Abstract

In this talk, I will introduce the theory of balanced incomplete block designs (BIBDs).

I'll show some of their basic properties, demonstrate an elegant construction through finite projective and affine planes, and use them to study three seemingly unrelated problems, one about a family card game, one about projection sizes of partitions of the unit square, and one about secure secret sharing.

No prior knowledge about combinatorial designs is required.

Basic Combinatorial Designs and Applications

Presenter: Harry Sha

November 23, 2022

Table of Contents

The Motivating Problems

BIBDs

(Finite) Projective Planes

Secret Sharing

Spot It![1]

Here's the game -

- I have a deck of cards. Each card has 8 (distinct) objects.
- I reveal two cards at a time.
- First person to shout out the unique shared object wins

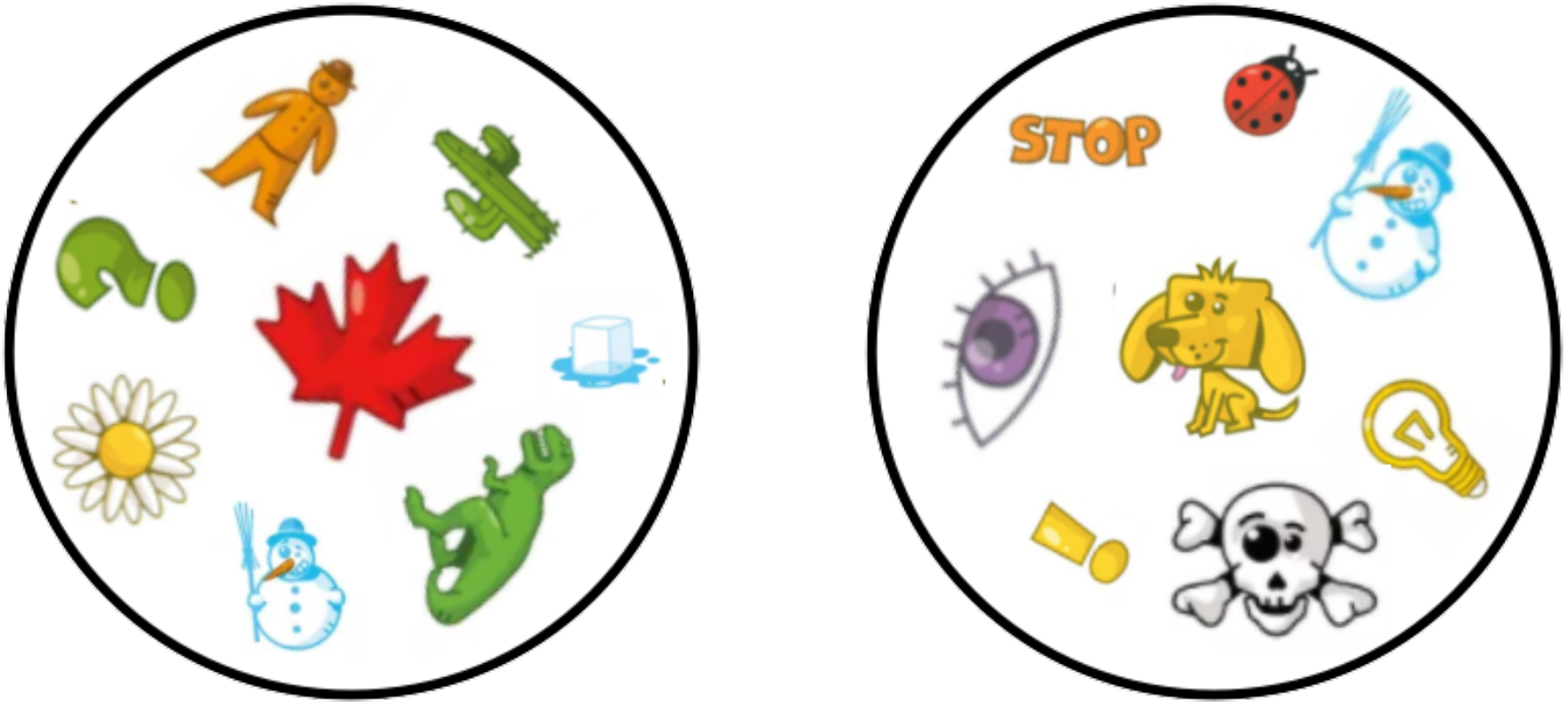
[1] I found this problem from a blog post by Joel Grus.

Spot It!

Ready?

Spot It!

Spot It!



Source: https://www.sfu.ca/~jtmulhol/teaching-musings.html

Spot It!

Every two cards share exactly one object, so there's no ambiguity and no possibility of a 'failed round.'

Questions:

- How many cards can we have relative to the total number of objects and number of objects per card?
- How can we design Spot It! decks?

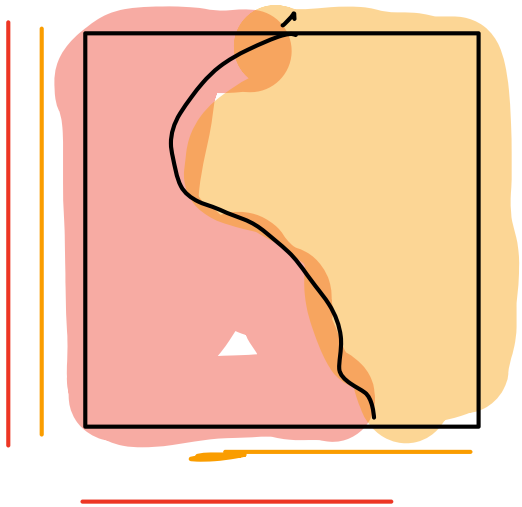
Shadows[2]

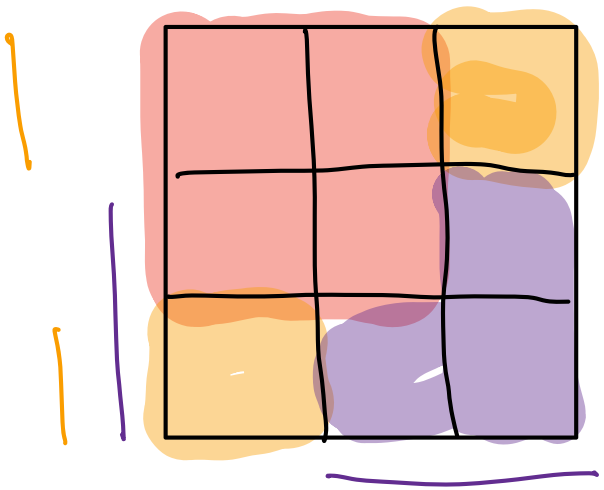
Consider a partition of the unit square $[0,1]^2$ into n parts.

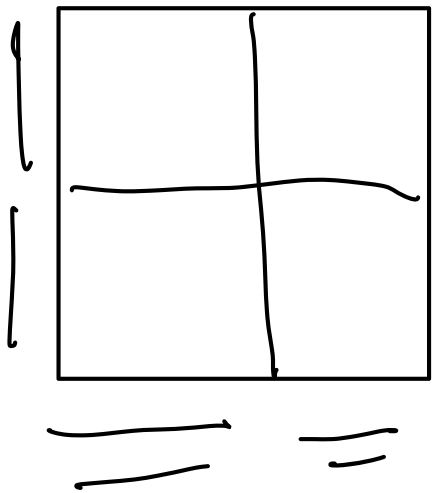
Each part casts a shadow on the horizontal axis and the vertical axis. We want to find a partition that minimizes the length of any of the $2n$ shadows.

[2] This is a problem I am working on

Examples $n = 2, 3, 4$







$n=7$?

Secret Sharing[3]

Goal: split a secret among w people such that you need at least t people to recover the secret (and no group of $t-1$ or fewer people can learn ANYTHING about the secret).

A scheme that does this is a (t, w)-secret sharing scheme.

[3] This is a classic.

Examples

w is the number of peoples
t is the minimum number of people required

password $\longrightarrow$ pa , ss , wo , rd . ✗

$t = w$: secret $\alpha \in \{0,1\}^n$:

$k_1, \ldots, k_w \in \{0,1\}^n$,

$$P_i = (\alpha \oplus k_1 \oplus \ldots \oplus k_w, k_i)$$

$t = 2$? size of the share is $N = 2^n$

$$\Theta(w^2 \log(N))$$

The Motivating Problems

BIBDs

(Finite) Projective Planes

Secret Sharing

This presentation is based on *Combinatorial Designs: Constructions and Analysis* by Douglas Stinson

Definition (Balanced Incomplete Block Design)

Let v, k, λ be positive integers such that $v > k \geq 2$. Let X be a set of size v and $\mathcal{A} \subseteq \binom{X}{k}$. Elements of X are called points, and elements of $\mathcal{A}$ are called blocks. $(X, \mathcal{A})$ is a (v, k, λ)-BIBD if

every pair of distinct points is contained in exactly λ blocks.

Definition (Balanced Incomplete Block Design)

Let v, k, λ be positive integers such that $v > k \geq 2$. Let X be a set of size v and $\mathcal{A} \subseteq \binom{X}{k}$. Elements of X are called points, and elements of $\mathcal{A}$ are called blocks. $(X, \mathcal{A})$ is a (v, k, λ)-BIBD if

every pair of distinct points is contained in exactly λ blocks.

balance :

Explanation of the name:

- Balanced because of the property in bold
- Incomplete because $k < v$, i.e. no block is the full set V.

Definition (Balanced Incomplete Block Design)

Let v, k, λ be positive integers such that $v > k \geq 2$. Let X be a set of size v and $\mathcal{A} \subseteq \binom{X}{k}$. Elements of X are called points, and elements of $\mathcal{A}$ are called blocks. $(X, \mathcal{A})$ is a (v, k, λ)-BIBD if

every pair of distinct points is contained in exactly λ blocks.

Explanation of the name:

- Balanced because of the property in bold
- Incomplete because $k < v$, i.e. no block is the full set V.

Question: Do BIBDs exist, and how can we construct them?
Question: Is there a $(9, 5, 1)$-BIBD?

Parameters of BIBDs

- v. Number of points.
- k. Block size.
- λ. Number of blocks containing a pair of points.
- r. Number of blocks containing a single point. This is called the replication number
- b. Number of blocks.

In this talk, we mostly care about $\lambda = 1$.

Example

v. Number of points.
k. Block size.
λ. Number of blocks containing a pair of points.

$$X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$\mathcal{A} = \{0123, 0145, 0246, 0378, 0579,$$
$$0689, 1278, 1369, 1479, 1568,$$
$$2359, 2489, 2567, 3458, 3467\}$$

$(X, \mathcal{A})$ is a $(10, 4, 2)$-BIBD.

Example

v. Number of points.
k. Block size.
λ. Number of blocks containing a pair of points.

$X = [v]$, $\mathcal{A} = \binom{[v]}{k}$.
$(X, \mathcal{A})$ is a $(v, k, \binom{v-2}{k-2})$-BIBD.

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

v. Number of points.
k. Block size.
λ. Number of blocks containing a pair of points.
r. Number of blocks containing a single point.

Strategy: Fix x, and let r_x be the number of blocks in which x appears. Count the number of times (x, y) appears in a block.

1. $\lambda(v-1)$
2. $r_x(k-1)$.

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

v. Number of points.
k. Block size.
λ. Number of blocks containing a pair of points.
r. Number of blocks containing a single point.

$$b = \frac{vr}{k}$$

v. Number of points.
k. Block size.
r. Number of blocks containing a single point.
b. Number of blocks.

Strategy: Let b be the number of blocks, and write out each block. How many points did we write down?

$bk = vr$

$$b = \frac{vr}{k}$$

v. Number of points.
k. Block size.
r. Number of blocks containing a single point.
b. Number of blocks.

Divisibility Conditions

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

These basic properties of BIBDs place restrictions on which BIBDs can exist. I.e. r and b have to be integral $\Longrightarrow$

- $\lambda(v-1)$ must be divisible by $k-1$, and
- $\lambda v(v-1)$ must be divisible by $k(k-1)$.

Divisibility Conditions

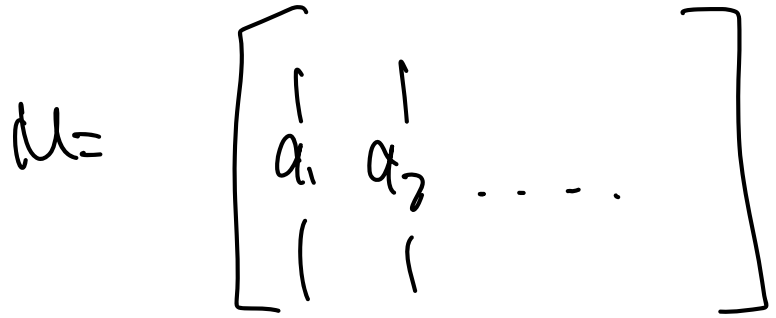
$$r = \frac{\lambda(v-1)}{k-1}$$
$$b = \frac{vr}{k}$$

These basic properties of BIBDs place restrictions on which BIBDs can exist. I.e. r and b have to be integral $\Longrightarrow$

- $\lambda(v-1)$ must be divisible by $k-1$, and
- $\lambda v(v-1)$ must be divisible by $k(k-1)$.

For example, to answer the question from earlier, there is no $(v = 9, k = 5, \lambda = 1)$-BIBD

Incidence Matrices and Duals



Definition (Incidence Matrix)

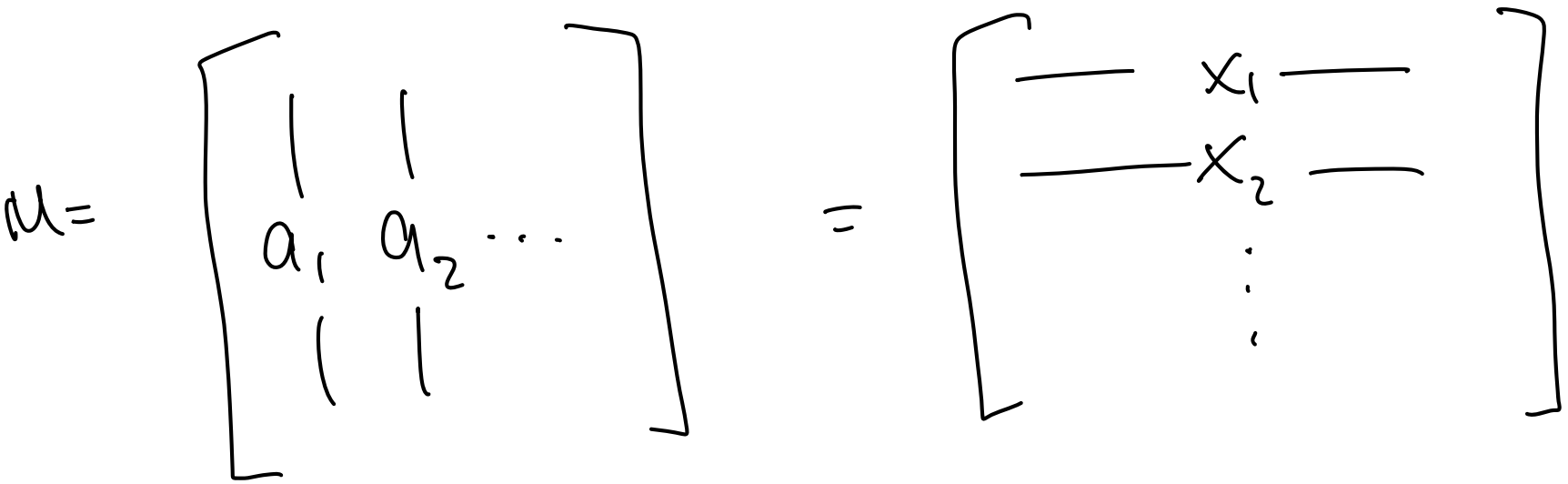
The incidence matrix for a (v, k, λ)-BIBD is a matrix $M \in \mathbb{R}^{v \times b}$ where

$$M_{ij} = \begin{cases} 1 & i\text{th point is in the } j\text{th block} \\ 0 & \text{else} \end{cases}$$

Definition (Dual)

The dual of a (v, k, λ)-BIBD is a design with incidence matrix M^T.

Diagram



row sums = r

col sum = k.

for every two rows ∃ λ cols for which there's a 1 in both rows.

dual

row sums = ~~r~~ k

col sum = ~~k~~ . r cols

for every two ~~rows~~ raw ∃ λ ~~cols~~ for which the

rows.

Properties of the dual

$$M_{ij} = \begin{cases} 1 & i\text{th point is in the } j\text{th block} \\ 0 & \text{else} \end{cases}$$

Let $(X, \mathcal{A})$ be a (v, b, r, k, λ)-BIBD, and let $(Y, \mathcal{B})$ be the dual. Then

- there are b points and v blocks.
- every block $B \in \mathcal{B}$ has size r.
- every point $v \in Y$ occurs in k blocks.
- every pair of blocks intersect in exactly λ-points.

Properties of the dual

$$M_{ij} = \begin{cases} 1 & i\text{th point is in the } j\text{th block} \\ 0 & \text{else} \end{cases}$$

Let $(X, \mathcal{A})$ be a (v, b, r, k, λ)-BIBD, and let $(Y, \mathcal{B})$ be the dual. Then

- there are b points and v blocks.
- every block $B \in \mathcal{B}$ has size r.
- every point $v \in Y$ occurs in k blocks.
- every pair of blocks intersect in exactly λ-points.

If $\lambda = 1$, letting Y be the set of objects and $\mathcal{B}$ be the set of cards, we get a valid Spot It! deck of v cards and b objects.

Fisher's Inequality

Theorem (Fisher's Inequality)

If $(X, \mathcal{A})$ *is a* (v, k, λ, r, b)*-BIBD, then* $v \leq b$.

Fisher's Inequality

Theorem (Fisher's Inequality)

If $(X, \mathcal{A})$ is a (v, k, λ, r, b)-BIBD, then $v \leq b$.

I.e., the number of cards is at most the number of objects.

Proof

Strategy: Show the incidence matrix, a $v \times b$ matrix has rank v.

$b \geq v$

Proof

$\operatorname{rank}(MM^T) = v$

$M = \begin{bmatrix} — x_1 — \\ — x_2 — \\ \vdots \end{bmatrix}$

$MM^T = \begin{bmatrix} r & \lambda & \\ \lambda & & \\ & & \end{bmatrix} = \lambda J + (r-\lambda)\cdot I$.

Let $x \in \ker(MM^T)$

$$x^T(\lambda J + (r-\lambda)I)x .$$

$$= x^T\lambda J x + x^T(r-\lambda)Ix$$

$$= \lambda\left(\sum x_i\right)^2 + (r-\lambda)\sum x_i^2 \quad \Rightarrow$$

Proof

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

Definition (Symmetric BIBD (SBIBD))

A (v, k, λ)-BIBD is a (v, k, λ)-SBIBD if the number of points is equal to the number of blocks ($v = b$). Equivalently,

- $r = k$
- $\lambda(v-1) = k(k-1)$

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

Definition (Symmetric BIBD (SBIBD))

A (v, k, λ)-BIBD is a (v, k, λ)-SBIBD if the number of points is equal to the number of blocks ($v = b$). Equivalently,

- $r = k$
- $\lambda(v-1) = k(k-1)$

These are tight for Fisher's Inequality and represent the Spot It! decks that have a maximal number of cards for a given number of objects.

SBIBD

- Note that $v = \frac{k(k-1)}{\lambda} + 1$, so we technically just need to provide the parameter k and λ to specify a SBIBD.
- For example, if the block size $k = n + 1$, and $\lambda = 1$, we know that there are $n^2 + n + 1$ points.

"Symmetric" because

- number of points = number of blocks
- block size = replication number
- There's another reason...

A theorem about SBIBDs

Theorem

Suppose $(X, \mathcal{A})$ *is a* (v, k, λ)*-BIBD. If* $(X, \mathcal{A})$ *is symmetric, then for any distinct* $A_1, A_2 \in \mathcal{A}$, $|A_1 \cap A_2| = \lambda$

For SBIBDs, not only is every pair of points contained in λ blocks, but every pair of blocks share λ points.

Remark: The converse is also true!

Proof

Theorem. Suppose $(X, \mathcal{A})$ is a (v, k, λ)-BIBD. If $(X, \mathcal{A})$ is symmetric, then for any distinct $A_1, A_2 \in \mathcal{A}$, $|A_1 \cap A_2| = \lambda$

Strategy: Consider $MM^T a_i$ in two ways.

Proof

Theorem. Suppose $(X, \mathcal{A})$ is a (v, k, λ)-BIBD. If $(X, \mathcal{A})$ is symmetric, then for any distinct $A_1, A_2 \in \mathcal{A}$, $|A_1 \cap A_2| = \lambda$

$MM^T = \begin{bmatrix} r & \lambda & \cdots \\ \lambda & r & \\ \vdots & & \ddots \end{bmatrix}$

$MM^T a_i = \sum_{j \in A_i} (r-\lambda) e_j + \lambda \mathbb{1}$

$M = (a_1 \; a_2 \; \cdots)$ ($a_1, a_2, \ldots$ are the columns $x_1, x_2, \ldots$)

$M(M^T a_i) = M \begin{bmatrix} |A_1 \cap A_i| \\ |A_2 \cap A_i| \\ \vdots \end{bmatrix} = \sum_{j \in [b]} |A_i \cap A_j| \cdot a_i = \begin{bmatrix} r \\ \vdots \\ r \end{bmatrix}$

$\sum_{j \in A_i} (r-\lambda) e_j + \lambda \mathbb{1} = \left(\sum_{j \in A_i} (r-\lambda) e_j + k\lambda \mathbb{1} \right)$

$= (r-\lambda) a_i + \frac{k\lambda}{r} \sum a_j$

$= (r-\lambda) a_i + \lambda \sum a_j$

$\Rightarrow |A_i \cap A_j| = \lambda$

Proof

Theorem. Suppose $(X, \mathcal{A})$ is a (v, k, λ)-BIBD. If $(X, \mathcal{A})$ is symmetric, then for any distinct $A_1, A_2 \in \mathcal{A}$, $|A_1 \cap A_2| = \lambda$

The Motivating Problems

BIBDs

(Finite) Projective Planes

Secret Sharing

Euclidean Geometry

Any two lines either intersect at a unique point or are parallel.

Euclidean Geometry

Any two lines either intersect at a unique point or are parallel.

However, there is a fascinating phenomenon.

Euclidean Geometry

Any two lines either intersect at a unique point or are parallel.

However, there is a fascinating phenomenon.

Projective Planes

Definition

A projective plane is a set of points P, a set of lines L, and an incidence relation such that

- For any two distinct points, there is exactly one line incident with both of them.
- For any two distinct lines, there is exactly one point incident with both of them.
- Non-Degenerate Condition: There are four points such that no line is incident with more than two of them.

If the set of points P is finite, then the order of the projective plane is one less than the number of points in a line.

Finite Projective Planes (Alt)

Definition

For $n \geq 2$, a finite projective plane of order n is a

$$(n^2 + n + 1, n + 1, 1)\text{-SBIBD}.$$

Finite Projective Planes (Alt)

Definition

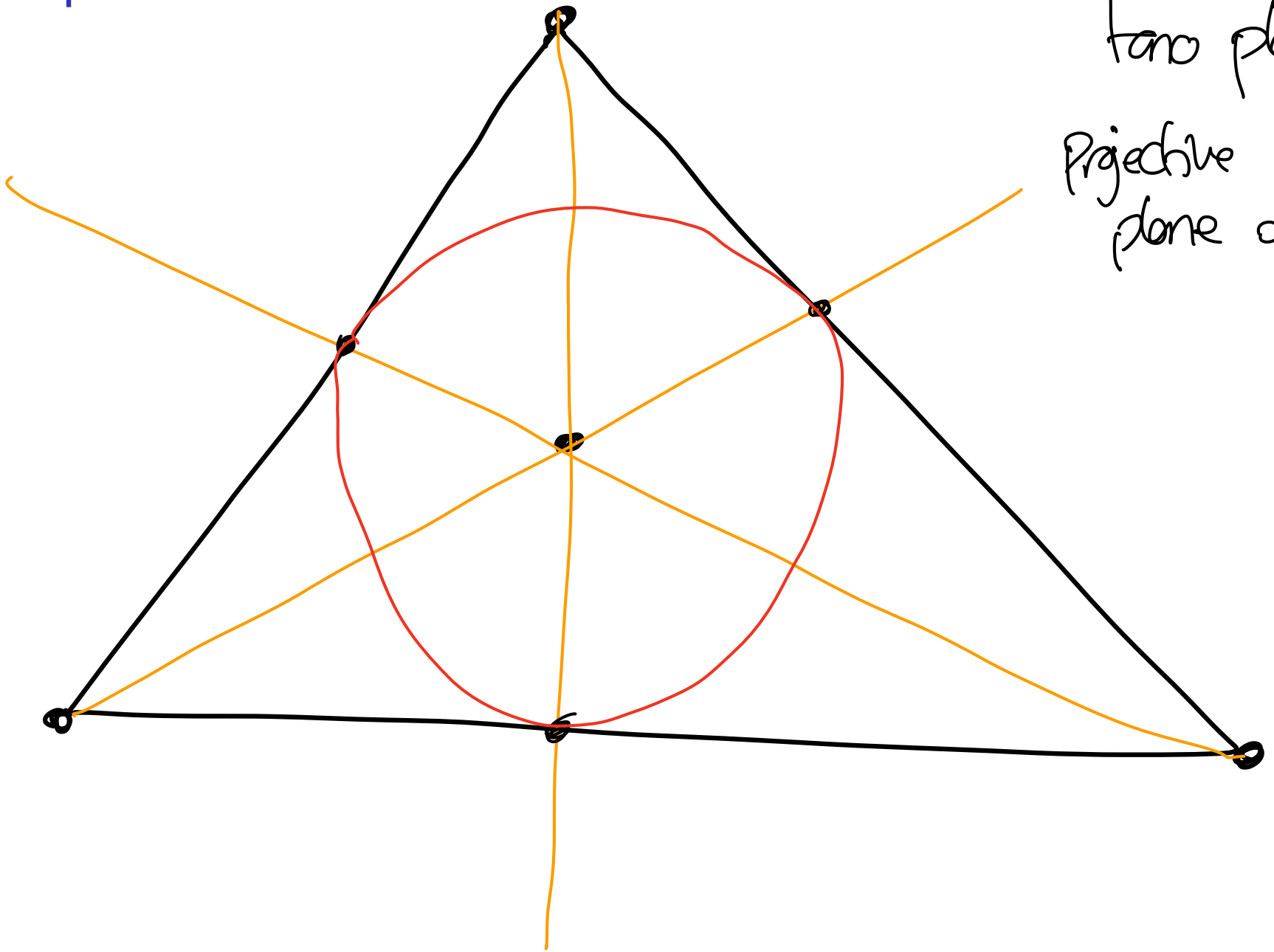
For $n \geq 2$, a finite projective plane of order n is a

$$(n^2 + n + 1, n + 1, 1)\text{-SBIBD}.$$

Remarks:

- Points are points, lines are blocks, and a point p and line l are incident if $p \in l$.
- Every two distinct points are incident with exactly one line is the balanced condition.
- Every pair of lines has exactly one point incident with both is true from the theorem about SBIBDs.

Example



Construction of Projective Planes

Let q be a prime power, and $\mathbb{F}_q$ be the finite field of order q. Consider the vector space $\mathbb{F}_q^3$. Define

- X to be the set of 1-dimensional subspaces of $\mathbb{F}_q^3$, and
- $\mathcal{A}$ to be the set of 2-dimensional subspaces of $\mathbb{F}_q^3$.

We'll show that $(X, \mathcal{A})$ is an SBIBD. By abuse of notation, we say that a 1-dimensional subspace C is in a 2-dimensional subspace D if $C \subseteq D$.

Proof

X: 1-dimensional subspaces of $\mathbb{F}_q^3$
$\mathcal{A}$: 2-dimensional subspaces of $\mathbb{F}_q^3$
WTS. $(X, \mathcal{A})$ is a $(q^2+q+1, q+1, 1)$-SBIBD

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

$$\frac{q^2-1}{q-1} = q+1 \qquad = k \quad .$$

Existence of Finite Projective Planes

The construction works for any finite field, giving us a finite projective plane of order q for every prime power q!

Existence of Finite Projective Planes

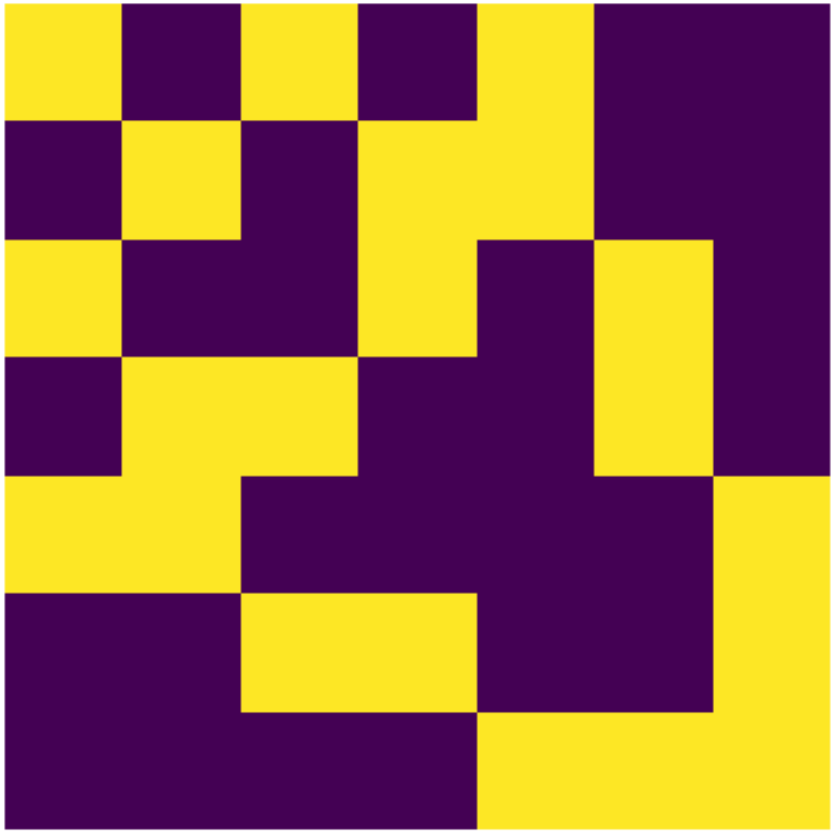
Open Question: Do finite projective planes of non-prime power order exist?

Existence of Finite Projective Planes

Open Question: Do finite projective planes of non-prime power order exist?

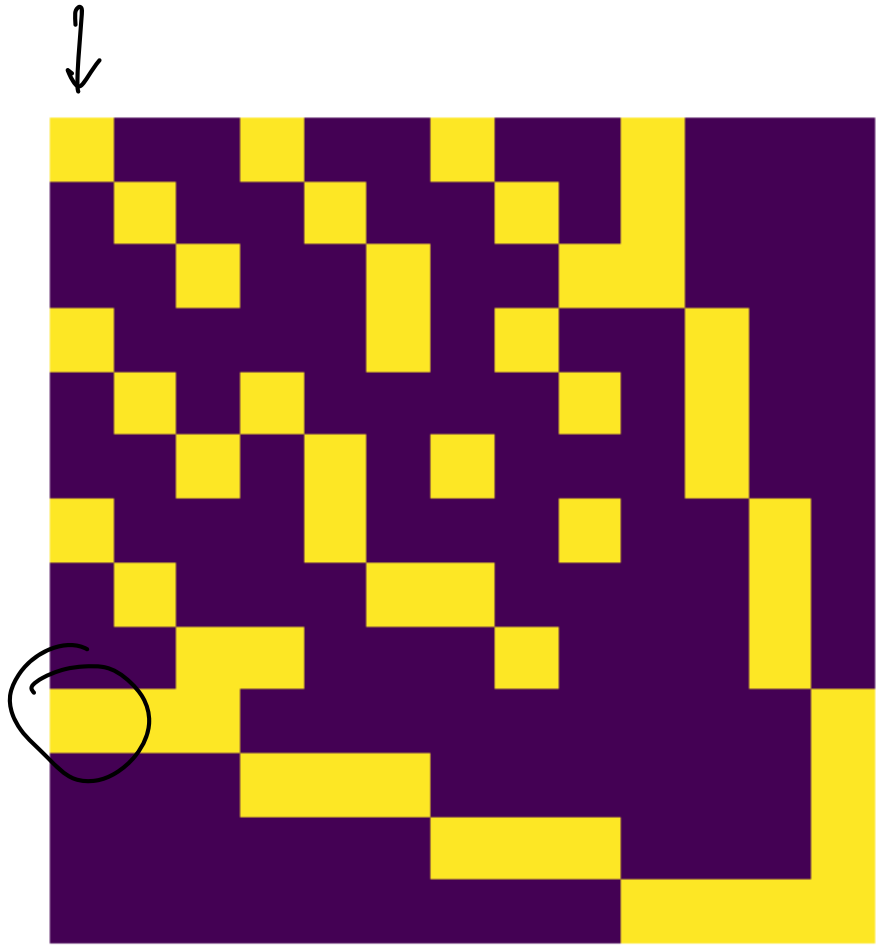
- Conjecture: No.
- We know there is no finite projective plane of order 6 (by a theorem of Bruck-Ryser-Chowla from 1949) and no finite projective plane of order 10 by heavy computer calculation.

Spot it - A solution



Incidence matrix of the finite projective plane of order 2.

Spot it - A solution



Incidence matrix of the finite projective plane of order 3

Shadows

$b = v = 7$

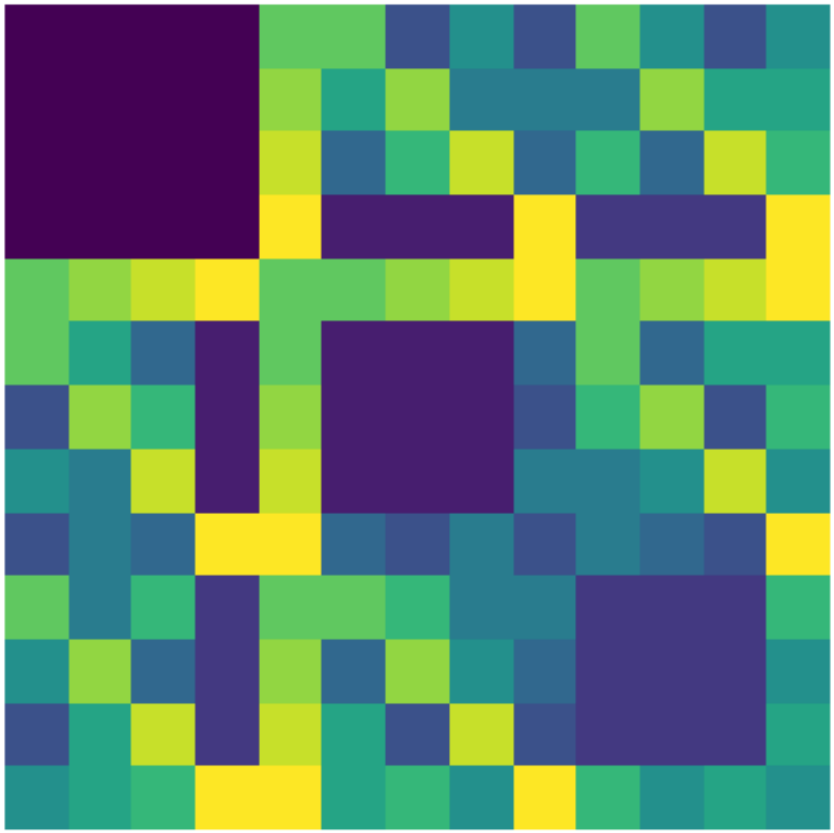
$r = k = 3$

3/7 projection length.

(thin & tight)

Projective plane of order 2. $G_{i,j} = c$ iff points i and j are in line c.

Shadows



Projective plane of order 3. $G_{i,j} = c$ iff points i and j are in line c.

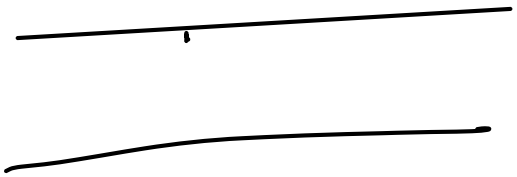
Projective Planes

Definition

A projective plane is a set of points P, and a set of lines L, and an incidence relation such that

- For any two distinct points, there is exactly one line incident with both of them.
- For any two distinct lines is exactly one point incident with both of them.
- Non-Degenerate Condition: There are four points such that no line is incident with more than two of them.

~~Projective~~ Affine Planes



Definition

An ~~projective~~ affine plane is a set of points P, and a set of lines L, and an incidence relation such that

- For any two distinct points, there is exactly one line incident with both of them.
- ~~For any two distinct lines is exactly one point incident with both of them.~~ For any line l and any point P not incident with l, there is exactly one line incident with P that does not meet l.
- Non-Degenerate Condition: There are four points such that no line is incident with more than two of them.

Affine Planes Alt.

Projective planes are
$(q^2 + q + 1, q + 1, 1)$-SBIBD

Definition

An affine plane of order q is a $(q^2, q, 1)$-BIBD

Affine Planes Alt.

Projective planes are
$(q^2 + q + 1, q + 1, 1)$-SBIBD

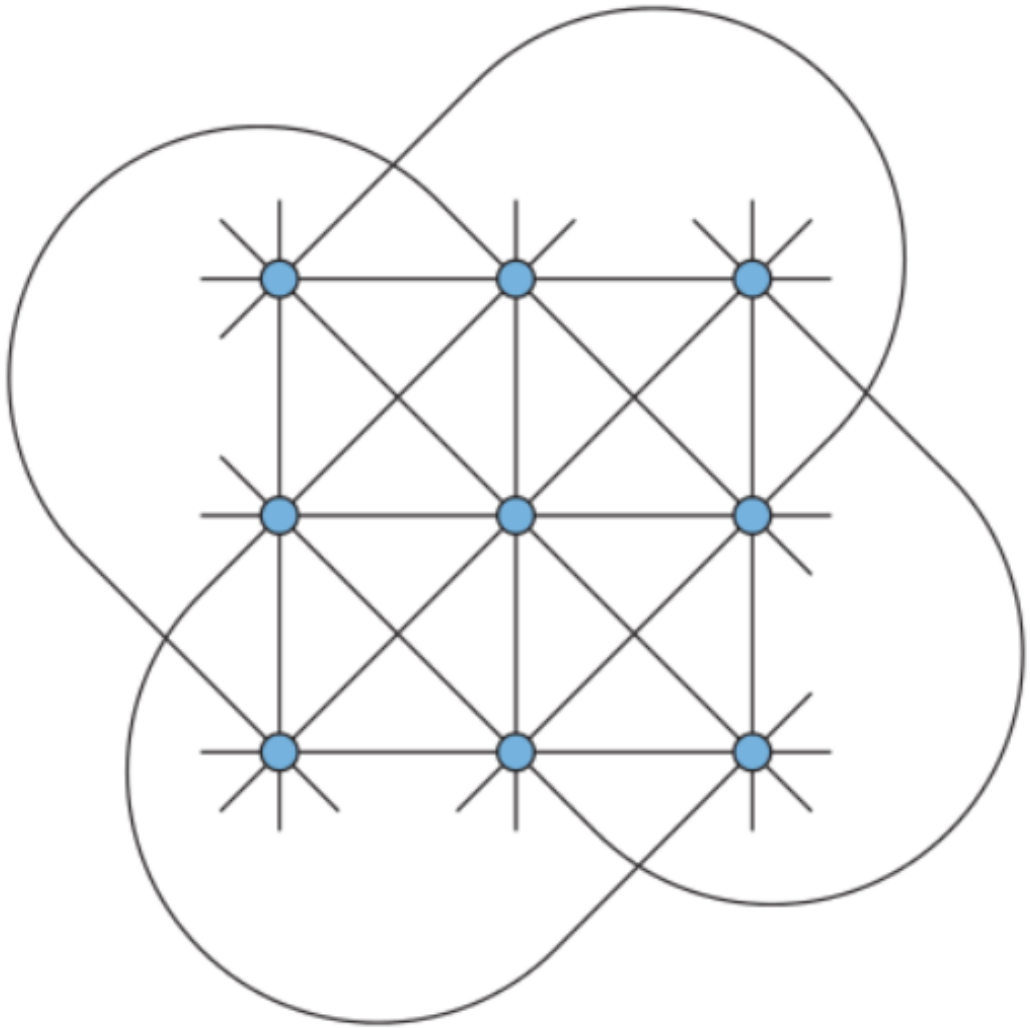
Definition

An affine plane of order q is a $(q^2, q, 1)$-BIBD

Notes

- $r = q + 1$ (Each point is in $q + 1$ lines)
- $b = q^2 + q$ (There are $q^2 + q$ lines).

9, 3, 1



Affine Plane of Order 3

Source: https://en.wikipedia.org/wiki/Affine_plane_(incidence_geometry)

Constructing Affine Planes

Let $(X, \mathcal{A})$ be the projective plane of order q, and let $L \in \mathcal{A}$ be any line (block).

Remove L and all the points on L

$$(X \setminus L, \{A \setminus L : A \in \mathcal{A}, A \neq L\})$$

It turns out this is an affine plane.

Fact about Affine Planes

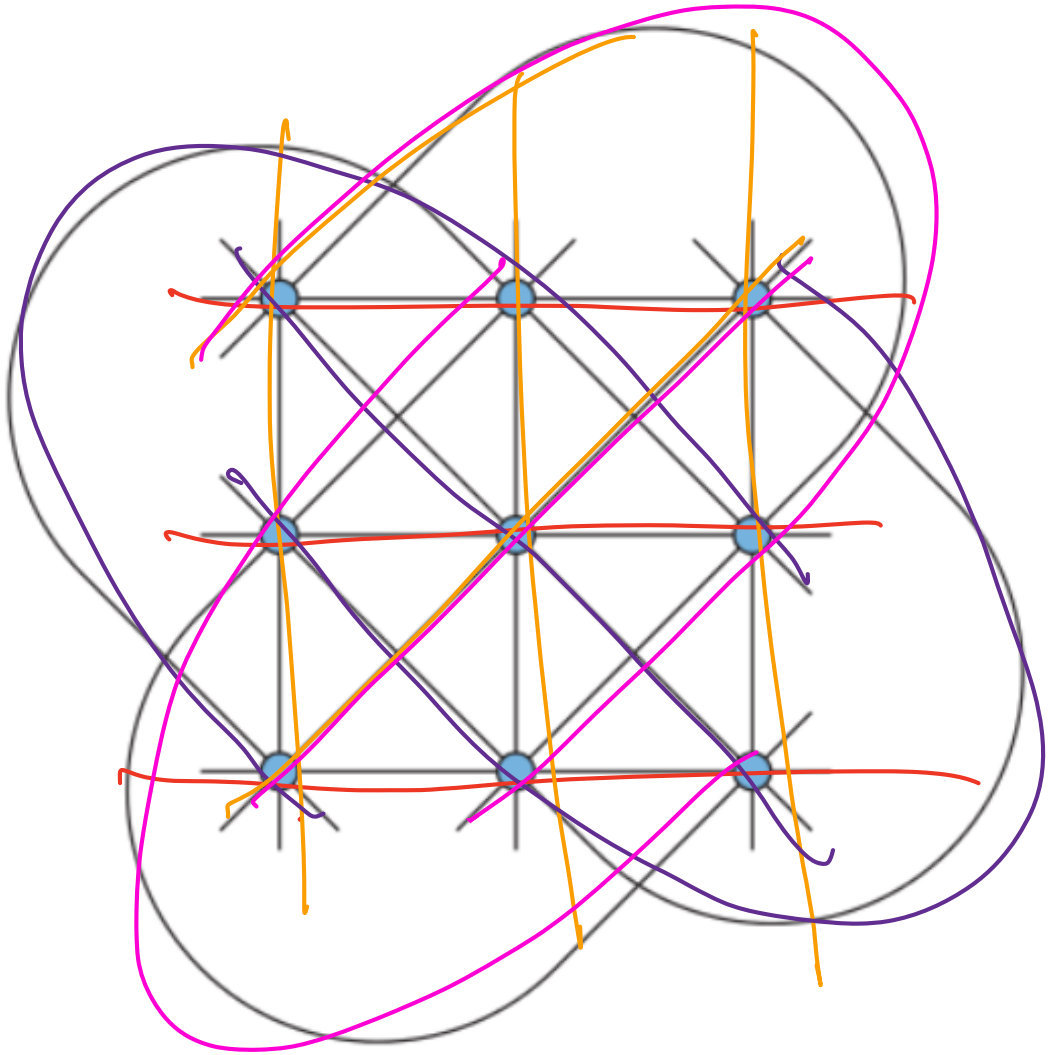
Theorem

Suppose $(X, \mathcal{A})$ is an affine plane. Then there is an equivalence relation $\sim$ over $\mathcal{A}$ such that if S is any equivalence class of $\sim$, S is a partition of X. That is

- $\bigcup_{A \in S} A = X$.
- *Blocks in S are pairwise disjoint*

"There is a partition of $\mathcal{A}$ into partitions of X."

The equivalence relation is essentially $L \sim L'$ iff L and L' are parallel.



The Motivating Problems

BIBDs

(Finite) Projective Planes

Secret Sharing

Secret Sharing Construction

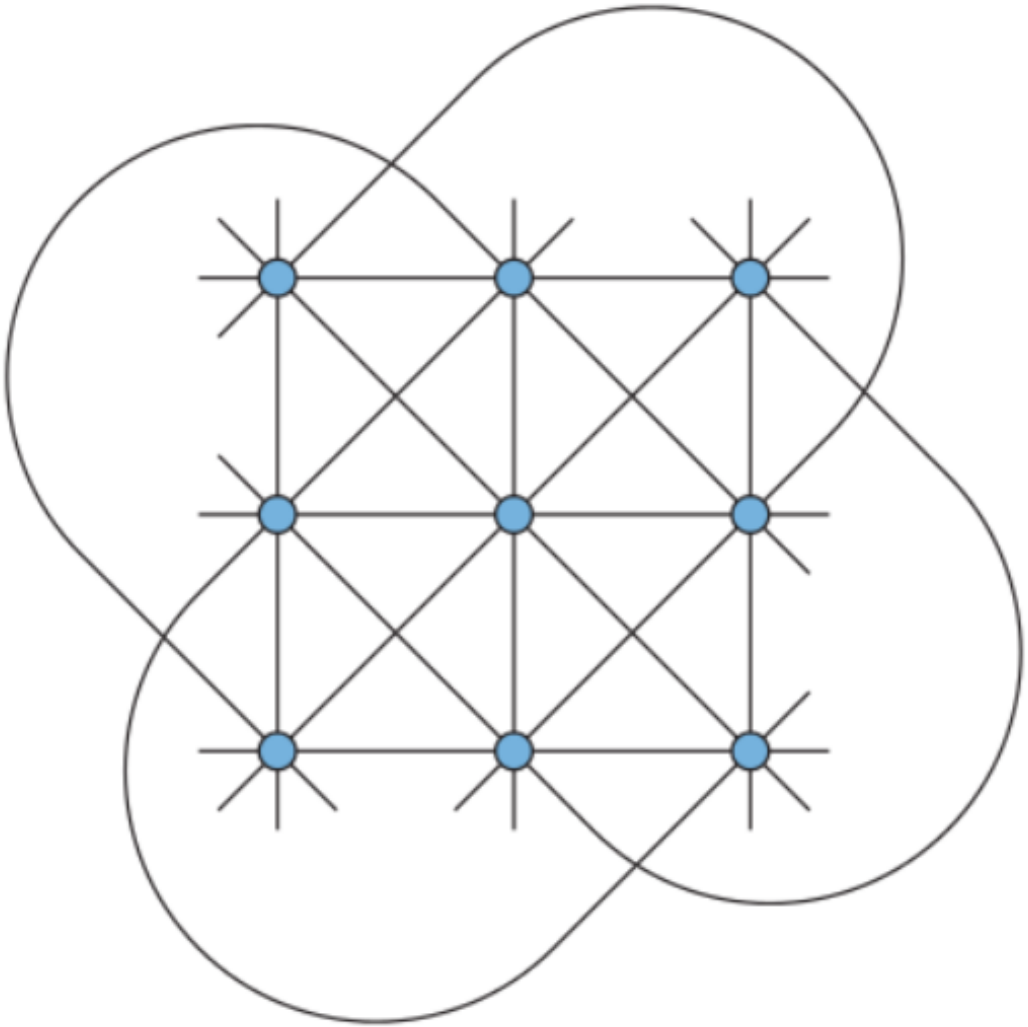
Affine planes are $(q^2, q, 1)$-BIBDs.
$r = q + 1$, and $b = q^2 + q$

Let $(X, \mathcal{A})$ be an affine plane of order q. We will use $(X, \mathcal{A})$ to construct a $(2, q)$-secret sharing scheme (q shares, any group of 2 or more people can reveal the secret, but no individual can learn anything).

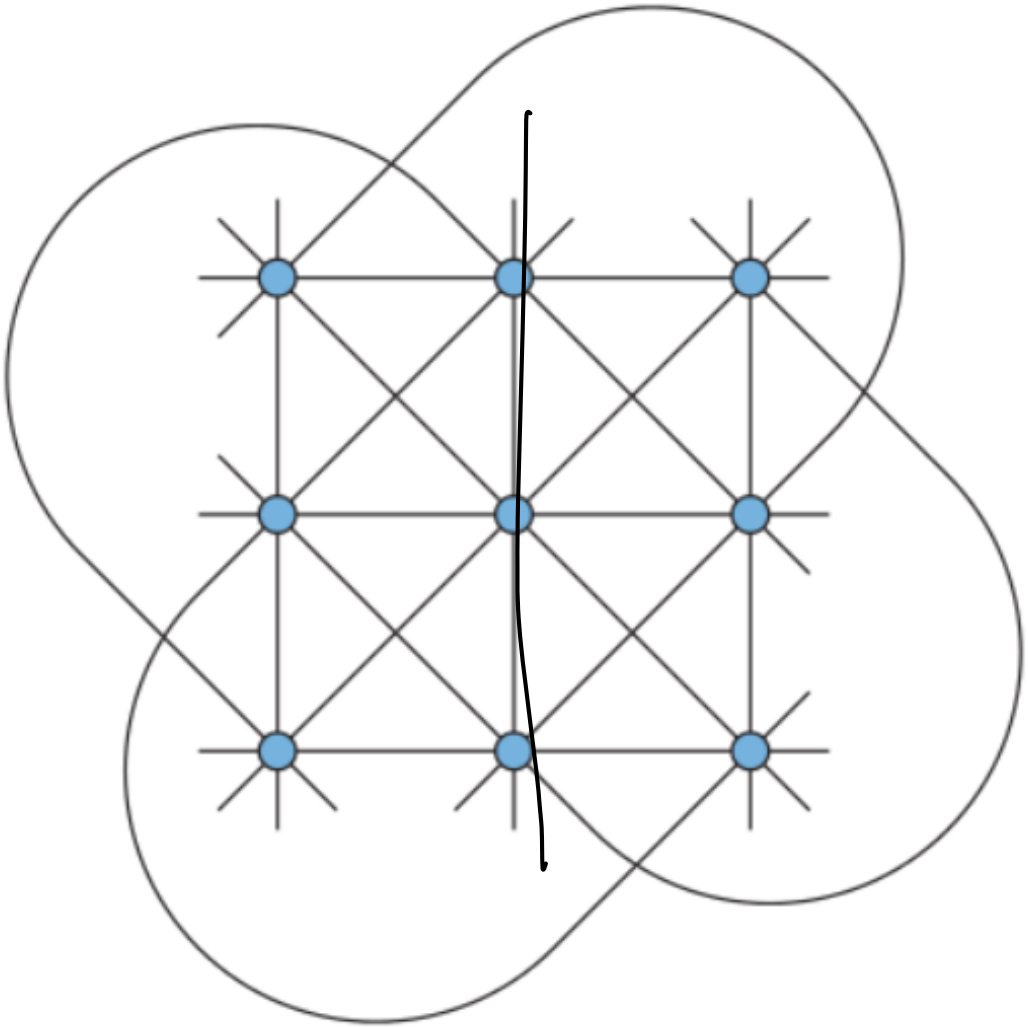
Let $\Pi_1, ..., \Pi_r$ be the partition of $\mathcal{A}$ of defined by $\sim$. The secret is an integer $K \in [r]$.

- Let A be some line in Π_K
- Give each of the $w \leq q$ people one element from A.

Groups of 2 can recover the secret



Individuals cannot recover the secret



Efficiency

- w people
- $r = q + 1$ possible secrets
- $\log(v) = \Theta(\log(q))$ share size.

Thank you!

Shamir Secret Sharing for $t \geq 2$

Theorem (Bruck-Ryser-Chowla Theorem)

If there is a projective plane of order n such that $n \equiv 1, 2 \pmod 4$, then n must be the sum of two squares.

More General Fisher's

Theorem

Suppose we have a collection of sets $S_1, ..., S_v$ in the universe $[b]$. Such that the intersection of any two sets has the same size, I.e., for any i, j, $|S_i \cap S_j| = \lambda$ for $\lambda \geq 1$. Then

$$v \leq b$$

This is the same as the original statement but for the dual of the BIBD and removing the block size and replication number restrictions.

Theorem (Ray-Chaudhuri-Wilson Theorem)

Let $F \subseteq \wp([n])$. Such that $\forall A, B \in F$, $|A \cap B| \in \{\lambda_1, ..., \lambda_s\}$. I.e., the size of the intersection of any two sets must be one of s numbers. Then,

$$|F| \leq \binom{n}{\leq s}.$$

Where $\binom{n}{\leq s}$ is the sum of the binomial coefficients up to and including s.

Projective Geometries

Generalizing the construction for projective planes to be over $\mathbb{F}_q^{d+1}$ instead of $\mathbb{F}_q^3$, we get that there exists symmetric

$$\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right)\text{-BIBDs}$$

The points are 1-dimensional subspaces, and the blocks are d-dimensional subspaces.