $|\mathrm{G}_{24}|$ is the number of triples abx, which is $2^4 \cdot 2^4 \cdot 2^4 = 2^{12}$. Thus G_{24} has dimension 12. ☐

1.4.2 Basis

$$(a+x)(b+x)(a+b+x) = a0^8a + 0^8bb + xxx.$$

These are in G_{24}. If a_i, b_i, c_i for $1 \le i \le 4$ are bases of H' and K' then a basis of G_{24} is

$$a_i 0^8 a_i, \qquad 0^8 b_i b_i, \qquad x_i x_i x_i, \qquad 1 \le i \le 4.$$

Thus

$$H' = \mathrm{sp}(a_1, a_2, a_3, a_4) = \mathrm{sp}(b_1, b_2, b_3, b_4), \qquad K' = \mathrm{sp}(x_1, x_2, x_3, x_4).$$

1.4.3 Minimum distance

Theorem 1.15. G_{24} *has minimum distance* $\mathrm{d}(\mathrm{G}_{24}) = 8$.

This will take a few steps to prove. For $v, w \in \mathbb{Z}_2^n$, define $[v, w]$ as the number of places where v and w both have one.

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

1. $\mathrm{wt}(v+w) = \mathrm{wt}\, v + \mathrm{wt}\, w - 2[v, w]$.
2. *Suppose* $4 \mid \mathrm{wt}\, v$ *and* $4 \mid \mathrm{wt}\, w$. *Then* $4 \mid \mathrm{wt}(v+w)$ *if and only if* $[v, w]$ *is even.*

Proof.

1. Let $r = \mathrm{wt}\, v, s = \mathrm{wt}\, w, t = [v, w]$. Reordering the coordinates, we get

$$\begin{array}{rcccc} v = & \overbrace{1\dots1}^{t} & \overbrace{1\dots1}^{r-t} & \overbrace{0\dots0}^{s-t} & 0\dots0 \\ w = & 1\dots1 & 0\dots0 & 1\dots1 & 0\dots0 \\ v+w = & 0\dots0 & 1\dots1 & 1\dots1 & 0\dots0 \end{array}.$$

   Thus $\mathrm{wt}(v+w) = r + s - 2t$.

2. Follows from 1.

$\square$

Lecture 7 Tuesday 23/10/18

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

Proof. Let $r = [a, x]$ and $s = [b, x]$. Reordering coordinates,

$$\begin{array}{rccccc} x = & \overbrace{1\dots1}^{u} & \overbrace{1\dots1}^{s-u} & \overbrace{1\dots1}^{r-u} & 1\dots1 & 0\dots0 \\ a = & 1\dots1 & 1\dots1 & 0\dots0 & 0\dots0 & \dots \\ b = & 1\dots1 & 0\dots0 & 1\dots1 & 0\dots0 & \dots \\ a+b = & 0\dots0 & 1\dots1 & 1\dots1 & 0\dots0 & \dots \end{array}.$$

Then $[a, x] + [b, x] + [a+b, x] = r + s + r - u + s - u = 2(r + s - u)$. $\square$

Proposition 1.18. *If* $c \in \mathrm{G}_{24}$ *then* $4 \mid \mathrm{wt}\, c$.

Proof. Let

$$c = (a+x)(b+x)(a+b+x) = ab(a+b) + xxx = v + w, \qquad a, b \in H', \qquad x \in K'.$$

Then $a, b, a+b \in H'$ and $x \in K'$, so $4 \mid \mathrm{wt}\, v$ and $4 \mid \mathrm{wt}\, w$, and $[v, w] = [a, x] + [b, x] + [a+b, x]$ is even by 1.17. So $4 \mid \mathrm{wt}(v+w) = \mathrm{wt}\, c$ by 1.16. $\square$

Proof of 1.15. Suppose $\mathrm{d}(\mathrm{G}_{24}) < 8$. By 1.18, there exists $0 \neq c \in \mathrm{G}_{24}$ such that $\mathrm{wt}\, c = 4$, so

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

By 1.16, $\mathrm{wt}(a + x) = \mathrm{wt}\, a + \mathrm{wt}\, x - 2[a, x]$, so $\mathrm{wt}(a + x)$ is even. Similarly, $\mathrm{wt}(b + x)$ and $\mathrm{wt}(a + b + x)$ are even. One of $a+x, b+x, a+b+x$ must be zero since $\mathrm{wt}\, c = 4$. That is, $x = a, b, a+b$, so $x \in H' \cap K' = \left\{0^8, 1^8\right\}$, by 1.13. Now $a + x, b + x, a + b + x \in H'$, so have weight zero, four, or eight. As $\mathrm{wt}\, c = 4$, two of $a + x, b + x, a + b + x$ are zero. That is, x is two of $a, b, a + b$, and the other is then zero. The following are the possibilities.

- $a = b = x$ and $a + b = 0$, so $c = 0^8 0^8 x$.
- $a = a + b = x$ and $b = 0$, so $c = 0^8 x 0^8$.
- $b = a + b = x$ and $a = 0$, so $c = x 0^8 0^8$.

So $\mathrm{wt}\, c = 0$ or $\mathrm{wt}\, c = 8$, a contradiction. Thus $\mathrm{d}(\mathrm{G}_{24}) \geq 8$. As there exists $c \in \mathrm{G}_{24}$ of weight eight, $\mathrm{d}(\mathrm{G}_{24}) = 8$. ☐

Theorem 1.19. *The extended Golay code* G_{24} *has length* 24*, dimension* 12*, and minimum distance eight.*

1.4.4 Construction of G_{23}

Definition. The **Golay code** $\mathrm{G}_{23} \subseteq \mathbb{Z}_2^{23}$ is the codewords of G_{24} with the last bit removed.

As G_{24} is a linear code, so is G_{23}. Also, $|\mathrm{G}_{23}| = |\mathrm{G}_{24}| = 2^{12}$ so $\dim \mathrm{G}_{23} = 12$.

Theorem 1.20. G_{23} *is* 3*-perfect.*

Proof.

- 3-error correcting, that is want $\mathrm{d}(\mathrm{G}_{23}) \geq 7$. Since G_{23} has the codeword $0^8 0^8 1^7$ for $a = b = x = 1^8$, $\mathrm{d}(\mathrm{G}_{23}) \leq 7$. Since $\mathrm{d}(\mathrm{G}_{24}) = 8$, $\mathrm{d}(\mathrm{G}_{23}) \geq 7$. Thus $\mathrm{d}(\mathrm{G}_{23}) = 7$ and 3-error correcting.
- Then
$$|\mathrm{G}_{23}| = 2^{12} = \frac{2^{23}}{\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}}.$$
Thus G_{23} is 3-perfect.

☐

Proposition 1.21.

1. *Codewords in* G_{24} *have weights* $0, 8, 12, 16, 24$. *If* N_i *is the number of codewords of weight* i*, then* $N_i = N_{24-i}$.
2. *Codewords in* G_{23} *have weights* $0, 7, 8, 11, 12, 15, 16, 23$. *If* M_i *is the number of codewords of weight* i*, then* $M_i = M_{23-i}$.
3. *Codewords in* G_{24} *are those of* G_{23} *with a parity check bit* $x_{24} = x_1 + \dots + x_{23}$ *added.*

Proof.

1. By 1.18, $4 \mid \mathrm{wt}\, c$ for all $c \in \mathrm{G}_{24}$, and $\mathrm{wt}\, c \geq 8$ by 1.15. Also, $1^{24} \in \mathrm{G}_{24}$, so there is a bijection $x \mapsto x + 1^{24}$, from the codewords of weight i, to the codewords of weight $24 - i$, so $N_i = N_{24-i}$, so there are codewords of weights $0, 24, 8, 16$. Last time in example we saw codeword of weight 12. No codewords of weight 20 since no codewords of weight 4.
2. There are codewords of weights 0 and 23. Since G_{24} has $0^8 1^8 0^8$, there are codewords of weights 8 and 15 in G_{23}. Since G_{24} has $0^8 0^8 1^8$, there are codewords of weights 7 and 16 in G_{23}. Since G_{24} has codewords of weight 12, there are codewords of weights 11 and 12.
3. This follows from the fact that all weights in G_{24} are even.

☐

1.4.5 The 5-design associated with G_{24}

How do we calculate N_i and M_i? The best way is via the following. Recall that a t-design with parameters (v, k, r_t), or a t-(v, k, r_t) design, is a pair $(X, \mathcal{B})$ where X is a set of v points and $\mathcal{B}$ is a collection of subsets of X of size k called blocks such that every set of t points lies in exactly r_t blocks. To avoid degeneracy cases, assume $X, \mathcal{B} \neq \emptyset$ and $v \geq k \geq t$, so $r_t > 0$. Use the codewords of weight eight in G_{24} to define a t-design for $t = 5$. Let $X = \{1, \dots, 24\}$. Let

$$\mathrm{B}_c = \{i \in X \mid c(i) = 1\}, \qquad c \in \mathrm{G}_{24}, \qquad \mathrm{wt}\, c = 8, \qquad \mathcal{B} = \{\mathrm{B}_c \mid c \in C, \ \mathrm{wt}\, c = 8\},$$

so $N_8 = |\mathcal{B}|$. These blocks are called **octads**.

Example. Let $c = 1^8 0^8 0^8$. Then $\mathrm{B}_c = \{1, \dots, 8\}$.

Lecture 8 Tuesday 23/10/18

Theorem 1.22. *$(X, \mathcal{B})$ is a 5-$(24, 8, 1)$ design.*

Proof. Prove $r_t = 1$. There is a bijection

$$\{ \text{ vectors } v \text{ in } \mathbb{Z}_2^n \ \} \qquad \leftrightsquigarrow \qquad \{ \text{ subsets } S_v = \{i \in X \mid v(i) = 1\} \text{ of } X = \{1, \dots, n\} \ \}.$$

Let $v \in \mathbb{Z}_2^{24}$ such that $\mathrm{wt}\, v = 5$, that is $|S_v| = 5$. The aim is to show there exists a unique $c \in \mathrm{G}_{24}$ of weight eight such that $S_v \subseteq S_c = \mathrm{B}_c$. Delete the last bit of v to get $v' \in \mathbb{Z}_2^{23}$. Then $\mathrm{wt}\, v' = 4$ or $\mathrm{wt}\, v' = 5$. As G_{23} is 3-perfect, there exists a unique $c' \in \mathrm{G}_{23}$ such that $\mathrm{d}(v', c') \leq 3$.

- If $\mathrm{wt}\, v' = 4$, then $\mathrm{wt}\, c' = 7$ and $S_{v'} \subseteq S_{c'}$, so $v = v'1$ and $c = c'1 \in \mathrm{G}_{24}$. Thus $S_v \subseteq S_c$.
- If $\mathrm{wt}\, v' = 5$, then $\mathrm{wt}\, c' = 7$ or $\mathrm{wt}\, c' = 8$ and $S_{v'} \subseteq S_{c'}$, so $v = v'0$ and either $c = c'0 \in \mathrm{G}_{24}$ if $\mathrm{wt}\, c' = 8$, or $c = c'1 \in \mathrm{G}_{24}$ if $\mathrm{wt}\, c' = 7$. Then $S_v \subseteq S_c$.

Suppose there exists c_0 such that $\mathrm{wt}\, c_0 = 8$ and $S_v \subseteq S_{c_0}$. Well, $[c, c_0] \geq 5$, since $S_v \subseteq S_c \cap S_{c_0}$. So

$$\mathrm{wt}(c + c_0) = \mathrm{wt}\, c + \mathrm{wt}\, c_0 - 2[c, c_0] \leq 8 + 8 - 10 = 6.$$

But $c + c_0 \in \mathrm{G}_{24}$ and $\mathrm{d}(\mathrm{G}_{24}) = 8$. Thus $c = c_0$. $\square$

Using this design, we can obtain lots of information about G_{23} and G_{24}, such as N_i and M_i. We need some design theory.

Proposition 1.23. *Let $(X, \mathcal{B})$ be a t-(v, k, r_t) design. Then $(X, \mathcal{B})$ is also a $(t-1)$-(v, k, r_{t-1}) design, where*

$$r_{t-1} = \frac{v - t + 1}{k - t + 1} r_t.$$

Proof. Let $S \subseteq X$ with $|S| = t - 1$. Let $r(S)$ be the number of blocks containing S. Let N be the number of pairs (x, B) where $x \in X \setminus S$ and B is a block such that $S \cup \{x\} \subseteq B$. Then

$$N = (\text{the number of points in } X \setminus S) \times (\text{the number of blocks } B \text{ containing } S \cup \{x\}) = (v - t + 1) r_t,$$

and

$$N = (\text{the number of } B \text{ containing } S) \times (\text{the number of } x \text{ in } B \setminus S) = r(S)(k - t + 1).$$

Thus

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

$\square$

Corollary 1.24. *A t-(v, k, r_t) design is an s-(v, k, r_s) design for all $0 \leq s \leq t - 1$ where*

$$r_{t-1} = \frac{v - t + 1}{k - t + 1} r_t, \qquad \dots, \qquad r = r_1 = \frac{v - 1}{k - 1} r_2, \qquad b = r_0 = \frac{v}{k} r_1.$$

Applying this to the 5-design from G_{24},

$$r_5 = 1, \qquad r_4 = \frac{20}{4}(1) = 5, \qquad r_3 = \frac{21}{5}(5) = 21, \qquad r_2 = \frac{22}{6}(21) = 77,$$

$$r = r_1 = \frac{23}{7}(77) = 253, \qquad b = r_0 = \frac{24}{8}(253) = 759.$$

Proposition 1.25.

1. *In G_{24}, the number of codewords of weight eight is $N_8 = 759$.*
2. *In G_{23}, the number of codewords of weights seven and eight are $M_7 = 253$ and $M_8 = 506$.*

Proof.

1. N_8 is the number of octads, which is $b = 759$.
2. $c' \in \mathrm{G}_{23}$ has weight seven if and only if $c' + e_{24} \in \mathrm{G}_{24}$ has weight eight. So M_7 is the number of octads containing one, which is $r_1 = 253$, and $M_8 = N_8 - M_7 = 759 - 253 = 506$.

$\square$

The other values N_{12}, M_{11}, M_{12} are in sheet 2. [2]

1.4.6 Check matrix

Observe that the dot product on $\mathbb{Z}_2^n$ is $x \cdot y = xy^\intercal \in \mathbb{Z}_2$.

Proposition 1.26. *For all $c, d \in \mathrm{G}_{24}$, $c \cdot d = 0$.*

Proof. $\mathrm{wt}\,(c+d) = \mathrm{wt}\,c + \mathrm{wt}\,d - 2\,[c,d]$. As $4 \mid \mathrm{wt}\,c, \mathrm{wt}\,d, \mathrm{wt}\,(c+d)$, $[c,d]$ is even. Hence $c \cdot d = cd^\intercal = [c,d] = 0$. $\square$

Let $b_1, \dots, b_{12}$ be a basis of G_{24}. Take

$$A = \begin{pmatrix} b_1 \\ \vdots \\ b_{12} \end{pmatrix},$$

a 12×24 matrix, since for all $c \in \mathrm{G}_{24}$, by 1.26, $Ac^\intercal = 0$.

1.4.7 Error correction

Suppose a codeword c is sent and t errors are made, where $1 \le t \le 3$. So the received vector is

$$x = c + e_{i_1} + \dots + e_{i_t} \in \mathbb{Z}_2^{24}.$$

To see if x_1 is correct, there are 253 codewords in G_{24} of weight eight with one in the first coordinate. Call them $c_1, \dots, c_{253}$. Let the corresponding octads be $\mathrm{B}_1, \dots, \mathrm{B}_{253}$. That is, those containing one. Consider the dot products $x \cdot c_i$ for $1 \le i \le 253$. If x were in G_{24}, then $x \cdot c_i = 0$ for all i. But $x \notin \mathrm{G}_{24}$. We count how many of these are one.

Proposition 1.27. *The number of dot products $x \cdot c_i$ equal to one is*

t	x_1 *correct*	x_1 *incorrect*
1	77	253
2	112	176
3	125	141

Hence the number tells whether x_1 is correct. Lecture 9 Wednesday 24/10/18

[2] Exercise

Proof. Let L be the number of $x \cdot c$ that equal one.

$t = 1$. Here $x = c + e_k$. If x_1 is correct, then $1 \neq k$, so

$$x \cdot c_i = e_k \cdot c_i = \begin{cases} 1 & k \in \mathrm{B}_i \\ 0 & k \notin \mathrm{B}_i \end{cases}.$$

Thus L is the number of i such that $k \in \mathrm{B}_i$, which is $r_2 = 77$, the number of octads containing 1 and k. If x_1 is incorrect, then $k = 1$, so $x \cdot c_i = e_1 \cdot c_i = 1$. Thus $L = r_1 = 253$.

$t = 2$. Let $x = c + e_k + e_l$. If x_1 is correct, then

$$x \cdot c_i = e_k \cdot c_i = e_l \cdot c_i = \begin{cases} 1 & k \in \mathrm{B}_i \text{ and } l \notin \mathrm{B}_i, \text{ or } k \notin \mathrm{B}_i \text{ and } l \in \mathrm{B}_i \\ 0 & \text{else} \end{cases},$$

so the number of i such that $k \in \mathrm{B}_i$ and $l \notin \mathrm{B}_i$ is $r_2 - r_3 = 77 - 21 = 56$. Thus $L = 56 + 56 = 112$. If x_1 is incorrect, then $x = c + e_1 + e_k$, so

$$x \cdot c_i = e_1 c_i + e_k c_i = 1 + \begin{cases} 1 & k \in \mathrm{B}_i \\ 0 & k \notin \mathrm{B}_i \end{cases} = \begin{cases} 0 & k \in \mathrm{B}_i \\ 1 & k \notin \mathrm{B}_i \end{cases}.$$

Thus L is the number of B_i not containing k, which is $r_1 - r_2 = 253 - 77 = 176$.

$t = 3$. Sheet 2. [3]

∎

1.5 Cyclic codes

1.5.1 Some ring theory

Recall that a **commutative ring** R has $+$ and $\times$ such that

- $(R, +)$ is an abelian group,
- $\times$ is commutative and associative, and
- $\times$ is distributive over $+$.

Example. The **polynomial ring** $\mathbb{Z}_2[x]$ is the ring of polynomials

$$f(x) = a_0 + \dots + a_n x^n, \qquad a_i \in \mathbb{Z}_2.$$

A subset $I \subseteq R$ is an **ideal** if I is a subgroup of $(R, +)$ and $IR \subseteq I$, that is $ir \in I$ for all $i \in I$ and $r \in R$.

Example. For $a \in R$,

$$I = \langle a \rangle = \{ar \mid r \in R\}$$

is a **principal ideal**. In $\mathbb{Z}_2[x]$, if $a = x^n - 1$ then

$$\langle a \rangle = \{(x^n - 1) f(x) \mid f(x) \in \mathbb{Z}_2[x]\}.$$

The **coset** of I in $(R, +)$ is

$$r + I = \{r + i \mid i \in I\},$$

and $r + I = s + I$ if and only if $r - s \in I$. Define the **quotient ring**

$$R/I = \{\text{cosets } r + I \mid r \in R\},$$

where addition and multiplication are

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I, \qquad (r_1 + I) + (r_2 + I) = (r_1 r_2) + I.$$

These are well-defined, and R/I is a ring. Our main example is the ring

$$\mathbb{Z}_2[x] / \langle x^n - 1 \rangle, \qquad n \in \mathbb{N}.$$

[3] Exercise

Example. Let $R = \mathbb{Z}_2[x]$ and $I = \langle x^2 - 1 \rangle$. Then

$$R/I = \{0 + I, 1 + I, x + I, x + 1 + I\},$$

so $x^2 + I = x^2 + (1 + x^2) + I = 1 + I$ and $x^3 + I = x(x^2) + I = x + I$. Writing $\overline{x} = x + I$,

$$R/I = \{0, 1, \overline{x}, \overline{x} + 1\},$$

so $\overline{x}(\overline{x} + 1) = \overline{x}^2 + \overline{x} = 1 + \overline{x}$, since $\overline{x}^2 = 1$.

Example. Let $R = \mathbb{Z}_2[x]$ and $I = \langle x^3 - 1 \rangle$. Then $\overline{x}(1 + \overline{x}^2) = \overline{x} + 1$.

In general is the following.

Proposition 1.28.

$$\mathbb{Z}_2[x] / \langle x^n - 1 \rangle = \left\{ a_0 + \dots + a_{n-1}\overline{x}^{n-1} \;\middle|\; a_i \in \mathbb{Z}_2 \right\}, \qquad \overline{x} = x + \langle x^n - 1 \rangle,$$

where multiplication is determined by $\overline{x}^n = 1$.

Hence there exists a bijection

$$\begin{array}{cccc} \pi & : & \mathbb{Z}_2^n & \longrightarrow & \mathbb{Z}_2[x] / \langle x^n - 1 \rangle \\ & & (a_0, \dots, a_{n-1}) & \longmapsto & a_0 + \dots + a_{n-1}\overline{x}^{n-1} \end{array}.$$

This is an isomorphism of groups.

1.5.2 Cyclic codes

Definition. A linear code $C \subseteq \mathbb{Z}_2^n$ is **cyclic** if $(x_1, \dots, x_n) \in C$ implies that $(x_n, x_1, \dots, x_{n-1}) \in C$, which implies all further shifts $(x_{n-1}, x_n, x_1, \dots, x_{n-2}) \in C$, etc.

Example.

- $C = \{000, 110, 101, 011\}$ is cyclic.
- Ham 3 is cyclic with check matrix

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

  since the shifted matrix

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

  gives the same code.
- G_{23} is equivalent to a cyclic code. Have to permute the coordinates.

Example. Let $C = \{000, 110, 101, 011\}$. Then

$$\pi(C) = \left\{0, 1 + \overline{x}, 1 + \overline{x}^2, \overline{x} + \overline{x}^2\right\} \subseteq \mathbb{Z}_2[x] / \left\langle x^3 - 1 \right\rangle.$$

Proposition 1.29. $C \subseteq \mathbb{Z}_2^n$ *is a cyclic linear code if and only if* $\pi(C)$ *is an ideal of* $\mathbb{Z}_2[x] / \langle x^n - 1 \rangle$.

Proof.

$\Longleftarrow$ Suppose $I = \pi(C)$ is an ideal. Then C is linear, since $c, d \in C$ implies that $\pi(c), \pi(d) \in I$, so $\pi(c) + \pi(d) = \pi(c + d) \in I$, so $c + d \in C$. Then C is cyclic, since letting $c = (c_0, \dots, c_{n-1}) \in C$ implies that $\pi(c) = c_0 + \dots + c_{n-1}\overline{x}^{n-1}$, so

$$\overline{x}\pi(c) = c_0\overline{x} + \dots + c_{n-1}\overline{x}^n = c_{n-1} + c_0\overline{x} + \dots + c_{n-2}\overline{x}^{n-1} = \pi((c_{n-1}, c_0, \dots, c_{n-2})),$$

so $(c_{n-1}, c_0, \dots, c_{n-2}) \in C$. So C is a cyclic linear code.

$\Longrightarrow$ Sheet 2. [4]

□

[4] Exercise

Lecture 10
Tuesday
30/10/18

Fact. $\mathbb{Z}_2[x]$ has a division algorithm. Given $f(x), g(x) \in \mathbb{Z}_2[x]$ such that $g \neq 0$, there exist $q(x), r(x) \in \mathbb{Z}_2[x]$ such that
$$f(x) = q(x)g(x) + r(x), \qquad \deg r < \deg g.$$

Definition. A polynomial $p(x) \in \mathbb{Z}_2[x]$ is **irreducible** if it cannot be factorised as a product of polynomials of smaller degree.

Example.

- $x^2 + 1 = (x+1)^2$ is not irreducible.
- $x^2 + x + 1$ is irreducible.
- $x^4 + x^2 + 1 = \left(x^2 + x + 1\right)^2$ is not irreducible, since $(a+b)^2 = a^2 + b^2$ for $a, b \in \mathbb{Z}_2[x]$.
- $x^4 + x + 1$ is irreducible.

Fact. Every polynomial in $\mathbb{Z}_2[x]$ is a unique product of irreducible polynomials, so can define **highest common factor** and **lowest common multiple** of polynomials in $\mathbb{Z}_2[x]$.

1.5.3 Construction

Fix $n \in \mathbb{N}$. Let $p(x) \in \mathbb{Z}_2[x]$ such that $p(x)$ divides $x^n - 1$. Have an ideal
$$\langle p(\overline{x}) \rangle = \{p(\overline{x}) f(\overline{x}) \mid f(\overline{x}) \in \mathbb{Z}_2[x] / \langle x^n - 1 \rangle\} \subseteq \mathbb{Z}_2[x] / \langle x^n - 1 \rangle, \qquad \overline{x} = x + \langle x^n - 1 \rangle.$$

Fact. Every ideal in $\mathbb{Z}_2[x] / \langle x^n - 1 \rangle$ arises in this way for some $\phi(x)$ dividing $x^n - 1$.

By 1.29, $\pi^{-1}(\langle p(\overline{x}) \rangle)$ is a cyclic linear code.

Example.

- Let $n = 3$. Then
$$x^3 - 1 = (x+1)\left(x^2 + x + 1\right).$$
Take $p(x) = x + 1$, so
$$\langle p(\overline{x}) \rangle = \left\{0, 1 + \overline{x}, 1 + \overline{x}^2, \overline{x} + \overline{x}^2\right\}.$$
This gives the cyclic code
$$C = \{000, 110, 011, 101\}.$$
- Let $n = 6$. Then
$$x^6 - 1 = (x+1)^2\left(x^2 + x + 1\right)^2.$$
So $x^6 - 1$ has nine possible divisors, so nine possible cyclic linear codes. Take
$$p(\overline{x}) = \left(\overline{x}^2 + \overline{x} + 1\right)^2 = \overline{x}^4 + \overline{x}^2 + 1,$$
so
$$C = \{000000, 101010, 010101, 111111\}.$$

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

Proposition 1.30. *If the generator polynomial has degree $n - k$, then* $\dim C = k$.

Proof. True if $k = 0$, that is $p(x) = x^n - 1$, so $C = \{0\}$. Assume $k \geq 1$. Claim that
$$p(\overline{x}), \ldots, \overline{x}^{k-1} p(\overline{x})$$
is a basis for $\pi(C)$.

- Linear independence.
$$\sum_{i=0}^{k-1} \lambda_i x^i p(x), \qquad \lambda_i \in \mathbb{Z}_2,$$
has degree less than n, so is not in $\langle x^n - 1 \rangle$ unless all $\lambda_i = 0$. Thus
$$\sum_{i=0}^{k-1} \lambda_i \overline{x}^i p(\overline{x}) = 0 \in \mathbb{Z}_2[x] / \langle x^n - 1 \rangle$$
implies that $\lambda_i = 0$.
- Span. The span of the given set is
$$\left\{ g(\overline{x}) p(\overline{x}) \mid g(\overline{x}) \in \mathbb{Z}_2[x] / \langle x^n - 1 \rangle \text{ of degree less than } k \right\}.$$
Need to show this is equal to
$$\left\{ f(\overline{x}) p(\overline{x}) \mid f(\overline{x}) \in \mathbb{Z}_2[x] / \langle x^n - 1 \rangle \right\}.$$
For $f(x) \in \mathbb{Z}_2[x]$, there exists $q(x), r(x)$ such that
$$f(x) p(x) = q(x)(x^n - 1) + r(x), \qquad \deg r < n.$$
Then $p(x)$ divides $r(x)$, so $r(x) = p(x) g(x)$ for some g, so $\deg g + n - k < n$, so $\deg g < k$. So $g(\overline{x}) p(\overline{x}) = f(\overline{x}) p(\overline{x})$.

□

Example. Let $n = 7$. Then
$$x^7 - 1 = (x + 1)\left(x^3 + x + 1\right)\left(x^3 + x^2 + 1\right).$$
Let $p(x) = x^3 + x + 1$. Then $\dim C = 4$ and a basis is
$$1101000, \qquad 0110100, \qquad 0011010, \qquad 0001101.$$

1.5.4 Check matrix

Let $p(x)$ divide $x^n - 1$, the generator polynomial for the cyclic linear code C. Assume $p(x) \neq x^n - 1$. Then
$$x^n - 1 = p(x) q(x), \qquad p(x) = p_0 + \cdots + p_{n-k} x^{n-k}, \qquad q(x) = q_0 + \cdots + q_k x^k, \qquad p_i, q_i \in \mathbb{Z}_2.$$
Basis of C is the rows of the $k \times n$ matrix
$$G = \begin{pmatrix} p_0 & \cdots & p_{n-k} & & 0 \\ & \ddots & \ddots & \ddots & \\ 0 & & p_0 & \cdots & p_{n-k} \end{pmatrix}.$$
This is the **generator matrix** of C. Define an $(n-k) \times n$ matrix
$$H = \begin{pmatrix} 0 & & q_k & \cdots & q_0 \\ & \iddots & \iddots & \iddots & \\ q_k & \cdots & q_0 & & 0 \end{pmatrix}.$$

Proposition 1.31. $HG^\intercal = 0$. *That is, H is the check matrix for C.*

Proof. Sheet 2. [5] □

Example. Let $n = 7$, and $p(x) = x^3 + x + 1$ and $q(x) = (x + 1)\left(x^3 + x^2 + 1\right)$. The check matrix is
$$H = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} = \mathrm{Ham}\, 3.$$

Lecture 11 is a class test.

Lecture 11 Tuesday 30/10/18

[5] Exercise

1.6 BCH codes

Lecture 12 Wednesday 31/10/18

This is a family of codes where we have good control of length, dimension, minimum distance, and error correction process.

1.6.1 Some more ring theory

Fact. For every $k \in \mathbb{Z}_{\geq 1}$, there exists a finite field of order 2^k. The construction is

$$\mathbb{F}_{2^k} = \mathbb{Z}_2[x] / \langle p_k(x) \rangle,$$

where $p_k(x)$ is irreducible of degree k.

Example. Let $\mathbb{F}_4 = \mathbb{Z}_2[x] / \langle x^2 + x + 1 \rangle$. Write $\alpha = x + \langle x^2 + x + 1 \rangle$. The elements of $\mathbb{F}_4$ are

$$\{0, 1, \alpha, \alpha + 1\}.$$

Example. Let $\mathbb{F}_8 = \mathbb{Z}_2[x] / \langle x^3 + x + 1 \rangle$. Write $\alpha = x + \langle x^3 + x + 1 \rangle$. The elements of $\mathbb{F}_8$ are

$$\{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}.$$

Fact. The multiplicative group $(\mathbb{F}_{2^k}^*, \times)$ is cyclic. That is, there exists $\beta \in \mathbb{F}_{2^k}$ such that $\mathbb{F}_{2^k}^* = \langle \beta \rangle$ and the order of β is $2^k - 1$. Call such a β a **primitive element**.

Example.

- $\mathbb{F}_4^* = \langle \alpha \rangle$, since $\alpha^2 = \alpha + 1$.
- $\mathbb{F}_8^* = \langle \alpha \rangle$.
- $\mathbb{F}_{16} = \mathbb{Z}_2[x] / \langle x^4 + x + 1 \rangle$. Let $\alpha = x + \langle x^4 + x + 1 \rangle$.
  - α is a primitive element, since α has order 15.
  - α^3 is not, since α^3 has order five.
  - $\alpha^5 = \alpha^2 + \alpha$ is not, since α^5 has order three.

Caution that $x + \langle p_k(x) \rangle$ is not necessarily a primitive element of $\mathbb{Z}_2[x] / \langle p_k(x) \rangle$.

Fact. Every element $\gamma \in \mathbb{F}_{2^k}^*$ has a **minimal polynomial**, which is a polynomial $m(x) \in \mathbb{F}_2[x]$ that is irreducible for which $m(\gamma) = 0$, and $m(x)$ is unique, $\deg m = k$, and $m(x)$ divides $x^{2^k - 1} - 1$.

Example. For $\mathbb{F}_8$,

- the minimal polynomial of α is $x^3 + x + 1$,
- the minimal polynomial of α^2 is $x^3 + x + 1$, since $\alpha^6 + \alpha^2 + 1 = (\alpha^3 + \alpha + 1)^2 = 0$, and
- the minimal polynomial of α^3 is $x^3 + x^2 + 1$, since $(1 + \alpha)^3 = \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^2 = (1 + \alpha)^2 + 1$.

Note. In general, if $\gamma \in \mathbb{F}_{2^k}^*$, then γ and γ have the same minimal polynomial, since $m(\gamma^2) = m(\gamma)^2 = 0$.

1.6.2 Definition of BCH codes

Let $k, d \in \mathbb{Z}_{\geq 2}$. Let β be a primitive element of $\mathbb{F}_{2^k}$. For each $i \geq 1$, let $m_i(x)$ be the minimal polynomial of β^i. Let $p(x)$ be the least common multiple of $m_1(x), \dots, m_{d-1}(x)$. The cyclic code of length $2^k - 1$ with generator polynomial $p(x)$ is called the **BCH code** of length $2^k - 1$ and **designed distance** d.

Example. Let $\mathbb{F}_8$ with primitive element α as above.

$d = 3$. $m_1(x)$ is the minimal polynomial of α, which is $x^3 + x + 1$, and $m_2(x)$ is the minimal polynomial of α^2, which is $x^3 + x + 1$. So $p(x) = x^3 + x + 1$ and the BCH code is $\operatorname{Ham} 3$.

$d = 4$. $m_3(x)$ is the minimal polynomial of α^3, which is $x^3 + x^2 + 1$. So

$$p(x) = (x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

and the BCH code is $\{0^7, 1^7\}$.

Theorem 1.32. *Let $n = 2^k - 1$ and let C be a BCH code of length n and designed distance d. Then*

1. $\mathrm{d}(C) \geq d$, *and*
2. *letting $t = \lfloor d/2 \rfloor$, that is $d = 2t$ or $d = 2t + 1$, then* $\dim C \geq n - kt$.

Example. Let $\mathbb{F}_{16}$ with α primitive element as above.

$d = 3$. $p(x) = x^4 + x + 1$. So the BCH code has length 15, dimension 11, and minimum distance at least three. This is $\mathrm{Ham}\, 4$.

$d = 5$. $m_3(x)$ is the minimal polynomial of α^3, which is $x^4 + x^3 + x^2 + x + 1$, so

$$p(x) = \left(x^4 + x + 1\right)\left(x^4 + x^3 + x^2 + x + 1\right).$$

So the BCH code has length 15, dimension seven, and minimum distance at least five.

Note. For code C of length 15 correcting two errors, the Hamming bound implies that $\dim C \leq 8$, and the G-V bound implies that there exists a code of dimension six.

Proof of 1.32.

1. Omitted.
2. Let $p(x) = \mathrm{lcm}(m_1(x), \dots, m_{d-1}(x))$. Know
   - $m_i(x) = m_{2i}(x)$ for all i, since α^i and α^{2i} have the same minimal polynomial,
   - $d - 1 \leq 2t$, and
   - $\deg m_i(x) \leq k$ for all i.

   Thus $p(x)$ is the product of at most t of the m_i, so $\dim C = n - \deg p \leq n - kt$.

□

1.7 Automorphism group of a code

Recall that the **symmetric group** $\mathcal{S}_n$ is the group of all permutations, that is bijections, of $\{1, \dots, n\}$. Recall that equivalent codes are those for which the columns have been permuted in some way.

Definition. The **automorphism group** of a code $C \subseteq \mathbb{Z}_2^n$ is

$$\mathrm{Aut}\, C = \left\{\sigma \in \mathcal{S}_n \;\middle|\; \forall (c_1, \dots, c_n) \in C,\ \left(c_{\sigma(1)}, \dots, c_{\sigma(n)}\right) \in C\right\}.$$

Remark. For a linear code C, C is cyclic if and only if $\langle (1 \dots n) \rangle \leq \mathrm{Aut}\, C$.

Example.

- Let $C = \{0^n, 1^n\}$. Then $\mathrm{Aut}\, C = \mathcal{S}_n$.
- Let $C = \{000, 110, 011, 101\}$. Then $\mathrm{Aut}\, C = \mathcal{S}_3$.

Definition. Let $\mathrm{M}_{23} = \mathrm{Aut}\, \mathrm{G}_{23}$ and $\mathrm{M}_{24} = \mathrm{Aut}\, \mathrm{G}_{24}$. These are called **Mathieu groups**.

These groups are very famous. They are two of the 26 **sporadic simple groups**.

2 Graphs

2.1 Strongly regular graphs

2.1.1 Regular graphs

Lecture 13 Tuesday 06/11/18

Definition. A **graph** Γ is a pair (V, E) where $V = V(\Gamma)$ is a set of **vertices** and $E = E(\Gamma)$ is a set of 2-subsets of V called **edges**. Assume $V \neq \emptyset$. Write $u \sim v$ if and only if $\{u, v\} \in E$. A graph is **regular of valency** k if every vertex has k **neighbours**.

Definition. The **complement** $\overline{\Gamma}$ of a graph Γ is the graph with vertex set V such that $u \sim v$ in $\overline{\Gamma}$ if and only if $u \nsim v$ in Γ.

Example.

Γ $\qquad$ $\overline{\Gamma}$

Definition. A **path** in Γ is a sequence of vertices $v_0, \dots, v_k$ such that $v_i \sim v_{i+1}$ for all i. The path has **length** k. Then Γ is **connected** if there is a path between any two vertices. If $v, w \in V$, the **distance** $\mathrm{d}(v, w)$ between v and w is the length of the shortest path from v to w. Write $\mathrm{d}(v, w) = \infty$ if no such path. For $x \in V$, define

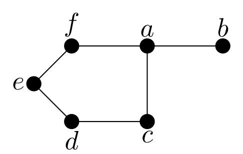
$$\Gamma_i(x) = \{v \in V \mid \mathrm{d}(x, v) = i\}, \qquad i \geq 0.$$

Write $\Gamma(x) = \Gamma_1(x)$, the set of things **adjacent** to x.

Definition. Let Γ be a connected graph. The **diameter** of Γ is

$$\operatorname{diam} \Gamma = \max\{\mathrm{d}(v, w) \mid v, w \in V\}.$$

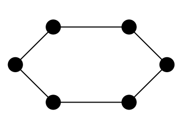
Example. Let Γ be



.

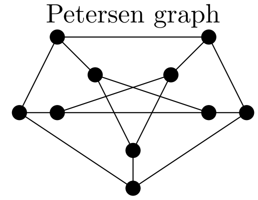
- $\mathrm{d}(a, b) = 1$ and $\mathrm{d}(b, e) = 3$.
- Γ is connected.
- $\Gamma(a) = \Gamma_1(a) = \{f, c, b\}, \Gamma_2(a) = \{d, e\}, \Gamma_0(a) = \{a\}$.
- $\operatorname{diam} \Gamma = 3$.

Example.



diam = 3

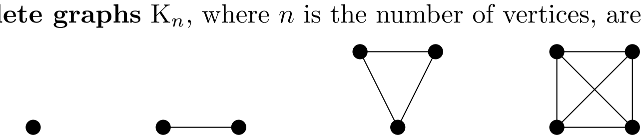
Petersen graph



diam = 2

Note. $\operatorname{diam} \Gamma \leq 1$ if and only if every pair of distinct vertices is adjacent.

Example. **Complete graphs** K_n, where n is the number of vertices, are



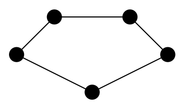
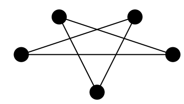
K_1 $\qquad$ K_2 $\qquad$ K_3 $\qquad$ K_4 $\qquad$ $\dots$.

Definition. Graphs $\Gamma = (V, E)$ and $\Gamma' = (V', E')$ are **isomorphic** if there exists a bijection $\phi : V \to V'$ such that $u \sim v$ in Γ if and only if $\phi(u) \sim \phi(v)$ in Γ'. That is,

$$E' = \phi(E) = \{\{\phi(u), \phi(v)\} \mid \{u, v\} \in E\}.$$

That is, ϕ sends edges to edges and non-edges to non-edges.

Example.

 $\cong$ 

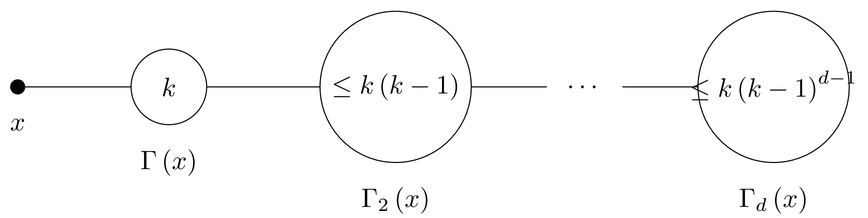
Proposition 2.1. *Let Γ be a connected graph that is regular of valency k and has diameter $d \geq 1$. Then*

$$|V(\Gamma)| \leq 1 + k + k(k-1) + \cdots + k(k-1)^{d-1} = \mathrm{N}(k, d).$$

Proof. Let $x \in V(\Gamma)$. Then

$$V(\Gamma) = \Gamma_0(x) \cup \Gamma_1(x) \cup \cdots \cup \Gamma_d(x),$$

so



Thus

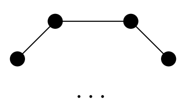
$$|V(\Gamma)| = 1 + k + |\Gamma_2(x)| + \cdots + |\Gamma_d(x)| \leq 1 + k + k(k-1) + \cdots + k(k-1)^{d-1}.$$

$\square$

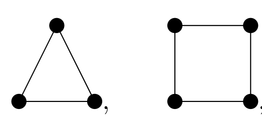
Definition. A **Moore graph** is a connected regular graph of valency k and diameter d such that $|V(\Gamma)| = \mathrm{N}(k, d)$.

Example.

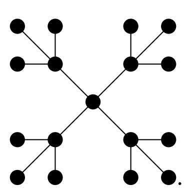
- Let $k = 2$. Then $|V(\Gamma)| = 1 + 2d$ so Γ is a $(1 + 2d)$-gon



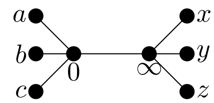
- Let $k = 3$ and $d = 2$. Then $|V(\Gamma)| = 1 + 3 + 6 = 10$, such as the Petersen graph.
- Let $k = 4$ and $d = 2$. Then $|V(\Gamma)| = 1 + 4 + 12 = 17$. Claim that there is no such graph. Suppose $\Gamma = (V, E)$ is such a graph of $|V| = 17$, valency four, and diameter two. Γ has no



since Γ is

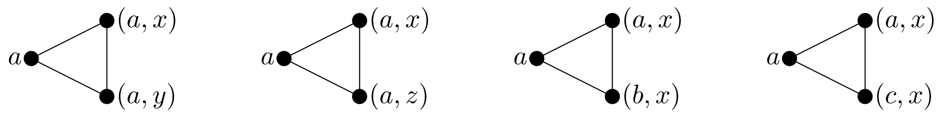


Take an edge $0 \sim \infty$, so

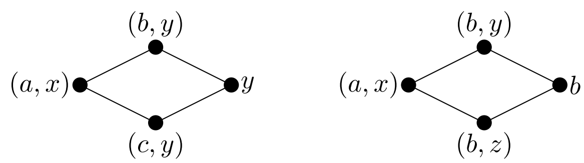


.

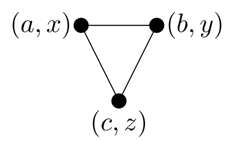
a is not adjacent to x, y, z, since no squares, so a and x have a common neighbour say (a, x). Similarly get vertices $(a, y), (a, z), (b, x), (b, y), (b, z), (c, x), (c, y), (c, z)$. This gives nine vertices, else get squares. This accounts for all vertices in Γ. Also, $(a, x) \nsim (a, y), (a, x) \nsim (a, z), (a, x) \nsim (b, x), (a, x) \nsim (c, x)$, since there are no triangles



Now (a, x) has two neighbours from $(b, y), (b, z), (c, z), (c, z)$. Say $(a, x) \sim (b, y)$. Then $(a, x) \nsim (c, y)$ and $(a, x) \nsim (b, z)$, since there are no squares



so $(a, x) \sim (c, z)$. Now (b, y) has two neighbours in $(a, x), (a, z), (c, x), (c, z)$. Since $(b, y) \sim (a, x)$, $(b, y) \nsim (c, x)$ and $(b, y) \nsim (a, z)$, so $(b, y) \sim (c, z)$. But then



,

a contradiction.

A question is for which values of k is there a Moore graph of valency k and diameter two? The answer is only $k = 2$, the **5-cycle**, $k = 3$, the Petersen graph, $k = 7$, the **Hoffman-Singleton graph**, or $k = 57$, which is unknown. We will prove this using the theory of strongly regular graphs.

Lecture 14 Tuesday 06/11/18

Lecture 14 is a problems class.

2.1.2 Strongly regular graphs

Lecture 15 Wednesday 07/11/18

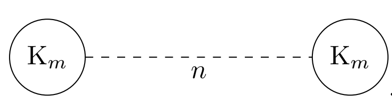
Definition. A **strongly regular graph** with parameters (v, k, λ, μ), or $\operatorname{srg}(v, k, \lambda, \mu)$ is a graph with v vertices that is regular of valency k such that

- every pair of adjacent vertices have exactly λ common neighbours, and
- every pair of non-adjacent vertices have exactly μ common neighbours, and

Note. We do not include the complete graphs K_n or $\overline{\mathrm{K}_n}$, that is λ and μ are defined.

Example.

- $n \cdot \mathrm{K}_m$ is the disjoint union of n copies of K_m,

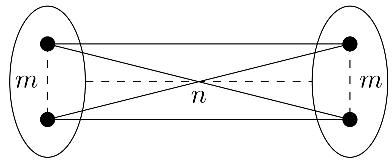


.

For $n, m \geq 2$,

$$n \cdot \mathrm{K}_m = \operatorname{srg}(nm, m - 1, m - 2, 0).$$

- $K_{n[m]}$ is the graph with n parts of size m such that $u \sim v$ if and only if u and v are in different parts, the **complete multipartite graph**

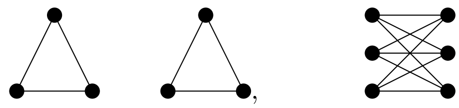


For $n, m \geq 2$,

$$K_{n[m]} = \text{srg}\left(nm, nm - m, nm - 2m, nm - m\right).$$

When $n = 2$, this is the **complete bipartite graph**.

Note. $K_{n[m]} = \overline{n \cdot K_m}$. For example,



$2 \cdot K_3$ $K_{2[3]}$

Proposition 2.2. *Let* $\Gamma = \text{srg}\left(v, k, \lambda, \mu\right)$. *Then*

1. *if* $\mu > 0$, *then* $\operatorname{diam} \Gamma = 2$, *so* Γ *is connected,*
2. *if* $\mu = 0$, *then* $\Gamma \cong n \cdot K_m$ *for some* $n, m \geq 2$, *and*
3. *if* $\mu = k$, *then* $\Gamma \cong K_{n[m]}$ *for some* $n, m \geq 2$.

Proof.

1. If u and v are distinct vertices then either $u \sim v$ or $u \nsim v$, in which case u and v have a common neighbour.
2. Suppose $\mu = 0$. Let u be a vertex with neighbours $u_1, \dots, u_k$. Since $\mu = 0$, $u_i \sim u_j$ for all $i \neq j$, else, u is a common neighbour of u_i and u_j. So the vertices $u, u_1, \dots, u_k$ form K_{k+1}. Any other vertex v also lies in a K_{k+1}. Repeat.
3. Sheet 3. [6]

$\square$

Proposition 2.3. *Let* $\Gamma = \text{srg}\left(v, k, \lambda, \mu\right)$. *Then*

$$\overline{\Gamma} = \text{srg}\left(v, v - k - 1, v - 2k + \mu - 2, v - 2k + \lambda\right).$$

Proof. Sheet 3. [7] $\square$

Example.

- Moore graphs with diameter two is

$$\text{srg}\left(1 + k^2, k, 0, 1\right),$$

since no triangles, so $\lambda = 0$, and no squares, so $\mu = 1$.

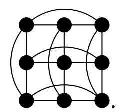
[6] Exercise
[7] Exercise

- The **Triangular graph** $\mathrm{T}(n)$ for $n \geq 2$, has
  - vertices 2-subsets of $\{1, \dots, n\}$, and
  - $\{i, j\} \sim \{k, l\}$ if and only if $|\{i, j\} \cap \{k, l\}| = 1$,

  so $v = \binom{n}{2}$ and $k = 2(n-2)$. Then $\{i, j\} \sim \{i, k\}$ has common neighbours $\{i, l\}$ for $l \neq i, j, k$, and also $\{j, k\}$, so $\lambda = n - 2$, and $\{i, j\} \nsim \{k, l\}$ has common neighbours are $\{i, k\}, \{i, l\}, \{j, k\}, \{j, l\}$, so $\mu = 4$. Thus for $n \geq 4$,
  $$\mathrm{T}(n) = \operatorname{srg}\left(\binom{n}{2}, 2(n-2), n-2, 4\right).$$
  Show $\overline{\mathrm{T}(5)}$ is the Petersen graph. Sheet 3. [8]

- The **Lattice graph** $\mathrm{L}(n)$ has
  - vertices (i, j) for $i, j \in \{1, \dots, n\}$, and
  - $(i, j) \sim (k, l)$ if and only if $i = k$ or $j = l$.

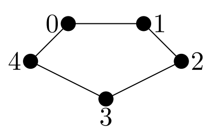
  For example, for $n = 3$,

  .

  Thus for $n \geq 2$,
  $$\mathrm{L}(n) = \operatorname{srg}\left(n^2, 2(n-1), n-2, 2\right).$$

- Let $p \equiv 1 \mod 4$ be a prime. Then $\mathbb{Z}_p$ is a field. Let $Q = \left\{x^2 \mid x \in \mathbb{Z}_p^*\right\}$. This is a subgroup of $\left(\mathbb{Z}_p^*, \times\right)$. Define a homomorphism
  $$\begin{array}{cccc} \phi & : & \mathbb{Z}_p^* & \longrightarrow & Q \\ & & x & \longmapsto & x^2 \end{array}.$$
  Then $K = \ker \phi = \left\{x \in \mathbb{Z}_p^* \mid x^2 = 1\right\} = \{\pm 1\}$, so $|Q| = \left|\mathbb{Z}_p^*\right| / |K| = (p-1)/2$, and $\mathbb{Z}_p^*$ has a unique element of order two, namely $-1 \equiv p - 1 \in \mathbb{Z}_p^*$. Since $p \equiv 1 \mod 4$, $|Q|$ is even, so $-1 \in Q$. The **Payley graph** $\operatorname{Pay}(p)$ has
  - vertices $\mathbb{Z}_p$, and
  - $x \sim y$ if and only if $x - y \in Q$.

  Note that $-1 \in Q$, so $x - y \in Q$ if and only if $y - x \in Q$. For example, for $p = 5$, $Q = \{1, 4\}$, so

Proposition 2.4. *For* $p \equiv 1 \mod 4$,
$$\operatorname{Pay}(p) = \operatorname{srg}\left(p, \frac{p-1}{2}, \frac{p-5}{2}, \frac{p-1}{4}\right).$$

Proof. Sheet 3. [9] $\square$

[8] Exercise
[9] Exercise

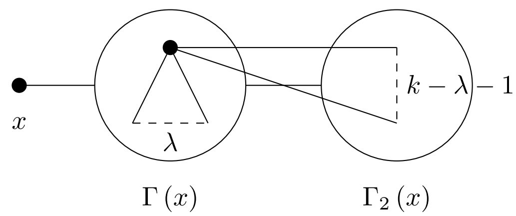
2.2 Some theory of strongly regular graphs

2.2.1 Properties

Proposition 2.5. *If* $\Gamma = \mathrm{srg}\,(v, k, \lambda, \mu)$ *then*

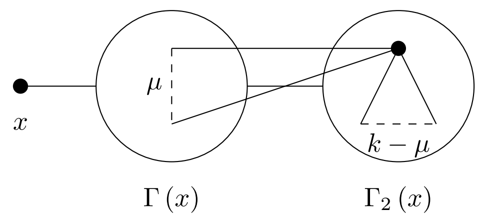
$$k\,(k - \lambda - 1) = \mu\,(v - k - 1)\,.$$

Proof. Let x be a vertex. Each vertex in $\Gamma\,(x)$ has λ neighbours in $\Gamma\,(x)$, so has $k - \lambda - 1$ neighbours in $\Gamma_2\,(x)$, so



.

Each vertex in $\Gamma_2\,(x)$ has μ neighbours in $\Gamma\,(x)$, so has $k - \mu$ neighbours in $\Gamma_2\,(x)$, so



.

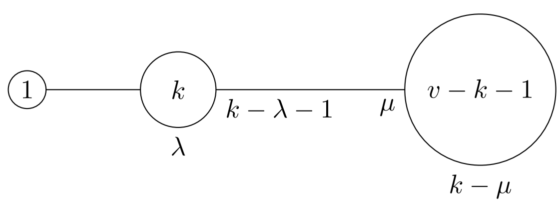
Let N be the number of $\{u, v\}$ such that $u \in \Gamma\,(x)$ and $v \in \Gamma_2\,(x)$. Then counting N two ways,

$$k\,(k - \lambda - 1) = N = \mu\,(v - k - 1)\,.$$

$\square$

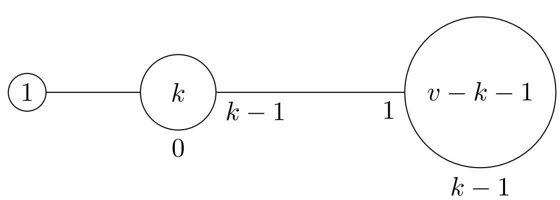
Lecture 16 Tuesday 13/11/18

Distance distribution diagram (DDD) for $\mathrm{srg}\,(v, k, \lambda, \mu)$ is



.

Example. Let $\Gamma = \mathrm{srg}\,(v, k, 0, 1)$. Then



.

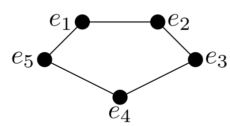
2.5 implies that $k\,(k - 1) = v - k - 1$, so $v = k^2 + 1$. Thus Γ is a Moore graph of dimension two.

2.2.2 Adjacency matrices

Definition. Let Γ be a graph with vertices $e_1, \dots, e_v$. The **adjacency matrix** A of Γ is $A = (a_{ij})$ where

$$a_{ij} = \begin{cases} 1 & e_i \sim e_j \\ 0 & \text{otherwise} \end{cases}.$$

Example. Let Γ be



.

Then

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

A is symmetric, entries 0's and 1's, and 0's on the diagonal. For strongly regular graphs, A has nice properties.

Proposition 2.6. *Let $\Gamma = \operatorname{srg}(v, k, \lambda, \mu)$, with adjacency matrix A. Let $\mathrm{J} = (x_{ij})$ be a $v \times v$ matrix where $x_{ij} = 1$ for all i and j. Then*

1. $A\mathrm{J} = k\mathrm{J}$, *and*
2. $A^2 = (\lambda - \mu) A + (k - \mu) \mathrm{I} + \mu \mathrm{J}$.

Proof.

1. $$A \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = k \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix},$$

   so $A\mathrm{J} = k\mathrm{J}$.

2. A is symmetric, so $A = A^\intercal$. Let $V = \{e_1, \dots, e_v\}$. Then

   $$\left(A^2\right)_{ij} = \left(AA^\intercal\right)_{ij} = A_{i \cdot} A^\intercal_{\cdot j} = A_{i \cdot} \cdot A_{j \cdot} = \left|\{e_k \in V \mid e_i \sim e_k,\ e_j \sim e_k\}\right| = \begin{cases} k & i = j \\ \lambda & i \sim j \\ \mu & i \nsim j,\ i \neq j \end{cases}.$$

   Then A^2 has k on the diagonal, λ where A has one, and μ where A has zero, off the diagonal. Thus

   $$A^2 = k\mathrm{I} + \lambda A + \mu (\mathrm{J} - A - \mathrm{I}) = (\lambda - \mu) A + (k - \mu) \mathrm{I} + \mu \mathrm{J}.$$

□

The key to the study of strongly regular graphs are the eigenvalues of the adjacency matrix A. For any graph with adjacency matrix A, since A is a real symmetric matrix, it has real eigenvalues and is diagonalisable, that is there exists an invertible matrix P such that

$$P^{-1} A P = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_v \end{pmatrix}.$$

We call the λ_i the **eigenvalues** of Γ. The **multiplicity** of λ_i is the number of times, with repeats, that it appears, which is equal to the algebraic multiplicity and the geometric multiplicity.

2.2.3 Main theorem

Theorem 2.7 (Main theorem). *Let $\Gamma = \mathrm{srg}(v, k, \lambda, \mu)$ where $\mu > 0$, that is Γ is connected. Let A be the adjacency matrix of Γ. Then*

1. *A has exactly three distinct eigenvalues k, r_1, r_2 where r_1 and r_2 are the roots of*
$$x^2 - (\lambda - \mu) x - (k - \mu) = (x - r_1)(x - r_2),$$
2. *the eigenvalue k has multiplicity one, and eigenvalues r_1 and r_2 have multiplicities m_1 and m_2 where*
$$m_1 + m_2 = v - 1, \qquad r_1 m_1 + r_2 m_2 = -k,$$
3. *either $r_1, r_2 \in \mathbb{Z}$ or*
$$(v, k, \lambda, \mu) = (4\mu + 1, 2\mu, \mu - 1, \mu).$$

We will prove this later. The $\mathrm{srg}(4\mu + 1, 2\mu, \mu - 1, \mu)$ are called the **conference graphs**.

Note. Conference matrix theorem is that these graphs only exist when $4\mu + 1$ is a sum of two squares. Proved by Belevitch in 1950, and elementary linear algebra proof by van Lint and Seidel in 1966.

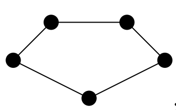
2.2.4 Application to Moore graphs

First some applications.

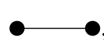
Theorem 2.8. *If there exists a Moore graph of diameter two and valency k, then $k = 2, 3, 7, 57$.*

Note. For diameter at least three, the only Moore graphs are $(2d + 1)$-gons, where $k = 2$, by Morell in 1973.

Proof. Let Γ be such a graph with adjacency matrix A. Note that $\Gamma = \mathrm{srg}\left(k^2 + 1, k, 0, 1\right)$. Since $\mu = 1 > 0$, 2.7 applies. By 2.7.1, A has three eigenvalues k, r_1, r_2 where r_1 and r_2 are the roots of
$$x^2 - (\lambda - \mu) x - (k - \mu) = x^2 + x - (k - 1).$$
Then
$$r_1, r_2 = \frac{1}{2}\left(-1 \pm \sqrt{4k - 3}\right).$$
By 2.7.2, the multiplicities of r_1 and r_2 are m_1 and m_2 where
$$m_1 + m_2 = k^2, \qquad r_1 m_1 + r_2 m_2 = -k.$$
Then
$$\frac{m_1}{2}\left(-1 + \sqrt{4k - 3}\right) + \frac{m_2}{2}\left(-1 - \sqrt{4k - 3}\right) = -k,$$
so
$$\sqrt{4k - 3}\,(m_1 - m_2) = (m_1 + m_2) - 2k = k^2 - 2k = k(k - 2). \tag{2}$$
By 2.7.3, either $r_1, r_2 \in \mathbb{Z}$, or $(v, k, \lambda, \mu) = (5, 2, 0, 1)$, then Γ is


,

and $k = 2$, so done. Thus assume $r_1, r_2 \in \mathbb{Z}$. Then $\sqrt{4k - 3} \in \mathbb{Z}$. By (2), $4k - 3 \mid k^2 (k - 2)^2$. Now $\gcd(4k - 3, k)$ divides three and $\gcd(4k - 3, k - 2)$ divides five, so $4k - 3 \mid 3^2 \cdot 5^2$ and $4k - 3$ is square. So $4k - 3 = 1^2, 3^2, 5^2, 3^2 \cdot 5^2$, so $k = 1, 3, 7, 57$. But $k \neq 1$ or else Γ is


,

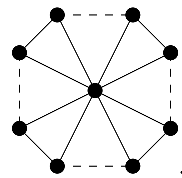
which is complete. ∎

2.2.5 Friendship theorem

Lecture 17 Tuesday 13/11/18

This is the following.

Theorem 2.9. *In a graph Γ in which any two vertices have exactly one common neighbour, there exists a vertex that is adjacent to all other vertices. That is, the graph of Γ is a windmill*



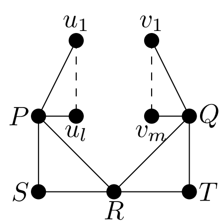
.

Proof. Assume Γ has more than one vertex. Suppose for a contradiction that no vertex is adjacent to every other vertex.

Step 1. Γ is regular, so $\mathrm{srg}(v,k,1,1)$. For a vertex P, let $v(P)$ be the number of neighbours of P. First show,

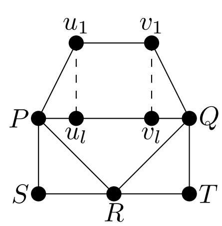
$$P \nsim Q \qquad \implies \qquad v(P) = v(Q). \tag{3}$$

P and Q have a unique common neighbour R. P and R have a unique common neighbour S. Q and R have a unique common neighbour T. Let the remaining neighbours of P be $u_1, \dots, u_l$, and let the remaining neighbours of Q be $v_1, \dots, v_m$, so



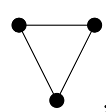
.

$u_i \neq v_j$ since R is the unique neighbour of P and Q. Now u_1 and Q have a common neighbour, not R or T, since if T, then P and T would have two common neighbours, and if R, then S and u_1 would have two common neighbours. So common neighbour is one of v_i, say v_1. Similarly, u_2 and Q have a unique common neighbour, not R or T, not v_1, otherwise u_1 and u_2 have two common neighbours. So u_2 is adjacent to some v_i where $i > 1$, say v_2. Carrying on, u_l is adjacent to v_l, hence $m \geq l$. Similarly, $l \geq m$, so



.

Thus $v(P) = l + 2 = v(Q)$. So (3) holds. Now there exist P and Q such that $P \nsim Q$. If not then Γ is complete, so Γ is



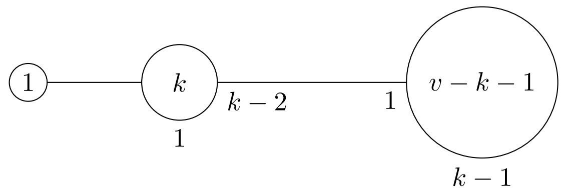
,

a contradiction of assumption. Let R be the unique common neighbour of P and Q. Let S be any vertex other than P, Q, and R. Then S is not adjacent to both P and Q, so without loss of generality $S \nsim P$. By (3), $v(S) = v(P) = v(Q)$. By assumption, R is not adjacent to every vertex in Γ, so there exists S' such that $R \nsim S'$ so $v(R) = v(S') = v(P) = v(Q)$. Thus Γ is regular. Hence

$$\Gamma = \mathrm{srg}(v,k,1,1), \qquad k \geq 3,$$

since no strongly regular graph has $k = 1$, and if $k = 2$, then $\Gamma = \mathrm{K}_3$, a contradiction.

Step 2. There is no such Γ. DDD is



.

2.5 implies that $k(k-2) = v-k-1$, so $v = k^2-k+1$. Since $\mu > 0$, we can apply 2.7. By 2.7.1 the eigenvalues of Γ are k, r_1, r_2 where r_1 and r_2 are the roots of $x^2-(k-1)$. So $r_1 = \sqrt{k-1}$ and $r_2 = -\sqrt{k-1}$. By 2.7.2, r_i have multiplicities m_i where

$$m_1+m_2 = v-1 = k^2-k = k(k-1), \qquad m_1\sqrt{k-1}-m_2\sqrt{k-1} = -k,$$

that is $\sqrt{k-1}\,(m_1-m_2) = -k$, so $(k-1)(m_1-m_2)^2 = k^2$, so $k-1 \mid k^2$. But $\gcd(k-1,k) = 1$, so $k-1 = 1$, that is $k = 2$, a contradiction.

□

2.2.6 Proof of the main theorem

Proof of 2.7. Let $\Gamma = \mathrm{srg}(v,k,\lambda,\mu)$ where $\mu > 0$. Let A be the adjacency matrix of Γ. By 2.6, $A\mathrm{J} = k\mathrm{J}$ and

$$A^2 = (\lambda-\mu)A + (k-\mu)\mathrm{I} + \mu\mathrm{J}. \tag{4}$$

Let

$$\overline{1} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Step 1. Prove that k is an eigenvalue. $A\overline{1} = k\overline{1}$ so k is an eigenvalue with eigenvector $\overline{1}$.

Step 2. Let r_1 and r_2 be the roots of

$$x^2-(\lambda-\mu)x-(k-\mu).$$

Prove that A has at most three distinct eigenvalues k, r_1, r_2, and any eigenvector not in $\mathrm{sp}\,\overline{1}$ has eigenvalue r_1 or r_2. Let w be an eigenvector, so $Aw = \epsilon w$ for some ϵ. Assume w is not in $\mathrm{sp}\,\overline{1}$. By (4)

$$A^2w = (\lambda-\mu)Aw + (k-\mu)\mathrm{I}w + \mu\mathrm{J}w.$$

Then $\mathrm{J}w = c\overline{1}$ where c is the sum of entries in w. Then

$$\epsilon^2 w = (\lambda-w)\epsilon w + (k-\mu)w + \mu c\overline{1},$$

so

$$\left(\epsilon^2-(\lambda-\mu)\epsilon-(k-\mu)\right)w = \mu c\overline{1} \in \mathrm{sp}\,\overline{1}.$$

Thus

$$\epsilon^2-(\lambda-\mu)\epsilon-(k-\mu) = 0.$$

Step 3. Prove that k has multiplicity one, and $k \ne r_1, r_2$. If $k = r_1$ or $k = r_2$, then

$$k^2-(\lambda-\mu)k-(k-\mu) = 0.$$

By 2.5, $k(k-\lambda-1) = \mu(v-k-1)$, so

$$\mu v = k^2-(\lambda-\mu)k-(k-\mu) = 0,$$

so $\mu = 0$, a contradiction of assumption. Thus $k \ne r_1, r_2$. By step 2, k has multiplicity one.

Step 4. Prove that the multiplicities of r_1 and r_2 satisfy

$$m_1 + m_2 = v - 1, \qquad r_1 m_1 + r_2 m_2 = -k,$$

where if r_i is not an eigenvalue then $m_i = 0$. k has multiplicity one, so eigenvalues are

$$k, \qquad \underbrace{r_1, \dots, r_1}_{m_1}, \qquad \underbrace{r_2, \dots, r_2}_{m_2},$$

so $1 + m_1 + m_2 = r$. There exists an invertible matrix P such that

$$P^{-1}AP = \begin{pmatrix} k & & & & & & 0 \\ & r_1 & & & & & \\ & & \ddots & & & & \\ & & & r_1 & & & \\ & & & & r_2 & & \\ & & & & & \ddots & \\ 0 & & & & & & r_2 \end{pmatrix}.$$

Then

$$k + m_1 r_1 + m_2 r_2 = \operatorname{Tr} P^{-1}AP = \operatorname{Tr} P^{-1}(PA) = \operatorname{Tr} A = 0,$$

where **trace** is the sum of the diagonal elements.

Lecture 18 Wednesday 14/11/18

Step 5. Prove that either $r_1, r_2 \in \mathbb{Z}$ or

$$(v, k, \lambda, \mu) = (4\mu + 1, 2\mu, \mu - 1, \mu).$$

Let r_1 and r_2 be the roots of

$$x^2 - (\lambda - \mu) x - (k - \mu).$$

So

$$r_1, r_2 = \frac{1}{2}\left(\lambda - \mu \pm \sqrt{(\lambda - \mu)^2 + 4(k - \mu)}\right) = \frac{1}{2}\left(\lambda - \mu \pm \sqrt{D}\right).$$

By step 4,

$$\frac{m_1}{2}\left(\lambda - \mu + \sqrt{D}\right) + \frac{m_1}{2}\left(\lambda - \mu - \sqrt{D}\right) = -k,$$

so

$$(\lambda - \mu)(m_1 + m_2) + \sqrt{D}(m_1 - m_2) = -2k. \tag{5}$$

- Suppose $m_1 \ne m_2$. Then $\sqrt{D} \in \mathbb{Q}$, so $\sqrt{D} \in \mathbb{Z}$, since $\sqrt{D} = a/b$ implies that $D = a^2/b^2 \in \mathbb{Z}$, so $b^2 \mid a^2$, so $b \mid a$. Suppose $r_i \notin \mathbb{Z}$, then $r_1, r_2 \in \mathbb{Z}$ and have the form $x/2$, where x is odd, so $r_1 r_2 \notin \mathbb{Z}$. But $r_1 r_2 = -(k - \mu) \in \mathbb{Z}$, a contradiction. Thus $r_1, r_2 \in \mathbb{Z}$.
- Suppose $m_1 = m_2 = m$. From step 4, $2m = v - 1$. From (5), $(\lambda - \mu)(2m) = -2k$, so $m(\mu - \lambda) = k$. Then $m \mid k$. But $0 < k < v - 1 = 2m$, since Γ is not K_v or $\overline{\mathrm{K}_v}$, so $k = m$, so $\mu - \lambda = 1$, so $\lambda = \mu - 1$. By 2.5,

  $$k(k - \lambda - 1) = \mu(v - k - 1) = \mu k,$$

  since $2k = v - 1$, so $\mu = k - \lambda - 1$. Thus $k = \mu + \lambda + 1 = 2\mu$, and $v = 2m + 1 = 4\mu + 1$.

So step 5 holds.

Step 6. Prove that $r_1 \ne r_2$. Suppose $r_1 = r_2$. Then

$$0 = D = (\lambda - \mu)^2 + 4(k - \mu) \ge 0,$$

since $\mu \le k$, so $\lambda = \mu = k$. But $\lambda \le k - 1$, a contradiction.

Step 7. Prove that $m_1, m_2 > 0$. Suppose $m_2 = 0$. By step 4, $m_1 = v - 1$ and $m_1 r_1 = -k$. Then $r_1 \in \mathbb{Q}$. By the same argument in the proof of step 5, $r_1 \in \mathbb{Z}$. Then $m_1 \mid k$ so $v - 1 \le k < v - 1$, a contradiction.

2.7.1 holds by steps $1, 2, 3, 6, 7$, 2.7.2 holds by steps 3 and 4, and 2.7.3 holds by step 5. $\square$

2.2.7 Strongly regular graphs with small v

A question is what are the possible parameters of $\mathrm{srg}(15, k, \lambda, \mu)$?

Example.

- $\mathrm{T}(6) = \mathrm{srg}(15, 8, 4, 4)$.
- $\overline{\mathrm{T}(6)} = \mathrm{srg}(15, 6, 1, 3)$.
- $3 \cdot \mathrm{K}_5 = \mathrm{srg}(15, 4, 3, 0)$.
- $5 \cdot \mathrm{K}_3 = \mathrm{srg}(15, 2, 1, 0)$.
- $\mathrm{K}_{3[5]} = \mathrm{srg}(15, 10, 5, 10)$.
- $\mathrm{K}_{5[3]} = \mathrm{srg}(15, 12, 9, 12)$.

Proposition 2.10. *If $\Gamma = \mathrm{srg}(15, k, \lambda, \mu)$ then the parameters of Γ are those of $\mathrm{T}(6), 3 \cdot \mathrm{K}_5, 5 \cdot \mathrm{K}_3$ or their complements.*

Proof. If $k > 7$, then the valency of $\overline{\Gamma}$ is at most seven. Suppose $k \le 7$. If $\mu = 0$, then 2.2 implies that Γ is $3 \cdot \mathrm{K}_5$ or $5 \cdot \mathrm{K}_3$. Suppose $\mu > 0$, so Γ is connected of diameter two. Note that $2 \le k$. The following are the cases.

$k = 2$. Γ is a 15-gon, which is not diameter two.

$k = 3$. $3(2 - \lambda) = 11\mu$, a contradiction.

$k = 4$. $4(3 - \lambda) = 10\mu$, so $2(3 - \lambda) = 5\mu$, a contradiction.

$k = 5$. $5(4 - \lambda) = 9\mu$, a contradiction.

$k = 6$. $6(5 - \lambda) = 8\mu$, so $3(5 - \lambda) = 4\mu$, so $3 \mid \mu$ and $4 \mid (5 - \lambda)$, so $\mu = 3$ and $\lambda = 1$. Thus $(15, 6, 1, 3)$ and $\overline{\mathrm{T}(6)}$ has these parameters.

$k = 7$. $7(6 - \lambda) = 7\mu$, so $6 - \lambda = \mu$. Let r_1 and r_2 be the roots of

$$x^2 - (\lambda - \mu)x - (k - \mu) = x^2 - (2\lambda - 6)x - (\lambda + 1),$$

so

$$r_1, r_2 = \lambda - 3 \pm \sqrt{(\lambda - 3)^2 + \lambda + 1} = \lambda - 3 \pm \sqrt{\lambda^2 - 5\lambda + 10}.$$

By 2.7.3, $r_1, r_2 \in \mathbb{Z}$, since k is odd, so $\sqrt{\lambda^2 - 5\lambda + 10} \in \mathbb{Z}$, and $\lambda < k - 1 = 6$, so $\lambda = 2, 3$. Let $\lambda = 2$. Then $r_1, r_2 = 1, -3$, so $m_1 + m_2 = 14$ and $m_1 - 3m_2 = -7$. Thus $4m_2 = 21$, a contradiction, and $\lambda = 3$ is similar.

□

2.3 Two weight codes

Lecture 19 Tuesday 20/11/18

Definition. A linear code $C \subseteq \mathbb{Z}_2^n$ is a **two weight code** if there exist $w_1, w_2 \in \mathbb{N}$ such that every non-zero codeword in C has weight w_1 or w_2.

Example.

- The extended Hamming code H' is a two weight code with non-zero weights four and eight.
- $C = \left\{x \in \mathbb{Z}_2^5 \mid \mathrm{wt}\, x \text{ even}\right\}$ is a two weight code with non-zero weights two and four.

Definition. For a non-zero linear code $C \subseteq \mathbb{Z}_2^n$, a **generator matrix** for C is a $k \times n$ matrix whose rows form a basis of C where $k = \dim C$.

2.3.1 Macdonald codes

Definition. Let G be a matrix whose columns are vectors in $\mathbb{Z}_2^k \setminus \{0\}$ where $k \geq 1$. A **simplex code** is a linear code $C \subseteq \mathbb{Z}_2^n$ where $n = 2^k - 1$ with generator matrix G.

Fact. A simplex code of length $2^k - 1$ for $k \geq 1$ has exactly one non-zero weight, namely 2^{k-1}. A typical non-zero element of C has the form xG where $x \in \mathbb{Z}_2^k \setminus \{0\}$. Write $G = \begin{pmatrix} y_1 & \dots & y_n \end{pmatrix}$, so the columns are y_i. Then $xG = \begin{pmatrix} x \cdot y_1 & \dots & x \cdot y_n \end{pmatrix}$. The weight of xG is the number of y_i such that $x \cdot y_i = 1$. By linear algebra, $\left\{y \in \mathbb{Z}_2^k \mid x \cdot y = 0\right\}$ is a subspace of $\mathbb{Z}_2^k$ of dimension $k-1$. Thus $\operatorname{wt} xG = 2^k - 1 - \left(2^{k-1} - 1\right) = 2^{k-1}$.

Definition. Let $\overline{G}$ be a matrix whose columns are vectors in $\mathbb{Z}_2^k \setminus \langle e_{k-i+1}, \dots, e_k \rangle$ where $1 \leq i < k$. A **Macdonald code** is a linear code of length $2^k - 2^i$ with generator matrix $\overline{G}$.

By the fact above this code is a two weight code with weights 2^{k-1} and $2^{k-1} - 2^{i-1}$.

Example. Let $k = 3$, and

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

The non-zero weight is four.

- Let $i = 1$. Removing $(0,0,1)^\intercal$,

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

  The non-zero weights are four and three.

- Let $i = 2$. Removing $(0,0,1)^\intercal, (0,1,0)^\intercal, (0,1,1)^\intercal$,

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

  The non-zero weights are four and two.

2.3.2 Strongly regular graphs from two weight codes

Definition. A linear code $C \subseteq \mathbb{Z}_2^n$ is **projective** if it has a generator matrix whose columns are non-zero and pairwise distinct.

Theorem 2.11 (Delsarte)**.** *Let $C \subseteq \mathbb{Z}_2^n$ be a linear two weight projective code, with weights w_1 and w_2 where $w_1 < w_2$. Let $\Gamma(C)$ be the graph with vertex set C where $x \sim y$ if $\mathrm{d}(x,y) = \operatorname{wt}(x+y) = w_1$. Then $\Gamma(C)$ is strongly regular.*

Example. Let $C = H', w_1 = 4, w_2 = 8$. In $\overline{\Gamma(C)}$, $x \sim y$ if and only if $x + y = 1^8$. So $\overline{\Gamma(C)}$ is

.

This is $8 \cdot \mathrm{K}_2$. Thus $\Gamma(C) = \mathrm{K}_{8[2]}$.

Proof. Let $k = \dim C$, and b_1 and b_2 be the number of codewords of weight w_1 and w_2 respectively. For $i = 1, 2$, let A_i be a $b_i \times n$ matrix whose rows are codewords of weight w_i. Let

$$A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix},$$

a $(b_1 + b_2) \times n$ matrix. Claim that each column of A has weight 2^{k-1}. Let

$$\begin{array}{cccc} \phi_i & : & C & \longrightarrow & \mathbb{Z}_2 \\ & & (c_1, \dots, c_n) & \longmapsto & c_i \end{array}.$$

Now col i of A is not zero, since C is projective. So $\operatorname{im}\phi_i = \mathbb{Z}_2$. Thus $\ker\phi_i$ has dimension $k-1$. So col i has $2^{k-1}-1$ zeroes and 2^{k-1} ones. Thus

$$b_1 + b_2 = 2^k - 1, \qquad b_1 w_1 + b_2 w_2 = n2^{(k-1)},$$

which is the number of ones in A. So we can compute b_1 and b_2 in terms of the given parameters, w_1, w_2, k, n. Let $i \le j \le n$. Let r_1 and r_2 be the number of zeroes in col j of A_1 and A_2 respectively. Claim that r_1 and r_2 are independent of the choice j. Let $C' = \ker\phi_j$. This is a linear code of dimension $k-1$ such that the j-th entry is zero, with r_i codewords of weight w_i for $i = 1, 2$. In the matrix whose rows are elements of C the j-th column is zero and all other columns are non-zero, since C is projective. Thus we can compute r_1 and r_2 as above,

$$r_1 + r_2 = |C'| - 1 = 2^{k-1} - 1, \qquad r_1 w_1 + r_2 w_2 = (n-1)\, 2^{k-2}.$$

Now each column of A_i has r_i zeroes. Let $a_1, \dots, a_{b_1}$ be the rows of A_i, the codewords in C of weight w_1. We can compute

$$D = \sum_{i=1}^{b_1} \mathrm{d}(a_i, a_1) = (n - w_1)(b_1 - r_1) + w_1 r_1,$$

since reordering gives that

$$\begin{array}{ccc} & \overbrace{0 \quad \dots \quad 0}^{n-w_1} & \overbrace{1 \quad \dots \quad 1}^{w_1} \\ a_1 & & \\ a_2 & \begin{pmatrix}\text{column has} \\ b_1 - r_1 \text{ ones}\end{pmatrix} & \begin{pmatrix}\text{column has} \\ r_1 \text{ zeroes}\end{pmatrix} \\ \vdots & & \\ a_{b_1} & & \end{array}.$$

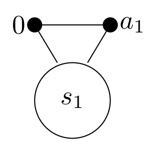
Let s_1 be the number of a_i such that $\mathrm{d}(a_i, a_1) = w_1$, and s_2 be the number of a_i such that $\mathrm{d}(a_i, a_1) = w_2$, so

$$s_1 + s_2 = b_1 - 1, \qquad s_1 w_1 + s_2 w_2 = D.$$

We can compute s_1 in terms of n, k, w_1, w_2. Now consider the graph $\Gamma(C)$. In this graph, neighbours of zero are $a_1, \dots, a_{b_1}$. If $x \in C$, then neighbours of x are $x + a_1, \dots, x + a_{b_1}$, since

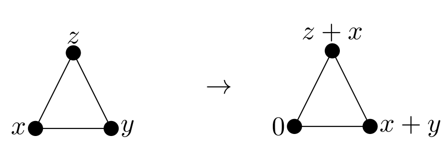
- $\mathrm{wt}(x + xa_1) = \mathrm{wt}\, a_1 = w_1$, so $x + a_i \sim x$, and
- if $y \sim x$, then $\mathrm{wt}(y + x) = w_1$, so $y + x = a_i$ for some i,

so $\Gamma(C)$ is regular of valency b_1. Then



.

Since a_1 was an arbitrary neighbour of zero, if $0 \sim c$ then zero and c have s_1 common neighbours. For an edge $\{x, y\}$, there is a bijection



.

Thus x and y also have s_1 common neighbours. Similarly, working with codewords of weight w_2, we get that the number of common neighbours of two non-adjacent vertices is constant. $\square$

Lecture 20 Tuesday 20/11/18

Lecture 20 is a problems class.

2.4 Automorphism group of a graph

Lecture 21 Wednesday 21/11/18

Definition. Let $\Gamma = (V, E)$ be a graph. The **automorphism group** of Γ is

$$\mathrm{Aut}\,\Gamma = \{\phi \in \mathrm{Sym}\,V \mid \phi \text{ is a graph isomorphism}\} = \{\phi \in \mathrm{Sym}\,V \mid v \sim w \iff \phi(v) \sim \phi(w)\}.$$

It is a subgroup of $\mathrm{Sym}\,V$.

Example.

- If $\Gamma = \mathrm{K}_n$, so $V = \{1, \dots, n\}$, then $\mathrm{Aut}\,\Gamma = \mathcal{S}_n$.
- If $\Gamma = \overline{\mathrm{K}_n}$ then $\mathrm{Aut}\,\overline{\Gamma} = \mathcal{S}_n$.
- $\mathrm{Aut}\,\Gamma = \mathrm{Aut}\,\overline{\Gamma}$ for all graphs Γ. Sheet 3. [10]
- We may view $\mathcal{S}_n$ as a subgroup of $\mathrm{Aut}\,\mathrm{T}(n)$ where $\mathrm{T}(n)$ is a triangular graph. Let $\sigma \in \mathcal{S}_n$. Define

$$\begin{array}{cccc} \phi_\sigma & : & V(\mathrm{T}(n)) & \longrightarrow & V(\mathrm{T}(n)) \\ & & \{i, j\} & \longmapsto & \{\sigma(i), \sigma(j)\} \end{array}, \qquad i, j \in \{1, \dots, n\}, \qquad i \neq j.$$

  Check $\phi_\sigma \in \mathrm{Aut}\,\mathrm{T}(n)$. [11] Define

$$\begin{array}{cccc} \phi & : & \mathcal{S}_n & \longrightarrow & \mathrm{Aut}\,\mathrm{T}(n) \\ & & \sigma & \longmapsto & \phi_\sigma \end{array}.$$

  Check this is a injective group homomorphism. [12]

  - Group homomorphism, since
$$\phi_\sigma \phi_\tau = \phi_{\sigma\tau}, \qquad \sigma, \tau \in \mathcal{S}_n.$$
  - Injective. Suppose $\phi_\sigma = \mathrm{id}$. Then
$$\{\sigma(i), \sigma(j)\} = \phi_\sigma(\{i, j\}) = \{i, j\}, \qquad \{i, j\} \in V(\mathrm{T}(n)).$$
    Claim that $\sigma = 1$, since $\sigma(1) = 1, 2$ and $\sigma(1) = 1, 3$, so $\sigma(1) = 1$, and similarly $\sigma(i) = i$ for all i.

[10] Exercise
[11] Exercise
[12] Exercise

3 Designs

3.1 t-designs

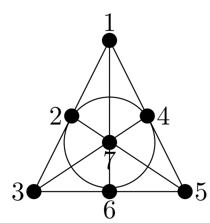
Definition. A t-(v, k, r_t) **design**, or t-**design** with parameters (v, k, r_t), is a pair $(X, \mathcal{B})$ where

- X is a set of size V, where its elements are called **points**,
- $\mathcal{B}$ is a collection of k-subsets of X, where its elements are called **blocks**, and
- every t-subset of X lies in exactly r_t blocks.

Assume that $X \neq \emptyset$, $\mathcal{B} \neq \emptyset$, and $v \geq k \geq t \geq 0$. Say $(X, \mathcal{B})$ is **trivial** if $\mathcal{B}$ is all the k-subsets of X. A 1-design is a **design**. Write $r = r_1$ and $b = |\mathcal{B}|$.

Example.

- Octads of G_{24} form a 5-$(24, 8, 1)$ design.
- The codewords of weight four in the extended Hamming code H' form a 3-$(8, 4, 1)$ design. Sheet 4. [13]
- Let
$$X = \mathbb{Z}_2^k \setminus \{0\}, \qquad \mathcal{B} = \{\{x, y, x + y\} \mid x, y \in X, \ x \neq y\}, \qquad k \geq 3.$$
This is a 2-$\left(2^k - 1, 3, 1\right)$ design. Sheet 4. [14] When $k = 3$, this is the Fano plane



.

Recall 1.24.

Proposition 3.1. *A t-(v, k, r_t) design is an s-(v, k, r_s) design for all $0 \leq s < t$ where*
$$r_s = \frac{(v - t + 1) \dots (v - s)}{(k - t + 1) \dots (k - s)} r_t.$$

Corollary 3.2. *If there exists a t-(v, k, r_t) design, then*
$$(k - t + 1) \dots (k - s) \mid (v - t + 1) \dots (v - s) \, r_t, \qquad 0 \leq s < t.$$

Example.

- Does there exist a 2-$(56, 11, 1)$ design?
$$r = r_1 = \frac{56 - 2 + 1}{11 - 2 + 1} (1) = \frac{55}{10} \notin \mathbb{Z},$$
so no.
- Does there exist a 2-$(46, 10, 1)$ design?
$$r = r_1 = \frac{46 - 2 + 1}{10 - 2 + 1} (1) = \frac{45}{9} = 5, \qquad b = r_0 = \frac{46}{10} (5) = 23.$$
So there is no contradiction. But no such design exists, see soon.

Existence conjecture is that given t, k, r_t, fixed, if divisibility conditions hold, is there a t-(v, k, r_t) design for all but finitely many v? Yes, by Keevash in 2014 and 2018.

[13] Exercise
[14] Exercise

3.2 Some theory of 2-designs

When $(X, \mathcal{B})$ is a 2-(v, k, r_2) design, write λ for r_2.

Proposition 3.3. *For a* 2-(v, k, λ) *design,*

$$bk = vr, \qquad r\,(k-1) = \lambda\,(v-1)\,.$$

Proof.

- In 3.1, take $s = 0$ and $t = 1$, so $b = r_0 = vr/k$.
- In 3.1, take $s = 1$ and $t = 2$, so $r = r_1 = \lambda\,(v-1)\,/\,(k-1)$.

□

The following is the first major result.

Theorem 3.4 (Fisher's inequality)**.** *Suppose there exists a* 2-(v, k, λ) *design, where* $v > k$*, that is more than one block. Then* $b \geq v$ *and* $r \geq k$*.*

Lecture 22 Tuesday 27/11/18

Example. Does there exist a 2-$(46, 10, 1)$ design? Saw that $b = 23 < 46 = v$, a contradiction. So no.

3.2.1 Incidence matrices

Definition. Let $(X, \mathcal{B})$ be a 2-(v, k, λ) design. Let $X = \{x_1, \dots, x_v\}$ and $\mathcal{B} = \{\mathrm{B}_1, \dots, \mathrm{B}_b\}$. Then the **incidence matrix** of (X, B) is the matrix (a_{ij}) where

$$a_{ij} = \begin{cases} 1 & x_i \in \mathrm{B}_j \\ 0 & x_i \notin \mathrm{B}_j \end{cases}.$$

So the incidence matrix A is indexed by x_i and B_j. Every column has k ones, and every row has r ones.

Proposition 3.5. *Let* A *be the incidence matrix of a* 2-(v, k, λ) *design. Then*

$$AA^\intercal = \begin{pmatrix} r & & \lambda \\ & \ddots & \\ \lambda & & r \end{pmatrix} = \lambda \mathrm{J}_v + (r - \lambda)\,\mathrm{I}_v,$$

a $v \times v$ *matrix.*

Proof.

$$\left(AA^\intercal\right)_{ij} = A_{i\cdot} \cdot A_{j\cdot} = \left|\{B \in \mathcal{B} \mid x_i \in B,\ x_j \in B\}\right| = \begin{cases} r & i = j \\ \lambda & i \neq j \end{cases}.$$

□

Proposition 3.6. *For* A *as in 3.5,*

$$\det AA^\intercal = (r - \lambda)^{v-1}\,(\lambda\,(v-1) + r)\,.$$

Proof.

$$\begin{aligned} \left|\begin{pmatrix} r & & \lambda \\ & \ddots & \\ \lambda & & r \end{pmatrix}\right| &= \left|\begin{pmatrix} r & \lambda - r & \dots & \lambda - r \\ \lambda & r - \lambda & & 0 \\ \vdots & & \ddots & \\ \lambda & 0 & & r - \lambda \end{pmatrix}\right| && \text{subtract column one from all others} \\ &= \left|\begin{pmatrix} r + (v-1)\,\lambda & 0 & \dots & 0 \\ \lambda & r - \lambda & & 0 \\ \vdots & & \ddots & \\ \lambda & 0 & & r - \lambda \end{pmatrix}\right| && \text{add all other rows to row one} \\ &= (r - \lambda)^{v-1}\,(\lambda\,(v-1) + r)\,. \end{aligned}$$

□

Proposition 3.7. *Let C be an $m \times n$ matrix and D an $n \times r$ matrix. Then*

$$\operatorname{rk} CD \leq \operatorname{rk} C, \qquad \operatorname{rk} CD \leq \operatorname{rk} D.$$

Proof. Let $D = \begin{pmatrix} d_1 & \dots & d_r \end{pmatrix}$. Then $\operatorname{col\,sp} CD = \operatorname{sp}(Cd_1, \dots, Cd_r) \subseteq \operatorname{col\,sp} C$. Similarly, $\operatorname{row\,sp} CD \subseteq \operatorname{row\,sp} D$. ☐

Proof of 3.4. Since $bk = vr$, suffices to show $b \geq v$. Since $\lambda(v-1) = r(k-1)$, the assumption $v > k$ implies that $r \geq \lambda$. By 3.7,

$$\det AA^\intercal = (r-\lambda)^{v-1}((v-1)\lambda + r) \neq 0,$$

so $\operatorname{rk} AA^\intercal = v$. But A is $v \times b$, so $\operatorname{rk} A \leq b$. Hence by 3.7, $v = \operatorname{rk} AA^\intercal \leq \operatorname{rk} A \leq b$. ☐

3.2.2 Symmetric 2-designs

The extremal case of Fisher is $b = v$, so $k = r$.

Definition. A 2-(v,k,λ) design is **symmetric** if $b = v$.

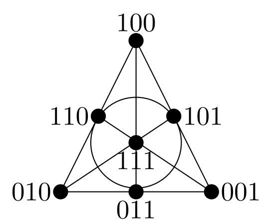
Example. Let

$$X = \mathbb{Z}_2^3 \setminus \{0\}, \qquad \mathcal{B} = \{\{x, y, x+y\} \mid x, y \in X, \ x \neq y\}.$$

This is a 2-$(7,3,1)$ design. Then

$$r = \frac{v-1}{k-1}\lambda = \frac{6}{2}(1) = 3 = k,$$

so symmetric, and $b = v = 7$. This is the Fano plane



.

Note. This is the smallest example of a projective plane.

Definition. A **projective plane** is a symmetric 2-$(v,k,1)$ design where $k \geq 3$.

Theorem 3.8. *In a symmetric 2-(v,k,λ) design, if v is even, then $k-\lambda$ is a square.*

Example. Does there exist a 2-$(22,7,2)$ design?

$$r = \frac{v-1}{k-1}\lambda = \frac{21}{6}(2) = 7 = k,$$

so design is symmetric and $b = v = 22$ is even, but $k - \lambda = 7 - 2 = 5$ is not a square, so no by 3.8.

Proof. As $b = v$, the incidence matrix A is $v \times v$, a square. So $\det A$ exists and $\det A = \det A^\intercal$. Then $\det AA^\intercal = \det A \det A^\intercal = \det A^2$. By 3.5,

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

Now $\lambda(r-1) = r(k-1) = k(k-1)$. Then

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

The right hand side is the square of an integer, so $(r-\lambda)^{v-1}$ is a square, but $v-1$ is odd so $r - \lambda = k - \lambda$ is a square. ☐

Note. If v is odd, then the **Bruck-Ryser-Chowla theorem** gives another necessary condition for the existence of a 2-(v,k,λ) design. The Diophantine equation

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

has a solution $x, y, z \in \mathbb{Z}$, not all zero. Various proofs, by linear algebra and number theory.

Theorem 3.9. *In a symmetric 2-(v,k,λ) design, any two distinct blocks intersect in λ points.*

Example.

- In the Fano plane, any two lines meet in one point.
- In a projective plane, any two blocks, or **lines**, intersect in one point. In fact, projective planes are usually defined using the axioms, a set of points and a set of lines such that
  - any two points lie on a unique line,
  - any two lines meet in a unique point, and
  - there exist four points, no three of which lie on a line.

Lecture 23 Tuesday 27/11/18

Proof of 3.9. By 3.5,

$$AA^{\intercal} = \lambda \mathrm{J} = (k-\lambda)\,\mathrm{I} = \begin{pmatrix} k & & \lambda \\ & \ddots & \\ \lambda & & k \end{pmatrix}. \tag{6}$$

Considering $A^{\intercal}A$,

$$\left(A^{\intercal}A\right)_{ij} = A^{\intercal}_{i\cdot}A_{\cdot j} = A_{\cdot i}\cdot A_{\cdot j} = \left|\mathrm{B}_i \cap \mathrm{B}_j\right|.$$

If $A^{\intercal}A = AA^{\intercal}$, then $\left|\mathrm{B}_i \cap \mathrm{B}_j\right| = \lambda$ when $i \ne j$. Show $A^{\intercal}A = AA^{\intercal}$.

- A is a square matrix, so $\det A$ exists.
- As before, we saw $\det A^2 = (r-\lambda)^{v-1}\left(\lambda\,(v-1)+r\right)$. If $r=\lambda$, then $r=\lambda=k=v$, by standard equations, so $v=b=1$, but $v \ge 2$, a contradiction.
- Thus $\det A \ne 0$, so A is invertible.
- $A\mathrm{J} = r\mathrm{J}$ and $\mathrm{J}A = k\mathrm{J}$. So $A\mathrm{J} = \mathrm{J}A$.
- By (6), A commutes with $AA^{\intercal}$, that is $A\left(AA^{\intercal}\right) = \left(AA^{\intercal}\right)A$. Multiply on the left by A^{-1} to get $AA^{\intercal} = A^{\intercal}A$.

$\square$

Note. A converse to 3.9 exists. A 2-(v,k,λ) design with $v > k$ and the property that any two blocks meet in λ points is symmetric. Sheet 4. [15]

3.3 Automorphism group of a design

3.3.1 Isomorphisms of designs

Definition. Designs $(X_1, \mathcal{B}_1)$ and $(X_2, \mathcal{B}_2)$ are **isomorphic** if there exists a bijection $\phi : X_1 \to X_2$ such that $\phi\left(\mathcal{B}_1\right) = \mathcal{B}_2$, where

$$\phi\left(\mathcal{B}_1\right) = \left\{\phi\left(B\right) \mid B \in \mathcal{B}_1\right\}, \qquad \phi\left(B\right) = \left\{\phi\left(b\right) \mid b \in B\right\}, \qquad B \in \mathcal{B}_1.$$

Note. Isomorphic designs have the same parameters, but the converse need not be true.

Example. Let

$$X = \mathbb{Z}_7, \qquad \mathcal{B}_1 = \left\{013 + i \mid i \in \mathbb{Z}_7\right\}, \qquad X = \mathbb{Z}_2^3 \setminus \{0\}, \qquad \mathcal{B}_2 = \left\{\{x, y, x+y\} \mid x, y \in X_2,\ x \ne y\right\},$$

which are 2-$(7,3,1)$. Is $(X_1, \mathcal{B}_1) \cong (X_2, \mathcal{B}_2)$? The answer is yes. Want a bijection $X_1 \to X_2$, where

$$013 \mapsto \{100, 010, 110\}, \qquad 124 \mapsto \{010, 001, 011\}.$$

[15] Exercise

The rest is forced, so

$$235 \mapsto \{001, 110, 111\} \qquad 346 \mapsto \{110, 011, 101\} \qquad 450 \mapsto \{011, 111, 100\}$$
$$561 \mapsto \{111, 101, 010\} \qquad 602 \mapsto \{101, 100, 001\}.$$

Have an isomorphism

$$0 \mapsto 100, \qquad 1 \mapsto 010, \qquad 2 \mapsto 001, \qquad 3 \mapsto 110, \qquad 4 \mapsto 011, \qquad 5 \mapsto 111, \qquad 6 \mapsto 101.$$

In fact send

$$0 \mapsto x, \qquad 1 \mapsto y, \qquad 2 \mapsto z, \qquad x \neq y, \qquad z \notin \{x, y, x+y\}.$$

Then get an isomorphism. There are $7 \cdot 6 \cdot 4 = 168$ possible isomorphisms.

3.3.2 Automorphisms of designs

Definition. Let $\mathcal{D} = (X, \mathcal{B})$ be a design. The **automorphism group** of $\mathcal{D}$ is

$$\operatorname{Aut} \mathcal{D} = \{\phi \in \operatorname{Sym} X \mid \phi(\mathcal{B}) = \mathcal{B}\}.$$

Prove $\operatorname{Aut} \mathcal{D}$ is a subgroup of $\operatorname{Sym} X$. Sheet 4. [16]

Example.

- Let $\mathcal{D}$ be a trivial design, so $\mathcal{B}$ is the k-subsets of X. Then $\operatorname{Aut} \mathcal{D} = \operatorname{Sym} X$.
- $\operatorname{Aut} \mathcal{D} = \mathrm{GL}_3(\mathbb{Z}_2)$ where $\mathcal{D}$ is the design from the last example.

3.4 Constructions of 2-designs

3.4.1 Difference sets

Example. Let

$$X = \mathbb{Z}_7 = \{0, \dots, 6\}, \qquad \mathrm{B}_0 = \{0, 1, 3\}.$$

Use B_0 to define seven blocks

$$\mathrm{B}_i = \mathrm{B}_0 + i = \{x + i \mid x \in \mathrm{B}_0\}, \qquad 0 \leq i \leq 6.$$

Let $\mathcal{B} = \{\mathrm{B}_i \mid i \in \mathbb{Z}_7\}$. The blocks are $013, 124, 235, 346, 450, 561, 602$. Claim that $(X, \mathcal{B})$ forms a 2-$(7, 3, 1)$ design. Consider $\mathrm{B}_0 = \{0, 1, 3\}$. The differences $a - b$ where $(a, b) \in \mathrm{B}_0$ and $a \neq b$ are

$$0 - 1 = 6, \qquad 0 - 3 = 4, \qquad 1 - 0 = 1, \qquad 1 - 3 = 5, \qquad 3 - 0 = 3, \qquad 3 - 1 = 2.$$

So the differences are $1, \dots, 6$, and each occurs exactly once, so the claim holds by the statement below.

Definition. Let $\lambda, v \in \mathbb{N}$. Let

$$\emptyset \neq \mathrm{B}_0 \subseteq \mathbb{Z}_v = \{0, \dots, v - 1\}.$$

Say B_0 is a **λ-difference set** if for all $d \in \mathbb{Z}_v^*$, there exist exactly λ pairs (a, b) such that $a - b = d$.

$\lambda = 1$ implies that $|\mathrm{B}_0| \geq 2$.

Proposition 3.10. *Let $X = \mathbb{Z}_v$ and $\mathrm{B}_0 \subseteq \mathbb{Z}_v$ be a λ-difference set with $\mathrm{B}_0 = k$. Let*

$$\mathcal{B} = \{\mathrm{B}_0 + i \mid i \in \mathbb{Z}_v\}.$$

Then $(X, \mathcal{B})$ is a 2-(v, k, λ) design that is symmetric.

Proof. Let $r, s \in \mathbb{Z}_v$ for $r \neq s$. Then $r, s \in \mathrm{B}_0 + i$ if and only if $r - i, s - i \in \mathrm{B}_0$. The number of such i is the number of pairs (a, b) with $a, b \in \mathrm{B}_0$ and $a - b = r - s$. This equals λ. Thus r and s lie in exactly λ blocks. $\square$

[16] Exercise

Example.

- Let
$$X = \mathbb{Z}_{11}, \qquad \mathcal{B} = \left\{x^2 \mid x \in \mathbb{Z}_{11}^*\right\} = \{1, 4, 9, 5, 3\}.$$
The differences $a - b$, where there are 20 of them, each occurs twice. So
$$(X, \{\mathrm{B}_0, \dots, \mathrm{B}_0 + 10\})$$
is a 2-$(11, 5, 2)$ design, which is symmetric.

- Let
$$X = \mathbb{Z}_{13}, \qquad \mathcal{B} = \{0, 1, 3, 9\}.$$
This is a 1-difference set, so get a 2-$(13, 4, 1)$ design.

The following is a family. Let p be an odd prime and $Q = \left\{x^2 \mid x \in \mathbb{Z}_p^*\right\}$. Seen Q is a subgroup of $\left(\mathbb{Z}_p^*, \times\right)$ of order $(p-1)/2$.

Proposition 3.11. *If $p \equiv 3 \mod 4$, then Q is a λ-difference set where $\lambda = (p-3)/4$, so get a symmetric 2-$(p, (p-1)/2, (p-3)/4)$ design.*

Example. $p = 7$ and $p = 11$ is in the examples above. The next p is 19, so parameters are $(19, 9, 4)$.

Proof. Since $p \equiv 3 \mod 4$, $|Q| = (p-1)/2$ is odd. Since $-1 \in \mathbb{Z}_p^*$ has order two, the cosets of Q in $\left(\mathbb{Z}_p^*, \times\right)$ are Q and $(-1)Q = -Q$. So $\mathbb{Z}_p^* = Q \cup -Q$. For $q \in \mathbb{Z}_p^*$, define
$$S_q = \{(a, b) \mid a, b \in Q, \ a - b = q\}.$$

- $a - b = q$ if and only if $ra - rb = rq$. So $(a, b) \in S_q$ if and only if $(ra, rb) \in S_q$. Thus $|S_q| = |S_{rq}|$ for all $r \in Q$ and $q \in \mathbb{Z}_p^*$. In particular, $|S_q|$ is constant for $q \in Q$.
- Now $(a, b) \in S_q$ if and only if $(b, a) \in S_{-q}$ so $|S_q| = |S_{-q}|$ for all $q \in \mathbb{Z}_p^*$. Since $Q \cup (-Q) = \mathbb{Z}_p^*$, $|S_q|$ is constant for $q \in \mathbb{Z}_p^*$.

Thus Q is a λ-difference set for some λ. To find λ, the number of ordered pairs (a, b) for $a, b \in Q$ and $a \neq b$ is $|Q|(|Q| - 1)$. Also equals $\lambda(p-1)$. Since $|Q| = (p-1)/2$, $\lambda = (p-3)/4$. ☐

3.4.2 Affine planes

Let the **Euclidean plane** be $\mathbb{R}^2$. We define the points as vectors in $\mathbb{R}^2$, and the blocks as straight lines, by Cartesian equations
$$y = mx + c, \qquad x = d,$$
or by vector equations
$$\{v + \lambda w \mid \lambda \in \mathbb{R}\} = v + \operatorname{sp} w, \qquad w \neq 0.$$
Any two points lie on a unique line, since points are x and y implies that the line is $x + \operatorname{sp}(y - x)$. This is naturally an infinite 2-design. To make a finite 2-design, we replace $\mathbb{R}$ by any finite field F, such as $\mathbb{Z}_p$. The points are vectors in $F^2 = \{(a, b) \mid a, b \in F\}$, the vector space over F with basis $(1, 0)$ and $(0, 1)$, and the blocks, or lines, are sets of the form
$$v + \operatorname{sp} w, \qquad v, w \in F^2, \qquad w \neq 0.$$

Note.

- There are q^2 points where $|F| = q$. A fact is that q is a power of a prime.
- The lines are solution sets of equations $y = mx + c$ if and only if the line is $(0, c) + \operatorname{sp}(1, m)$.
- The lines are solution sets of equations $x = d$ if and only if the line is $(d, 0) + \operatorname{sp}(0, 1)$.

Lecture 24
Wednesday
28/11/18

Example. Let $F = \mathbb{Z}_3$. There are nine lines $y = mx + c$ and $x = d$.

- $y = x$ is
$$\{(0,0), (1,1), (2,2)\} = \mathrm{sp}(1,1).$$
- $y = x + 1$ is
$$\{(0,1), (1,2), (2,0)\} = (0,1) + \mathrm{sp}(1,1).$$
- $x = 1$ is
$$\{(1,0), (1,1), (1,2)\} = (1,0) + \mathrm{sp}(0,1).$$

Proposition 3.12.

1. *Every line has q points.*
2. *Two points lie in a unique line.*

Hence, if $\mathcal{L}$ is the set of lines, then $\left(F^2, \mathcal{L}\right)$ is a 2-$\left(q^2, q, 1\right)$ design.

Proof.

1. A line has the form
$$v + \mathrm{sp}\, w = \{v + \lambda w \mid \lambda \in F\}, \qquad w \neq 0.$$
This has size q since $|F| = q$.
2. Let $a, b \in F^2$ where $a \neq b$. Then a and b are in the line
$$L = a + \mathrm{sp}(b - a) = \{a + \lambda(b - a) \mid \lambda \in F\}.$$
Suppose L' is a line on a and b, so
$$L' = v + \mathrm{sp}\, w, \qquad v, w \in F^2, \qquad w \neq 0.$$
Then $a = v + \lambda_1 w$ and $b = v + \lambda_2 w$ for some $\lambda_1, \lambda_2 \in F$. Note that $\lambda_1 \neq \lambda_2$. Then $b - a = (\lambda_2 - \lambda_1) w$, so
$$L = \{a + \lambda(b - a) \mid \lambda \in F\} = \{(v + \lambda_1 w) + \lambda(\lambda_2 - \lambda_1) w \mid \lambda \in F\} = v + \mathrm{sp}\, w = L'.$$

$\square$

Definition. The 2-$\left(q^2, q, 1\right)$ design $\left(F^2, \mathcal{L}\right)$ is the **affine plane over** F, denoted by $\mathrm{AG}(2, F)$.

Thus any two lines meet in zero or one point. Call two lines **parallel** if they meet in zero points.

Example. $y = mx + c$ and $y = mx + d$ where $c \neq d$ are parallel.

Proposition 3.13. $\mathrm{AG}(2, F)$ *has $q^2 + q$ lines, where $q = |F|$. They fall into $q + 1$ pairwise disjoint sets of size q, each consisting of parallel lines.*

Proof. The $q + 1$ sets are
$$\mathcal{L}_m = \{y = mx + c \mid c \in F\}, \qquad m \in F, \qquad \mathcal{L}_\infty = \{x = d \mid d \in F\}.$$
Each set contains q parallel lines. $\square$

Definition. The sets $\mathcal{L}_m$ for $m \in F \cup \{\infty\}$ are called **parallel classes** of lines.

Proposition 3.14. *Each point in F^2 lies on exactly one line in each parallel class.*

Proof. Each parallel class contains q pairwise disjoint lines. Each line has q points. This accounts for $q^2 = \left|F^2\right|$ points. $\square$

3.4.3 Projective planes

Recall that a projective plane is a symmetric 2-$(v, k, 1)$ design with $k \geq 3$.

- Any two points lie on a unique line.
- Any two lines meet in a unique point, by 3.9.

We can extend $\mathrm{AG}(2, F)$ to get a projective plane.

Example. In $\mathrm{AG}(2, \mathbb{Z}_3)$, there are four parallel classes of lines $\mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_\infty$. For each parallel class, add a new point p_m to the lines in $\mathcal{L}_m$ where $m \in F \cup \{\infty\}$. Now we have the 13 points

$$p \in F^2, \qquad p_0, \qquad p_1, \qquad p_2, \qquad p_\infty.$$

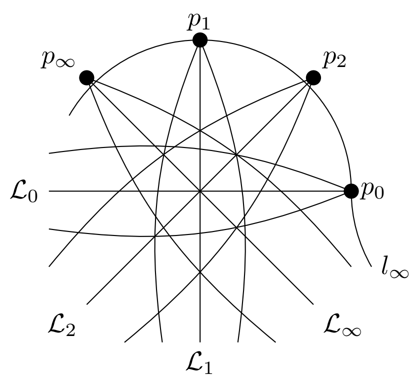
We have the 12 lines

$$(y = x) \cup \{p_0\} = \{00, 11, 22, p_0\}, \qquad (y = x + 1) \cup \{p_1\} = \{01, 12, 20, p_1\}, \qquad \dots.$$

Add one more line

$$l_\infty = \{p_0, p_1, p_2, p_\infty\}.$$

Now we have 13 points and 13 lines. These form the projective plane over $\mathbb{Z}_3$,



.

Definition. In general, for a finite field F for $|F| = q$,

- start with $\mathrm{AG}(2, F)$, points F^2, and lines $y = mx + c$ and $x = d$,
- add $q + 1$ new points p_m for $m \in F \cup \{\infty\}$,
- to each line in $\mathcal{L}_m$, add the point p_m for $m \in F \cup \{\infty\}$, and
- add one more line $l_\infty = \{p_m \mid m \in F \cup \{\infty\}\}$, the **line at infinity**.

Now have $q^2 + q + 1$ points,

$$F^2, \qquad p_m, \qquad m \in F \cup \{\infty\},$$

and $q^2 + q + 1$ lines,

$$l \in \mathrm{AG}(2, F), \qquad l_\infty.$$

This is the **projective plane over** F, denoted by $\mathrm{PG}(2, F)$.

Proposition 3.15. $\mathrm{PG}(2, F)$ *is a symmetric* 2-$\left(q^2 + q + 1, q + 1, 1\right)$ *design, so is actually a projective plane.*

Proof. Need to show that any two points lie on a unique line. Let x and y be points of $\mathrm{PG}(2, F)$ where $x \neq y$.

- Suppose $x, y \in F^2$. Then the unique line on x and y is the unique line $x + \mathrm{sp}(y - x)$ from $\mathrm{AG}(2, F)$.
- Suppose $x \in F^2$ and $y = p_m$ for some $m \in F \cup \{\infty\}$. Then x lies on a unique line in the parallel class $\mathcal{L}_m$, by 3.14, say l, and $l \cup \{\infty\}$ is the unique line on x and y.
- Suppose $x = p_{m_1}$ and $y = p_{m_2}$ for some $m_1, m_2 \in F \cup \{\infty\}$. Then l_∞ is the unique line on x and y.

$\square$

3.4.4 More on projective planes

Lecture 25 Tuesday 04/12/18

Recall the axioms.

- Two points are on a unique line.
- Two lines intersect in a unique point.
- There exist four points, no three of which are collinear.

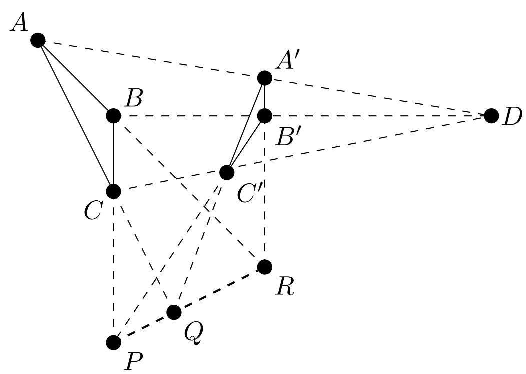
Sheet 4 implies that a projective plane defined by these axioms is equivalent to a 2-$\left(n^2+n+1, n+1, 1\right)$ design where $n > 1$. [17] Call this the **projective plane** of **order** n.

Example.

- The Fano plane is the projective plane of order two.
- $\text{PG}(2, F)$ is a projective plane over a field F, and $|F| = q$ where q is a power of a prime p, which is a 2-$\left(q^2+q+1, q+1, 1\right)$ design. So $\text{PG}(2, F)$ has order q.

Note. There exist other projective planes. The smallest has order nine.

Take triangles ABC and $A'B'C'$, so



.

Desargues condition is that AA', BB', CC' all meet in a point if and only if P, Q, R are collinear.

- **Desargues theorem** is that $\text{PG}(2, F)$ for F a finite field satisfies this condition. Conversely, any finite projective plane satisfying this condition is isomorphic to $\text{PG}(2, F)$ for some finite field F. Call the projective planes $\text{PG}(2, F)$ **Desarguesian**.
- There exist **non-Desarguesian** projective planes, but they all have order a prime power. A question is do all finite projective planes have order a prime power? A corollary of Bruck-Ryser-Chowla is that if a projective plane of order n exists where $n \equiv 1 \mod 4$ or $n \equiv 2 \mod 4$, then n is a sum of squares. Bruck-Ryser-Chowla implies that for a symmetric 2-(v, k, λ) design for v odd,

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

  has an integer solution. Then $v = n^2 + n + 1$ is odd, and $n \equiv 1, 2 \mod 4$ implies that $v \equiv 3 \mod 4$. So $z^2 = nx^2 - y^2$. So $nx^2 = z^2 + y^2$. Thus $n = (z/x)^2 + (y/x)^2$, so $n = a^2 + b^2$ where $a, b \in \mathbb{Z}$, by number theory.

Example. Say n is not a prime power.

- $n = 6 \equiv 2 \mod 4$ is not a sum of squares. Thus no projective plane of order six.
- $n = 10 \equiv 2 \mod 4$ but $10 = 1 + 9$ so cannot use theorem. No such projective plane exists by a massive computer computation.
- $n = 12$ is unknown.

[17] Exercise

3.4.5 Higher-dimensional geometry

Let F be a finite field. Define
$$F^n = \{(x_1, \dots, x_n) \mid x_i \in F\}.$$
This is a vector space over F of dimension n, and $|F^n| = q^n$ where $q = |F|$.

Definition. For $1 \le m \le n$, define the **q-binomial coefficients**
$$\binom{n}{m}_q = \frac{(q^n - 1) \dots \left(q^{n-m+1}\right)}{(q^m - 1) \dots (q - 1)}.$$

Example.
$$\binom{n}{1}_q = \frac{q^n - 1}{q - 1}, \qquad \binom{4}{2}_2 = \frac{\left(2^4 - 1\right)\left(2^3 - 1\right)}{\left(2^2 - 1\right)(2 - 1)} = \frac{15 \cdot 7}{3 \cdot 1} = 35, \qquad \binom{2}{1}_q = q + 1.$$

Lecture 26 is a problems class.

Lecture 26 Tuesday 04/12/18

Lecture 27 Wednesday 05/12/18

Proposition 3.16. *Let $1 \le m \le n - 1$, F be a field, and $|F| = q$.*

1. *The number of m-dimensional subspaces of F^n is $\binom{n}{m}_q$.*
2. *If $0 \ne v \in F^n$, then the number of m-dimensional subspaces of F^n containing v is*
$$\begin{cases} 1 & m = 1 \\ \binom{n-1}{m-1}_q & m \ge 2 \end{cases}.$$
3. *If $v, w \in F^n$ are linearly independent and $m \ge 2$, then the number of m-dimensional subspaces of F^n containing v and w is*
$$\begin{cases} 1 & m = 2 \\ \binom{n-2}{m-2}_q & m > 2 \end{cases}.$$

The proof is later. Now define a design as follows. Let $n \ge 2$ and $1 \le m \le n - 1$. The points are vectors in F^n, and the blocks are subsets of the form
$$v + W = \{v + w \mid w \in W\}, \qquad v \in F^n,$$
and W is any m-dimensional subspace of F^n.

Example. Let $n = 2$ and $m = 1$. The points are vectors in F^2, and the blocks are subsets of the form
$$v + \operatorname{sp} w, \qquad v, w \in F^2, \qquad w \ne 0.$$
This is $\mathrm{AG}(2, F)$.

Proposition 3.17.

1. *This is a 2-(q^n, q^m, λ) design where*
$$\lambda = \begin{cases} 1 & m = 1 \\ \binom{n-1}{m-1}_q & m \ge 2 \end{cases}.$$
2. *If $F = \mathbb{Z}_2$ and $m \ge 2$, then this is a 3-$(2^n, 2^m, r_3)$ design where*
$$r_3 = \begin{cases} 1 & m = 2 \\ \binom{n-2}{m-2}_2 & m > 2 \end{cases}.$$

We call this design $\mathrm{AG}(n, F)_m$.

Example.

- $\mathrm{AG}\left(3,\mathbb{Z}_3\right)_1$ is a 2-$(27,3,1)$ design, which are points and lines in $\mathbb{Z}_3^3$.
- $\mathrm{AG}\left(3,\mathbb{Z}_3\right)_2$ is a 2-$(27,9,4)$ design.
- $\mathrm{AG}\left(3,\mathbb{Z}_2\right)_2$ is a 3-$(8,4,1)$ design. A fact is that this is isomorphic to the design obtained from weight four codewords in the extended Hamming code H'.

Proof of 3.17.

1. The lines have the size of an m-dimensional subspace, which is q^m. Let $v, w \in F^n$ be distinct. Any block containing v has the form $v + W$ for some m-dimensional subspace W. Now $w \in v + W$ if and only if $v - w \in W$. The number of blocks containing v and w is the number of m-dimensional subspaces of F^n containing $v - w$, which is what we want by 3.16.

2. Let $F = \mathbb{Z}_2$ and $m \geq 2$. Let $\{v_1, v_2, v_3\}$ be a 3-subset of F^n. Any block containing v_1 has the form $v_1 + W$ for some m-dimensional subspace W. Then $v_2, v_3 \in v_1 + W$ if and only if $v_1 - v_2, v_1 - v_3 \in W$. The number of blocks containing v_1, v_2, v_3 is the number of m-dimensional subspaces containing $v_1 - v_2$ and $v_2 - v_3$, so $F = \mathbb{Z}_2$ implies that these are linearly independent, which is what we want by 3.16.

$\square$

Proof of 3.16.

1. An m-dimensional subspace W has a basis $w_1, \dots, w_m$. Let N be the number of pairs $\left(\left(w_1, \dots, w_m\right), W\right)$ where $\left(w_1, \dots, w_m\right)$ is an ordered list of linearly independent vectors, and $W = \mathrm{sp}\left(w_1, \dots, w_m\right)$.

   - Then N is the number of such m-tuples times one. Counting the number of m-tuples $\left(w_1, \dots, w_m\right)$ where $\{w_i\}$ is linearly independent,

     $$q^n - 1 \text{ choices of } w_1 \in F^n \setminus \{0\}, \qquad q^n - q \text{ choices of } w_2 \in F^n \setminus \mathrm{sp}\, w_1, \qquad \dots.$$

     Thus $N = \left(q^n - 1\right) \dots \left(q^n - q^{m-1}\right)$.

   - On the other hand, N is the number of m-dimensional subspaces times the number of ordered bases of a particular m-dimensional subspace W, so

     $$N = (\text{number of } m\text{-dimensional subspaces}) \times \left(q^m - 1\right) \dots \left(q^m - q^{m-1}\right).$$

     Thus the number of m-dimensional subspaces is

     $$\frac{\left(q^n - 1\right) \dots \left(q^n - q^{m-1}\right)}{\left(q^m - 1\right) \dots \left(q^m - q^{m-1}\right)} = \frac{\left(q^n - 1\right) \dots \left(q^{n-m+1} - 1\right)}{\left(q^m - 1\right) \dots \left(q - 1\right)} = \binom{n}{m}_q.$$

2. Let $0 \neq v \in F^n$.

   - If $m = 1$, then $\mathrm{sp}\, v$ is the only one-dimensional subspace containing v, as desired.
   - Suppose $m \geq 2$. Extend to a basis $v, v_2, \dots, v_n$ of F^n. Let $V_0 = \mathrm{sp}\left(v_2, \dots, v_n\right)$. Let W be an m-dimensional subspace of F^n containing v. Let $W_0 = W \cap V_0$ be a subspace of V_0. Note that $W_0 \cap \mathrm{sp}\, v = \{0\}$. Let $w \in W$. Then $w = \lambda v + w_0$ where $w_0 \in V_0$, so $w_0 = w - \lambda v \in W$. So $w_0 \in W_0$. Thus $W = \mathrm{sp}\, v + W_0$. Hence $W = \mathrm{sp}\, v \oplus W_0$, so W_0 has dimension $m - 1$. Proved that any m-dimensional subspace of F^n containing v has the form $\mathrm{sp}\, v \oplus U$ where U is an $(m-1)$-dimensional subspace of V_0. Thus the number of W, the number of $(m-1)$-dimensional subspaces of V_0, which is $(n-1)$-dimensional, is $\binom{n-1}{m-1}_q$, by 1.

3. Similar.

$\square$

3.5 Designs and strongly regular graphs

Have seen two weight codes give strongly regular graphs, by 2.11. Have seen Golay codes give designs. Now see certain designs give strongly regular graphs.

Lecture 28 Tuesday 11/12/18

Definition. A 2-design is **quasisymmetric** if there are $x, y \in \mathbb{Z}$ for $x \neq y$ such that any two blocks intersect in x or y points, and both occur.

Note. Symmetric if and only if two blocks meet in λ points and $v > k$, by 3.9 and sheet 4. [18]

Example.

- $\mathrm{AG}(2, F)$ has lines meeting in zero or one point.
- Golay code G_{23} has
  - points 23 coordinate positions, and
  - blocks B_c such that $\mathrm{wt}\, c = 7$, which are seven coordinate positions with one.

  This is a 4-$(23, 7, 1)$ design, by sheet 2. [19] Then $c \neq d$ implies that $|\mathrm{B}_d \cap \mathrm{B}_c| = 1$ or $|\mathrm{B}_d \cap \mathrm{B}_c| = 3$.

Theorem 3.18. *Let $(X, \mathcal{B})$ be a quasisymmetric 2-design with blocks intersecting in x or y points with $x < y$. Define a graph $\Gamma(\mathcal{B})$ by $\mathrm{B}_1 \sim \mathrm{B}_2$ if and only if $|\mathrm{B}_1 \cap \mathrm{B}_2| = x$. Then $\Gamma(\mathcal{B})$ is strongly regular.*

Example. Let $(X, \mathcal{B}) = \mathrm{AG}(2, F)$ and $|F| = q$. Then $\Gamma(\mathcal{B})$ has vertices lines and $l_1 \sim l_2$ if and only if l_1 and l_2 are parallel. Thus $\Gamma(\mathcal{B})$ is a union of $q + 1$ complete graphs.

Proposition 3.19. *Suppose Γ is a graph with v vertices and adjacency matrix A. Assume $\Gamma \neq \mathrm{K}_v, \overline{\mathrm{K}_v}$. Then the following are equivalent.*

1. *Γ is strongly regular.*
2. *$A^2 = \alpha A + \beta \mathrm{I} + \gamma \mathrm{J}$ for some $\alpha, \beta, \gamma \in \mathbb{R}$.*

Proof.

$1 \implies 2$ 2.6.

$2 \implies 1$ Assume 2. Then

$$\left(A^2\right)_{ij} = \begin{cases} \beta + \gamma & i = j \\ \alpha + \gamma & i \neq j,\ i \sim j \\ \gamma & i \neq j,\ i \nsim j \end{cases}.$$

Also,

$$\left(A^2\right)_{ij} = A_{i \cdot} A_{\cdot j} = A_{i \cdot} \cdot A_{j \cdot} = |\{k \in \Gamma \mid i \sim k,\ j \sim k\}|.$$

So

$$\Gamma = \mathrm{srg}\left(v, \beta + \gamma, \alpha + \gamma, \gamma\right).$$

□

[18] Exercise

[19] Exercise

Proof of 3.18. Let M be the $v \times b$ incidence matrix of $(X, \mathcal{B})$ and A be the $b \times b$ adjacency matrix of $\Gamma(\mathcal{B})$. By 3.5,

$$MM^\intercal = \lambda \mathrm{J}_v + (r - \lambda)\mathrm{I}_v, \tag{7}$$

$$M\mathrm{J}_{b\times t} = r\mathrm{J}_{v\times t}, \qquad \mathrm{J}_{t\times v}M = k\mathrm{J}_{t\times b}. \tag{8}$$

Considering $M^\intercal M$, a $b \times b$ matrix,

$$\left(M^\intercal M\right)_{ij} = M_{\cdot i} \cdot M_{\cdot j} = |\mathrm{B}_i \cap \mathrm{B}_j| = \begin{cases} k & i = j \\ x & i \neq j,\ \mathrm{B}_i \sim \mathrm{B}_j \\ y & i \neq j,\ \mathrm{B}_i \nsim \mathrm{B}_j \end{cases}.$$

Hence

$$M^\intercal M = k\mathrm{I}_b + xA + y\left(\mathrm{J}_b - A - \mathrm{I}_b\right) = (x - y)A + (k - y)\mathrm{I}_b + y\mathrm{J}_b. \tag{9}$$

As $x \neq y$

$$A = fM^\intercal M + g\mathrm{I}_b + k\mathrm{J}_b, \qquad f = \frac{1}{x - y}, \qquad g = \frac{y - k}{x - y}, \qquad k = \frac{-y}{x - y}.$$

Now we use (7) to (9) to compute

$$\begin{aligned} A^2 &= \left(fM^\intercal M + g\mathrm{I}_b + k\mathrm{J}_b\right)\left(fM^\intercal M + g\mathrm{I}_b + k\mathrm{J}_b\right) \\ &= f^2 M^\intercal MM^\intercal M + g^2\mathrm{I}_b + k^2\mathrm{J}_b^2 + 2fgM^\intercal M + 2gk\mathrm{J}_b + kfM^\intercal M\mathrm{J}_b + kf\mathrm{J}_b M^\intercal M. \end{aligned}$$

To use 3.19, show that each term here can be expressed in terms of $A, \mathrm{I}_b, \mathrm{J}_b$.

$$\begin{aligned} M^\intercal MM^\intercal M &= M^\intercal\left(\lambda\mathrm{J}_v + (r - \lambda)\mathrm{I}_v\right)M && \text{by } (7), \\ &= \lambda k\mathrm{J}_{b\times v}M + (r - \lambda)M^\intercal M && \text{by } (8), \\ &= \lambda k^2\mathrm{J}_b + (r - \lambda)M^\intercal M && \text{by } (8), \\ &= (r - \lambda)(x - y)A + (r - \lambda)(k - y)\mathrm{I}_b + \left(\lambda k^2 + (r - \lambda)y\right)\mathrm{J}_b && \text{by } (9). \end{aligned}$$

$$\mathrm{J}_b^2 = b\mathrm{J}_b \qquad .$$

$$M^\intercal M = (x - y)A + (k - y)\mathrm{I}_b + y\mathrm{J}_b \qquad \text{by } (9).$$

$$\begin{aligned} M^\intercal M\mathrm{J}_b &= rM^\intercal\mathrm{J}_v && \text{by } (8), \\ &= rk\mathrm{J}_b && \text{by } (8). \end{aligned}$$

$$\begin{aligned} \mathrm{J}_b M^\intercal M &= r\mathrm{J}_v M && \text{by } (8), \\ &= rk\mathrm{J}_b && \text{by } (8). \end{aligned}$$

From these, there exist $\alpha, \beta, \gamma \in \mathbb{Q}$ with

$$A^2 = \alpha A + \beta\mathrm{I}_b + \gamma\mathrm{J}_b,$$

so by 3.19, $\Gamma(\mathcal{B})$ is strongly regular. Work out the parameters. [20] □

Lecture 29 Tuesday 11/12/18

Lecture 29 is a class test.
Lecture 30 is a problems class.

Lecture 30 Wednesday 12/12/18

[20] Exercise