M3P17 Algebraic Combinatorics

0 Introduction

Combinatorics in the study of discrete structures. These include:

(1) codes (subsets of $\mathbb{Z}_2^n$, where $\mathbb{Z}_2 = \{0, 1\}$),

(2) graphs (vertices and edges),

(3) designs (collection of subsets of a given set).

Codes

Aims of coding theory: To find codes C such that:

(1) C has many codewords,

(2) C corrects enough errors,

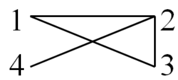
(3) the length of C is not too big.

Graphs

Definition:

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

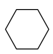
Example:

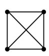
If $V = \{1, 2, 3, 4\}$, $E = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{2, 4\}\}$, then the graph is  .

Definition:

For a vertex x, call the other vertices joined to x by an edge the neighbours of x. Call Γ a regular graph if every vertex has the same number of neighbours (say, k), and call k the valency of Γ.

Example:

(1)  is regular with valency 2.

(2)  is regular with valency 3.

Definition:

A graph Γ is strongly regular if:

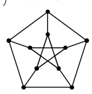
(1) Γ is regular with valency k,

(2) any pair of joined vertices has the same number of common neighbours a,

(3) any pair of non-joined vertices has the same number of common neighbours b.

Example:

(1) $\square$ is strongly regular, with $k = 2$, $a = 0$, $b = 2$.

(2) The Petersen graph  is strongly regular, with $k = 3$, $a = 0$, $b = 1$.

Proposition 0.1 (Friendship Thorem):

In a community where any 2 people have exactly 1 common acquaintance, there is someone who knows everyone.

Proof of Proposition 0.1:

Let vertices = people, and join 2 vertices iff they know each other. Since every 2 vertices have exactly 1 common neighbour, the graph must look like  ie. a windmill (all known proofs use linear algebra).

Designs

Suppose we have v varieties of chocolate to be tested by consumers. We want each customer to test k varieties, and each variety to be tested by r consumers.

Example:

Let $v = 8$, $k = 4$, $r = 3$, then number of consumers $= \dfrac{vr}{k} = 6$. Call the consumers c_1, ..., c_6, then c_1 tests 1234, c_2 tests 5678, c_3 tests 1357, c_4 tests 2468, c_5 tests 1247, c_6 tests 3568.

Definition:

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

(1) every set in $\mathcal{B}$ has size k,

(2) every element of X lies in r subsets of $\mathcal{B}$.

The subsets in $\mathcal{B}$ are called the blocks of the design, and the parameters of the design are (v, k, r).

Example:

The example $(8, 4, 3)$ above is a design.

Definition:

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

Example:

The example $(8, 4, 3)$ above is not a 2-design.

In general, for $t \geq 1$, call $\mathcal{B}$ a t-design if any t points lie in the same number of blocks.

The larger t is, the stronger the condition is. For large t, non-trivial t-designs are rare (in fact, the 1st non-trivial 6-design was found only in the 1980s).

Example:

Let p be a prime, then $\mathbb{Z}_p$ is a field. Call $\mathbb{Z}_p^2 = \{(x_1, x_2) : x_i \in \mathbb{Z}_p\}$ 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 and b are fixed vectors in $\mathbb{Z}_p^2$, then any 2 vectors in $\mathbb{Z}_p^2$ lie on a unique line. Now let $X = \mathbb{Z}_p^2$, $\mathcal{B} =$ collection of lines, then $(X, \mathcal{B})$ is a 2-design with parameters $(p^2, p, p+1)$ (because there are $p+1$ choices for b and p choices for the corresponding $a \Rightarrow r = \dfrac{kp(p+1)}{v} = p+1$).

1 Error-correcting Codes

Define $\mathbb{Z}_2 = \{0, 1\}$, with addition and multiplication mod 2, and $\mathbb{Z}_2^n = \{(x_1, \cdots, x_n) : x_i \in \mathbb{Z}_2\}$. With the usual addition and scalar multiplication, $\mathbb{Z}_2^n$ is a vector space over $\mathbb{Z}_2$, with standard basis $e_1, \cdots, e_n$ (where $e_k = \underbrace{0 \cdots 01}_{k} 0 \cdots 0$) 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, and the distance between 2 vectors in $\mathbb{Z}_2^n$ is $d(x, y) =$ number of coordinates where x and y differ.

Example:

$d(10111, 01110) = 3$.

Proposition 1.1 (Triangle Inequality):

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

Proof of Proposition 1.1:

Let $A = \{i : x_i \neq z_i\}$, $B = \{i : x_i = y_i, x_i \neq z_i\}$, $C = \{i : x_i \neq y_i, x_i \neq z_i\}$, then $|A| = |B| + |C|$, $d(x, z) = |A|$, $d(x, y) \geq |C|$ and $d(y, z) \geq |B| \Rightarrow d(x, y) + d(y, z) \geq |C| + |B| = |A| = d(x, z)$.

Definition:

Let $C \subseteq \mathbb{Z}_2^n$ be a code. The minimum distance of C is $d(C) = \min\{d(x, y) : x, y \in C, x \neq y\}$.

Remark:

Let $C \subseteq \mathbb{Z}_2^n$, $e \in \mathbb{N}$, then we say C corrects e errors if whenever a codeword $c \in C$ is sent, and $\leq e$ errors are made such that the vector w is received, the closest codeword to w is c.

Definition:

$C \subseteq \mathbb{Z}_2^n$ corrects e errors if $\forall c_1, c_2 \in C$ and $w \in \mathbb{Z}_2^n, d(c_1, w), d(c_2, w) \leq e \Rightarrow c_1 = c_2$.

Remark:

Equivalently, for $c \in C$, define a sphere $S_e(c) = \{w \in \mathbb{Z}_2^n : d(c, w) \leq e\}$, then C corrects e errors if $S_e(c_1) \cap S_e(c_2) = \varnothing \ \forall c_1, c_2 \in C$, $c_1 \neq c_2$.

Proposition 1.2:

Code C corrects e errors iff $d(C) \geq 2e + 1$.

Proof of Proposition 1.2:

Suppose $d(C) \geq 2e+1$. Pick $x, y \in C$, then if $w \in \mathbb{Z}_2^n$ satisfies $d(x,w), d(y,w) \leq e$, by Proposition 1.1, $d(x,y) \leq d(x,w) + d(y,w) \leq 2e \Rightarrow x = y \Rightarrow C$ corrects e errors.

Conversely, pick $x, y \in C$ such that $x \neq y$, $d(x,y) \leq 2e$. Let x, y possibly differ at bits $b_1, \cdots, b_{2e}$. Pick $w \in \mathbb{Z}_2^n$, such that $w_{b_i} = x_{b_i}$ for $1 \leq i \leq e$, $w_{b_i} = y_{b_i}$ for $e+1 \leq i \leq 2e$, and $w_i = x_i = y_i$ everywhere else, then $d(x,w), d(y,w) \leq e$ but $x \neq y \Rightarrow C$ does not correct e errors.

Linear codes

Definition:

A linear code is a code $C \subseteq \mathbb{Z}_2^n$ which is a subspace of $\mathbb{Z}_2^n$ ie. $0 \in C$ and $x, y \in C \Rightarrow x+y \in C$.

Proposition 1.3:

Let A be a $m \times n$ matrix over $\mathbb{Z}_2$. Then $C = \{x \in \mathbb{Z}_2^n : Ax = 0\}$ is a linear code, and $\dim C = n - \operatorname{rank} A$.

Proof of Proposition 1.3:

Easy peasy.

Example:

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

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

Proposition 1.4:

If C is a linear code with $\dim C = k$, then $|C| = 2^k$.

Proof of Proposition 1.4:

Let $c_1, \cdots, c_k$ be a basis of C, then every $c \in C$ is a unique linear combination $c = \lambda_1 c_1 + \cdots + \lambda_k c_k$ where $\lambda_i \in \mathbb{Z}_2 \Rightarrow |C| = \prod_i (\text{number of choices for } \lambda_i) = 2^k$.

Minimum distance

Definition:

For $x \in \mathbb{Z}_2^n$, the weight of x is $\operatorname{wt}(x) =$ number of coordinates of x equal to 1.

Remark:

$\text{wt}(x) = d(x, 0)$, and $\text{wt}(x + y) = d(x, y)$.

Proposition 1.5:

Let C be a linear code, then $d(C) = \min\{\text{wt}(c) : c \in C \setminus \{0\}\}$.

Proof of Proposition 1.5:

Let $c \in C \setminus \{0\}$ have minimal weight r. Since C is linear, $0 \in C$ and $d(c, 0) = \text{wt}(c) = r \Rightarrow d(C) \le r$. Now let $x, y \in C$ and $x \ne y$, then $x + y \in C \setminus \{0\} \Rightarrow d(x, y) = \text{wt}(x + y) \ge r \Rightarrow d(C) \ge r$. Hence $d(C) = r$.

Example:

Consider $C_3 \subseteq \mathbb{Z}_2^6$. Check that $\min\{\text{wt}(c) : c \in C \setminus \{0\}\} = 3$, hence $d(C_3) = 3 \Rightarrow C_3$ corrects 1 error by Proposition 1.2.

Check matrices

Definition:

Suppose A is a $m \times n$ matrix over $\mathbb{Z}_2$ and $C = \{x \in \mathbb{Z}_2^n : Ax = 0\}$. Then we call A a check matrix of the linear code C.

Proposition 1.6:

Suppose the check matrix A of the linear code C satisfies:

(1) A has no zero column,

(2) A does not have 2 equal columns.

Then C corrects 1 error.

Proof of Proposition 1.6:

Suppose C does not correct 1 error, then $d(C) \le 2$ by Proposition 1.2 $\Rightarrow$ by Proposition 1.5, $\exists c \in C \setminus \{0\}$ such that $\text{wt}(c) = 1$ or 2. If $\text{wt}(c) = 1$, then $c = e_i \Rightarrow$ if $Ac = 0$, then the i-th column of A is 0 ($\Rightarrow\Leftarrow$). If $\text{wt}(c) = 2$, then $c = e_i + e_j \Rightarrow$ if $Ac = 0$, then $Ae_i + Ae_j = 0 \Rightarrow$ the i-th and j-th column of A are equal ($\Rightarrow\Leftarrow$) $\Rightarrow C$ corrects 1 error.

Example:

(1) $C_3 = \left\{ x \in \mathbb{Z}_2^6 : \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} x = 0 \right\}$ corrects 1 error by Proposition 1.6.

(2) Suppose a code C corrects 1 error and has a $3 \times n$ check matrix. By Proposition 1.6, to find the maximum dimension of C, we need to find the largest n such that $\exists\, 3 \times n$ matrix with distinct non-zero columns in $\mathbb{Z}_2^3 \Rightarrow n = 2^3 - 1 = 7$. Pick $A = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$, then C has dimension 4, and can send 16 messages $abcd$ using codewords $abcdxyz$, where $x = a + b + c$, $y = a + b + d$ and $z = a + c + d$. This is called a Hamming code, denoted $\mathrm{Ham}(3)$.

Hamming codes

Definition:

Let $k \geq 3$, then a Hamming code $\mathrm{Ham}(k)$ is a code for which the check matrix has all the non-zero vectors in $\mathbb{Z}_2^k$ as columns.

Proposition 1.7:

(1) $\mathrm{Ham}(k)$ has length $2^k - 1$ and dimension $2^k - 1 - k$.

(2) $\mathrm{Ham}(k)$ corrects 1 error.

Proof of Proposition 1.7:

(1) Since there are $2^k - 1$ non-zero vectors in $\mathbb{Z}_2^k$, the check matrix of $\mathrm{Ham}(k)$ is $k \times (2^k - 1)$ and has rank $k \Rightarrow$ the result follows.

(2) Follows easily from Proposition 1.6.

Definition:

Let $C, C' \subseteq \mathbb{Z}_2^n$ be codes. Call C and C' equivalent codes if there is a permutation of their coordinates which sends the codewords in C bijectively to those in C'.

Example:

All Hamming codes $\mathrm{Ham}(k)$ are equivalent.

Correcting 1 error

Suppose we have a code C correcting 1 error, with check matrix A. A codeword c is sent, and 1 error is made, so that c' is received. Since $c' = c + e_i$ for some i, $Ac' = A(c + e_i) = Ac + Ae_i = 0 + Ae_i = i$-th column of $A \Rightarrow$ the error occurred in the i-th entry of c.

Example:

Let $C = \text{Ham}(3)$. Suppose we receive $c' = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}^\top$, then $Ac' = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} =$ 6th column of $A \Rightarrow$ the corrected codeword is $c = 1101010$.

Correcting > 1 error

Proposition 1.8:

Let $d \geq 2$, C be a code with check matrix A. Then:

(1) $d(C) \geq d$ if every set of $d-1$ columns of A is linearly independent,

(2) $d(C) = d$ if, in addition, $\exists$ a set of d columns of A that are linearly dependent.

Proof of Proposition 1.8:

(1) Suppose $d(C) \leq d-1$, then $\exists c \in C \setminus \{0\}$ with $\text{wt}(c) = r \leq d-1 \Rightarrow c = e_{i_1} + \cdots + e_{i_r} \Rightarrow Ac = Ae_{i_1} + \cdots + Ae_{i_r} = (\text{sum of columns } i_1, \cdots, i_r \text{ of } A) = 0 \Rightarrow$ these columns are linearly dependent $(\Rightarrow\Leftarrow) \Rightarrow d(C) \geq d$.

(2) Suppose columns $i_1, \cdots, i_d$ of A are linearly dependent, in addition to (1). Let $\lambda_1 A_{i_1} + \cdots + \lambda_d A_{i_d} = 0$ for some $\lambda_r \in \mathbb{Z}_2$. Since any $d-1$ columns of A are linearly independent, we must have $\lambda_r = 1$ $\forall r \Rightarrow A(e_{i_1} + \cdots + e_{i_d}) = 0 \Rightarrow$ write $c = e_{i_1} + \cdots + e_{i_d}$, then $c \in C$ and $\text{wt}(c) = d \Rightarrow$ since $d(C) \geq d$ by (1), we must have $d(C) = d$.

Example:

If we want a linear code of length 9 and dimension 2 which corrects 2 errors, the check matrix A should be 7×9 (of rank 7), and we also need $C = \left\{x \in \mathbb{Z}_2^9 : Ax = 0\right\}$. By Proposition 1.8, to have $d(C) \geq 5$, we need every set of 4 columns of A to be linearly independent. Take $A = \begin{pmatrix} c_1 & c_2 & I_7 \end{pmatrix}$, then we need $\text{wt}(c_1), \text{wt}(c_2) \geq 4$, and $\text{wt}(c_1 + c_2) \geq 3 \Rightarrow$ let $c_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}^\top$, $c_2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}^\top$, then they define the code $C = \{abaaa(a+b)bbb : a, b \in \mathbb{Z}_2\} = \left\{0^9, 101111000, 010001111, 111110111\right\}$.

Hamming bound

Proposition 1.9:

$|S_e(v)| = 1 + \binom{n}{1} + \cdots + \binom{n}{e}$.

Proof of Proposition 1.9:

Let d_i = number of $x \in \mathbb{Z}_2^n$ such that $d(v,x) = i$, then $|S_e(v)| = d_0 + d_1 + \cdots + d_e$. The vectors with distance i from v are precisely those differing from v at exactly i coordinates $\Rightarrow d_i = \binom{n}{i} \Rightarrow$ the result follows.

Theorem 1.10 (Hamming bound):

Let C be a code of length n, correcting e errors. Then $|C| \leq \dfrac{2^n}{1 + \binom{n}{1} + \cdots + \binom{n}{e}}$.

Proof of Theorem 1.10:

Since C corrects e errors, the spheres $S_e(c)$ for $c \in C$ are all disjoint $\Rightarrow \left|\bigcup_{c \in C} S_e(c)\right| = |C|\,|S_e(c)|$. But $\bigcup_{c\in C} S_e(c) \subseteq \mathbb{Z}_2^n$, so $2^n \geq \left|\bigcup_{c \in C} S_e(c)\right| = |C| \left[1 + \binom{n}{1} + \cdots + \binom{n}{e}\right] \Rightarrow |C| \leq \dfrac{2^n}{1 + \binom{n}{1} + \cdots + \binom{n}{e}}$.

Example:

Let C be a linear code of length 9 that corrects 2 errors, then by Theorem 1.10, $|C| \leq \dfrac{2^9}{1 + \binom{9}{1} + \binom{9}{2}} = \dfrac{2^9}{46} < 2^4 \Rightarrow \dim C \leq 3$. From the previous example, $\exists C$ with $\dim C = 2$. To find if $\exists C$ with $\dim C = 3$, we need a 6×9 check matrix A with any 4 columns linearly independent. Take $A = \begin{pmatrix} c_1 & c_2 & c_3 & I_6 \end{pmatrix}$, then c_1, c_2, c_3 satisfy $\mathrm{wt}(c_i) \geq 4\ \forall i$, $\mathrm{wt}(c_i + c_j) \geq 3\ \forall i \neq j$, and $\mathrm{wt}(c_1 + c_2 + c_3) \geq 2$. After a tedious exercise, it can be shown that $\nexists c_i \Rightarrow \nexists C$.

Perfect codes

Definition:

A code $C \in \mathbb{Z}_2^n$ is e-perfect ($e \geq 1$) if it corrects e errors, and $|C| = \dfrac{2^n}{1 + \binom{n}{1} + \cdots + \binom{n}{e}}$.

Remark:

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

Proposition 1.11:

Let $C = \mathbb{Z}_2^n$, then $|C| = \dfrac{2^n}{1+n} \Leftrightarrow n = 2^k - 1, |C| = 2^{n-k}$ for some k.

Proof of Proposition 1.11:

If $|C| = \dfrac{2^n}{1+n}$, then $1 + n = 2^k$ for some k.

Conversely, if $n = 2^k - 1$ and $|C| = 2^{n-k}$, then obviously $|C| = \dfrac{2^n}{1+n}$.

Proposition 1.12:

Ham(k) is a 1-perfect code.

Proof of Proposition 1.12:

Ham(k) has length $n = 2^k - 1$, dimension $n-k$ and corrects 1 error $\Rightarrow |\text{Ham}(k)| = 2^{n-k} = \dfrac{2^n}{1+n} \Rightarrow$ the result follows.

Remark:

The only e-perfect codes are:

(1) Ham(k), with $e = 1$,

(2) $C = \{0\cdots 0, 1\cdots 1\}$, with length $n = 2e+1$ and dimension 1,

(3) the Golay code G_{23}, with $n = 23$, $e = 3$, $\dim G_{23} = 12$.

Gilbert-Varshamov bound

Example:

Let C be a linear code of length 15, correcting 2 errors. Then the Hamming bound gives $|C| \le \dfrac{2^{15}}{1 + \binom{15}{1} + \binom{15}{2}} = \dfrac{2^{15}}{121} < 2^9 \Rightarrow \dim C \le 8$.

Theorem 1.13 (GV bound):

Let $n, k, d \in \mathbb{Z}^+$ such that $1 + \dbinom{n-1}{1} + \cdots + \dbinom{n-1}{d-2} < 2^{n-k}$, then $\exists$ a linear code of length n and dimension k, such that $d(C) \ge d$.

Example:

Let $n = 15$ and $d = 5$, then we have $1 + \dbinom{14}{1} + \dbinom{14}{2} + \dbinom{14}{3} = 470 < 2^9 = 2^{15-6} \Rightarrow \exists$ a code of dimension 6, but we still do not know if $\exists$ codes of dimension 7 or 8.

Proof of Theorem 1.13:

Assume $1 + \dbinom{n-1}{1} + \cdots + \dbinom{n-1}{d-2} < 2^{n-k}$. We want to construct 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. Choose the 1st $n-k$ columns of A to be $e_1, \cdots, e_{n-k}$, then clearly they are linearly independent. Now suppose inductively that there are i columns $c_1, \cdots, c_i \in \mathbb{Z}_2^{n-k}$ where $n-k \le i \le n-1$, such that any $d-1$ of these are linearly independent. The number of vectors in $\mathbb{Z}_2^{n-k}$ which are the sum of $\le d-2$ of $c_1, \cdots, c_i$ is $\le 1 + \dbinom{i}{1} + \cdots + \dbinom{i}{d-2} \le 1 + \dbinom{n-1}{1} + \cdots + \dbinom{n-1}{d-2} < 2^{n-k}$, so $\exists c_{i+1} \in \mathbb{Z}_2^{n-k}$ which is not the sum of $\le d-2$ of $c_1, \cdots, c_i \Rightarrow$ if we have $A_i = \begin{pmatrix} c_1 & \cdots & c_i \end{pmatrix}$, we can extend it to get $A_{i+1} = \begin{pmatrix} c_1 & \cdots & c_{i+1} \end{pmatrix} \Rightarrow$

repeat until we get $A = A_n$ that satisfies all the required properties.

The Golay code

The Golay code is a code of length 23, dimension 12, which corrects 3 errors and is perfect. To construct it, we first construct the extended Golay code G_{24}. Start with $H = \text{Ham}(3)$, with 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 $\begin{pmatrix} 0&0&1&0&1&1&1 \\ 0&1&0&1&0&1&1 \\ 1&0&0&1&1&0&1 \end{pmatrix}$. Add the parity check bit (= sum of bits) to H and K to obtain H' and K' respectively, then we get $H' = \begin{Bmatrix} 00000000 & 11111111 \\ 10001110 & 01110001 \\ 01001101 & 10110010 \\ 00101011 & 11010100 \\ 00010111 & 11101000 \\ 11000011 & 00111100 \\ 10100101 & 01011010 \\ 10011001 & 01100110 \end{Bmatrix}$, $K' = \begin{Bmatrix} 00000000 & 11111111 \\ 11100010 & 00011101 \\ 01100101 & 10011010 \\ 10101001 & 01010110 \\ 11010001 & 00101110 \\ 10000111 & 01111000 \\ 01001011 & 10110100 \\ 00110011 & 11001100 \end{Bmatrix}$, both of which are linear codes of length 8 and dimension 4, with codewords of weight 0, 4 or 8. Also, the 14 codewords in H' of weight 4 form a design with parameters $(16, 8, 7)$ (v = number of bits $\times$ number of choices per bit $= 8 \times 2 = 16$).

Proposition 1.14:

$H \cap K = \{0^7, 1^7\}$, and $H' \cap K' = \{0^8, 1^8\}$.

Proof of Proposition 1.14:

Let $v \in H \cap K$, then $v = abcd(a+b+c)(a+b+d)(a+c+d)$ since $v \in H \Rightarrow$ since $v \in K$ too, we have $c + (a+b+c) + (a+b+d) + (a+c+d) = b + d + (a+b+d) + (a+c+d) = a + d + (a+b+c) + (a+c+d) = 0 \Rightarrow a + c = c + d = a + b = 0 \Rightarrow a = b = c = d = 0$ or 1 $\Rightarrow v = 0^7$ or 1^7. Also, by considering parity check bits, $H' \cap K' = \{0^8, 1^8\}$.

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 $a, b \in H'$, $x \in K'$.

Example:

(1) $a = b = x = 0^8 \Rightarrow v = 0^{24}$.

(2) $a = b = x = 1^8 \Rightarrow v = (0^8, 0^8, 1^8)$.

(3) $a = x = 1^8$, $b = 0^8 \Rightarrow v = (0^8, 1^8, 0^8)$.

(4) $a = b = 0^8$, $x = 1^8 \Rightarrow v = 1^{24}$.

(5) $a = 10001110$, $b = 10011001$, $x = 01001011 \Rightarrow v = 110001011101001001011100$.

Proposition 1.15:

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

Proof of Proposition 1.15:

Clearly $0^{24} \in G_{24}$. Now suppose $a_1, a_2, b_1, b_2 \in H'$, $x_1, x_2 \in K'$, 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 $a_1 + a_2, b_1 + b_2 \in H'$ and $x_1 + x_2 \in K' \Rightarrow G_{24}$ is a linear code.
Moreover, $(a_1 + x_1, b_1 + x_1, a_1 + b_1 + x_1) = (a_2 + x_2, b_2 + x_2, a_2 + b_2 + x_2) \Rightarrow a_1 = a_2$, $b_1 = b_2$, $x_1 = x_2 \Rightarrow$ distinct choices of (a, b, x) gives distinct elements of $G_{24} \Rightarrow |G_{24}| =$ number of triples $(a, b, x) = |H'|^2 |K'| = 2^{12} \Rightarrow \dim |G_{24}| = 12$.

Remark:

$(a+x, b+x, a+b+x) = (a, 0, a)+(0, b, b)+(x, x, x) \Rightarrow$ if a_i, b_i and x_i $(1 \le i \le 4)$ are bases for H', H' and K' respectively, then $\{(a_i, 0, a_i), (0, b_i, b_i), (x_i, x_i, x_i)\}$ form a basis for G_{24}.

Definition:

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

Proposition 1.16:

Let $v, w \in \mathbb{Z}_2^n$, then:

(1) $\mathrm{wt}(v + w) = \mathrm{wt}(v) + \mathrm{wt}(w) - 2[v, w]$,

(2) if $4 \mid \mathrm{wt}(v)$ and $4 \mid \mathrm{wt}(w)$, then $4 \mid \mathrm{wt}(v + w)$ iff $[v, w]$ is even.

Proof of Proposition 1.16:

(1) Let $r = \mathrm{wt}(v)$, $s = \mathrm{wt}(w)$ and $t = [v, w]$, then we have (reordering coordinates if required) $v = \underbrace{1\cdots1}_{t}\underbrace{1\cdots1}_{r-t}\underbrace{0\cdots0}_{s-t}0\cdots0$, $w = \underbrace{1\cdots1}_{t}\underbrace{0\cdots0}_{r-t}\underbrace{1\cdots1}_{s-t}0\cdots0 \Rightarrow v + w = \underbrace{0\cdots0}_{t}\underbrace{1\cdots1}_{r-t}\underbrace{1\cdots1}_{s-t}0\cdots0 \Rightarrow \mathrm{wt}(v + w) = r + s - 2t = \mathrm{wt}(v) + \mathrm{wt}(w) - 2[v, w]$.

(2) Follows easily from (1).

Proposition 1.17:

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

Proof of Proposition 1.17:

Let $r = [a, x]$, $s = [b, x]$, $u =$ number of places where a, b, x are all 1. Then (reordering coordinates if needed) $x = \underbrace{1\cdots1}_{u}\underbrace{1\cdots1}_{r-u}\underbrace{1\cdots1}_{s-u}0\cdots0$, $a = \underbrace{1\cdots1}_{u}\underbrace{1\cdots1}_{r-u}\underbrace{0\cdots0}_{s-u}0\cdots0$, $b = \underbrace{1\cdots1}_{u}\underbrace{0\cdots0}_{r-u}\underbrace{1\cdots1}_{s-u}0\cdots0 \Rightarrow a+b = \underbrace{0\cdots0}_{u}\underbrace{1\cdots1}_{r-u}\underbrace{1\cdots1}_{s-u}0\cdots0 \Rightarrow [a,x]+[b,x]+[a+b,x] = r+s+(r+s-2u) = 2(r+s-u)$, which is even.

Proposition 1.18:

If $c \in G_{24}$, then $4 \mid \mathrm{wt}(c)$.

Proof of Proposition 1.18:

Let $c = (a+x, b+x, a+b+x)$ for some $a, b \in H'$, $x \in K'$, then $c = (a, b, a+b) + (x, x, x)$. Let $v = (a, b, a+b)$, $w = (x, x, x)$, then $4 \mid \mathrm{wt}(v), \mathrm{wt}(w)$ since $4 \mid \mathrm{wt}(a), \mathrm{wt}(b), \mathrm{wt}(a+b), \mathrm{wt}(x)$, and $[v, w] = [a, x] + [b, x] + [a+b, x]$ is even by Proposition 1.17 $\Rightarrow 4 \mid \mathrm{wt}(v+w) = \mathrm{wt}(c)$ by Proposition 1.16(2).

Theorem 1.19:

$d(G_{24}) = 8$.

Proof of Theorem 1.19:

Suppose $d(G_{24}) < 8$, then by Proposition 1.18, $\exists c \in G_{24} \setminus \{0\}$ such that $\mathrm{wt}(c) = 4$. Let $c = (a+x, b+x, a+b+x)$ for some $a, b \in H'$, $x \in K'$, then $\mathrm{wt}(a+x) = \mathrm{wt}(a) + \mathrm{wt}(x) - 2[a, x]$ is even. Similarly, $\mathrm{wt}(b+x)$ and $\mathrm{wt}(a+b+x)$ are all even $\Rightarrow \geq 1$ of $a+x$, $b+x$, $a+b+x$ must be $0 \Rightarrow x = a, b$ or $a+b \Rightarrow x \in H' \cap K' = \left\{0^8, 1^8\right\}$ by Proposition 1.14 $\Rightarrow a+x, b+x, a+b+x \in H' \Rightarrow a+x, b+x, a+b+x$ have weight 0, 4 or 8 $\Rightarrow$ 2 of these are 0^8. If $a+x = b+x = 0^8$, then $a = x = b \Rightarrow c = (0^8, 0^8, x)$. If $a+x = a+b+x = 0^8$, then $a = x$, $b = 0^8 \Rightarrow c = (0^8, x, 0^8)$. If $b+x = a+b+x = 0^8$, then $b = x$, $a = 0^8 \Rightarrow c = (x, 0^8, 0^8)$. Either way, $\mathrm{wt}(c) = 0$ or 8 $(\Rightarrow\Leftarrow) \Rightarrow d(G_{24}) \geq 8 \Rightarrow$ since $(1^8, 0^8, 0^8) \in G_{24}$, $d(G_{24}) = 8$.

The 3-perfect code G_{23}

Definition:

The Golay code G_{23} is the code of length 23 consisting of codewords in G_{24} with the last bit deleted.

Remark:

G_{23} is linear, and $|G_{23}| = |G_{24}| = 2^{12} \Rightarrow \dim G_{23} = 12$.

Theorem 1.20:

G_{23} is 3-perfect.

Proof of Theorem 1.20:

$d(G_{24}) = 8 \Rightarrow d(G_{23}) \geq 7$, and $(0^8, 0^8, 1^8) \in G_{24} \Rightarrow d(G_{23}) = 7 \Rightarrow G_{23}$ corrects 3 errors.
Also, $|G_{23}| = \dfrac{2^{23}}{1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}} = \dfrac{2^{23}}{2048} = 2^{12} \Rightarrow G_{23}$ is 3-perfect.

Remark:

Codewords in G_{24} are those in G_{23} with parity check bit added.

A 5-design from G_{24}

Define X = set of 24 coordinate positions in G_{24}, and a block B_c = set of 8 coordinate positions of the 1's in each codeword $c \in G_{24}$ of weight 8. Call the blocks the octads of G_{24}.

Theorem 1.21:

The octads of G_{24} form the blocks of a 5-design, where every set of 5 points lies in a unique octad.

Proof of Theorem 1.21:

There is a correspondence $\mathbb{Z}_2^{24} \leftrightarrow$ subsets of X, $v \leftrightarrow P_v$ = set of positions of 1's in v. Let $v \in \mathbb{Z}_2^{24}$ have weight 5, and delete the last bit of v to get $v' \in \mathbb{Z}_2^{23}$, with $\mathrm{wt}(v') = 4$ or 5, $P_{v'} \subseteq \{1, \cdots, 23\}$. Since G_{23} is 3-perfect, $\exists! c' \in G_{23}$ such that $v' \in S_3(c')$ ie. $d(v', c') \leq 3$.
If $\mathrm{wt}(v') = 4$, then $\mathrm{wt}(c') = 7$, and $P_{v'} \subseteq P_{c'}$. Add the parity check bit of c' to get $c \in G_{24}$, with $\mathrm{wt}(c) = 8 \Rightarrow P_v = P_{v'} \cup \{24\} \subseteq P_{c'} \cup \{24\} = P_c$.
Otherwise, if $\mathrm{wt}(v') = 5$, then $\mathrm{wt}(c') = 7$ or 8, and $P_{v'} \subseteq P_{c'}$ too. Again, add the parity check bit of c' to get $c \in G_{24}$, with $\mathrm{wt}(c) = 8 \Rightarrow P_v = P_{v'} \subseteq P_{c'} \subseteq P_c$.
Either way, $\exists! c \in G_{24}$ where $\mathrm{wt}(c) = 8$, with $P_v \subseteq P_c = B_c \Rightarrow$ the result follows.

Proposition 1.22:

(1) Codewords in G_{24} have weight 0, 8, 12, 16 or 24, and $N_i = N_{24-i}$, where N_i is the number of codewords in G_{24} with weight i.

(2) Codewords in G_{23} have weight 0, 7, 8, 11, 12, 15, 16 or 23, and $M_i = M_{23-i}$, where M_i is the number of codewords in G_{23} with weight i.

Proof of Proposition 1.22:

(1) The map $G_{24} \to G_{24}$, $c \mapsto c + 1^{24}$ is a bijection that sends codewords of weight i to

codewords of weight $24 - i \Rightarrow N_i = N_{24-i}$. Also, pick $c \in G_{24} \setminus \{0\}$, then $4 \mid \text{wt}(c)$ by Proposition 1.18 and $\text{wt}(c) \geq 8$ by Theorem 1.19 $\Rightarrow \text{wt}(c) = 8$, 12, 16 or 24.

(2) Similar to (1).

Proposition 1.23:

Let X be a set of v points, $\mathcal{B}$ be a t-design with blocks of size k, in which any t points lie in r_t blocks. Then $\mathcal{B}$ is a $(t-1)$-design, and $r_{t-1} = \left(\dfrac{v-t+1}{k-t+1}\right) r_t$.

Proof of Proposition 1.23:

Pick $S \subseteq X$, $|S| = t-1$, $r(S)$ = number of blocks containing S. Consider pairs (x, B), where $x \in X \setminus S$ and B is a block containing $S \cup \{x\}$, then the number of such pairs = ways to choose x × ways to choose B given $x = (v - (t-1)) \times r_t$.

On the other hand, the number of such pairs is also = ways to choose B × ways to choose x given $B = r(S) \times (k - (t-1)) \Rightarrow r(S) = \left(\dfrac{v-t+1}{k-t+1}\right) r_t \Rightarrow$ the result follows.

Corollary 1.24:

A t-design is also an s-design $\forall 1 \leq s \leq t$, and $r_{t-2} = \left(\dfrac{v-t+2}{k-t+2}\right) r_{t-1}, \cdots, r = r_1 = \left(\dfrac{v-1}{k-1}\right) r_2$, $b = r_0 = \dfrac{vr}{k}$.

Proof of Corollary 1.24:

Follows easily from Proposition 1.23.

Proposition 1.25:

(1) In G_{24}, $N_{16} = N_8$ = number of octads = 759.

(2) In G_{23}, $M_7 = 253$, $M_8 = 506$.

Proof of Proposition 1.25:

(1) Applying Corollary 1.24 to the 5-design formed by the octads of G_{24} gives $r_5 = 1$, $r_4 = \left(\dfrac{24-5+1}{8-5+1}\right) r_5 = 5$, $r_3 = \left(\dfrac{24-4+1}{8-4+1}\right) r_4 = 21$, $r_2 = \left(\dfrac{24-3+1}{8-3+1}\right) r_3 = 77$, $r_1 = \left(\dfrac{24-2+1}{8-2+1}\right) r_2 = 253$, $N_{16} = N_8 = r_0 = \left(\dfrac{24-1+1}{8-1+1}\right) r_1 = 759$.

(2) M_7 = (number of octads containing point 24) $= r_1 = 253 \Rightarrow M_8 = N_8 - M_7 = 506$.

Error correction in G_{24}

Proposition 1.26:

$\forall c, d \in G_{24}$, $c \cdot d = c^\top d = 0 \in \mathbb{Z}_2$.

Proof of Proposition 1.26:

By Proposition 1.18, $4 \mid \mathrm{wt}(c), \mathrm{wt}(d), \mathrm{wt}(c+d)$ $\forall c, d \in G_{24}$ $\Rightarrow$ by Proposition 1.17, since $\mathrm{wt}(c+d) = \mathrm{wt}(c) + \mathrm{wt}(d) - 2[c, d]$, $[c, d]$ is even $\Rightarrow c^\top d = 0$.

Remark:

With a basis $\{c_i : 1 \leq i \leq 12\}$ of G_{24}, let $A = \begin{pmatrix} c_1 & \cdots & c_{12} \end{pmatrix}^\top$ with size 12×24, then $Ac = \begin{pmatrix} c_1 \cdot c & \cdots & c_{12} \cdot c \end{pmatrix}^\top = 0$ $\forall c \in G_{24}$. Moreover, since $\dim G_{24} = 12$, G_{24} is the solution space for $Ax = 0 \Rightarrow A$ is a check matrix for G_{24}.

Suppose $c \in G_{24}$ is sent and $t \leq 3$ errors are made, such that the received vector is $x = c + e_{i_1} + \cdots + e_{i_t}$. Let the 253 codewords in G_{24} with weight 8 and a 1 in the 1st coordinate be $c_1, \cdots c_{253}$, with corresponding octads $B_1, \cdots B_{253}$, then $c_i \cdot x = 0$ for $1 \leq i \leq 253$ if $x \in G_{24}$, else we can count how many $c_i \cdot x = 1$ there are.

Proposition 1.27:

The number of i such that $c_i \cdot x = 1$ is:

t	1	2	3	4
x_1 correct	77	112	125	128
x_1 wrong	253	176	141	128

Proof of Proposition 1.27:

When $t = 1$, $x = c + e_j$ for some $c \in G_{24} \Rightarrow c_i \cdot x = c_i \cdot (c + e_j) = c_i \cdot e_j = 1$ iff $j \in B_i$. If x_1 is correct, then $j \neq 1 \Rightarrow$ (number of $c_i \cdot x = 1$) = (number of B_i containing j) = (number of octads containing 1 and j) $= r_2 = 77$. Otherwise, if x_1 is wrong, then $k = 1 \Rightarrow$ (number of $c_i \cdot x = 1$) = (number of B_i containing 1) $= r_1 = 253$.

When $t = 2$, $x = c + e_j + e_k$ for some $c \in G_{24} \Rightarrow c_i \cdot x = c_i \cdot e_j + c_i \cdot e_k = 1$ iff exactly 1 of $j, k \in B_i$. If x_1 is correct, then $j, k \neq 1 \Rightarrow$ (number of $c_i \cdot x = 1$) = (number of octads containing 1 and j but not k, or 1 and k but not j) $= 2(r_2 - r_3) = 2(77 - 21) = 112$. Otherwise, if x_1 is wrong, let $j = 1$ WLOG $\Rightarrow$ (number of $c_i \cdot x = 1$) = (number of B_i containing 1 but not k) $= r_1 - r_2 = 253 - 77 = 176$.

When $t = 3$, $x = c + e_j + e_k + e_l$ for some $c \in G_{24} \Rightarrow c_i \cdot x = 1$ iff exactly 1 or 3 of $j, k, l \in B_i$. If x_1 is correct, then $j, k, l \neq 1 \Rightarrow$ (number of $c_i \cdot x = 1$) $= 3(r_2 - 2r_3 + r_4) + r_4 = 3(77 - 42 + 5) + 5 = 125$. Otherwise, if x_1 is wrong, let $j = 1$ WLOG $\Rightarrow$ (number of $c_i \cdot x = 1$) $= (r_1 - 2r_2 + r_3) + r_3 = (253 - 154 + 21) + 21 = 141$.

When $t = 4$, $x = c + e_j + e_k + e_l + e_m$ for some $c \in G_{24} \Rightarrow c_i \cdot x = 1$ iff exactly 1 or 3 of $j, k, l, m \in B_i$. If x_1 is correct, then $j, k, l, m \neq 1 \Rightarrow$ (number of $c_i \cdot x = 1$) $=$

$4(r_2 - 3r_3 + 3r_4 - r_5) + 4(r_4 - r_5) = 4(77 - 63 + 15 - 1) + 4(5 - 1) = 128$. Otherwise, if x_1 is wrong, let $j = 1$ WLOG $\Rightarrow$ (number of $c_i \cdot x = 1$) $= (r_1 - 3r_2 + 3r_3 - r_4) + 3(r_3 - r_4) = (253 - 231 + 63 - 5) + 3(21 - 5) = 128$.

Cyclic codes

Definition:

A linear code $C \in \mathbb{Z}_2^n$ is cyclic if $(c_1, \cdots, c_n) \in C \Rightarrow (c_n, c_1, \cdots, c_{n-1}) \in C$.

Remark:

The definition implies that all other cyclic shifts are also $\in C$.

Example:

(1) $C = \{000, 110, 101, 011\} \subseteq \mathbb{Z}_2^3$ is cyclic.

(2) Ham(3), with check matrix $A = \begin{pmatrix} 1&0&1&1&1&0&0 \\ 1&1&1&0&0&1&0 \\ 0&1&1&1&0&0&1 \end{pmatrix}$ is cyclic, because the shifted check matrix $A' = \begin{pmatrix} 0&1&0&1&1&1&0 \\ 0&1&1&1&0&0&1 \\ 1&0&1&1&1&0&0 \end{pmatrix}$ is in fact $\begin{pmatrix} A_1 + A_2 \\ A_3 \\ A_1 \end{pmatrix}$, where $A_i = i$-th row of A.

(3) G_{23} is equivalent to a cyclic code.

Ideals

Definition:

A commutative ring $(R, +, \times)$ is a set R with $+, \times$ such that:

(1) $(R, +)$ is an abelian group with identity 0,

(2) $(R, \times)$ is commutative and associative,

(3) $\forall a, b, c \in R$, $a \times (b + c) = (a \times b) + (a \times c)$.

Example:

$\mathbb{Z}_2[x]$ is the ring of polynomials $a_0 + a_1x + \cdots + a_nx^n$ with $a_i \in \mathbb{Z}_2$ and normal $+, \times$ for polynomials.

Definition:

Let R be a commutative ring, then a subset $I \subseteq R$ is an ideal if:

(1) I is (am!) a subgroup of $(R, +)$,

(2) $IR = \{ir : i \in I, r \in R\} \subseteq I$.

Example:

Let $a \in R$, and define $(a) = \{ar : r \in R\}$, then (a) is an ideal, called the principal ideal generated by a.

Quotient rings

Let I be an ideal of R. For $x \in R$, define the coset $x + I = \{x + i : i \in I\}$, and call the set of all cosets $\dfrac{R}{I}$. Define $+, \times$ on $\dfrac{R}{I}$ by $(x+I)+(y+I) = (x+y)+I$, $(x+I)(y+I) = xy+I$, then they are well-defined, and make $\dfrac{R}{I}$ into a (commutative) ring, called the quotient ring.

Example:

Consider $\dfrac{\mathbb{Z}_2[x]}{I}$, where $I = \left(x^2-1\right)$, then $\{I, 1+I, x+I, 1+x+I\} \subseteq \dfrac{\mathbb{Z}_2[x]}{I}$. Now let $f(x)+I \in \dfrac{\mathbb{Z}_2[x]}{I}$, then $f(x) = (x^2-1)q(x)+r(x)$, where $\deg r < 2 \Rightarrow f(x)+I = r(x)+(x^2-1)q(x)+I = r(x)+I$ since $(x^2-1)q(x) \in I \Rightarrow r(x)$ is either $1, x, 1+x$ or 0 $\Rightarrow \dfrac{\mathbb{Z}_2[x]}{I} = \{I, 1+I, x+I, 1+x+I\}$.

Notation:

Write $x+I = \bar{x}$, then $\dfrac{\mathbb{Z}_2[x]}{I} = \{0, 1, \bar{x}, 1+\bar{x}\}$.

Proposition 1.28:

Let $R = \dfrac{\mathbb{Z}_2[x]}{I}$ where $I = (x^n-1)$, $\bar{x} = x+I \in R$, then $R = \left\{a_0 + \cdots + a_{n-1}\bar{x}^{n-1} : a_i \in \mathbb{Z}_2\right\}$, with the usual addition and multiplication determined by the relation $\bar{x}^n = 1$.

Proof of Proposition 1.28:

Let $S = \left\{a_0 + \cdots + a_{n-1}\bar{x}^{n-1} : a_i \in \mathbb{Z}_2\right\}$, then clearly $S \subseteq R$. Now let $f(\bar{x}) \in R$, then $f(x) = (x^n-1)q(x)+r(x)$, where $\deg r < n \Rightarrow f(\bar{x}) = r(\bar{x}) + (\bar{x}^n-1)q(\bar{x}) = r(\bar{x}) \in S \Rightarrow R \subseteq S \Rightarrow R = S$.

Example:

Let $R = \dfrac{\mathbb{Z}_2[x]}{(x^3-1)}$, then $(1+\bar{x})(1+\bar{x}^2) = 1+\bar{x}+\bar{x}^2+\bar{x}^3 = \bar{x}+\bar{x}^2$.

Remark:

By Proposition 1.28, $\exists$ a bijection $\pi : \mathbb{Z}_2^n \to \dfrac{\mathbb{Z}_2[x]}{(x^n-1)}$, $(a_0, \cdots, a_{n-1}) \mapsto a_0 + \cdots + a_{n-1}\bar{x}^{n-1}$, which is also an isomorphism of groups under $+$.

Example:

Let $C = \{000, 110, 011, 101\} \subseteq \mathbb{Z}_2^3$, then $\pi(C) = \left\{0, 1+\bar{x}, \bar{x}+\bar{x}^2, 1+\bar{x}^2\right\} \subseteq \dfrac{\mathbb{Z}_2[x]}{(x^3-1)}$.

Proposition 1.29:

$C \subseteq \mathbb{Z}_2^n$ is a cyclic (linear) code iff $\pi(C)$ is an ideal of $\dfrac{\mathbb{Z}_2[x]}{(x^n-1)}$.

Proof of Proposition 1.29:

Suppose $\pi(C) = I$ is an ideal. Let $c, d \in C$, then $\pi(c), \pi(d) \in I \Rightarrow \pi(c+d) = \pi(c) + \pi(d) \in I \Rightarrow c + d \in C \Rightarrow C$ is a linear code. Now write $c = (c_0, \cdots, c_{n-1}) \in C$, then $\pi(c) = c_0 + \cdots + c_{n-1}\bar{x}^{n-1} \in I \Rightarrow c_{n-1} + c_0\bar{x} + \cdots + c_{n-1}\bar{x}^{n-1} = c_{n-1}\bar{x}^n + c_0\bar{x} + \cdots + c_{n-1}\bar{x}^{n-1} = \bar{x}\pi(c) \in I \Rightarrow (c_{n-1}, c_0, \cdots, c_{n-2}) \in C \Rightarrow C$ is a cyclic code.
Conversely, suppose C is a cyclic code, then $I = \pi(C)$ is a subgroup of $\dfrac{\mathbb{Z}_2[x]}{(x^n-1)}$ since C is linear and $0 = \pi(0^n) \in I$. Let $f(\bar{x}) = f_0 + \cdots + f_{n-1}\bar{x}^{n-1} \in I$, then $\pi^{-1}(f(\bar{x})) = (f_0, \cdots, f_{n-1}) \in C \Rightarrow (f_{n-1}, f_0, \cdots, f_{n-2}) \in C \Rightarrow \bar{x}f(\bar{x}) = f_0\bar{x} + \cdots + f_{n-1}\bar{x}^n = f_{n-1} + f_0\bar{x} + \cdots + f_{n-2}\bar{x}^{n-1} \in I$. Similarly, $\bar{x}^i f(\bar{x}) \in I \ \forall i \Rightarrow g(\bar{x})f(\bar{x}) \in I \ \forall g(\bar{x}) \in \dfrac{\mathbb{Z}_2[x]}{(x^n-1)} \Rightarrow I = \pi(C)$ is an ideal.

Basic construction of cyclic codes

Definition:

Fix $n \in \mathbb{N}$, let $p(x) \in \mathbb{Z}_2[x]$, $p(x) \mid x^n - 1$, I be the ideal of $\dfrac{\mathbb{Z}_2[x]}{(x^n-1)}$ defined by $I = (p(\bar{x})) = \left\{p(\bar{x})f(\bar{x}) : f(\bar{x}) \in \dfrac{\mathbb{Z}_2[x]}{(x^n-1)}\right\}$. Then $p(x)$ is called a generator polynomial for the cyclic code $C = \pi^{-1}(I) \subseteq \mathbb{Z}_2^n$.

Example:

(1) Let $n = 3$, $p(x) = x + 1$, then $p(x) \mid x^3 - 1 \Rightarrow I = (p(\bar{x})) = \left\{0, 1+\bar{x}, 1+\bar{x}^2, \bar{x}+\bar{x}^2\right\} \Rightarrow$ the corresponding cyclic code is $C = \{000, 110, 101, 011\}$.

(2) Let $n = 6$, then $x^6 - 1 = (x^3+1)^2 = (x+1)^2(x^2+x+1)^2$ in $\mathbb{Z}_2[x] \Rightarrow$ number of $p(x)$ dividing $x^6 - 1 =$ (number of choices for $(x+1)^i(x^2+x+1)^j$ where $0 \leq i, j \leq 2$) $= (2+1)(2+1) = 9$.

(3) From (2), let $p(x) = (x^2+x+1)^2 = x^4 + x^2 + 1$, then $C = \pi^{-1}\left((\bar{x}^4 + \bar{x}^2 + 1)\right) = \{000000, 101010, 010101, 111111\}$.

Proposition 1.30:

If $\deg p = n - k$, then $\dim C = k$.

Proof of Proposition 1.30:

It suffices to show that $S = \{p(\bar{x}), \cdots, \bar{x}^{k-1}p(\bar{x})\}$ is a basis for $(p(\bar{x})) = \pi(C)$ as a subspace of $\dfrac{\mathbb{Z}_2[x]}{(x^n-1)}$ over $\mathbb{Z}_2$. Suppose $f(\bar{x}) = \displaystyle\sum_{i=0}^{k-1} \lambda_i \bar{x}^i p(\bar{x}) = 0$ in $\dfrac{\mathbb{Z}_2[x]}{(x^n-1)}$ for some $\lambda_i \in \mathbb{Z}_2$, then $x^n - 1 \mid f(x) \Rightarrow f(x) = 0$ in $\mathbb{Z}_2[x]$ since $\deg f \leq (n-k) + (k-1) = n-1 \Rightarrow$ by comparing coefficients, $\lambda_i = 0\ \forall i \Rightarrow S$ is a linearly independent set.

Now pick $h(\bar{x}) \in (p(\bar{x}))$, then $h(\bar{x}) = g(\bar{x})p(\bar{x})$ for some $g(\bar{x}) \in \dfrac{\mathbb{Z}_2[x]}{(x^n-1)}$. Long division gives $g(x)p(x) = q(x)(x^n-1) + r(x)$ where $\deg r < n \Rightarrow p(x) \mid q(x)(x^n-1) + r(x) \Rightarrow p(x) \mid r(x)$. Let $r(x) = p(x)s(x)$, then $\deg s \leq n-(n-k) = k \Rightarrow$ since $g(x)p(x) = q(x)(x^n-1)+p(x)s(x)$, $h(\bar{x}) = g(\bar{x})p(\bar{x}) = 0 + p(\bar{x})s(\bar{x}) \Rightarrow h(\bar{x})$ is a linear combination of elements in $S \Rightarrow (p(\bar{x})) \subseteq \mathrm{Sp}(S) \Rightarrow S$ is a basis for $(p(\bar{x})) = \pi(C)$.

Example:

Let $n = 7$, then $x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$ in $\mathbb{Z}_2[x]$. Pick $p(x) = x^3 + x + 1$ and let C be its corresponding cyclic code, then $\dim C = 4$, and a basis of C is $\{1101000, 0110100, 0011010, 0001101\}$.

Check matrices for cyclic codes

Let $p(x) = p_0 + \cdots + p_{n-k}x^{n-k} \mid x^n - 1$ be the generator polynomial for a cyclic code C, and call $G = \begin{pmatrix} p_0 & \cdots & p_{n-k} & & 0 \\ & \ddots & & \ddots & \\ 0 & & p_0 & \cdots & p_{n-k} \end{pmatrix}$ (a $k \times n$ matrix) the generator matrix of C.

Proposition 1.31:

Let $q(x) = q_0 + \cdots + q_k x^k = \dfrac{x^n-1}{p(x)}$ in $\mathbb{Z}_2[x]$, and $H = \begin{pmatrix} 0 & & q_k & \cdots & q_0 \\ & \iddots & & \iddots & \\ q_k & \cdots & q_0 & & 0 \end{pmatrix}$ (a $(n-k) \times n$ matrix), then H is a check matrix for C.

Proof of Proposition 1.31:

Let $q(x)p(x) = \displaystyle\sum_{d=0}^{n} f_d x^d$, then $f_d = \sum q_i p_{d-i} = 0$ for $1 \leq d \leq n-1$ since $q(x)p(x) = x^n - 1 \Rightarrow HG^\top = \begin{pmatrix} 0 & & q_k & \cdots & q_0 \\ & \iddots & & \iddots & \\ q_k & \cdots & q_0 & & 0 \end{pmatrix} \begin{pmatrix} p_0 & & 0 \\ \vdots & \ddots & \\ p_{n-k} & & p_0 \\ & \ddots & \vdots \\ 0 & & p_{n-k} \end{pmatrix} = \begin{pmatrix} f_{n-1} & \cdots & f_{n-k} \\ \vdots & \ddots & \vdots \\ f_k & \cdots & f_1 \end{pmatrix} = 0$. Pick

$c \in C$, then c can be written as a linear combination of the rows of $G \Rightarrow Hc = \sum H(\text{some columns of } G^\top) = \sum 0 = 0 \Rightarrow H$ is a check matrix for C.

Example:

Let $n = 7$, then $x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$. Pick $p(x) = x^3+x+1$, then $G = \begin{pmatrix} 1&1&0&1&0&0&0 \\ 0&1&1&0&1&0&0 \\ 0&0&1&1&0&1&0 \\ 0&0&0&1&1&0&1 \end{pmatrix}$. Also, $q(x) = (x+1)(x^3+x^2+1) = x^4+x^2+x+1 \Rightarrow H = \begin{pmatrix} 0&0&1&0&1&1&1 \\ 0&1&0&1&1&1&0 \\ 1&0&1&1&1&0&0 \end{pmatrix}$ is a check matrix for the cyclic code C generated by $p(x) \Rightarrow C = \mathrm{Ham}(3)$.

BCH codes

It is usually hard to tell what $d(C)$ of a cyclic code C is, but some special cyclic codes allow $d(C)$ to be computed.

Definition:

A polynomial $f(x) \in \mathbb{Z}_2[x]$ with $\deg f \geq 1$ is irreducible if it cannot be factorized as a product of polynomials in $\mathbb{Z}_2[x]$ of smaller degree.

Example:

(1) $x, x+1$ are irreducible.

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

(3) The irreducible polynomials of degree 3 are x^3+x+1 and x^3+x^2+1.

(4) The irreducible polynomials of degree 4 are x^4+x+1 and x^4+x^3+1 (note that $x^4+x^2+1 = (x^2+x+1)^2$ is reducible).

Remark:

(1) Every polynomial in $\mathbb{Z}_2[x]$ is a unique product of irreducible polynomials (using the Euclidean algorithm for polynomials).

(2) For $k \geq 1$, $\exists$ a finite field $\mathbb{F}_{2^k} = \dfrac{\mathbb{Z}_2[x]}{(p_k(x))}$ of order 2^k, where $p_k(x) \in \mathbb{Z}_2[x]$ has degree k and is irreducible.

(3) The multiplicative group $\mathbb{F}_{2^k}^* = (\mathbb{F}_{2^k} \setminus \{0\}, \times)$ is cyclic. If $\mathbb{F}_{2^k}^* = \langle \beta \rangle$, then β is called a primitive element of $\mathbb{F}_{2^k}$.

(4) Every $\gamma \in \mathbb{F}_{2^k}$ has a minimum polynomial, which is the unique irreducible polynomial

$m(x) \in \mathbb{Z}_2[x]$ satisfying $m(\gamma) = 0$. Also, $\deg m \leq k$, and $m(x) \mid x^{2^k-1} - 1$.

Example:

(1) Let $I = \left(x^2 + x + 1\right)$, then $\mathbb{F}_4 = \dfrac{\mathbb{Z}_2[x]}{I} = \{0 + I, 1 + I, x + I, 1 + x + I\}$. Write $\alpha = x + I$, then $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$, with $\alpha^2 + \alpha + 1 = 0$.

(2) $\mathbb{F}_8 = \dfrac{\mathbb{Z}_2[x]}{(x^3 + x + 1)} = \left\{0, 1, \alpha, 1 + \alpha, \alpha^2, 1 + \alpha^2, \alpha + \alpha^2, 1 + \alpha + \alpha^2\right\}$, where $\alpha = x + I$, $\alpha^3 + \alpha + 1 = 0$.

(3) $\mathbb{F}_4^* = \langle \alpha \rangle = \langle 1 + \alpha \rangle$ has primitive elements α and $1 + \alpha$.

(4) $|\mathbb{F}_8^*| = 7 \Rightarrow$ all its elements (except 1) are primitive.

(5) Let $I = \left(x^4 + x + 1\right)$, $\mathbb{F}_{16} = \dfrac{\mathbb{Z}_2[x]}{I}$, $\alpha = x + I$, then $\alpha^4 + \alpha + 1 = 0$. Also, since $\operatorname{ord}(\alpha) \mid |\mathbb{F}_{16}^*| = 15$, $\alpha^3 \neq 1$ and $\alpha^5 = \alpha^2 + \alpha \neq 1$, $\operatorname{ord}(\alpha) = 15 \Rightarrow \mathbb{F}_{16}^* = \langle \alpha \rangle$.

(6) In $\mathbb{F}_8$, α and α^2 have minimum polynomial $x^3 + x + 1$ (note that $\alpha^6 + \alpha^2 + 1 = (\alpha^3 + \alpha + 1)^2 = 0$), and α^3 has minimum polynomial $x^3 + x^2 + 1$.

Definition:

Let $k, d \in \mathbb{Z}_{\geq 2}$, β be a primitive element of $\mathbb{F}_{2^k}$, $m_i(x)$ be the minimum polynomial of β^i, $p(x) = \operatorname{lcm}\{m_1(x), \cdots, m_{d-1}(x)\}$ and $n = 2^k - 1$, then $p(x) \mid x^n - 1$, and the cyclic code of length n generated by $p(x)$ is called the BCH code of length n and designed distance d.

Example:

(1) Let $k = 3, d = 3$. In $\mathbb{F}_8$, pick a primitive element α, then $m_1(x) = m_2(x) = x^3 + x + 1 \Rightarrow$ the BCH code is $\operatorname{Ham}(3)$.

(2) Let $d = 4$, then $m_3(x) = x^3 + x^2 + 1 \Rightarrow p(x) = (x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + \cdots + 1 \Rightarrow$ the BCH code is $\left\{0^7, 1^7\right\}$.

Theorem 1.32:

Let $n = 2^k - 1$, C be the BCH code of length n and designed distance d. Then:

(1) $d(C) \geq d$,

(2) $\dim C \geq n - \left\lfloor \dfrac{d}{2} \right\rfloor k$.

Proof of Theorem 1.32:

Too hard.

Remark:

$\deg p \leq (d-1)k \Rightarrow \dim C = n - \deg p \geq n - (d-1)k \Rightarrow$ the bound in Theorem 1.32 is much better than expected.

Example:

(1) Let $k = 4$, then $\exists$ a primitive element $\alpha \in \mathbb{F}_{16}$ with minimum polynomial $x^4 + x + 1 \Rightarrow m_1(x) = m_2(x) = m_4(x) = x^4 + x + 1$, and $m_3(x) \mid x^5 - 1$ since $\operatorname{ord}(\alpha^3) = 5 \Rightarrow m_3(x) = x^4 + x^3 + x^2 + x + 1$.

(2) Let $d = 3$, then $p(x) = \operatorname{lcm}\{m_1, m_2\} = x^4 + x + 1$ from (1) $\Rightarrow$ the BCH code C has dimension $15 - \deg p = 11$ and $d(C) \geq d = 3$.

(3) Let $d = 5$, then $p(x) = \operatorname{lcm}\{m_1, m_2, m_3, m_4\} = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$ from (1) $\Rightarrow$ the BCH code C has dimension $15 - \deg p = 7$ and $d(C) \geq d = 5$.

Remark:

Since $1 + \binom{14}{1} + \binom{14}{2} + \binom{14}{3} = 1 + 14 + 91 + 364 = 470 \geq 2^{15-7}$, the GV bound cannot prove that $\exists$ a linear code of length 15 and dimension 7 which corrects 2 errors $\Rightarrow$ BCH beats GV.

2 Strongly Regular Graphs

Definition:

(1) A graph $\Gamma = (V, E)$ is a set of vertices V and a set of edges E.

(2) Γ is regular with valency k if every vertex has k neighbours.

(3) A path in Γ of length r is a sequence of vertices $v_0, \cdots, v_r$ where v_i is joined to v_{i+1} $\forall i$.

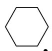
(4) Γ is connected if $\exists$ a path from v to w $\forall v, w \in V$.

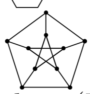
(5) If Γ is connected, the distance between v and w is $d(v, w) =$ length of shortest path from v to w, and the diameter of Γ is $\mathrm{diam}(\Gamma) = \max\{d(v, w) : v, w \in V\}$.

(6) 2 graphs (V, E) and (V', E') are isomorphic if $\exists$ a bijection $V \to V'$ which sends E to E'.

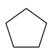
Example:

(1)  is a disconnected graph.

(2)  is connected, with regular valency 2 and diameter 3.

(3)  is the Petersen graph, connected with regular valency 3 and diameter 2.

(4) $\mathrm{diam}(\Gamma) = 1 \Rightarrow$ any 2 vertices are joined by an edge. Such a graph with v vertices is called the complete graph K_v.

(5)  $\cong$ .

Proposition 2.1:

Suppose Γ is a connected graph that is regular with valency k and diameter d. Then $|V(\Gamma)| \leq N(k, d) = 1 + \sum_{i=1}^{d} k(k-1)^{i-1}$.

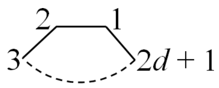
Proof of Proposition 2.1:

Pick $x \in V(\Gamma)$. For $i \geq 1$, let $D_i = \{y \in V(\Gamma) : d(x, y) = i\}$, then $|D_1| = k \Rightarrow |D_2| \leq (k-1)|D_1| = k(k-1) \Rightarrow |D_3| \leq (k-1)|D_2| = k(k-1)^2 \Rightarrow \cdots \Rightarrow$ since $\mathrm{diam}(\Gamma) = d$, $V(\Gamma) = \{x\} \cup D_1 \cup \cdots \cup D_d \Rightarrow |V(\Gamma)| = 1 + \sum_{i=1}^{d} |D_i| \leq 1 + \sum_{i=1}^{d} k(k-1)^{i-1}$.

Definition:

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

Example:

(1) Let $k = 2$, then $|V(\Gamma)| = 1 + \sum_{i=1}^{d} 2 = 2d + 1$. Indeed, 

is a Moore graph.

(2) Let $k = 3$, $d = 2$, then $|V(\Gamma)| = 1 + 3 + 6 = 10$. The Petersen graph is such a graph, and is the only such Moore graph up to isomorphism.

(3) Let $d = 2$, then $|V(\Gamma)| = 1 + k + k(k-1) = k^2 + 1$, and there are no $\triangle$s nor $\square$s in Γ. Let $k = 4$, and pick 2 joined vertices $v, w \in V(\Gamma)$, with neighbours a, b, c and x, y, z respectively. Since $\operatorname{diam}(\Gamma) = 2$, a and x must have a common neighbour (a, x) which is a new vertex. Similarly, there are new vertices $(a, y), \cdots, (c, z)$. Also, there are 2 neighbours of (a, x) among the 9 new vertices that are not of the form $(a, ?)$ nor $(?, x)$ (else there will be a $\triangle$), so the possibilities are $(b, y), (b, z), (c, y), (c, z)$. WLOG, if (a, x) and (b, y) are joined, then (a, x) cannot be joined to (b, z) nor (c, y) (else there will be a $\square$) $\Rightarrow$ (a, x) and (c, z) are joined. Similarly, (b, y) is joined to (a, x) and (c, z), and (c, z) is joined to (a, x) and (b, y) ($\Rightarrow\Leftarrow$ since there is a $\triangle$) $\Rightarrow \nexists \Gamma$.

Definition:

A graph Γ is strongly regular with parameters (v, k, a, b) if:

(1) Γ has v vertices,

(2) Γ is regular with valency k,

(3) any 2 joined vertices of Γ have a common neighbours,

(4) any 2 non-joined vertices of Γ have b common neighbours.

Proposition 2.2:

If Γ is strongly regular with parameters (v, k, a, b), then:

(1) Γ is connected and $\operatorname{diam}(\Gamma) = 2$ if $b > 0$,

(2) Γ is a disjoint union of complete graphs K_{k+1} if $b = 0$.

Proof of Proposition 2.2:

(1) If $b > 0$, then $\exists$ a path of length 2 between any 2 non-joined vertices of $\Gamma \Rightarrow \operatorname{diam}(\Gamma) = 2$.

(2) If $b = 0$, let the neighbours of a vertex $x \in V(\Gamma)$ be $x_1, \cdots, x_k$, then x_i, x_j are joined $\forall i \neq j$ (else $b > 0$) $\Rightarrow x, x_1, \cdots, x_k$ form a complete graph K_{k+1}. Any other vertex $y \in V(\Gamma)$ is not joined to $x \Rightarrow y$ is not joined to $x_1, \cdots, x_k$ too $\Rightarrow y$ and its neighbours for another K_{k+1}.

Example:

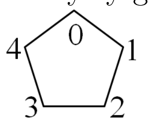
(1) Moore graphs of diameter 2 are strongly regular, with parameters $(k^2 + 1, k, 0, 1)$, since

there are no $\triangle$s and $\square$s.

(2) For $n \geq 4$, let the $\binom{n}{2}$ pairs from $\{1, \cdots, n\}$ be vertices of Γ, and join $\{i, j\}$, $\{k, l\}$ iff $|\{i, j\} \cap \{k, l\}| = 1$. Then Γ is strongly regular with parameters $v = \binom{n}{2}$, $k = 2n - 4$, $a = n - 2$, $b = 4$, called the triangular graph $T(n)$.

(3) Let the ordered pairs (i, j) (where $i, j \in \{1, \cdots, n\}$) be vertices of Γ, and join (i, j), (k, l) iff $i = k$ or $j = l$. Then Γ is strongly regular with parameters $v = n^2$, $k = 2n - 2$, $a = n - 2$, $b = 2$, called the lattice graph $L(n)$.

(4) Let $p > 2$, $p \equiv 1 \pmod 4$ be a prime, such that $\mathbb{Z}_p = \{0, \cdots, p-1\}$ (with addition and multiplication mod p) is a field. Let $Q = \left\{x^2 : x \in \mathbb{Z}_p^*\right\}$, $\psi : \mathbb{Z}_p^* \to Q$, $x \mapsto x^2$, then ψ is a homomorphism with $\operatorname{Ker} \psi = \left\{x : x^2 = 1\right\} = \{x : (x+1)(x-1) = 0\} = \{\pm 1\} \Rightarrow |Q| = |\operatorname{Im} \psi| = \dfrac{|\mathbb{Z}_p^*|}{|\operatorname{Ker} \psi|} = \dfrac{p-1}{2} \equiv 0 \pmod 2 \Rightarrow -1 \in Q$, since Q must contain an element of order 2. Let $V(\Gamma) = \mathbb{Z}_p$, and join x, y iff $x - y \in Q$ (iff $y - x \in Q$), then Γ is called the Payley graph $P(p)$.

(5) $P(5)$ is 

.

Proposition 2.3:

$P(p)$ is strongly regular, with parameters $v = p$, $k = \dfrac{p-1}{2}$, $a = \dfrac{p-5}{4}$, $b = \dfrac{p-1}{4}$.

Proof of Proposition 2.3:

Clearly $k = |Q| = \dfrac{p-1}{2}$. Now pick $x, y \in V(P(p))$ where $x \neq y$, and we aim to find the number of $z \in V(P(p))$ such that $(x, z), (y, z) \in E(P(p))$ ie. $z - x = n^2 \pmod p$, $z - y = m^2 \pmod p \Rightarrow x - y = m^2 - n^2 = (m+n)(m-n) \pmod p$. Since $\mathbb{Z}_p$ is a field, number of distinct solutions $(m+n, m-n) \in \mathbb{Z}_p^2 =$ (number of distinct divisors of q) $= p - 1 \Rightarrow$ number of distinct solutions $(m, n) \in \mathbb{Z}_p^2 = p - 1$. But $x - y \in Q \Rightarrow (\pm m, 0), (0, \pm n)$ should be excluded (else $z = x$ or $z = y$). Also, note that $(c, d), (m, n)$ give the same value of $z \Leftrightarrow c^2 - m^2 \equiv (c+m)(c-m) \equiv d^2 - n^2 \equiv (d+n)(d-n) \equiv 0 \pmod p \Leftrightarrow c = \pm m, d = \pm n$. Hence x, y have $\dfrac{(p-1)-4}{2^2} = \dfrac{p-5}{4}$ common neighbours z if they are joined, $\dfrac{p-1}{2^2} = \dfrac{p-1}{4}$ common neighbours otherwise $\Rightarrow P(p)$ is strongly regular, with $a = \dfrac{p-5}{4}$, $b = \dfrac{p-1}{4}$.

Proposition 2.4:

If Γ is strongly regular with parameters (v, k, a, b), then $k(k - a - 1) = b(v - k - 1)$.

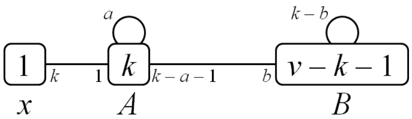
Proof of Proposition 2.4:

Pick $x \in V(\Gamma)$, and let A be the set of k neighbours of x, B be the set of $v - k - 1$ non-neighbours of x, N be the number of edges joining a vertex in A to a vertex in B. Each vertex in A is joined to $k-a-1$ vertices in B, and each vertex in B is joined to b vertices in $A \Rightarrow (k-a-1)\,|A| = N = b\,|B| \Rightarrow k(k-a-1) = b(v-k-1)$.

Example:

Moore graphs of diameter 2 are strongly regular, with parameters $(v,k,0,1) \Rightarrow k(k-1) = v-k-1 \Rightarrow v = k^2+1$ indeed.

Remark:

We can draw the "balloon" picture 

if Γ is strongly regular.

Definition:

Replace all edges of Γ with non-edges and vice-versa but keep the same vertex set, then the new graph obtained is Γ^c, called the complement of Γ.

Proposition 2.5:

If Γ is strongly regular with parameters (v,k,a,b), then Γ^c is also strongly regular, with parameters $(v, v-k-1, v-2k+b-2, v-2k+a)$.

Proof of Proposition 2.5:

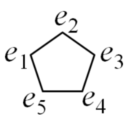
Pick $x \in \Gamma^c$, and let B be the set of neighbours of x in Γ^c (ie. the set of non-neighbours of x in Γ), A be the set of non-neighbours of x in Γ^c (ie. the set of neighbours of x in Γ), then clearly $|B| = v-k-1$. Also, in Γ, any vertex $v \in A$ is joined to $k-a-1$ vertices in $B \Rightarrow$ in Γ^c, v is joined to $|B|-(k-a-1) = v-k-1-k+a+1 = v-2k+a$ vertices in B. Moreover, in Γ, any vertex $w \in B$ is joined to $k-b$ other vertices in $B \Rightarrow$ in Γ^c, w is joined to $|B|-(k-b)-1 = v-k-1-k+b-1 = v-2k+b-2$ vertices in B. Hence Γ^c is strongly regular, with parameters $(v, v-k-1, v-2k+b-2, v-2k+a)$.

Adjacency matrices

Definition:

Let Γ be a graph with vertex set $\{e_1, \cdots, e_v\}$. The adjacency matrix of Γ is the $v \times v$ matrix $A = (a_{ij})$, with $a_{ij} = 1$ if e_i is joined to e_j, 0 otherwise.

Example:

The adjacency matrix for 

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

Remark:

(1) A is symmetric, with all entries 0 or 1.

(2) A has 0's on its main diagonal.

Proposition 2.6:

Let Γ be a strongly regular graph with parameters (v, k, a, b), A be its adjacency matrix, and J be the $v \times v$ matrix consisting of all 1's. Then:

(1) $AJ = kJ$,

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

Proof of Proposition 2.6:

(1) Γ is regular with valency $k \Rightarrow$ each row of A has exactly k 1's $\Rightarrow AJ = kJ$.

(2) Since A is symmetric, $(A^2)_{ij} = (AA^\top)_{ij} =$ (row i of A) $\cdot$ (column j of $A^\top$) $=$ (row i of A) $\cdot$ (row j of A) $= k$ if $i = j$, a if $i \neq j$ and e_i, e_j are joined, b otherwise $\Rightarrow$ A^2 has k's on its main diagonal, a's where A has 1's, and b's where A has 0's $\Rightarrow A^2 = kI + aA + b(J - A - I) = (a-b)A + (k-b)I + bJ$.

Eigenvalues of adjacency matrices

The adjacency matrix A of a graph Γ is real and symmetric, so it has real eigenvalues and is diagonalizable.

Definition:

The multiplicity of an eigenvalue λ is the number of times it appears in $\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_v \end{pmatrix} =$ $P^{-1}AP$ for some P.

Lemma 2.7:

Let A be a real $v \times v$ matrix with eigenvalues $\lambda_1, \cdots, \lambda_v$, then $\mathrm{Trace}(A) = \sum_{i=1}^{v} \lambda_i$.

Proof of Lemma 2.7:

$\lambda_1, \cdots, \lambda_v$ are the roots of $\det(xI - A) = (x - a_{11}) \cdots (x - a_{vv}) + (\text{terms of degree} \leq v - 2) = x^v - (a_{11} + \cdots + a_{vv})x^{v-1} + \cdots$. Since $\det(xI - A)$ is also $= (x - \lambda_1) \cdots (x - \lambda_v)$, comparing coefficients of x^{v-1} gives $\sum_{i=1}^{v} \lambda_i = \sum_{i=1}^{v} a_{ii} = \text{Trace}(A)$.

Theorem 2.8:

Let Γ be a strongly regular graph with parameters (v, k, a, b) and adjacency matrix A. Assume WLOG that $v > 2k$ (else pick Γ^c), and suppose Γ is connected (ie. $b > 0$). Then:

(1) A has exactly 3 distinct eigenvalues k, r_1, r_2, where r_1, r_2 satisfy $x^2 - (a-b)x - (k-b) = 0$,

(2) eigenvalue k has multiplicity 1, and if m_1, m_2 are the multiplicities of r_1, r_2 respectively, then $m_1 + m_2 = v - 1$ and $m_1 r_1 + m_2 r_2 = -k$,

(3) $r_1, r_2 \in \mathbb{Z}$ unless (v, k, a, b) has the form $(4b + 1, 2b, b - 1, b)$.

Proof of Theorem 2.8:

By Proposition 2.6(1), $AJ = kJ \Rightarrow$ let $\mathbf{j} = \begin{pmatrix} 1 & \cdots & 1 \end{pmatrix}^\top$, then $A\mathbf{j} = k\mathbf{j} \Rightarrow k$ is an eigenvalue of A.

Now let $\mathbf{w}$ be an eigenvector of A with $\mathbf{w} \notin \text{Sp}(\mathbf{j})$ such that $A\mathbf{w} = \lambda\mathbf{w}$, then by Proposition 2.6(2), $A^2\mathbf{w} = (a-b)A\mathbf{w} + (k-b)I\mathbf{w} + bJ\mathbf{w} \Rightarrow \lambda^2\mathbf{w} = (a-b)\lambda\mathbf{w} + (k-b)\mathbf{w} + b(c\mathbf{j})$ (where c = sum of coordinates of $\mathbf{w}$) $\Rightarrow (\lambda^2 - (a-b)\lambda - (k-b))\mathbf{w} = bc\mathbf{j} \in \text{Sp}(\mathbf{j}) \Rightarrow$ since $\mathbf{w} \notin \text{Sp}(\mathbf{j})$, $\lambda^2 - (a-b)\lambda - (k-b) = 0$ ie. λ satisfies $x^2 - (a-b)x - (k-b) = 0$.

Let the roots of $x^2 - (a-b)x - (k-b) = 0$ be r_1 and r_2, and suppose $k = r_1$ or $r_2 \Rightarrow k^2 - (a-b)k - (k-b) = 0$. But by Proposition 2.4, $k(k-a-1) = b(v-k-1) \Rightarrow k^2 - (a-b)k - (k-b) = bv \Rightarrow bv = 0 \Rightarrow b = 0$ $(\Rightarrow\Leftarrow) \Rightarrow k \neq r_1, r_2 \Rightarrow$ the eigenspace for k is $\text{Sp}(\mathbf{j}) \Rightarrow k$ has multiplicity 1. Moreover, if $r_1 = r_2$, then $(a-b)^2 + 4(k-b) = 0 \Rightarrow$ since $k \geq b$, we must have $(a-b)^2 = 4(k-b) = 0 \Rightarrow a = b = k$ ($\Rightarrow\Leftarrow$ as $k - 1 \geq a$) $\Rightarrow r_1 \neq r_2$. Hence k, r_1, r_2 are all distinct.

Let the multiplicities of r_1 and r_2 be m_1 and m_2 respectively, then $m_1 + m_2 = v - 1$ since A is a $v \times v$ matrix, and $m_1 r_1 + m_2 r_2 + k = \text{Trace}(A) = 0 \Rightarrow m_1 r_1 + m_2 r_2 = -k$.

Now let $D = (a-b)^2 + 4(k-b)$, then $r_1, r_2 = \frac{1}{2}((a-b) \pm \sqrt{D}) \Rightarrow 2(m_1 r_1 + m_2 r_2) = (m_1 + m_2)(a-b) + (m_1 - m_2)\sqrt{D} = -2k \Rightarrow$ if $m_1 \neq m_2$, then $\sqrt{D} \in \mathbb{Q} \Rightarrow \sqrt{D} \in \mathbb{Z} \Rightarrow r_1, r_2$ are either both $\in \mathbb{Z}$ or both of the form $z + \frac{1}{2}$ for some $z \in \mathbb{Z}$. If the latter is true, then $r_1 r_2 = -(k-b) \notin \mathbb{Z}$ $(\Rightarrow\Leftarrow) \Rightarrow r_1, r_2 \in \mathbb{Z}$. In particular, if $m_2 = 0$, then $m_1 = v - 1$ and $m_1 r_1 = -k \Rightarrow v - 1 \mid k \Rightarrow v - 1 \leq k$ ($\Rightarrow\Leftarrow$ since $v > 2k$) $\Rightarrow m_1, m_2 > 0 \Rightarrow A$ has exactly 3 eigenvalues.

Otherwise, if $m_1 = m_2 = m$, then $2m = v - 1$ and $2m(a-b) = -2k \Rightarrow (v-1)(a-b) = -2k \Rightarrow v - 1 \leq 2k$. Since $v > 2k$ by assumption, we must have $v = 2k+1 \Rightarrow a - b = -1 \Rightarrow$ by Proposition 2.4, $k(k-a-1) = b(v-k-1) = bk \Rightarrow b = k-a-1 = k-b \Rightarrow k = 2b \Rightarrow (v,k,a,b) = (4b+1, 2b, b-1, b)$.

Remark:

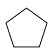
If $v \leq 2k$, then Γ^c is strongly regular, and $v' = v > v + (v - 2k - 2) = 2(v-k-1) = 2k' \Rightarrow$ Theorem 2.8 applies to Γ^c if it is connected. Otherwise, Γ^c is a disjoint union of complete graphs $\Rightarrow$ we know what Γ^c is.

Theorem 2.9:

If $\exists$ a Moore graph of valency k and diameter 2, then k = 2, 3, 7 or 57.

Proof of Theorem 2.9:

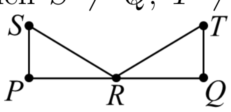
Let Γ be such a Moore graph, then Γ is strongly regular with parameters $(k^2+1, k, 0, 1)$. Let A be the adjacency matrix of Γ, then since $b > 0$ and $k^2 + 1 > 2k$ for $k > 1$, by Theorem 2.8(1), A has 3 eigenvalues k, r_1, r_2 where r_1, r_2 are the roots of $x^2 + x - (k-1) = 0 \Rightarrow r_1, r_2 = \frac{1}{2}(-1 \pm \sqrt{4k-3})$. Also, by Theorem 2.8(2), the multiplicities of r_1, r_2 satisfy $m_1 + m_2 = k^2$ and $m_1 r_1 + m_2 r_2 = -k \Rightarrow \frac{1}{2}(-m_1 - m_2) + \frac{1}{2}(m_1 - m_2)\sqrt{4k-3} = -k \Rightarrow (m_1 - m_2)\sqrt{4k-3} = k^2 - 2k$.

If $k = 2b = 2$, then $\Gamma =$  . Otherwise, if $k > 2$, $r_1, r_2 \in \mathbb{Z} \Rightarrow \sqrt{4k-3} \in \mathbb{Z}$ by Theorem 2.8(3). Let $n = \sqrt{4k-3}$, then $k = \frac{n^2+3}{4} \Rightarrow n(m_1 - m_2) = k(k-2) = \frac{n^2+3}{4} \times \frac{n^2-5}{4} \Rightarrow m_1 - m_2 = \frac{(n^2+3)(n^2-5)}{16n} \in \mathbb{Z} \Rightarrow n \mid (n^2+3)(n^2-5) \Rightarrow n \mid 15 \Rightarrow n$ = 1, 3, 5 or 15 $\Rightarrow k$ = 1 ($\Rightarrow\Leftarrow$), 3, 7 or 57. Hence k = 2, 3, 7 or 57.

Theorem 2.10 (Friendship Theorem):

If Γ is a graph in which any 2 vertices have exactly 1 common neighbour, then $\exists$ a vertex that is joined to all the other vertices.

Proof of Theorem 2.10:

Such $\exists$ such a Γ but no vertex is joined to all the other vertices. Let $v(P)$ be the number of neighbours of P, and R be the common neighbour of P and Q, where P and Q are not joined. Let S be the common neighbour of P and R, and T be the common neighbour of Q and R, then $S \neq Q$, $T \neq P$ and $S \neq T$ (else P and Q have 2 common neighbours) ie. we have 

. Let the remaining neighbours of P be $u_1, \cdots, u_r$, then the common neighbour of u_1 and Q cannot be T (else P and T have 2 common neighbours) nor R (else P and R have 2 common neighbours) $\Rightarrow$ it is a new vertex v_1. Similarly, the common neighbour of u_2 and Q cannot be T, R nor v_1 (else P and v_1 have 2 common neighbours) $\Rightarrow$ it is a new vertex $v_2 \Rightarrow$ repeating $\forall u_i$ gives $v(P) = r + 2 \leq v(Q)$. Likewise, $v(Q) \leq v(P) \Rightarrow v(P) = v(Q) \Rightarrow$ any 2 non-joined vertices have the same number of neighbours.

Now let B be a vertex that is not P, Q nor R, then $v(B) = v(P) = v(Q)$ since B is not joined to either P or Q (or both). Also, by assumption, let C be a vertex that is not joined to R, then $v(Q) = v(C) = v(R)$ too $\Rightarrow$ every vertex has the same number of neighbours as $Q \Rightarrow \Gamma$ is regular $\Rightarrow \Gamma$ is strongly regular with parameters $(v, k, 1, 1)$.

By Proposition 2.4, $k(k-2) = v-k-1 \Rightarrow v = k^2 - k + 1 \Rightarrow v > 2k$ iff $k \geq 3$. If $k = 2$, then $\Gamma = \triangle$ $(\Rightarrow\Leftarrow) \Rightarrow v > 2k \Rightarrow$ let A be the adjacency matrix of Γ, then by Theorem 2.8(1), A has 3 eigenvalues k, r_1, r_2 where r_1, r_2 are the roots of $x^2 - (k-1) = 0 \Rightarrow r_1 = \sqrt{k-1}$, $r_2 = -\sqrt{k-1}$. Also, by Theorem 2.8(2), $m_1 + m_2 = v - 1 = k^2 - k$ and $m_1 r_1 + m_2 r_2 = -k \Rightarrow (m_1 - m_2)\sqrt{k-1} = -k \Rightarrow (m_1 - m_2)^2(k-1) = k^2 \Rightarrow k - 1 \mid k^2 \Rightarrow k - 1 \mid 1 \Rightarrow k = 0$ or 2 $(\Rightarrow\Leftarrow) \Rightarrow \nexists\Gamma$.

Strongly regular graphs with small v

Example:

(1) $T(6)$ has parameters $(15, 8, 4, 4)$.

(2) $T(6)^c$ has parameters $(15, 6, 1, 3)$.

(3) $(K_3)^5$ has parameters $(15, 2, 1, 0)$, and $(K_5)^3$ has parameters $(15, 4, 3, 0)$.

(4) $\left[(K_3)^5\right]^c$ has parameters $(15, 12, 9, 12)$, and $\left[(K_5)^3\right]^c$ has parameters $(15, 10, 5, 10)$.

Proposition 2.11:

If Γ is strongly regular with $v = 15$, then $\Gamma = T(6), (K_3)^5, (K_5)^3$ or their complements.

Proof of Proposition 2.11:

Let Γ have parameters $(15, k, a, b)$. If $15 \leq 2k$, replace Γ by $\Gamma^c \Rightarrow$ assume WLOG that $15 > 2k$. If $b = 0$, then $\Gamma = (K_3)^5$ or $(K_5)^3$ by Proposition 2.2. If $b > 0$, then $2 \leq k \leq 7$.

If $k = 2$, then Γ is a 15-gon ($\Rightarrow\Leftarrow$ since Γ is not strongly regular).

If $k = 3$, by Proposition 2.4, $3(2-a) = 11b \Rightarrow 11 \mid 2 - a \Rightarrow a = 2 \Rightarrow b = 0$ $(\Rightarrow\Leftarrow)$.

If $k = 4$, by Proposition 2.4, $4(3-a) = 10b \Rightarrow 5 \mid 3 - a \Rightarrow a = 3 \Rightarrow b = 0$ $(\Rightarrow\Leftarrow)$.

If $k=5$, by Proposition 2.4, $5(4-a)=9b \Rightarrow 9 \mid 4-a \Rightarrow a=4 \Rightarrow b=0$ ($\Rightarrow\Leftarrow$).

If $k=6$, by Proposition 2.4, $6(5-a)=8b \Rightarrow 8 \mid 5-a \Rightarrow a=1 \Rightarrow b=3 \Rightarrow \Gamma = T(6)^c$.

If $k=7$, by Proposition 2.4, $7(6-a)=7b \Rightarrow b=6-a$. Also, by Theorem 2.8, the eigenvalues of the adjacency matrix of Γ are $7, r_1, r_2$ where r_1, r_2 are the roots of $x^2-(a-b)x-(k-b) = x^2-(2a-6)x-(1+a)=0 \Rightarrow r_1, r_2 = a-3 \pm \sqrt{(a-3)^2+(1+a)} = a-3 \pm \sqrt{a^2-5a+10}$. Since $r_1, r_2 \in \mathbb{Z}$, $a^2-5a+10$ is a perfect square, and $0 \le a \le k-1 = 5 \Rightarrow a=2$ or 3. If $a=2$, then $r_1=1$, $r_2=-3 \Rightarrow m_1+m_2=14$ and $m_1-3m_2=-7 \Rightarrow 4m_2=21$ ($\Rightarrow\Leftarrow$). If $a=3$, then $r_1=2$, $r_2=-2 \Rightarrow m_1+m_2=14$ and $2m_1-2m_2=-7 \Rightarrow 4m_1=21$ ($\Rightarrow\Leftarrow$).

Hence $\Gamma = T(6)^c, (K_3)^5$ or $(K_5)^3 \Rightarrow \Gamma = T(6), (K_3)^5, (K_5)^3$ or their complements.

2-weight codes & strongly regular graphs

Definition:

A linear code $C \subseteq \mathbb{Z}_2^n$ is a 2-weight code if $\exists w_1, w_2 > 0$, $w_1 \neq w_2$, such that $\mathrm{wt}(c) = w_1$ or w_2 $\forall c \in C \setminus \{0\}$, and both occur.

Example:

(1) $H' \subseteq \mathbb{Z}_2^8$ has weights 0, 4 or 8 $\Rightarrow$ it is a 2-weight code.

(2) $C = \left\{v \in \mathbb{Z}_2^5 : \mathrm{wt}(v) \text{ even}\right\}$ is a 2-weight code.

(3) $C = \{c \in G_{24} : c_{16} = \cdots = c_{24} = 0\}$ has weights 0, 8 or 12 $\Rightarrow C$ is a 2-weight code.

Definition:

A linear code is projective if it has a generator matrix whose columns are distinct and non-zero.

Example:

H' is projective, with generator matrix $\begin{pmatrix} 1&1&1&1&1&1&1&1 \\ 0&1&1&1&0&0&0&1 \\ 0&1&0&0&1&1&0&1 \\ 0&0&1&0&1&0&1&1 \end{pmatrix}$.

Theorem 2.12:

Let $C \subseteq \mathbb{Z}_2^n$ be a projective 2-weight linear code, with weights $w_1, w_2 > 0$, $w_1 \neq w_2$. Define Γ with $V(\Gamma) = C$, and join a, b iff $d(a,b) = \mathrm{wt}(a+b) = w_1$, then Γ is strongly regular.

Proof of Theorem 2.12:

Let $\dim C = k$ and b_i be the number of codewords of weight w_i for $i = 1, 2$, then clearly Γ

is regular with valency b_1. Define A_i to be the $b_i \times n$ matrix whose rows are the codewords with weight w_i, $A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$, and $\phi_t : C \to \mathbb{Z}_2$ by $\phi_t(x_1, \cdots, x_n) = x_t$. Since every column of A has a non-zero element, ϕ_t is surjective $\Rightarrow \dim \operatorname{Ker} \phi_t = k - 1 \Rightarrow$ each column of A has $2^{k-1} - 1$ 0's and 2^{k-1} 1's $\Rightarrow$ number of 1's in $A = n \times 2^{k-1} = b_1 w_1 + b_2 w_2 \Rightarrow$ we can solve for b_i as $b_1 + b_2 = 2^k - 1$.

For any fixed j, let r_i be the number of 0's in column j of A_i. Since codewords $c \in C$ with $c_j = 0$ form a 2-weight projective subcode of C, we can calculate r_i in the same way we did for b_i (ie. $r_1 + r_2 = 2^{k-1} - 1$ and $r_1 w_1 + r_2 w_2 = (n-1) \times 2^{k-2}$) $\Rightarrow$ every column of A_i has r_i 0's. Let A_1 have rows $a_1, \cdots, a_{b_1}$, $s_p =$ number of a_m such that $d(a_j, a_m) = w_p$, then $s_1 + s_2 = b_1 - 1$ and $s_1 w_1 + s_2 w_2 = \sum_{m=1}^{b_1} d(a_j, a_m) = w_1 r_1 + (n - w_1)(b_1 - r_1) \Rightarrow$ we can solve for s_p.

It follows that a_j and 0^n are joined and have s_1 common neighbours $\forall j$. Moreover, for any edge (x, y) with $\mathrm{wt}(x + y) = w_1$, z is a common neighbour of x and y iff $x + z$ is a common neighbour of 0^n and $x+y \Rightarrow$ any pair of joined vertices have s_1 common neighbours. Likewise for A_2, any pair of non-joined vertices has a constant number of common neighbours $\Rightarrow \Gamma$ is strongly regular.

Example:

Let $C = H'$, $w_1 = 8$, $w_2 = 4$, and join $a, b \in \Gamma^c$ iff $d(a, b) = 8$ ie. $a = b + 1^8$, then Γ^c has valency 1, and in fact $\Gamma^c = (K_2)^8 \Rightarrow \Gamma$ is also strongly regular.

3 Designs

Definition:

Let X be a set of v points, then a t-design with parameters (v,k,r_t) is a collection $\mathcal{B}$ of subsets of X, all of which have size k (called blocks), such that any t points of X lie in r_t blocks.

Remark:

$\mathcal{B}$ is trivial if every set of size k is a block.

Example:

(1) Octads in G_{24} form a 5-design with parameters $(24,8,1)$.

(2) Let $X = \mathbb{Z}_2^n \setminus \{0\}$ with blocks $\{x,y,x+y\}$, then $\mathcal{B}$ is a 2-design with parameters $(2^k-1,3,1)$.

Proposition 3.1:

A t-design is also an s-design $\forall 1 \leq s \leq t$, and $r_s = \dfrac{(v-t+1)\cdots(v-s)}{(k-t+1)\cdots(k-s)} r_t$.

Proof of Proposition 3.1:

Follows from Corollary 1.24.

Notation:

Write $r = r_1$, $b = r_0 =$ number of blocks, then $bk = vr$ by Proposition 3.1.

Example:

(1) $\nexists$ a 2-design with parameters $(56,11,1)$ since $r = r_1 = \dfrac{56-2+1}{11-2+1} \times 1 = \dfrac{55}{10} \notin \mathbb{Z}$.

(2) Consider a 2-design with parameters $(46,10,1)$, then $r = \dfrac{45}{9} = 5 \Rightarrow b = \dfrac{vr}{k} = \dfrac{46 \times 5}{10} = 23 \Rightarrow$ we do not know if it exists.

Some theory of 2-designs

Notation:

Write $r_2 = \lambda$, such that the parameters of a 2-design become (v,k,λ).

Proposition 3.2:

For a 2-design, $r(k-1) = \lambda(v-1)$.

Proof of Proposition 3.2:

Consider pairs (ij, B) where $B \in \mathcal{B}$, $i, j \in B$, $i \neq j$, then the number of such pairs is = ways to choose $i, j \in X$ × ways to choose B containing $i, j = \binom{v}{2}\lambda$.
On the other hand, this number is also = ways to choose $B \in \mathcal{B}$ × ways to choose $i, j \in B = b\binom{k}{2}$ ⇒ by Proposition 3.1, $\frac{\lambda v(v-1)}{2} = \frac{bk(k-1)}{2} = \frac{vr(k-1)}{2} \Rightarrow \lambda(v-1) = r(k-1)$.

Incidence matrices

Definition:

Let $\mathcal{B}$ be a t-design ($t \geq 1$) with points $x_1, \cdots, x_v$ and blocks $B_1, \cdots, B_b$, then the incidence matrix of $\mathcal{B}$ is the $v \times b$ matrix $A = (a_{ij})$, with $a_{ij} = 1$ if $x_i \in B_j$, 0 otherwise.

Remark:

Each row of A has r 1's, and each column of A has k 1's.

Proposition 3.3:

Let $\mathcal{B}$ be a 2-design with parameters (v, k, λ) and incidence matrix A, then $AA^\top$ (a $v \times v$ matrix) $= \lambda J_v + (r - \lambda)I_v$.

Proof of Proposition 3.3:

$(AA^\top)_{ij}$ = (row i of A) · (row j of A) = (number of blocks containing both i and j) = λ if $i \neq j$, r otherwise ⇒ the result follows.

Proposition 3.4:

Let A be the incidence matrix of a 2-design with parameters (v, k, λ), then $\det AA^\top = (r-\lambda)^{v-1}(r + (v-1)\lambda)$.

Proof of Proposition 3.4:

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

Theorem 3.5 (Fisher's Inequality):

Let $\mathcal{B}$ a 2-design with parameters (v, k, λ), with $v > k$, then $b \geq v$ (and $r \geq k$).

Proof of Theorem 3.5:

By Proposition 3.2, $v > k \Rightarrow r > \lambda$. Let A be the incidence matrix of $\mathcal{B}$, then by Proposition 3.4, $\det AA^\top > 0 \Rightarrow AA^\top$ is invertible $\Rightarrow v = \operatorname{rank} AA^\top \leq \operatorname{rank} A \leq b$.

Example:

From the previous example, a 2-design with parameters $(46, 10, 1)$ must have $b = 23 < v$ $(\Rightarrow\Leftarrow) \Rightarrow$ no such design exists.

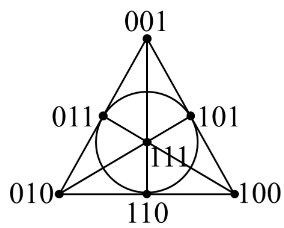
Symmetric 2-designs

Definition:

A 2-design is symmetric if $v = b$ (or equivalently $k = r$).

Example:

Let $X = \mathbb{Z}_2^3 \setminus \{0\}$ with blocks $\{x, y, x+y\}$, then $\mathcal{B}$ is a 2-design with parameters $(7, 3, 1)$. In addition, $r(k-1) = \lambda(v-1) \Rightarrow (3-1)r = (7-1) \Rightarrow r = 3 = k \Rightarrow \mathcal{B}$ is a symmetric 2-design. $\mathcal{B}$ is also called the Fano plane, and is the smallest projective plane ie. a symmetric 2-design with $\lambda = 1$.



Theorem 3.6:

If $\exists$ a symmetric 2-design with parameters (v, k, λ) where v is even, then $k - \lambda$ is a square.

Proof of Theorem 3.6:

Since $b = v$, the incidence matrix A of such a design is $v \times v \Rightarrow \det A$ exists and is $\in \mathbb{Z}$. By Proposition 3.4 and Proposition 3.2, $\det A^2 = \det A \det A^\top = \det AA^\top = (r-\lambda)^{v-1}(r + r(k-1)) = (k-\lambda)^{v-1}(k + k(k-1)) = (k-\lambda)^{v-1}k^2 \Rightarrow (k-\lambda)^{v-1}$ is a square $\Rightarrow$ since $v-1$ is odd, $k - \lambda$ must be a square.

Example:

Suppose $\mathcal{B}$ is a 2-design with parameters $(22, 7, 2)$, then by Proposition 3.2, $r(k-1) = \lambda(v-1) \Rightarrow (7-1)r = 2(22-1) \Rightarrow r = 7 = k \Rightarrow \mathcal{B}$ is symmetric. But v is even and $k - \lambda = 5$ is not a square $\Rightarrow$ by Theorem 3.6, $\nexists \mathcal{B}$.

Remark:

If v is odd, then the Bruck-Ryser-Chowla Theorem says that if a symmetric 2-design with parameters (v, k, λ) exists, then $z^2 = (k-\lambda)x^2 + (-1)^{\frac{v-1}{2}}\lambda y^2$ has a non-zero solution for $x, y, z \in \mathbb{Z}$.

Theorem 3.7:

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

Proof of Theorem 3.7:

Let A be the $v \times v$ incidence matrix of $\mathcal{B} = \{B_1, \cdots, B_v\}$, and consider $A^\top A$. Since $JA = kJ = rJ = AJ$ and $IA = AI$, $A(A^\top A) = (AA^\top)A = (\lambda J + (r-\lambda)I)A = A(\lambda J + (r-\lambda)I) = A(AA^\top)$ by Proposition 3.3. From the proof of Proposition 3.6, since $\det A^2 = (k-\lambda)^{v-1}k^2 \neq 0$ (else $r = k = \lambda \Rightarrow k = v \Rightarrow \mathcal{B}$ is a trivial design with $b = 1$), A is invertible $\Rightarrow A^\top A = AA^\top \Rightarrow |B_i \cap B_j| = (\text{column } i \text{ of } A) \cdot (\text{column } j \text{ of } A) = (A^\top A)_{ij} = (AA^\top)_{ij} = \lambda \ \forall i \neq j$.

Difference sets

Example:

Let $X = \mathbb{Z}_7$, $B_0 = \{0, 1, 3\} \subseteq X$. For $0 \leq i \leq 6$, define $B_0 + i = \{b + i : b \in B_0\}$, then these 7 subsets of X form the blocks of a symmetric 2-design with parameters $(7, 3, 1)$.

Definition:

Let $\lambda, v \in \mathbb{Z}^+$, $B_0 \subseteq \mathbb{Z}_v$. Call B_0 a λ-difference set if $\forall d \in \mathbb{Z}_v \setminus \{0\}$, there are exactly λ pairs $(b_1, b_2) \in B_0 \times B_0$ such that $b_1 - b_2 = d$.

Proposition 3.8:

Suppose B_0 is a λ-difference set in $\mathbb{Z}_v$. Let $k = |B_0|$, and for $i \in \mathbb{Z}_v$, define $B_0 + i = \{b + i : b \in B_0\}$. Then the subsets $B_0 + i$ form the blocks of a symmetric 2-design with parameters (v, k, λ).

Proof of Proposition 3.8:

All v subsets $B_0 + i$ have size k, so it suffices to show that any 2 points in $\mathbb{Z}_v$ lie in λ blocks. Pick $r, s \in \mathbb{Z}_v$, $r \neq s$, then $r, s \in B_0 + i \Leftrightarrow r - i, s - i \in B_0 \Rightarrow$ (number of choices for i) $=$ (number of pairs $\in B_0 \times B_0$ with difference $r - s$) $= \lambda \Rightarrow$ the result follows.

Example:

(1) Let $v = 11$, $B_0 = \{1, 4, 9, 5, 3\} \subseteq \mathbb{Z}_{11}$, then by Proposition 3.8, since B_0 is a 2-difference set, we have a symmetric 2-design with parameters $(11, 5, 2)$.

(2) Let $v = 13$, $B_0 = \{0, 1, 3, 9\} \subseteq \mathbb{Z}_{13}$, then B_0 is a 1-difference set $\Rightarrow$ we have a symmetric 2-design with parameters $(13, 4, 1)$.

Proposition 3.9:

Let p be a prime, $Q = \left\{x^2 : x \in \mathbb{Z}_p \setminus \{0\}\right\}$. If $p \equiv 3 \pmod 4$, then Q is a $\frac{p-3}{4}$-difference set, and the corresponding symmetric 2-design has parameters $\left(p, \frac{p-1}{2}, \frac{p-3}{4}\right)$.

Proof of Proposition 3.9:

Note that $Q \leq (\mathbb{Z}_p^*, \times)$, and $|Q| = \frac{p-1}{2} \equiv 1 \pmod 2 \Rightarrow -1 \notin Q \Rightarrow Q \cup (-Q) = \mathbb{Z}_p^*$. For $q \in Q$, define $S_q = \{(x_1, x_2) \in Q \times Q : x_1 - x_2 = q\}$. Since $r \in Q \Rightarrow qr \in Q$ and $x_1 - x_2 = q \Leftrightarrow rx_1 - rx_2 = rq$, we have $(x_1, x_2) \in S_q \Leftrightarrow (rx_1, rx_2) \in S_{rq} \Rightarrow |S_q| = |S_{rq}| \Rightarrow |S_q|$ is constant for $q \in Q$. Moreover, $-q \in -Q$, and $(x_1, x_2) \in S_q \Leftrightarrow (x_2, x_1) \in S_{-q} \Rightarrow |S_q| = |S_{-q}| \Rightarrow |S_x|$ is constant $\forall x \in Q \cup (-Q) = \mathbb{Z}_p^* \Rightarrow Q$ is a difference set in $\mathbb{Z}_p$, with $\lambda = \frac{|Q| \times (|Q| - 1)}{|\mathbb{Z}_p^*|} = \frac{p-1}{2} \times \frac{p-3}{2} \div (p-1) = \frac{p-3}{4} \Rightarrow$ the result follows.

Affine planes

Definition:

Let F be a finite field, then $F^2 = \{(x_1, x_2) : x_1, x_2 \in F\}$ is a 2-dimensional vector space over F. Define points to be vectors in F^2 and lines to be subsets of the form $\{v + \lambda w : \lambda \in F\} \subseteq F^2$ for some fixed $v, w \in F^2$, then this collection of points and lines is called the affine plane over F, denoted $AG(2, F)$.

Remark:

(1) If $|F| = q$, then number of points $= q^2$.

(2) Lines are solution sets of linear equations ie. $y = mx + c \leftrightarrow \{(0, c) + \lambda(1, m) : \lambda \in F\}$, $x = c \leftrightarrow \{(c, 0) + \lambda(0, 1) : \lambda \in F\} \Rightarrow$ number of lines $= q^2 + q$.

Proposition 3.10:

Every line has q points, and every 2 points lie on a unique line ie. $AG(2, F)$ is a 2-design with parameters $(q^2, q, 1)$.

Proof of Proposition 3.10:

Each line $v + \mathrm{Sp}(w) = \{v + \lambda w : \lambda \in F\}$ obviously has q points. Now pick $a, b \in F^2$, then a, b lie on $L = \{a + \lambda(b - a) : \lambda \in F\}$. Suppose a, b also lie on $L' = v + \mathrm{Sp}(w)$, then $a = v + \lambda_1 w$, $b = v + \lambda_2 w \Rightarrow b - a = (\lambda_2 - \lambda_1) w \Rightarrow L' = v + \mathrm{Sp}(w) = v + \lambda_1 w + \mathrm{Sp}(w) = a + \mathrm{Sp}(b - a) = L$.

In $AG(2, F)$, any 2 lines L_1, L_2 meet at 0 or 1 point. If they meet at 0 points, then they are called parallel lines.

Proposition 3.11:

The $q^2 + q$ lines in $AG(2, F)$ fall into $q + 1$ disjoint sets, each containing q parallel lines.

Proof of Proposition 3.11:

The $q + 1$ disjoint sets are $\mathcal{L}_m =$ (set of lines $y = mx + c$ where $c \in F$) for $m \in F$, and $\mathcal{L}_\infty$ = (set of lines $x = c$ where $c \in F$).

Remark:

These $q + 1$ sets of lines are called the parallel classes of lines.

Proposition 3.12:

Each point in F^2 lies in exactly 1 line for each parallel class.

Proof of Proposition 3.12:

Each parallel class has q disjoint lines, each with q points $\Rightarrow$ the result follows easily.

Projective planes

Definition:

A projective plane is a symmetric 2-design with $\lambda = 1$.

Remark:

By Theorem 3.7, any 2 blocks of a projective plane meet at 1 point.

Definition:

Equivalently, a projective plane is a set of points and lines (subsets of points) such that:

(1) any 2 points lie on a unique line,

(2) any 2 lines meet at a unique point,

(3) $\exists$ 4 points where no 3 points lie on a line.

Remark:

(1) It follows (not so trivially) that all lines have the same number of points, so a projective plane is indeed a 2-design with $\lambda = 1$. In addition, it is also symmetric.

(2) $\exists$ a converse to Theorem 3.7: If $\mathcal{B}$ is a 2-design with parameters (v, k, λ), such that any 2 blocks intersect at exactly λ points, then $\mathcal{B}$ is symmetric.

Example:

Lines in $AG(2, \mathbb{Z}_3)$ fall into 4 parallel classes $\mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_\infty$. Introduce points p_0, p_1, p_2, p_∞ to each line in $\mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_\infty$ respectively, and add a new line $L_\infty = \{p_0, p_1, p_2, p_\infty\}$, then we have a projective plane.

Proposition 3.13:

Let F be a finite field, $|F| = q$, and start with $AG(2, F)$. Add $q+1$ new points p_m $(m \in F)$ and p_∞ to each line in $\mathcal{L}_m$ and $\mathcal{L}_\infty$ respectively, and add a new line $L_\infty = \{p_m : m \in F\} \cup \{p_\infty\}$, then the points $F^2 \cup \{p_m : m \in F\} \cup \{p_\infty\}$ and the new lines form a projective plane.

Proof of Proposition 3.13:

There are q^2+q+1 points and q^2+q+1 lines, and each line has $q+1$ points $\Rightarrow$ the points and lines form a symmetric 2-design. Now pick any 2 distinct points a, b. If $a, b \in F^2$, then a, b lie on a unique line in $AG(2, F) \Rightarrow a, b$ lie on a unique extended line. If $a \in F^2$ and $b = p_m$ for some $m \in F \cup \{\infty\}$, then by Proposition 3.12, a lies on a unique line $L \in \mathcal{L}_m \Rightarrow$ the unique line containing a, b is $L \cup \{p_m\}$. If a, b are both p_m for some $m \in F \cup \{\infty\}$, then the unique line containing a, b is L_∞. Hence any 2 points lie on a unique line $\Rightarrow \lambda = 1 \Rightarrow$ the result follows.

Definition:

This projective plane is called $PG(2, F)$, the projective plane over F.

Remark:

$PG(2, F)$ is a symmetric 2-design with parameters $(q^2+q+1, q+1, 1)$.

Isomorphisms

Definition:

Let $(X_1, \mathcal{B}_1)$ and $(X_2, \mathcal{B}_2)$ be designs. A map $\phi : X_1 \to X_2$ is an isomorphism of designs if ϕ is bijective, and sends the blocks in $\mathcal{B}_1$ to the blocks in $\mathcal{B}_2$ bijectively.

Notation:

If $\exists \phi$, write $(X_1, \mathcal{B}_1) \cong (X_2, \mathcal{B}_2)$.

Example:

Let $X_1 = \mathbb{Z}_7$, $\mathcal{B}_1 =$ 2-design with blocks $B_0 + i$ where $B_0 = \{0, 1, 3\}$, with parameters

$(7,3,1)$, and $X_2 = \mathbb{Z}_2^3 \setminus \{0\}$, $\mathcal{B}_2 =$ blocks of the form $\{x, y, x+y\}$, which is also a 2-design with parameters $(7,3,1)$. We try our luck and construct $\phi : X_1 \to X_2$, $0 \mapsto 100$, $1 \mapsto 010$, $2 \mapsto 001$, then $\{0,1,3\} \mapsto \{100, 010, 110\} \Rightarrow 3 \mapsto 110$, $\{1,2,4\} \mapsto \{010, 001, 011\} \Rightarrow 4 \mapsto 011$, $\cdots$, $5 \mapsto 111$, $6 \mapsto 101 \Rightarrow$ the blocks in $\mathcal{B}_1$ (amazingly) get mapped to the blocks in $\mathcal{B}_2 \Rightarrow (X_1, \mathcal{B}_1) \cong (X_2, \mathcal{B}_2)$. In fact, we can map $0 \mapsto x$, $1 \mapsto y$, $2 \mapsto z$ for any $z \notin \{x, y, x+y\}$ to get an isomorphism $\Rightarrow$ number of isomorphisms $= 7 \times 6 \times 4 = 168$.

Remark:

The set of isomorphisms $\mathcal{B} \to \mathcal{B}$ form a group under composition, called the automorphism group $\mathrm{Aut}(\mathcal{B})$.

Higher-dimensional geometry

Definition:

Let F be a finite field with $|F| = q$, then $F^n = \{(x_1, \cdots, x_n) : x_i \in F\}$.

Remark:

F^n is an n-dimensional vector space over F, with q^n vectors.

Definition:

Let $1 \leq m \leq n$, then the q-binomial coefficient is $\binom{n}{m}_q = \dfrac{(q^n - 1)\cdots(q^{n-m+1} - 1)}{(q^m - 1)\cdots(q-1)}$.

Example:

(1) $\binom{n}{1}_q = \dfrac{q^n - 1}{q - 1}$.

(2) $\binom{4}{2}_2 = \dfrac{(2^4 - 1)(2^3 - 1)}{(2^2 - 1)(2 - 1)} = \dfrac{15 \times 7}{3 \times 1} = 35$.

(3) $\binom{n}{m}_1 = \binom{n}{m}$ (consider limits as $q \to 1$).

Proposition 3.14:

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

(2) For a fixed $v \in F^n \setminus \{0\}$, the number of m-dimensional subspaces of F^n containing v is $\binom{n-1}{m-1}_q$ if $m > 1$, 1 if $m = 1$.

(3) For linearly independent $v, w \in F^n \setminus \{0\}$, the number of m-dimensional subspaces of F^n containing v, w is $\binom{n-2}{m-2}_q$ if $m > 2$, 1 if $m = 2$.

Proof of Proposition 3.14:

(1) Let $S(m)$ be the number of m-dimensional subspaces of F^n, $(w_1, \cdots, w_m)$ be an ordered m-tuple of linearly independent vectors in F^n, and $W = \text{Sp}(w_1, \cdots, w_m)$, then the number of pairs $((w_1, \cdots, w_m), W)$ is = ways to choose $(w_1, \cdots, w_m) \times 1$ = ways to choose $w_1 \times$ ways to choose $w_2 \notin \text{Sp}(w_1) \times \cdots \times$ ways to choose $w_m \notin \text{Sp}(w_1, \cdots, w_{m-1}) = (q^n - 1)(q^n - q) \cdots (q^n - q^{m-1})$.

On the other hand, the number of such pairs is also = ways to choose $W \times$ ways to choose $(w_1, \cdots, w_m) = S(m) \times$ ways to choose $w_1 \in W \times$ ways to choose $w_2 \in W \setminus \text{Sp}(w_1) \times \cdots \times$ ways to choose $w_m \in W \setminus \text{Sp}(w_1, \cdots, w_{m-1}) = S(m) \times (q^m - 1)(q^m - q) \cdots (q^m - q^{m-1}) \Rightarrow S(m) = \dfrac{(q^n - 1) \cdots (q^n - q^{m-1})}{(q^m - 1) \cdots (q^m - q^{m-1})} = \dfrac{(q^n - 1) \cdots (q^{n-m+1} - 1)}{(q^m - 1) \cdots (q - 1)} = \binom{n}{m}_q$.

(2) Let W be an m-dimensional subspace containing v, and $V = \text{Sp}(v_2, \cdots, v_n)$ where $\{v, v_2, \cdots, v_n\}$ is a basis of F^n, then $W \not\subseteq V \Rightarrow \dim(W \cap V) = m - 1 \Rightarrow W = \text{Sp}(v) + (W \cap V) \Rightarrow$ ways to choose W = (number of $(m-1)$-dimensional subspaces of V) $= \binom{n-1}{m-1}_q$ if $m > 1$, 1 if $m = 1$.

(3) Similar to (2).

Proposition 3.15:

Let $n \geq 2$, $1 \leq m \leq n - 1$. Define points = vectors $\in F^n$, and blocks = subsets of the form $v + W$ where $v \in F^n$ and W is a m-dimensional subspace of F^n. Then we have:

(1) a 2-design with parameters (q^n, q^m, λ), where $\lambda = \binom{n-1}{m-1}_q$ if $m > 1$, 1 if $m = 1$,

(2) a 3-design with parameters $(2^n, 2^m, r_3)$ if $F = \mathbb{Z}_2$ and $m \geq 2$, where $r_3 = \binom{n-2}{m-2}_2$ if $m > 2$, 1 if $m = 2$.

Proof of Proposition 3.15:

(1) Note that all blocks $v + W$ have the same size $|W| = q^m$. Now pick $v_1, v_2 \in F^n$, $v_1 \neq v_2$, then any block containing v_1 is of the form $v_1 + W$, and $v_2 \in v_1 + W \Leftrightarrow v_1 - v_2 \in W \Rightarrow$ by Proposition 3.14(2), λ = number of blocks containing v_1, v_2 = (number of W containing $v_1 - v_2$) $= \binom{n-1}{m-1}_q$ if $m > 1$, 1 if $m = 1 \Rightarrow$ the result follows.

(2) Pick distinct $v_1, v_2, v_3 \in \mathbb{Z}_2^n$, then $v_2, v_3 \in v_1 + W \Leftrightarrow v_2 - v_1, v_3 - v_1 \in W$. Moreover, if $v_2 - v_1$, $v_3 - v_1$ are linearly dependent, then $v_2 - v_1 = c(v_3 - v_1)$ for some $c \in Z_2 \Rightarrow c = 0$ or $1 \Rightarrow v_1 = v_3$ or $v_2 = v_3$ $(\Rightarrow\Leftarrow) \Rightarrow v_2 - v_1$, $v_3 - v_1$ are linearly independent $\Rightarrow$ by Proposition 3.14(3), r_3 = number of blocks containing v_1, v_2, v_3 = (number of W containing $v_2 - v_1$ and $v_3 - v_1$) $= \binom{n-2}{m-2}_q$ if $m > 2$, 1 if $m = 2 \Rightarrow$ the result follows.

Definition:

This design is denoted $AG(n, F)_m$.

Example:

(1) Let $n = 2$, $m = 1$, then the design is $AG(2, F)$, with blocks of the form $v + \mathrm{Sp}(w)$ ie. lines in F^2.

(2) $AG(3, \mathbb{Z}_3)$ is a 2-design with parameters $(27, 3, 1)$.

(3) $AG(3, \mathbb{Z}_3)_2$ is a 2-design with parameters $(27, 9, 4)$.

(4) $AG(3, \mathbb{Z}_2)_2$ is a 3-design with parameters $(8, 4, 1)$.

(5) The codewords of weight 4 in H' form a 3-design isomorphic to $AG(3, \mathbb{Z}_2)_2$.

2-designs & strongly regular graphs

Definition:

A 2-design is quasi-symmetric if $\exists x, y \in \mathbb{Z}$, $x \neq y$, such that any 2 blocks intersect at either x or y points, and both occur.

Example:

(1) In $AG(2, F)$, any 2 lines meet at 0 or 1 point $\Rightarrow AG(2, F)$ is quasi-symmetric.

(2) Consider points = 23 coordinate positions of G_{23}, blocks = B_c for $c \in G_{23}$, $\mathrm{wt}(c) = 7$, then we have a 4-design with parameters $(23, 7, 1)$. For $c, d \in G_{23}, \mathrm{wt}(c) = \mathrm{wt}(d) = 7$, $c \neq d$, we have $\mathrm{wt}(c+d) = \mathrm{wt}(c) + \mathrm{wt}(d) - 2[c, d] = 14 - 2[c, d] = 8$ or $12 \Rightarrow |B_c \cap B_d| = [c, d] = 3$ or 1, and it is easily checked that both occur $\Rightarrow$ this design is quasi-symmetric.

Proposition 3.16:

Let $\Gamma(\neq K_v, K_v^c)$ be a graph with v vertices and adjacency matrix A, then TFAE:

(1) Γ is strongly regular,

(2) $A^2 = \alpha A + \beta I + \gamma J$ for some $\alpha, \beta, \gamma \in \mathbb{R}$.

Proof of Proposition 3.16:

(1) is true $\Rightarrow$ by Proposition 2.6, (2) is also true.

(2) is true $\Rightarrow$ number of common neighbours of i, j = (row i of A) $\cdot$ (row j of A) = (row i of A) $\cdot$ (column j of A) = $(A^2)_{ij} = \beta + \gamma$ if $i = j$, $\alpha + \gamma$ if $i \neq j$ and i is joined to j, γ if $i \neq j$ and i is not joined to $j \Rightarrow \Gamma$ is strongly regular with parameters $(v, \beta + \gamma, \alpha + \gamma, \gamma) \Rightarrow$ (1) is also true.

Theorem 3.17:

Let $\mathcal{B}$ be a quasi-symmetric 2-design, such that any 2 blocks intersect at either x or y points. Let $\Gamma(\mathcal{B})$ be a graph, with vertices = blocks of $\mathcal{B}$, and join $B_1, B_2 \in \mathcal{B}$ iff $|B_1 \cap B_2| = x$. Then $\Gamma(\mathcal{B})$ is strongly regular.

Proof of Theorem 3.17:

Let M be the $v \times b$ incidence matrix of $\mathcal{B}$ and A be the $b \times b$ adjacency matrix of $\Gamma(\mathcal{B})$, then $(M^\top M)_{ij} =$ (column i of M) $\cdot$ (column j of M) $= |B_i \cap B_j| = k$ if $i = j$, x if B_i is joined to B_j in $\Gamma(\mathcal{B})$, y otherwise $\Rightarrow M^\top M = kI_b + xA + y(J_b - A - I_b) = (x-y)A + (k-y)I_b + yJ_b \Rightarrow$ since $x \neq y$, $A = rM^\top M + sI_b + tJ_b$ for some $r, s, t \in \mathbb{R} \Rightarrow A^2 = r^2 M^\top M M^\top M + s^2 I_b + t^2 J_b^2 + 2rsM^\top M + 2stJ_b + rtM^\top MJ_b + rtJ_bM^\top M$.

By Proposition 3.3, $MM^\top = \lambda J_v + (r-\lambda)I_v$, $MJ_b = rJ$, $J_vM = kJ$ where $J = v \times b$ matrix consisting of all 1's $\Rightarrow M^\top MM^\top M = M^\top(\lambda J_v + (r-\lambda)I_v)M = (\lambda kJ^\top + (r-\lambda)M^\top)M = \lambda k^2 J_b + (r-\lambda)[(x-y)A + (k-y)I_b + yJ_b] = (r-\lambda)(x-y)A = (r-\lambda)(k-y)I_b + (\lambda k^2 + (r-\lambda)y)J_b$, $J_b^2 = bJ_b$, $M^\top MJ_b = M^\top(rJ) = r(J^\top M)^\top = rkJ_b$, and $J_bM^\top M = (MJ_b)^\top M = rJ^\top M = rkJ_b \Rightarrow A^2 = \alpha A + \beta I_b + \gamma J_b$ for some $\alpha, \beta, \gamma \in \mathbb{R} \Rightarrow$ by Proposition 3.16, $\Gamma(\mathcal{B})$ is strongly regular.

Example:

(1) Let the vertices of Γ be lines of $AG(2, F)$, and join L_1, L_2 iff $|L_1 \cap L_2| = 0$ ie. L_1 and L_2 are parallel. Then $\Gamma = (K_q)^{q+1}$, where $q = |F|$.

(2) Let the vertices of Γ be the 253 blocks B_c of G_{23} where $\mathrm{wt}(c) = 7$, and join B_c, B_d iff $|B_c \cap B_d| = 3$ ie. $\mathrm{wt}(c+d) = 8$. Then Γ is strongly regular, with $k =$ (number of d such that $\mathrm{wt}(c+d) = 8$ for a fixed c with $\mathrm{wt}(c) = 7$).