# Steiner Triple Systems

# Definition

*Welcome to the Sacred Order of Steiner Systems.*

*Our Motto: When in doubt … count!*

**A Steiner Triple System, denoted by STS(v), is a pair (S,T) consisting of a set S with v elements, and a set T consisting of triples of S (called blocks) such that every pair of elements of S appear together in a unique triple of T.**

# Examples

I. v = 7

S = {0,1,2,...,6}   T = {013, 124, 235, 346, 450, 561, 602}

II. v = 3 (a trivial example)

S = {0,1,2}   T = {012}

III. v = 1 (an even more trivial example)

S = {1}   T = ∅

IV. v = 9 (something with a bit more meat)

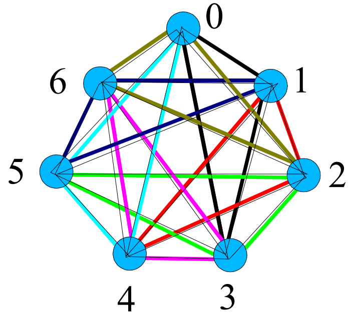
S = {1,2,...,9}

T = {123, 147, 159, 168, 456, 258, 267, 249, 789, 369, 348, 357}

# A Graph Theoretic View

Another way to look at Steiner Triple Systems -

Consider the complete graph on v vertices, $K_v$. A decomposition of $K_v$ into edge disjoint triangles ($K_3$'s) is equivalent to a Steiner Triple System.



# Necessity

The existence question (*for which v's does an STS(v) exist?*) was first posed by W.S.B. Woolhouse (Prize question 1733, Lady's and Gentlemens' Diary, 1844).

The problem was solved in 1847 by Rev. T.P. Kirkman:

**Theorem 1.1.3**: *A Steiner triple system of order v exists if and only if $v \equiv 1$ or 3 (mod 6).*

We will first prove the necessity of this condition. The sufficiency involves constructing STS(v)'s and we shall take up that task next.

# Necessity

**Theorem 1.1.3**: *A Steiner triple system of order v exists if and only if $v \equiv 1$ or 3 (mod 6).*

*Pf (necessity)*: Let (S,T) be an STS(v). Any triple, {a,b,c} contains three 2-element subsets and S contains ½ v(v-1) 2-element subsets. As every pair appears in a unique triple, we have $3|T| = \frac{1}{2} v(v-1)$, so

$$|T| = v(v-1)/6.$$

For any $x \in S$, the triples containing x partition S-{x} into pairs, thus v-1 is even, so v is odd. Therefore, $v \equiv 1,3$ or 5 (mod 6). However, if v = 6k+5, computing |T| gives:

$$|T| = (6k+5)(6k+4)/6 = (36k^2 +54k + 20)/6$$

which is not an integer, so this case is eliminated. ❑

# An Old Problem

Arrange the 16 face cards of a deck of playing cards in a 4 x 4 array so that each denomination (Ace, King, Queen, Jack) and each suit (Clubs, Hearts, Diamonds, Spades) appears only once in each row and column.

| | | | |
|---|---|---|---|
| ♠A | ♥K | ♦Q | ♣J |
| ♦J | ♣Q | ♠K | ♥A |
| ♣K | ♦A | ♥J | ♠Q |
| ♥Q | ♠J | ♣A | ♦K |

An enumeration by type of the solutions to this problem was published in **1723**.

# Latin Squares

If we seperate the denominations and the suits we obtain:

| | | | |
|---|---|---|---|
| ♠ | ♥ | ♦ | ♣ |
| ♦ | ♣ | ♠ | ♥ |
| ♣ | ♦ | ♥ | ♠ |
| ♥ | ♠ | ♣ | ♦ |

| | | | |
|---|---|---|---|
| A | K | Q | J |
| J | Q | K | A |
| K | A | J | Q |
| Q | J | A | K |

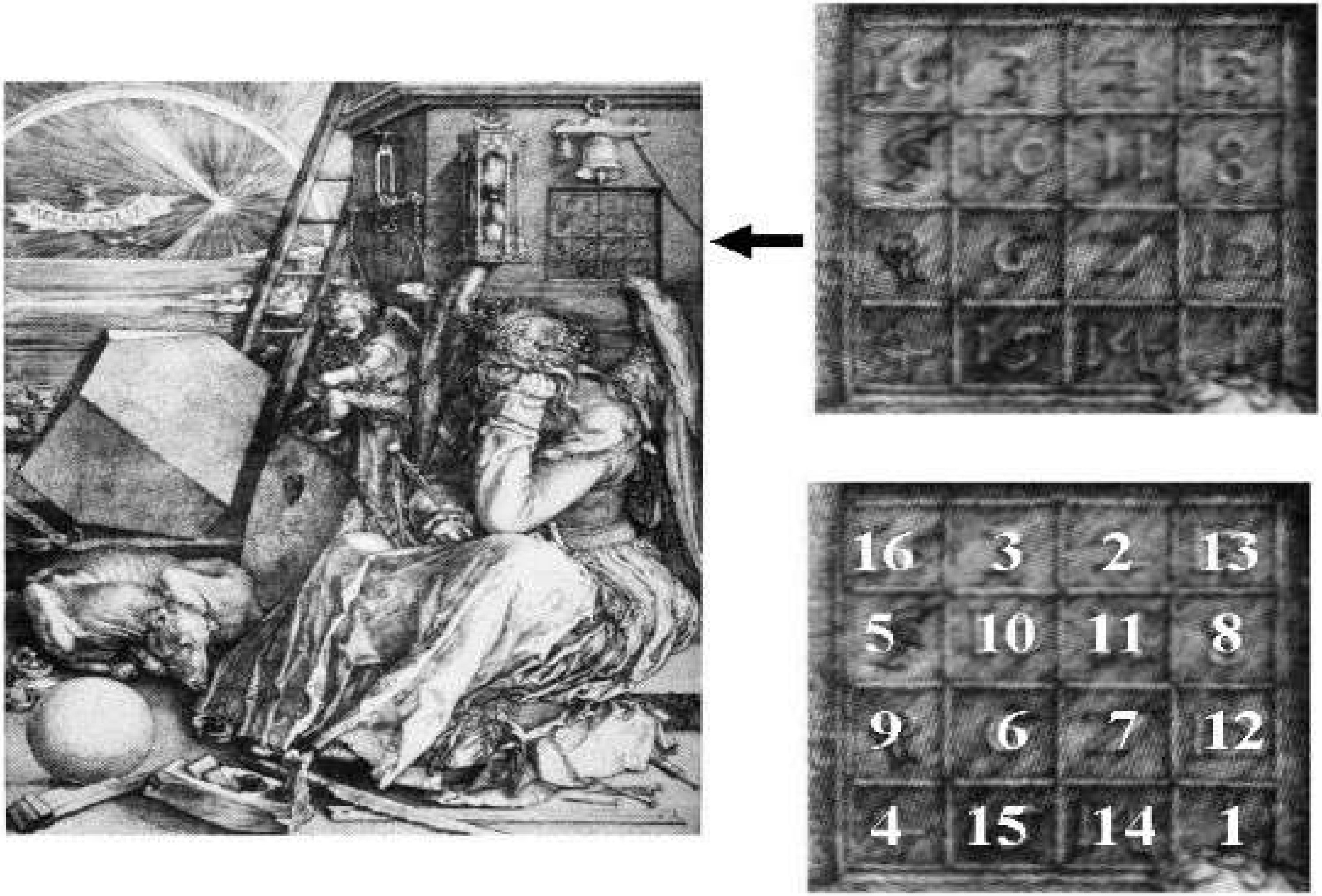
Each of these is a 4x4 Latin square.

A **Latin square** is an n x n square matrix whose entries consist of n symbols such that each symbol appears exactly once in each row and each column.

# Latin Squares

Latin squares have a long history. The concept probably originated with problems concerning the movement and disposition of pieces on a chess board. However, the earliest written reference is the solutions of the card problem published in 1723.  The Latin square concept certainly goes back further than this written document. In his famous etching ***Melencholia I***, the 16th Century artist Albrecht Dürer portrays an order 4 magic square,a relative of Latin squares, in the background. Magic squares can also be found in the ancient Chinese literature.

# Melencholia I



| | | | |
|---|---|---|---|
| 16 | 3 | 2 | 13 |
| 5 | 10 | 11 | 8 |
| 9 | 6 | 7 | 12 |
| 4 | 15 | 14 | 1 |

Albrecht Dürer's *Melencholia I* (1514)
with Magic Square of order 4.

# Latin Squares

The systematic development of Latin squares started with Euler (1779) and was carried on by Cayley (1877-1890) who showed that the multiplication table of a group is an appropriately bordered special Latin square. In the 1930's the concept arose once again in the guise of multiplication tables when the theory of quasi-groups and loops began to be developed as a  generalization of the group concept. Latin squares played an important role in the foundations of finite geometries, a subject which was also in  development at this time.

Also in the 1930's, a big application area for Latin squares was opened by R.A.Fisher who used them and other combinatorial structures in the design of statistical experiments.

# Quasigroups

A **Quasigroup** $(S,\otimes)$ is a set S together with a binary operation $(\otimes)$ such that:

1. The operation is closed (i.e., $a\otimes b\in S,\ \forall\ a,b\in S$)
2. Given $a,b\in S$ the equations

    i) $a\otimes x = b$ and
    ii) $y\otimes a = b$

    have unique solutions for x and y.

# Example

A simple example of a finite quasigroup is given by the set {0,1,2} with the operation ⊗ defined by a⊗b = 2a+b+1 where the operations on the right are the usual multiplication and addition modulo 3. The multiplication table for this quasigroup is given below:

| (⊗) | **0** | **1** | **2** |
|---|---|---|---|
| **0** | 1 | 2 | 0 |
| **1** | 0 | 1 | 2 |
| **2** | 2 | 0 | 1 |

# Latin Squares and Quasigroups

The simple result which causes our interest in these algebraic forms is:

**Theorem I.1.1.1** - *The multiplication table of a quasigroup is a Latin square.*

*Proof*: Let $a_1$ ,$a_2$ ,...,$a_n$ be the elements of the quasigroup and let its multiplication table be as below:

$$\begin{array}{c|cccccc}
 & a_1 & a_2 & \cdots & a_s & \cdots & a_n \\ \hline
a_1 & a_{11} & a_{12} & \cdots & a_{1s} & \cdots & a_{1n} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
a_r & a_{r1} & a_{r2} & \cdots & a_{rs} & \cdots & a_{rn} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
a_n & a_{n1} & a_{n2} & \cdots & a_{ns} & \cdots & a_{nn}
\end{array}.$$

# Latin Squares and Quasigroups

**Theorem I.1.1.1** - *The multiplication table of a quasigroup is a Latin square.*

*Proof (cont)*: Where the entry $a_{rs}$ which occurs in the r-th row and s-th column is the product $a_r \otimes a_s$ of the elements $a_r$ and $a_s$ . If the same entry occured twice in the r-th row, say in the s-th and t-th columns so that $a_{rs} = a_{rt} = b$ say, we would have two solutions to the equation $a_r \otimes x = b$, in contradiction to the quasigroup axiom. Similarly, if the same entry occurred twice in the s-th column, we would have two solutions to the equation $y \otimes a_s = c$ for some c. We conclude that each element of the quasigroup occurs exactly once in each row and column, and so the unbordered multiplication table (which is an nxn array) is a latin square. ❑

# Quasigroup Properties

A quasigroup (latin square) is ***idempotent*** if $a \otimes a = a\ \forall\ a$ (cell (i,i) contains symbol i for $1 \leq i \leq n$.)

A quasigroup (latin square) is ***commutative*** if $a \otimes b = b \otimes a\ \forall\ a,b$ (cells (i,j) and (j,i) contain the same symbol for $1 \leq i,j \leq n$.)

Examples of commutative idempotent 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 |

# Commutative Idempotent LS's

There is no commutative idempotent latin square of even order (prove this).

For any n = 2k+1, there exists a commutative idempotent latin square of order n.

Start with the addition table of the cyclic group $\mathbb{Z}_{2n+1}$ and rename the elements so that the main diagonal is in the appropriate order.

$$
\begin{array}{ccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 \\
1 & 2 & 3 & 4 & 5 & 6 & 0 \\
2 & 3 & 4 & 5 & 6 & 0 & 1 \\
3 & 4 & 5 & 6 & 0 & 1 & 2 \\
4 & 5 & 6 & 0 & 1 & 2 & 3 \\
5 & 6 & 0 & 1 & 2 & 3 & 4 \\
6 & 0 & 1 & 2 & 3 & 4 & 5
\end{array}
\quad \Rightarrow \quad
\begin{array}{ccccccc}
\mathbf{0} & 4 & 1 & 5 & 2 & 6 & 3 \\
4 & \mathbf{1} & 5 & 2 & 6 & 3 & 0 \\
1 & 5 & \mathbf{2} & 6 & 3 & 0 & 4 \\
5 & 2 & 6 & \mathbf{3} & 0 & 4 & 1 \\
2 & 6 & 3 & 0 & \mathbf{4} & 1 & 5 \\
6 & 3 & 0 & 4 & 1 & \mathbf{5} & 2 \\
3 & 0 & 4 & 1 & 5 & 2 & \mathbf{6}
\end{array}
$$

# Bose Construction (v=6n+3)

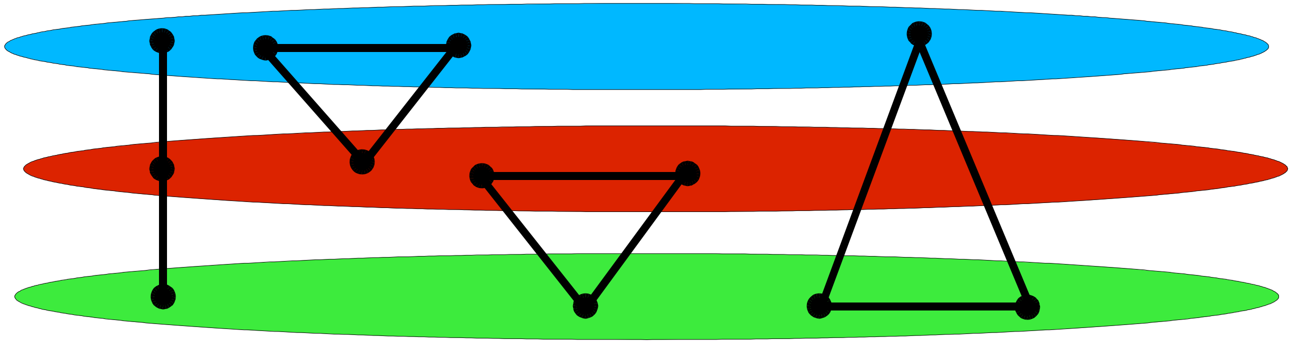
The Bose construction of an STS(6n+3) for any natural number n, utilizes a commutative idempotent quasigroup (Q,⊗) of order 2n+1.

The set S consists of the 6n+3 ordered pairs of Q x {0,1,2} and the triples T are of two types:

Type 1 : {(i,0), (i,1), (i,2)} for each i ∈ Q.

Type 2 : {(i,k), (j,k), (i⊗j, k+1 (mod 3))} for i ≠ j

We can visualize the triples by considering 3 copies of Q:



# Bose Construction

To show that this construction gives an STS we first count the number of triples:

There are 2n+1 triples of type 1 and $3(2n+1)(2n)/2 = 6n^2+3n$ triples of type 2. Thus,

$$|T| = 6n^2+5n+1 = (6n+3)(6n+2)/6 = v(v-1)/6.$$

To prove that this is an STS we need only show that each pair of distinct elements of S are contained in a triple (since the number of triples is correct this will force each pair to be in a unique triple).

# Bose Construction

Let $(a,b)$ and $(c,d)$ be distinct elements of $S$.

If $a = c$ then this pair is in a triple of type 1. We now assume that $a \neq c$. If $b = d$, the pair is in a triple of type 2.

We now also assume that $b \neq d$. Now, either $d = b+1 (\mathrm{mod}\ 3)$ or $d = b-1\ (\mathrm{mod}\ 3)$. In the first case, let $x$ be the unique solution of $a \otimes x = c$ in $Q$. The triple containing the pair is thus $\{(a,b), (x,b), (c,d)\}$. In the second case, let $y$ be the unique solution of $y \otimes c = a$ in $Q$. The triple is then $\{(y,d), (c,d), (a,b)\}$.

# Half-Idempotent Commutative Latin Squares

While there are no commutative idempotent latin squares of even order, we can obtain something similar.

A latin square (quasigroup) L of order 2n is ***half-idempotent*** if the cells (i,i) and (n+i,n+i) contain the symbol i, for every $1 \leq i \leq n$.

Examples:

| | | | |
|---|---|---|---|
| 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 |

# Half-Idempotent Commutative Latin Squares

Commutative half-idempotent latin squares exist for all even orders 2n (n ≥ 1):

Write the addition table for $\mathbb{Z}_{2n}$ and then rename the elements so that the main diagonal is appropriate:

$$\begin{array}{cccccc} 0&1&2&3&4&5\\ 1&2&3&4&5&0\\ 2&3&4&5&0&1\\ 3&4&5&0&1&2\\ 4&5&0&1&2&3\\ 5&0&1&2&3&4 \end{array} \quad \Rightarrow \quad \begin{array}{cccccc} 1&4&2&5&3&6\\ 4&2&5&3&6&1\\ 2&5&3&6&1&4\\ 5&3&6&1&4&2\\ 3&6&1&4&2&5\\ 6&1&4&2&5&3 \end{array}$$

using the bijection 0 → 1, 1 → 4, 2 → 2, 3 → 5, 4 → 3, 5 → 6.

# Skolem Construction (v=6n+1)

This construction of an STS(6n+1) starts with a set S consisting of the 6n ordered pairs of Qx{0,1,2}, where (Q,⊗) is a commutative half-idempotent quasigroup of order 2n, together with a special symbol called ∞.

To describe the triples we assume that the quasigroup Q has symbols {1,2,...,2n}. The triples are then:

Type 1: {(i,0), (i,1), (i,2)} for $1 \le i \le n$. (note: it stops at n)

Type 2: { ∞, (i,k), (n+i, k-1 mod 3)} for $1 \le i \le n$.

Type 3: {(i,k), (j,k), (i⊗j, k+1 (mod 3))} for $1 \le i < j \le 2n$.

Note that the type 3 triples here are precisely the same as the type 2 triples in the Bose construction.

# Skolem Construction

We again count the number of triples:

There are n triples of type 1, 3n triples of type 2 and $3(2n)(2n-1)/2 = 6n^2 – 3n$ triples of type 3. This gives

$$|T| = 6n^2 + n = (6n+1)(6n)/6 = v(v-1)/6.$$

Again, to show that we have constructed an STS, we need to show that each pair of elements is contained in a triple.

Any pair including the symbol $\infty$ is contained in a type 2 triple.

Suppose (a,b) and (c,d) are a pair of elements of S.

If $a = c$ and $a \le n$, then the pair is contained in a triple of type 1.

# Skolem Construction

Suppose (a,b) and (c,d) are a pair of elements of S. Now suppose that $a = c$ and $a > n$. Since $b \neq d$, either $d = b+1 \pmod 3$ or $d = b-1 \pmod 3$. In the first case, let x be the unique solution of $a \otimes x = a$ in Q. Since $a > n$, $x \neq a$. The triple containing the pair is thus {(a,b), (x,b), (a,d)}. In the second case, let y be the unique solution of $y \otimes a = a$ in Q. Again, $y \neq a$ and the triple is then {(y,d), (a,d), (a,b)}.

We can now assume that $a \neq c$. If $b = d$, then a triple of type 3 contains the pair, so we can also assume that $b \neq d$. Again, either $d = b+1 \pmod 3$ or $d = b-1 \pmod 3$. In the first case, let x be the unique solution of $a \otimes x = c$ in Q. If $x \neq a$, then the type 3 triple {(a,b), (x,b), (c,d)} contains the pair. If on the other hand $x = a$, then $a > n$, since $a \neq c$. In this case, $a = n + c$ and the pair is in the type 2 triple {∞, (c,d), (n+c,b)}. The other possibility for d is treated similarly.

# Theorem 1.1.3

These two constructions prove the sufficiency part of the existence theorem for Steiner Triple systems.

We will now ask the question ... How close to an STS can we get with a set of size v = 6n+5? As we shall see, we can get very close .... all the blocks have size 3 except for one of size 5. This of course is not an STS, but it is of interest and will be useful for other constructions.

# Linear Spaces

A ***Linear Space*** is a pair (S,B) where S is a set and B is a collection of subsets of S (whose sizes may vary) such that every pair of elements of S appear together in a unique subset in B. The subsets of B are called **blocks**.

Linear spaces are also called ***Pairwise Block Designs*** (PBD's), a terminology preferred by design theorists (and the authors of our text).

Note that STS's are just PBD's with the additional restriction that all blocks have size 3.

# The 6n+5 Construction

We can construct a PBD with 6n+5 elements having one block of size 5 and all remaining blocks of size 3.

The construction uses an idempotent commutative quasigroup $(Q,\otimes)$ on the set $\{1,2,...,2n+1\}$ and a permutation of this set, $\alpha = (1)(2\ 3\ 4\ ...\ 2n+1)$.

The set S consists of two special elements $\infty_1$ and $\infty_2$, and the ordered pairs of $Q \times \{0,1,2\}$.

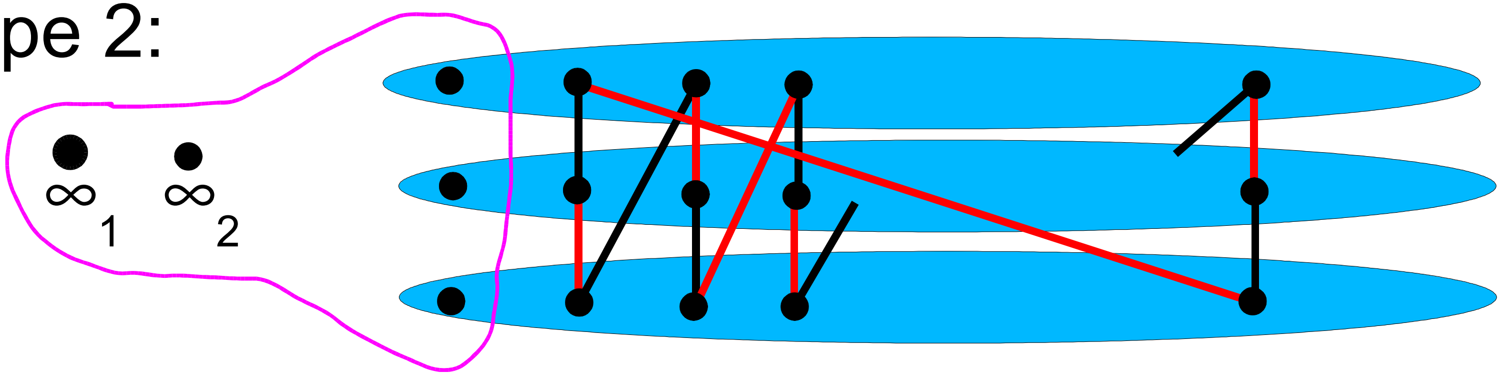
The blocks are:

Type 1: (the unique block of size 5)

$\{\infty_1, \infty_2, (1,0), (1,1), (1,2)\}$

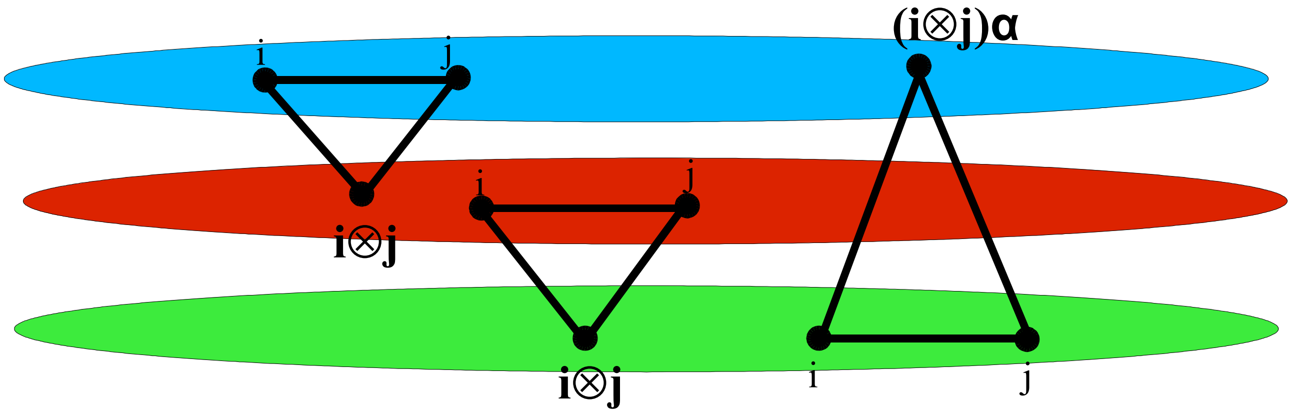
# The 6n+5 Construction

Type 2:



Black edges together with $\infty_1$ and red edges with $\infty_2$

Type 3:


i
j
i⊗j
i
j
i⊗j
(i⊗j)α
i
j