CO434 - Combinatorial Designs

University of Waterloo
Nicholas Pun
Winter 2020

Contents

Lecture 1: Introduction

This course is concerned with combinatorial objects satisfying certain regularity/balanced conditions. We will go over the following topics:

- Classical results in design theory
- Constructions of designs
- Structural theorems
- Non-existence results
- Lots of algebra (abstract and linear)
- Some number theory!

1.1 The 36 Officers Problem (Euler, 1782)

Problem statement: We have 36 pieces that are

- 1 of 6 chess pieces: King, Queen, Bishop, Rook, Knight, Pawn, and
- 1 of 6 colors (one piece of each colour)

Can we arrange these on a 6-by-6 square such that each row and each column uses exactly one piece of each type and one piece of each colour? Euler thought this was impossible.

Note that this is easy for 5 chess pieces and 5 colours. Consider (using numbers 1 through 5 in place of the different chess pieces):

1	2	3	4	5
2	3	4	5	1
3	4	5	1	2
4	5	1	2	3
5	1	2	3	4

Which was constructed by taking the sequence 12345 and shifting it left each row.

Further, this is impossible for 2 pieces and 2 colours. In fact, Euler conjectured that this is impossible for $n \equiv 2 \pmod 4$

However, this was wrong! (In fact, 2 ad 6 are the only numbers for which this is impossible, and we'll gain a better understanding of why through this course!)

1.2 Statistical Experimental Design

Here is a take on design theory. Consider the following scenario where:

- We have v kinds of wine we want to compare,

- But, we can only accurately compare k kinds per day.
- And, we only want to compare each pair exactly once.

Can we decide on what to drink each day in order to accomplish these tasks?

Example 1.1 (Fano Plane)**.** Suppose $v = 7, k = 3$.

We will call the objects we want to compare (in this case, the wines) points and the experiment for the day a block.

Here our points be labelled with numbers: $\{0, 1, 2, \ldots, 6\}$

And our blocks for each day will be:

Day 1: $\{0, 1, 3\}$

Day 2: $\{1, 2, 4\}$

Day 3: $\{2, 3, 5\}$

Day 4: $\{3, 4, 6\}$

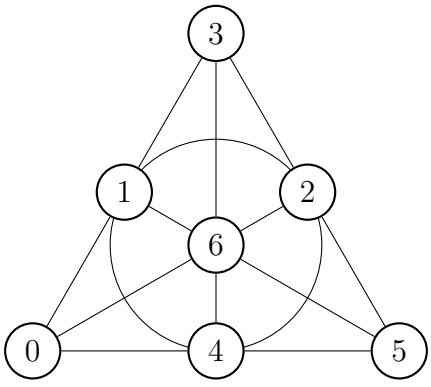
Day 5: $\{4, 5, 0\}$

Day 6: $\{5, 6, 1\}$

Day 7: $\{6, 0, 2\}$

Note that we can obtain the next day's experiment by adding 1 modulo 7. And, finally we can check that every pair appears in exactly one block. △

This example actually has a nice visualization:



Note that each collinear line gives us a block (We count the line through 1, 2, and 4 as a "straight" line) How did we come up with this? We'll answer this through the course! For now, let's look at another example:

Example 1.2 (Game of Set)**.** In this game, we have 81 cards, each with 4 attributes:

- Colour: Red, Green, or Purple

- Number: 1, 2, or 3
- Shading: Open, Shaded, or Solid
- Shape: Oval, Diamond, or Squiggle

A Set is a triple of cards with the property that in each attribute, they are all the same or all different.

Note. Each pair of cards is in a unique Set!

This is since on each attribute, the pair is either matching or different, and there is a unique third card that can complete the pattern. △

How do the above examples compare?

Balancing Properties of the Two Examples

Fano Plane	Set
Each block has 3 points	Each Set has 3 cards
Each point is in 3 blocks	Each card is in 40 different Sets*
Each pair of points is in exactly one block	Each pair of cards is in a unique set

*Why is this true? For every card, we can choose any other card in the deck (There are 80 such choices) But, we observed earlier that for every pair, there is a unique 3rd card that completes a Set. So, in fact, we'll treat the remaining 80 cards as pairs.

1.3 Basic Definitions

Definition 1.1. A design is a pair $(V, \mathcal{B})$ where

- V is a finite set of elements called points
- $\mathcal{B}$ is a collection (multiset) of (usually non-empty) subsets of V, called blocks

We call a design simple if $\mathcal{B}$ is a set (there are no repeated blocks)

Definition 1.2. A t-design ($t \in \mathbb{N}$) is a design $(V, \mathcal{B})$ in which all blocks have the same size k, and there is a constant λ_t such that every t-tuple of points lie in exactly λ_t blocks.

The two examples we just saw were 2-designs with $\lambda_2 = 1$ and also 1-designs with $\lambda_1 = 3$ for the Fano plane and $\lambda_1 = 40$ for the game of Set.

Definition 1.3. A Balanced Incomplete Block Design (BIBD) is a design that is a 2-design and a 1-design.

Exercise. If $\lambda_2 \neq 0$, then show that every 2-design is automatically a 1-design

Lecture 2: BIBDs and Examples

Recall Definition 1.3, the definition for Balanced Incomplete Block Designs (BIBD).

The parameters (v, b, r, k, λ) of a BIBD are defined as follows:

- $v = |V|$ - The number of points
- $b = |\mathcal{B}|$ - The number of blocks (also λ_0)
- $r = \lambda_1$ - Each point lies in r blocks
- $k = |\alpha|, \forall \alpha \in \mathcal{B}$ - The size of the blocks
- $\lambda = \lambda_2$ - Each pair of points are in λ blocks

We call v, k, λ the primary parameters and b, r the secondary parameters.

We'll call a BIBD with these parameters a:

- (v, k, λ)-BIBD, or
- 2-(v, k, λ)-BIBD, or
- (v, b, r, k, λ)-BIBD

Example 2.1. The Fano Plane (Example 1.1) is a $(7, 3, 1)$-BIBD (and also a $(7, 7, 3, 3, 1)$-BIBD) $\triangle$

A BIBD is trivial if $k \in \{0, 1, v-1, v\}$

Convention: We will assume that our BIBDs are non-trivial designs (Since otherwise some statements *may* be false)

Definition 2.1. Let $(V, \mathcal{B})$ be a design, we define the complement design $(V, \overline{\mathcal{B}})$ where $\overline{\mathcal{B}} = \{V \setminus \alpha \mid \alpha \in \mathcal{B}\}$

Example 2.2 (Complement of the Fano Plane)**.**
$V = \{0, 1, 2, \ldots, 6\}$ - The points stay the same.

$\mathcal{B} = \{013, 124, 235, 346, 450, 561, 602\}$ - These were the blocks we had before.

$\overline{\mathcal{B}} = \{2456, 0356, 0146, 0125, 1236, 0234, 1345\}$ - These make a $(7, 7, 4, 4, 2)$-BIBD $\triangle$

Exercise. The complement of a (v, b, r, k, λ)-BIBD is a $(v, b, b-r, v-k, b-2r+\lambda)$-BIBD

2.1 Difference Sets

Let $(G, +, 0)$ be an abelian group. A difference set S is a subset of G with the property that there exists a constant λ such that $\forall g \neq 0, |\{(a, b) \in S \times S \mid a - b = g\}| = \lambda$. If $|G| = v, |S| = k$, we call this a (v, k, λ)-difference set

Example 2.3. Let $G = \mathbb{Z}_7, S = \{0, 1, 3\}$. We can check that this is a difference set by taking the difference between every pair of elements $(a, b) \in S \times S$

		a		
		0	1	3
	0	0	1	3
b	1	6	0	2
	3	4	5	0

Each number from 1 to 6 appear exactly once, so this is a $(7, 3, 1)$-difference set. △

Example 2.4. Let $G = \mathbb{Z}_{11}, S = \{0, 2, 3, 4, 8\}$ creates an (11,5,2)-difference set. △

Theorem 2.1. If $S \subseteq G$ is a (v, k, λ)-difference set, then we construct a (v, k, λ)-BIBD as follows:

- $V = G$
- $\mathcal{B} = \{g + S \mid s \in S\}$

Note. $v = b$ and $k = r$

Proof. Exercise! □

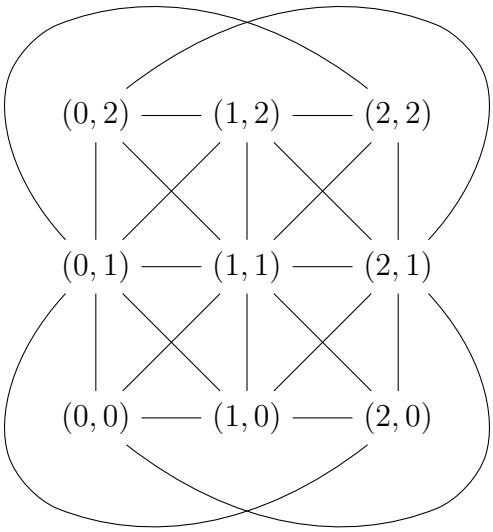
Problem: How to we find difference sets? We'll see later in the course!

2.2 Affine Space

Let V be a vector space over a finite field $\mathbb{F}$. An affine line in V is a set of points of the form $\{xt + y \mid t \in \mathbb{F}\}$, where $x, y \in V$, $x \neq 0$. Let $\mathcal{B}$ be the set of all affine lines in V, then $(V, \mathcal{B})$ is a BIBD with $\lambda = 1, k = |\mathbb{F}|$

When $\dim_{\mathbb{F}} V = 2$, we call this an affine plane.

Example 2.5. Let $\mathbb{F} = \mathbb{Z}_3, V = \mathbb{Z}_3^2$. This creates a $(9, 12, 4, 3, 1)$-BIBD.



For example, with $y = (1, 0), x = (2, 1)$, we have:

- $(1, 0) = 0x + y$
- $(0, 1) = 1x + y$
- $(2, 2) = 2x + y$

all of which are located on the same line. △

Example 2.6. The game of Set is a 4-dimensional affine space over Z_3 △

2.3 Relations between Parameters

Theorem 2.2. The parameters (v, b, r, k, λ) of a BIBD satisfy:

$$\frac{v}{k} = \frac{b}{r} \tag{2.1}$$

$$\frac{v(v-1)}{k(k-1)} = \frac{b}{\lambda} \tag{2.2}$$

$$\frac{v-1}{k-1} = \frac{r}{\lambda} \tag{2.3}$$

Proof:

When $\dim(A) = 2$, we call this an affine plane.

Ex. The game of Set is an 4-dimensional affine space over $\mathbb{Z}_3$.

Relations b/w Parameters:

Theorem:
The parameters (v, b, r, k, λ) of a BIBD satisfy:

① $\frac{v}{k} = \frac{b}{r}$

② $\frac{v(v-1)}{k(k-1)} = \frac{b}{\lambda}$

③ $\frac{v-1}{k-1} = \frac{r}{\lambda}$.

Proof:
Let's count pairs (x, α), where $x \in V$ and $\alpha \in B$, and $x \in \alpha$.

There are v choices for x. For each choice of x, there are r blocks containing x, so r choices for α.
Therefore, the # of pairs is vr.

There are b choices for α. For each choice of α, there are k elements to choose, so k choices for x.
Therefore, the # of pairs is bk.

This gives us equation ①, since $vr = bk$.

Proof (cont'd)

For ②, we count triples (x, y, α), $x, y \in V$, $x \neq y$, $\alpha \in \mathcal{B}$, $x, y \in \alpha$. (Exercise! Fill this in)

And ③ is ②/①. ∎

Ex: If $F = GF(q)$ (Galois Field with q elements), $V = F^n$, then then affine space is the design with parameters (v, b, r, k, λ) where:

$v = q^n$, $k = q$, $\lambda = 1$

and using the theorem, we can solve for b, r:

$$b = \lambda \frac{v(v-1)}{k(k-1)} = \frac{q^{n-1}(q^n - 1)}{q-1}$$

$$r = \lambda \frac{v-1}{k-1} = \frac{q^n - 1}{q-1}.$$

Uploading scans of my notes for now ... I'll type these up one day ...

Lecture 3:

Last time:
(v,b,r,k,λ)- BIBD defn and
① $vr = bk$
② $\frac{v(v-1)}{k(k-1)} = \frac{b}{\lambda}$
③ $\frac{v-1}{k-1} = \frac{r}{\lambda}$.

(Cross out defn of order last class's. in nodes!)

Corollary: (Necessary Conditions)
If a (v,k,λ)-BIBD exists, then $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$ and $\lambda(v-1) \equiv 0 \pmod{k-1}$

Proof:
Since b is an integer, and $b = \frac{\lambda v(v-1)}{k(k-1)}$, then $k(k-1)$ divides $\lambda v(v-1)$.

Similarly, since r is an integer and $r = \frac{\lambda(v-1)}{k-1}$, then $k-1$ divides $\lambda(v-1)$. ☆

Ex: A Steiner Triple System is a $(v,3,1)$-BIBD. Determine all values of v satisfying the necessary conditions.
→ Needs to satisfy $v(v-1) \equiv 0 \pmod 6$
$v-1 \equiv 0 \pmod 2$
which gives us the 2 possibilities:
$v \equiv 1 \pmod 6$
$v \equiv 3 \pmod 6$

Question: Are these sufficient? ②

Isomorphism:

Let $(V, \mathcal{B})$ and $(V', \mathcal{B}')$ be designs. We say that these are isomorphic if there exists a bijection $f: V \to V'$ such that $\mathcal{B}' = \{\{f(x) : x \in X\} \mid X \in \mathcal{B}\}$.

Other ways to specify a design:

- Incidence Structure:

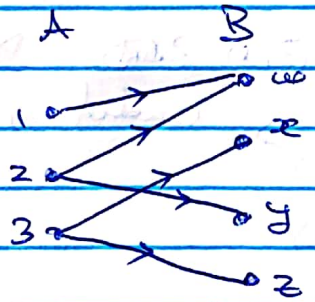
Def'n An incidence structure is a relation "$\to$" on (A, B) where A and B are sets. For any pair $(a,b) \in A \times B$, either $a \to b$ or $a \not\to b$. (We call this "$\to$" an incidence or incidence relation)

Given an incidence relation $\to$ on (A, B), we construct a design $(V, \mathcal{B})$:

$V = A$

$\mathcal{B} = \{\{a : a \to b\} \mid b \in B\}$

Ex.



$V = \{1, 2, 3\}$

$\mathcal{B} = \{\{1, 2\}$, (from w)
$\{3\}$, (from x)
$\{2\}$, (from y)
$\{3\}\}$. (from z)

Note: $\{3\}$ exists in the design twice.

Note: This incidence structure is effectively a bipartite graph, and 2 designs are isomorphic iff their incidence structures/bipartite graphs are isomorphic

- Incidence Matrix:

Given a design (V, B), write $V = \{x_1, x_2, \ldots, x_v\}$, $B = \{a_1, a_2, \ldots, a_b\}$. The incidence matrix N is the $v \times b$ matrix. (one row for every point, one column for every block), where

$$N_{ij} = \begin{cases} 1 & \text{if } x_i \in x_j \\ 0 & \text{otw.} \end{cases}$$

Each column of the matrix specifies a block of the design.

Ex:

$$N = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} w & x & y & z \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

Proposition

(V, B) is a (v, b, r, k, λ)-BIBD iff its incidence matrix N satisfies the following conditions:

(a) $N J_b = r J_v$

(b) $J_v N = k J_b$

(c) $N N^T = (r - \lambda) I_v + \lambda J_v$.

→ Proof

(2)

Proof:

$$N\mathbb{1}_b = \begin{pmatrix} \sum_{j=1}^{b} N_{1j} \\ \vdots \\ \sum_{j=1}^{b} N_{vj} \end{pmatrix}, \quad \text{so } N\mathbb{1} = r\mathbb{1} \text{ iff } \sum_{j=1}^{b} N_{ij} = r \text{ for}$$

all $i = 1, \ldots, v$. and $\sum_{j=1}^{b} N_{ij}$ is the # of blocks containing the blocks the point x_i, ~~and it is~~ ~~is~~ is i

So $\sum_{j=1}^{b} N_{ij} = r$, iff x_i lies in r blocks $\forall i$

Similarly, $\mathbb{1}^T N = k\mathbb{1}^T$ iff each block has k points.

Finally, consider NN^T.

$$(NN^T)_{ii} = \sum_{j=1}^{b} N_{ij}(N_{ji}^T) = \sum_{j=1}^{b} N_{ij} \cdot N_{ij} \quad \text{since } N_{ij} = 0 \text{ or } 1.$$

$$= \sum_{j=1}^{b} N_{ij}$$

Hence $(NN^T)_{ii} = r$ iff x_i is in r blocks.

Aside: $(r-\lambda) I_v + \lambda J_v = \begin{pmatrix} r-\lambda & & 0 \\ & \ddots & \\ 0 & & r-\lambda \end{pmatrix} + \begin{pmatrix} \lambda & \lambda & \cdots & \lambda \\ \vdots & & & \vdots \\ \lambda & \cdots & & \lambda \end{pmatrix}$.

$$= \begin{pmatrix} r & & \lambda \\ & \ddots & \\ \lambda & & r \end{pmatrix}.$$

Proof (cont'd)

And, for $i \neq j$,

$$(NN^T)_{ij} = \sum_{k=1}^{v} N_{ik} N^T_{kj} = \sum_{l=1}^{b} (N_{il} N_{jl})$$

$$= \begin{cases} 1 & \text{if } x_i \in x_l \text{ and } x_j \in x_l \\ 0 & \text{otw} \end{cases}$$

This is the number of blocks containing both x_i and x_j

So, $(NN^T)_{ij} = \lambda \ \forall i \neq j$ iff every pair of points is in λ blocks. ∎

Example:

Let's do one of the exercise on complements using incidence matrices: If $(V, \mathcal{B})$ is a (v, b, r, k, λ)-BIBD, let $(V, \bar{\mathcal{B}})$ be the complement design. Let N and $\bar{N}$ be the incidence matrices

$\bar{N} = K - N$ where $K = J_{v \times b} = \mathbb{1}_v \mathbb{1}_b^T$.

Check (a), (b), (c) for $\bar{N}$:

(a) $\bar{N}\mathbb{1}_b = (K - N)\mathbb{1}_b = K\mathbb{1}_b - N\mathbb{1}_b = b\mathbb{1}_v - r\mathbb{1}_v = (b-r)\mathbb{1}_v$

(b) $\mathbb{1}_v^T \bar{N} = \cdots = (v-k)\mathbb{1}_b^T$

(c) $\bar{N}\bar{N}^T = (b - N)(k - N)^T$

$= KK^T - NK^T - KN^T + NN^T$

$= \mathbb{1}_v \mathbb{1}_b^T \mathbb{1}_b \mathbb{1}_v^T - N\mathbb{1}_b \mathbb{1}_v^T - \mathbb{1}_v \mathbb{1}_b^T N^T + NN^T$

$= b\mathbb{1}_v \mathbb{1}_v^T - r\mathbb{1}_v \mathbb{1}_v^T - r\mathbb{1}_v \mathbb{1}_v^T + (r-\lambda)I_v + \lambda J_v$

$= (r-\lambda)I_v + (b - 2r + \lambda)J_v$ ③

Exercise (which will be discussed next class)
Is $(r-\lambda)I_v + \lambda J$ invertible?

Cor: In any non-trivial BIBD, the rows of N are linearly independent

Proof:
Since $NN^T = (r-\lambda)I_v + \lambda J_v$ invertible, $\Rightarrow$ rank(N) = rank$(NN^T) = v$
& So, N has v rows $\Rightarrow$ v rows of N is linearly independent.

Cor: (Fisher's Inequality)
In any non-trivial (v,b,r,k,λ)-BIBD, $b \geq v$.

Lecture 4:

Last time:

- $\text{rank}(XX^T) = \text{rank}(X)$ (Theorem from linear algebra)
  "If A is a real $k \times k$ matrix, then A and AA^T have the same column space
  $\Rightarrow \text{rank}(A) = \dim \text{Col}(A) = \dim \text{Col}(AA^T) = \text{rank}(AA^T)$"
  (Analogous thm for $\mathbb{C}$: $\text{rank}(XX^+) = \text{rank}(X)$., and thm is false for finite fields),

(Takeaway: For this course, the field we work over will make a difference)

- $(c-\lambda)I_v + \lambda J_{v \times v}$ invertible.

  Proof #1:

  First, let's figure out the eigenvalues of J_v:

  $\text{rank}(J_v) = 1$. So, the eigenvalues are: $\underbrace{0, \ldots, 0}_{v-1}, \theta$.

  Now, $\text{tr}(J_v) =$ sum of eigenvalues $= v = \theta$

  Then, for the matrix we care about, the eigenvalues are:

  $f(J_v)$, where $f(x) = cx + (c-\lambda)$

  This has eigenvalues

  $f(0), \ldots, f(0), f(v)$

  None of which are 0 & Invertible

Proof #2:

Thm: If A is an invertible matrix. Then, there is a poly. $p(x)$ s.t. $A^{-1} = p(A)$.

What do the powers of $(c-\lambda)I_v + \lambda J_v$ look like?:

Answer: They are all of the form: $sI + tJ$

$\therefore$ If $(c-\lambda)I + \lambda J$ is invertible, then its inverse must be of same form:

$$((c-\lambda)I_v + \lambda J_v)^{-1} = sI + tJ.$$

So:

Try to solve:

$$(sI + tJ)((c-\lambda)I_v + \lambda J_v) = I. \quad \square$$

Fisher's Inequality: $b \geq v$.

Proof:

b = # of cols N

$\geq \text{rank}(N) = v$. $\square$

—— (End of first "section": Intro to design) ——

Jan 15th

Next: We'll look at the extreme situation where Fisher's inequality is an equality.

Symmetric Designs:

Defn: A BIBD is symmetric if $v=b$.

Example.

(i) The Fano plane is symmetric.

(ii) Any design from a difference construction is symmetric

Basic facts:

- $v=b$ iff $r=k$.
- The incidence matrix of a symmetric design is invertible. (Since rows are l.i., and the matrix is square)
- All symetric designs are simple (Since if not, then the incidence matrix has 2 identical cols corresponding to the identical blocks. But the matrix is invertible so this cannot happen).
- $\frac{v(v-1)}{k(k-1)} = \frac{b}{\lambda}$ and $v=b$

  $\Rightarrow v = 1 + \frac{k(k-1)}{\lambda}$.

  * Does taking the complement give you the other value of k?

In particular $k(k-1) \equiv 0 \pmod{\lambda}$.

Lemma: The incidence matrix of a symmetric design is normal. (i.e. $NN^T = N^TN$)

Proof:

We have $NJ = N\mathbb{1}\mathbb{1}^T = (r\mathbb{1})\mathbb{1}^T = kJ$, and

$JN = \mathbb{1}\mathbb{1}^TN = \mathbb{1}(k\mathbb{1}) = kJ$.

So, $NJ = JN$.

Then,

$NNN^T = N((r-\lambda)I + \lambda J)$ (N commutes w I and J)

$= ((r-\lambda)I + \lambda J)N$

$= NN^TN$

And since N invertible $N^{-1}NNN^T = N^{-1}NN^TN \Rightarrow NN^T = N^TN$ ∎.

Defn (Order)

The order of a symmetric design is $n = k-\lambda = r-\lambda$.

Thus: $NN^T = N^TN = nI + \lambda J$

Theorem: Let $(V, \mathcal{B})$ be a symmetric design with params (v,k,λ). For any 2 blocks, $\alpha, \beta \in \mathcal{B}$, $\alpha \neq \beta$, we have $|\alpha \cap \beta| = \lambda$.

Jan 15th

Proof:

Since $NN^T = nI + \lambda J$.

$$\lambda = (N^T N)_{ij} = \sum_{k=1}^{v} N^t_{ik} N_{kj}$$

$$= \sum_{k=1}^{v} N_{ki} N_{kj}$$

$$= |\alpha_i \cap \alpha_j|$$

Def'n (Dual Design)

Let $(V, \mathcal{B})$ be a design. The dual design is $(\mathcal{B}, \tilde{V})$ where:

$$\tilde{V} = \{\{\alpha \in \mathcal{B} \mid v \in \alpha\} \mid v \in V\}.$$

If N is the incidence matrix of $(V, \mathcal{B})$, then N^T ——— " ——— $(\mathcal{B}, \tilde{V})$

Notes:

- If $(V, \mathcal{B})$ is a symmetric design, then the dual is also a symmetric design with the same parameters.
- (In general, the dual of a BIBD is not a BIBD)
- "Symmetric" refers to this very specific parameter symmetry.

It is not necessarily true that a symmetric design and its dual are isomorphic

Finite Fields Primer:

- Existence: $\exists$ a finite field $GF(q)$ with q elements (order q) iff $q = p^d$ (p prime).
  (p is called the "characteristic")
- Uniqueness: any 2 fields with the same # of elements are isomorphic.
- Construction: $GF(q) = \mathbb{Z}_p[x] / \langle f(x) \rangle$, where $f(x) \in \mathbb{Z}_p[x]$ is irreducible of degree d.

Example:

To construct $GF(4)$, we need $f(x) \in \mathbb{Z}_2[x]$ irreducible of degree 2:

x^2, x^2+1, x^2+x, x^2+x+1.

$x^2 = x \cdot x$; $x^2+1 = (x+1)^2$; $x^2+x = x(x+1)$

So, all these factor

We can only use this one

So: $GF(4) = \mathbb{Z}_2[x] / \langle x^2+x+1 \rangle$

Elements of $GF(4)$: $0, 1, x, x+1$.

Mult table:

	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Jan 15th

- Additive Group Structure:

$(GF(q), +) \cong (\mathbb{Z}_p^d, +)$

In particular: For $a \in GF(q)$

$pa = \underbrace{a + \cdots + a}_{p \text{ times}} = 0$

- Subfields:

$GF(q)$ is a subfield of $GF(q_2)$ iff $q_2 = q_1^k$.

In which case, $GF(q_2)$ is an k-dimensional vector space over $GF(q_1)$.

- Linear Algebra:

Most of linear algebra works the same way regardless of the field.

Next time: Counting vector spaces.

- If $V = GF(q)^n$, how many linear subspaces of V (of dim k).

Comb 354

Jan 20th

Lecture 5:

Note:

Other ways to express Fisher's inequality:

$b \geq v \iff r \geq k \iff v \geq 1 + \frac{k(k-1)}{\lambda}$.

Counting vector spaces over finite fields:

Let V be a d-dimensional vector space over $GF(q)$.

How many m-dimensional linear subspaces?

$$\frac{(q^d-1)(q^d-q)(q^d-q^2)\cdots(q^d-q^{m-1})}{(q^m-1)(q^m-q)(q^m-q^2)\cdots(q^m-q^{m-1})} = \binom{d}{m}_q.$$

↑ # of different bases of size m. (list of m linearly independent vectors)

↑ # of lists that gives a basis for any particular m-dimensional subspace

$q^d - 1$ ← The first vector cannot be zero!

↪ any $v \in V = GF(q)^d$. : First Vector

$q^d - q$: 2nd Vector

↪ multiples of the first vector

etc.

→ The numerator gives us a list of l.i vectors (out of a basis of size d).

(and similarly for the denominator).

A construction:

Let q be a prime power and $\mathbb{F} = GF(q)$.

Let W be a finite dimensional vector space over $\mathbb{F}$ of dimension d (Eg. $W = \mathbb{F}^d$).

Let $\mathcal{I} = \{1\text{-dim'l linear subspaces of } W$ (i.e. The set of lines$)$

Let $\mathcal{H} = \{(d-1)\text{-dim'l} \longrightarrow " \longrightarrow \}$ (i.e hyperplanes)

$(\mathcal{I}, \mathcal{H})$ is an incidence structure under the relation $\subseteq$ (i.e. For $l \in \mathcal{I}$, $h \in \mathcal{H}$, either $l \subseteq h$ or $l \not\subseteq h$).

Theorem: $(\mathcal{I}, \mathcal{H})$ is the incidence structure of a symmetric design with parameters

$$v = \frac{q^d - 1}{q - 1}, \quad k = \frac{q^{d-1} - 1}{q - 1}, \quad \lambda = \frac{q^{d-2} - 1}{q - 1}.$$

Proof:

$v = |\mathcal{I}| =$ # of 1-dim'l linear subspaces of W

$= \frac{q^d - 1}{q - 1}$.

$k =$ # of 1-dim'l linear subspaces of $h \in \mathcal{H}$ ← $(d-1)$-dim'l vector space

$= \frac{q^{d-1} - 1}{q - 1}$. (so, same formula, but with $d-1$ vs. d.)

↑ (Note: Does not depend on choice of h).

Jan 20th

Proof: (Cont'd)

Finally, if $l_1, l_2 \in \mathcal{L}$, l_1, l_2 distinct. A hyperplane contains both iff it contains $l_1 + l_2$ ← The 2-dim'l vector space containing lin. combs of the lines.

Such hyperplanes are in bijection with $(d-3)$-dim'l subspaces of $W/(l_1+l_2)$ (mod).

Since $\dim(W/(l_1+l_2)) = d-2$, there are:

$$\lambda = \frac{(q^{d-2}-1)(q^{d-2}-q)\cdots(q^{d-2}-q^{d-4})}{(q^{d-3}-1)(q^{d-3}-q)\cdots(q^{d-3}-q^{d-4})}$$

$$= \frac{1\cdot q\cdot q^2\cdots q^{d-4}(q^{d-2}-1)(q^{d-3}-1)(q^{d-4}-1)\cdots(q^2-1)}{1\cdot q\, q^2\cdots q^{d-4}(q^{d-3}-1)(q^{d-4}-1)\cdots(q-1)}$$

$$= \frac{q^{d-2}-1}{q-1}$$

such hyperplanes.

(Exercise: Check that this design is symmetric) ∎

Defn

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

Corollary: If q is a prime power, there exists a projective plane of order q. (i.e. $k = q+1$). ②

Proof:

If $d=3$ in the construction just given, we get:

$$v = \frac{q^3-1}{q-1} = q^2+q+1$$

$$k = \frac{q^3-1}{q-1} = q+1$$

$$\lambda = \frac{q-1}{q-1} = 1.$$

□

Open Problem: Is there a projective plane of order n, n is not a prime power.

Derived and Residual Designs:

Given any symmetric design $(V, \mathcal{B})$, we can construct 2 new (even-symmetric) BIBDs:

Let $\alpha \in \mathcal{B}$:

$$\mathrm{Der}(V, \mathcal{B}, \alpha) = (\alpha, \{\beta \cap \alpha \mid \beta \in \mathcal{B}, \beta \neq \alpha\})$$

$$\mathrm{Res}(V, \mathcal{B}, \alpha) = (V \setminus \alpha, \{\beta \setminus \alpha \mid \beta \in \mathcal{B}, \beta \neq \alpha\})$$

Exercise: Check that these are BIBDs and work out the parameters.

Exercise 2: What is the precise relation b/w these constructions? (Hint: Something to do with complements, can go from Der → Res)

Jan 28th

Congruence of matrices:

Defn Let F be a field (we will usually take $F = \mathbb{Q}$ here). Let $A, B \in M_{n\times n}(F)$. We say that A is **congruent** to B over F if there exists an invertible $P \in M_{n\times n}(F)$ such that:

$$P^T A P = B$$

and we write $A \approx_F B$ or $A \approx B$ (if F is understood from context)

Note: This is different from similar matrices, where A is similar to B iff $P^{-1}AP = B$.

Unlike similarity, congruence of matrices is very sensitive to the field. Clear. ~~Similarity~~ If similarity is achieved in a field extension, it can be achieved in the original field)

Example

over $\mathbb{R}$,

$$\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \approx_{\mathbb{R}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \approx_{\mathbb{R}} \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$$

Take $P = \begin{pmatrix} \sqrt{3} & 0 \\ 0 & \sqrt{3} \end{pmatrix}$ ↑ ↑ Take $P = \begin{pmatrix} \sqrt{5} & 0 \\ 0 & \sqrt{5} \end{pmatrix}$

But over $\mathbb{Q}$, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \approx_{\mathbb{Q}} \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$, but $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \not\approx_{\mathbb{Q}} \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$

Why? 5 can be written as the sum of 2 squares, but 3 cannot.

Moral: Congruence over $\mathbb{Q}$ is quite trivial number theory problem.
What does this have to do with designs?
Prop: If a symmetric (v,k,λ)-design exists, then $I_v \equiv \text{or} \; I_v + \lambda J_v$ $(v=k-\lambda)$.
Proof: The incidence matrix $N \in M_{v\times b}(\mathbb{R})$ is invertible and $NJ_{vb} = JN = nJ_{vb}$, $J^2 = vJ$

⑤

So, $S = \lambda^2 + I^2$

Let $P = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$ ← Note that this is almost orthogonal.

Then,

$$P^T \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} P = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$$

Now, suppose that we had

$$P^T \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} P = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}.$$

Let's write $P = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, then: $(a,b,c,d \in \mathbb{Q})$

$$P^T \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} P = \begin{pmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}.$$

In particular, we need:
$a^2+b^2 = 3$, where $a,b \in \mathbb{Q}$.
But (we claim) this equation has no rational solns.

To continue, we need:
Theorem (Fermat Sum of Squares Theorem)
Let n be a positive integer. Then, $x^2+y^2 = n$ has an integer solution with $x, y \in \mathbb{Z}$ if and only if $n = m^2 p_1 p_2 \cdots p_k$, where $m \in \mathbb{Z}$, and $p_1, \ldots, p_k$ are distinct primes where $p_i \not\equiv 3 \pmod 4$ $\forall 1 \le i \le k$.

So, write $a = x/m$, $b = y/m$, $x,y,m \in \mathbb{Z}$
Then, $a^2+b^2 = 3$ iff $x^2+y^2 = 3m^2$
and $3m^2$ is not of the required form, since $3 \equiv 1 \pmod 4$
$\therefore P$ does not exist (Eck, ... see top of page ...)

Lecture 6:

Strategy (towards same big theorem)
- If a symmetric (v,k,λ)-design exists $\Rightarrow I_v \tilde{=}_Q nI_v + \lambda J_v$ (and so if we can show that some matrix is not congruent, then no symmetric design exists!
- We will show that $I_v \tilde{=}_Q nI_v + \lambda J_v$ iff some smaller matrices are congruent iff some equation has rational solutions (this will require some number theory tools)

Bruck-Ryser-Chowla $\Rightarrow$ If symetric design exists $\Rightarrow$ Some equation has rational solution.

(Today: We will do more on congruence)

Recall: $A \tilde{=}_{\mathbb{Q}} B$ iff $P^T A P = B$, P invertible

For today, we will do everything over $\mathbb{F} = \mathbb{Q}$. and we will write $\tilde{=}$ to mean $\tilde{=}_{\mathbb{Q}}$.

Basic Facts:
- $\tilde{=}$ is an equivalence relation
- $\begin{pmatrix} A_1 & & \\ & A_2 & \\ & & \ddots \\ & & & A_s \end{pmatrix} \tilde{=} \begin{pmatrix} A_{\sigma(1)} & & \\ & A_{\sigma(2)} & \\ & & \ddots \\ & & & A_{\sigma(s)} \end{pmatrix}$ for any permutation σ.

  Block diagonal matrix
- If $A_i \tilde{=} B_i$, $i = 1, \ldots, s$, then $\begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_s \end{pmatrix} \tilde{=} \begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_s \end{pmatrix}$.

Theorem (Witt Cancellation Theorem)

Let
$$A = \left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right), \quad B = \left(\begin{array}{c|c} B_1 & 0 \\ \hline 0 & B_2 \end{array}\right)$$

If $A \simeq B$ and $A_1 \simeq B_1$, and A_1, B_1 invertible, then $A_2 \simeq B_2$.

Bilinear Forms:

Defn Let V be a vector space over $\mathbb{Q}$. A **bilinear form** on V is a map: $\alpha: V \times V \to \mathbb{Q}$ - such that:

$$\alpha(x+ty, z) = \alpha(x,z) + t\alpha(y,z)$$
$$\alpha(x, y+tz) = \alpha(x,y) + t\alpha(x,z)$$

for all $x, y \in V$, $t \in \mathbb{Q}$.

We say α is a **symmetric** form if $\alpha(x,y) = \alpha(y,x)$ $\forall x, y \in V$.

If $x_1, \ldots, x_n$ is a basis for V, the **Gram matrix** of α is $A_{ij} = \alpha(x_i, x_j)$ and we write $A = [\alpha]_{x_1, \ldots, x_n}$.

If we know the Gram matrix of α, then we know α.
To compute $\alpha(u,v)$, we write $u = \sum_{i=1}^{n} a_i x_i$, $v = \sum_{i=1}^{n} b_i x_i$,
then $\alpha(u,v) = \alpha\left(\sum_{i=1}^{n} a_i x_i, \sum_{i=1}^{n} b_i x_i\right)$

$$= \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j \underbrace{\alpha(x_i, x_j)}_{\hookrightarrow \text{Gram matrix.}}$$

Jan 22nd

Proposition: $A, B \in M^{n\times n}$.
$A \sim B$ if and only if there is a vector space V and a bilinear form $\alpha: V\times V \to \mathbb{Q}$ such that
$A = [\alpha]_{x_1,\dots,x_n}$ for some basis $x_1,\dots,x_n$
$B = [\alpha]_{y_1,\dots,y_n}$ —"— $y_1,\dots,y_n$

Proof:
($\Rightarrow$). Suppose $A \sim B$, then $P^t A P = B$ for some invertible matrix P.
Let $\alpha: \mathbb{Q}^n \times \mathbb{Q}^n \to \mathbb{Q}$ where $\alpha(x,y) = x^t A y$.
Let $e_1,\dots,e_n$ be the standard basis for $\mathbb{Q}^n$.
Then $P_{e_1},\dots,P_{e_n}$ is also a basis (cols of P)
We can check that:
$A = [\alpha]_{e_1,\dots,e_n}$, and
$B = [\alpha]_{P_{e_1},\dots,P_{e_n}}$

($\Leftarrow$) Suppose $A = [\alpha]_{x_1,\dots,x_n}$ and $B = [\alpha]_{y_1,\dots,y_n}$ where x, y are two different bases. There is a change of basis matrix P, (P invertible)
$$y_i = \sum_{k=1}^{n} P_{ki} x_k.$$

And we can check that $P^t A P = B$. ∎

Proposition:
The Gram matrix of α is symmetric iff α is a symmetric form.
Proof: Exercise!

Since we're exclusively interested in symmetric matrices, we'll focus on symmetric forms.

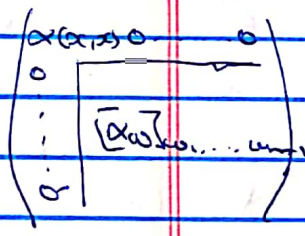
Theorem

Let $\alpha: V \times V \to \mathbb{Q}$ be a symmetric form. There exists a basis $x_1, \ldots, x_n$ for V s.t. $[\alpha]_{x_1, \ldots, x_n}$ is diagonal.

Note: If $W \leq V$ is a subspace, then we get a symmetric form $\alpha_W: W \times W \to \mathbb{Q}$ by restricting α.

Proof:

By Induction.



Base Case: If $\alpha(x,x) = 0$ for all $x \in V$

Using

$$\alpha(x,y) = \frac{\alpha(x+y, x+y) - \alpha(x,x) - \alpha(y,y)}{2}$$

We get $\alpha(x,y) = 0 \quad \forall x, y \in V$

$\therefore$ In any basis, the Gram matrix is $0 \leftarrow$ diagonal

Otherwise (Induction Step):

Let $x \in V$ s.t. $\alpha(x,x) \neq 0$ → This is seemingly any vector, so resulting diagonal matrix is far from unique.

Let $W = \{w \in V \mid \alpha(x,w) = 0\} = \ker \alpha(x, \cdot)$

Since $\alpha(x, \cdot)$ is a rank one linear map, $\dim W = \dim V - 1$.

Note $x \notin W$ (by our assumption that $\alpha(x,x) \neq 0$)

By IH, $\exists$ a basis

$w_1, \ldots, w_{n-1}$ for W. Such that $[\alpha_W]_{w_1, \ldots, w_{n-1}}$ diagonal. Then, since $x \notin W$, $x, w_1, \ldots, w_{n-1}$ is a basis for V and we can check $[\alpha]_{x, w_1, \ldots, w_{n-1}}$ is diagonal

□

Corollary:
Every symmetric matrix is congruent to a diagonal matrix.

BUT, this diagonal matrix is not unique.

Defn (Isometry)
Let α be a symmetric form on V. An invertible linear map $T: V \to V$ is an isometry of α if $\alpha(Tx, Ty) = \alpha(x, y)$ $\forall x, y \in V$.
(We can understand this as if "preserves inner products")

Lemma:
If $x, y \in V$, $\alpha(x,x) = \alpha(y,y) \neq 0$, then there exists an isometry $T: V \to V$ such that $Tx = y$.
Proof: HW Exercise.

Proof: (of with Classification Theorem)

Special Case: $A_1 = B_1 \leftarrow 1 \times 1$ matrix.

$$A = \left(\begin{array}{c|c} c & 0 \\ \hline 0 & A_2 \end{array}\right), \quad B = \left(\begin{array}{c|c} c & 0 \\ \hline 0 & B_2 \end{array}\right), \quad c \in \mathbb{Q}, c \neq 0.$$

By assumption $A \cong B$, so there is a symmetric form $\alpha: V \times V \to \mathbb{Q}$ and bases $x, w_1, \ldots, w_{n-1}$ and $y, z_1, \ldots, z_{n-1}$ such that $A = [\alpha]_{x, w_1, \ldots, w_{n-1}}$ and $B = [\alpha]_{y, z_1, \ldots, z_{n-1}}$.

Note that $\alpha(x,x) = A_{11} = c = B_{11} = \alpha(y,y) \neq 0$ so there is an isometry $T: V \to V$ such that $Tx = y$.

Proof: (Cont)

Let $W = \{z \in V \mid \alpha(y,z) = 0\} = \ker(y,\cdot)$

As before, $\dim W = \dim V - 1$, and since $\alpha(y,z_i) = B_{i,i+1} = 0$, $z_1, \ldots, z_{n-1} \in W$ and they are linearly independent, so they are a basis for W.

Then, $[\alpha_W]_{z_1,\ldots,z_{n-1}} = B_2$.

Also, $\alpha(y, \tau w_i) = \alpha(\tau x, \tau w_i) = \alpha(x, w_i) = A_{1,i+1} = 0$

$\therefore \tau w_1, \ldots, \tau w_{n-1}$ is a basis for W and $[\alpha]_{\tau w_1,\ldots,\tau w_{n-1}} = A_2$

Because $\alpha_W(\tau w_i, \tau w_j) = \alpha(w_i, w_j) = A_{i+1,j+1}$.

$\Rightarrow A_2 \simeq B_2$ (for the special case).

General Case:

Use the fact that $A_1 \simeq B_1 \simeq D$ for some diagonal matrix D. Since A, B invertible, D is invertible. Using the special case, repeatedly cancel all diagonal entries of D to deduce $A_2 \simeq B_2$.

$$\left(\begin{array}{c|c} D & 0 \\ \hline 0 & A_2 \end{array}\right) \simeq \left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right) \simeq \left(\begin{array}{c|c} B_1 & 0 \\ \hline 0 & B_2 \end{array}\right) \simeq \left(\begin{array}{c|c} D & 0 \\ \hline 0 & B_2 \end{array}\right)$$

A $\qquad$ B $\qquad$ $\blacksquare$

Fact that we'll use (and hopefully prove):

$I_n \simeq nI_1$ for all $n \in \mathbb{Z}_{>0}$.

Note: Not true for 6×6 matrices:

If it were:

$$\left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \simeq \left(\begin{array}{cc|cc} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ \hline 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{array}\right)$$

4×4 $\quad$ 2×2 $\quad$ 4×4 $\quad$ 2×2

But by Witt Cancellation, the 2 argument both cancel, and we would be left with $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \simeq \left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right)$, which is false.

Jan 27th

Lecture 7:

The story so far:

(1) If a symmetric (v,k,λ)-design exists then $I_v \simeq nI_v + \lambda J_v$. $(n=k-\lambda)$

(2) With Cancellation:

$$\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} \simeq \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}, \quad A_1 \simeq B_1 \Rightarrow A_2 \simeq B_2$$

(and some invertibility condition)

(3) $I_u \simeq nI_u$ $(n \in \mathbb{Z}_{>0})$. ← Proof next time

Lemma:

If a symmetric (v,k,λ)-design exists, then

$$\left(\begin{array}{c|c} I_v & 0 \\ \hline 0 & -\lambda \end{array}\right) \simeq n \cdot \left(\begin{array}{c|c} I_v & 0 \\ \hline 0 & -\lambda \end{array}\right)$$

$(v+1)\times(v+1)$ matrix

Proof: (Outline)

We already know that if the design exists, then $I_v \simeq nI_v + \lambda J_v$.

$$\Rightarrow \left(\begin{array}{c|c} I_v & 0 \\ \hline 0 & -\lambda \end{array}\right) \simeq \left(\begin{array}{c|c} nI_v + \lambda J_v & 0 \\ \hline 0 & -\lambda \end{array}\right)$$

Using

$$P = \left(\begin{array}{c|c} I_v & \frac{1}{k} \mathbb{1}_v \\ \hline \mathbb{1}_v^T & k \end{array}\right)$$

we can check that

$$\left(\begin{array}{c|c} nI_v + \lambda J_v & 0 \\ \hline 0 & -\lambda \end{array}\right) \simeq \left(\begin{array}{c|c} nI_v & 0 \\ \hline 0 & -n\lambda \end{array}\right).$$

□

Theorem (Bruck-Ryser-Chowla (BRC))

Suppose a symmetric (v,k,λ)-design exists and let $n=k-\lambda$.

(a) If v is even, then n is a square

(b) If $v\equiv 1 \pmod 4$ then the equation $n=a^2-\lambda b^2$ has a solution $(a,b)\in\mathbb{Q}$.

(c) If $v\equiv 3 \pmod 4$ then the equation $n=a^2+\lambda b^2$ has a solution $(a,b)\in\mathbb{Q}$.

Proof:

Remark: Often, (b) and (c) are combined into a single statement:

If v is odd, then the equation:

$n=a^2+(-1)^{\frac{v-1}{2}}\lambda b^2$ has a solution $(a,b)\in\mathbb{Q}$

(But the proofs are completely different)

Proof:

(a) There exists a matrix $P\in M_{v\times v}(\mathbb{R})$ such that

$$P^T\begin{pmatrix} I_v & 0 \\ 0 & -\lambda \end{pmatrix}P = \begin{pmatrix} nI_v & 0 \\ 0 & -n\lambda \end{pmatrix}$$

Taking determinants of both sides

$$\det(P^T)\det\left(\begin{pmatrix} I_v & 0 \\ 0 & -\lambda \end{pmatrix}\right)\det(P) = \det\left(\begin{pmatrix} nI_v & 0 \\ 0 & -n\lambda \end{pmatrix}\right).$$

$$\Rightarrow \det(P)^2\cdot(-\lambda) = n^v(-n\lambda).$$

$$\Rightarrow \det(P)^2\cdot n^v = n.$$ ← LHS is a square since v is even.

$$\det(P)^2 \quad \det(P)^2$$
$$\overline{n^v} \leftarrow \text{if } v=2k \left(\frac{\det(P)}{n^k}\right)^2$$

Proof (cont.)

(b) $(V \equiv 1 \pmod 4)$

Starting with $\begin{pmatrix} I_V & 0 \\ 0 & -\lambda \end{pmatrix} \simeq \begin{pmatrix} nI_V & 0 \\ 0 & -n\lambda \end{pmatrix}$

Using with Cancellation to cancel as many I_V and nI_V's pairs as possible! ($\frac{V-1}{4}$ such blocks)

This gives:

$$\begin{pmatrix} 1 & 0 \\ 0 & -\lambda \end{pmatrix} \simeq \begin{pmatrix} n & 0 \\ 0 & -n\lambda \end{pmatrix}$$

Therefore, $\exists$ invertible matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Q})$ s.t.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -\lambda \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & -n\lambda \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} a^2 - \lambda b^2 & \square \\ \square & \square \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & -n\lambda \end{pmatrix}$$

(other entries don't matter)

$\Rightarrow a^2 - \lambda b^2 = n$ has a solution with $a, b \in \mathbb{Q}$.

(c) Since $\begin{pmatrix} I_V & 0 \\ 0 & -\lambda \end{pmatrix} \simeq \begin{pmatrix} nI_V & 0 \\ 0 & -n\lambda \end{pmatrix}$, then

$$\begin{pmatrix} I_V & 0 & 0 \\ 0 & -\lambda & 0 \\ 0 & 0 & n \end{pmatrix} \simeq \begin{pmatrix} nI_V & 0 & 0 \\ 0 & -n\lambda & 0 \\ 0 & 0 & n \end{pmatrix}$$

$(V+3)\times(V+2)$-matrix

$$\simeq \begin{pmatrix} nI_{V+1} & 0 \\ 0 & -n\lambda \end{pmatrix}$$

$$\begin{pmatrix} I_{V+1} & 0 \\ 0 & \square \end{pmatrix} \longrightarrow$$

By reordering diagonal elements

and $I_{v+1} \simeq nI_{v+1}$ since $v+1$ is a multiple of 4.

$$\Rightarrow \begin{pmatrix} n & 0 \\ 0 & -\lambda \end{pmatrix} \simeq \begin{pmatrix} 1 & 0 \\ 0 & -\lambda n \end{pmatrix}$$

Therefore, $\exists$ an invertible matrix $\begin{pmatrix} p & r \\ q & s \end{pmatrix} \in M_{2\times 2}(\mathbb{Q})$ s.t.

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -n\lambda \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & -\lambda \end{pmatrix}$$

$$\Rightarrow \left(\begin{array}{c|c} p^2 - n\lambda q^2 & \square \\ \hline \square & \square \end{array}\right) = \left(\begin{array}{c|c} n & \\ \hline & \end{array}\right)$$

So $p^2 - n\lambda q^2 = n$.

Claim: $p \neq 0$, since in $p^2 - n\lambda q^2 = n$: p^2 is +ve, $-n\lambda q^2$ is +ve, n is +ve. ($\lambda, q^2 > 0$, so $-n\lambda q < 0$ and $n > 0$, so $p \neq 0$)

Let $a = n/p$ and $b = nq/p$.

Then:

$$n = a^2 + \lambda b^2$$

□

Example: Prove that there is no projective plane of order 6.

Recall:

Projective plane = symmetric $(v, k, 1)$-design.

And order 6 $\Rightarrow k = 7$ and $v = \frac{k(k-1)}{\lambda} + 1 = 43$

So, we want to show that no $(43, 7, 1)$-design exists.

By BRC, if even a design exists then $a^2 + b^2 = 6$ has a solution $a, b \in \mathbb{Q}$ (since $43 \equiv 3 \pmod 4$). But, we've shown that $3 = a^2 + b^2$ has no solution for $a, b \in \mathbb{Q}$, and by same reasoning (Fermat's SOS thm), this equation also has no rational solutions. $\therefore$ Design does not exist

But the Fermat SOS Thm only helps if λ is a square. For other values of λ, we use Legendre's theorem.

Defn (Quadratic Residue)
If $GF(q)$ is a finite field, then

$$QR(q) = \{a^2 \mid a \in GF(q), a \neq 0\}$$

$$a \in GF(q)^\times := a \in GF(q) \setminus \{0\}$$

$QR(q)$ is called the set of quadratic residues in $GF(q)$.

Example:
$q=5$, $GF(5) = \mathbb{Z}_5$, $QR(5) = \{1,4\}$ ← considered modulo 5

Theorem (Legendre)
Suppose A, B, C are nonzero integers such that ABC is square-free (i.e. Not divisible by any perfect square other than 1)
Then TFAE:
(1) $Ax^2 + By^2 + Cz^2 = 0$ has a non-trivial integer solution $(x,y,z) \in \mathbb{Z}^3 \setminus \{0,0,0\}$.
(2) The following conditions hold:
(i) A, B, C do not all have the same sign
(ii) For every odd prime p:
If $p \nmid A$ then $-BC \in QR(q)$ and symmetrically for B and C.

Proof:

($\Leftarrow$) May discuss this direction later.

($\Rightarrow$) Suppose that $Ax^2+By^2+Cz^2=0$ have a non-trivial integer sol'n. Then:

(i) is clear,

For (ii), we may assume $\gcd(x,y,z)=1$. (If they have a common factor, we can divide through by it).

Suppose $p \mid A$, then working modulo p, we have:

$$By^2 + Cz^2 = 0 \pmod p$$

Claim $p \nmid z$.

Proof: Suppose it does, then $By^2 \equiv 0 \pmod p$. and since ABC is squarefree, $p \nmid B$ (otherwise $p^2 \mid ABC$) $\Rightarrow y^2 \equiv 0 \pmod p$

$\Rightarrow p \mid y$.

Then, $\underbrace{Ax^2}_{\text{divisible by } p} + \underbrace{By^2 + Cz^2}_{\text{divisible by } p^2} = 0$,

So, Ax^2 must have an extra factor of p. But A is squarefree so $p^2 \nmid A$ and $\gcd(x,y,z)=1$, so $p \nmid x$.

$\therefore p^2 \nmid Ax^2$, which is impossible

So, $z \neq 0$ in $GF(p)$ and so it is invertible.

$\Rightarrow -BC \equiv (Byz^{-1})^2 \pmod p$

$\Rightarrow -BC \in QR(p)$. ∎

Lecture 8:

Last time:

Legendre's Theorem:

$Ax^2 + By^2 + Cz^2 = 0$ has a non-trivial integer solution

iff

A, B, C doesn't all have the same sign

AND $\forall$ odd primes p,

- If $p \nmid$, then $-BC \in QR(p)$, etc.

Example:

Show that $15 = a^2 + 7b^2$ has no rational solution.

Solution:

Write $a = x/z$, $b = y/z$, $x, y, z \in \mathbb{Z}$.

Then, we need to show:

$$15z^2 = x^2 + 7b^2 \Rightarrow x^2 + 7b^2 - 15z^2 = 0$$

Note: $1 \cdot (7)(-15)$ is squarefree, so we can use Legendre's

Take $p = 3$, then $p \nmid$, but $-AB = -7 \notin QR(3)$.

(Since $QR(3) = \{1\}$, but $-7 \equiv 2 \pmod 3$)

$\therefore$ By Legendre's Thm, this has no sol'n's.

Example:

Show that $5 = 2a^2 + 21b^2$ has no rational solution

Solution:

If we did the same thing as above:

Let $a = x/z$, $b = y/z$. This gives: $2x^2 + 21y^2 - 5z^2 = 0$

But, $2 \cdot 21 \cdot (-5)$ is not squarefree.

Solution: (Cont'd)

Instead, try $a = \frac{1}{6}\cdot\frac{x}{z}$ and $b = \frac{1}{3}\cdot\frac{x}{z}$. This gives:

$$5 = 12\left(\frac{1}{6}\cdot\frac{x}{z}\right)^2 + 21\left(\frac{1}{3}\cdot\frac{y}{z}\right)^2$$

$$\Rightarrow 3x^2 + 7y^2 - 15z^2 = 0$$

And from here, this is just the first example.

Note: Picking the correct rationals is always possible.

Now, let's prove this fact!

Theorem:

$\forall n \in \mathbb{Z}_{>0}$, $n\mathbb{Z}_u \tilde{=}_R \mathbb{Z}_u$.

Recall:

(1) Euclidean algorithm (for gcds)

(2) Complex numbers can be viewed as matrices:

$$a+bi \longleftrightarrow \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Defn

A quaternion is a 4×4 real matrix of the form:

$$A = \begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix}$$

The modulus of A is $|A| = \sqrt{a^2+b^2+c^2+d^2}$

(Caution: $|A| \neq \det(A)$. In fact, $\det(A) = |A|^4$)

Denote the set of all quaternions by $\mathbb{H}$

Properties:

- $\mathbb{H}$ is a vector space over $\mathbb{R}$.

Moreover, if $A, B \in \mathbb{H}$, then:

- $AB \in \mathbb{H}$
- $A^T \in \mathbb{H}$. (This plays the role of complex conjugation)
- If $A \neq 0$, then A is invertible and $A^{-1} \in \mathbb{H}$.
- In fact, $AA^T = A^TA = |A|^2 I_4$.
  Hence, $A^{-1} = \frac{1}{|A|^2} A^T$.
- $|AB| = |A| \cdot |B|$.
- $|A| = 0$ iff $A = 0$.

Defn $A \in \mathbb{H}$ is called a Hurwitz quaternion if:

- $A_{ij} \in \mathbb{Z}$ $\forall i,j$ OR
- $A_{ij} \in \mathbb{Z} + \frac{1}{2}$ $\forall i,j$

Denote the set of all Hurwitz quaternions by $\mathbb{A}$.

Additional Properties:

If $A, B \in \mathbb{A}$, then:

- $A + B \in \mathbb{A}$
- $mA \in \mathbb{A}$, $m \in \mathbb{Z}$
- $AB \in \mathbb{A}$.
- $A^T \in \mathbb{A}$
- $A^{-1} \in \mathbb{A}$ iff $|A| = 1$.
- $|A|^2 \in \mathbb{Z}_{\geq 0}$.
- If $X \in \mathbb{H}$, $\exists$ a Hurwitz quaternion $[X] \in \mathbb{A}$ such that $|X - [X]| < 1$. ("Rounding")

We will prove that there exists a Hurwitz Quaternion $P \in \mathbb{A}$ s.t. $P^T I_4 P = n I_4$
(and in particular this shows $I_4 \sim_{\mathbb{A}} n I_4$ since all entries in $\mathbb{A}$ are rational)

The thing that makes this work is that we can still do the Euclidean Algorithm in $\mathbb{A}$.
Caution: $\mathbb{A}$ is not commutative.

Lemma: (Euclidean Algorithm for Hurwitz Quaternions)
Let $A_0, A_1 \in \mathbb{A}$ ($A_0 \neq 0$). There exists a Hurwitz Quaternion $G \in \mathbb{A}$ satisfying:
(1) $G^{-1}A_0 \in \mathbb{A}$, $G^{-1}A_1 \in \mathbb{A}$ ($\Leftrightarrow G$ is a left divisor of A_0 and A_1)
(2) $G = A_0X_0 + A_1X_1$ for some $X_0, X_1 \in \mathbb{A}$.
We say that G is a left gcd of A_0, A_1.
Proof:
Construct a sequence $A_0, A_1, A_2, \ldots$ as follows:
For $k = 0, 1, 2, \ldots$ define:
$A_{k+2} = A_k - A_{k+1}[A_{k+1}^{-1}A_k]$ (A)
$= A_{k+1}(A_{k+1}^{-1}A_k - [A_{k+1}^{-1}A_k])$ (B)
as long as $A_{k+1} \neq 0$.

Jan 20th

Proof (cont'd)

(A) Shows that $A_k \in \mathcal{A}$

(B) Shows that $|A_{k+2}| < |A_{k+1}|$ (since $|A_{k+1}A_k - \bar{L}A_{k+1}A_k| < 1$)

So, this must terminate, i.e. we have $A_{d+1} = 0$ for some d.

Let $G_k = A_d$ and check that we get (1) and (2).

∎

Lemma

For every odd prime p, there exists $1 \le m < p$, $m \in \mathbb{Z}$, such that and $x, y \in \mathbb{Z}$ such that $1 + x^2 + y^2 = mp$.

Proof: $p = 2$, Exercise, So, assume p odd

Consider 2 lists of numbers

(1) $0^2, 1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$ ← All distinct mod p

(2) $-1-0^2, -1-1^2, -1-2^2, -1-3^2, \ldots, -1-\left(\frac{p-1}{2}\right)^2$ ←

The two lists together have $p+1$ numbers

$\therefore$ $\exists\, x^2$ in first list, $-1-y^2$ in the 2nd list ⟵ two #'s must be congruent to each other (Pigeonhole)

$x^2 \equiv -1-y^2 \pmod{p}$

$\therefore 1 + x^2 + y^2 = mp$

(Check that $m < p$)

↳ True since the #'s we used weren't big enough

∎

Lemma:

For every prime p, there exists a Hurwitz Quaternion G_p s.t. $\overline{G_p} G_p = \sqrt{p}$.

⟷

Proof:

Let $A_0 = \begin{pmatrix} 1 & \dots \\ x & \dots \\ y & \dots \\ 0 & \dots \end{pmatrix} \in \mathbb{A}$ (where x and y are from the previous lemma)

Let $A_1 = pI_4$.

Then, $|A_0| = \sqrt{1+x^2+y^2} = \sqrt{mp}$, $(1 \le m < p)$

$|A_1| = p$

If $p=2$, then $m=1$, so pick $G_p = A_0$.

Otherwise, let G_p be the left gcd of A_0 and A_1.

Since $G_p \in \mathbb{A}$, $G_p^{-1} A_0 \in \mathbb{A}$, $G_p^{-1} A_1 \in \mathbb{A}$

Then:

$$|G_p|^2 |G_p^{-1} \cdot A_0|^2 = |A_0|^2 = mp$$

($|G_p^{-1} \cdot A_0|^2$ must be an integer)

$\therefore |G_p|^2$ divides mp

And, similarly $|G_p|^2 \cdot |G_p^{-1} \cdot A_1|^2 = |A_1|^2 = p^2$, so $|G_p|^2$ divides p^2 and so divides $p = \gcd(p^2, mp)$

Thus, $|G_p| = \sqrt{p}$ or $|G_p| = 1$

To rule out the 2nd case, note that if $|G_p| = 1$, then $G_p^{-1} \in \mathbb{A}$

Write $G_p = A_0 X_0 + A_1 X_1$ $(X_0, X_1 \in \mathbb{A})$

and $A_0^\dagger = A_0^\dagger G_p G_p^{-1} = A_0^\dagger (A_0 X_0 + A_1 X_1) G_p^{-1}$

$$= (mpI_4 X_0 + p A_0^\dagger A_1 X_1) G_p^{-1}$$

$$= p(\underbrace{mI_4 X_0 + A_0^\dagger A_1 X_1}_{\in \mathbb{A}}) G_p^{-1}$$

So, $A_0^\dagger$ is p times a Hurwitz quaternion, but we know what A_0 is! A contradiction.

□.

Jan 24th

Proof (of theorem)

Write $n = p_1 p_2 \cdots p_k$ where $p_1, \ldots, p_k$ primes

Take $P = G_{\mathbb{Z}^{p_1}} G_{\mathbb{Z}^{p_2}} \cdots G_{\mathbb{Z}^{p_k}}$.

Then,

$$|P| = |G_{\mathbb{Z}^{p_1}}| |G_{\mathbb{Z}^{p_2}}| \cdots |G_{\mathbb{Z}^{p_k}}| = \sqrt{n}.$$

So, $P^T I_4 P = P^T P = |P^2| I_4 = n I_4$. □

Lecture 9:

Last time we showed:

$\forall n \in \mathbb{Z}_{\geq 1}$, $\exists$ a Hurwitz quaternion N such that $NN^T = nI_4$.

Corollary (Lagrange's 4-square theorem)

For every $n \in \mathbb{Z}_{\geq 0}$, $\exists\ a,b,c,d \in \mathbb{Z}$ s.t. $n = a^2+b^2+c^2+d^2$.

Proof:

If N has integer coeffs, i.e.

$N = \begin{pmatrix} a & — \\ b & — \\ c & — \\ d & — \end{pmatrix}$, then $NN^T = nI_4 \Leftrightarrow a^2+b^2+c^2+d^2 = n$.

and we're done.

However, if N has $\mathbb{Z}+\frac{1}{2}$ coeffs then this only gives us $n = a^2+b^2+c^2+d^2$, where $a,b,c,d \in \mathbb{Z}+\frac{1}{2}$.

Let:

$$H = \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{pmatrix} \in Hl$$

(and is also a Hurwitz quaternion)

Note that $\frac{1}{2}H \in lA$, $HH^T = 4I_4$, so $UU^T = I_4$, so U is an orthogonal matrix. $\rightarrow$ Can check that U is a unit in lA and $U^6 = 1$. (so $U^{-1} = U^5$).

Exercise: Check that if $A \in lA$, then at least one of the matrices A, $\frac{1}{2}HA$, $\frac{1}{2}H^TA$ has integer coefficients.

(all have same modulus since $U = \frac{1}{2}H$ is orthogonal.)

Now, use whichever matrix has integer coeffs. $\square$.

Hadamard Matrices and Designs:

Defn: A Hadamard Matrix H is an $n \times n$ matrix such that $HH^T = nI_n$, and all entries of H are in $\{1, -1\}$.

Remark: $HH^T = nI_n \iff H^TH = nI_n$ (so H will be normal).

Examples:

(1) ← Not very interesting (1-by-1 matrix)

$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ ← 2×2 matrix

H_2 as defined before.

$\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$ is also a Hadamard matrix.

Defn: A monomial matrix M is an $n \times n$ matrix with entries in $\{0, -1, 0, 1\}$ such that there is exactly one non-zero entry in each row/column.

Note: We can produce more Hadamard matrices by permuting rows/cols or multiplying by -1.

→ Since $HH^T \Rightarrow$ rows of H are orthogonal, so the negative of a row is still orthogonal and similarly with H^TH and cols

Monomial matrices encode this exactly)

Example (Monomial matrix)

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

If H is an $n \times n$ Hadamard matrix and M_1, M_2 are $n \times n$ monomial matrices, then $M_1 H M_2$ is also a Hadamard matrix. We say that H and $M_1 H M_2$ are monomially equivalent.

Example:

Let $H_1 = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$ and $H_2 = \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{pmatrix}$ as defined before

Then, we can get from $H_1 \to H_2$ by:

1) Multiply 1st row by -1
2) Cyclically permute cols 2, 3, 4.

We write this:

$$H_2 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} H_1 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Remark: The smallest n for which there exist 2 $n \times n$ Hadamard matrices which are not monomially equivalent is at $n = 16$.

Proposition:
Every Hadamard matrix is monomially equivalent to one in which any entry in the first row and first column is 1.

Proof:
Multiplying the first row by -1 if necessary we can assume that $H_{11} = 1$.

Now, multiply row i by H_{i1} and multiply col j by H_{1j} for $i = 2, \ldots, m$, $j = 2, \ldots, m$ ∎

A Hadamard matrix in this form is said to be standardized.

Note: Every Hadamard matrix is monomially equivalent to many standardized matrices.

Theorem:
If H is an $m \times m$ Hadamard matrix, then $m = 1, m = 2$ or $m = 4n$.

Proof:
Assume that $m \geq 3$, and H is standardized. Look at the first 3 rows of H.

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & * & * & \cdots & * \\ 1 & * & * & \cdots & * \end{bmatrix}$$ ← 3 rows

There are only 4 possible cols.

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}.$$

Proof: (Cont'd)

Suppose the number of each type is a, b, c, and d respectively. The dot product of any 2 rows of a HM is 0.

$(\text{row } 1) \cdot (\text{row } 2) = a+b-c-d = 0$

$(\text{row } 1) \cdot (\text{row } 3) = a-b+c-d = 0$

$(\text{row } 2) \cdot (\text{row } 3) = a-b-c+d = 0.$

$\Rightarrow a=b=c=d$

and we also know that $a+b+c+d = m \cdot (\text{row } 1)(\text{row } 1)^T$ (from)

and so we see that $m=4a$. □

Remark: More generally, if Q is a $k \times m$ matrix ($k \geq 3$) with ± 1 entries and $QQ^T = mI_k$, then $m=4n$. (the proof is the same).

Kronecker Products of Matrices:

Defn: If A, B are matrices, the Kronecker Product $A \otimes B$ is the block matrix obtained by replacing A_{ij} with block $A_{ij}B$.

Properties:

- Entries of $A \otimes B$ are all possible products of an entry in A with an entry in B.
- Non-commutative, but $A \otimes B$ and $B \otimes A$ are related by permuting rows and columns.

- Associative: $A \otimes (B \otimes C) = (A \otimes B) \otimes C$.
- Bilinear:
$$A \otimes (sB + tC) = sA \otimes B + tA \otimes C$$
$$(sA + tB) \otimes C = sA \otimes C + tB \otimes C.$$
- $(A \otimes B)^T = A^T \otimes B^T$.
- $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$, if RHS makes sense.
Special Case: If x, y are column vectors (i.e. $m \times 1$ matrices), then:
$$(A \otimes B)(x \otimes y) = (Ax) \otimes (By).$$
- If A, B are square matrices then
$$\operatorname{tr}(A \otimes B) = \operatorname{tr}(A)\operatorname{tr}(B)$$
(and $A \otimes B$ is also square).

Theorem:
If H_1 and H_2 are Hadamard matrices, then $H_1 \otimes H_2$ is a Hadamard matrix.

Proof:
$H_1 \otimes H_2$ has ± 1 entries (since the entries are products of ± 1).
To see that it is Hadamard:
$$(H_1 \otimes H_2)(H_1 \otimes H_2)^T$$
$$= (H_1 \otimes H_2)(H_1^T \otimes H_2^T)$$
$$= (H_1 H_1^T) \otimes (H_2 H_2^T)$$
$$= (m_1 I_{m_1}) \otimes (m_2 I_{m_2})$$
$$= m_1 m_2 (I_{m_1} \otimes I_{m_2})$$
$$= m_1 m_2 I_{m_1 m_2}.$$
□

Feb 8th

Lecture 10:

Theorem: For a symmetric (v, k, λ)-design, we have:

$$4n - 1 \leq v \leq n^2 + n + 1$$

$4n-1$: Related to Hadamard matrices

n^2+n+1: either a projective plane or its complement

(where $n = k - \lambda$)

Proof:

The upper bound is achieved by projective planes and their complements. (A266)

For the lower bound, we have

$$v = 1 + \frac{k(k-1)}{\lambda}.$$

$$\Rightarrow v \geq 1 + \frac{(n+\lambda)(n+\lambda-1)}{\lambda} = \frac{n^2-n}{\lambda} + 2n + \lambda.$$

Thinking of v as a function of λ with n fixed, v is minimized when the derivative $= 0$:

$$\frac{\partial}{\partial \lambda}\left(\frac{n^2-n}{\lambda} + 2n + \lambda\right) = 0$$

$$\Rightarrow \lambda = \sqrt{n^2 - n}.$$

So:

$$v \geq \frac{n^2-n}{\sqrt{n^2-n}} + 2n + \sqrt{n^2-n}.$$

$$= 2\sqrt{n^2-n} + 2n = \sqrt{4n^2-4n} + 2n.$$

Is this ever a square?

Yes. Since $4n^2 - 4n + 1 = (2n-1)^2$, is a square.

Proof (cont)

So, we can round the bound up:

$$v \geq \sqrt{4n^2-4n} + 2n$$
$$\geq \sqrt{4n^2-4n+1} + 2n$$
$$= (2n-1) + 2n$$
$$= 4n-1.$$

□

Defn

A Hadamard design is a symmetric design in which $v = 4n-1$.

Proposition:

The parameters of a Hadamard design are (since $v = 4n-1$)

$$(v,k,\lambda) = (4n-1, 2n-1, n-1)$$

OR $(v,k,\lambda) = (4n-1, 2n, n)$

Proof:

Use $v = 1 + \frac{k(k-1)}{\lambda}$ with $v = 4n-1$, $k = n+\lambda$ and solve for λ.

□.

Examples:

(a) The Fano plane is a $(7,3,1)$-design (with $n=2$)

(b) We constructed "projective geometries" (i.e. The design from lines/hyperplanes incidence structure)

This had parameters:

$$\left(\frac{q^{d}-1}{q-1}, \frac{q^{d-1}-1}{q-1}, \frac{q^{d-2}-1}{q-1} \right)$$ q prime power.

Examples (cont'd)

(b) If $q \equiv 2$, this is a Hadamard design.

Theorem: (standardized)

If H is a Hadamard matrix (size $4n$-by-$4n$), then:

(a) $\frac{J+H}{2} = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \\ 1 & & N \end{pmatrix}$

where N is the incidence matrix of a $(4n-1, 2n-1, n-1)$-design.

(b) $\frac{J-H}{2} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \\ 0 & & \end{pmatrix}$

These 2 designs are complements

where N is the incidence matrix of a $(4n-1, 2n, n)$ design

(c) Conversely, if N is the incidence matrix of a $(4n-1, 2n-1, n-1)$-design, then:

$$2\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & N & \\ 1 & & \end{pmatrix} - J$$

is a standardized H.M.

C_{52}

(d) If N' is the IM of a $(4n-1, 2n, n)$-design, then

$$J - 2\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \\ 0 & & N' \end{pmatrix}$$

is a standardized HM.

Proof:

We'll prove (a), the others are similar.

First note:

$$JH^T = \begin{pmatrix} 4n & 0 & \cdots & 0 \\ 4n & 0 & \cdots & 0 \\ \vdots & \vdots & & \\ 4n & 0 & \cdots & 0 \end{pmatrix}$$

→ All orthogonal to $\pm I$

All rows are the same since all rows of J are the same

Since H is standardized, every row of J is the first row of H. And, the rows of H are orthogonal.

$$HJ = \begin{pmatrix} 4n & \cdots & 4n \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$ (By transpose)

Now, consider:

$$\left(\frac{H+J}{2}\right)\left(\frac{H+J}{2}\right)^T = \frac{HH^T + HJ + JH^T + JJ}{4}$$

$$\begin{pmatrix} 4n & & 0 \\ & \ddots & \\ 0 & & 4n \end{pmatrix} = \frac{4nI + \begin{pmatrix} 4n & \cdots & 4n \\ & 0 & \\ & \vdots & \end{pmatrix} + \begin{pmatrix} 4n & & 0 \\ \vdots & & \\ 4n & & \end{pmatrix} + 4nJ}{4}$$

→ $\begin{pmatrix} 4n & \cdots & 4n \\ \vdots & & \vdots \\ 4n & \cdots & 4n \end{pmatrix}$

Feb 5th

Root (Cont'd):

$$= \begin{pmatrix} 4n & 2n & \cdots & 2n \\ 2n & 2n & n & \cdots & n \\ \vdots & n & \ddots & & \vdots \\ 2n & n & \cdots & n & 2n \end{pmatrix} = \left(\begin{array}{c|c} 4n & 2n\mathbb{1}^T \\ \hline 2n\mathbb{1} & n\mathbb{J} + n\mathbb{J} \end{array}\right).$$

On the other hand:

$$\left(\frac{H+\mathbb{J}}{2}\right)\left(\frac{H+\mathbb{J}}{2}\right)^T$$

$$= \left(\begin{array}{c|c} \mathbb{J} & \mathbb{1}^T \\ \hline \mathbb{1} & N \end{array}\right)\left(\begin{array}{c|c} \mathbb{J} & \mathbb{1}^T \\ \hline \mathbb{1} & N^T \end{array}\right)$$

$$= \left(\begin{array}{c|c} 4n & \mathbb{1}^T + \mathbb{1}^T N^T \\ \hline N\mathbb{1} + \mathbb{1} & \mathbb{J} + NN^T \end{array}\right)$$

$\therefore$ $N\mathbb{1} + \mathbb{1} = 2n\mathbb{1}$.
$\mathbb{1}^T + \mathbb{1}^T N^T = 2n\mathbb{1}^T$.
$n\mathbb{J} + n\mathbb{J} = \mathbb{J} + NN^T$.

→ These 2 are just transpose of each other, so one is redundant, we'll just use the 1st and 3rd eqn.

Proof (cont'd)

$\Rightarrow$ $NH = (2n-1)H$ → $k-r$

$NN^T = nI + (n-1)J$ → λ

And these are 2 of the 3 equations that N should satisfy.

To get the 3rd equation, consider:

$$\left(\frac{H+J}{2}\right)^T \left(\frac{H+J}{2}\right)$$

and compute this in 2 ways, this will give ##

$H^T N = (2n-1)H^T$ → k

$N^T N = nI + (n-1)J$

$k-\lambda$, λ

Since N is a 0,1-matrix and satisfies the 3 eqs, we're done ∎

Remark:

Since there are many ways to standardize a Hadamard matrix, we get multiple designs for the same $4n$. These designs may not be isomorphic.

Theorem:

Let $q = 4n-1$ be a prime power (i.e. $q \equiv 3 \pmod 4$)

$QR(q) = \{x^2 \mid x \in GF(q)^\times\}$ → units of $GF(q)$

is a $(4n-1, 2n-1, n-1)$-difference set.

Corollary:
If $4n-1$ is a prime power, then a $4n \times 4n$ Hadamard matrix exists.

Lemma:
Let $x \in GF(q)^\times$:

$$x \in QR(q) \iff x^{\frac{q-1}{2}} = 1$$

$$x \notin QR(q) \iff x^{\frac{q-1}{2}} = -1.$$

In particular:
- If $q \equiv 1 \pmod 4$, then $x \in QR(q) \iff -x \in QR(q)$
- If $q \equiv 3 \pmod 4$, then $x \in QR(q) \iff -x \notin QR(q)$.

Proof:
$GF(q)^\times$ is a group under multiplication of order $q-1$.
(it is also a cyclic group!)

By Cayley's theorem:

$$x^{q-1} \equiv 1 \quad \forall x \in GF(q)^\times$$

$$\Rightarrow \left(x^{\frac{q-1}{2}}\right)^2 \equiv 1$$

$$\Rightarrow \left(x^{\frac{q-1}{2}} + 1\right)\left(x^{\frac{q-1}{2}} - 1\right) = 0$$

$$\Rightarrow x^{\frac{q-1}{2}} \equiv \pm 1.$$

If $x \in QR(q)$. Then $x = a^2$ for some $a \in GF(q)$, so

$$x^{\frac{q-1}{2}} = (a^2)^{\frac{q-1}{2}} = a^{q-1} \equiv 1$$

Proof (cont.) ——— ⊛

Note that $x^{\frac{q-1}{2}} = 1$ is a polynomial eqn of degree $\frac{q-1}{2}$. Therefore, it can have at most $\frac{q-1}{2}$ solutions.

Claim: $|QR(q)| = \frac{q-1}{2}$

Proof:

The squaring map $\varphi : QR(q)^\times \to QR(q)^\times$, $a \mapsto a^2$ is two-to-one,

because $\varphi^{-1}(a) = \{x \in QR(q)^\times \mid x^2 = b\}$

↳ Quadratic, thus has 2 sols, $\pm\sqrt{x}$. □

Since ⊛ has as many solutions as there are quadratic residues, the quadratic residues are the only solutions

∴ If $x \notin QR(q)$, then $x^{\frac{q-1}{2}} \neq 1 \Rightarrow x^{\frac{q-1}{2}} \equiv -1$. (since $x^{\frac{q-1}{2}} \equiv \pm 1$)

Finally, if $q \equiv 1 \pmod 4$, then $x^{\frac{q-1}{2}} \equiv (-x)^{\frac{q-1}{2}} \Leftrightarrow x \in QR(q)$

$\Leftrightarrow -x \in QR(q)$

And if $q \equiv 3 \pmod 4$, $x^{\frac{q-1}{2}} \equiv -(-x)^{\frac{q-1}{2}} \Leftrightarrow x \in QR(q)$

$\Leftrightarrow -x \notin QR(q)$

□.

Lecture 11:

Last time:

Thm: If $q=4n-1$ prime power, $QR(q)$ is a $(4n-1, 2n-1, n-1)$-difference set.

We showed: Lemma: $x \in QR(q) \iff -x \notin QR(q)$ (assuming $x \neq 0$)

In particular, there are $\frac{q-1}{2}$ quadratic residues (or $2n-1$).

So, it remains to show that $\lambda = n-1$ for this (alleged) difference set.

Proof (Thm)

We need to show that this satisfies the definition of a difference set, i.e. For each $x \in GF(q)^\times$, there are $n-1$ ways to write $x = r-s$, $r, s \in QR(q)$.

Equivalently, we must show that there are $(4n-1)$ ways to write $x = a^2 - b^2$ $(a, b \in GF(q)^\times)$.

$\iff x = (a-b)(a+b)$

↑ The factor of 4 comes in since a^2, b^2 have 2 square roots each.

Claim: $x = a^2 - b^2 \iff a = \frac{c + c^{-1}x}{2}$, $b = \frac{c - c^{-1}x}{2}$, where $c \neq 0$

Proof:

($\Rightarrow$) Suppose $x = (a-b)(a+b)$. Put $c = a-b$. Since $x \neq 0$, then $c \neq 0$. Now solve for a, b in terms of x

$$\frac{x}{c} = a+b \quad \Rightarrow \quad \frac{x}{c} + c = 2a$$

$$c = a-b \qquad \frac{x}{c} - c = 2b$$

Proof (thm) (cont)

Proof (claim) (cont)

($\Leftarrow$) Check that

$$\left(\frac{c+c^{-1}x}{2}\right)^2 - \left(\frac{c^{-1}x-c}{2}\right)^2 = x.$$

□

But, we haven't checked that $a, b \neq 0$.

Claim: $ab \neq 0 \Leftrightarrow c^2 \neq \pm x$.

Proof:

If $c^2 = x$, then $b = 0$ and if $c^2 = -x$, then $a = 0$

(Plug x into the formulas for a, b.)

If neither, then neither $a, b = 0$. □

Combining claims (1) and (2), the pairs $(a,b) \in \mathbb{R}^2$ s.t. $x = a^2 - b^2$ $(a, b \neq 0)$ is the # of $c \in \mathbb{R}(a)$ s.t. $c \neq 0$ and $c^2 \neq \pm x$.

Finally, by the lemma, either $x \in \mathbb{R}(a)$ or $-x \in \mathbb{R}(a)$, but not both.

If $x \in \mathbb{R}(a)$, there are 2 values of c s.t. $c^2 = x$ and no values of c such that $c^2 = -x$.

If $-x \in \mathbb{R}(a)$, other way around.

↪

Proof: (Cont.)

Either way, there are 3 values of c that don't work, therefore the # of solutions is $q-3 := (n-1)$ from "good c's".

In particular, this is the same for every value of $x \in QR(q)^*$.

So, it's a difference set

I

Remark:

If $q \equiv 1 \pmod 4$, then the last part of the argument breaks down. Since

$$x \in QR(q) \iff -x \in QR(q)$$

and so there are 5 forbidden values of c (including $c=0$)

And further, if $x \notin QR(q)$ (so $-x \notin QR(q)$), then there is only 1 forbidden value of c ($c \neq 0$).

So, we definitely don't get a ~~different~~ difference set in general if $q \equiv 1 \pmod 4$.

BUT, we can do something slightly different -

Conference Matrices:

Def'n: An $n \times n$ matrix C is a conference matrix if $c_{ii} = 0$, $c_{ij} \in \{1, -1\}$ for $i \neq j$ and $CC^T = (n-1)I_n$.

↘ Dot product of any row w itself.

Note: As with Hadamard matrices, the condition $CC^T = (n-1)I_n$ $\Rightarrow C^TC = (n-1)I_n$

Example:

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

Symmetric

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

Skew Symmetric.

Monomial Equivalence:

If C is a conference matrix, M_1, M_2 monomial matrices [If $M_1 C M_2$ has 0's on the diagonal then its a conference matrix.

(If we think about this for a bit, this condition is true $\Leftrightarrow$ $M_1 M_2$ is a diagonal matrix)

Lecture 12:

Last time:

Conference Matrices

$$C = \begin{pmatrix} 0 & \cdots & \pm 1 \\ \pm 1 & \ddots & \\ & & 0 \end{pmatrix}$$ and satisfy $CC^T = (n-1)I_n$.

Theorem:

If C is an $n \times n$ conference matrix (where $n \geq 2$), then one of the following must be true:

(i) $n \equiv 2 \pmod 4$ and C is monomially equivalent to a symmetric matrix, or.

(ii) $n \equiv 0 \pmod 4$ and C is monomially equivalent to a skew-symmetric matrix.

Proof: (Exercise - Sketch)

Take diagonal monomial matrices M_1, M_2 so that:

$$\tilde{C} = M_1 C M_2$$

$$= \begin{cases} \begin{pmatrix} 0 & 1 & \cdots & 1 \\ \vdots & & * & \end{pmatrix} & \text{if } n \equiv 2 \pmod 4 \\ \begin{pmatrix} 0 & 1 & \cdots & 1 \\ -1 & & * & \end{pmatrix} & \text{if } n \equiv 0 \pmod 4 \end{cases}$$

Now check that $\tilde{C} = \pm \tilde{C}^T$.

To do this, look at rows $1, i, j$ of $\tilde{C}$

$$\begin{bmatrix} 0 & 1 & \cdots & 1 \\ \{ & \{ & & \} \end{bmatrix} \rightarrow 3 \times n \text{ submatrix}$$

The possible columns are:

$$\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\-1\end{pmatrix}, \begin{pmatrix}1\\-1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\\-1\end{pmatrix}, \begin{pmatrix}0\\c_{ij}\\c_{ij}\end{pmatrix}, \begin{pmatrix}1\\0\\c_{ji}\end{pmatrix}, \begin{pmatrix}c_{ij}\\1\\0\end{pmatrix}.$$

These will be ± 1.

Dot product of rows $= 0 \Rightarrow$ Relationship b/w c_{ij} and c_{ji}

$$(c_{ij} = \pm c_{ji})$$

□

A conference matrix is standardized if $c_{1j} = 1$ for $j \geq 2$ and $C = \pm C^T$.

If C is standardized the $(n-1)\times(n-1)$ submatrix obtained by deleting the first row and column is called the core.

Theorem:

If C is a skew-symmetric conference matrix, then $I + C$ is a Hadamard matrix.

Proof:

$I + C$ has only ± 1 entries (since the 0's are only on the diagonal).

And:

$$(I + C)(I + C)^T = I + C + C^T + CC^T.$$

$C + C^T = 0$, since C skew-symmetric

$$= I_n + (n-1)I_n = nI_n.$$

□

Feb 6th

Theorem:

If C is a symmetric correlation matrix:

$$\left(\begin{array}{c|c} C+I & -(C-I) \\ \hline C-I & C+I \end{array}\right)$$

is a Hadamard matrix.

Note:

This should remind us of complex #'s: $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

Proof:

Like the last theorem:

$$\left(\begin{array}{c|c} C+I & -C+I \\ \hline C-I & C+I \end{array}\right)\left(\begin{array}{c|c} C+I & -C+I \\ \hline C-I & C+I \end{array}\right)^T.$$

$$= \left(\begin{array}{c|c} C+I & -C+I \\ \hline C-I & C+I \end{array}\right)\left(\begin{array}{c|c} C^T+I & C^T-I \\ \hline -C^T+I & C^T+I \end{array}\right).$$

$$= \ldots \text{ (Exercise!)}$$

□.

Theorem:
If an $n \times n$ conference matrix exists and $n \equiv 2 \pmod 4$, then $n-1$ is a sum of 2 squares.

(Example: There is no 22×22 conference matrix, since 21 is not a sum of 2 squares)

Proof:
Since $CC^T = (n-1)I_n \Leftrightarrow CJ_nC^T = (n-1)J_n$
$\Rightarrow J_n \simeq (n-1)J_n$

Since $n \equiv 2 \pmod 4$, by Williamson conclusion, we have that $J_2 \simeq (n-1)J_2$
$\Rightarrow$ (By HW Problem 2) $n-1$ is a sum of 2 squares. □

A construction
Let q be a prime power.
Let $a_1, a_2, \ldots, a_q$ be the elements of $GF(q)$ listed in some order
Let P be the $q \times q$ matrix.

$$P = \begin{cases} 0 & \text{if } i=j \\ 1 & \text{if } a_i - a_j \in GR(q) \\ -1 & \text{ow} \end{cases}$$

P is called the Paley matrix of $GF(q)$

Feb 28th

Theorem:
If q is odd, then P is the core of a Standardized conference matrix.
i.e. If $q \equiv 1 \pmod 4$, then

$$\begin{pmatrix} 0 & 1 & \cdots & 1 \\ \vdots & & & \\ \vdots & & P & \\ 1 & & & \end{pmatrix}$$ is a symmetric conference matrix

and if $q \equiv 3 \pmod 4$, then

$$\begin{pmatrix} 0 & 1 & \cdots & 1 \\ -1 & & & \\ \vdots & & P & \\ -1 & & & \end{pmatrix}$$ is a skew-symmetric conference matrix.

Proof: Reduce this to a problem of checking facts about quadratic residues. — Switch to stuff we've already done. ☐

What do we have so far?

any prime power $\longrightarrow$ Conference Matrix $\Longrightarrow$ Hadamard Matrix (May be twice as big) $\Longleftrightarrow$ Hadamard Design.

$q \equiv 3 \pmod 4$ QR Difference Set.

Remark: When $q \equiv 3 \pmod 4$, the two constructions give the same Hadamard matrix.

In Summary:

We can construct $4n \times 4n$ Hadamard matrices when

- (Kronecker Products): $4n = m_1 m_2$ and there exist $m_1 \times m_1$ and $m_2 \times m_2$ HMs
- $4n-1$ is a prime power (QR difference set)
- $2n-1$ is a prime power
  (If $2n-1 \equiv 1 \pmod 4$, use Paley matrix).
  If $2n-1 \equiv 3 \pmod 4$, combine 2 above)

Regular Hadamard Matrices:

A Hadamard matrix H is regular if $H\mathbb{1} = 2h\mathbb{1}$ for some $h \in \mathbb{R}$ (so $\mathbb{1}$ is an eigenvector, and all rows sum to $2h$)

Note: - Any row sum of H is even $\Rightarrow h \in \mathbb{Z}$
- h can be positive or negative

Proposition:

If H is a regular $4n \times 4n$ Hadamard Matrix with $H\mathbb{1} = 2h\mathbb{1}$, then $H^T\mathbb{1} = 2h\mathbb{1}$ and $h^2 = n$.

Proof:

Since $H\mathbb{1} = 2h\mathbb{1}$, $\mathbb{1}$ is an eigenvector of H with eigenvalue $2h$. So, $H^{-1}\mathbb{1} = (2h)^{-1}\mathbb{1}$ (i.e. H^{-1} has $(2h)^{-1}$ as an eigenvalue). But $H^T = (4n)H^{-1} \Rightarrow H^T\mathbb{1} = (4n)H^{-1}\mathbb{1} = \frac{2n}{h}\mathbb{1}$.

Now, compute $\mathbb{1}^T H \mathbb{1} = \mathbb{1}^T H^T \mathbb{1}$
$\mathbb{1}^T(2h)\mathbb{1}$ $\quad$ $\mathbb{1}^T(\frac{2n}{h})\mathbb{1}$
$\Rightarrow 2h = \frac{2n}{h} \Rightarrow$ Both conclusions we want ☐.

Feb 12th

Theorem:
If H is a regular Hadamard matrix, then $\frac{J-H}{2}$ is the incidence matrix of a symmetric design called a Menon design, with parameters $(4h^2, 2h^2-h, h^2-h)$, $h \in \mathbb{Z}$.

Lecture 13:

Linear Spaces:

Let $(V, \mathcal{L})$ be an incidence structure. Call the elements of V points and the elements of $\mathcal{L}$ lines.

For $x, y \in V$, if there is $l \in \mathcal{L}$ incident with both, we say that l joins x and y. If l is unique, we write $l = x \vee y$ (i.e. "join" y)

For $l, m \in \mathcal{L}$, if there is $x \in V$ incident with both, we say that l and m meet at x. If x is unique, we write $x = l \wedge m$ (i.e. "meet" m)

Defn

$(V, \mathcal{L})$ is a linear space if for any 2 distinct $x, y \in V$, there is a unique $l \in \mathcal{L}$ joining x and y. ($x \vee y$ is always defined)

And, $(V, \mathcal{L})$ is a dual linear space if for any 2 distinct $l, m \in \mathcal{L}$, there is a unique point $x \in V$ at which they meet ($l \wedge m$ is always defined)

Example: Every $(v, k, 1)$-BIBD is a linear space

Notes: (1) If $(V, \mathcal{L})$ is a linear space, then any 2 distinct lines meet at 1 or 0 points

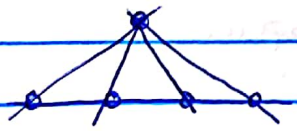
Proof:

If l, m meet at both x and y, then l joins x and y and so does m, so $(V, \mathcal{L})$ is not a linear space.

If l, m do not meet at any point of $l=m$, then we say l and m are parallel.

(2) $(V, \mathcal{L})$ is a linear space $\Leftrightarrow$ its dual is a linear space. So, any statement about linear spaces also apply to dual linear spaces, with the roles of lines/points swapped.

Example: A projective plane is both a linear space and a dual linear space
(because it is symmetric. i.e. Its dual is also a linear space!)
(since it is a $(v, k, 1)$-BIBD)
In this case, $v = n^2+n+1$, $k = n+1$, $\lambda = 1$.

Exercise (In-class)
Find an example of an incidence structure that is linear and dual linear, but not an projective plane
Example:
(a)
(b) 
(c) 

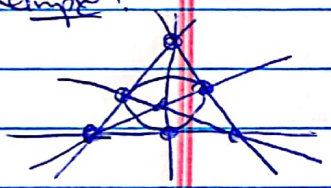
Turns out that apart from those silly examples, the 2 properties: linear and dual linear $\Rightarrow$ projective plane

Defn
A set of points is collinear if they are all incident with a common line.

An s-arc is a set of s points such that no 3 are collinear (Cb doesn't have 3-arcs)

An incidence structure is t-thick if every point lies on at least 3 lines and every line has at 3 points (Cc doesn't have a 4-arc and is not thick)

Example:



The Fano plane has 4-arcs and is thick

These characterize the "trivial" / silly examples. If we throw these out:

Theorem (Characterization of Projective Planes)
TFAE:
(a) $(V, \mathcal{L})$ is linear, dual linear and contains a 4-arc
(b) $(V, \mathcal{L})$ is — " — thick
(c) $(V, \mathcal{L})$ is a symmetric $(n^2+n+1, n+1, 1)$-BIBD.

Proof:

(a) $\Leftrightarrow$ (b) Exercise. (Easy)

(c) $\Rightarrow$ (b) Linear + dual linear we've already shown. It remains to show strict (Exercise)

(Use properties of symmetric designs)

(b) $\Rightarrow$ (c)

Assume (b). Let $l \in \mathcal{L}$ and let $n+1$ be the # of points on l. Let x be any point not on l. (Why does x exist? - Exercise to think about)

There is a bijection btw points on l and lines through x:

$y \mapsto x \vee y$

$m \wedge l \mapsto m$ { Mutual Inverses.

"point on l" "line through x"

$\Rightarrow$ x is on $n+1$ lines

By the same reasoning, any line not through x has $n+1$ points.

Since $(\mathcal{V}, \mathcal{L})$ is strict, for any 2 lines l, m, we can find a point x not on either $\therefore$ All lines have $n+1$ points

Similarly, all points are on $n+1$ lines.

$\therefore (\mathcal{V}, \mathcal{L})$ is a BIBD, with $k = r = n+1$

(Exercise: $v = n^2 + n + 1$)

□

Recall the construction of affine planes:

$V = \mathbb{F}^2$

$\mathcal{B} = \{$affine lines in $\mathbb{F}^2\}$

$= \{x + W \mid \dim W = 1\}$

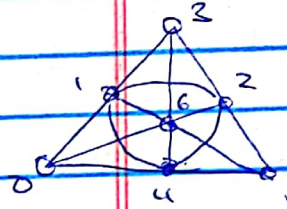
Recall: Derived and Residual designs of a symmetric BIBD

Derived: $(\alpha, \{\beta \cap \alpha \mid \beta \in \mathcal{B} \setminus \{\alpha\}\})$

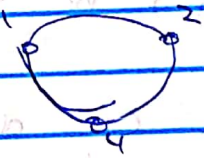
Residual: $(V \setminus \alpha, \{\beta \setminus \alpha \mid \beta \in \mathcal{B}\})$

In the case of the projective plane:
Fix a line $l_\infty \in \mathcal{L}$. The residual with respect to l_∞ is the incidence structure obtained by deleting all points on l_∞ from each line and deleting l_∞ itself.

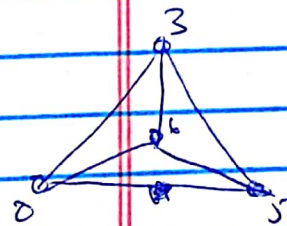
Example:
For Fano Plane:



$l_\infty =$



Residual:



(which is just ~~the~~ K3,3)

Theorem (Characterization of Affine Planes)

TFAE:

(a) $(V, \mathcal{L})$ is a linear space containing a 3-arc and for every line l and every point x, there is a unique line through x parallel to l.

(b) $(V, \mathcal{L})$ is an $(n^2, n, 1)$-BIBD

(c) $(V, \mathcal{L})$ is the residual of a projective plane

Proof:

(c) $\Rightarrow$ (b) Exercise (Figure out pieces of the residual design)

(b) $\Rightarrow$ (a) Assume (b).

If $(V, \mathcal{L})$ is an $(n^2, n, 1)$-BIBD Then,

$$r = \frac{\lambda(v-1)}{k-1} = \frac{1(n^2-1)}{(n-1)} = n+1$$

Let $x \in V$, $l \in \mathcal{L}$. If x is on l, then l is the unique line through x parallel to l.

Else, let $(y_1, \ldots, y_n)$ be the points on l.

Then,

$x y_1, \ldots, x y_n$ are all lines through x that meet l. Since $r = n+1$, there is therefore one more line through x and it doesn't meet l, which is what we went.

Check that $(V, \mathcal{L})$ has a 3-arc.

Next time: (a) $\Rightarrow$ (c).

Lecture 14:

Affine planes:

(a) $(V, \mathcal{L})$ is a linear space containing a 3-arc and "unique parallel lines" axiom

(b) $(V, \mathcal{L})$ is a $(v^2, n, 1)$-BIBD

(c) $(V, \mathcal{L})$ is the residual of a projective plane

Proof:

(b) $\Rightarrow$ (a) Done.

(c) $\Rightarrow$ (b) Done.

Today: (a) $\Rightarrow$ (c)

Let $(V, \mathcal{L})$ be a linear space satisfying axioms of (a).

First we note that parallelism is an equivalence relation. Symmetry + Reflexive are obvious. For transitivity, suppose $l_1 \| l_2$ and $l_2 \| l_3$ but $l_1 \nparallel l_3$, then let $\{x\} = l_1 \cap l_3$. But now l_1 and l_3 are two different parallel lines goes through x, violating the uniqueness axiom.

Call the equivalence class "parallel classes" and write $[l]$ to denote the parallel class of $l \in \mathcal{L}$.

We need to construct a projective plane $(\bar{V}, \bar{\mathcal{L}})$ whose residual is $(V, \mathcal{L})$

Proof: (cont)

$\bar{\mathcal{L}} = \mathcal{L} \cup \{l_\infty\}$ ← New line

$\bar{\mathcal{V}} = \mathcal{V} \cup \{$parallel classes$\}$

$\{\pi_1, \ldots, \pi_{n+2}\}$, where $\pi_1, \ldots, \pi_{n+2}$ are the parallel classes of $(\mathcal{V}, \mathcal{L})$

with the following incidence relations:

- If $x \in \mathcal{V}$, $l \in \mathcal{L}$, incidence is as in $(\mathcal{V}, \mathcal{L})$
- For $x \in \mathcal{V}$, l_∞, x is not incident with l_∞
- For π_i, $l \in \mathcal{L}$ π_i is incident with l iff $l \in \pi_i$.
- For π_i, l_∞ π_i is incident with l_∞

Check that $(\bar{\mathcal{V}}, \bar{\mathcal{L}})$ is linear, dual-linear and has a 4-arc

Ovals and Hyperovals:

Defn Let $\mathcal{C}$ be an s-arc in a projective plane. A

- A secant is a line that contains exactly 2 points of $\mathcal{C}$.
- A tangent —— " —— 1 point of $\mathcal{C}$
- A passant —— " —— 0 points of $\mathcal{C}$.

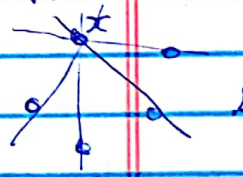
Lemma:

Let $\mathcal{C}$ be an s-arc in a projective plane of order n. Then, every point of $\mathcal{C}$ has $n+2-s$ tangents. In particular, $s \leq n+2$. Moreover if $s = n+2$, then n is even.

Proof:

Let $x \in \mathcal{C}$. There are $n+1$ lines through x. $s-1$ of them are secants and rest are passants (since $x \in \mathcal{C}$)

Example:



So, there are $(n+1)-(s-1)$ tangents

To show the moreover, suppose $s = n+2$, then there are no tangents (since $n+1-s = 0$). So, every line is either a secant or a passant. Let $y \in \mathcal{C}$, every line through y meets $\mathcal{C}$ at an even # of points (0 or 2), so $s = |\mathcal{C}|$ is even. $\Rightarrow$ $n = s-2$ is even. ∎

Defn

An oval is an $(n+1)$-arc in a projective plane of order n.

A hyperoval is an $(n+2)$-arc — " —.

Example:

Let q be a prime power. Let $(V, \mathcal{L})$ be the standard projective plane of order q.

points = 1-dim'l linear subspaces of $GF(q)^3$

lines = 2-dim'l — " —

Write $[x:y:z] = \text{Span}\{(x,y,z) \in V \mid (x,y,z) \neq (0,0,0)\}$.

→

Claim: $\mathcal{O} = \{[x:y:z] \mid xy + yz + xz = 0\}$ is an oval

Proof:

First, note that the intersection b/w any line ℓ and $\mathcal{O}$ is given by a quadratic equation. $\therefore$ ℓ has at most two points of $\mathcal{O}$. $\therefore$ no three points of $\mathcal{O}$ are collinear.

Next: Count points $[x:y:z] \in \mathcal{C}$.

Case 1: $x=0$

Then, $[x:y:z] \in \mathcal{O}$ iff $yz=0$, so either $y=0$ or $z=0$ (but not both)

This gives 2 points $[0:0:1]$, $[0:1:0]$

Case 2: $x \neq 0$.

Rescaling, we can assume $x=1$, then WLOG, $[1:y:z] \in \mathcal{O}$.

iff

$$y + yz + z = 0 \Rightarrow z = -\frac{y}{y+1}.$$

This gives $q-1$ points since $y=-1$ is no good.

In total, this is $q+1$ points, $\therefore$ $\mathcal{O}$ is an oval. $\square$

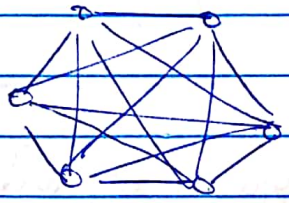
Exercise: If $q = 2^d$, then check that $\mathcal{O} \cup \{[1:1:1]\}$ is a hyperoval.

Feb 26th

Theorem: All projective planes of order 4 are isomorphic

Proof:

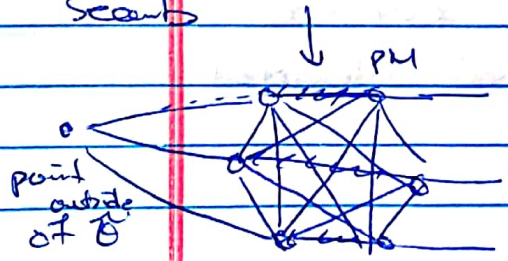
Let $\tilde{\Theta}$ be a hyperoval in a projective plane (V, L) of order 4. Regard points $\tilde{\Theta}$ as vertices of K_6.



Every point/line can be identified with some feature of K_6

Points	Incidence Relation	Lines
6 points on $\tilde{\Theta}$	$\Longleftrightarrow$	15 secants of $\tilde{\Theta}$
6 vertices of K_6	$\Longleftrightarrow$	15 edges of K_6
15 perfect matchings	$\Longleftrightarrow$	6 passants
15 points not on $\tilde{\Theta}$	$\Longleftrightarrow$	1-factorization of K_6

Under each PM corresponds to a unique point since they we have ~~points~~ drew overlapping secants



□

Scanned with CamScanner

Latin Squares:

Defn A latin square of order n is an nxn array in which every row and every column is a permutation of [n]

Example:

1	2	3
3	1	2
2	3	1

is a latin square of order 3

Example: Multiplication table for any group

Notation: We will either use:

- Matrix Notation:

  A_{xy} = Entry in row x, col. y

-or-

- Write $x \circ y$ for entry in row x, col y.

  "Think of $\circ$ as a binary operation"

Defn A latin square is idempotent if $x \circ x = x$

Example: The latin square above is not idempotent.

The following is:

(1)	3	2
3	(2)	1
2	1	(3)

Defn: A latin square is symmetric if $x \circ y = y \circ x$.

Example: Our previous example is also symmetric

Lemma: A symmetric, idempotent latin square of order n iff n is odd

Proof:

($\Leftarrow$) If n is odd, define $x \circ y = \frac{x+y}{2}$ (mod n)

($\Rightarrow$) Conversely, consider the set of pairs $\{\{x,y\} \mid x \circ y = 1\}$

Note: Can't have $1 = x$ elements. (since they are sets)

1-element $\Rightarrow x \circ x \equiv 1$

If a latin square is symmetric and idempotent, then this set contains 1 singleton and $\frac{n-1}{2}$ pairs. So, n is odd

$\square$

Lecture 15:

Recall:

Last time:

∃ symmetric idempotent LS of order n iff n odd

Example:

1 3 2
3 2 1 Order 3
2 1 3

Lemma: ∃ a symmetric LS of order $2n$ s.t.

$$x \circ x = \begin{cases} x & \text{if } 1 \le x \le n \\ x-n & \text{if } n+1 \le x \le 2n \end{cases}$$

Such a Latin Square is called "half-idempotent"

Example:

1 3 2	4 6 5
3 2 1	6 5 4
2 1 3	5 4 6

- Start with an odd order
- Copy on diagonal
- Shift for every other quadrant

4 6 5	1 3 2
6 5 4	3 2 1
5 4 6	2 1 3

Proof: Start with $x \circ y = x+y \pmod{2n}$ and then ← Gives 2,4,6... along diagonal

rename the entries. → Some just have to rename

□

Application:

Recall a Steiner-triple system is a $(v,3,1)$-BIBD

Recall: Necessary conditions $\Rightarrow v \equiv 1$ or $3 \pmod 6$

We can now show that these conditions are sufficient.

Theorem:

If $v \equiv 1$ or $3 \pmod 6$, then a $(v,3,1)$-BIBD exists

Proof:

Case 1 (Base Construction)

Let $v = 3n$ where n is odd. Take a symmetric, idempotent LS of order n, and construct a $(v,3,1)$-BIBD as follows:

Points: $[n] \times [3]$

Blocks: $\{(x,1), (x,2), (x,3)\}$ $x \in [n]$

and

$\{(x,1), (y,1), (xoy, 2)\}$
$\{(x,2), (y,2), (xoy, 3)\}$
$\{(x,3), (y,3), (xoy, 1)\}$

$x, y \in [n]$, $x < y$.

Case 2 (Skolem Construction)

Let $v = 6n+1$ and take a symmetric, half-idempotent LS of order $2n$. Construct a $(v,3,1)$-BIBD as follows:

Points: $[2n] \times [3] \cup \{\infty\}$

Proof Cont'd

Blocks: $\{(x,1),(x,2),(x,3)\}$ $1 \le x \le 2n$

(Copy that we used before) $x,y \in [2n]$ $x \neq y$

$\{(x+n,1),(x,2),\omega\}$

$\{(x+n,2),(x,3),\omega\}$

$\{(x+n,3),(x,1),\omega\}$

And, check that both designs work. □

Orthogonal Arrays: of order n

From a Latin Square we can construct an orthogonal array $OA(n,3)$. This is a $n^2 \times 3$ array whose rows are $(x,y,x \circ y)$, for all $x,y \in [n]$

i.e. row index, col index, entry in LS.

Note: The order of the rows don't matter.

Defn (Orthogonal Array)

An orthogonal array $OA(n,2)$ is an $n^2 \times 2$ array in which the rows are all pairs (x,y) with $x,y \in [n]$, in some order.

An $OA(n,k)$ is an $n^2 \times k$ array in which each pair of columns is an $OA(n,2)$.

We claim that the $n^2 \times 3$ array we write down from a Latin square is equivalent to an $OA(n^2, 3)$.
This is since in $(x_{xy}, \exists x_{xy})$:

(x, y) record the indices, every pair exists here (i.e. this is an $OA(n, 2)$)

(x, x_{xy}) is saying "each row has every element from 1 to n";

(y, x_{xy}) is saying "each col has every element from 1 to n"

Two OAs are equivalent if we can obtain one from the other by permuting rows and columns and apply a permutation of $[n]$ to entries in any column.

From an $OA(n,k)$ A, we associate an incidence structure $([n^2], [n] \times [k])$ in which $i \to (x,j) \iff A_{ij} = x$.
($i \in [n^2]$, $j \in [k]$, $x \in [n]$)
(incidence relation)

Example:

$$\begin{pmatrix} (1,1) \\ (1,2) \\ (2,1) \\ (2,2) \end{pmatrix} \longrightarrow \left(\begin{array}{c|c|c} 01 & 01 & 01 \\ 01 & 10 & 10 \\ 10 & 01 & 10 \\ 10 & 10 & 01 \end{array}\right)$$

(In terms of the incidence matrix)

Replace $1 \to (0,1)$
$2 \to (1,0)$

↑ this is the incidence matrix of the affine plane of order 2

In general, this is not the incidence structure of a BIBD.

The dual design is called a transversal design. Transversal designs have the property that points are partitioned into k "groups" of size n.

Any 2 points from 2 different groups are in a unique block. Two points from the same group are not in a common block.

Application:
Suppose we have a $(v,k,1)$-BIBD (V,B) and we want to construct a $(vk,k,1)$-BIBD.
Start by making k disjoint copies of V
$V' = V \times [k]$
$B' = \{ x \times \{j\} \mid x \in B, j \in [k] \}$
and also add the blocks B'' coming from a transversal design, then:
$(V', B' \cup B'')$ is a $(vk,k,1)$-BIBD

To better understand Odds. Ods.
We will associate

Theorem:
If ~~OA~~ OA(n,k) exists, then $k \leq n+1$.
Equality occurs iff graph is complete.
Proof:
~~For~~ For each $j \in [k]$, the edges colored i & j form n copies of K_n, hence there are $n\binom{n}{2}$ edges colored j.
From the defn of an Od. no edge can have more than 1 color. Hence the graph is simple and has exactly $kn\binom{n}{2}$ edges.

$$kn\binom{n}{2} \leq \binom{n^2}{2} \Rightarrow k \leq n+1$$

Lastly equality occurs iff the graph is complete.

□

Thm

(i) If an $OA(n, n+1)$ exists $(n \geq 2)$, then its incidence structure is an affine plane

(ii) Conversely, for every affine plane of order n, it is the incidence structure of an $OA(n, n+1)$

(iii) If $k < n+1$, then the incidence structure of an $OA(n, k)$ is never a BIBD

Proof:

(i) Let A be an $OA(n, n+1)$. The incidence structure has points $i \in [n^2]$ and lines $(x, j) \in [n] \times [n+1]$ where $i \to (x, j) \Leftrightarrow A_{ij} = x$.

We must show that this is an affine plane.

Since the graph is complete, every pair of points i, i' is joined by a unique edge with some unique color j.

$x = A_{ij} \Leftrightarrow (x, j) = i \vee i'$ ← In particular, $i \vee i'$ is always defined, so this is a linear space

Finally, each line has exactly n points and there are n^2 points in total, so this is an $(n^2, n, 1)$-BIBD. ∎

(ii) and (iii) are exercises. ← This one is easy

Corollary: If an affine plane of order n exists then there exists an $OA(n, k)$ for all $k \leq n+1$.

Product Construction:

If A is an $OA(n, k)$ and B is an $OA(m, k)$, we can construct an $OA(mn, k)$ as follows

Let $* : [n] \times [n] \to [mn]$ be any bijection.

If $(A_{i1}, A_{i2}, \ldots, A_{ik})$ is a row of A and $(B_{i1}, \ldots, B_{ik})$ is a row of B, then

$$(A_{i1} * B_{i1}, \ldots, A_{ik} * B_{ik})$$

will be a row of the new array $A \times B$

Exercise: Check that $A * B$ is an $OA(mn, k)$

Mar 4th

Lecture 16:

Projective Planes of order n $\longleftrightarrow$ Affine Planes of order n

$\Updownarrow$

$OA(n, n+1)$ $\qquad$ $OA(n,3) \longleftrightarrow$ Latin Square of order n.

Example: Construct an $OA(20,5)$.

Sol'n: There exist affine planes of order 4 and 5

$\Updownarrow$ $\qquad$ $\Updownarrow$

Can construct $OA(4,5)$ $\qquad$ Can construct $OA(5,6)$

$\Downarrow$

Delete a column to ~~a set~~ $OA(5,5)$

$\searrow \quad \swarrow$

Product Construction: $OA(20,5)$.

Mutually Orthogonal Latin Squares:

Two ~~orthogonal~~ Latin Squares σ and σ' are orthogonal if:

$(x \circ_4 \ldots x \circ' y) \qquad (x,y) \in [n]^2$

are the rows of an $OA(n,2)$

$\Rightarrow$

Example:

(1)	2	3	4
2	(1)	4	3
3	4	(1)	2
4	3	2	(1)

and

(1)	3	4	2
2	4	3	(1)
3	(1)	2	4
4	2	(1)	3

are orthogonal latin squares

We can check:

(1,1), (2,3), (3,4), ... gives us all the possible pairs

col 1, row 1 col 2, row 1 col 3, row 2

We can also see that each of the 1's in the left are paired with a different # in the right

Note: The question for the first class is asking about mutually orthogonal LSs of order 6!

A set of Latin Squares is mutually orthogonal if every pair of LSs in the set is orthogonal

(In the def'n before, 2 LSs are orthogonal iff $(x,y, x_0y_0, x_0'y') \; (x,y) \in \mathbb{Z}_n^2$ are the rows of an $OA(n,4)$

So, more generally, a set of k mutually orthogonal latin squares (MOLS) is equivalent to an $OA(n, k+2)$

(From the $OA(n, k+2)$, use cols $(1, 2, i)$ to get k MOLS).

From k MOLs, construct the $OA(n, k+2)$ with rows:
$(x, y, xoy, xo'y, xo''y, \ldots)$ $(x,y) \in [n]^2$

Example Continued
Since we can construct an $OA(20, 5)$ we can find 3 MOLs of order 20.

Corollary:
If n is odd or $n \equiv 0 \pmod 4$, then there exist orthogonal Latin Squares of order n.
Proof:
We can write $n = q_1 q_2 \cdots q_s$, where $q_1, \ldots, q_s$ are prime powers and $q_i \geq 3$. There exist an affine plane of order q_i for each $i \Rightarrow$ there exist an $OA(q_i, q_i+1)$
$\Rightarrow OA(q_i, q_i+1)$ since each $q_i \geq 3$.
By the product construction, $\exists OA(n, 4)$, which is equivalent to a pair of orthogonal Latin Squares. □

Turns out that as $n \to \infty$, the maximum # of mutually orthogonal Latin Squares $\to \infty$
Proof: Uses Wilson's theorem

Existence of Designs:

Defn Let v be a positive integer, $k \subseteq \mathbb{Z}_{\geq 2}$. A linear space $(V, \mathcal{B})$ is called a PBD(v,k) (a pairwise balanced design), if $|V| = v$ and $|\alpha| \in k$

Example: A $(v,k,1)$-BIBD is a PBD$(v, \{k\})$

Example: Starting from an OA(n,k), we get a transversal design in which the blocks have size k, and "groups" have size n. Any 2 points of a transversal design are in a common group and a common block, but not both.
Combining groups and blocks, we get a PBD$(nk, \{k,n\})$

(Necessary Conditions)
Proposition:
If PBD(v,k) exists, then
$v-1 \equiv 0 \pmod{\ell}$, and
$v(v-1) \equiv 0 \pmod{m}$
where $\ell = \gcd\{k-1 \mid k \in k\}$ and $m = \gcd\{k(k-1) \mid k \in k\}$

Note: If k is a single element, then we just get the previous conditions for a BIBD: i.e. $v-1 \equiv 0 \pmod{k}$ and $v(v-1) \equiv 0 \pmod{k(k-1)}$

Proof:

This follows from:

$$v-1 = \sum_{\substack{x \in B \\ x \in \alpha}} (|\alpha| - 1) \quad \text{for } x \in V$$

$$v(v-1) = \sum_{\alpha \in B} b|\alpha|(|\alpha|-1)$$

and $\sum_{\substack{x \in B \\ x \in \alpha}} (|\alpha|-1)$ is divisible by l, since by defn. l is a gcd of #'s of this form, and because with $\sum_{\alpha \in B} |\alpha|(|\alpha|-1)$ □

Write $B(K) = \{v \in \mathbb{Z}_{\geq 2} \mid a\ PBD(v,K) \text{ exists}\}$

$K_{lm} = \{v \in \mathbb{Z}_{\geq 2} \mid v-1 \equiv 0 \pmod{l} \text{ and } v(v-1) \equiv 0 \pmod{m}\}$

Def'n: A set K is called PBD-closed if $B(K) = K$.

Example:

- $B(K)$ is PBD-closed ($B(B(K)) = B(K)$)

  Proof:

  First, for all $k \in K$, a $PBD(k, K)$ exists. (Trivial Construction, one block with all the points inside it).

  So, $B(B(K)) \geq B(K)$.

  Suppose we have $v \in B(B(K))$. There exists a $PBD(v, B(K))$, say $(V, \mathcal{B})$. Moreover, for each block $x \in \mathcal{B}$, there exists a $PBD(|x|, K)$ since $|x| \in B(K)$, say $(x, \mathcal{C}_x)$.

  Let $\mathcal{C} = \bigcup_{\alpha \in B} \mathcal{C}_\alpha$. Check that $(V, \mathcal{C})$ is a $PBD(v, K)$. □

- $\{e, m\}$ is PBD-closed:
  Follows from the necessary conditions
  (If a PBD$(v, \{e, m\})$ exists $\Rightarrow v \equiv e \pmod{m}$)
  Exercise: Work through details.

- For any k, λ
  $\{v \mid$ a (v, k, λ)-BIBD exists$\}$
  is PBD-closed
  (Note: case where $\lambda = 1$ is a special case of $B(B(k)) = B(k)\}$,
  i.e. the case $k = \{k\}$)

- For fixed k,
  $\{r \mid$ a $(v, b, r, k, 1)$-BIBD exists$\}$
  is PBD-closed
  Proof: See text

- For fixed s, the set of v s.t. $\exists$ s idempotent
  MOLS is PBD-closed (on HW)

Wilson's Existence Theorem:

Every PBD-closed set K is of the form

$K = K_{1,m} \setminus$ (finite set).

where

$l = \gcd\{k-1 \mid k \in K\}$ and $m = \gcd\{k(k-1) \mid k \in K\}$

In particular, the necessary conditions for the existence of a PBD(v, K) are sufficient with finitely many exceptions.

Example: For which values of v does a $(v,4,2)$-BIBD exist?

Sol'n:

Let K_a be the set of all even v. K is PBD-closed, and moreover since a $(4,4,2)$-BIBD (trivial design) exists and a $(7,4,2)$-BIBD (complement of Fano plane) exists, so $4, 7 \in K$. and we can see that $K = K_{1,6} \setminus$ (finite set) as $K_{1,6} = \{v \mid v \in 1 \pmod 3\}$ and there is no other $K_{1,m}$ such that $K_{1,m} \supsetneq K_{1,6}$

Lecture 17:

Recall:
$(G, +)$ Abelian Group, $D \subseteq G$ difference set
$\rightsquigarrow (G, \mathcal{B})$ $\mathcal{B} = \{g + D \mid g \in G\}$.
symmetric design

The Multiplier Theorem:
Goal: Construct difference sets / prove that they don't exist

Def'n: Let $(V, \mathcal{B})$ be a design.
An automorphism of $(V, \mathcal{B})$ is a permutation $\sigma: V \to V$ that induces a permutation of $\mathcal{B}$. That is to say, there exists a permutation $\tilde{\sigma}: \mathcal{B} \to \mathcal{B}$ s.t. $\tilde{\sigma}(\alpha) = \{\sigma(x) \mid x \in \alpha\}$.
(We assume $\mathcal{B}$ is just a set of sets, i.e. Don't worry about multisets)

Proposition:
Let $(V, \mathcal{B})$ be a design:
$V = \{x_1, \ldots, x_v\}$, $\mathcal{B} = \{\alpha_1, \ldots, \alpha_b\}$
Let $\sigma: V \to V$ and $\tilde{\sigma}: \mathcal{B} \to \mathcal{B}$ be permutations. Let N be the incidence matrix of $(V, \mathcal{B})$. Let P be the permutation matrix of σ and $\tilde{P}$ be the permutation matrix of $\tilde{\sigma}$.
Then, σ is the automorphism of $(V, \mathcal{B})$ with induced permutation $\tilde{\sigma}$ iff: $PN = N\tilde{P}^T$.
Pf:
Check:
$(PN)_{ij} = \begin{cases} 1 & \text{if } \sigma^{-1}(x_i) \in \alpha_j \\ 0 & \text{o/w} \end{cases}$ and $(N\tilde{P}^T)_{ij} = \begin{cases} 1 & \text{if } x_i \in \tilde{\sigma}(\alpha_j) \\ 0 & \text{o/w} \end{cases}$

$\Rightarrow$ ⊙

We are interested in the case where the design comes from a difference set $D \subseteq G$.

Example: For any $h \in G$, the map $\sigma(g) = h+g$ is an automorphism of $(G, \mathcal{B})$

Note: If $(G, \mathcal{B})$ is a design coming from difference set $D \subseteq G$, then $D \in \mathcal{B}$
↳ $0+D$.

Moreover, every block $D' \in \mathcal{B}$ is also a difference set and gives rise to the same design.

Define an integer $m \in \mathbb{Z}$ is a multiplier of $(G, \mathcal{B})$ if $\sigma(g) = mg$ is an automorphism.

$$mg := \begin{cases} \underbrace{g + \cdots + g}_{m \text{ times}} & \text{if } m \geq 0 \\ \underbrace{-g - g - \cdots - g}_{m \text{ times}} & \text{if } m < 0 \end{cases}$$

Proposition:
If $(G, \mathcal{B})$ comes from the difference set $D \subseteq G$, then TFAE:
(1) m is a multiplier for the design
(2) $mD \in \mathcal{B}$.
(3) $mD = h+D$ for some $h \in G$

$\hookrightarrow$

Proof:

(2) ⇒ (3) Easy

(1) ⇒ (2) Also easy

(3) ⇒ (1) Suppose $mD = h+D$. Consider $\sigma: G \to G$, $\sigma(g) = mg$ and $\tilde{\sigma}: \mathcal{B} \to \mathcal{B}$, $\tilde{\sigma}(\alpha) = m\alpha$ (equiv. $\tilde{\sigma}(g+D) = mg + h + D$)
$= \{\sigma(x) \mid x \in \alpha\}$

We need to show

(A) σ is a permutation

(B) $\tilde{\sigma}$ is ——"——

(A): σ is a map from $V \to V$, so it suffice to show that σ is surjective - Let $x \in G$. Since D is a difference set, can write $x = g_1 - g_2$, $g_1, g_2 \in D$.

Also,

$x = \underbrace{(h+g_1)} - \underbrace{(h+g_2)}$, where $(h+g_1), (h+g_2) \in h+D = mD$

multiples of n.

$\therefore h + g_1 \in mD \subseteq \text{image}(\sigma)$ and likewise with $h+g_2$.

So, x is the difference of elements in image(σ) and this is a subgroup of G, this implies $x \in \text{image}(\sigma)$. So, σ is surjective.

(B): It suffices to show that $\tilde{\sigma}$ is injective. Suppose

$\tilde{\sigma}(g+D) = \tilde{\sigma}(g'+D) \Rightarrow \underbrace{mg+h+D} = \underbrace{mg'+h+D}$

Since symmetric designs are simple, this implies that these 2 blocks must be the same:

$\Rightarrow mg+h = mg'+h \Rightarrow mg = mg' \Rightarrow \sigma(g) = \sigma(g')$

Proof.

And since $\tilde{\tau}$ is a permutation (by (A)), $g=s'$. This proves $\tilde{\sigma}$ is injective.

□

Example: (Fano Plane)

$G = \mathbb{Z}/7$, $D = \{0, 1, 3\}$

Claim: 2 is a multiplier.

This is because:

$2D = \{0, 2, 6\} = 6 + D$

is a block of the design.

Claim: 3 is not a multiplier.

This is because:

$3D = \{0, 3, 2\} \notin B$.

Note: We could also use $D' = \{1, 2, 4\}$ to construct the Fano Plane and

$2D' = \{2, 4, 1\} = D'$.

~~Super easy to see that 2 is a multiplier.~~

In this case, we say that D' is fixed by the multiplier 2.

Theorem:
Let (G, B) be a design from a difference set.
(i) For every multiplier m, there is a block $D \in B$ s.t. $mD = D$
(ii) If $\gcd(v, k) = 1$, then $\exists D \in B$ s.t. $mD = D$ for every multiplier m.

Proof:
$\sigma : G \to G$ $\qquad \tilde{\sigma} : B \to B$.
(i) Let $\sigma(g) = mg$ and $\tilde{\sigma}(x) = mx$. Assuming m is a multiplier, σ is an automorphism with induced permutation $\tilde{\sigma}$.
In terms of matrices:

$$PN = NP^T$$

Since (G, B) is a symmetric design, N is invertible,

$$P^T = N^{-1} P N$$

So, P, P^T are similar and have the same eigenvalues.
$\therefore$ σ and $\tilde{\sigma}$ have the same cycle type
Now, σ has a fixed point: $\sigma(0) = 0$, so $\tilde{\sigma}$ has a fixed point, i.e. $\exists D \in B$ s.t. $\tilde{\sigma}(D) = mD = D$.

(ii) Let $\varphi : B \to G$ be the map $\varphi(x) = \sum_{g \in x} g$
Claim: If $\gcd(v, k) = 1$, the φ is a bijection
Proof: (Exercise)
Then, the $D = \varphi^{-1}(0)$ and check that $mD = D$ for every multiplier m. ∎

(3)

Putting this all together:

Upshot is that constructing difference sets with a given multiplier m is easy.

WLOG, we can assume that D is fixed by the multiplier. Then, D must be a union of orbits of the map $g \to mg$.

Example:

Construct a projective plane of order 4 via a difference set with multiplier 2.

Soln:

The difference set has params $(21, 5, 1)$

Let $G = \mathbb{Z}_{21}$. The orbits of $x \to 2x$ are:

$\{0\}$, $\{1, 2, 4, 8, 16, 11\}$, $\{3, 6, 12\}$

$\{5, 10, 20, 19, 17, 13\}$,

$\{7, 14\}$, $\{9, 18, 15\}$

The only possibilities are $D = \{3, 6, 12, 7, 14\}$ or $D = \{9, 18, 16, 7, 14\}$ (since $|\{1, 2, 4, 8, 16, 11\}| = |\{5, 10, 20, 19, 17, 13\}| = 6 > 5$)

Check: Both choices of D work

(If they did, it shows that those ~~exist~~ no difference set w multiplier 2)

03/07

The Multiplier Theorem (Hall-Ryser)

Let D be a (v,k,λ)-difference set in an abelian group G, of order $n = k-\lambda$. If p is a prime such that $p > \lambda$ and $p \mid n$, then p is a multiplier.

Example:

(So, $p=2$ was chosen specifically in the previous example)

Example:

If $n=0$ (mod 6), prove that there is no $(n^2+n+1, n+1, 1)$-difference set.

Sol'n

Suppose D is such a difference set. By the multiplier theorem, 2 and 3 are both multipliers. Since $\gcd(v,k) = \gcd(n^2+n+1, n+1) = 1$, we may assume $D = 2D = 3D$. But now, take any $x \in D$, $x \neq 0$. Since $D = 2D$, $2x \in D$ and since $D = 3D$, $3x \in D$. But now, $x = (3x - 2x) = (2x - x)$ contradicts that $\lambda = 1$.

Lecture 18:

Multiplier Theorem: ((G abelian group)
If $D \overset{\text{diff}}{\subseteq} G$ is a (v,k,λ)-difference set and p is a prime s.t. $p > \lambda$ and $p \nmid (n = k-\lambda)$, then p is a multiplier for D.

We consider matrices whose rows and columns are indexed by elements of G.

Note that the points of the design associated to D are the elements of G.
The blocks $B = \{g+D \mid g \in G\}$ are also indexed by elements of G.
$\therefore$ The incidence matrix $\overset{\text{most}}{A}$ naturally viewed as a matrix with rows/cols indexed by G.

Definition and Facts:
For $g \in G$, let X^g be the matrix

$$(X^g)_{ab} = \begin{cases} 1 & \text{if } a-b = g \\ 0 & \text{o/w} \end{cases}$$

$(a,b \in G)$
This construction have the following properties:
- X^g is a permutation matrix.
  (Every row/col has exactly one 1)
- $(X^g)^T = (X^g)^T$ (since it is a permutation matrix and further, $(X^g)^T = X^{-g}$ $(-g \in G)$

- If $g, h \in G$, then
  $X^g X^h = X^{gh}$

Let $\mathbb{G} = \text{Span}\{X^g \mid g \in G\}$

- $\mathbb{G}$ is closed under multiplication

($\mathbb{G}$ is isomorphic to the group algebra of G)

- X^g are the only permutation matrices in $\mathbb{G}$

For $S \subseteq G$, write $X^S = \sum_{g \in S} X^g \in \mathbb{G}$

(Caution: $X^{-S} \neq (X^S)^{-1}$)

↑ Take all the elements in S and negate them.

Instead, $X^{-S} = (X^S)^T$.

- $X^\emptyset = I$
- $X^G = J$
- $X^D = N \iff$ Proof: $(X^D)_{ab} = \sum_{\substack{g \in D \\ a-b=g}} 1 = \begin{cases} 1 & \text{if } a-b \in D \\ 0 & \text{o/w} \end{cases}$

$a \in b+D \iff a-b \in D$

↑ Incidence matrix

Proof (Multiplier Theorem)

P is a multiplier

$\Leftrightarrow pD = gH$ for some $g \in G$

$\Leftrightarrow X^{pD} = X^{gH} \left(= \sum_{h \in D} X^{gh} = X^g \sum_{h \in D} X^h\right)$

$\Leftrightarrow X^{pD} = X^g X^D$

$\Leftrightarrow X^{pD} X^{-D} = X^g \underbrace{X^D X^{-D}}_{= N \cdot N^T}$ (Since $X^{-D} = N^T$ is invertible)

$= nJ + \lambda J$.

$\Leftrightarrow X^{pD} X^{-D} = X^g (nI + \lambda J)$

$X^g \cdot \lambda J = \lambda J$ since X^g is a permutation matrix

$\Leftrightarrow X^{pD} X^{-D} = nX^g + \lambda J$. ← fo

$\Leftrightarrow X^{pD} X^{-D} - \lambda J = nX^g$ ← We want to prove this!

We will show that $\frac{1}{n}(X^{pD} X^{-D} - \lambda J)$ gives a permutation matrix (Since X^g is a permutation matrix)

Let $M = X^{pD} X^{-D} - \lambda J$.

We will show that if $p > \lambda$ and $p \nmid n$, then:

① M has nonnegative entries, and $\Leftrightarrow \frac{1}{n} M$ has nonnegative entries

② $MM^T = n^2 I$ ($\Leftrightarrow \frac{1}{n} M$ is orthogonal).

Together, ① and ② $\Rightarrow \frac{1}{n} M$ is a permutation matrix.

and since $\frac{1}{n} M \in G$, it must be X^g for some $g \in G$.

Ca

②

Proof: (cont)

Proof of ①.

Consider M modulo p.

Although it is not true that $X^{pD} = (X^D)^p$, it is true that $X^{pD} \equiv (X^D)^p \pmod{p}$.

Recall: that $(\sum x_i)^p \equiv \sum x_i^p \pmod{p}$

Example:

$$(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$$
$$= x^5 + y^5 \pmod{5}.$$

Here:

$$(X^D)^p = \left(\sum_{g \in G} X^g\right)^p$$
$$= \sum_{g \in G} (X^g)^p \pmod{p}$$
$$= \sum_{g \in G} \underbrace{X^g \cdots X^g}_{p \text{ times}} \pmod{p}$$
$$= \sum_{g \in G} X^{pg} = X^{pD}.$$

So,

$$M \equiv (X^D)^p \cdot X^{-D} - XJ \pmod{p}$$
$$\equiv (X^D)^{p-1} \underbrace{X^D X^{-D}}_{NN^T} - XJ \pmod{p}$$
$$\equiv (X^D)^{p-1} (nJ + XJ) - XJ \pmod{p}$$
$$\underbrace{\quad}_{=0, \text{ since } p|n}$$
$$\equiv (X^D)^{p-1} XJ - XJ.$$

↪

Proof: (Cont'd)

$\equiv \lambda((X^D)^{p-1}J - J) \pmod p$

$\hookrightarrow X^D J = D^N J = \lambda J = (\alpha+\lambda)J$

$\equiv \lambda((\alpha+\lambda)^{p-1}J - J) \pmod p$

$\equiv \lambda((\alpha+\lambda)^{p-1} - 1)J \pmod p$

$\equiv 1$ (By FLT)

$\equiv 0 \pmod p$

$\hookrightarrow$ Zero matrix.

So, every entry of M is divisible by p.

And also:

$M = \underbrace{X^D X^{-D}}_{\text{has nonnegative entries}} - \lambda J$

all entries of M are $\geq -\lambda$.

Since $p > \lambda$, there are no negative multiples of p that are $\geq -\lambda$

$\therefore$ Every entry of M is ≥ 0.

Proof of (2).

Recall $v = (\alpha + \frac{k(k-1)}{\lambda}) = 1 + \frac{(\alpha+\lambda)(\alpha+\lambda-1)}{\lambda}$

$\equiv 1 + \frac{\lambda(\lambda-1)}{\lambda} \pmod p$ (λ invertible mod p since $p > \lambda$ and p prime)

$\equiv \lambda \pmod p$

$\therefore \gcd(v, p) = 1$.

(3)

Proof: (cont'd).

It follows that pD is a difference set

(key point: $\exists q \in \mathbb{Z}$ such $pq \equiv 1 \pmod{v}$ and $\forall x$

$p s_1 - p s_2 = x$ iff $s_1 - s_2 = qx$

$\Rightarrow$ # of ways to write x as a difference in pD

$\Rightarrow$ # ____ " ____ qx as a difference in D)

$\therefore X^{pD}$ is the incidence matrix of a symmetric (v,k,λ)-BIBD.

Also, X^{-D} is the incidence matrix of a symetric (v,k,λ)-BIBD

Exercise: If N_1, N_2 are the incidence matrices of 2 (possibly different) symmetric (v,k,λ)-designs, then $H = N_1 N_2 - \lambda J$ must satisfy $HH^T = n^2 I$.

(and so ② follows)

$$HH^T = (N_1 N_2 - \lambda J)(N_1 N_2 - \lambda J)^T$$
$$= (N_1 N_2 - \lambda J)(N_2^T N_1^T - \lambda J)$$
$$= \ldots \text{ (crunch it out)}$$

∎

Open (?) Problem: We used that $p > \lambda$ to deduce $\gcd(v,p) = 1$. Can we replace $p > \lambda$ by the weaker condition $\gcd(v,p) = 1$? Clearly, the proof doesn't work, but there are no known counterexamples!

Missed a definition in lecture 15 (there's a big blank chunk):

Application: suppose we have a $(v, k, 1)$ BIBD $(\mathcal{V}, \mathcal{B})$, and we want to construct a $(vk, k, 1)$ BIBD. Start by making k distinct copies of $\mathcal{V}$.

$$\mathcal{V}' = \mathcal{V} \times [k]$$

$$\mathcal{B}' = \{\alpha\{j\} : \alpha \in \mathcal{B}, j \in [k]\}$$

Add blocks $\mathcal{B}''$ coming from a transversal design, $(\mathcal{V}, \mathcal{B}' \cup \mathcal{B}'')$ is a $(vk, k, 1)$ BIBD.

To better understand OAs, we will associate a edge-coloured graphs.

- Vertices: $[n^2]$, rows of the OA
- Edges: make an edge $\{i, i'\}$ coloured $j \in [k]$ if $A_{ij} = A_{i'j}$.

This graph determines the OA up to equivalence.

References

[1] Douglas R. Stinson. *Combinatorial designs: constructions and analysis*. Springer, 2004.