

Steiner Triple Systems

Existence, representation and construction

Luca Vecchi

University of Milan

December 4, 2018

Introduction

Outline

- Challenge on *combinatorial design*
- What is it?:
 - ▶ existence or non-existence
 - ▶ representation
 - ▶ construction

What is Steiner Triple System

(Definition) Steiner Triple Systems (STS)

is an ordered pair (S, T) (a *design*) where S is a finite set of *point/symbol* and T is a set of subsets of 3-symbol in which all possible pair of S are contained **once and only once**.

What is Steiner Triple System

(Definition) Steiner Triple Systems (STS)

is an ordered pair (S, T) (a *design*) where S is a finite set of *point/symbol* and T is a set of subsets of 3-symbol in which all possible pair of S are contained **once and only once**.

More formally:

- define S such that $|S| = v$
- then $T = \{\{a, b, c\} \in S \times S \times S\}$
such that $\forall a, b \in S, a \neq b$
$$\sum_{\{x,y,z\} \in T} (\mathbb{I}_{\{a,b\} \in \{x,y\}} + \mathbb{I}_{\{a,b\} \in \{y,z\}} + \mathbb{I}_{\{a,b\} \in \{z,x\}}) = 1$$

More compact way to define STS by define the *order* v of STS by $v = |S|$

Examples of STS

$$S = \{a\}, T = \emptyset$$

$$S = \{a, b\}, T = \emptyset$$

$$S = \{a, b, c\}, T = \{\{a, b, c\}\}$$

$$S = \{a, b, c, d\}, T = \emptyset$$

$$S = \{a, b, c, d, e\}, T = \emptyset$$

$$S = \{a, b, c, d, e, f\}, T = \emptyset$$

$$S = \{a, b, c, d, e, f, g\}, T =$$

$$\{\{a, b, c\}, \{c, d, e\}, \{e, f, a\}, \{f, b, d\}, \{a, g, d\}, \{e, g, b\}, \{c, g, f\}\}$$

...

Balanced incomplete blocks design

(Definition) (v, k, λ) – BIBD

v, k and λ be positive integers such that $v > k \geq 2$. A balanced incomplete block design is a *design* (S, T) such that satisfy these properties:

- 1 $|S| = v$
- 2 $\forall t \in T \quad |t| = k$
- 3 for all distinct pairs are contained in exactly λ blocks (t)

Why **balanced** and **incomplete**?

balanced they share the same property (2)

incomplete by reason of $v = |S| > k = |t| \quad \forall t \in T$

What is Steiner Triple System 2

λ blocks (t) of $(v, k, \lambda) - \text{BIBD}$ iff $\lambda = 1, k = 3$.

$(v, k, \lambda) - \text{BIBD}$

v, k and λ be positive integers such that $v > k \geq 2$. A balanced incomplete block design is a *design* (S, T) such that satisfy these properties:

- 1 $|S| = v$
- 2 $\forall t \in T \quad |t| = k$
- 3 $\forall s \in S$ is contained in exactly λ blocks (t)

What is Steiner Triple System 2

λ blocks (t) of (v, k, λ) – BIBD iff $\lambda = 1, k = 3$.

(v, k, λ) – BIBD

v, k and λ be positive integers such that $v > k \geq 2$. A balanced incomplete block design is a *design* (S, T) such that satisfy these properties:

- 1 $|S| = v$
- 2 $\forall t \in T \quad |t| = k$
- 3 $\forall s \in S$ is contained in exactly λ blocks (t)

All theory from BIBD is shared too in STS

Existence proof

Theorem

A STS of order v **exists** if and only if $v \equiv 1, 3 \pmod{6}$

Proof.

(\Rightarrow) We know that all possible pairs are $\binom{v}{2}$, and by definition these pairs are partitioned (non-overlapping and union make all) into 3-element groups. Those groups are $|T| = \frac{\binom{v}{2}}{3} = \frac{v(v-1)}{6}$. Then for $\forall x \in S$ can be defined $T(x) = \{t \setminus \{x\} \mid x \in t \in T\}$. So if an $x \in S$ is fixed and then for every set t which contain x we remove the point x then we carry out $v-1$ point partitioned in 2-element set. As we can't make 2-element partition from a group of odd element, $v-1$ is even! So v is odd and it's equal to say $v \equiv 1, 3, 5 \pmod{6}$. The $\frac{v(v-1)}{6}$ is not an integer for every $v \equiv 5 \pmod{6}$. As a result $\text{STS} \Rightarrow v \equiv 1, 3 \pmod{6}$ □

Existence proof 2

$$(S, T) : |S| = v \wedge v \equiv 1, 3 \pmod{6} \Rightarrow STS(v)$$

In addition we suppose:

- each distinct pair of S belongs to *at least* one triple in T
- $|T| \leq \frac{v(v-1)}{6}$

Proof.

(Absurd) Assume the contrary and make a list L as follows: for every pair write down the triple with which it is associated. Then $|L| > \binom{v}{2}$ as there exists a pair with two triples. Now since each triple is counted by exactly three pairs so $|T| = |L|/3 > \frac{\binom{v}{2}}{3}$, a contradiction. \square

Proof.

For each distinct pair of S belongs to at least one triple and if the number of triples is less than or equal to the right number of triples, then each pair of symbols in S belongs to exactly one triple in T . \square

Corollary

A STS of order v has $|T| = \frac{v(v-1)}{6}$

Representation

How to represent

- through display each 3-set of T
($\{\{a, b, c\}, \{b, d, e\}, \dots, \{d, f, g\}\}$)
- through a *complete graph*

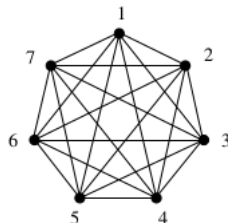


Figure: A complete graph of order $v = 7$

Example

Why a focus on representation?

- we talk about combinatorial design (display somehow somethings)
- help to design algorithm

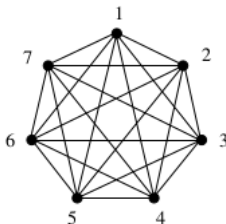


Figure: A complete graph of order $v = 7$

Focus on

How to choose a proper partition of the graph ?

Example

First non-dummy: STS of *order 7*

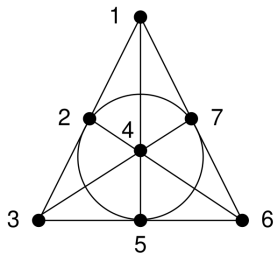


Figure: Fano plane

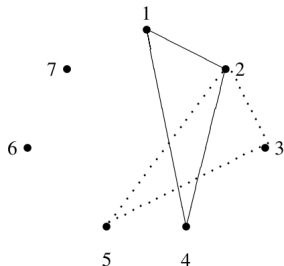


Figure: Building methods on STS(7)

Construction methods

How to create

- Bose method
- Skolem
- $6n + 5$
- With quasigroups with holes
- Wilson
- $2n + 1$
- $2n + 7$
- Even-Odd

Bose construction

We need first define:

idempotent commutative quasigroups of order $2n + 1$

But first: recap

(Definition) latin square of order n

is an $n \times n$ array where each row and column contains all symbols $\{1, \dots, n\}$ exactly one time.

1	3	2
2	1	3
3	2	1

Table: Latin square of order 3

(Definition) Quasigroup

A *quasigroup* of order n is an algebraic structure, a pair (Q, \circ) where $|Q| = n$ and $\circ : Q \times Q \rightarrow Q$.

$\forall a, b \in Q$ then $\exists! x, y$ (unique!) to the equations $a \circ x = b$ and $x \circ a = b$.

An examples of quasigroup are $(\mathbb{Z}_n, -), (\mathbb{Z}_n, +)$.

Quasigroup and latin square

Theorem

The multiplication table of a quasigroup is a Latin square

A quasigroup (G, \circ) is a latin square of order $v = |G|$:

1	3	2
2	1	3
3	2	1

Table: Latin square of order 3

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

Table: Quasigroup of order 3

Quasigroup and latin square

Theorem

The multiplication table of a quasigroup is a Latin square

A quasigroup (G, \circ) is a latin square of order $v = |G|$:

1	3	2
2	1	3
3	2	1

Table: Latin square of order 3

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

Table: Quasigroup of order 3

A (Q, \circ) is said:

idempotent $\forall i : 1 \leq i \leq |G|$ the cell (i, i) contains α such that $\alpha \leq i$

commutative $\forall i, j : 1 \leq i < j \leq |G|$ the cell (i, j) contains the same of (j, i)

Commutative idempotent latin square

1	3	2
3	2	1
2	1	3

Table: C. I. latin square of order 3

Commutative idempotent latin square

1	3	2
3	2	1
2	1	3

Table: C. I. latin square of order 3

How can we create a *C.I. latinsquare/quasigroup of order v* ?

Theorem

*idempotent commutative quasigroups exist **if and only if** they have odd order.*

Great! We look at the half of all possible

Construction method of CI quasigroup

- 1 Let v be the order of quasigroup, take $(Z_v, +)$ where $+$ is the addition in Z_v .
- 2 For all element $i := i + 1$
- 3 Take the elements of main diagonal $\langle d_1, \dots, d_v \rangle$. Build a permutation $\sigma_v = \{(d_1, 1), (d_2, 2), \dots, (d_v, v)\}$.
- 4 Apply σ_v for all element of the *multiplication table*

As result you have a CI quasigroup.

Construction method of CI quasigroup of order 7

$Z_7, +$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	4	5	6	7	1
3	3	4	5	6	7	1	2
4	4	5	6	7	1	2	3
5	5	6	7	1	2	3	4
6	6	7	1	2	3	4	5
7	7	1	2	3	4	5	6

- 1 Let v be the order of quasigroup, take $(Z_v, +)$ where $+$ is the addition in Z_v .
- 2 For all element $i := i + 1$

Construction method of CI quasigroup of order 7

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	4	5	6	7	1
3	3	4	5	6	7	1	2
4	4	5	6	7	1	2	3
5	5	6	7	1	2	3	4
6	6	7	1	2	3	4	5
7	7	1	2	3	4	5	6

$$\sigma_v = \{(1, 1), (3, 2), (5, 3), (7, 4), (2, 5), (4, 6), (6, 7)\}$$

- 1 Let v be the order of quasigroup, take $(Z_v, +)$ where $+$ is the addition in Z_v .
- 2 For all element $i := i + 1$
- 3 Take the elements of main diagonal $\langle d_1, \dots, d_v \rangle$. Build a permutation $\sigma_v = \{(d_1, 1), (d_2, 2), \dots, (d_v, v)\}$.
- 4 Apply σ_v for all element of the *multiplication table*

Construction method of CI quasigroup of order 7

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	4	5	6	7	1
3	3	4	5	6	7	1	2
4	4	5	6	7	1	2	3
5	5	6	7	1	2	3	4
6	6	7	1	2	3	4	5
7	7	1	2	3	4	5	6

	1	2	3	4	5	6	7
1	1	5	2	6	3	7	4
5	5	2	6	3	7	4	1
2	2	6	3	7	4	1	5
6	6	3	7	4	1	5	2
3	3	7	4	1	5	2	6
7	7	4	1	5	2	6	3
4	4	1	5	2	6	3	7

We apply $\sigma_v = \{(1, 1), (3, 2), (5, 3), (7, 4), (2, 5), (4, 6), (6, 7)\}$ as result we have a idempotent commutative quasigroup of order v .

Bose construction($v \equiv 3 \pmod{6}$)

Let $v = 6n + 3$ and let (Q, \circ) be an idempotent commutative quasigroup of order $2n + 1$, where $Q = \{1, 2, 3, \dots, 2n + 1\}$. Let $S = Q \times \{1, 2, 3\}$ and define T to contain the following types of triples.

Type 1: For $1 \leq i \leq 2n + 1$, $\{(i, 1), (i, 2), (i, 3)\} \in T$

Type 2: For $1 \leq i < j \leq 2n + 1$, $\{(i, 1), (j, 1), (i \circ j, 2)\}, \{(i, 2), (j, 2), (i \circ j, 3)\}, \{(i, 3), (j, 3), (i \circ j, 1)\} \in T$

Then (S, T) is a Steiner triple system of order $6n + 3$.

Type of partitions

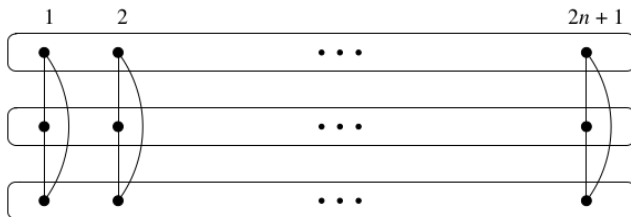


Figure: Type 1

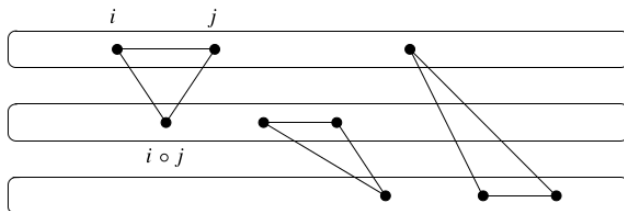


Figure: Type 2

Proof

$|T|$ is made up with 2 type:

- *Type 1*: $2n + 1$ triples
- *Type 2*: $\binom{2n+1}{2}$ choices for i and j , for all of them there are 3 another type.

Then $|T| = (2n + 1) + 3 \frac{(2n+1)2n}{2} = \frac{(2n+1)(6n+2)}{2} = v(v-1)/6$ have the right number of triple.

Show that at least one every pairs is contained in at least 1 triple:

Practical example

Cyclic Steiner triple system

STS \Rightarrow Idempotent totally symmetric quasigroup construction

Kirkamn triple systems

Intersections of Steiner Triple Systems

Teirlink's Algorithm

Embedding partial of Steiner Triple Systems

Teirlink's Algorithm

References I