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

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

(Today: We will do more on congruence)

Recall: $A \simeq_{\mathbb{F}} B$ iff $P^T A P = B$, P invertible

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

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

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

Theorem (Witt Cancellation Theorem)

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

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:

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

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

If we know the Gram matrix of α, then we know α. To compute $\alpha(u,v)$, we write $u = \sum_1^n a_i x_i$, $v = \sum_1^n b_i x_i$, then

$$\alpha(u,v) = \alpha\left(\sum^n a_i x_i, \sum^n b_i x_i\right) = \sum_{i=1}^n \sum_{j=1}^n a_i b_j \underbrace{\alpha(x_i, x_j)}_{\text{Gram matrix.}}$$

Jan 22nd

Proposition: $A, B \in M^{n\times n}$.
$A \simeq B$ 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 $A \simeq B$, then $P^TAP = B$ for some invertible matrix P.
Let $\alpha: \mathbb{Q}^n \times \mathbb{Q}^n \to \mathbb{Q}$ where $\alpha(x,y) = x^TAy$.
Let $e_1,\dots,e_n$ be the standard basis for $\mathbb{Q}^n$.
Then $Pe_1,\dots,Pe_n$ is also a basis (columns of P)
We can check that:

$A = [\alpha]_{e_1,\dots,e_n}$, and

$B = [\alpha]_{Pe_1,\dots,Pe_n}$

($\Leftarrow$) 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 $P^TAP = B$. $\square$

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

80

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

Proof:

By Induction.

$$\begin{pmatrix} \alpha(x,x) & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & [\alpha_W]_{w_1, \ldots, w_{n-1}} & \\ 0 & & & \end{pmatrix}$$

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

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

Otherwise (Inductive Step):

Let $x \in V$ s.t. $\alpha(x,x) \neq 0$

This is seemingly any vector so the 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 the 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.

$\square$

Jan 22nd

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

BUT, this diagonal matrix is not unique.

Def'n (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 product")

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

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 $Tx = y$.

<u>Proof</u>: (cont)

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

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

Then $[\alpha_W]_{z_1,\dots,z_n} = B_2$.

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

$\therefore Tw_1, \dots, Tw_{n-1}$ is a basis for W and $[\alpha]_{Tw_1,\dots,Tw_{n-1}} = A_2$

(because $\alpha_W(Tw_i, Tw_j) = \alpha(w_i, w_j) = A_{i+1,j+1}$).

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

<u>General Case</u>:

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 $A_2 \simeq B_2$.

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

$\blacksquare$

Fact <u>that we'll use</u> (and hopefully prove):

$$I_n \simeq n I_1 \quad \text{for all } n \in \mathbb{Z}_{>0}$$

<u>Note</u>: Not true for 6×6 matrices:

If it were:

$$\begin{pmatrix} \underbrace{1 \;\cdots\; }_{4\times 4} & 0 \\ 0 & \underbrace{I_2}_{2\times 2} \end{pmatrix} \simeq \begin{pmatrix} \underbrace{3 \;\cdots\; }_{4\times 4} & 0 \\ 0 & \underbrace{3}_{2\times 2} \end{pmatrix},$$

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