Steiner Triple Systems

Lucia Moura
School of Electrical Engineering and Computer Science
University of Ottawa
lmoura@uottawa.ca

Summer 2022

Steiner triple systems

Definition

A *Steiner triple system* of order v, denoted STS(v), is a $(V, \mathcal{B})$ design with v points and each block $B \in \mathcal{B}$ has $|B| = 3$ (which we call a triple) and such that each pair of distinct elements $x, y \in V$ occur together in exactly one triple of $\mathcal{B}$.

Or in other words, an STS(v) is precisely a $(v, 3, 1)$-BIBD.

STS(7): $V = \{1, \ldots, 7\}$,
$\mathcal{B} = \{123, 145, 167, 246, 257, 347, 356\}$
STS(9): $V = \{1, \ldots, 9\}$,

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

A $(v, 3, \lambda)$-BIBD is a *triple system*. Triple systems is the subject of a whole book by Colbourn and Rosa (1999).

Necessary conditions for the existence of an STS(v)

Using the same arguments as for BIBDs, we conclude that for an STS(v), we have point replication and number of blocks given by

$$\begin{aligned} r &= \frac{v-1}{2} \\ b &= \frac{v(v-1)}{6} \end{aligned}$$

Since r is an integer, we must have $2|(v-1)$, i.e v odd.
So $v \equiv 1, 3, 5 \pmod 6$
Since b is an integer, we must have $6|v(v-1)$.
For $v \equiv 5 \pmod 6$, we cannot have $6|v(v-1)$.

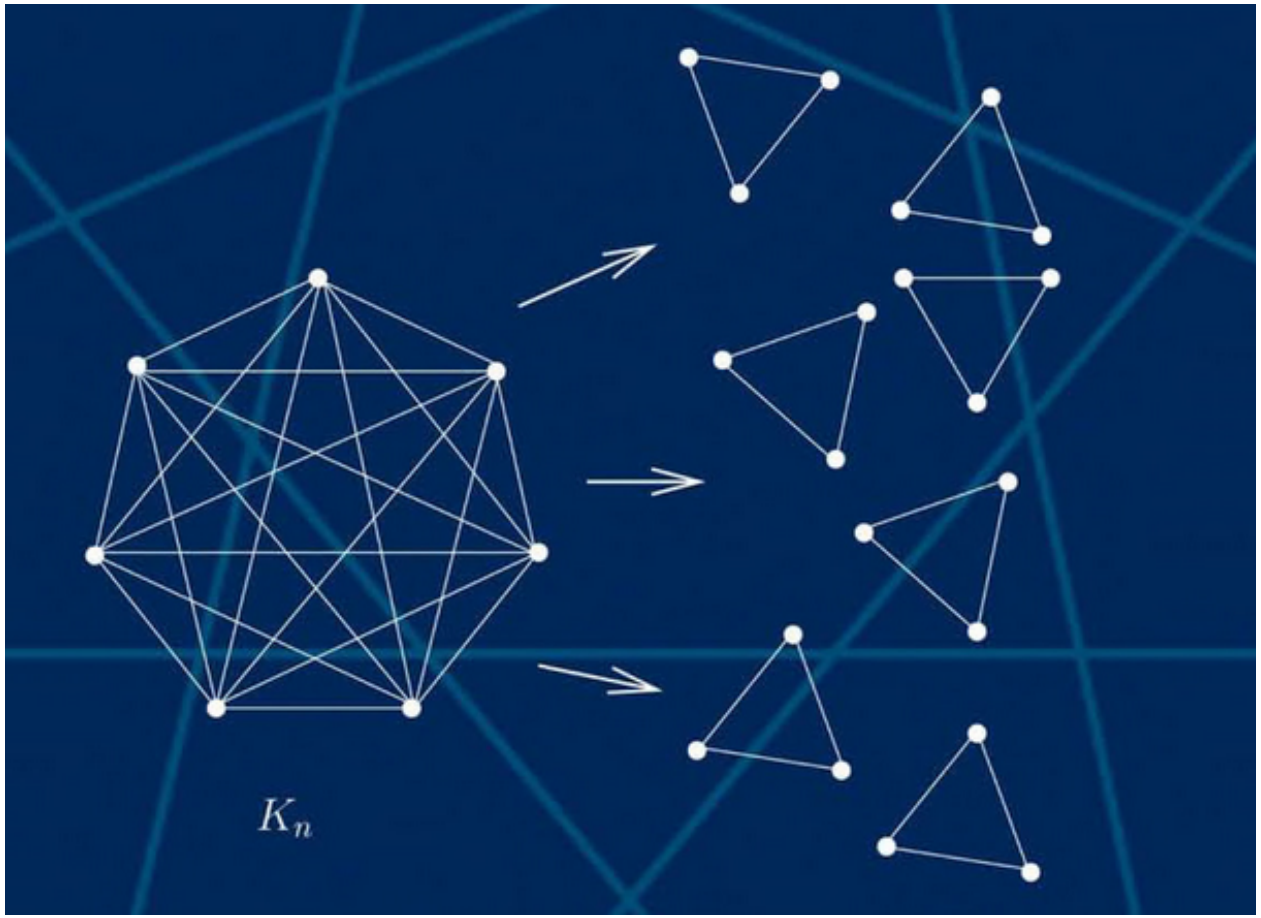
Proposition (Necessary conditions for the existence of an STS)

If an STS(v) exists, then

$$v \equiv 1, 3 \pmod 6$$

Steiner triple systems and graph decompositions

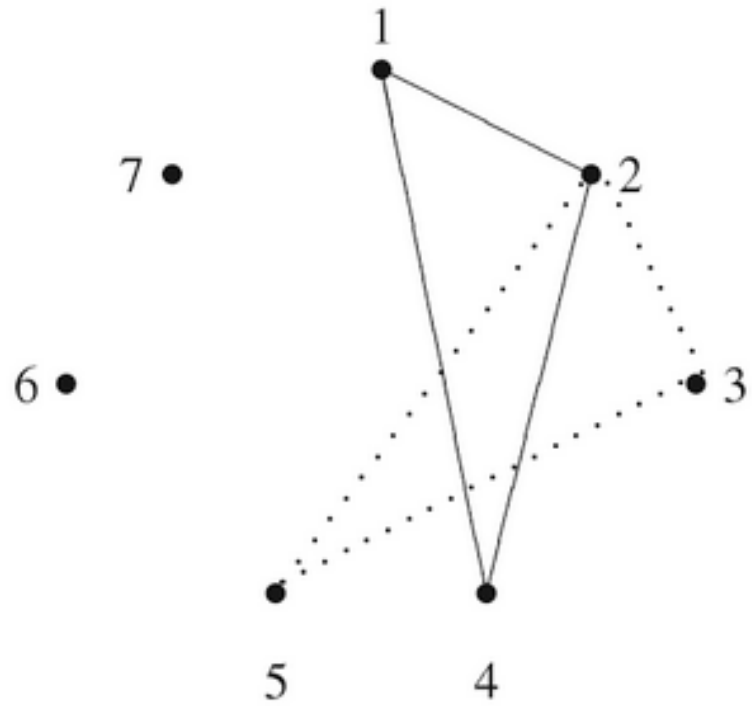
An STS(v) is equivalent to partitioning the edges of a complete graph K_v into triangles.



Ref. picture from cover book of book by Lindner and Rodger 2008

Steiner triple systems and graph decompositions

Cyclic STS(7) is equivalent to cyclic rotation of triangles in K_7.



Ref. picture from Lindner and Rodger 2008

Existence

Steiner triple systems were defined for the first time by W.S.B. Woolhouse (prize question 1733, Lady's and Gentleman's Diary, 1844) which asked for which positive integers does a STS(v) exists.

This was solved by Rev. T.P. Kirkman, who proved in 1847 that the necessary conditions are sufficient.

Theorem

An STS(v) exists if and only if $v \equiv 1, 3 \pmod 6$

Here we will show simpler constructions than Kirkman's: Bose and Skolem's constructions.

Latin squares

We will need Latin squares to build STSs.

Definition

A *Latin square* of order n is an $n \times n$ array, with symbols in $\{1, \ldots, n\}$, such that each row and each column contains each of the symbols in $\{1, \ldots, n\}$ exactly once.

Examples of Latin squares of order 3

1	2	3
3	1	2
2	3	1

1	3	2
3	2	1
2	1	3

Latin Squares and quasigroups

Definition

A *quasigroup* of order n is a pair $(Q, \circ)$ where Q is a set of size n and $\circ$ is a binary operation on Q such that for evert pair of elements $a, b \in Q$, the equations $a \circ x = b$ and $y \circ a = b$ each have a unique solution.

Note that the operation table for $\circ$ of a quasigroup is equivalent to a Latin square.

Examples of quasigroups of order 3

$\circ$	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

$\circ$	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

Idempotent and symmetric Latin squares

Definition

A Latin square is *idempotent* if cell (i, i) contains symbol i for all $1 \leq i \leq n$.
A Latin square is *symmetric (or commutative)* if cell (i, j) and (j, i) contain the same symbol i.

Examples of idempotent and symmetric Latin squares:

1	3	2
3	2	1
2	1	3

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

Idempotent and symmetric Latin squares of odd order

We can define the binary operation $\circ$ that defined the Latin square for n odd as:

$$x \circ y = \left(\frac{n+1}{2}\right)(x+y) \bmod n.$$

This is idempotent since
$x \circ x = \left(\frac{n+1}{2}\right)(2x) \bmod n = (n+1)x \bmod n = x.$
This is commutative since operation $+$ in $\mathbb{Z}_n$ is commutative.

$\circ$	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

$\circ$	0	1	2	3	4
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

Bose construction for STS(v), $v \equiv 3 \bmod 6$

Let $v = 6n + 3$ and let $(Q, \circ)$ be an idempotent commutative quasigroup of order $2n + 1$ where $Q = \{0, \ldots, 2n\}$.

Let $V = Q \times \{0, 1, 2\}$ and define $\mathcal{B}$ to contain triples of two types:
Type 1: for all $0 \leq x \leq 2n$, $\{(x, 0), (x, 1), (x, 2)\}$.
Type 2: for all $0 \leq x < y \leq 2n$, $\{(x, 0), (y, 0), (x \circ y, 1)\}$, $\{(x, 1), (y, 1), (x \circ y, 2)\}$, $\{(x, 2), (y, 2), (x \circ y, 0)\}$.

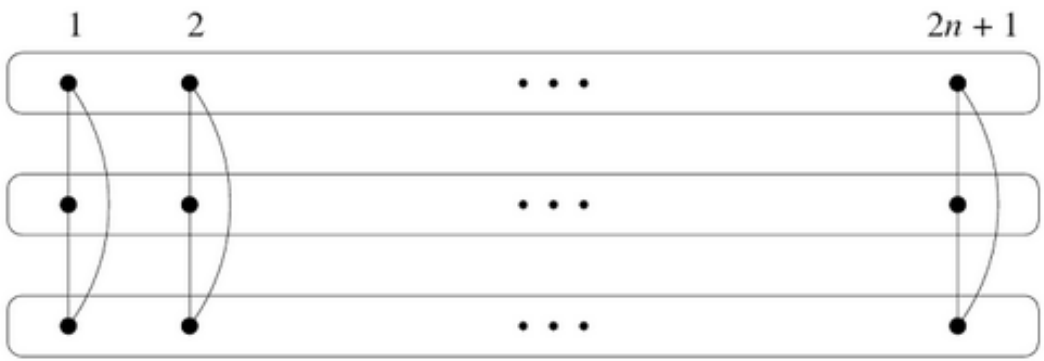
Proposition

The design $(V, \mathcal{B})$ defined above is an STS$(6n + 3)$.

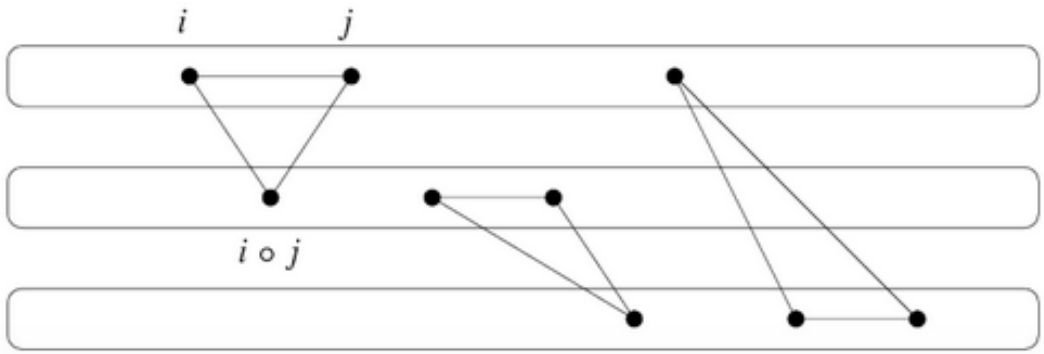
Practice: Do the construction for $n = 1$ to build an STS(9) using an idempotent symmetric Latin square of order 3.

Bose construction in pictures

Type 1 triples.



Type 2 triples.



(Ref. picture from Lindner and Rodger 2008)

Verification

The number of blocks is $(2n+1) + 3(\frac{(2n+1)(2n)}{2}) =$
$(2n+1)(3n+1) = (v/3)((v-1)/2) = v(v-1)/6$.
So it is enough to show that every pair of points appear in at least one block, since the counting of blocks would then garantee that they appear exactly once.
Consider an arbitrary pair of points (x,i) and (y,j).

- Case $x = y$: (x,i) & (x,j) share block $\{(x,0),(x,1),(x,2)\}$.
- Case $i = j$: (x,i) & (y,i) share block $\{(x,i),(y,i),(x \circ y,(i+1) \bmod 3)\}$
- Case $x \neq y$, $i \neq j$: Order pairs so that $j = (i+1) \bmod 3$. Since we have a quasigroup, there exists a unique z such that $x \circ z = y$. And since the quasigroup is idempotent and $x \neq y$, we have $x \neq z$. So $(x,i),(y,i)$ share block $\{(x,i),(z,i),(x \circ z = z \circ x = y,(i+1) \bmod 3 = j)\}$.

Conclusion: the construction gives an STS$(6n+3)$. $\square$

Skolem construction for STS(v), $v \equiv 1 \bmod 6$

Definition

A Latin square of order $2n$ is *half-idempotent* if cells (i, i) and $(n + i, n + i)$ contains symbol i for all $1 \leq i \leq n$.

We will use half-idempotent commutative Latin squares to build STS$(6n + 1)$.
We can build half-idempotent commutative Latin squares by considering the table for the quasigroup $(\mathbb{Z}_{2n}, +)$ and relabling the symbols so that the diagonal has the symbols in the right order.
This relabling is possible, since $x + x = 2x$ for $x \in \mathbb{Z}_{2n}$ give each even residue of $\mathbb{Z}_{2n}$ twice.

Examples of half-idempotent commutative Latin squares

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

relabling:

0	2	1	3
2	1	3	0
1	3	0	2
3	0	2	1

Skolem construction for STS(v), $v \equiv 1 \bmod 6$

Let $v = 6n + 1$ and let $(Q, \circ)$ be an half-idempotent commutative quasigroup of order $2n$ where $Q = \{0, \ldots, 2n - 1\}$.

Let $V = \{\infty\} \cup (Q \times \{0, 1, 2\})$ and define $\mathcal{B}$ to contain triples of three types:

Type 1: for all $0 \leq x \leq n - 1$, $\{(x, 0), (x, 1), (x, 2)\}$.

Type 2: for all $0 \leq x \leq n - 1$, $\{\infty, (n + x, 0), (x, 1)\}$,
$\{\infty, (n + x, 1), (x, 2)\}, \{\infty, (n + x, 2), (x, 0)\}$

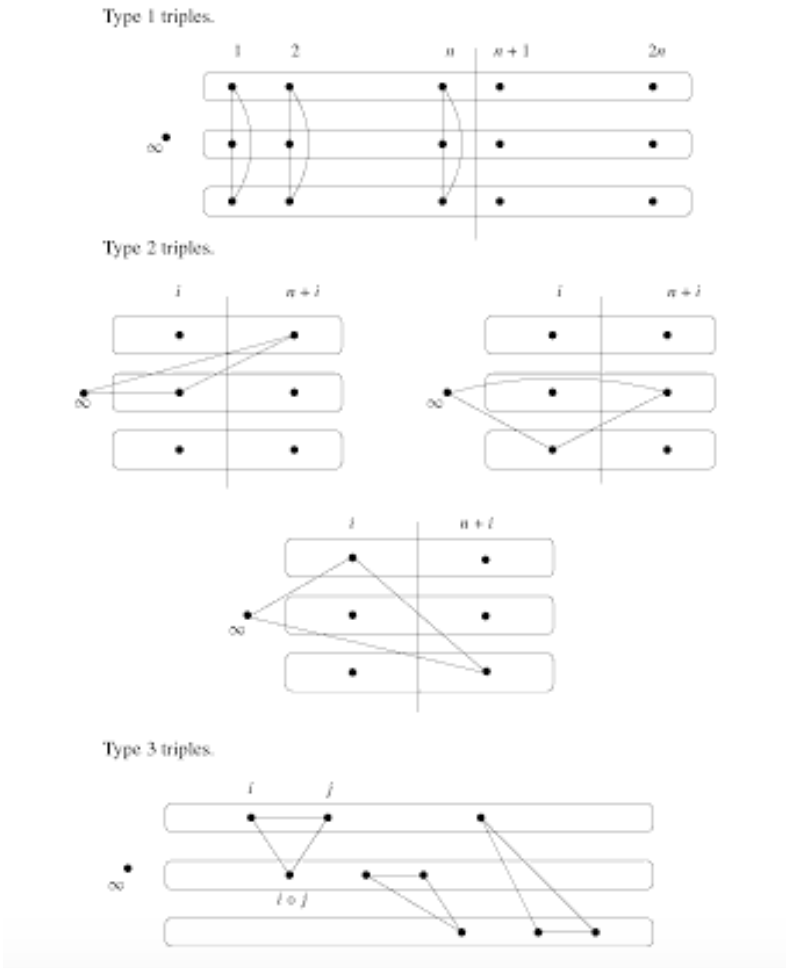
Type 3: for all $0 \leq x < y \leq 2n - 1$, $\{(x, 0), (y, 0), (x \circ y, 1)\}$,
$\{(x, 1), (y, 1), (x \circ y, 2)\}$, $\{(x, 2), (y, 2), (x \circ y, 0)\}$.

Proposition

The design $(V, \mathcal{B})$ defined above is an STS$(6n + 1)$.

Practice: Do the construction for $n = 1$ to build an STS(7) using an idempotent symmetric Latin square of order 2.

Skolem construction in pictures



(Ref. picture from Lindner and Rodger 2008)

Verification

The number of blocks is $b = 4n + 3(2n(2n-1)/2) = 4n + 6n^2 - 3n = (6n+1)6n/6 = v(v-1)/6$, so we have the right number of blocks, and only need to verify that pair of points P, Q occur at least once. The second coordinate is taken in $\mathbb{Z}_3$ so when we write $i+1$ we are doing $(i+1) \bmod 3$.

- $P = (x,i), Q = \infty$: if $x \leq n-1$ then it is $\{\infty, (n+x, i-1), (x,i)\}$; if $x \geq n$, then it is in $\{\infty, (x,i), (x-n-1, i+1)\}$.
- $P = (x,i), Q = (x,j), i \neq j$:
  if $x \leq n-1$, then it appears in a Type 1 block.
  If $x \geq n$, so wlog $j = i+1$. Equation $x \circ y = x$ has a unique solution y, and we know $y \neq x$ since $x \geq n$. Then points $(x,i), (x,i+1)$ are in $\{(x,i), (y,i), (x \circ y = y \circ x = x, i+1)\}$ (Type 3).

Verification (continued)

- Case $(x,i),(y,j)$ with $x \neq y$. We can assume wlog $x < y$.
  We have 3 cases to consider: $i = j$, $j = i+1$ or $i = j+1$.
  - $(x,i),(y,i)$: in a Type 3 block $\{(x,i),(y,i),(x \circ y, i+1)\}$.
  - $(x,i),(y,i+1)$:
    In this case, $z \circ x = y$ has a unique solution z; note that $z \neq x$ since $x < y$ and $x \circ x \leq x$ for all x (half-idempotent).
    Then (x,i) & $(y,i+1)$ are in
    $\{(x,i),(z,i),(x \circ z = z \circ x = y, i+1)\}$
  - $(x,j+1)$, (y,j):
    In this case, $z \circ y = x$ has a unique solution z.
    If $z = y$ then $z = x + n$, then the pair is in
    $\{\infty,(y = z = n + x, j),(x, j+1)\}$.
    If $z \neq y$ then the pair is in
    $\{(y,j),(z,i),(y \circ z = z \circ y = x, j+1)\}$.

□

References

- C.J. Colbourn and A. Rosa, Triple Systems, Oxford University Press, 1999.
- C.C. Lindner and C.A. Rodger, Design Theory, CRC Press, 2008. (chapter 1)
- D. R. Stinson, Combinatorial Designs: Constructions and Analysis, 2004.