1 Your First Day Of Co-op

Today we will talk about designs. Before we formally introduce the question we will try to answer today, let's consider some examples.

Example 1.1

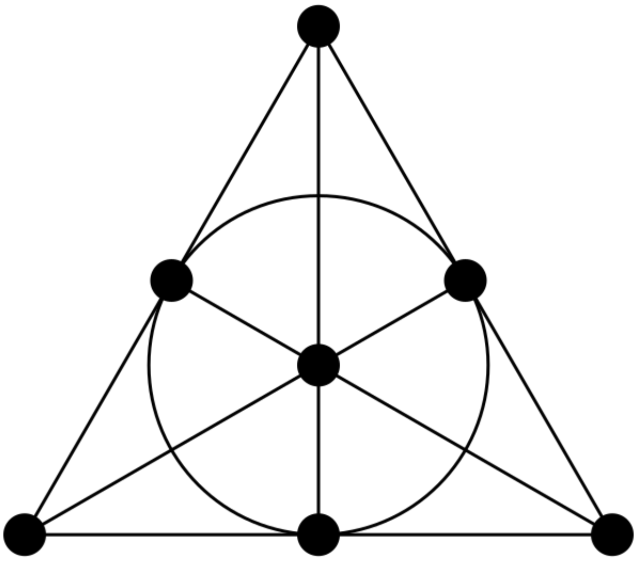
Let's recall the game (that I never played before) called "Spot It". Here is the rule:

1. We have b many cards, on each card k many distinct symbols coming from a set of v many symbols in total.
2. Any two cards always only share one common symbol.
3. The goal of the game is to be the first one to find out the common symbol.

Now, say you are hired as a co-op student for a card game, and you boss turns to you and say, "we want to make a "spot it" game with the following rules":

1. b many cards, on each card there is k many distinct symbols, with a total of $b = v$ many symbols.
2. each symbol must appear in exactly r many cards.
3. each pair of symbols must appear in exactly λ card.

Here is an example (this is called the Fano plane) with $b = v = 7$, $k = 3$, $r = 3$ and $\lambda = 1$:



Here the dots means symbols, lines means cards, dots on the line means that symbol is in that card.

Your boss says, "your task is very simple, design a similar game as above, but with bigger parameters, in particular, I want $r = 7$ and $\lambda = 1$".

Is this possible?

Here is another example.

Example 1.2

Suppose you are hired to taste wines, say v different kind of wines.

If you drink too many wines in one day, you lose the ability to distinguish them, as they all just become taste the same. Say you can only taste k kind of wines each day.

The goal is to figure out a way to compare each pair of wines exactly once.

Here is one example of such design: say $v = 7, k = 3$, and the wines are labelled $P = \{0, 1, 2, ..., 6\}$. Then on day i, we taste:

1. $0, 1, 3$
2. $1, 2, 4$
3. $2, 3, 5$
4. $3, 4, 6$
5. $4, 5, 0$
6. $5, 6, 1$
7. $6, 0, 2$

By doing this, we ended up with comparing each pair of wines exactly once (e.g. we have done comparing 3 and 5 on day 3).

Remark 1.3: Observations

- This is very systematic, as day 2 is just all the numbers in day 1 plus 1 mod 7 and so on.
- From this design, we can get many other designs, simply add 1 to all the numbers above, and mod 7. So day 1 becomes tasting $1, 2, 4$ and so on.
- We cannot pick any three elements and get such a design, for example if day 1 is $\{0, 1, 2\}$ then in day 2 we are overlapping in tasting.
- In short, what we are doing is just given a finite set P, we find some collection of subsets of P, subject to certain regularity conditions.

What do I mean by regularity conditions? Observe:

1. each of the day (we call them blocks) has 3 points from P
2. each point in P is in 3 blocks
3. each pair of points is in exactly one block

Now let's turn this into a definition:

Definition 1.4

A ***design*** is a pair $(V, \mathscr{B})$ such that:

1. V is a finite set, where the elements of V are called ***points***
2. $\mathscr{B}$ is a multiset of subsets of V called ***blocks***

Definition 1.5

A design is ***simple*** if $\mathscr{B}$ is a set, i.e. no repeated blocks.

Definition 1.6

Let $t \in \mathbb{N}$, then a ***t-design*** is a design in which all blocks have the same size, and there exists a constant λ_t so every t-tuple of distinct points lies in exactly λ_t blocks.

In particular, we see the wine tasting example is both a 1-design and 2-design of the set $P = \{0, 1, 2, ..., 6\} = \mathbb{Z}/7\mathbb{Z}$.

Definition 1.7

A ***BIBD*** (short for ***balanced incomplete block design***) is a design $(V, \mathscr{B})$ which is both a 1-design and 2-design.

Remark 1.8: Parameters Of BIBD

We have five parameters for BIBD, namely (v, b, r, k, λ):

1. $v = |V|$ is the number of points
2. $b = |\mathscr{B}|$ is the number of blocks (note $b = \lambda_0$)
3. $r = \lambda_1$ is the number such that every point is in r many blocks
4. $k = |\alpha|$ is the size of blocks
5. $\lambda = \lambda_2$ is the number such that each pair of points is in λ many blocks

In short, we will often write (v, k, λ)-design instead of (v, b, r, k, λ), and call v, k, λ the primary parameters, and b, r the secondary parameters.

Question 1.9

Now your coop question turns into the following: Can we find a BIBD with $\lambda = 1$, $v = b$ and $r - \lambda = 6$?

Definition 1.10

A BIBD is ***symmetric*** if $v = b$.

Okay, so we want to study designs. We note we will introduce a lot of black boxes.

2 Basic Designs

Proposition 2.1

Let V be BIBD design with parameters (v,b,r,k,λ). Then:

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. We only show (3). Let $x\in V$ and consider the set S of pairs (y,α) where $y\in V\backslash\{x\}$ and α is a block contains x,y. We can count this set in two ways:

1. If r_x is the number of blocks containing x, then we get a pair for each such block α, and each element of α other than x. Thus we have $|S|=r_x(k-1)$
2. If $y\in V\backslash\{x\}$, then we have λ blocks containing both x and y, so $|S|=(v-1)\lambda$.

But then we see

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

But then $r=r_x$ as V is BIBD.

Using this, for our problem we immediately conclude the following:

$$\frac{v}{k}=\frac{b}{r}\Rightarrow\frac{1}{k}=\frac{1}{r}\Rightarrow k=r=7$$

Next, we see

$$\frac{v-1}{k-1}=\frac{r}{\lambda}\Rightarrow v-1=(k-1)\cdot\frac{r}{\lambda}=42\Rightarrow v=b=43$$

Thus, at this point, we already know what the configuration must be, for our BIBD design, i.e. it must be a $(43,43,7,7,1)$-design.

How do we show it exists or not?

3 Interlude: Linear Algebra

This is a linear algebra course, so of course we will use linear algebra to our aid!

Here is how you translate a design into a linear algebra problem:

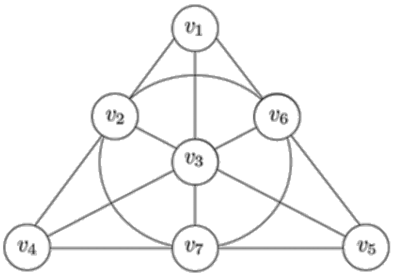
Definition 3.1

Let $(V, \mathscr{B})$ be a design with $V = \{x_1, ..., x_v\}$ and $\mathscr{B} = \{\alpha_1, ..., \alpha_b\}$, the ***incidence matrix*** of this design is a $v \times b$ matrix $M = (m_{ij})_{i,j}$ given by

$$m_{ij} = \begin{cases} 1 & \text{if } x_i \in A_j \\ 0 & \text{otherwise} \end{cases}$$

Example 3.2

The Fano plane



has incidence matrix

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

Definition 3.3

Let $\mathbb{F}$ be a field, A, B be two n by n $\mathbb{F}$-matrices. We say A, B are congruent over $\mathbb{F}$ if we can find invertible n by n $\mathbb{F}$-matrix P suc hthat

$$P^T A P = B$$

In this case we write $A \approx_{\mathbb{F}} B$.

Example 3.4

Over $\mathbb{Q}$, we have the following:

1. $\mathrm{Id}_2 \approx_{\mathbb{Q}} 5\,\mathrm{Id}_2$
2. $\mathrm{Id}_2 \not\approx_{\mathbb{Q}} 3\,\mathrm{Id}_2$

> Here is why: for $5\,\mathrm{Id}_2$, we just use
>
> $$P = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}$$
>
> For $3\,\mathrm{Id}_2$, set
>
> $$P = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$
>
> Then we see $P^T \,\mathrm{Id}_2\, P = 3\,\mathrm{Id}_2$ implies $a^2 + b^2 = 3$. There are no rational solution to this and hence it is impossible.

Next, we need bring out some very big guns, that we definitely does not have time to prove in the tutorial, but the proof is included in the appendix.

To save space, we will write I_n for the identity matrix, and J_n for the n by n matrix with all entries equal 1.

Proposition 3.5

If a symmetric (v,k,λ)-design exists, then $I_v \approx_{\mathbb{Q}} n \cdot I_v + \lambda \cdot J_v$.

Proof. Appendix.

Theorem 3.6: Witt Cancellation

Let $A = \mathrm{diag}(A_1, A_2)$ and $B = \mathrm{diag}(B_1, B_2)$ be n by n symmetric matrices with diagonal block matrices. Suppose $A \approx_{\mathbb{Q}} B$ and $A_1 \approx_{\mathbb{Q}} B_1$ and A_1, A_2 are invertible, then $A_2 \approx_{\mathbb{Q}} B_2$.

Here symmetric matrix means $A = A^T$.

Proof. Appendix

Theorem 3.7

For all $n \geq 1$, $I_4 \approx_{\mathbb{Q}} nI_4$

Proof. Appendix

4 Finale

Now, we are ready to answer your first day co-op question!

Lemma 4.1

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

$$\begin{bmatrix} I_v & 0 \\ 0 & -\lambda \end{bmatrix} \approx_{\mathbb{Q}} n \cdot \begin{bmatrix} I_v & 0 \\ 0 & \lambda \end{bmatrix}$$

Proof. If such design exists, then by Proposition 3.5 we get $I_v \approx_{\mathbb{Q}} nI_v + \lambda J_v$. But then if we let

$$P = \begin{bmatrix} I_v & \frac{\lambda}{k}\vec{1}_v \\ \vec{1}_v^T & k \end{bmatrix}$$

we get

$$\begin{bmatrix} nI_v + \lambda J_v & 0 \\ 0 & -\lambda \end{bmatrix} \approx_{\mathbb{Q}} n \begin{bmatrix} I_v & 0 \\ 0 & -\lambda \end{bmatrix}$$

Here $\vec{1}_n$ is the column vector filled with 1 of length n. This concludes the proof as we also have

$$\begin{bmatrix} I_v & 0 \\ 0 & -\lambda \end{bmatrix} \approx_{\mathbb{Q}} \begin{bmatrix} nI_v + \lambda J_v & 0 \\ 0 & -\lambda \end{bmatrix}$$

Theorem 4.2: Bruck-Ryser-Chowla

Suppose a symmetric (v, k, λ)-design exists. Let $n = k - \lambda$, then:

1. *If v is even, then $n := k - \lambda$ must be a square*
2. *If $v \equiv 1 \pmod 4$, then the equation $n = a^2 - \lambda b^2$ has a rational solution $(a, b) \in \mathbb{Q}^2$*
3. *If $v \equiv 3 \pmod 4$, then the equation $n = a^2 + \lambda b^2$ has a solution $(a, b) \in \mathbb{Q}^2$*

Proof. **DONT PROVE POINT 1 SINCE THEY DONT KNOW DETERMINANTS!!!!!**

(1): There exists $P \in M_n(\mathbb{Q})$ invertible such that

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

Now take determinants, we see $\det(P)^2 \cdot (-\lambda) = n^v(-\lambda n)$. Thus we see $\det(P)^2 = n^{b+1}$ where v is odd. Since n^{v+1} is a square with $v+1$ odd, we must have n is a square.

(2): Start with the equation

$$\begin{bmatrix} I_v & 0 \\ 0 & -\lambda \end{bmatrix} \approx_{\mathbb{Q}} n \begin{bmatrix} I_v & 0 \\ 0 & -\lambda \end{bmatrix}$$

We use Witt Cancellation Theorem 3.6 to cancel out as many I_4 with nI_4 as possible. Since $v \equiv 1 \pmod 4$, this left us with equation

$$\begin{bmatrix} 1 & 0 \\ 0 & -\lambda \end{bmatrix} \approx_{\mathbb{Q}} \begin{bmatrix} n & 0 \\ 0 & -n\lambda \end{bmatrix}$$

This is the same as we can find invertible 4 by 4 matrix

$$P = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

such that

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

Compare the $(1,1)$-entry of this equation we obtain our rational solution $a^2 - \lambda b^2 = n$ as desired.

(3): Similar. But this time, since $v \equiv 3 \pmod 4$, we need to patch our diagonal matrices. Namely, we start with

$$\begin{bmatrix} I_v & 0 \\ 0 & -\lambda \end{bmatrix} \approx_{\mathbb{Q}} n \begin{bmatrix} I_v & 0 \\ 0 & -\lambda \end{bmatrix}$$

Then by adding a diagonal $\operatorname{diag}(1, n)$ at the end, we obtain the following equation

$$\begin{bmatrix} I_v & & & \\ & -\lambda & & \\ & & 1 & \\ & & & n \end{bmatrix} \approx_{\mathbb{Q}} \begin{bmatrix} nI_v & & & \\ & -\lambda n & & \\ & & 1 & \\ & & & n \end{bmatrix}$$

Now, for the matrix on the left, we can swap the location of 1 and $-\lambda$ and still get congruent relation, and on the right we can swap the location of n and $-\lambda n$ and get a congruent relation. Thus we get

$$\begin{bmatrix} I_{v+1} & & \\ & -\lambda & \\ & & n \end{bmatrix} \approx_{\mathbb{Q}} \begin{bmatrix} nI_{v+1} & & \\ & -\lambda n & \\ & & 1 \end{bmatrix}$$

Now use Witt Cancellation we get

$$\begin{bmatrix} -\lambda & 0 \\ 0 & n \end{bmatrix} \approx_{\mathbb{Q}} \begin{bmatrix} -\lambda n & 0 \\ 0 & 1 \end{bmatrix}$$

Apply the definition of congruence, we obtain the desired equation and find a rational solution as desired.

Theorem 4.3

There does not exists a symmetric $(43, 7, 1)$*-design.*

Proof. For the sake of contradiction, say there exists such a design. Then we see $v = 43$ and so $v \equiv 3 \pmod 4$. By the above theorem, we must have a rational solution $(a, b) \in \mathbb{Q}^2$ to the equation $6 = a^2 + b^2$. But this is ballock, says our number theorist friends, by the following theorem.

Theorem 4.4

Let n be a positive integer. Then the equation $x^2 + y^2 = n$ has solution in $\mathbb{Z}$ iff $n = m^2 p_1 ... p_l$ with $m \in \mathbb{Z}$ and p_i distinct primes and $p_i \not\equiv 3 \pmod 4$.

1 Appendix

Proposition 1.1

$(V, \mathscr{B})$ is an (v, b, r, k, λ)-BIBD iff its incidence matrix N satisfies the following conditions:

1. *$N1_b = r1_v$, where 1_b is the column vector of size b contains all 1, and 1_r is the column vector of size 4 contains all 1.*
2. *$1_v^T N = k1_b^T$ where 1_v^T is transpose.*
3. *$NN^T = (r-\lambda)\,\mathrm{Id}_v + \lambda\lambda J_v$ where J_m is the $m \times m$ matrix contains all 1.*

Proof.

$$N1_b = \begin{bmatrix} \sum_{j=1}^b N_{1j} \\ \vdots \\ \sum_{j=1}^b N_{vj} \end{bmatrix}$$

and so $N1_b = r1_v$ iff $\sum_{j=1}^b N_{ij} = r$ for all $i = 1, \ldots, v$ iff x_i lies in exactly r blocks for all i.

Similarly, $1_v^T N = k1_b^T$ iff each block has k points.

Finally, consider NN^T. We see $(NN^T)_{ii}$ is equal

$$\sum_{j=1}^b N_{ij}N_{ij}^T = \sum_{j=1}^b N_{ij}^2 = \sum_{j=1}^b N_{ij}$$

So $(NN^T)_{ii} = r$ for all i iff the first condition holds.

For $i \neq j$, we see

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

where in the last sum, it is equal 1 iff x_i and x_j are both in α_l. Hence, the last sum is the number of blocks containing both x_i and x_j. Thus $(NN^T)_{ij} = \lambda$ iff every pair of distinct points lies in λ many blocks.

Thus (1) to (3) are equivalent to the three conditions defining a BIBD.

Lemma 1.2

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