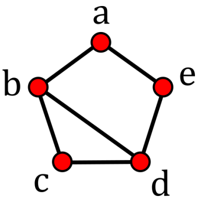
Design Theory

Recall: Graphs

- Recall the concept of a **graph**.
- For example, let $G = (V, E)$ be the graph where
  - $V = \{a, b, c, d, e\}$ is its **vertex** set, and
  - $E = \{ab, bc, cd, de, ae, bd\}$ is its **edge** set.
  - E is a collection of 2-element subsets of V and could be written as such:

$$\{\{a, b\}, \{b, c\}, \{c, d\}, \{d, e\}, \{a, e\}, \{b, d\}\}.$$

- For a better understanding, we may draw the graph of G:



- In what follows, we study other abstract mathematical objects called combinatorial designs, however, these are often harder to visualize.

Motivating Example?

- We first consider taking 3-element subsets instead of 2-element subsets.
- One direction gives the concept of a hypergraph.
- Instead, we analyze mathematical objects with lots of **symmetry**.

Example

- Let $X = \{0, 1, 2, 3, 4, 5\}$ and $\mathcal{B} = \{012, 023, 034, 045, 051, 124, 235, 341, 452, 513\}$.
- We call the elements of X **points** (instead of "vertices").
- $\mathcal{B}$ is a collection of 3-element subsets of X which more formally is written as:

$$\mathcal{B} = \{\{0,1,2\}, \{0,2,3\}, \{0,3,4\}, \{0,4,5\}, \{0,5,1\}, \{1,2,4\}, \{2,3,5\}, \{3,4,1\}, \{4,5,2\}, \{5,1,3\}\}.$$

- We call the elements of $\mathcal{B}$ **blocks** (instead of "edges").
- We call $\mathcal{B}$ the **block set** (instead of "edge set").

Observe: Every pair of points is in **exactly** 2 blocks (e.g., points $0, 1$ are in 012 and 051).

Question: How could we visualize $(X, \mathcal{B})$?

One way is to draw a pentagon with a point inside (the centre point is labelled by 0). Then blocks correspond to triples which contain exactly one pentagon edge.

Block designs

Combinatorial design theory deals with the existence, construction and properties of systems of finite sets whose arrangements satisfy some notion of balance or symmetry.

Applications include

- tournament scheduling,
- software testing,
- cryptography,
- group testing (in statistics),
- mathematical chemistry and biology.

Block designs

A general definition is below (we will focus on designs with specified parameters).

Definition

- Let t, k, v, λ be integers with $t < k < v$ and $\lambda > 0$.
- A t-(v, k, λ) **design** is a pair $(X, \mathcal{B})$ such that:
  - X is a set of cardinality v whose elements are called **points**,
  - $\mathcal{B}$ is a collection of k-subsets of X called **blocks**,
  - and any t points are contained in exactly λ blocks.

The Main Problem

For which values of parameters do designs exist?

- A t-design with $\lambda = 1$ is called a **Steiner system** and denoted by $S(t, k, v)$.
- $S(2, q+1, q^2+q+1)$ is called a **finite projective plane**.
- $S(2, 3, n)$ is called a **Steiner triple system**.

Definition

A $\boxed{\textbf{Steiner triple system}}$, denoted by STS($n$), consists of a set X of n points and a set $\mathcal{B}$ of 3-element subsets of X (called **blocks** or **triples**), with the property that any **two** points of X lie in a **unique** triple. We call n the **order** of the Steiner triple system.

Main Problem

For which values of n does a STS(n) exist?

Example ($n = 3$)

$$X = \{1, 2, 3\} \text{ and } \mathcal{B} = \{123\}$$

Exercise

Show that an STS(n) does not exist for $n = 4, 5, 6$.

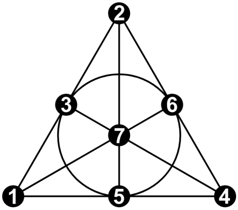
The Fano plane

Example ($n = 7$)

The following is an STS(7):

$$X = \{1, 2, 3, 4, 5, 6, 7\} \text{ and } \mathcal{B} = \{123, 145, 167, 246, 257, 347, 356\}$$

Every pair ij is in exactly one block.
One illustration comes from finite geometry as follows:



This is called the **Fano plane**. It is a projective plane of order $q = 2$.
In a finite projective plane:

- For every two distinct points, there is exactly one line that contains both points.
- There exists a set of four points, no three of which belong to the same line.
- The intersection of any **two distinct lines contains exactly one point**.

History:

- Steiner triple systems were first defined by Woolhouse in 1845 in a recreational mathematics magazine.
- The problem was solved by Kirkman in 1847 and also in 1853 by Steiner (who was unaware of Kirkman's work.
- These systems were named after Steiner since his work was more widely known.
- In 1850, Kirkman posed a variation of the problem known as Kirkman's schoolgirl problem, which asks for triple systems having an additional property (resolvability).

Kirkman's Schoolgirls Problem

Fifteen schoolgirls walk each day in five groups of three. Arrange the girls' walks for a week so that, in that time, each pair of girls walks together in a group just once.

Solution to Kirkman's 'nine' schoolgirls problem

An STS(9) gives a solution to the 'nine' schoolgirls problem.

Kirkman's 'nine' Schoolgirls Problem

Nine schoolgirls walk for four days in three groups of three each day. Arrange the girls' walks so that each pair of girls walks together in a group just once.

The walking scheme is as follows.

Day 1:	123	456	789
Day 2:	147	258	369
Day 3:	159	267	348
Day 4:	357	168	249

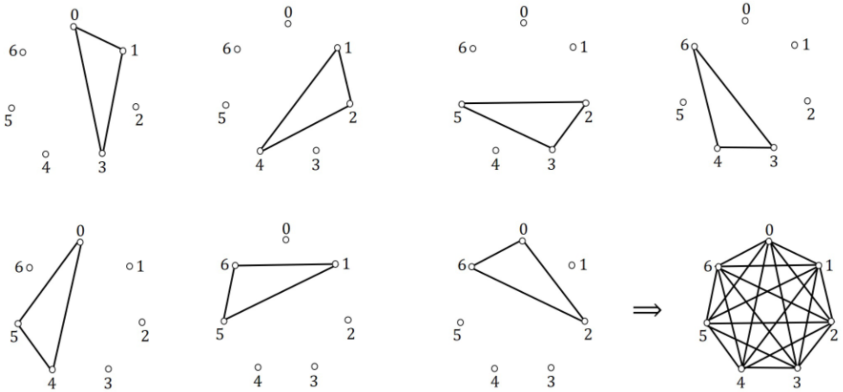
Steiner triple systems: A graph theory interpretation

Definition

A $\boxed{\textbf{decomposition}}$ of a graph G is a set of subgraphs that partition the edges of G.

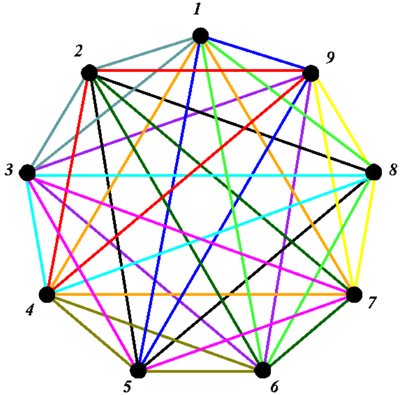
Fact

An STS(n) is equivalent to a decomposition of K_n into triangles (cliques of size 3).



STS(9)

Below is a decomposition of K_9 into 12 triangles, where each triangle is a different colour.



Each triangle corresponds to a block in an $\mathsf{STS}(9) = (X, \mathcal{B})$:

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

$$\mathcal{B} = \{123, 147, 159, 168, 249, 258, 267, 348, 357, 369, 456, 789\}$$

Existence

Theorem

Let $n > 0$. There exists an STS(n) iff $n \equiv 1$ or $3 \pmod 6$.

Proof. ($\Longrightarrow$) We consider when a decomposition of the edges of the complete graph K_n into triangles can exist.

- Every vertex v must belong to $\dfrac{n-1}{2}$ triangles since $\deg(v) = n - 1$.
- Thus, n must be odd, i.e., $n \equiv 1, 3$ or $5 \pmod 6$.
- To rule out $n \equiv 5 \pmod 6$, assume $n = 6k + 5$.
- Since there are $\dfrac{\binom{n}{2}}{3}$ triangles in total, $n(n-1)/6$ must be a positive integer.
- Then
$$n(n-1)/6 = (6k+5)(3k+2)/3$$
  is a positive integer.
- However, neither $6k + 5$ nor $3k + 2$ are divisible by 3, a contradiction.
- Thus, we must have $n \equiv 1$ or $3 \pmod 6$.

($\Longleftarrow$) Kirkman provided a recursive construction to create a larger Steiner triple system from smaller ones. We omit the details here. □

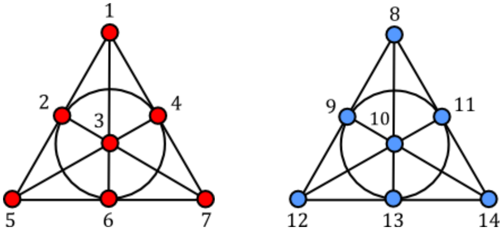
The Transylvania lottery problem (unknown origin)

Problem

- You enter a lottery by choosing any three distinct numbers from $\{1, 2, 3, \ldots, 14\}$.
- After tickets are purchased, three numbers are drawn randomly from 1 to 14 and any ticket that matches at least two of the drawn numbers wins a prize.
- What is the fewest number of tickets you must purchase to guarantee a win?

The number of possible tickets is $\dfrac{14 \cdot 13 \cdot 12}{3!} = 364$.

The Transylvania lottery solution with Fano planes



You can win by buying 14 tickets with the following numbers:

$$\{\{1,2,5\},\{1,3,6\},\{1,4,7\},\{2,3,7\},\{2,4,6\},\{3,4,5\},\{5,6,7\},$$
$$\{8,9,12\},\{8,10,13\},\{8,11,14\},\{9,10,14\},\{9,11,13\},\{10,11,12\},\{12,13,14\}\}.$$

- At least two of the winning numbers must either be low numbers (1 to 7) or must be high numbers (8 to 14).
- We have covered every possible pair of two low numbers and every possible pair of two high numbers, thus, we are guaranteed to match at least two numbers on one of our tickets.
- If it so happens that all three random numbers are either high or all three are low, then either we have matched them perfectly, or we have three different winning tickets that each have two matching numbers.