M3/4 P55 Algebraic combinatorics

Spring 2015

Contents

Introduction

- Combinatorics is a study of discrete structures.
- in the scope of this course we will deal with:
  - Codes
    - Subsets of $\mathbb{Z}_2^n$ where $\mathbb{Z}_2 = \{0, 1\}$
  - Graphs
    - sets of vertices with edges connecting them. Essentailly a set with a collection of pairs. They can also be represented as adjacency matrices
  - Designs
    - Originated in statistical theory of experiments
    - Collections of subsets of agiven set

- We will use tools from linear algebra to study those discrete structurs.
- `http://wwwf.imperial.ac.uk/~mwl/m3p17/`

0.1 Codes

Everyday language consists of an alphabet and words which are distinguished admissible strings of letters.

For a machine language the alphabet is going to consist of:

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

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

A corresponds to 01000001
B corresponds to 01000010

And so on

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

$$L \to 01001100$$

etc.

Transmitted over a digital medium.

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

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

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

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

E.g. *Algubreic Cumbinatorocs* can easily be corrected, because there are not

many similar words in the English language, and there is a set of admissible words in English, not every combination of letters is a word.

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

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

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

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

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

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

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

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

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

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

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

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

Well:

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

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

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

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

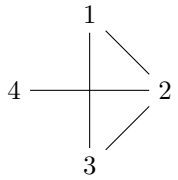
The aim of coding theory: Find codes C s.t:

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

0.2 Graphs

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

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

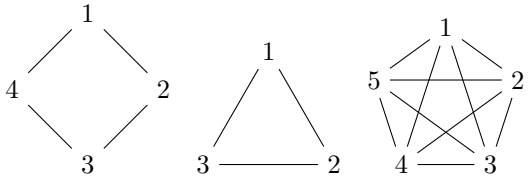


We will study a special type of graphs that can be expressed as codes and lend themselves well to algebraic methods

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

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

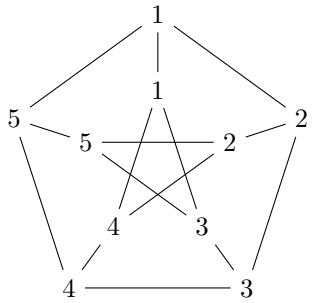
E.g. any polygon is a regular graph with a valency = 2



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

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

Petersen graph is a strongly regular graph of valency 3



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

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

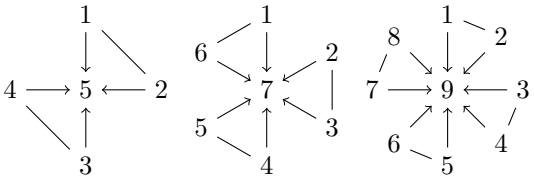
Theorem 0.2 (Friendship Theorem, Erds, Remyi)**.**
In a community where any two people have exactly one common acquaintance, there is someone who knows everyone.

This can be described as a graph:

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

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

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



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

0.3 Designs

Used in statistics and experimental design.

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

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

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

consumers $c_1, , c_6$ testing:

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

Definition.
Let X be a set, $v = |X|$ and let $\mathscr{B}$ be a collection of subsets of X.

Call $(X, \mathscr{B})$ (or just $\mathscr{B}$) a *design* if:

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

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

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

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

The larger t is, the stronger this condition is.

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

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

In general for $t \geq 1$ say $\mathscr{B}$ is a t-design if any t points lie in the same number of blocks.
The larger t is, the stronger this condition is.
For large t, nontrivial t-designs are rather rare. (e.g. the first nontrivial 6-design was found in 1980s).

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

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

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

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

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

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

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

$$X = \mathbb{Z}_p^2$$

$$\text{Blocks } = \text{ collection of lines}$$

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

1 Error correcting codes

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

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

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

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

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

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

Proof.
Let:

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

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

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

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

1.1 Error correction

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

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

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

Equivalent definition:

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

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

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

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

Then by the triangle inequality

$$d(c_1, c_2) \leq d(c_1, w) + d(c_2, w)$$
$$d(c_1, c_2) \leq 2e$$

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

□

1.2 Linear codes

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

I.e:

1. $0 \in C$

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

Basic construction of codes using matrices:

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

E.g:

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

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

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

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

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

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

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

1.3 Minimum Distance

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

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

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

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

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

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

Then $x + y \in C$ and so

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

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

□

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

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

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

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

1.4 Check matrix

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

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

We call A a check matrix of the linear code C

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

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

Then C corrects 1 error.

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

Examples

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

   Corrects 1 error by 1.6

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

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

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

   This sends 16 messages abcd using codewords abcdxyz where

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

   This is called a Hamming code Ham(3)

1.5 Correcting an error

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

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

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

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

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

1.6 Hamming Codes

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

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

2. Ham(k) corrects 1 error

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

2. Follows from 1.6

□

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

E.g all Hamming codes ham(k) are equivalent.

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

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

1. *Suppose every set of $d-1$ columns of A is linearly independent. If that is true, then the minimum distance $d(C) \geq d$*
2. *Suppose in addition to (1) that $\exists$ a set of d columns of A that are linerarly dependent. then $d(C) = d$*

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

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

So

$$\begin{aligned} 0 = Ac &= Ae_{i_1} + ... + Aei_r \\ &= \text{col}i_1 + ... + \text{col}i_r \end{aligned}$$

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

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

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

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

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

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

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

□

E.g

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

Take

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

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

Need:

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

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

so take

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

This defines the code

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

1.7 Hamming bounds

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

Recall:

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

Proposition 1.9 (1.9)**.** $|S_e(v)| =$ *sum of binomial coefficients*

Proof. Let:

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

Then:

$$|S_e(v)| = d_i + d_1 + ... + d + e$$

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

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

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

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

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

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

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

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

is there one of dim 3?

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

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

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

1. $wt(c_i) \geq 4 \qquad \forall i$

2. $wt(c_i + c_j) \geq 3 \qquad \forall i \neq j$

3. $wt(c_1 + c_2 + c + 3) \geq 2$

Do $\exists$ such $c_1, c_2, c_3 \in \mathbb{Z}_2^6$?
Answer: No, see problem sheet 2

1.8 Perfect Codes

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

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

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

1-perfect codes

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

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

for some k

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

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

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

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

Theorem 1.13. *The only* e-perfect *codes are:*

1. $e = 1$, *Ham(k)*

2. $n = 2e + 1 \qquad C = \{0...0, 1...1\}$ *of dim 1*

3. $e = 3, n = 23, dimC = 12$, *the* Golay code

Miraculous arithmetic:

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

Hamming bound is a result for non existence of codes C of length n, correcting e errors.

This time we will concern ourselves with an existence result

Gilbert-Varshamov bound

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

Ans:

Hamming bound gives

$$|C| \leq \frac{2^1 5}{1 + 15 + \binom{15}{2}} = \frac{2^1 5}{|2|} < 2^9$$

Hence $dimC \leq 8$

More on this later.

Theorem 1.14 (G-V bound)**.** *[1.12] Let n, k, d be positive integers such that*

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

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

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

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

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

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

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

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

We construct such a matrix inductively, column by column.

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

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

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

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

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

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

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

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

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

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

satisfies property (2)

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

1.9 The Golay Code

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

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

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

And its reverse K, with check matrix

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

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

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

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

Proposition 1.15 (1.13)**.** $H \cap K = \{0^7, 1^7\}$ & $H' \cap K' = \{0^8, 1^8\}$

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

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

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

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

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

□

$H = Ham(3)$ $\qquad$ $H' = H +$ parity check

$K =$ reverse of H $\qquad$ $K' = K +$ parity check

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

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

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

Proposition 1.16. *G_24 is a linear code of dimension 12.*

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

Closure

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

$(a_1 + x_1, b_1 + x_1, a_1 + b_1 + x_1) + (a_2 + x_2, b_2 + x_2, a_2 + b_2 + x_2) =$
$= (a_1 + a_2 + x_1 + x_2, b_1 + b_2 + x_1, +x_2, a_1 + a_2 + b_1 + b_2 + x_1 + x_2) \in G_24$
Since: $\quad a_1, a_2, b_1, b_2 \in H \qquad x_1, x_2 \in K'$

Dimension

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

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

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

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

So $dim G_24 = 12$

Basis

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

□

Theorem 1.17. *G_24 has minimum distance 8*

[1.15]

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

□

Proposition 1.18 (1.16)**.**
Let $v, w \in \mathbb{Z}_2^n$

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

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

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

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

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

Proposition 1.19.
If $a, b, x \in \mathbb{Z}_2^n$ then $[a, x] + [b, x] + [a + b, x]$ is even.

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

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

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

Proposition 1.20 (1.18)**.** *If $c \in G_2 4$ then 4 divides $wt(c)$.*

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

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

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