Steiner Triple Systems

Existence,representation and construction

Luca Vecchi

University of Milan

December 5, 2018

Introduction

Outline

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

It has been shown that there is only one STS of orders $v = 3$, 7 or 9. There are two nonisomorphic designs for $v = 13$ and 80 distinct STS's with $v = 15$. This work was done by hand but the $v = 15$ case was verified by computer. Some upper and lower bounds are known for other STS's but no other exact counts.

Of course, it is well known that Steiner Triple Systems are equivalent to idempotent totally symmetric quasigroups and so are connected to Latin Squares.

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

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

Examples of STS

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

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 $v = |S| \quad > \quad k = |t| \ \forall t \in T$

What is Steiner Triple System 2

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

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

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 $(v, k, \lambda) - \mathrm{BIBD}$ iff $\lambda = 1,\ k = 3$.

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

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

[Kirkman, 1847]Existence proof

Theorem

A STS of order v **exists** *if and only if* $v \equiv 1, 3\ mod(6)$

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. Thoose groups are $|T| = \frac{\binom{v}{2}}{3} = \frac{v(v-1)}{6}$. Then for $\forall x \in S$ can be defined $T(x) = \{t \setminus \{x\} | x \in t \in T\}$. 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 $v \equiv 1, 3, 5 mod(6)$. The $\frac{v(v-1)}{6}$ is not an integer for every $v \equiv 5 mod(6)$. As a result STS $\Rightarrow v \equiv 1, 3\ mod(6)$ $\square$

Existence proof 2

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

In addition we suppose:

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

Proof 1.

(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 towo triples. Now since each triple is counted by exactly three pairs so $|T| = |L|/3 > \frac{\binom{v}{2}}{3}$, a contradiction. □

Proof 2.

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 sumbols in S belongs to exactly one triple in T. □

Proof 3.

We costruct 2 methods to prove sufficient costraint to the Theorem by showing 2 methods:

- Bose construction
- Skolem construction

□

Representation

How to represent

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

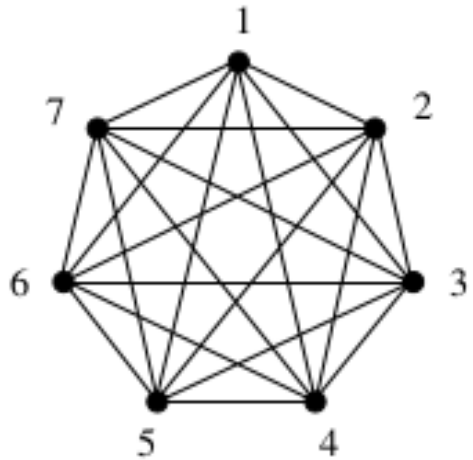


Figure: A complete graph of order $v = 7$

Example

Why a focus on representation?

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

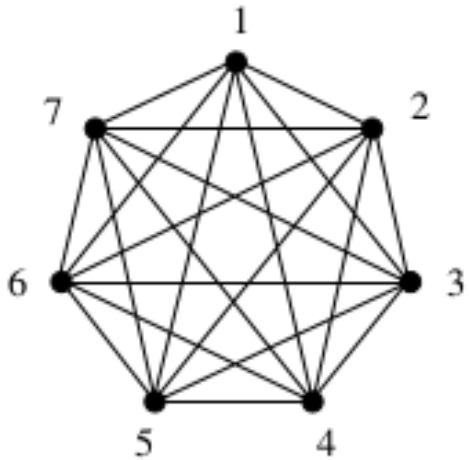


Figure: A complete graph of order $v = 7$

Focus on

How to choose a proper partition of the graph ?

Example

First non-dummy: STS of *order* 7

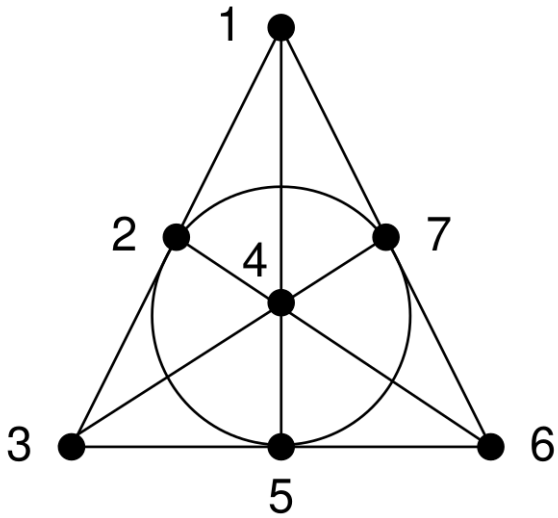


Figure: Fano plane

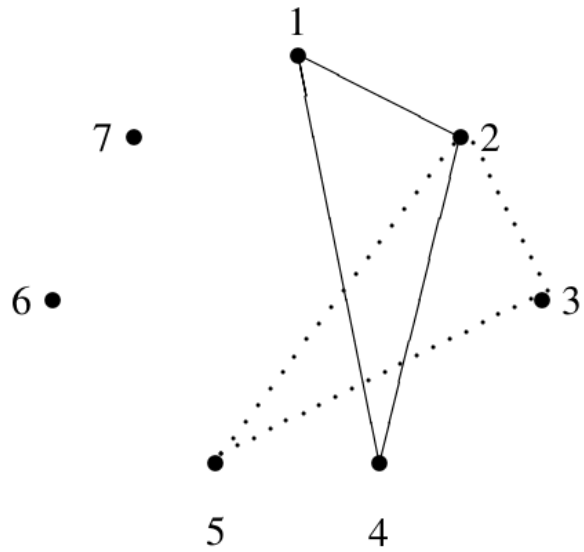


Figure: Building methods on STS(7)

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 $\{1, ..., n\}$ exactly one time.

1	3	2
2	1	3
3	2	1

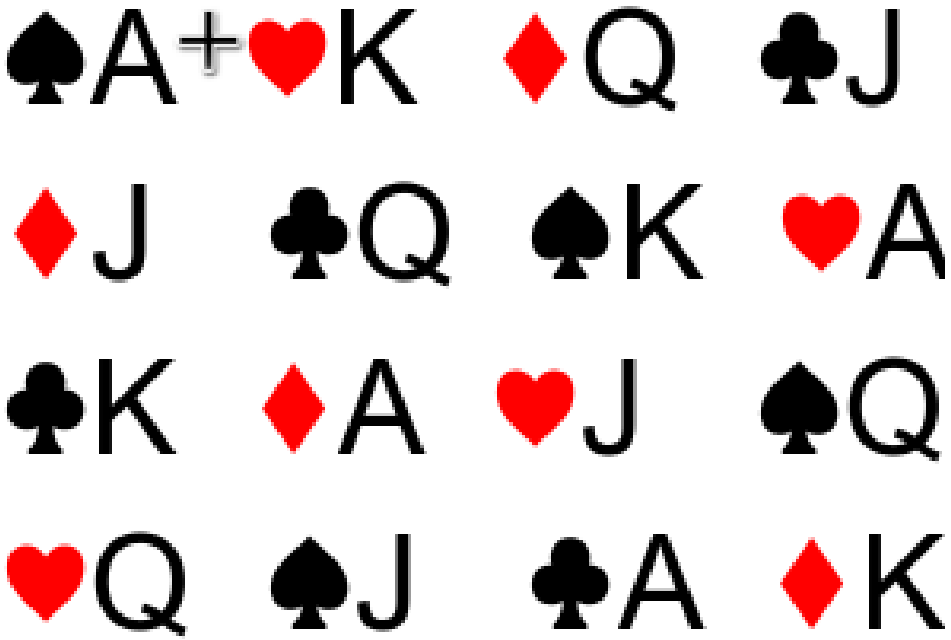
Table: Latin square of order 3

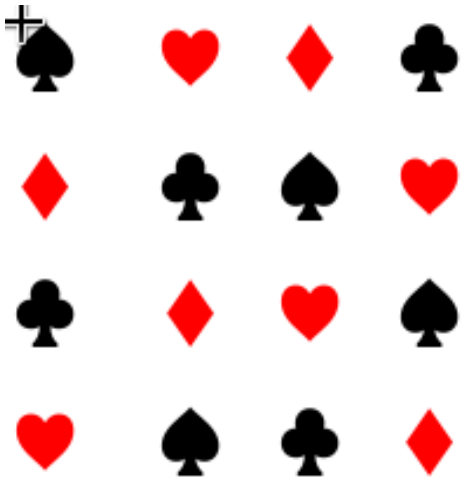
(Definition) Quasigroup

A *quasigroup* of *order* n is an algebric structure, a pair $(Q, \circ)$ where $|Q| = n$ and $\circ : Q \times Q \to Q$.
$\forall a, b \in Q$ then $\exists! x, y$ (unique!) to the equations $a \circ x = b$ and $x \circ a = b$.

An examples of quasigroup are $(\mathrm{Z_n}, -)$,$(\mathrm{Z_n}, +)$.

(Example) Latin square





A	K	Q	J
J	Q	K	A
K	A	J	Q
Q	J	A	K

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* ?

contenuto...

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 $< d_1, ..., d_v >$. Build a permutation $\sigma_v = \{(d_1, 1), (d_2, 2), ..., (d_v, v)\}$.
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 $< d_1, ..., d_v >$. Build a permutation $\sigma_v = \{(d_1, 1), (d_2, 2), ..., (d_v, v)\}$.
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($v \equiv 3 mod(6)$)

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

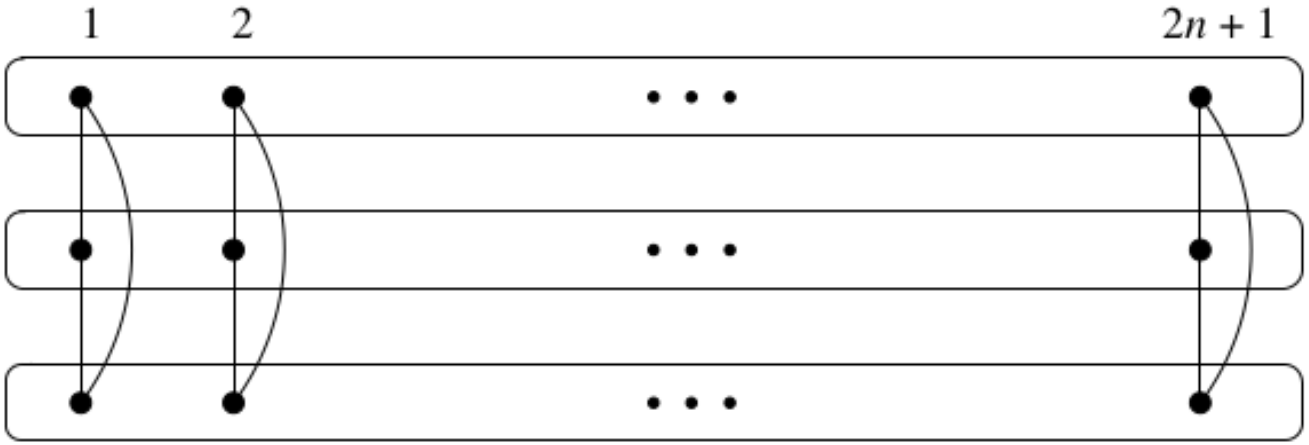


Figure: Type 1

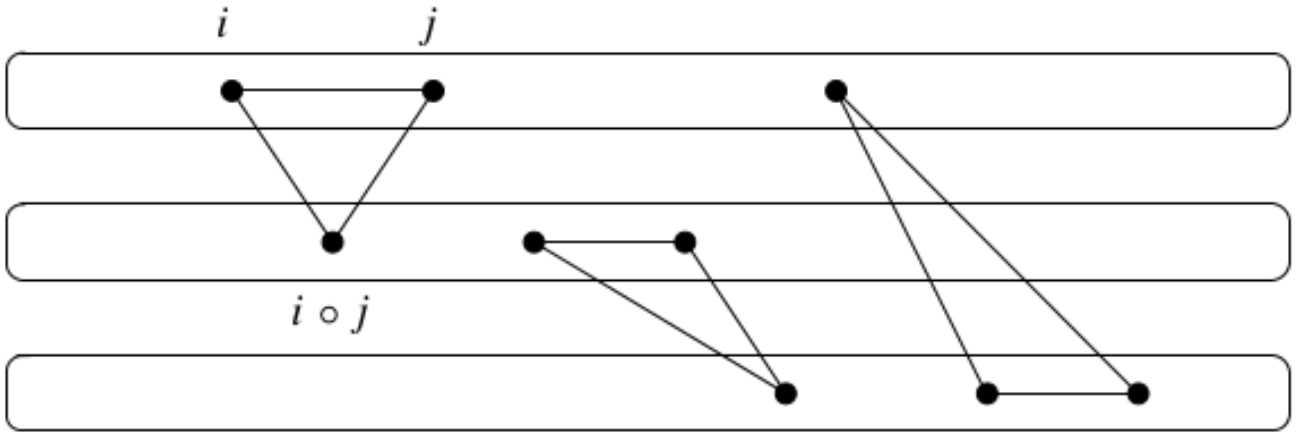


Figure: Type 2

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.
To show that every pairs is contained in at least 1 triple, think about 2 possible pair of point $(a,b),(c,d) \in Q \times \{1,2,3\}$:

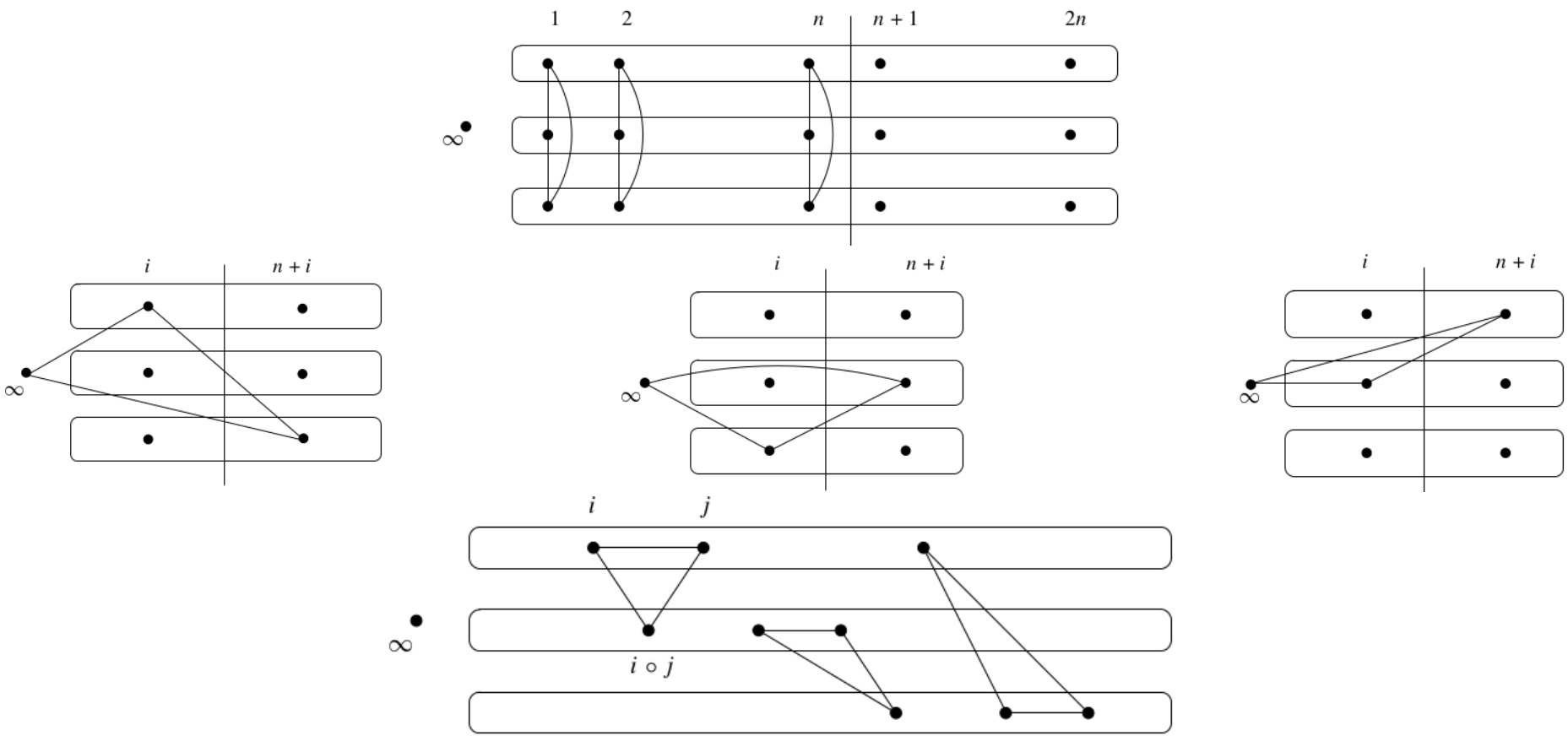
Cont..

$\forall (a,b),(c,d) \in Q \times \{1,2,3\}$

- $a = c \wedge b = d$ impossible
- if $a = c$ (so $b \neq d$) is contained in at least 1 triple of *type 1* $\{\{(a,1),(a,2),(a,3)\},\{(x,1),(a,1),(b,2)\},...\}$
- if $b = d \wedge a \neq c$ impossible) is contained in at least 1 triple of *type 2* $\{\{(a,b),(c,b),(a \circ c, b+1 mod(3)\ )\},\{(x,1),(a,1),(b,2)\},...\}$
- $a \neq c \wedge b \neq d$.Assume $b = 1$ and $d = 2$. Since $(Q,\circ)$ is a quasigroup $a \circ i = c$ and $j \circ a = c$ for some i,j. Because the *commutative* $i = j$ and because *idempotent* only $a \circ a = a$, all the others we are sure that $i \neq a$. So $\{(a,1),(i,1),(a \circ i = c,2)\}$.

All possible point have been shown that are in T.

Example Bose construction



Skolem construction ($v \equiv 3 mod(6)$)

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

Half-idempotent commutative latin square

(Definition)Half-idempotent commutative latin square

A latin square (multiplication table of quasigroup of the same order) L of order $2n$ is *half-idempotent* if the cells (i, i) contain the same symbol i of the cell $(n + i, n + i) \quad \forall 1 \leq i \leq n$

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

Half-idempotent latin square of order 4 ($n = 2$)

Half-idempotent commutative latin square

(Definition)Half-idempotent commutative latin square

A latin square (multiplication table of quasigroup of the same order) L of order $2n$ is *half-idempotent* if the cells (i, i) contain the same symbol i of the cell $(n+i, n+i) \quad \forall 1 \leq i \leq n$

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

Half-idempotent latin square of order 4 ($n = 2$)

Commutative half-idempotent latin squares exist for all *even* order.

Example half-idempotent quasigroup

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

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

Example half-idempotent quasigroup

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

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

How can we algorithmically build a H-I Latin Square?

How costruct H-I latin square/quasigroup

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

Table: Quasigroup $(\mathrm{Z}_6, +mod(6))$

How costruct H-I latin square/quasigroup

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

Table: Quasigroup $(Z_6, +mod(6))$

The bijection σ is built increasing all value by 1(or by taking the next element). Then by taking the main diagonal from the left grid $(< 1, 3, 5, ... >)$ and assign the right number $(< 1, 2, 3, ... >)$

How costruct H-I latin square/quasigroup

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

Table: Quasigroup $(Z_6, +mod(6))$

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

Table: Applied func σ on the quasigroup

The bijection σ is built increasing all value by 1(or by taking the next element). Then by taking the main diagonal from the left grid $(< 1, 3, 5, ... >)$ and assign the right number $(< 1, 2, 3, ... >)$

Example Skolem construction

Let $v = 6n + 1$ and let $(Q, \circ)$ be a half-idempotent commutative quasigroup of order $2n$, where $Q = \{1, 2, 3, ..., 2n\}$. Let $S = \{\infty\} \cup (Q \times \{1, 2, 3\})$. We define T as follow:

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

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

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

We have to prove (in a similar way of Bose) there are the right number of $t \in T$ and every pair (from $\binom{6n+1}{2}$) is contained almost 1.

1: Right number of $|T|$.

We sum up 3 different element:

- *type 1*: for $1 \leq i \leq n$, $\{(i,1),(i,2),(i,3)\} \in T$ are n
- *type 2*: for $1 \leq i \leq n$, $\{\infty,(n+i,3),(i,2)\},\{\infty,(n+i,2),(n+i,3)\},\{\infty,(n+i,3),(i,1)\} \in T$ are $3n$
- *type 3*: for $1 \leq i < j \leq 2n$,$\{(i,1),(j,1),(i \circ j,2)\},\{(i,2),(j,2),(i \circ j,3)\},\{\} \in T$ are $3\binom{2n}{2}$

We have to prove $|T| = \frac{v(v-1)}{6} = \frac{(6n+1)(6n)}{6} = n + n + 3\binom{2n}{2}$.
Easily $n + 3n + 3\binom{2n}{2} = \frac{2n*4+2n*(6n-3)}{2} = \frac{2n(6n+1)}{2} = \frac{3}{3}\frac{2n(6n+1)}{2} = \frac{6n(6n+1)}{2} = |T|$ □

2: every pair of point $\in T$.

We have to prove all possible pair of point (a, b) and (c, d):

- $a = c = \infty \wedge b \neq d$
- $a = c \neq \infty \wedge b \neq d$
- $a = \infty \neq b \wedge b = d$
- $a \neq c \wedge b \neq d$

2: every pair of point $\in T$.

We have to prove all possible pair of point (a, b) and (c, d):

- $a = c = \infty \wedge b \neq d$
- $a = c \neq \infty \wedge b \neq d$
- $a = \infty \neq b \wedge b = d$
- $a \neq c \wedge b \neq d$

□

All covered by Skolem construction $\wedge$ $|T|$ is the right number $\Rightarrow$ is a STS($2n$)

Practical example

[1850] The Lady's and Gentleman's Diary/Kirkman's shoolgirl problem

A teacher would like to take 15 schoolgirls out for a walk, the girls being arranged in 5 rows of three. The teacher would like to ensure equal chances of friendship between any two girls. Hence it is desirable to find different row arrangements for the 7 days of the week such that any pair of girls walk in the same row exactly one day of the week.

[1850] The Lady's and Gentleman's Diary/Kirkman's shoolgirl problem

A teacher would like to take 15 schoolgirls out for a walk, the girls being arranged in 5 rows of three. The teacher would like to ensure equal chances of friendship between any two girls. Hence it is desirable to find different row arrangements for the 7 days of the week such that any pair of girls walk in the same row exactly one day of the week.

Solution

[1971 (Ray-Chaudhuri and Wilson)] it asks for a Steiner Triple System on $6t + 3$ varieties whose blocks can be partitioned into $3t + 1$ sets so that any variety appears only once in a set.

Important remark

Theorem

If a $(v, k, \lambda) - BIBD$ *exist, then* $\lambda(v-1) \equiv 0(mod(k-1))$ *and* $\lambda v(v-1) \equiv (modk(k-1))$.

Theorem

A STS of order v **exists** *if and only if* $v \equiv 1, 3\ mod(6)$

Theorem

If a $(v, k, \lambda) - BIBD$ *exist, then* $\lambda(v-1) \equiv 0(mod(k-1))$ *and* $\lambda v(v-1) \equiv (modk(k-1))$.

Only **necessary**.

Theorem

A STS of order v **exists** *if and only if* $v \equiv 1, 3\ mod(6)$

Necessary and **sufficient**.

STS on OEIS

Steiner systems , sequences related to :

Steiner systems, quadruple (SQS's): A051390* A124120 A124119

Steiner systems: A001293* (S(5,8,24))

Steiner systems: A187567 and A187585 (S(2,4,n))

Steiner triple systems (STS's): A001201*, A030128*, A030129*, A051390*, A002885 (cyclic), A006181, A006182, A051391

Isomorphisms between two *design*

Isomorphism

Two designs (X, A) and (Y, B) where $|X| = |Y|$ are *isomorphic* if there *exists* a bijection $\alpha : X \to Y$ such that:

$$[\{\alpha(x) : x \in A\} : A\mathrm{A}] = \mathrm{B}$$

Then α is called isomorphism.

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

$$Y = \{a, b, c, d, e, f, g\}, \quad \text{and}$$
$$\mathcal{B} = \{abd, bce, cdf, deg, aef, bfg, acg\}.$$

Beyond Existence or non-existence

The existence of non-isomorphic STS is complex and a open field.

Beyond Existence or non-existence

The existence of non-isomorphic STS is complex and a open field.

(A030129) Number of nonisomorphic Steiner triple systems (STS's) $S(2,3,n)$ on n points

$< 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 2, 0, 80, 0, 0, 0, 11084874829 >$

(A051390)Number of nonisomorphic Steiner quadruple systems (SQS's) of order n

$< 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 4, 0, 1054163 >$

References