These notes are based on a course of lectures given by Professor Liebeck during Autumn Term 2007 at Imperial College London. In general the notes follow the lectures very closely and only few changes were made mostly to make the typesetting easier. These notes have not been checked by Professor Liebeck and should not be regarded as official notes for the course. In particular, all the errors are made by me. However, I don't take any responsibility for their consequences; use at your own risk (and attend lectures, they are fun). Please email me at as1005@ic.ac.uk with any comments or corrections.

Anton Stefanek
March 2008
# Contents

## 1 Introduction

1.1 Codes ........................................... 1  
1.2 Graphs ........................................... 2  
1.3 Designs ........................................... 2

## 2 Error-correcting codes

2.1 Code correction ..................................... 5  
2.2 Linear codes ..................................... 6  
2.3 The Check Matrix .................................. 7  
   2.3.1 Check matrix and error correction ......... 8  
2.4 Hamming codes .................................... 9  
2.5 Correcting one error ................................ 9  
2.6 Correcting more than one error .................. 9  
2.7 The Hamming Bound ................................ 11  
2.8 Codes correcting 1 error .......................... 12  
2.9 Perfect Codes ..................................... 12  
2.10 Gilbert-Varshamov bound ......................... 13  
2.11 The Golay Code .................................. 14  
   2.11.1 Some numerology for $G_{24}$ and $G_{23}$ .. 17

## 3 Strongly regular graphs

3.1 Theory of strongly regular graphs .................. 22  
3.2 Adjacency matrix .................................. 22  
   3.2.1 Eigenvalues of $A$ ............................ 23  
   3.2.2 Strongly regular graphs with small $v$ .... 28

## 4 Designs

4.1 Theory of $t$-designs ............................... 31  
   4.1.1 Incidence matrix ............................. 32  
   4.1.2 Symmetric $t$-designs ....................... 34  
4.2 Difference sets ................................... 35  
   4.2.1 A family of difference sets ................. 35  
4.3 Affine Planes .................................... 36  
4.4 Projective planes ................................ 37  
4.5 Higher-dimensional geometry ...................... 38

## 5 Some connections

5.1 Isomorphisms of designs ........................... 41
Chapter 1

Introduction

Algebraic combinatorics – we will study

1. error-correcting codes (subsets of $\mathbb{Z}_2^n$),
2. graphs (vertices and edges),
3. designs.

These are "combinatorial" objects. We will study them using linear algebra (vector spaces, matrix theory, eigenvalues,...) and a little group theory.

Prerequisites – none, except a bit of memory.

Books, office hours – see www.ma.ic.ac.uk/~mwl.

Coursework – 1 piece.

1.1 Codes

Code is a language for machine communication. The alphabet consists of 0, 1, the words are selected strings of characters from the alphabet. Recall that

$$\mathbb{Z}_2 = \{0, 1\}$$

(residue classes modulo 2) with

$$0 + 0 = 0, \ 1 + 0 = 0 + 1 = 1, \ 1 + 1 = 0.$$ 

A code of length $n$ is a subset of $\mathbb{Z}_2^n$, where

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

Example.

1. Two messages "yes"(1) and "no"(0) are to be sent. Code \{(111, 000) \subseteq \mathbb{Z}_2^3\} corrects one error: if we send "yes" as 111 and it is received as 101, this can be corrected to 111.

2. We have 8 messages $abc$, $a, b, c \in \mathbb{Z}_2$ and codewords $abcxyz$ where $x = a + b$, $y = a + c$ and $z = b + c$. So code is

\[
\begin{align*}
\{ &000000, 100110, 010101, 001011, \\
&110011, 101101, 011110, 111000 \} \subseteq \mathbb{Z}_2^6.
\end{align*}
\]

This code corrects 1 error. For example, message 000000 is received with one error as 000100 and is then corrected back to nearest codeword 000000.

Aim is to find good codes – sending lots of messages, correcting an appropriate number of errors.
1.2 Graphs

A graph consists of a set $V$ of vertices and a set $E$ of edges of pairs of vertices. We denote this as $\Gamma = \Gamma(V,E)$.

**Example.** $V = \{1, 2, 3\}$, $E = \{(1, 2), (1, 3)\}$.

For any vertex $x \in V$, the neighbours of $x$ are the vertices joined to $x$ by an edge.

**Definition.** Graph $\Gamma$ is *regular* if every vertex has the same number of neighbours. Call this number the *valency* of $\Gamma$.

**Example.**

```
Example of regular graphs with valency 2, 3 and a non regular graph.
```

**Definition.** Graph $\Gamma$ is *strongly regular* if

1. $\Gamma$ is regular,
2. any two joined vertices have the same number $a$ of common neighbours,
3. any two non-joined vertices have the same number $b$ of common neighbours.

**Example.**

```
The square is strongly regular, valency 2, $a = 0$, $b = 2$. The pentagon is strongly regular too, valency 2, $a = 0$, $b = 1$. The hexagon is regular, but not strongly regular. The Petersen graph has valency 3, $a = 0$, $b = 1$.
```

Here is a theorem we will prove using the theory of strongly regular graphs:

**Theorem 1.1** (Friendship theorem). In a community where any 2 people have exactly 1 mutual acquaintance, there is someone who knows everybody. That is, if in a graph every two vertices have exactly one common neighbour, there is a vertex joined to all the other vertices of the graph.

The only known proof uses lots of linear algebra.

1.3 Designs

Manufacturer makes products in $v$ varieties. Consumers test these for fairness:

1. each consumer tests the same number $k$ of varieties,
2. each variety is tested by the same number $r$ of consumers.
Example. Let \( v = 8, \ k = 4 \) and \( r = 3 \). Varieties are 1, 2, \ldots, 8.

<table>
<thead>
<tr>
<th>Consumer</th>
<th>C_1</th>
<th>C_2</th>
<th>C_3</th>
<th>C_4</th>
<th>C_5</th>
<th>C_6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Varieties</td>
<td>1234</td>
<td>5678</td>
<td>1357</td>
<td>2468</td>
<td>1247</td>
<td>3568</td>
</tr>
</tbody>
</table>

Definition. Let \( X \) be a set, \( |X| = v \) and let \( \mathcal{B} \) be a collection of subsets of \( X \), all of size \( k \). Then \( \mathcal{B} \) is a design if every element of \( X \) lies in the same number \( r \) of subsets in \( \mathcal{B} \). The subsets in \( \mathcal{B} \) are the blocks of the design. The parameters are \((v, k, r)\).

Example. In the above example, \( X = \{1, 2, \ldots, 8\} \) with \( \mathcal{B} = \{\{1, 2, 3, 4\}, \{5, 6, 7, 8\}, \ldots\} \).

What parameters \((v, k, r)\) can occur?

Lemma 1.2. If there exists a design with parameters \((v, k, r)\), then

1. \( k \) divides \( vr \),
2. \( \frac{vr}{k} \leq \binom{v}{2} \).

Proof. Count the pairs \((x, B)\) with \( x \in X \) and \( B \in \mathcal{B} \). The number of pairs is:

\[
\text{(number of } x\text{'s)} \times \text{(number of } B\text{'s per } x\text{)} = vr.
\]

It is also

\[
\text{(number of } B\text{'s)} \times \text{(number of } x\text{'s per } B\text{)} = bk
\]

where \( b \) is the number of blocks. So \( bk = vr \). Therefore \( b = \frac{vr}{k} \), an integer, so \( k \mid vr \) and \( \frac{vr}{k} \leq \binom{v}{2} \). \( \square \)

Definition. A design \( \mathcal{B} \) is a 2-design if any 2 elements of \( X \) lie in the same number of blocks. 2-design

This says that any 2 varieties are compared by the same number of consumers.

Example. 1234, 5678, 1357, 2468, 1247, 3568 is not a 2-design – 1, 2 are in two blocks, 1, 6 in none.

More generally, for \( t \in \mathbb{N} \), \( \mathcal{B} \) is a \( t \)-design if every set of \( t \) elements in \( X \) lies in (is a subset of) the same number of blocks.

t-design

For 2-designs, there are lots of nice examples and nice theory. The \( t \)-designs for \( t > 2 \) are much harder to find. For example the first (non-trivial – when \( \mathcal{B} \) is the collection of all the \( k \)-subsets of \( X \)) 6-design wasn’t found until 1982.

Example (A 2-design from geometry). Let \( p \) be a prime. Then \( \mathbb{Z}_p \) is a field. Define the plane \( \mathbb{Z}_p^2 = \{(x_1, x_2) \mid x_i \in \mathbb{Z}_p\} \) with \( p^2 \) points. Define \( X = \mathbb{Z}_p^2 \), \( \mathcal{B} \) as the lines in this plane, i.e. vectors satisfying a linear equation. Any 2 points are on a unique line.
Chapter 2

Error-correcting codes

Recall that $\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_n^2 = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{Z}_2\}$. This is a vector space over $\mathbb{Z}_2$ with addition

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

and scalar multiplication

$$\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$$

for $\lambda \in \mathbb{Z}_2$. We will abbreviate vectors, for example we will write $(1,0,1,1,0)$ as $10110$.

**Definition.** A (binary) code of length $n$ is a subset $C$ of $\mathbb{Z}_n^2$. The vectors in $C$ are called code words.

**Example.** $d(10110, 01100) = 3$.

**Proposition 2.1** (Triangle inequality). For $x, y, z \in \mathbb{Z}_n^2$,

$$d(x, y) + d(y, z) \geq d(x, z).$$

**Proof.** Let $A$ be the set of coordinate positions where $x$ and $z$ differ, i.e. $A = \{i \mid x_i \neq z_i\}$, so $d(x, z) = |A|$. Let

$$B = \{i \mid x_i = y_i, x_i \neq z_i\},$$

$$C = \{i \mid x_i \neq y_i, x_i \neq z_i\}.$$

Then $|B| + |C| = |A| = d(x, z)$ and

$$|B| \leq d(y, z),$$

$$|C| \leq d(x, y).$$

**Definition.** The minimum distance of a code $C$ is

$$d(C) = \min \{d(x, y) \mid x, y \in C, x \neq y\}.$$
Proposition 2.2. Code $C$ corrects $e$ errors iff $d(C) \geq 2e + 1$.

Proof.

$\Rightarrow$ Sheet 1, question 2.

$\Leftarrow$ Suppose $d(C) \geq 2e + 1$. Let $c, c' \in C$ and $x \in \mathbb{Z}_2^n$ with $d(c, x) \leq e$, $d(c', x) \leq e$. Then by 2.1

$$d(c, c') \leq d(c, x) + d(x, c') \leq 2e.$$

As $d(C) \geq 2e + 1$, this implies $c = c'$. So $C$ corrects $e$ errors.

2.2 Linear codes

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

Note. $C$ is a subspace iff

1. $0 \in C$,
2. if $x, y \in C$, then $x + y \in C$.

(closure under multiplication is trivial since the scalars are 0, 1).

Basic source of linear codes:

Proposition 2.3. If $A$ is a $m \times n$ matrix over $\mathbb{Z}_2$, then

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

is a linear code.

Proof. Obvious.

Example. Code $C_3$ has codewords $abcxyz$ with $x = a + b$, $y = a + c$, $z = b + c$ is

$$\left\{ (x_1, \ldots, x_6) \left| \begin{array}{l} x_4 = x_1 + x_2, \ x_5 = x_1 + x_3, \\ x_6 = x_2 + x_3 \end{array} \right. \right\}$$

and that is

$$\left\{ x \in \mathbb{Z}_2^6 \mid \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} x = 0 \right\}.$$ 

So $C_3$ is linear.

Linear codes have bases, dimension and so on.

Proposition 2.4. If $C$ is a linear code of dimension $m$ then

$$|C| = 2^m.$$

Proof. Let $c_1, \ldots, c_m$ be the basis of $C$. So every codeword in $C$ has a unique expression as a linear combination of the basis

$$\lambda_1 c_1 + \cdots + \lambda_m c_m = 0$$

for $\lambda_i \in \mathbb{Z}_2$. There are $2^m$ such expressions.

Example. Basis of $C_3$ is 100110, 010101, 001011 so $\dim(C) = 3$ and $|C| = 8$. 

**Definition.** For \( x \in \mathbb{Z}_2^n \) the weight of \( x \) is
\[
\text{wt}(x) = \text{number of 1's in } x.
\]

**Example.** \( \text{wt}(101011) = 4. \)

**Lemma 2.5.** For \( x, y, z \in \mathbb{Z}_2^n \), \( d(x, y) = d(x + z, y + z). \)

**Proof.** Observe that \( x + z \) and \( y + z \) are \( x, y \) respectively, changed in the positions where \( z \) has a 1. So \( x + z, y + z \) differ in the same positions as \( x \) and \( y \) do. ■

**Proposition 2.6.** If \( C \) is a linear code
\[
d(C) = \min \{ \text{wt}(c) \mid c \in C, \ c \neq 0 \}.
\]

**Proof.** Let \( c \in C, c \neq 0 \) with \( c \) of the minimum weight \( r \). Now \( 0, c \in C \) and \( d(0, c) = \text{wt}(c) = r \). So
\[
d(C) \leq r.
\]

Next, if \( x, y \in C \) with \( x \neq y \),
\[
d(x, y) = d(x + y, y + y)
= d(x + y, 0)
= \text{wt}(x + y).
\]

Since \( C \) is linear, \( x + y \in C \), so \( \text{wt}(x + y) \geq r \). Hence
\[
d(C) \geq r.
\]

So \( d(C) = r \) by \( \leq \) and \( \geq \). ■

**Example.** \( C_3 \) has minimum weight 3, so \( d(C_3) = 3 \). So by \( \square \) \( C_3 \) corrects 1 error.

Aim is to find codes \( C \) with \( \text{dim}(C) \) large (lots of messages), \( d(C) \) (corrects lots of errors) and small length (save space).

### 2.3 The Check Matrix

**Definition.** If \( A \) is a \( n \times n \) matrix over \( \mathbb{Z}_2 \) and \( C = \{ x \in \mathbb{Z}_2^n \mid Ax = 0 \} \) we call \( A \) a check matrix of the linear code \( C \).

**Example.** The code \( C_3 \) has a check matrix
\[
\begin{pmatrix}
1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 1
\end{pmatrix}.
\]

**Proposition 2.7.** If \( A \) is \( n \times n \) and \( C = \{ x \in \mathbb{Z}_2^n \mid Ax = 0 \} \) then
\[
\text{dim}(C) = n - \text{rank}(A).
\]

**Proof.** This is the rank-nullity theorem applied to the linear transformation \( x \to Ax \) in \( \mathbb{Z}_2^n \to \mathbb{Z}_2^{m} \). The rank-nullity theorem says that
\[
\text{dim}(\text{Ker } T) + \text{dim}(\text{Im } T) = \text{dim}(\mathbb{Z}_2^{m})
\]
that is
\[
\text{dim}(C) + \text{rank}(A) = n.
\] ■
Example. Let
\[ A = \begin{pmatrix}
1 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1
\end{pmatrix}, \]
\[ C = \{ x \in \mathbb{Z}_2^6 \mid Ax = 0 \}. \]
What is \( \dim(C) \)? Reduce \( A \) to echelon form to get
\[ \begin{pmatrix}
1 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}. \]
So \( \rank(A) = 3 \) and \( \dim(C) = 6 - 3 = 3 \).

2.3.1 Check matrix and error correction

Given code with check matrix \( A \), what properties of \( A \) tell us how many errors the code can correct? In case of one error:

**Proposition 2.8.** Let \( C \) be a code with check matrix \( A \). Suppose

1. all columns of \( A \) are different,
2. no column of \( A \) is the zero column.

Then \( C \) corrects (at least) one error.

**Proof.** By 2.2, we need to show that \( d(C) \geq 3 \). By 2.8, this is equivalent to showing that \( \wt(c) \geq 3 \) for all \( c \in C, c \neq 0 \). Assume (for a contradiction) that there exists \( c \in C \) with \( c \neq 0 \) and \( \wt(c) \leq 2 \). If \( \wt(c) = 1 \), then
\[ c = \begin{pmatrix}
0 \\
\vdots \\
1 \\
\vdots \\
0
\end{pmatrix} = e_i \]
(\( e_i \) is the \( i \)th standard basis vector). As \( c \in C, Ac = 0 \), so \( 0 = Ae_i = i \)th column of \( A \), contradicting assumption (2). If \( \wt(c) = 2 \) then
\[ c = e_i + e_j \]
so \( 0 = A(e_i + e_j) = i \)th column + \( j \)th column. This means that columns \( i \) and \( j \) are the same (\( A \) is over \( \mathbb{Z}_2 \)), contradicting the assumption (1).

**Example.** By 2.8 \( C_3 \) corrects 1 error.
What is the maximum dimension of a code \( C \) such that

1. a check matrix of \( C \) has rank 3,
2. \( C \) corrects 1 error?

If \( C \subseteq \mathbb{Z}_2^n \), then \( \dim(C) = n - 3 \), so we need to maximise \( n \). Look for a \( 3 \times n \) check matrix \( A \) with all columns different and non-zero. Take \( A \) to have as columns all the nonzero vectors in \( \mathbb{Z}_2^3 \). So
\[ A = \begin{pmatrix}
1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 1
\end{pmatrix}. \]
Then \( C = \{ x \in \mathbb{Z}_2^7 \mid Ax = 0 \} \) that is

\[
C = \left\{ x \in \mathbb{Z}_2^7 \left| \begin{array}{l}
  x_5 = x_1 + x_2 + x_3, \\
  x_6 = x_1 + x_2 + x_4, \\
  x_7 = x_1 + x_3 + x_4
\end{array} \right. \right\}.
\]

This corrects one error (by 2.8) and has dimension 4, the largest possible.

### 2.4 Hamming codes

**Definition.** Let \( k \geq 2 \). A **Hamming code** \( \text{Ham}(k) \) is a code whose check matrix has as its columns all the nonzero vectors in \( \mathbb{Z}_2^k \).

**Note.**

1. Check matrix of \( \text{Ham}(k) \) is \( k \times (2^k - 1) \) since \( |\mathbb{Z}_2^k| = 2^k \).
2. The code \( \text{Ham}(k) \) corrects one error by 2.8.

**Example.** The code \( \text{Ham}(3) \) is the code from the previous matrix. The check matrix of \( \text{Ham}(4) \) is

\[
\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1
\end{pmatrix}.
\]

### 2.5 Correcting one error

Code \( C \subseteq \mathbb{Z}_2^n \) correcting 1 error: suppose that \( c \in C \) is sent and 1 error is made, so the received word is \( c' = c + e_i \). Observe that if \( A \) is a check matrix of \( C \) then

\[
Ac' = Ac + Ae_i = 0 + Ae_i = i^{th} \text{ column of } A.
\]

So there is a procedure for correcting 1 error:

1. Receive vector \( w \in \mathbb{Z}_2^n \). Find \( Aw \).
2. If \( Aw = 0 \) then \( w \in C \), no correction required. If \( Aw \neq 0 \) then \( Aw \) is a column of \( A \), say the \( i^{th} \)
   column.
3. Corrected codeword is then \( w + e_i \).

### 2.6 Correcting more than one error

**Proposition 2.9.** Let \( d \geq 2 \) and let \( C \) be a linear code with check matrix \( A \). Assume that every set of \( d - 1 \) columns of \( A \) is linearly independent. Then

1. \( d(C) \geq d \),
2. \( d(C) = d \) if there exists a set of \( d \) linearly dependent columns of \( A \).

**Proof.**
(1) Suppose that \( d(C) \leq d - 1 \). Then by (2.6) there exists codeword \( c \in C, c \neq 0 \), with \( \text{wt}(c) \leq d - 1 \). Say \( c = e_{i_1} + \cdots + e_{i_r}, r \leq d - 1 \). Then as \( c \in C \), \( Ac = 0 \), so

\[
0 = Ae_{i_1} + \cdots + Ae_{i_r} = \text{column 1 of } A + \cdots + \text{column } i_r \text{ of } A.
\]

So columns \( i_1, \ldots, i_r \) are linearly dependent, contradicting the hypothesis.

(2) Suppose there exists a set \( c_{i_1}, \ldots, c_{i_d} \) of linearly dependent columns of \( A \). As any \( d - 1 \) of these are linearly independent, the dependence relation must be

\[
c_{i_1} + \cdots + c_{i_d} = 0.
\]

This means that

\[
A(e_{i_1} + \cdots + e_{i_d}) = 0.
\]

So \( e_{i_1} + \cdots + e_{i_d} \) is a codeword in \( C \) of weight \( d \). Hence \( d(C) \leq d \) and so \( d(C) = d \) by (1).

**Example.** Find a linear code of length 9, dimension 2, correcting 2 errors. We need \( d(C) \geq 5 \) by (2.2). So we need to find check matrix \( A \) such that

1. \( A \) is \( 7 \times 9 \) (of rank 7 to get dimension 2),
2. every set of 4 columns is linearly independent.

Try

\[
A = \begin{pmatrix}
  c_1 & c_2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
  \cdot & \cdot & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
  \cdot & \cdot & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
  \cdot & \cdot & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
  \cdot & \cdot & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
  \cdot & \cdot & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
  \cdot & \cdot & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\]

For condition (2), we need

(a) \( \text{wt}(c_1) \geq 4, \text{wt}(c_2) \geq 4 \),

(b) \( \text{wt}(c_1 + c_2) \geq 3 \).

Here (a) ensures that no set of 4 columns \( \{c_1, e_i, e_j, e_k\} \) or \( \{c_2, e_i, e_j, e_k\} \) is linearly dependent and (b) ensures that no set \( \{c_1, c_2, e_i, e_j\} \) is linearly dependent. Take

\[
c_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad c_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}.
\]

Then \( \text{wt}(c_1) = 4 \) and \( \text{wt}(c_1 + c_2) = 6 \). So our check matrix is

\[
A = \begin{pmatrix}
  1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
  1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
  1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
  1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
  0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
  0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
  0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\]
and the code is
\[ C = \{ x \in Z_2^9 \mid Ax = 0 \} = \{ abaaa(a + b)bba \mid a, b \in Z_2 \} \]
of length 9, dimension 2 and corrects 2 errors.

### 2.7 The Hamming Bound

Suppose a code \( C \subseteq Z_2^n \) corrects \( e \) errors. What is the maximum possible number of codewords in \( C \)?

Recall, for \( c \in Z_2^n \), \( e \in \mathbb{N} \)
\[ S_e(c) = \{ x \in Z_2^n \mid d(c, x) \leq e \}. \]

**Lemma 2.10.** For any \( c \in Z_2^n \) and \( e \geq 1 \),
\[ |S_e(c)| = 1 + n + \binom{n}{2} + \cdots + \binom{n}{e}. \]

**Proof.** The set \( S_e(c) \) consists of
- \( c \) – there is 1,
- \( c \) with one bit changed – there are \( n \),
- \( c \) with two bits changed – there are \( \binom{n}{2} \),
  
  \[ \vdots \]
- \( c \) with \( e \) bits changed – there are \( \binom{n}{e} \).

**Theorem 2.11 (The Hamming Bound).** Suppose code \( C \subseteq Z_2^n \) corrects \( e \) errors. Then
\[ |C| \leq \frac{2^n}{1 + n + \binom{n}{2} + \cdots + \binom{n}{e}}. \]

**Proof.** As \( C \) corrects \( e \) errors, all the spheres \( S_e(c) \) for \( c \in C \) are disjoint. By [Lemma 2.10] therefore,
\[ |\bigcup_{c \in C} S_e(c)| = |C| \cdot \left( 1 + n + \binom{n}{2} + \cdots + \binom{n}{e} \right). \]

Since \( \bigcup_{c \in C} S_e(c) \subseteq Z_2^n \), the right hand side is less than or equal to \( |Z_2^n| = 2^n \) and so
\[ |C| \cdot \left( 1 + n + \binom{n}{2} + \cdots + \binom{n}{e} \right) \leq 2^n. \]

**Example.** Let \( C \) be a linear code of length 9, correcting 2 errors. What is the maximum possible dimension of \( C \)? By [Theorem 2.11]
\[ |C| \leq \frac{2^9}{1 + 9 + \binom{9}{2}} = \frac{2^9}{46}. \]

As \( |C| = 2^k \) where \( k \) is the dimension of \( C \) and \( |C| \leq 2^9/46 < 2^4 \), we get \( k < 4 \). We found such \( C \) of dimension 2 before. Is there a linear code of length 9, dimension 3, correcting 2 errors? We are looking for a check matrix \( A \) which is \( 6 \times 9 \) (rank 6), with any 4 columns linearly independent. Try
\[ A = \begin{bmatrix} c_1 & c_2 & c_3 & 1 & 0 & 0 & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & 0 & 1 & 0 & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & 0 & 0 & 1 & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & 0 & 0 & 0 & 1 & 0 & 0 \\ \cdot & \cdot & \cdot & 0 & 0 & 0 & 0 & 1 & 0 \\ \cdot & \cdot & \cdot & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \]

We need
(a) \( \text{wt}(c_i) \geq 4 \),
(b) \( \text{wt}(c_i + c_j) \geq 3 \),
(c) \( \text{wt}(c_1 + c_2 + c_3) \geq 2 \).

See the Sheet 2.

2.8 Codes correcting 1 error

Hamming bound says that if \( C \subseteq \mathbb{Z}_2^n \) corrects 1 error, then

\[
|C| \leq \frac{2^n}{1 + n}.
\]

Can equality arise? Equivalently, can \( \bigcup_{c \in C} S_1(c) = \mathbb{Z}_2^n \)?

**Proposition 2.12.** For \( C \subseteq \mathbb{Z}_2^n \), \( k \in \mathbb{N} \),

\[
|C| = \frac{2^n}{1 + n} \text{ iff } n = 2^k - 1 \text{ and } |C| = 2^{n-k}.
\]

**Proof.**

\( \Rightarrow \) We have, since \( |C| = 2^n/(1 + n) \), \( n + 1 = 2^k \) for some \( k \) and hence \( n = 2^k - 1 \), \( |C| = 2^{n-k} \).

\( \Leftarrow \) Since \( n = 2^{k-1} \), \( |C| = 2^{n-k} \), we have \( |C| = 2^n/(1 + n) \).

**Example.** Ham\((k)\) has length \( n = 2^k - 1 \) and dimension \( 2^k - 1 - k = n-k \). So \( |\text{Ham}(k)| = 2^{n-k} = 2^n/(1+n) \).

2.9 Perfect Codes

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

\[
|C| = \frac{2^n}{1 + n + \cdots + \binom{n}{e}}.
\]

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

**Example.** The code \( \text{Ham}(k) \) is 1-perfect.

**Note.** For an \( e \)-perfect code, \( 1 + n + \cdots + \binom{n}{e} \) must be a power of 2. For \( e = 2 \), this is \( 1 + n + \binom{n}{2} = n^2 + n + 2 = 2^k \) for some \( k \). This is rare, but possible. Perfect codes are rare.

**Example.** Q7 on Sheet 2 – if \( C \subseteq \mathbb{Z}_2^n \) is 3 perfect, then \( n = 7 \) or \( n = 23 \). For \( n = 7 \), \( C = \{0000000, 1111111\} \). For \( n = 23 \), there is the Golay code which is 3-perfect.

Famous general result:

**Theorem 2.13** (Van Lint & Tietraren, 1963). The only \( e \)-perfect codes are

(1) \( e = 1 \), \( \text{Ham}(k) \),
(2) \( n = 2e + 1 \), \( C = \{0^n, 1^n\} \),
(3) \( e = 3 \), \( n = 23 \), \( \dim(C) = 12 \), \( C \) is the Golay code.

**Note.** We have \( 1 + 23 + \binom{23}{2} + \binom{23}{3} = 2048 = 2^{11} \).

We will cover Golay Code later.
2.10 Gilbert-Varshamov bound

The Hamming bound is a non-existence result for codes – it says no code C of length n exists correcting e errors if |C| > \( \frac{2^n}{1 + \frac{e}{n+1}} \). The Gilbert-Varshamov bound is an existence result – it says if an inequality holds (stated later), then there does exist a code C with certain properties (stated later too).

**Example.** Let \( C \subseteq \mathbb{Z}_2^{11} \) be linear code correcting 2 errors. The Hamming bound tells us \( |C| \leq \frac{2^{11}}{1 + \frac{2}{11+1}} \). Since \( 2^{11}/67 < 2^5 \), so \( \text{dim}(C) \leq 4 \).

**Claim.** There exists such a \( C \) of dimension 3.

**Proof.** Need \( C \subseteq \mathbb{Z}_2^{11}, \text{dim}(C) = 3 \), \( d(C) \geq 5 \). So we need to find check matrix \( A \) such that

1. \( A \) is \( 8 \times 11 \) or rank 8 (\( \text{dim}(C) = n - \text{rank} A \))
2. any 4 columns of \( A \) are linearly independent (so by [2.9] \( d(C) \geq 5 \)).

Start with

\[
A = \begin{pmatrix}
I_8 & c_1 & \cdots & c_{11}
\end{pmatrix}
\]

We argue that \( A \) exists with required properties by "counting". The number of vectors in \( \mathbb{Z}_2^8 \) which are the sums of at most 3 of the columns \( c_1, \ldots, c_8 \) is at most

\[
N_8 = 1 + 8 + \binom{8}{2} + \frac{8}{3} = 1 + 8 + 28 + 56 < 2^8.
\]

So there exists a vector \( c_9 \in \mathbb{Z}_2^8 \) which is not the sum of at most 3 of the columns \( c_1, \ldots, c_8 \) and the matrix \( \begin{pmatrix} c_1 & \cdots & c_8 & c_9 \end{pmatrix} \) has any 4 columns linearly independent.

The number of vectors in \( \mathbb{Z}_2^8 \) which are the sums of at most 3 of the columns \( c_1, \ldots, c_9 \) is at most

\[
N_9 = 1 + 9 + \binom{9}{2} + \frac{9}{3} = 1 + 9 + 36 + 84 < 2^8.
\]

So there exists \( c_{10} \in \mathbb{Z}_2^8 \) which is not the sum of at most 3 of \( c_1, \ldots, c_{10} \) and the matrix \( \begin{pmatrix} c_1 & \cdots & c_9 & c_{10} \end{pmatrix} \) has any 4 columns linearly independent.

Similarly

\[
N_{10} = 1 + 10 + \binom{10}{2} + \frac{10}{3} = 1 + 10 + 45 + 120 < 2^8.
\]

So there exists \( c_{11} \in \mathbb{Z}_2^8 \) that is not a sum of 3 or fewer of \( c_1, \ldots, c_{10} \). So we have check matrix \( A = \begin{pmatrix} c_1 & \cdots & c_{11} \end{pmatrix} \).

We have shown that there exists a linear code \( C \subseteq \mathbb{Z}_2^{11} \) correcting 2 errors with dimension 3. What made the construction of the required \( 8 \times 11 \) check matrix work was the fact that \( 1 + 10 + \binom{10}{2} + \frac{10}{3} < 2^8 \).

**Theorem 2.14** (Gilbert-Varshamov bound). Let \( n, k, d \) be positive integers such that

\[
1 + n - 1 + \binom{n-1}{2} + \cdots + \frac{n-1}{d-2} < 2^{n-k}.
\]

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

**Proof.** We need to find a check matrix \( A \) such that \( A \) is \( (n-k) \times n \) (of rank \( n-k \)) and any \( d-1 \) columns of \( A \) are linearly independent. Start with \( A_{n-k} = I_{n-k} \). We will continue by adding columns to this, one by one, until we have \( n \) columns. Say we have \( i, n-k \leq i \leq n-1 \) columns \( c_1, \ldots, c_i \) with any \( d-1 \) of them
linearly independent. The number of vectors in $\mathbb{Z}_2^{n-k}$ which are sums of at most $d-2$ of the columns $c_1, \ldots, c_i$ is at most

$$1 + i + \binom{i}{2} + \cdots + \binom{i}{d-2}.$$ 

Since $i \leq n-1$, this sum is less than $2^{n-k}$. So there exists a vector $c_{i+1} \in \mathbb{Z}_2^{n-k}$ that is not a sum of at most $d-2$ of the columns $c_1, \ldots, c_i$. Then the matrix $A = \left( \begin{array}{cccc} c_1 & \cdots & c_i & c_{i+1} \end{array} \right)$ has any $d-1$ columns linearly independent. This process constructs matrices $A_{n-k}, A_{n-k+1}, \ldots, A_n$. Then $A_n$ is $(n-k) \times n$ and has any $d-1$ columns linearly independent.

Example. Linear codes of length 15 correcting 2 errors. Hamming bound says that, since

$$|C| \leq \frac{2^{15}}{1 + 15 + \binom{15}{2}} = \frac{2^{15}}{121} < 2^9,$$

there does not exists such $C$ with dimension greater than 8. It does not say anything about the existence of such codes with dimensions 8, 7, … The G-V bound, since $1 + 14 + \binom{14}{2} + \binom{14}{3} = 29$, says that there exists such $C$ of dimension 6. However, it does not say anything about the existence of such codes of dimensions 7 or 8.

2.11 The Golay Code

This is a 3-perfect code of length 23, dimension 12. We will construct it and prove various properties about it.

First we construct the extended Golay code, $G_{24} \subseteq \mathbb{Z}_2^{24}$. We start with Ham(3) = $H$ and its check matrix

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

and its "reverse" $K$ with check matrix

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

We can add parity check bits to $H$ and $K$ to get codes $H'$ and $K'$ of length 8. The codewords in $H'$ are

$$00000000, 11111111, 10001110, 01110001, 10110010, 01001101, 11010100, 00101011, 10110100, 01001011, 11001100, 00110011, 00111100, 11000011.$$ 

The codewords in $K'$ are

$$00000000, 11111111, 11100001, 00011101, 10011010, 01001101, 01010101, 10101001, 00101110, 11010001, 10110100, 01001011, 11001100, 00110011, 01111000, 10001111.$$
Proposition 2.15.

(1) \(|H'| = |K'| = 16,
(2) wt(x) = 0, 4 or 8 for all \( x \in H' \cup K' \),
(3) \( H' \cap K' = \{0 \cdots 0, 1 \cdots 1\} \).

Proof. (1) and (2) is clear. For (3), let \( w \in H \cap K \). As \( w \in H \), \( w = abcd(a + b + c)(a + b + d)(a + c + d) \) for some \( a, b, c, d \in \mathbb{Z}_2 \). As \( w \in K \)

\[
c + (a + b + c) + (a + b + d) + (a + c + d) = 0,
\]

\[
b + d + (a + b + d) + (a + c + d) = 0,
\]

\[
a + d + (a + b + c) + (a + c + d) = 0.
\]

Simplifying, we get \( a + c = c + d = a + b = 0 \), that is \( a = b = c = d \) and so \( w = 0000000 \) or \( 1111111 \).

Definition. The extended Golay code \( G_{24} \) consists of all vectors in \( \mathbb{Z}_2^{24} \) of the form \( (a + x, b + x, a + b + x) \) where \( a, b \in H' \) and \( x \in K' \).

Example. Take \( a = b = x = 0^8 \), then \( 0^{24} \in G_{24} \). Take \( a = b = 0^8, x = 1^8 \), then \( 1^{24} \in G_{24} \). Take \( a = 1^8, b = 0^8 \) and \( x = 1^8 \), then \( 0^81^80^8 \in G_{24} \) of weight 8. Take \( a = 10001110, b = 10011001, x = 01001011 \). Then \( 110000011010010011100 \in G_{24} \) of weight 12.

Proposition 2.16. \( G_{24} \) is a linear code.

Proof. We have \( 0^{24} \in G_{24} \) and if \((a_1 + x_1, b_1 + x_1, a_1 + b_1 + x_1), (a_2 + x_2, b_2 + x_2, a_2 + b_2 + x_2) \in G_{24} \) then

\[(a_1 + x_1 + a_2 + x_2, b_1 + x_1 + b_2 + x_2, a_1 + b_1 + x_1 + a_2 + b_2 + x_2) \in G_{24}\]

since \( a_1 + a_2, b_1 + b_2 \in H' \) and \( x_1 + x_2 \in K' \) (\( H' \) and \( K' \) are linear).

Proposition 2.17. \( G_{24} \) has dimension 12.

Proof. Suppose \((a_1 + x_1, b_1 + x_1, a_1 + b_1 + x_1) = (a_2 + x_2, b_2 + x_2, a_2 + b_2 + x_2) \) where \( a_i, b_i \in H' \) and \( x_i \in K' \). Then \( a_1 + x_1 = a_2 + x_2, b_1 + x_1 = b_2 + x_2 \) and \( a_1 + b_1 + x_1 = a_2 + b_2 + x_2 \). Adding all together, we get \( x_1 = x_2 \) and hence \( a_1 = a_2 \) and \( b_1 = b_2 \). So different choices of triples \( a, b, x \) give different codewords in \( G_{24} \). Hence

\( |G_{24}| = (\text{no. choices for } a) \times (\text{no. choices for } b) \times (\text{no. choices for } x) = (2^4)^3 = 2^{12} \).

Note. Here is a natural way to choose a basis of \( G_{24} \). Observe that

\[(a + x, b + x, a + b + x) = (a, 0, a) + (0, b, b) + (x, x, x),\]

a sum of three vectors in \( G_{24} \). So if \( a_i, b_i, i = 1, 2, 3, 4 \), form bases of \( H' \) and \( x_i, i = 1, 2, 3, 4 \), is a basis of \( K' \) then 12 basis vectors are

\[(a_1, 0, a_1), (0, b_1, b_1), (x_1, x_1, x_1) \text{ for } i = 1, 2, 3, 4.\]

The main property of \( G_{24} \) is (proved later):

Theorem 2.18. The minimum distance of \( G_{24} \) is 8, that is \( \min \{\text{wt}(c) \mid c \in G_{24}, c \neq 0\} = 8 \).

First we need to define for \( v, w \in \mathbb{Z}_2^n \) \([v, w]\) – the number of positions where both \( v \) and \( w \) have 1.

Lemma 2.19. For \( v, w \in \mathbb{Z}_2^n \), \( \text{wt}(v + w) = \text{wt}(v) + \text{wt}(w) - 2|v, w| \).

Proof. Let \( r = \text{wt}(v), s = \text{wt}(w), t = |v, w| \). Re-ordering coordinates we have \( v = 1^r 0 \cdots 0, w = 1^s 0 \cdots 0 1^t \cdots 1 \cdot 0 \cdots 0 \) and \( v + w = 0^r 1^{r-t} 1^s-t 0 \cdots 0 \) which has weight \( \text{wt}(v + w) = r - t + s - t = r + s - 2t \).

Lemma 2.20. Let \( v, w \in \mathbb{Z}_2^n \) with \( \text{wt}(v) \) and \( \text{wt}(w) \) both divisible by 4. Then \( \text{wt}(v + w) \) is divisible by 4 if and only if \( |v, w| \) is even.
Proof. Write \( \text{wt}(v) = 4a \) and \( \text{wt}(w) = 4b \). Then by \( 2.19 \) \( \text{wt}(v + w) = 4a + 4b - 2|v, w| \). This is divisible by 4 precisely when \( |v, w| \) is even. 

\[ \blacksquare \]

**Lemma 2.21.** If \( a, b, x \in \mathbb{Z}_2^n \) then \( |a, x| + |b, x| + |a + b, x| \) is even.

Proof. Let \( r = |a, x|, s = |b, x| \). Re-ordering coordinates, write \( x = 1 \ldots 10 \ldots 0, a = 1^r0^s \ldots 0, b = 1^u0^v \ldots u0^v \ldots u0^v \ldots \). So \( a + b = 0^u1^v1^u0^v \ldots 0 \ldots \) and hence

\[
|a, x| + |b, x| + |a + b, x| = r + s + r - u + s - u = 2(r + s - u),
\]

an even number. 

\[ \blacksquare \]

Key step in proof of the Theorem 2.18 is

**Proposition 2.22.** For all \( c \in G_{24} \), \( \text{wt}(c) \) is divisible by 4.

Proof. Let \( c = (a + x, b + x, a + b + x) \in G_{24} \) with \( a, b \in H' \) and \( x \in K' \). Write

\[
v = (a, b, a + b),
\]

\[
w = (x, x, x),
\]

\[
c = (a, b, a + b) + (x, x, x) = v + w.
\]

We apply \( 2.20 \)—we have \( a, b, a + b \in H' \), so they all have weight divisible by 4, hence \( \text{wt}(v) \) is divisible by 4. Also \( x \in K' \) has weight divisible by 4, so \( \text{wt}(w) \) is divisible by 4. Finally \( |v, w| = |a, x| + |b, x| + |a + b, x| \) is even by \( 2.21 \). Hence by \( 2.20 \) \( \text{wt}(c) = \text{wt}(v + w) \) is divisible by 4.

\[ \blacksquare \]

Proof of 2.18: Suppose that \( d(G_{24}) < 8 \). Then there exists \( c \in G_{24} \) with \( c \neq 0 \) and \( \text{wt}(c) < 8 \). By 2.22 we have \( \text{wt}(c) = 4 \). Write \( c = (a + x, b + x, a + b + x) \) where \( a, b \in H' \) and \( x \in K' \). By 2.19 we know that

\[ \text{wt}(a + x) = \text{wt}(a) + \text{wt}(x) - 2|a, x|. \]

As \( a \in H' \) and \( x \in K' \), these have even weights, so \( \text{wt}(a + x) \) is an even number. Similarly \( \text{wt}(b + x) \) and \( \text{wt}(a + b + x) \) are even. Then the sum of these three even numbers is 4 and hence one of them is 0, that is one of the vectors \( a + x, b + x, a + b + x \) is the zero vector. So \( x = a, b \) or \( a + b \). Hence \( x \) is in \( K' \cap H' \) and is therefore \( 8 \) or \( 0^8 \) by 2.12. Now all three of \( a + x, b + x, a + b + x \) belong to \( H' \). Since vectors in \( H' \) have weights \( 0, 4, 8 \) it follows that two of the three vectors are zero. The possibilities are that \( x = a = b \) and so \( c = 0^8 \), \( x = a = a + b \) and so \( c = 0^8x_0^8 \), or \( x = b = a + b \) and so \( c = x_0^8 \); all lead to contradiction since \( x \) is \( 8 \) or \( 1^8 \). Hence \( d(G_{24}) \geq 8 \) and since \( G_{24} \) has codewords of weight 8, \( d(G_{24}) = 8 \).

\[ \blacksquare \]

**Theorem 2.23.** To summarize, we have: \( G_{24} \) is a linear code of length 24, dimension 12 and minimum distance 8.

**Definition.** The Golay Code \( G_{24} \subseteq \mathbb{Z}_2^{23} \) consists of all the codewords in \( G_{24} \) with the last bit removed.

**Proposition 2.24.** \( G_{23} \) is linear of dimension 12 and has minimum distance 7.

**Proof.** Linearity and dimension follow from \( G_{24} \). As \( \text{wt}(c) \geq 8 \) for all \( c \in G_{24}, c \neq 0 \), we know that \( \text{wt}(x) \geq 7 \) for all \( x \in G_{23}, x \neq 0 \). Also \( 0^80^1 \in G_{24} \) (take \( a = b = x = 1^8 \)) and so \( 0^80^17 \in G_{23} \) is of weight 7. Hence \( d(G_{23}) = 7 \).

\[ \blacksquare \]

**Theorem 2.25.** \( G_{23} \) is a 3-perfect code.

**Proof.** As \( d(G_{23}) = 7 = 2 \cdot 3 + 1 \), \( G_{23} \) corrects 3 errors. To show it is 3-perfect, observe that \( |G_{23}| = 2^{12} \) and

\[
\frac{2^{23}}{1 + 23 + \left(23\right) + \left(23\right)} = \frac{2^{23}}{211} = 2^{12}.
\]

\[ \blacksquare \]
2. ERROR-CORRECTING CODES

2.11.1 Some numerology for \(G_{24}\) and \(G_{23}\)

Define

\[ N_i = \text{number of codewords in } G_{24} \text{ of weight } i, \]
\[ M_i = \text{number of codewords in } G_{23} \text{ of weight } i. \]

**Proposition 2.26.** Codewords in \(G_{24}\) have weights 0, 8, 12, 16 or 24 and

\[ N_0 = N_{24} = 1, \quad N_8 = N_{16}. \]

**Proof.** We know that for all \(c \in G_{24}\), \(c \neq 0\), \(wt(c)\) is divisible by 4 and is at least 8. Now \(1 \cdot 24 \in G_{24}\) and the map \(c \mapsto x + 1 \cdot 24\) is a bijection between the codewords of weight \(i\) and codes of weight \(24 - i\). So \(N_i = N_{24-i}\). Since \(N_4 = 0\), it follows that \(N_{20} = 0\). Also \(N_8 = N_{16}\). \(\blacksquare\)

**Proposition 2.27.** Codewords in \(G_{23}\) have weights 0, 7, 8, 11, 12, 15, 16 or 23 and

\[ M_0 = M_{23}, \quad M_7 = M_{16}, \quad M_8 = M_{15}, \quad M_{11} = M_{12}. \]

**Proof.** Again \(1 \cdot 23 \in G_{23}\) and the map \(x \mapsto x + 1 \cdot 23\) gives \(M_i = M_{23-i}\) for all \(i\). \(\blacksquare\)

**Proposition 2.28.** We have \(M_7 = 253\) and \(M_8 = 506\).

**Proof.** As \(G_{23}\) is 3-perfect, every vector in \(Z_2^{23}\) of weight 4 lies in a unique sphere \(S_5(\nu)\), where \(\nu \in G_{23}\) has weight 7. Count the pairs \((\nu, S_5(\nu))\) where \(\nu \in Z_2^{23}\) is of weight 4 and \(c \in G_{23}\) is of weight 7 with \(\nu \in S_5(c)\). The number of pairs is the number of \(\nu\)'s times the number of \(S_5(\nu)\)'s per \(\nu\), that is (by perfection of \(G_{23}\)) \(\binom{23}{4} \cdot 1\). It is also the number of \(S_3(c)\)'s times the number of \(\nu\)'s per \(S_3(c)\), that is \(M_7 \cdot \binom{23}{4}\). Hence

\[ M_7 = \binom{23}{4} = \frac{23 \cdot 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5}{4 \cdot 3 \cdot 2 \cdot 1} = 23 \cdot 11 + 253. \]

To calculate \(M_8\), count pairs \((\nu, S_5(\nu))\) where \(\nu \in Z_2^{23}\) is of weight 5, \(c \in G_{23}\) is of weight 7 or 8 and \(\nu \in S_5(c)\). The number of pairs is the number of \(\nu\)'s times the number of \(S_5(\nu)\)'s per \(\nu\), that is \(\binom{23}{5} \cdot 1\). It is also the number of \(c\)'s of weight 7 times the number of \(\nu\)'s in \(S_3(\nu)\) plus the number of \(c\)'s of weight 8 times the number of \(\nu\)'s in \(S_3(\nu)\), that is \(M_7 \cdot \binom{23}{5} + M_8 \cdot \binom{23}{8}\). So

\[ M_8 = \binom{23}{5} + M_8 \cdot \binom{23}{8} = \frac{23 \cdot 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} - 23 \cdot 11 \cdot \frac{7 \cdot 6}{2 \cdot 1} = 23 \cdot 11 \cdot 7 \cdot 19 - 3. \]

\[ M_8 = \frac{23 \cdot 11 \cdot 7 \cdot 16 \cdot 3 \cdot 2 \cdot 1}{8 \cdot 7 \cdot 6} = 506. \]

**Proposition 2.29.** In \(G_{24}\), \(N_8 = N_{16} = 759\) and \(N_{12} = 2576\).

**Proof.** By the definition of \(G_{23}\), \(N_8 = M_7 + M_8 = 253 + 506 = 759\). Finally \(N_{12} = 2^{12} - N_8 - N_{16} - 2\). \(\blacksquare\)

Using \(G_{24}\), define points to be the 24 coordinate positions 1,2,...,24. For each codeword \(c\) in \(G_{24}\) of weight 8 define block \(B_c\) to be the set of 8 positions where \(c\) has a 1. For example for \(c = 1^80^80^8\), \(B_c = \{1,2,...,8\}\). So we have 759 blocks called octads.
Theorem 2.30 (The Witt design). The 759 octads are the blocks of a 5-design in which any set of 5 points lies in a unique octad.

We will give two proofs of this theorem.

First proof. Let $S$ be a set of 5 points, and let $v_S$ be the corresponding vector in $\mathbb{Z}_{2}^{24}$ of weight 5. Delete the last bit of $v_S$ giving vector $v'_S \in \mathbb{Z}_{2}^{23}$ of weight 4 or 5. As $G_{23}$ is 3-perfect, $v'_S$ lies in a unique sphere $S_3(c)$ for $c \in G_{23}$ and clearly $c$ must have weight 7 or 8. Add parity check bit to $c$ to get $c' \in G_{24}$ of weight 8. Then the positions of the 1’s in $v'_S$ are also the positions of 1’s in $c$. Hence the same is true for $v_S$ and $c'$. In other words, $S$ is in $B_{c'}$. By the uniqueness of $S_3(c)$, this is the unique octad containing $S$.

Second proof. First, we will show that any 5 points lie in at most 1 octad, by showing that any 2 octads intersect in less than 5 points. Let $c_1, c_2 \in G_{24}$ be codewords of weight 8 and let $B_{c_1}$ and $B_{c_2}$ be the corresponding octads. Note that $|B_{c_1} \cap B_{c_2}| = [c_1, c_2]$. We know by 2.19 that $\text{wt}(c_1 + c_2) = \text{wt}(c_1) + \text{wt}(c_2) - 2[c_1, c_2]$. Also $\text{wt}(c_1) = \text{wt}(c_2) = 8$ and by 2.18 $\text{wt}(c_1 + c_2) \geq 8$ (as $c_1 + c_2 \in G_{24}$). Hence

$$2[c_1 + c_2] = \text{wt}(c_1) + \text{wt}(c_2) - \text{wt}(c_1 + c_2)$$

$$\leq 8 + 8 - 8 = 8.$$

So $|B_{c_1} \cap B_{c_2}| = |c_1, c_2| \leq 4$.

Next, we show that every set of 5 points lies in exactly one octad. By the previous, the number of 5-sets lying in some octad is the number of octads times the number of 5-sets per octad, that is

$$759 \times \binom{8}{5} = 759 \times \frac{8!}{5!3!} = \frac{23 \times 22 \times 21 \times 20}{5 \times 4 \times 3 \times 2 \times 1} = \frac{24!}{5!}$$

that is the total number of 5 sets. Hence every 5-set lies in some octad, hence in exactly 1 octad by the first part.
Chapter 3

Strongly regular graphs

Recall a graph \( \Gamma = (V, E) \) has a set of vertices \( V \) and a set of edges \( E \) where \( E \) consists of pairs of vertices. We say vertices \( i \) and \( j \) are joined (by an edge) if \( \{i, j\} \in E \). Graph \( \Gamma \) is regular of valency \( k \) if every vertex is joined to exactly \( k \) vertices.

A path in \( \Gamma \) is a sequence \( v_0, v_1, \ldots, v_r \) of vertices such that \( v_i, v_{i+1} \) are joined for all \( i \). Its length is defined to be \( r \), the number of edges in the path.

Say \( \Gamma \) is connected graph if for any \( v, w \in V \) there exists a path from \( v \) to \( w \) (that is with first vertex \( v \) and the last \( w \)). For \( v, w \in V \), define the distance \( d(v, w) \) to be the smallest length of a path from \( v \) to \( w \) and \( d(v, w) = \infty \) if no such path exists.

**Example.**

\[
\begin{array}{c}
\text{a} \\
\text{f} \\
\text{e} \\
\text{b} \\
\text{c} \\
\text{d}
\end{array}
\]

We have \( d(a, b) = 1 \), \( d(a, c) = 2 \), \( d(f, c) = 3 \).

**Definition.** Let \( \Gamma \) be a connected graph. The diameter of \( \Gamma \) is

\[
\text{diam}(\Gamma) = \max\{d(v, w) \mid v, w \in V\}.
\]

**Example.** The previous graph has diameter 3.

**Note.** If diameter of a graph \( \Gamma \) is 1, then \( \Gamma \) is a complete graph \( K_n \) – the graph with \( n \) vertices in which any two vertices are joined.

**Example.** Here is the \( K_4 \)

\[
\begin{array}{c}
\text{a} \\
\text{b} \\
\text{c} \\
\text{d}
\end{array}
\]

**Proposition 3.1.** Let \( \Gamma = (V, E) \) be a connected regular graph of valency \( k \) and diameter \( d \). Then

\[
|V| \leq 1 + k + k(k - 1) + k(k - 1)^2 + \cdots + k(k - 1)^{d-1} = 1 + k \sum_{i=0}^{d-1} (k-1)^i.
\]
Proof. Start with a vertex \( v \). Define 
\[ S_i = \{ x \in V \mid d(v, x) = i \}. \]

As \( \text{diam}(\Gamma) = d \), we know that 
\[ V = S_0 \cup S_1 \cup \cdots \cup S_d. \]

Now 
\[ |S_0| = |\{ v \}| = 1, \]
\[ |S_1| = |\{ x \in V \mid d(v, x) = 1 \}| = k, \]
\[ |S_2| = |\{ x \in V \mid d(v, x) = 2 \}| \]

For \( i \) total number of new neighbours of vertices in \( S_1 \)
\[ \leq |S_1| \cdot (k - 1) = k(k - 1), \]
\[ \vdots \]
\[ |S_i| \leq |S_{i-1}| \cdot (k - 1) = k(k - 1)^{i-1}. \]

So \( |V| \leq \sum_{i=0}^{d-1} |S_i| \leq 1 + \sum_{i=1}^{d-1} k(k - 1)^{i-1}. \)

\[ N(k, d) \]

Write
\[ N(k, d) = 1 + \sum_{i=1}^{d-1} k(k - 1)^{i-1}. \]

Moore graph

Definition. A Moore graph is a connected regular graph of valency \( k \), diameter \( d \) with \( |V| = N(k, d) \).

Example. For \( k = 2 \), we have \( N(2, d) = 1 + 2d \). Here \( \Gamma \) is \( (2d + 1) \)-gon with diameter \( d \), so is a Moore graph.

For \( k = 3 \) and \( d = 2 \), we have \( N(3, 2) = 1 + 3 + 3 \cdot 2 = 10 \). There exists such a graph – the Petersen graph.

Check that it does have valency 3 and diameter 2.

Figure 3.1: The Petersen graph is a Moore graph.

For \( k = 4, d = 2 \), we have \( N(4, 2) = 1 + 4 + 4 \cdot 3 = 17 \).

Claim. There exists no such Moore graph.
The Petersen graph is strongly regular with parameters $(10, 3, 0, 1)$.

**Example.** They must be joined (since contradiction.

Now assume $a$, $b$, $c$ be further neighbours of 0 and $x$, $y$, $z$ the further neighbours of $\infty$. Note that $a$, $b$, $c$ are not joined with $x$, $y$, $z$ as there would be a quadrilateral. As the diameter is 2, there exists a common neighbour of $a$ and $x$, say $(a, x)$. Get 9 further vertices $(a, x), \ldots, (c, z)$. Observe that $(a, x)$ is not joined with $(a, y)$, otherwise there would be a triangle. Also $(a, x)$ is not joined to $(b, x)$. So $(a, x)$ has two neighbours in

$$\{(b, y), (b, z), (c, y), (c, z)\}.$$  

Say (without loss of generality) that $(a, x)$ is joined to $(b, y)$. Then $(a, x)$ is not joined to $(c, y)$ or $(b, z)$. Otherwise there would be a quadrilateral $(a, x), (b, y), (c, y), y$. So $(a, x)$ is joined to $(c, z)$. Finally, $(b, y)$ is not joined to $(c, y), (b, z)$ or $(c, x)$. Hence $(b, y)$ must be joined to $(c, z)$. But now we have a triangle; a contradiction.

For which $k$ does there exist a Moore graph of valency $k$, diameter 2 (it will have $N(k, 2) = 1 + k + k(k - 1) = k^2 - 1$ vertices)? The only possible values of $k$ are 2, 3, 7 and 57; we will prove this later. The proof will be based on theory of strongly regular graphs.

**Definition.** A graph $\Gamma$ is strongly regular with parameters $(v, k, a, b)$ if

1. $\Gamma$ has $v$ vertices and is regular of valency $k$,
2. every pair of joint vertices has the same number $a$ of common neighbours,
3. every pair of non-joined vertices has the same number $b$ of common neighbours.

**Example.** The Petersen graph is strongly regular with parameters $(10, 3, 0, 1)$.

**Proposition 3.2.** Let $\Gamma$ be strongly regular with parameters $(v, k, a, b)$. Then one of the following holds:

1. $b > 0$ and $\text{diam}(\Gamma) = 2$,
2. $b = 0$ and $\Gamma$ is a disjoint union of complete graphs $K_{k+1}$ (parameters $(v, k, k - 1, 0)$).

**Proof.** If $b > 0$ then there is a path of length 2 between any two non-joined vertices, so $\text{diam}(\Gamma) = 2$. Now assume $b = 0$. Let $w$ be a vertex with neighbours $x_1, \ldots, x_k$. As $x_i, x_j$ have common neighbour $w$, they must be joined (since $b = 0$). So $w$, $x_1, \ldots, x_k$ form a complete graph. Now take any further vertex in $\Gamma$ and repeat.

**Example.** Moore graphs of $\text{diam}(2)$ are strongly regular – there are no triangles and quadrilaterals. The parameters are $(k^2 + 1, k, 0, 1)$.

The Triangular graphs $T(n)$, $n \geq 4$. Vertices are pairs $i j = \{i, j\} \subset \{1, 2, \ldots, n\}$, so $v = {n \choose 2}$. Join vertices $i j, k l$ iff $i j \cap k l = 1$. By Sheet 1, $T(n)$ is strongly regular with parameters $\left( \begin{array}{c} n \\ 2 \end{array} \right), 2(n - 2), n - 2, 4$.

The Lattice graphs $L(n)$. Vertices are $(a, b)$ with $a, b \in \{1, \ldots, n\}$, so $v = n^2$. Join $(a, b)$ and $(c, d)$ if and only if $a = c$ or $b = d$. Parameters are $(n^2, 2(n - 1), n - 2, 2)$.

The Paley graphs $P(p)$. Recall that if $p$ is prime, $\mathbb{Z}_p$ is a field. Assume $p \equiv 1 \pmod{4}$. Define $Q = \mathbb{Z}_p.$
\[ \left\{ x^2 \mid x \in \mathbb{Z}_p^* \right\} \] (where \( \mathbb{Z}_p^* = \mathbb{Z}_p - \{0\} \)). For example for \( p = 5 \), \( Q = \{1, 4\} \). We know \( Q \) is a subgroup of \((\mathbb{Z}_p^*, \times)\) of size \((p - 1)/2\). Also \(-1 \in Q \) and \( x \in Q \) iff \( x = y \in Q \). Then this graph is strongly regular. The parameters are \( v = p \) and \( k = (p - 1)/2 \). For \( a, b \) and proofs, see solution to Sheet 4. These are called Paley graphs \( P(p) \). Can be generalized with the same definition, replacing \( \mathbb{Z}_p \) with any finite field \( \mathbb{F}_q \) of \( q \) elements, where \( q \equiv 1 \mod 4 \).

### 3.1 Theory of strongly regular graphs

**Proposition 3.3** (The Balloon Equation). If \( \Gamma \) is a strongly regular graph with parameters \((v, k, a, b)\) then

\[
k(k - a - 1) = b(v - k - 1).
\]

**Proof.** Pick a vertex \( x \) and draw picture: Let \( A \) be the neighbours of \( x \), \( B \) the non-neighbours of \( x \). Each vertex in \( A \) is joined to \( k - a - 1 \) vertices in \( B \) and each vertex in \( B \) is joined to \( b \) vertices in \( A \). The total number of edges between \( A \) and \( B \) is \( k(k - a - 1) \) and also \((v - k - 1)b\).

\[
\begin{align*}
x & \quad A \quad k - a - 1 \quad B \\
k & \quad b & \quad v - k - 1
\end{align*}
\]

If \( \Gamma = (V, E) \) is a graph, then the **complement** of \( \Gamma \), written \( \Gamma^c \), is the graph with vertex set \( V \) and edge set \( E^c \) where \( \{x, y\} \in E^c \) iff \( \{x, y\} \notin E \).

**Example.**

\[
\begin{array}{c}
\Gamma = \begin{array}{c}
\bullet \\
\bullet \\
\bullet \\
\bullet \\
\bullet
\end{array} \\
\Gamma^c = \begin{array}{c}
\bullet \\
\bullet \\
\bullet \\
\bullet \\
\bullet
\end{array}
\end{array}
\]

**Proposition 3.4.** If \( \Gamma \) is a strongly regular graph with parameters \((v, k, a, b)\), then \( \Gamma^c \) is also strongly regular of valency \( v - k - 1 \).

**Proof.** Sheet 4, where you will also find the parameters of \( \Gamma^c \).

### 3.2 Adjacency matrix

**adjacency matrix**

Let \( \Gamma \) be a graph with vertex set \( e_1, \ldots, e_v \). The **adjacency matrix** of \( \Gamma \) is \( v \times v \) matrix \( A = (a_{ij}) \) where

\[
a_{ij} = \begin{cases} 
1 & \text{if } e_i \text{ joined to } e_j, \\
0 & \text{if not.}
\end{cases}
\]

**Example.** The adjacency matrix of a pentagon is

\[
A = \begin{pmatrix}
0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 0
\end{pmatrix}.
\]
Note. The adjacency matrix $A$ is symmetric ($a_{ij} = a_{ji}$) with 0's on the diagonal.

For strongly regular graphs, $A$ has many nice properties.

**Proposition 3.5.** Let $\Gamma$ be a strongly regular graph with parameters $(v, k, a, b)$ and adjacency matrix $A$. Let $J$ be the $v \times v$ matrix with all entries 1 (that is $v_{ij} = 1$ for all $i, j$). Then

1. $AJ = kJ$,
2. $A^2 = (a - b)A + (k - b)I + bJ$.

**Proof.**

1. As $\Gamma$ is regular of valency $k$, each row of $A$ has $k$ 1's so

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

so $AJ = kJ$.

2. As $A$ is symmetric, $A = A^T$, so $A^2 = AA^T$. Hence

$$ij\text{-entry of } A^2 = ij\text{-entry of } AA^T$$

$$= (\text{row } i \text{ of } A). (\text{column } j \text{ of } A^T)$$

$$= (\text{row } i \text{ of } A). (\text{row } j \text{ of } A)$$

$$= \text{number of common neighbours of } e_i \text{ and } e_j$$

$$= \begin{cases} k & \text{if } i = j, \\ a & \text{if } e_i \text{ joined to } e_j \text{ (}i \neq j\text{)}, \\ b & \text{if } e_i \text{ not joined to } e_j \text{ (}i \neq j\text{)}. \end{cases}$$

So $A^2$ has $k$ on diagonal, $a$ where $A$ has 1 and $b$ where $A$ has 0 (off-diagonal). Therefore

$$A^2 = kI + aA + b(J - I)$$

$$= (a - b)A + (k - b)I + bJ. \quad \blacksquare$$

### 3.2.1 Eigenvalues of $A$

As $A$ is real and symmetric, the Principal Axis theorem, the eigenvalues of $A$ are real and there exists invertible $P$ such that

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

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

**Example.** Let $D$ be a diagonal matrix with 000112 on the diagonal. Then $D$ has eigenvalues 0, 1, 2 with multiplicities 3, 2, 1.

Main theorem of this chapter:
Theorem 3.6. Let \( \Gamma \) be a strongly regular graph with parameters \((v, k, a, b)\) and assume that \( v > 2k \) and \( b > 0 \). Then

1. \( A \) has exactly 3 distinct eigenvalues. These are \( k, r_1 \) and \( r_2 \) where \( r_1 \) and \( r_2 \) are roots of the quadratic equation
   \[ x^2 - (a - b)x - (k - b) = 0. \]

2. The eigenvalue \( k \) has multiplicity 1 and the eigenvalues \( r_1, r_2 \) have multiplicities \( m_1, m_2 \) where
   \[ m_1 + m_2 = v - 1, \]
   \[ m_1 r_1 + m_2 r_2 = -k. \]

3. Either \( r_1, r_2 \in \mathbb{Z} \), or the parameters \((v, k, a, b)\) are of the form \((4b + 1, 2b, b - 1, b)\).

Note. The assumption that \( v > 2k \) and \( b > 0 \) is essential. But if \( b = 0 \), we know \( \Gamma \) by 3.2. If \( v \leq 2k \), then \( \Gamma^c \) is strongly regular of valency \( k' = v - k - 1 \) and \( v > 2k' \), so can apply Theorem 3.6 to \( \Gamma^c \) (unless \( \Gamma^c \) has its \( b = 0 \)).

Applications of Theorem 3.6

Moore graphs of diameter 2

Recall that a Moore graph of diameter 2 is regular of valency \( k \), diameter 2 and has the maximal possible number \( k^2 + 1 \) vertices. It has no triangles or quadrilaterals so is strongly regular with parameters \((k^2 + 1, k, 0, 1)\).

Theorem 3.7. If a Moore graph of valency \( k \), diameter 2 exists, then \( k = 2, 3, 7 \) or 57.

Proof. Suppose \( \Gamma \) is such a Moore graph, so has parameters \((k^2 + 1, k, 0, 1)\). Notice that \( b > 0 \) and \( v = k^2 + 1 > 2k \), so Theorem 3.6 applies.

1. By [3.6(1)], the eigenvalues of the adjacency matrix \( A \) of \( \Gamma \) are \( k \) and the roots \( r_1, r_2 \) of \( x^2 + x - (k - 1) = 0 \). These are \( \frac{1}{2} \left( -1 \pm \sqrt{4k - 3} \right) \).

2. By [3.6(2)], the multiplicities \( m_1, m_2 \) satisfy
   \[ m_1 + m_2 = k^2, \]
   \[ r_1 m_1 + r_2 m_2 = -k. \]

The equation (2) is
   \[ \frac{m_1}{2} \left( -1 + \sqrt{4k - 3} \right) + \frac{m_2}{2} \left( -1 - \sqrt{4k - 3} \right) = -k \]
   \[ -(m_1 + m_2) + \sqrt{4k - 3}(m_1 - m_2) = -2k. \]

From equation (1), \( m_1 + m_2 = k^2 \), so
   \[ \sqrt{4k - 3}(m_1 - m_2) = k^2 - 2k. \]

(3) By [3.6(3)], either \( r_1, r_2 \in \mathbb{Z} \) or \((v, k, a, b) = (4b + 1, 2b, b - 1, b)\). As \( b = 1 \), latter only happens if the parameters are \((5, 2, 0, 1)\), in which case \( \Gamma \) is the pentagon. So suppose now that \( k > 2 \) (so \( v > 5 \)).
Then \( r_1, r_2 \in \mathbb{Z} \). Hence \( n = \sqrt{4k^2 - 3} \in \mathbb{Z} \). By (\( \leq \)),

\[
m_1 - m_2 = \frac{k^2 - 2k}{4k - 3} = \frac{k(k - 2)}{4k - 3} = \frac{\left(\frac{n^2 + 3}{4}\right)\left(\frac{n^2 - 5}{4}\right)}{16n}.
\]

This is \( m_1 - m_2 \), so is an integer. However, \( \text{hcf}(n, n^2 + 3) \) divides 3 and similarly \( \text{hcf}(n, n^2 - 5) \) divides 5. Hence \( n \) divides 15, so can be 1, 3, 5 or 15. As \( k = \frac{n^2 + 3}{4} \), it follows that \( k = 1, 3, 7, 57 \).

\[\blacksquare\]

**Friendship Theorem**

**Theorem 3.8** (Friendship Theorem). In a community where any two people have exactly one common acquaintance, there is a person who knows everybody.

**Proof.** Define a graph \( \Gamma \) with vertices the people and join two people if they know each other. The assumption states that any two vertices in \( \Gamma \) have exactly one common neighbour. Suppose (for a contradiction), that there is no vertex which is joined to all the other vertices.

First, we show that under this assumption \( \Gamma \) is regular: Let \( P \) be a vertex. By assumption, there exists vertex \( Q \) not joined to \( P \). Let \( v(P), v(Q) \) be the number of neighbours of \( P \) and \( Q \). Then \( v(P) = v(Q) \): Let \( R \) be the common neighbour of \( P \) and \( Q \). Let \( S \) be the common neighbour of \( P \) and \( R \) and \( T \) be the common neighbour of \( Q \) and \( R \). Note that \( S \neq T \). Let \( u_1, \ldots, u_m \) be the remaining neighbours of \( P \) and \( v_1, \ldots, v_n \) the remaining neighbours of \( Q \). These are all distinct as \( R \) is the only common neighbour of \( P \) and \( Q \). Now \( u_1 \) and \( Q \) have one common neighbour. It is not \( P \) or \( R \), so it is one of the \( v_i \)'s, say \( v_1 \). Similarly, the common neighbour of \( u_2 \) and \( Q \) is one of the \( v_i \)'s, say \( v_2 \). Similarly, common neighbour of \( u_i \) and \( Q \) is \( v_i \) for \( i = 1, \ldots, m \). Hence \( n \geq m \). Likewise, by symmetry, \( m \geq n \) and hence \( n = m \), that is \( v(P) = v(Q) \).

Take non-joined vertices \( P \) and \( Q \). Let \( R \) be the common neighbour of \( P \) and \( Q \). For any further vertex \( S \), either \( S \) is not joined to \( P \) or \( S \) is not joined to \( Q \). So \( v(S) = v(P) \) or \( v(Q) \). Therefore \( v(S) = v(P) = v(Q) \). Finally, there exists a vertex \( S \) not joined to \( R \) (we supposed there is no vertex joined to all vertices). We get \( v(R) = v(S) \) and hence \( \Gamma \) is regular.

Now we get to a contradiction: By the first step, \( \Gamma \) is strongly regular with parameters \((v, k, 1, 1)\). The balloon equation \(3.3\) is \( k(k - 2) = v - k - 1 \). So

\[
v = k^2 - k + 1.
\]
Notice that \( k^2 - k + 1 > 2k \) iff \( k^2 - 3k + 1 > 0 \) iff \( k \geq 3 \), which is true (clearly \( k \neq 2 \) for this graph). So \( v > 2k \), 
\( b = 1 \) and Theorem 3.6 applies. By 3.6(1), the eigenvalues of adjacency matrix of \( \Gamma \) are \( k, r_1, r_2 \) where \( r_1, r_2 \) are roots of \( x^2 - (k - 1) = 0 \). So \( r_1, r_2 = \pm \sqrt{k - 1} \). By 3.6(2), multiplicities \( m_1, m_2 \) satisfy
\[
m_1 + m_2 = v - 1,
\]
\[
r_1 m_1 + r_2 m_2 = -k.
\]
So
\[
\sqrt{k - 1}(m_1 - m_2) = -k.
\]
Squaring, we get
\[
(k - 1)(m_1 - m_2)^2 = k^2
\]
and therefore \( k - 1 \) divides \( k^2 \). But \( \text{hcf}(k - 1, k) = 1 \) and also \( \text{hcf}(k - 1, k^2) = 1 \). It follows that \( k - 1 = 1 \), so \( k = 2 \), a contradiction. Hence there exists a vertex joined to all others. ■

**Proof of Theorem 3.6**

Need a little matrix theory.

**Definition.** If \( A = (a_{ij}) \) is a \( v \times v \) matrix, the **trace** of \( A \) is the sum of its diagonal elements
\[
\text{tr}(A) = \sum_{i=1}^{v} a_{ii}.
\]

**Lemma 3.9.** If \( A \) has eigenvalues \( \lambda_1, \ldots, \lambda_v \) (including multiple eigenvalues) then
\[
\text{tr}(A) = \sum_{i=1}^{v} \lambda_i.
\]

**Proof.** Let \( \lambda_1, \ldots, \lambda_v \) be the roots of the characteristic polynomial of \( A \)
\[
0 = |\lambda I - A| = \begin{vmatrix}
\lambda - a_{11} & -a_{12} & \cdots & -a_{1v} \\
-a_{21} & \lambda - a_{22} & \cdots & -a_{2v} \\
\vdots & \ddots & \ddots & \ddots \\
-a_{v1} & \cdots & \cdots & \lambda - a_{vv}
\end{vmatrix}
= \lambda^v + \lambda^{v-1}(-a_{11} - a_{22} - \cdots - a_{vv}) + \cdots
\]
This is \( (\lambda - \lambda_1) \cdots (\lambda - \lambda_v) \), which has \( \lambda^{v-1} \) coefficient \( -(A_1 + \cdots + \lambda_v) \). Therefore
\[
\sum_{i=1}^{v} \lambda_i = \sum_{i=1}^{v} a_{ii} = \text{tr}(A).
\]

**Proof of Theorem 3.6.** Let \( \Gamma \) be strongly regular with parameters \((v, k, a, b)\) with \( v > 2k \) and \( b > 0 \). By 3.5
\[
AJ = KJ,
\]
\[
A^2 = (a - b)A + (k - b)I + bf.
\]

*Step 1* - \( k \) is an eigenvalue of \( A \): If \( j = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \), \( Aj = kj \).

*Step 2* - \( A \) has at most 3 (distinct; shown later) eigenvalues \( k, r_1, r_2 \), where \( r_1, r_2 \) are roots of
\[
x^2 - (a - b)x - (k - b) = 0
\]
and eigenvectors of \( A \) not in \( \text{span}(j) \) have eigenvalues \( r_1 \) or \( r_2 \): Let \( w \) be an eigenvector of \( A \) not in \( \text{span}(j) \), with \( Aw = \lambda w \). Then,
\[
A^2 w = \lambda^2 w
\]
and so by
\[ \lambda^2 w = A^2 w = (a-b)\lambda w + (k-b)w + bJw. \]

Now \( Jw = cj \) where \( c \) is the sum of all entries in \( w \). So
\[ \{\lambda^2 - (a-b)\lambda - (k-b)\}w = bcj. \]

Since \( w \notin \text{span}(j) \), this implies that
\[ \lambda^2 - (a-b)\lambda - (k-b) = 0. \]

**Step 3** – the eigenvalue \( k \) has multiplicity 1 and \( k \neq r_1 \) or \( r_2 \): Suppose \( k = r_1 \) or \( r_2 \). Then \( k \) is a root of the above quadratic so
\[ k^2 - (a-b)k - (k-b) = 0. \]

Combine with the balloon equation 3.3 to get
\[ k(k - a - 1) = b(v - k - 1) \]
\[ k^2 - (a-b)k - (k-b) = bv. \]

Hence \( bv = 0 \), a contradiction (we assumed \( b > 0 \)). Therefore \( k \neq r_1 \) or \( r_2 \). By Step 2, it follows that the \( k \)-eigenspace is just \( \text{span}(j) \), 1-dimensional, so the multiplicity of \( k \) is 1.

**Step 4** – part (2) of 3.6 holds, that is multiplicities \( m_1, m_2 \) of the eigenvalues \( r_1, r_2 \) satisfy
\[ m_1 + m_2 = v - 1, \]
\[ r_1m_1 + r_2m_2 = -k. \]

Recall that as \( A \) is symmetric, there exists \( P \) such that \( P^{-1}AP \) is a diagonal \( v \times v \) matrix with \( m_1 \) entries being \( r_1 \), \( m_2 \) entries being \( r_2 \) and one being \( k \). So
\[ m_1 + m_2 = v - 1. \]

Also by 3.9 \( \text{tr}(A) \) equals to the sum of the eigenvalues of \( A \), so
\[ \text{tr}(A) = k + r_1m_1 + r_2m_2. \]

But since \( A \) is the adjacency matrix, it has \( 0 \)'s on the diagonal, so \( \text{tr}(A) = 0 \). Therefore
\[ r_1m_1 + r_2m_2 = -k. \]

**Step 5** – the roots of the quadratic \( r_1, r_2 \) are integers, unless
\[ (v, k, a, b) = (2b+1, 2b, b-1, b) : \]

We know that
\[ r_1, r_2 = \frac{1}{2} \left( a-b \pm \sqrt{(a-b)^2 + 4(k-b)} \right) \]
\[ = \frac{1}{2} \left( a-b \pm \sqrt{D} \right) \]

where \( D = (a-b)^2 + 4(k-b) \). Note that \( k > b \) so \( D > 0 \) and \( r_1 \neq r_2 \). By Step 4,
\[ m_1(a-b + \sqrt{D}) + m_2(a-b - \sqrt{D}) = -2k \]
\[ (m_1 + m_2)(a-b) + (m_1 - m_2)\sqrt{D} = -2k. \]
Suppose $m_1 - m_2 \neq 0$. Then $\sqrt{D}$ is clearly rational, hence an integer. This means either $r_1, r_2 \in \mathbb{Z}$ or $r_1 = \frac{2x+1}{2}$ and $r_2 = \frac{2y+1}{2}$ where $x, y \in \mathbb{Z}$. Latter case is impossible as $r_1 r_2 = -(k - b) \in \mathbb{Z}$. Hence if $m_1 \neq m_2$, then $r_1, r_2 \in \mathbb{Z}$. Now suppose $m_1 = m_2$. By \((s)\),
\[(m_1 + m_2)(a - b) = -2k.
\]
As $m_1 + m_2 = v - 1$,
\[(v - 1)(b - a) = 2k.
\]
As $v - 1 \geq 2k$, this implies that $v - 1 = 2k$ and $b - a = 1$. Also by the balloon equation \(3.3\)
\[k(k - a - 1) = b(v - k - 1) = bk
\]
so $b = k - a - 1$ so $k = a + b + 1 = 2b$. Hence the parameters are $(4b + 1, 2b, b - 1, b)$.

**Step 6:** $m_1, m_2 > 0$, that is $r_1, r_2$ are eigenvalues of $A$: Suppose $m_2 > 0$. Then $m_1 = v - 1$ and $r_1 m_1 = -k$ by Step 4 and $r_1 \in \mathbb{Z}$ by Step 5. So
\[r_1(v - 1) = -k.
\]
This means $v - 1$ divides $k$, a contradiction since $v > 2k$. This completes the proof. 

### 3.2.2 Strongly regular graphs with small $v$

What are the possible parameters of strongly regular graphs with $v = 15$? Note that $T(6)$ has parameters $(15, 8, 4, 4)$ and $T(6)^C$ has parameters $(15, 6, 1, 3)$. Assume that the valency $k \leq 7$ (so $v > 2k$). If $b = 0$, $\Gamma$ is union of $5 K_5$’s ($k = 2$) or of $3 K_5$’s ($k = 4$).

Suppose $\Gamma$ is strongly regular with parameters $(15, k, a, b)$ and $b > 0$. Assume $k \leq 7$. For $k = 3$, get (from the balloon equation \(3.3\))
\[3(2 - a) = 11b
\]
so $b = 0$, a contradiction. For $k = 4$, get
\[4(3 - a) = 10b
\]
so $b = 0$, a contradiction again. For $k = 5$, we get
\[5(4 - a) = 9b
\]
so $b = 0$, a contradiction.

For $k = 6$, get
\[6(5 - a) = 8b
\]
\[3(5 - a) = 4b
\]
So $b = 3$, $a = 1$.

In case $k = 7$ get
\[7(6 - a) = 7b
\]
\[6 - a = b
\]
We use the Theorem \(3.6\) the eigenvalues $r_1, r_2$ are roots of
\[x^2 - (a - b)x - (7 - b) = 0.
\]
So
\[r_1, r_2 = \frac{1}{2} \left( a - b \pm \sqrt{(a - b)^2 + 4(7 - b)} \right)
\]
As $a + b = 6$ we get
\[r_1, r_2 = \frac{1}{2} \left( 2a - 6 \pm \sqrt{(2a - 6)^2 + 4(a + 1)} \right).
\]
These are integers by 3.6(3), as \( a \neq b - 1 \). Therefore \( (2a - b)^2 + 4(a + 1) = a^2 - 5a + 10 \) is a square. As \( a + b = 6 \), we know that \( 0 \leq a \leq 5 \). Trying all these, we get \( a^2 - 5a + 10 \) to be a square when \( a = 2 \) or \( 3 \). In case \( a = 2 \), \( r_1, r_2 = 1, -3 \). By 3.6(2), multiplicities \( m_1, m_2 \in \mathbb{Z} \) satisfy

\[
\begin{align*}
m_1 + m_2 &= 14, \\
m_1 - 3m_2 &= -7.
\end{align*}
\]

Finally, \( 4m_2 = 21 \), a contradiction. In case \( a = 3 \), \( r_1, r_2 = \pm 2 \) and so

\[
\begin{align*}
m_1 + m_2 &= 14, \\
2m_1 - 2m_2 &= -7,
\end{align*}
\]

a contradiction again.

For \( k > 7 \), replace \( \Gamma \) by \( \Gamma^c \) to get strongly regular graph with \( k \leq 7 \) and argue as above.

The conclusion is that any strongly regular graph with 15 vertices either is \( K^3_5 \) or \( K^5_3 \) or complement of one of these or has parameters (15, 6, 1, 3) or (15, 8, 4, 4).

**Note.** In fact the only graph with parameters (15, 6, 1, 3) is \( T(6) \), but that is hard to show.
Chapter 4

Designs

Definition. A $t$-design is a collection $\mathcal{B}$ of subsets (blocks) of a set $X$, all of size $k$, such that any $t$ elements of $X$ lie in the same number $r_t$ of blocks. The parameters are $(v, k, r_t)$ where $v = |X|$. A design is a 1-design.

Example. The octads in $G_{24}$ form a 5-design with parameters $(24, 8, 1)$. The codewords of weight 4 in the extended Hamming code $H'$ form a 3-design with parameters $(8, 4, 1)$ (Sheet 3). The $X = \mathbb{Z}_2^k - \{0\}$ with blocks $\{u, v, u + v\}$ form a 2-design with parameters $(2^k - 1, 3, 1)$ (Sheet 1).

Proposition 4.1. If $\mathcal{B}$ is a $t$-design with parameters $(v, k, r_t)$ then $\mathcal{B}$ is also a $(t-1)$-design with parameters $(v, k, r_{t-1})$ with

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

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

$$(\text{number of } x\text{'s}) \times (\text{number of } B\text{'s}) = (v - (t - 1)) \times r_t$$

and also

$$(\text{number of } B\text{'s}) \times (\text{number of } x\text{'s per } B) = r(S) \times (k - (t - 1)).$$

Hence

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

Note. Similarly, a $t$-design is a $(t-2)$-design with

$$r_{t-2} = \frac{(v - t + 2)}{k - t + 2} \quad r_{t-1} = \frac{(v - t + 2)(v - t + 1)r_t}{(k - t + 2)(k - 2 + 1)}.$$  

Corollary 4.2. A $t$-design is also an $s$-design for any $s \leq t$ with

$$r_s = \frac{(v - t + 1)(v - t + 2) \cdots (v - s)}{(k - t + 1)(k - t + 2) \cdots (k - s)} r_t.$$  

In particular, $r_s$ is an integer.

Corollary 4.3. A $t$-design is a design with each point in $r = r_1$ blocks and the number of blocks $b = \frac{vr_t}{k}$.  

Example. Is there a 2-design with parameters $(56, 11, 1)$? If so,  

$$r_1 = \frac{v - 1}{k - 1} \quad r_2 = \frac{56}{10}.$$
This is not an integer, hence the answer is no. 

Does there exist a 2-design with parameters \((22, 7, 2)\)? Divisibility conditions are:

\[
 r = r_1 = \frac{22 - 2 + 1}{7 - 2 + 1}r_2 \\
= \frac{21}{6} = 7. 
\]

The number of blocks is

\[
b = \frac{vr}{k} = \frac{22 \cdot 7}{22} = 22. 
\]

So divisibility conditions are satisfied. We will need to find answer to this question later.

4.1 Theory of 2-designs

Let \(X\) be a set of \(v\) points and \(\mathcal{B}\) a collection of subsets of \(X\) in a 2-design with parameters \((c, k, r_2)\). Write \(\lambda = r_2\).

**Proposition 4.4.** Let \(r = r_1\) and \(b\) be the number of blocks. Then

\[
b = \frac{vr}{k}, \quad r(k - 1) = (v - 1)\lambda. 
\]

**Proof.** We have \(b = \frac{vr}{k}\) from the introduction. Also \(r = r_1 = \frac{v - 1}{k - 1}\lambda\) by 4.1.

**trivial**

**Definition.** Call \(\mathcal{B}\) a trivial \(t\)-design if \(\mathcal{B}\) consists of all \(k\)-subsets of \(X\).

**Proposition 4.5.** Suppose \(\mathcal{B}\) is a nontrivial design. Then \(r > \lambda\).

**Proof.** By the equation \(r(k - 1) = (v - 1)\lambda\) and so \(r = \frac{v - 1}{k - 1}\lambda\) with \(\frac{v - 1}{k - 1} \geq 1\). If \(r \leq \lambda\) then \(r = \lambda\) and \(v = k\), so \(\mathcal{B}\) is trivial.

4.1.1 Incidence matrix

**Definition.** Let \(\mathcal{B}\) be a 2-design and

\[
X = \{x_1, \ldots, x_v\}, \\
\mathcal{B} = \{B_1, \ldots, B_b\}. 
\]

The **incidence matrix** of \(\mathcal{B}\) is the \(v \times b\) matrix \(A = (a_{ij})\) where

\[
a_{ij} = \begin{cases} 
1 & \text{if } x_i \in B_j, \\
0 & \text{otherwise}.
\end{cases} 
\]

Note that each row sum is \(r\) (each point lies in \(r\) blocks) and each column sum is \(k\) (each block has \(k\) points).

**Proposition 4.6.** Let \(\mathcal{B}\) be a 2-design with parameters \((v, k, \lambda)\) and \(A\) be its incidence matrix. Then \(AA^T\) is the \(v \times v\) matrix

\[
AA^T = \begin{pmatrix} 
    r & \lambda & \cdots & \lambda \\
    \lambda & r & \cdots & \lambda \\
    \vdots & \ddots & \ddots & \vdots \\
    \lambda & \lambda & \cdots & r 
\end{pmatrix} = \lambda J + (r - \lambda)I. 
\]
Proof. The $i\,\text{-th}$ entry of $AA^T$ is

$$(AA^T)_{ij} = \text{number of blocks containing } x_i \text{ and } x_j = \begin{cases} \lambda & \text{if } i \neq j, \\ r & \text{if } i = j. \end{cases}$$

\[ \square \]

**Proposition 4.7.** Let $A$ be as above. Then

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

Proof. We have (subtracting first column from the others and then adding to the first row the other rows)

$$\det(AA^T) = \begin{vmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & \ddots & \ddots & \ddots \\ \lambda & \lambda & \cdots & r \end{vmatrix}$$

$$= \begin{vmatrix} r & \lambda r & \cdots & \lambda r \\ \lambda r - \lambda & r - \lambda & \cdots & 0 \\ \lambda & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots \\ r + (v-1)\lambda & 0 & \cdots & 0 \\ \lambda & r - \lambda & \cdots & 0 \\ \lambda & 0 & r - \lambda & \cdots \\ \vdots & \ddots & \ddots & \ddots \\ \lambda & 0 & 0 & \cdots & r - \lambda \end{vmatrix}$$

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

\[ \square \]

**Proposition 4.8.** If $C$ is $m \times n$ and $D$ is $n \times p$ then

$$\text{rank}(CD) \leq \text{rank}(C) \text{ and } \text{rank}(CD) \leq \text{rank}(D).$$

Proof. The column space of $CD$ is contained within the column space of $C$. Therefore $\text{rank}(CD) \leq \text{rank}(C)$ and similarly (considering the row spaces of $CD$ and $D$), $\text{rank}(CD) \leq \text{rank}(D)$. \[ \square \]

**Theorem 4.9 (Fisher’s Inequality).** If $B$ is a non-trivial 2-design with parameters $(v, k, \lambda)$, then $b \geq v$ and $r \geq k$.

Proof. As $r > \lambda$ by 4.5, we see that

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

Hence $AA^T$ is an invertible $v \times v$ matrix. So $\text{rank}(AA^T) = v$. By 4.8, $\text{rank}(AA^T) \leq \text{rank}(A)$. Since $A$ is $v \times b$, $\text{rank}(A) \leq b$. Therefore $b \geq \text{rank}(A) \geq \text{rank}(AA^T) = v$. Also $kb = vr$ and so $r \geq k$. \[ \square \]

Example. Is there a 2-design with parameters $(46, 10, 1)$? If so, we have $r = \frac{v-1}{k-1}\lambda = \frac{45}{9} = 5$. So $b = \frac{vr}{k} = \frac{45 \cdot 5}{10} = 23$. So $b < v$, a contradiction and no such 2-design exists.

The extremal case of Fisher’s Inequality arises when $b = v$ and $r = k$. 
4.1.2 Symmetric 2-designs

**Definition.** A 2-design $\mathcal{B}$ is symmetric if $b = v$ (equivalently $r = k$).

**Example.** Let $X = \mathbb{Z}_3^2 - \{0\}$ with blocks $\{u, v, u+v\}$, $u \neq v \in X$, the 2-design with parameters $(7,3,1)$. Then $r = \frac{v-1}{k-1} = 3 = k$ and $b = 7$, so this design is symmetric. This is the *Fano plane*.

\[ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \]

**Theorem 4.10.** Suppose there exists a symmetric 2-design with parameters $(v, k, \lambda)$ and $v$ is even. Then $k - \lambda$ is a square.

**Example.** Does there exist a 2-design with parameters $(22, 7, 2)$? Here $r = \lambda (v - 1) = 2 \cdot 21 = 7 = k$, $b = 22$. So this is a symmetric design. We have $v = 22$ even, but $k - \lambda = 5$, not a square. By 4.10, no such design exists.

**Proof of Theorem 4.10.** Let $\mathcal{B}$ be such a symmetric 2-design and $A$ be the incidence matrix of $\mathcal{B}$. As $\mathcal{B}$ is symmetric, $b = v$ and so $A$ is a square $v \times v$ matrix. So $\det(A)$ exists and is an integer. We know by 4.6 that $\det(A A^T) = (r - \lambda)^{v-1}(r + (v - 1)\lambda)$. Also $\det(A) = \det(A^T)$ and so $\det(A A^T) = \det(A)^2$. So

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

Now $\mathcal{B}$ is symmetric so $r = k$ and $(v - 1)\lambda = r(k - 1) = k(k - 1)$, so

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

So by 4.6

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

The right hand side is a square, hence so is $(k - \lambda)^{v-1}$. As $v - 1$ is odd, this forces $k - \lambda$ to be a square. ■

**Theorem 4.11.** If $\mathcal{B}$ is a symmetric 2-design with parameters $(v, k, \lambda)$ then any two distinct blocks of $\mathcal{B}$ intersect in exactly $\lambda$ points.

**Proof.** Let $A$ be the incidence matrix of $\mathcal{B}$. Then $AJ = kJ$ and $JA = kJ$ (rows and column sums of $A$ are equal to $k$). Also by 4.6 $AA^T = \lambda J + (k - \lambda)I$. Now $A$ commutes with $J$ and with $I$, hence $A$ commutes with $AA^T$. In other words $A(AA^T) = (AA^T)A$. By 4.6, $\det(A) \neq 0$, so $A$ is invertible. Multiplying on left by $A^{-1}$ we get $AA^T = A^T A$. Hence by 4.6

$$ A^T A = AA^T = \begin{pmatrix} k & \lambda & \cdots & \lambda \\ \lambda & k & \cdots & \lambda \\ \vdots \\ \lambda & \lambda & \cdots & k \end{pmatrix}. $$
Now \( i \)-th entry of \( A^T A = \text{row } i \text{ of } A^T \cdot \text{column } j \text{ of } A \)
\[= \text{column } i \text{ of } A \cdot \text{column } j \text{ of } A \]
\[= |B_i \cap B_j|.
\]
Hence \( |B_i \cap B_j| = \lambda \) for any \( i \neq j \).

**Note.** There exists a converse to the Theorem 4.11, see Sheet 5.

### 4.2 Difference sets

**Example.** Let \( X = \mathbb{Z}_7 = \{0, 1, 2, \ldots, 6\} \) with addition modulo 7. Let \( B_0 = \{0, 1, 3\} \) and define \( B_1, B_2, \ldots, B_6 \) by
\[B_i = B_0 + i = \{b + i \mid b \in B_0\}.
\]
So the blocks are 013, 124, 235, 346, 450, 561, 602.

**Claim.** These blocks form a symmetric 2-design with parameters \((7, 3, 1)\).

**Proof.** The differences in the set \( B_0 = \{0, 1, 3\} \) are
\[0 - 1 = 6 \quad 1 - 3 = 5 \]
\[0 - 3 = 4 \quad 3 - 0 = 3 \]
\[1 - 0 = 1 \quad 3 - 1 = 2.
\]
These are all different. Now \( a, b \in B_i \) iff \( a - i, b - i \in B_0 \); clearly there is only one possible \( i \) for \( a \neq b \).

**Definition.** Let \( v \) and \( \lambda \) be positive integers. A subset \( B_0 \subseteq \mathbb{Z}_v \) is a \( \lambda \)-difference set if for any \( d \in \mathbb{Z}_v^* \), there exist exactly \( \lambda \) ordered pairs \((a, b) \mid a, b \in B_0 \text{ and } a - b = d\).

**Proposition 4.12.** Let \( B_0 \) be a \( \lambda \)-difference set in \( \mathbb{Z}_v \) with \( |B_0| = k \). Define
\[B_i = B_0 + i \text{ for } i = 0, \ldots, v - 1.
\]
Then the sets \( B_i \) are blocks of a symmetric 2-design with parameters \((v, k, \lambda)\).

**Proof.** Let \( r, s \in \mathbb{Z}_v \) with \( r \neq s \). Then \( r, s \in B_i \) if and only if \( r - i, s - i \in B_0 \). The number of \( i \)'s for which this holds is equal to the number of pairs of elements in \( B_0 \) which differ by \( r - s \). This number is \( \lambda \). Hence \( B_i \) form a 2-design. The number of blocks is \( v \), so this design is symmetric.

### 4.2.1 A family of difference sets

**Theorem 4.13.** Let \( p \) be prime, \( p \equiv 3 \mod 4 \). Let \( Q = \{x^2 \mid x \in \mathbb{Z}_p^*\} \). Then \( Q \) is a \( \lambda \)-difference set in \( \mathbb{Z}_p \) where \( \lambda = \frac{p^2 - 3}{4} \) and \(|Q| = \frac{p - 1}{2}\).

**Corollary 4.14.** For each prime \( p \equiv 3 \mod 4 \) there exists a symmetric 2-design with parameters \((p, \frac{p^2 - 3}{4}, \frac{p - 1}{2})\). The blocks are \( Q_i = Q + i \) for \( i = 0, 1, \ldots, p - 1 \).

**Example.** For \( p = 7 \), \( Q = \{1, 4, 2\} \). The parameters are \((7, 3, 1)\). This is the example above (\( B_0 = \{1, 4, 2\} \)).
For \( p = 11 \), \( Q = \{1, 4, 9, 5, 3\} \). The parameters are \((11, 5, 2)\).
Here is an example of a difference set in \( \mathbb{Z}_{13} \). Let \( B_0 = \{0, 1, 3\} \). Check that this is a \( 1 \)-difference set that gives a symmetric design with parameters \((13, 4, 1)\).

For the proof of 4.13 we need:
Proposition 4.15. Let $p \equiv 3 \mod 4$ and $Q = \{x^2 \mid x \in Z_p^*\}$. Then

(1) $|Q| = \frac{p-1}{2}$ and $Q$ is a subgroup of $Z_p^*$.

(2) $-1 \in Q$ and $Z_p^* = Q \cup (-Q)$.

Proof. 

(1) $Q$ is a subgroup since $1 \in Q$, if $x_1, y_1 \in Q$ then $x_1^2 y_1^2 = (x_1 y_1)^2 \in Q$ and if $x_1, y_1 \in Q$ then $x_1^2 = (x_1^{-1})^2 \in Q$.
Define a map $\phi : Z_p^* \to Q$ by $\phi(x) = x^2$. It is a homomorphism since $\phi(xy) = (xy)^2 = x^2 y^2 = \phi(x)\phi(y)$ with image $\Im(\phi) = Q$. We also have $x \in \ker \phi$ iff $x^2 = 1$ iff $x^2 - 1 \in Z_p$ iff $p|x^2 - 1$ iff $p|(x-1)(x+1)$ iff $p|x+1$ or $p|x-1$ iff $x = \pm 1$ in $Z_p$. So $\ker \phi = \{\pm 1\}$. We know $Z_p^*/\ker \phi = \Im \phi$ and hence $|Q| = |\Im \phi| = |Z_p^*|/|\ker \phi| = (p-1)/2$.

(2) As $p \equiv 3 \mod 4$, $\frac{p-1}{2}$ is odd. By Lagrange, $Q$ therefore has no element of order 2 and hence $-1 \in Q$. Finally, the 2 right cosets of $Q$ are $Q$ and $(-Q)$ and $Z_p^*$ is their union. \hfill \blacksquare

Proof of 4.15. Let $p \equiv 3 \mod 4$ and $Q$ as above. For $q \in Q$ define

$$E_q = \{(x_1, x_2) \mid x_i \in Q, x_1 - x_2 = q\}.$$ 

Let $r \in Q$. Then for $x_1, x_2, q \in Q$, we have $r x_1, r x_2, r q \in Q$ and $x_1 - x_2 = q \iff r x_1 - r x_2 = r q$. Hence $(x_1, x_2) \in E_q \iff (r x_1, r x_2) \in E_{rq}$. So $|E_q| = |E_{rq}|$. Also if $q \in Q$ then $-q \notin Q$ by 4.15 and $(x_1, x_2) \in E_q$ iff $(x_2, x_1) \in E_{-q}$. So $|E_q| = |E_{-q}|$. As $Z_p^* = Q \cup (-Q)$ by 4.15 we have now shown that $|E_q|$ is constant over all $x \in Z_p^*$. Hence $Q$ is a $\lambda$-difference set for some $\lambda$. To find $\lambda$, consider the number of ordered pairs $(a, b)$ in $Q$ with $a \neq b$ which is $|Q|(|Q| - 1)$. This is also equal to $\lambda|Z_p^*| = \lambda(p-1)$. So

$$\lambda(p-1) = \left(\frac{p-1}{2}\right) \cdot \left(\frac{p-3}{2}\right)$$

$$\lambda = \frac{p-3}{4}.$$ 

\hfill \blacksquare

Note. Same construction, replacing $Z_p^*$ by a field $F$ with $|F| = 3 \mod 4$ (we also know that $|F| = p^k$ for $p$ prime) and $Q = \{x^2 \mid x \in F\}$, gives $\lambda$-difference set in $F$, $\lambda = \frac{p^k-3}{4}$.

Note. Similar proof shows that the Paley graphs are strongly regular.

4.3 Affine Planes

Think of the Euclidean plane $\mathbb{R}^2$. This is naturally a “2-design” where the blocks are straight lines. The parameters would be $(\infty, \infty, 1)$. To get a finite design with this idea, replace $\mathbb{R}^2$ by $Z_p^2$ for $p$ prime.

Let $p$ be a prime so that $F = Z_p$ is a field. Define points to be the vectors in $Z_p^2$ and the blocks to be “straight lines” – the set of solutions $(x, y) \in Z_p^2$ of a linear equation $y = mx + c$ or $x = c$ where $m, c \in F$.

Alternatively, lines are sets of the form

$$v + \text{span}(w) = \{v + \lambda w \mid \lambda \in F\}$$

where $v, w \in F^2$ and $w \neq 0$.

Example. Take $Z_3$. The points are $\{(x, y) \mid x, y \in Z_3\}$. There are 9 lines of the form $y = mx + c$ and 3 lines of the form $x = c$. Some of them are

$$\begin{align*}
y &= x & : 00, 11, 22 \\
y &= x + 1 & : 01, 12, 20 \\
y &= x + 2 & : 02, 10, 21 \\
\vdots \\
x &= 2 & : 20, 21, 22.
\end{align*}$$
Example. Lines \( y = mx + c \) and \( y = mx + d \) are parallel if \( c \neq d \).

Proposition 4.17. \( \text{AG}(2, F) \) has \( p^2 + p \) lines. These lines fall into \( p + 1 \) disjoint sets each containing \( p \) parallel lines.

Proof. The \( p + 1 \) sets of lines are

\[
\mathcal{L}_m = \{ \text{line } y = mx + c \mid c \in F \}
\]

and

\[
\mathcal{L}_\infty = \{ \text{line } x = c \mid c \in F \}.
\]

Each of these sets contains \( p \) parallel lines.

Call the sets \( \mathcal{L}_m, \mathcal{L}_\infty \) parallel classes.

Proposition 4.18. Each point in \( F^2 \) lies on exactly one line in each parallel class.

Proof. Each parallel class contains \( p \) disjoint lines and so contains \( p^2 \) points, hence the whole of \( F^2 \).

4.4 Projective planes

Example. Start with \( \text{AG}(2, \mathbb{Z}_3) \). For each parallel class \( \mathcal{L}_m \) (or \( \mathcal{L}_\infty \)) add a new point \( p_m \) (or \( p_\infty \)) to the lines in \( \mathcal{L}_m \). Define a new line \( l_\infty = \{ p_1, p_1, p_2, p_\infty \} \) to have a new structure with points 00, 01, 02, 10, 11, 12, 20, 21, 22, \( p_0, p_1, p_2, p_\infty \) and lines

\[
(y = x) \cup p_1 = 00, 11, 22, p_1,
\]

\[
(y = x + 1) \cup p_1 = 00, 11, 22, p_1,
\]

\[
\vdots
\]

\[
(x = 2) \cup p_\infty = 20, 21, 22, p_\infty
\]

and \( l_\infty = p_0, p_1, p_2, p_\infty \).

Let \( F = \mathbb{Z}_p \), \( p \) prime. Define the projective plane over \( F \) \( \text{PG}(2, F) \) as follows: start with the affine plane \( \text{AG}(2, F) \) (points \( F^2 \), lines \( y = mx + c, x = c \)) and add a total of \( p + 1 \) new points \( p_m, m \in F, p_\infty \). To each line in parallel class \( \mathcal{L}_m \) (\( \mathcal{L}_\infty \) respectively) add the point \( p_m \) (\( p_\infty \) respectively). Finally, define the “line at infinity”

\[
l_\infty = \{ p_m, p_\infty \mid m \in F \}.
\]

So points of \( \text{PG}(2, F) \) are \( F^2, p_m, p_\infty \) \( (p^2 + p + 1 \) of them) and lines of \( \text{PG}(2, F) \) are \( (y = mx + c) \cup p_m, (x = c) \cup p_\infty \) and \( l_\infty \) \( (p^2 + p + 1 \) of them, all of size \( p + 1 \)).
Proposition 4.19. PG(2, F) is a symmetric 2-design with parameters \((p^2 + p + 1, p + 1, 1)\).

Proof. Need to show that any 2 points lie on a unique line. Let \(P, Q\) be two points. If \(P, Q \in F^2\) they lie on a unique line in AG(2, F) by 4.17, hence on a unique line in PG(2, F). If \(P \in F^2\) and \(Q = p_m\) \((m \in F \cup \{\infty\})\) then by 4.18, \(P\) lies on a unique line \(l\) in the parallel class \(L_m\), and so \(P, Q\) lie on the line \(l \cup p_m\) and this is the only line containing \(P, Q\). Finally, if \(P, Q\) are both \(p_m\), then \(l_\infty\) is the only line containing \(P, Q\). ■

4.5 Higher-dimensional geometry

Let \(F = \mathbb{Z}_p\) \((p\text{-prime})\). Then \(F^n\) is a vector space over \(F\) of dimension \(n\).

Definition. Let \(m, n \in \mathbb{N}\) with \(1 \leq m \leq n\). The \(p\)-binomial coefficient \(\binom{n}{m}_p\) is

\[
\binom{n}{m}_p = \frac{(p^n - 1)(p^{n-1} - 1)\cdots(p^{n-m+1} - 1)}{(p^m - 1)(p^{m-1} - 1)\cdots(p - 1)}.
\]

Example. \(\binom{5}{2}_3 = \frac{3^5 - 1}{3^2 - 1} = \frac{242}{8} = 30\).

Proposition 4.20. Let \(1 \leq m \leq n - 1\). Then:

1. The number of \(m\)-dimensional subspaces of \(F^n\) is \(\binom{n}{m}_p\).

2. For \(0 \neq v \in F^n\), the number of \(m\)-dimensional subspaces of \(F^n\) containing \(v\) is

\[
\begin{cases}
1 & \text{if } m = 1, \\
\binom{n-1}{m-1}_p & \text{if } m > 1.
\end{cases}
\]

3. If \(v, w \in F^n\) are linearly independent, the number of \(m\)-dimensional subspaces containing \(v, w\) is

\[
\begin{cases}
0 & \text{if } m = 1, \\
1 & \text{if } m = 2, \\
\binom{n-2}{m-2}_p & \text{if } m > 2.
\end{cases}
\]

Proof will be given later.
Example. Let \( n = 2, m = 1 \). Points are the vectors in \( F^2 \) and blocks the subsets \( v + \text{span}(w) \), that is the lines in \( AG(2, F) \). So in this case, design is the affine plane \( AG(2, F) \).

**Proposition 4.21.**

1. \( AG(n, F)_m \) is a 2-design with parameters \((p^n, p^m, \lambda)\) where
   \[
   \lambda = \left\{ \begin{array}{ll} 
   1 & \text{if } m = 1, \\
   \frac{1}{(n-1)p} & \text{if } m > 1.
   \end{array} \right.
   \]
2. \( AG(n, F)_m \) is a 3-design iff \( F = Z_2 \) and \( m \geq 2 \), with parameters \((2^n, 2^m, r_3)\) where
   \[
   r_3 = \left\{ \begin{array}{ll} 
   1 & \text{if } m = 2, \\
   \frac{1}{(m-2)p} & \text{if } m > 2
   \end{array} \right.
   \]

**Example.** \( AG(3, Z_2)_2 \) is a 3-design with parameters \((8, 4, 1)\).

**Proof of 4.21**

1. Let \( v_1, v_2 \in F^n \). Any block containing \( v_1 \) is of the form \( v_1 + W \) where \( W \) is an \( m \)-dimensional subspace of \( F^n \). Also \( v_1, v_2 \in v + W \iff v_1 - v_2 \in W \). So the number of blocks containing \( v_1, v_2 \) is the number of \( m \)-dimensional subspaces \( W \) containing the vector \( v_1 - v_2 \). This number is \( \lambda \) as in (1).
2. Let \( F = Z_2 \) and let \( v_1, v_2, v_3 \in F^n \) be distinct. Then \( v_1, v_2, v_3 \in v + W \iff v_1 - v_2, v_1 - v_3 \in W \). As \( F = Z_2 \), the vectors \( v_1 - v_2, v_1 - v_3 \) are linearly independent. Hence the number of blocks containing \( v_1, v_2, v_3 \) is \( r_3 \) as in (2).

**Proof of 4.20**

1. Recall the number of non-zero vectors in \( V = F^n \) is \( p^n - 1 \). An \( m \)-dimensional subspace \( W \) is the span of a set \( v_1, \ldots, v_m \) of \( m \) linearly independent vectors in \( V \). The number of such (ordered) sets \( v_1, \ldots, v_m \) is
   \[
   (p^n - 1) \times (p^n - p) \times (p^n - p^2) \times \cdots \times (p^n - p^{m-1})
   \]
   (choose \( v_2 \in V \setminus \text{span}(v_1) \), \( p^n - p \) choices, choose \( v_3 \in V \setminus \text{span}(v_1, v_2) \), \( p^n - p^2 \) choices, etc.). How many choices of \( v_1, \ldots, v_m \) have the same \( m \)-dimensional subspace as their span? The number of (ordered) bases \( u_1, \ldots, u_m \) of \( W \) is
   \[
   (p^n - 1) \times (p^n - p) \times (p^n - p^2) \times \cdots \times (p^n - p^{m-1})
   \]
   Therefore the number of \( m \)-dimensional subspaces of \( V \) is
   \[
   \frac{(p^n - 1)(p^n - p) \cdots (p^n - p^{m-1})}{(p^m - 1)(p^m - p) \cdots (p^m - p^{m-1})} = \frac{(p^n - 1)(p^{n-1} - 1) \cdots (p^{n-m+1} - 1)}{(p^m - 1)(p^{m-1} - 1) \cdots (p - 1)} = \binom{n}{m}_p.
   \]
2. Clear if \( m = 1 \), so assume \( m \geq 2 \). An \( m \)-dimensional subspace containing \( v \) has basis \( v, v_2, \ldots, v_m \). The number of such sets of linearly independent vectors (ordered) is
   \[
   (p^n - p) \times (p^n - p^2) \times \cdots \times (p^n - p^{m-1}).
   \]
The number of such sets spanning the same $m$-dimensional subspace $W$ is

\[\frac{w_2^{w_2} (p^m - p) \times p^2 \times \cdots \times (p^m - p^{m-1})}{(p^m - p) \times (p^m - p^2) \times \cdots \times (p^m - p^{m-1})}.\]

So the number of $m$-dimensional subspaces containing $v$ is

\[\frac{(p^n - p)(p^n - p^2)\cdots(p^n - p^{m-1})}{(p^m - p)(p^m - p^2)\cdots(p^m - p^{m-1})} = \binom{n-1}{m-1}.\]

(3) Similar, counting the linearly independent sets $v, w, v_3, \ldots, v_m$. 

\[\blacksquare\]
Chapter 5

Some connections

We have seen some connections of codes leading to designs (e.g. $G_{24}$ gives us 5-design with parameters $(24,8,1)$, weight 4 codewords in $H'$ give us a 3-design with parameters $(8,4,1)$). Here are results giving other connections:

1. strongly regular graphs to designs,
2. designs to strongly regular graphs (more interesting),
3. codes, graphs, designs and groups.

There are many more connections; see the Cameron’s book.

**Proposition 5.1.**

1. Suppose $\Gamma$ is strongly regular graph with parameters $(v,k,a,a)$. Define a design with points the vertices of $\Gamma$ and blocks the sets $B_x$ of neighbours of $x$ for each vertex $x$. This is a symmetric 2-design with parameters $(v,k,a)$.

2. Suppose $\Gamma$ is strongly regular graph with parameters $(v,k,a,a+2)$. Define a design with points the vertices of $\Gamma$ and blocks the sets $x \cup B_x$ ($B_x$ as above) for each vertex $x$. This is a symmetric 2 design with parameters $(v,k+1,a+2)$

**Proof.**

1. Let $x, y$ be vertices of $\Gamma$. The blocks containing $x, y$ are $B_w$ for $w$ joined to both $x$ and $y$. Since $a = b$ for $\Gamma$, the number of such $w$'s is $a$.

2. The blocks containing $x, y$ in case they are joined is $B_w$, $w$ a common neighbour of $x$ and $y$ and also $B_x$ and $B_y$ – there are $a+2$ such blocks. If $x, y$ are not joined, blocks containing both are $B_w$ for $w$ a common neighbour of $x, y$ – there are $a+2$ such blocks.

**Example.** $T(6)$ has parameters $(15,8,4,4)$ and so we get a symmetric design with parameters $(15,8,4)$. $L(4)$ has parameters $(16,6,2,2)$ and so we get a symmetric design $(16,6,2)$. $T(6)^2$ has parameters $(15,6,1,3)$ and so we get a symmetric design $(15,6,3)$.

**Definition.** A 2-design is quasi-symmetric if there exist integers $x, y$ such that for any two blocks $B_1, B_2$, $|B_1 \cap B_2| = x$ or $y$.

**Note.** Why the name? Because if $|B_1 \cap B_2|$ is constant, then the design is symmetric (Sheet 5).

**Example.** In affine plane $AG(2,G)$, any two lines meet in 0 or 1 points. Golay code $G_{23}$ leads to a four design with points the 23 coordinate positions and the blocks equal positions of 1's in weight 7 codewords. The parameters are $(23,7,1)$. 
Claim. This design is quasi-symmetric.

Proof. Let \( B \) be the block corresponding to weight 7 codeword \( c \in G_{23} \). So for \( c, d \in G_{23} \) of weight 7, \(|B_c \cap B_d| = |c, d|\). We know that \( \text{wt}(c + d) = \text{wt}(c) + \text{wt}(d) - 2|c, d| = 14 - 2|c, d| \). So \( 2|B_c \cap B_d| = 14 - \text{wt}(c + d) \). As \( c + d \in G_{23} \) and \( \text{wt}(c + d) \) must be even and less than 14, it follows from \( 2.23 \) that \( \text{wt}(c + d) = 8 \) or 12, hence \(|B_c \cap B_d| = 1 \) or 3.

Theorem 5.2. Let \( \mathcal{B} \) be a quasi-symmetric 2-design with block intersections of size \( x, y \) where \( x < y \). Define \( \Gamma(\mathcal{B}) \) to have vertices the blocks in \( \mathcal{B} \) and join two vertices \( B_1 \) and \( B_2 \) if and only if \(|B_1 \cap B_2| = y\). Then \( \Gamma(\mathcal{B}) \) is a strongly regular graph.

Proof. Given as the advanced coursework.

Example. Let \( \mathcal{B} = \text{AG}(2, F) \). Vertices of \( \Gamma(\mathcal{B}) \) are the lines in \( \text{AG}(2, F) \) and we join two lines if they intersect (in one point). So in \( \Gamma(\mathcal{B})^c \) we join two lines if they are parallel. Each parallel class \( \mathcal{L}_m \) forms a complete graph \( K_p \), so \( \Gamma(\mathcal{B})^c \) is a union of disjoint complete graphs; a strongly regular graph with \( b = 0 \) by \( 3.2 \).

Let \( \mathcal{B} \) be a 4 design constructed from \( G_{23} \) as above. What are the parameters of \( \Gamma(\mathcal{B}) \)? We have \( v \) the number of blocks, that is the number of codewords of weight 7 in \( G_{23} \). For \( k, a, b \) see the advanced coursework.

Now a connection between designs, codes, graphs and groups.

5.1 Isomorphisms of designs

Let \( \mathcal{B}_1, \mathcal{B}_2 \) be designs with point sets \( X_1, X_2 \). We say \( \mathcal{B}_1, \mathcal{B}_2 \) are isomorphic if there exists a bijection \( \varphi : X_1 \to X_2 \) sending the blocks in \( \mathcal{B}_1 \) to the blocks in \( \mathcal{B}_2 \). Call \( \varphi \) an isomorphism.

Example. Let \( X = \mathbb{Z}_7 \), \( \mathcal{B}_1 \) be the blocks \( B_i = \{0, 1, 3\} + i \), a 2-design with parameters \((7, 3, 1)\). Let \( X_2 = \mathbb{Z}_2^3 - \{0\}, \mathcal{B}_2 \) be the blocks \( \{x, y, x + y\}, x, y \in X_2, x \neq y \). Is \( \mathcal{B}_1 = \mathcal{B}_2 \)? We can try to construct the bijection:

\[
\begin{align*}
013 & \rightarrow 100, 010, 110 \\
124 & \rightarrow 010, 001, 011 \\
234 & \rightarrow 001, 110, 111 \\
346 & \rightarrow 110, 011, 101 \\
450 & \rightarrow 011, 111, 100 \\
561 & \rightarrow 111, 101, 010 \\
602 & \rightarrow 101, 100, 001 \\
\end{align*}
\]

So the isomorphism is \( 0 \rightarrow x, 1 \rightarrow y, 2 \rightarrow z, 3 \rightarrow x + y \). In fact, any choice of linearly independent \( x, y, z \) would have worked.

Definition. For \( \mathcal{B} \) a design with point set \( X \), an isomorphism \( \mathcal{B} \rightarrow \mathcal{B} \) (i.e. a bijection \( X \rightarrow X \) sending blocks to blocks) is called an automorphism of \( \mathcal{B} \).

Notice that \( \phi \) is a bijection \( X \rightarrow X \), that is a permutation of \( X \), so \( \phi \in \text{Sym}(X) \), the group of all permutations of \( X \). Define \( \text{Aut}(\mathcal{B}) \) to be the set of all automorphisms of \( \mathcal{B} \).

Proposition 5.3. \( \text{Aut}(\mathcal{B}) \) is a subgroup of \( \text{Sym}(X) \). In particular, \( \text{Aut}(\mathcal{B}) \) is a group called the automorphism group of \( \mathcal{B} \).
Example. Let $\mathcal{B}$ be an affine plane $AG(2, Z_p)$. Let $G = \text{Aut}(\mathcal{B}) \leq \text{Sym}(Z_p^2)$. Then $G$ contains: (1) $g \in \text{GL}(2, Z_p)$: $g$ gives permutation $v \mapsto g v$ so $g \in \text{Sym}(Z_p^2)$. We have $g(v + \lambda w) = g v + \lambda g w$ and hence $g$ sends $v + \text{span}(w) \mapsto g v + \text{span}(gv)$ and so $g \in \text{Aut}(\mathcal{B})$. (2) Translation $t_x$ for $x \in Z_p^2$ with $t_x(v) = v + x$ for $v \in Z_p^2$. Then $t_x \in \text{Sym}(Z_p^2)$ and $t_x(v + \lambda w) = v + x + \lambda w$ so $t_x$ sends $v + \text{span}(w) \mapsto v + x + \text{span}(w)$. Hence $t_x \in \text{Aut}(\mathcal{B})$.

Note that for $A \in \text{GL}(2, Z_p)$ and $x \in Z_p^2$, we have $t_x(Av) = Av + x$ for all $v \in Z_p^2$. This is an affine transformation of $Z_p^2$. Denote it by $\pi_{A,x}$. We leave proofs of the following statements as an exercise:

1. $\{\pi_{A,x} \mid A \in \text{GL}(2, Z_p), x \in Z_p^2\}$ is a group. It is called the affine general linear group $\text{AGL}(2, Z_p)$.

2. Translations $T = \{t_x \mid x \in Z_p^2\}$ form a normal subgroup of $\text{AGL}(2, Z_p)$.

3. $T \cong (Z_p^2, +) \cong C_p \times C_p$ and $\text{AGL}(2, Z_p)/T \cong \text{GL}(2, Z_p)$.

4. $\text{Aut}(\mathcal{B}) \cong \text{AGL}(2, Z_p)$.

Example. Consider $\mathcal{B}$ a projective plane in $PG(2, Z_p)$. There is an alternative viewpoint on $PG(2, Z_p)$: Let $V = Z_p^3$, a 3-dimensional vector space over $Z_p$. Identify points in $PG(2, Z_p)$ with 1-spaces: $(a, b)$ with $\text{span}(1, a, b)$, $p_m$ with $\text{span}(0, 1, m)$ and $p_\infty$ with $\text{span}(0, 0, 1)$. Note that these are all the 1-spaces in $V$ since the number of those is $\binom{p^2-1}{1}_p = \frac{p^3-1}{p-1} = p^2 + p + 1$, the number of points in $PG(2, Z_p)$.

Claim. The lines in $PG(2, Z_p)$ are of the form $L_W$, where $W$ is a 2-space in $V$ and $L_W = \{\text{span}(v) \mid v \in W, v \neq 0\}$.

There are many automorphisms of $\mathcal{B}$: Let $g \in \text{GL}(3, Z_p)$. We have

$$g(\text{span}(v)) = \text{span}(g(v)).$$

Therefore $g$ sends $L_W$ to $L_{g(W)}$ and so is an automorphism of $\mathcal{B}$.

Final point

If $g = \lambda I$ for $\lambda \in Z_p$ then $g$ gives identity permutation. If we define $\pi_g$ to be the permutation of points given by $\pi_g$ then the map $g \mapsto \pi_g$ in $\text{GL}(3, Z_p) \to \text{Sym}(X)$ is a homomorphism with kernel $Z = \{\lambda I \mid \lambda \in Z_p\}$. So its image is isomorphic with $\text{GL}(3, Z_p)/Z = \text{PGL}(3, Z_p)$. So $\text{PGL}(3, Z_p) \leq \text{Aut}(\mathcal{B})$. In fact, we can prove that $\text{PGL}(3, Z_p) = \text{Aut}(\mathcal{B})$.
Index

$K_n$, 19
$L(n)$, 21
$N(k, d)$, 20
$P(p)$, 21
$S_e(c)$, 11
$T(n)$, 21
$[v, w]$, 15
$AG(n, F_m)$, 39
$bb Z_p$, 43
$Aut(\mathcal{B})$, 42
$\Gamma = (V, E)$, 19
$Ham(k)$, 9
$PG(2, F)$, 37
$\binom{n}{m}_q r$, 38
$\lambda$-difference set, 35
$wt(x)$, 7
$d(C)$, 5
$d(x, y)$, 5
$e$-perfect, 12
$t$-design, 3, 31
$2$-design, 5

affine plane, 37
alphabet, 1
automorphism, 42

block, 31
blocks, 3

check matrix, 7
code, 5
Golay, 12
Hamming, 9
linear, 6
codewords, 5
complement, 22
connected, 19
corrects, 5

design, 3, 31
trivial, 32
diameter, 19
distance, 3, 19

edges, 2, 19
extended Golay code, 15

Fano plane, 34
Golay Code, 16
graph, 2, 19
complete, 19
lattice, 21
Moore, 20
Paley, 21
regular, 2
strongly, 2
Triangular, 21

Hamming code, 9
isomorphic, 42
isomorphism, 42
joined, 19

Lattice graph, 21
length, 1, 19
minimum distance, 5
Moore graph, 20
multiplicity, 23
neighbours, 2
octads, 17
Paley graph, 21
parallel, 37
parallel classes, 37
parameters, 3, 31
path, 19
Petersen graph, 2
projective plane, 37
quadi-symmetric, 41
regular, 19
strongly regular, 21
trace, 26
Triangular graph, 21
valency, 2
vertices, 2

weight, 7
word, 1