Symmetries of Latin Squares

Ian Wanless

Monash University, Australia

Joint work with Brendan McKay, Doug Stones,
Petr Vojtěchovský and Xiande Zhang

Latin squares

A *Latin square* of order n is an $n \times n$ matrix in which each of n symbols occurs exactly once in each row and once in each column.

e.g. $\begin{pmatrix} 3 & 6 & 1 & 2 & 5 & 4 \\ 4 & 1 & 2 & 3 & 6 & 5 \\ 5 & 2 & 3 & 4 & 1 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \\ 1 & 4 & 5 & 6 & 3 & 2 \\ 2 & 5 & 6 & 1 & 4 & 3 \end{pmatrix}$ is a Latin square of order 6.

Latin squares

A *Latin square* of order n is an $n \times n$ matrix in which each of n symbols occurs exactly once in each row and once in each column.

e.g. $\begin{pmatrix} 3 & 6 & 1 & 2 & 5 & 4 \\ 4 & 1 & 2 & 3 & 6 & 5 \\ 5 & 2 & 3 & 4 & 1 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \\ 1 & 4 & 5 & 6 & 3 & 2 \\ 2 & 5 & 6 & 1 & 4 & 3 \end{pmatrix}$ is a Latin square of order 6.

Latin squares are very useful for designing experiments,

Latin squares

A *Latin square* of order n is an $n \times n$ matrix in which each of n symbols occurs exactly once in each row and once in each column.

e.g. $\begin{pmatrix} 3 & 6 & 1 & 2 & 5 & 4 \\ 4 & 1 & 2 & 3 & 6 & 5 \\ 5 & 2 & 3 & 4 & 1 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \\ 1 & 4 & 5 & 6 & 3 & 2 \\ 2 & 5 & 6 & 1 & 4 & 3 \end{pmatrix}$ is a Latin square of order 6.

Latin squares are very useful for designing experiments, scheduling tournaments,

Latin squares

A *Latin square* of order n is an $n \times n$ matrix in which each of n symbols occurs exactly once in each row and once in each column.

e.g. $\begin{pmatrix} 3 & 6 & 1 & 2 & 5 & 4 \\ 4 & 1 & 2 & 3 & 6 & 5 \\ 5 & 2 & 3 & 4 & 1 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \\ 1 & 4 & 5 & 6 & 3 & 2 \\ 2 & 5 & 6 & 1 & 4 & 3 \end{pmatrix}$ is a Latin square of order 6.

Latin squares are very useful for designing experiments, scheduling tournaments, creating codes for communication,

Latin squares

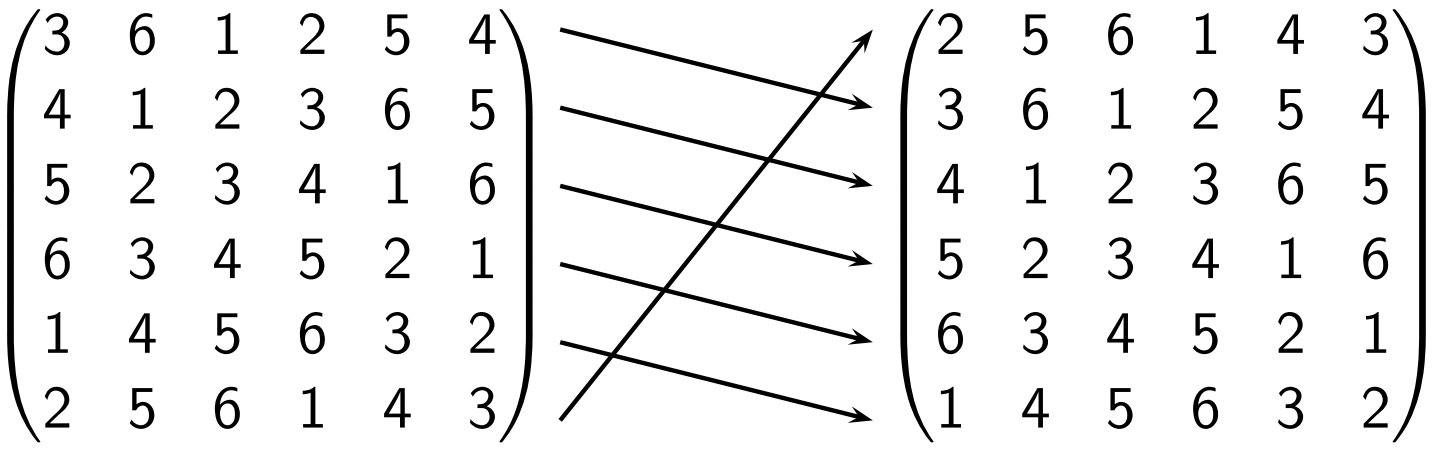
A *Latin square* of order n is an $n \times n$ matrix in which each of n symbols occurs exactly once in each row and once in each column.

e.g. $\begin{pmatrix} 3 & 6 & 1 & 2 & 5 & 4 \\ 4 & 1 & 2 & 3 & 6 & 5 \\ 5 & 2 & 3 & 4 & 1 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \\ 1 & 4 & 5 & 6 & 3 & 2 \\ 2 & 5 & 6 & 1 & 4 & 3 \end{pmatrix}$ is a Latin square of order 6.

Latin squares are very useful for designing experiments, scheduling tournaments, creating codes for communication, and entertaining commuters on trains.

Transformations and Symmetries

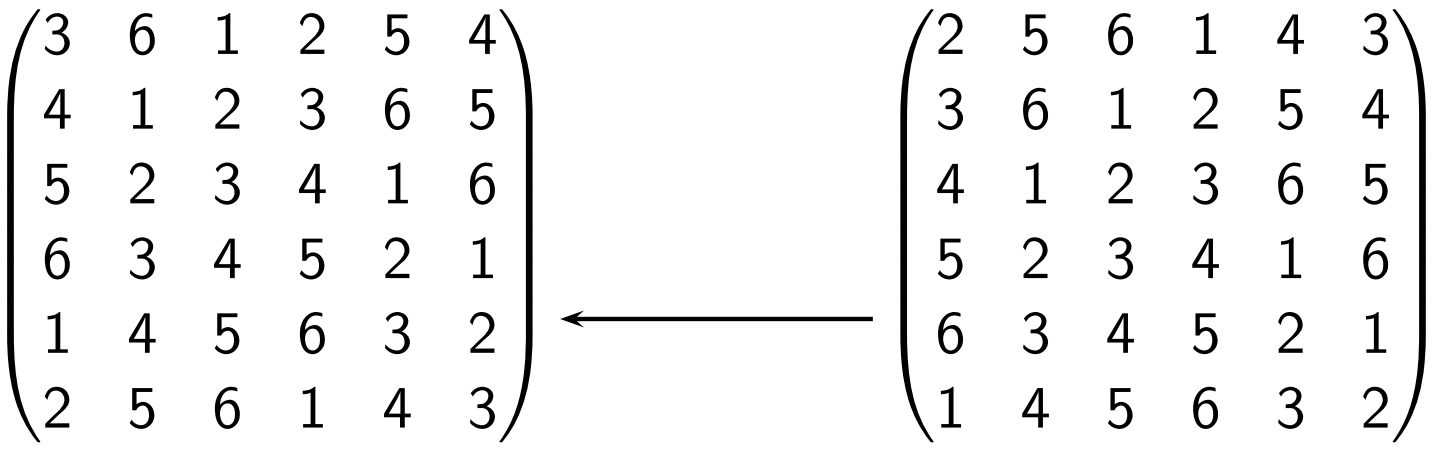
A *symmetry* of a Latin square is a transformation that leaves it unchanged.



Suppose we apply the permutation (123456) to the rows

Transformations and Symmetries

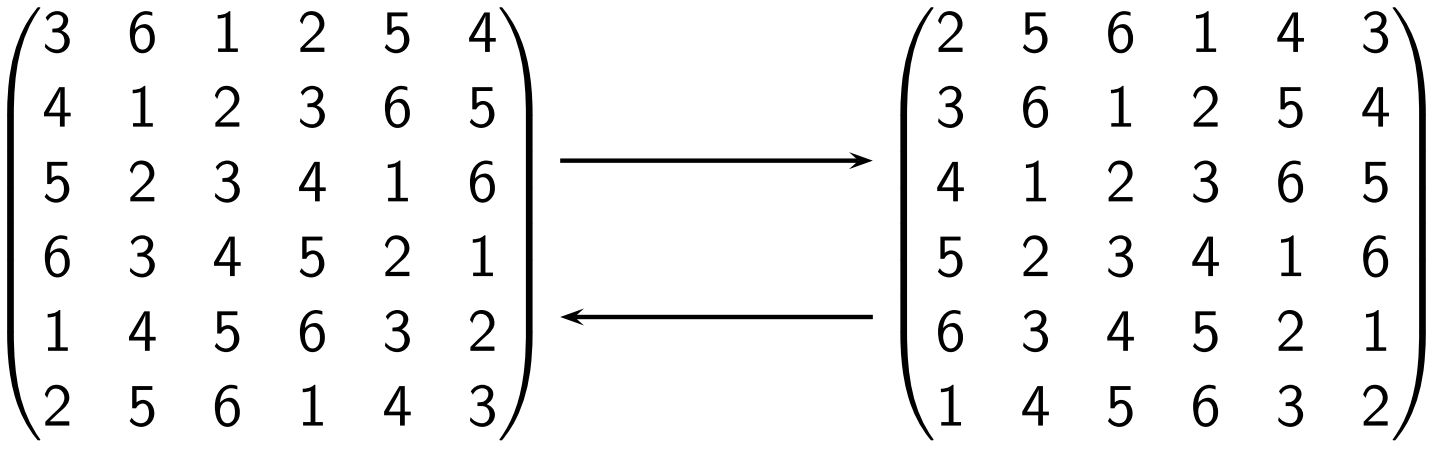
A *symmetry* of a Latin square is a transformation that leaves it unchanged.



Suppose we apply the permutation (123456) to the rows
. . . and then apply the permutation (123456) to the symbols.

Transformations and Symmetries

A *symmetry* of a Latin square is a transformation that leaves it unchanged.



Suppose we apply the permutation (123456) to the rows
. . . and then apply the permutation (123456) to the symbols.

The combination of these two transformations is a symmetry of our Latin square.

Another example

$$\begin{pmatrix} 4 & 1 & 3 & 5 & 2 \\ 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix}$$

Another example

$$\begin{pmatrix} 4 & 1 & 3 & 5 & 2 \\ 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix} \rightarrow \begin{pmatrix} 5 & 2 & 4 & 1 & 3 \\ 4 & 1 & 3 & 5 & 2 \\ 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}$$

If we apply the permutation (12345) to the rows,

Another example

$$\begin{pmatrix} 4 & 1 & 3 & 5 & 2 \\ 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix} \rightarrow \begin{pmatrix} 5 & 2 & 4 & 1 & 3 \\ 4 & 1 & 3 & 5 & 2 \\ 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix} \rightarrow \begin{pmatrix} 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \\ 5 & 2 & 4 & 1 & 3 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$$

If we apply the permutation (12345) to the rows, then to the columns,

Another example

$$\begin{pmatrix} 4 & 1 & 3 & 5 & 2 \\ 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix} \rightarrow \begin{pmatrix} 5 & 2 & 4 & 1 & 3 \\ 4 & 1 & 3 & 5 & 2 \\ 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix} \rightarrow \begin{pmatrix} 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \\ 5 & 2 & 4 & 1 & 3 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$$

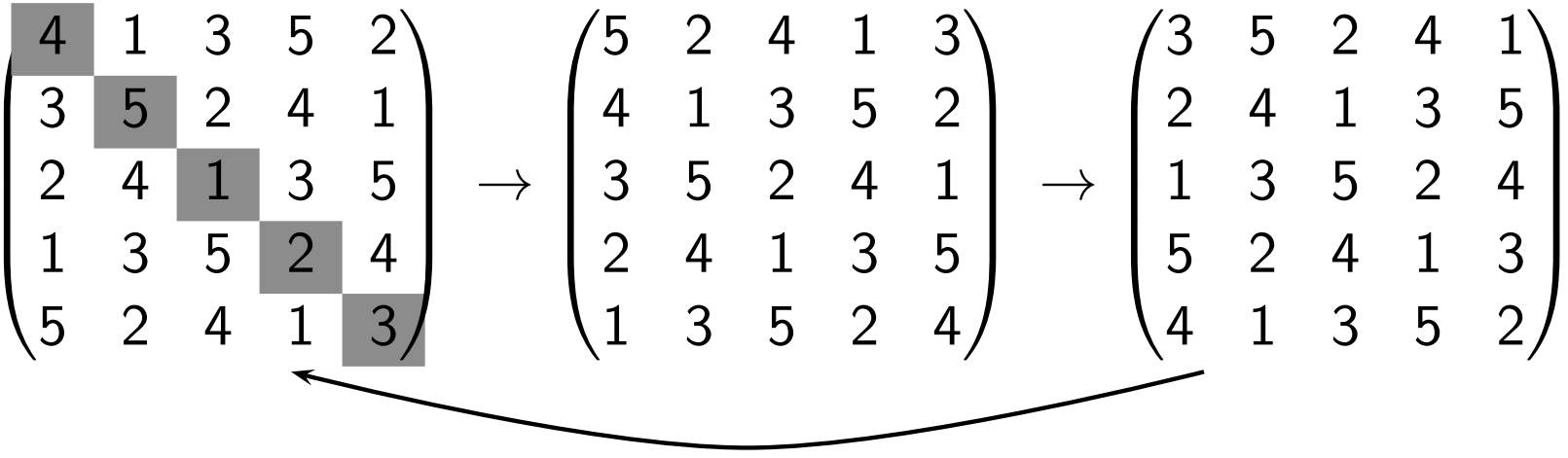
If we apply the permutation (12345) to the rows, then to the columns, then also to the symbols,

Another example

$$\begin{pmatrix} 4 & 1 & 3 & 5 & 2 \\ 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix} \rightarrow \begin{pmatrix} 5 & 2 & 4 & 1 & 3 \\ 4 & 1 & 3 & 5 & 2 \\ 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix} \rightarrow \begin{pmatrix} 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \\ 5 & 2 & 4 & 1 & 3 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$$

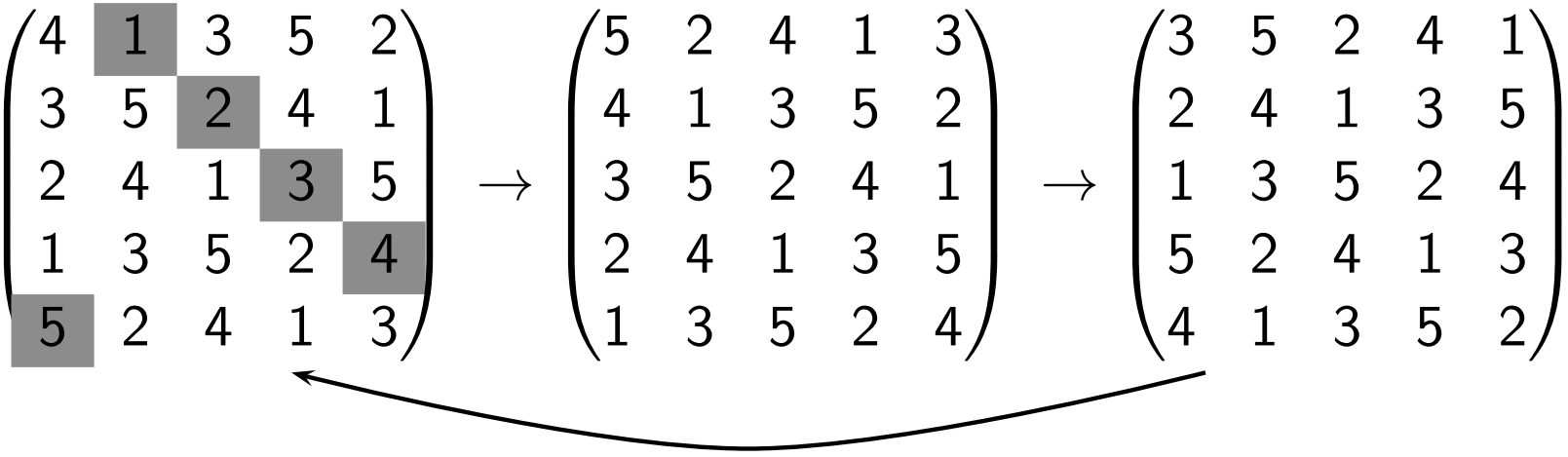
If we apply the permutation (12345) to the rows, then to the columns, then also to the symbols, we find a symmetry of the Latin square.

Another example



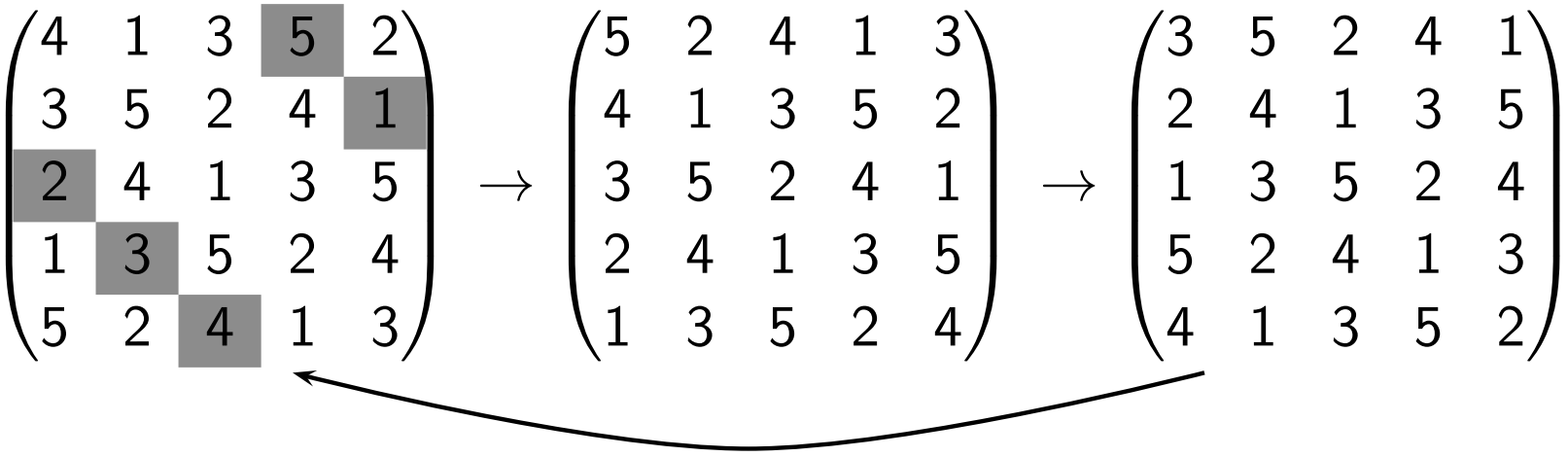
If we apply the permutation (12345) to the rows, then to the columns, then also to the symbols, we find a symmetry of the Latin square.

Another example



If we apply the permutation (12345) to the rows, then to the columns, then also to the symbols, we find a symmetry of the Latin square.

Another example



If we apply the permutation (12345) to the rows, then to the columns, then also to the symbols, we find a symmetry of the Latin square.

And another example

$$\begin{pmatrix} 1 & 6 & 5 & 2 & 3 & 4 & 7 \\ 6 & 2 & 7 & 3 & 5 & 1 & 4 \\ 5 & 7 & 3 & 1 & 4 & 6 & 2 \\ 2 & 3 & 1 & 4 & 7 & 5 & 6 \\ 7 & 4 & 2 & 6 & 1 & 3 & 5 \\ 3 & 5 & 4 & 7 & 6 & 2 & 1 \\ 4 & 1 & 6 & 5 & 2 & 7 & 3 \end{pmatrix}$$

. . . has a symmetry that applies the permutation $(123)(4)(567)$ to the rows, columns and symbols.

And another example

$$\begin{pmatrix}
1 & 6 & 5 & 2 & 3 & 4 & 7 \\
6 & 2 & 7 & 3 & 5 & 1 & 4 \\
5 & 7 & 3 & 1 & 4 & 6 & 2 \\
2 & 3 & 1 & 4 & 7 & 5 & 6 \\
7 & 4 & 2 & 6 & 1 & 3 & 5 \\
3 & 5 & 4 & 7 & 6 & 2 & 1 \\
4 & 1 & 6 & 5 & 2 & 7 & 3
\end{pmatrix}$$

. . . has a symmetry that applies the permutation (123)(4)(567) to the rows, columns and symbols.

And another example

$$\begin{pmatrix}
1 & 6 & 5 & 2 & 3 & 4 & 7 \\
6 & 2 & 7 & 3 & 5 & 1 & 4 \\
5 & 7 & 3 & 1 & 4 & 6 & 2 \\
2 & 3 & 1 & 4 & 7 & 5 & 6 \\
7 & 4 & 2 & 6 & 1 & 3 & 5 \\
3 & 5 & 4 & 7 & 6 & 2 & 1 \\
4 & 1 & 6 & 5 & 2 & 7 & 3
\end{pmatrix}$$

. . . has a symmetry that applies the permutation (123)(4)(567) to the rows, columns and symbols.

Symmetries like this, where the same permutation is applied to the rows, columns and symbols, are called *automorphisms*.

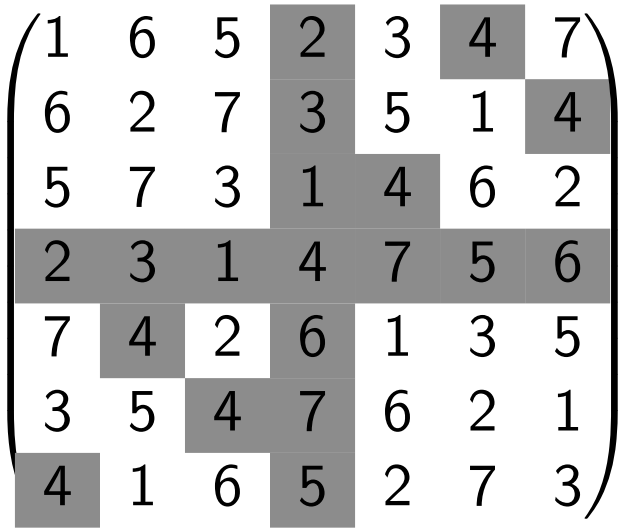
And another example

$$\begin{pmatrix}
1 & 6 & 5 & 2 & 3 & 4 & 7 \\
6 & 2 & 7 & 3 & 5 & 1 & 4 \\
5 & 7 & 3 & 1 & 4 & 6 & 2 \\
2 & 3 & 1 & 4 & 7 & 5 & 6 \\
7 & 4 & 2 & 6 & 1 & 3 & 5 \\
3 & 5 & 4 & 7 & 6 & 2 & 1 \\
4 & 1 & 6 & 5 & 2 & 7 & 3
\end{pmatrix}$$

. . . has a symmetry that applies the permutation (123)(4)(567) to the rows, columns and symbols.

Symmetries like this, where the same permutation is applied to the rows, columns and symbols, are called *automorphisms*.
[They are analogous to the automorphisms of groups.]

And another example



. . . has a symmetry that applies the permutation (123)(4)(567) to the rows, columns and symbols.

Symmetries like this, where the same permutation is applied to the rows, columns and symbols, are called *automorphisms*.
[They are analogous to the automorphisms of groups.]

More generally, a symmetry which permutes rows, columns and symbols (but might apply different permutations to each), is called an *autotopism*.

Automorphisms

Let $\mathcal{S}_n$ denote the symmetric group
(i.e. the set of permutations of $\{1, 2, \ldots, n\}$).

Automorphisms

Let $\mathcal{S}_n$ denote the symmetric group
(i.e. the set of permutations of $\{1, 2, \ldots, n\}$).

$\mathrm{aut}(n)$ is the subset of $\mathcal{S}_n$ consisting of all α that are an automorphism of some Latin square of order n.

Automorphisms

Let $\mathcal{S}_n$ denote the symmetric group
(i.e. the set of permutations of $\{1, 2, \ldots, n\}$).

$\mathrm{aut}(n)$ is the subset of $\mathcal{S}_n$ consisting of all α that are an automorphism of some Latin square of order n.

$$\begin{pmatrix} 4 & 1 & 3 & 5 & 2 \\ 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 6 & 5 & 2 & 3 & 4 & 7 \\ 6 & 2 & 7 & 3 & 5 & 1 & 4 \\ 5 & 7 & 3 & 1 & 4 & 6 & 2 \\ 2 & 3 & 1 & 4 & 7 & 5 & 6 \\ 7 & 4 & 2 & 6 & 1 & 3 & 5 \\ 3 & 5 & 4 & 7 & 6 & 2 & 1 \\ 4 & 1 & 6 & 5 & 2 & 7 & 3 \end{pmatrix}$$

These earlier examples showed that $(12345) \in \mathrm{aut}(5)$ and $(123)(4)(567) \in \mathrm{aut}(7)$.

Autotopism notation

We write a typical autotopism as a triple (α, β, γ) of permutations, on the understanding that it applies

- α to permute the rows
- β to permute the columns
- γ to permute the symbols.

Autotopism notation

We write a typical autotopism as a triple (α, β, γ) of permutations, on the understanding that it applies

- α to permute the rows
- β to permute the columns
- γ to permute the symbols.

$\mathrm{atp}(n)$ is the set of all triples in $\mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$ that are an autotopism of some Latin square of order n.

Autotopism notation

We write a typical autotopism as a triple (α, β, γ) of permutations, on the understanding that it applies

- α to permute the rows
- β to permute the columns
- γ to permute the symbols.

$\mathrm{atp}(n)$ is the set of all triples in $\mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$ that are an autotopism of some Latin square of order n.

The earlier examples show that
$\big((123456), \varepsilon, (123456)\big) \in \mathrm{atp}(6)$, [here ε is the identity]

Autotopism notation

We write a typical autotopism as a triple (α, β, γ) of permutations, on the understanding that it applies

- α to permute the rows
- β to permute the columns
- γ to permute the symbols.

$\mathrm{atp}(n)$ is the set of all triples in $\mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$ that are an autotopism of some Latin square of order n.

The earlier examples show that
$\big((123456), \varepsilon, (123456)\big) \in \mathrm{atp}(6)$, [here ε is the identity]
$\big((12345), (12345), (12345)\big) \in \mathrm{atp}(5)$
$\big((123)(4)(567), (123)(4)(567), (123)(4)(567)\big) \in \mathrm{atp}(7)$.

Autotopism notation

We write a typical autotopism as a triple (α, β, γ) of permutations, on the understanding that it applies

- α to permute the rows
- β to permute the columns
- γ to permute the symbols.

$\mathrm{atp}(n)$ is the set of all triples in $\mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$ that are an autotopism of some Latin square of order n.

The earlier examples show that
$\big((123456), \varepsilon, (123456)\big) \in \mathrm{atp}(6)$, [here ε is the identity]
$\big((12345), (12345), (12345)\big) \in \mathrm{atp}(5)$
$\big((123)(4)(567), (123)(4)(567), (123)(4)(567)\big) \in \mathrm{atp}(7)$.

This talk reports our attempts to understand $\mathrm{aut}(n)$ and $\mathrm{atp}(n)$.

Why should I care?

Symmetry is a key concept in mathematics.

Why should I care?

Symmetry is a key concept in mathematics. Latin squares are interesting *and* useful.

Why should I care?

Symmetry is a key concept in mathematics. Latin squares are interesting *and* useful. That's enough justification for me!!

Why should I care?

Symmetry is a key concept in mathematics. Latin squares are interesting *and* useful. That's enough justification for me!!

If you are still sceptical, symmetry of Latin squares. . . ,

Why should I care?

Symmetry is a key concept in mathematics. Latin squares are interesting *and* useful. That's enough justification for me!!

If you are still sceptical, symmetry of Latin squares. . . ,

- has been studied since [Euler 1782].

Why should I care?

Symmetry is a key concept in mathematics. Latin squares are interesting *and* useful. That's enough justification for me!!

If you are still sceptical, symmetry of Latin squares. . . ,

- has been studied since [Euler 1782].
- includes automorphisms of groups or Steiner triple systems as special cases.

Why should I care?

Symmetry is a key concept in mathematics. Latin squares are interesting *and* useful. That's enough justification for me!!

If you are still sceptical, symmetry of Latin squares. . . ,

- has been studied since [Euler 1782].
- includes automorphisms of groups or Steiner triple systems as special cases.
- plays a crucial rule in enumerations [McKay et al. 2007], [Hulpke et al. 2011].

Why should I care?

Symmetry is a key concept in mathematics. Latin squares are interesting *and* useful. That's enough justification for me!!

If you are still sceptical, symmetry of Latin squares. . . ,

- has been studied since [Euler 1782].
- includes automorphisms of groups or Steiner triple systems as special cases.
- plays a crucial rule in enumerations [McKay et al. 2007], [Hulpke et al. 2011].
- facilitates theoretical results on congruences satisfied by the number of Latin squares [Drisko 1998], [Stones&W. 2010]

Why should I care?

Symmetry is a key concept in mathematics. Latin squares are interesting *and* useful. That's enough justification for me!!

If you are still sceptical, symmetry of Latin squares. . . ,

- has been studied since [Euler 1782].
- includes automorphisms of groups or Steiner triple systems as special cases.
- plays a crucial rule in enumerations [McKay et al. 2007], [Hulpke et al. 2011].
- facilitates theoretical results on congruences satisfied by the number of Latin squares [Drisko 1998], [Stones&W. 2010]
- makes it feasible to find "nice" Latin squares in search spaces that would otherwise be too large [W.2005]

Why should I care?

Symmetry is a key concept in mathematics. Latin squares are interesting *and* useful. That's enough justification for me!!

If you are still sceptical, symmetry of Latin squares. . . ,

- has been studied since [Euler 1782].
- includes automorphisms of groups or Steiner triple systems as special cases.
- plays a crucial rule in enumerations [McKay et al. 2007], [Hulpke et al. 2011].
- facilitates theoretical results on congruences satisfied by the number of Latin squares [Drisko 1998], [Stones&W. 2010]
- makes it feasible to find "nice" Latin squares in search spaces that would otherwise be too large [W.2005]
- reduces the work in proving that certain properties hold for a Latin square [Bryant et al. 2002,2006] [Maenhaut et al. 2007].

Why should I care?

Symmetry is a key concept in mathematics. Latin squares are interesting *and* useful. That's enough justification for me!!

If you are still sceptical, symmetry of Latin squares. . . ,

- has been studied since [Euler 1782].
- includes automorphisms of groups or Steiner triple systems as special cases.
- plays a crucial rule in enumerations [McKay et al. 2007], [Hulpke et al. 2011].
- facilitates theoretical results on congruences satisfied by the number of Latin squares [Drisko 1998], [Stones&W. 2010]
- makes it feasible to find "nice" Latin squares in search spaces that would otherwise be too large [W.2005]
- reduces the work in proving that certain properties hold for a Latin square [Bryant et al. 2002,2006] [Maenhaut et al. 2007].
- is pivotal in the algebraic study of Moufang loops conjugacy closed loops, extra loops, Buchsteiner loops, . . .

Why should I care?

Symmetry is a key concept in mathematics. Latin squares are interesting *and* useful. That's enough justification for me!!

If you are still sceptical, symmetry of Latin squares. . . ,

- has been studied since [Euler 1782].
- includes automorphisms of groups or Steiner triple systems as special cases.
- plays a crucial rule in enumerations [McKay et al. 2007], [Hulpke et al. 2011].
- facilitates theoretical results on congruences satisfied by the number of Latin squares [Drisko 1998], [Stones&W. 2010]
- makes it feasible to find "nice" Latin squares in search spaces that would otherwise be too large [W.2005]
- reduces the work in proving that certain properties hold for a Latin square [Bryant et al. 2002,2006] [Maenhaut et al. 2007].
- is pivotal in the algebraic study of Moufang loops conjugacy closed loops, extra loops, Buchsteiner loops, . . .
- is connected to the character theory of quasigroups

Cycle structures

By the *cycle structure* of a permutation I mean a sorted list of the lengths of its cycles.

Cycle structures

By the *cycle structure* of a permutation I mean a sorted list of the lengths of its cycles.

So (123)(4)(567) has cycle structure [3,3,1] (which we might abbreviate to $[3^2, 1]$).

Cycle structures

By the *cycle structure* of a permutation I mean a sorted list of the lengths of its cycles.

So (123)(4)(567) has cycle structure [3,3,1] (which we might abbreviate to $[3^2, 1]$).
and (12345) has cycle structure [5].

Cycle structures

By the *cycle structure* of a permutation I mean a sorted list of the lengths of its cycles.

So (123)(4)(567) has cycle structure [3,3,1] (which we might abbreviate to $[3^2, 1]$).
and (12345) has cycle structure [5].

Cycles of length 1 are *fixed points*. All other cycles are *non-trivial*.

Cycle structures

By the *cycle structure* of a permutation I mean a sorted list of the lengths of its cycles.

So (123)(4)(567) has cycle structure [3,3,1] (which we might abbreviate to $[3^2, 1]$).
and (12345) has cycle structure [5].

Cycles of length 1 are *fixed points*. All other cycles are *non-trivial*.

Theorem: Whether (α, β, γ) is in $\mathrm{atp}(n)$ depends only on the cycle structures of α, β, and γ.

Cycle structures

By the *cycle structure* of a permutation I mean a sorted list of the lengths of its cycles.

So (123)(4)(567) has cycle structure [3,3,1] (which we might abbreviate to $[3^2, 1]$).
and (12345) has cycle structure [5].

Cycles of length 1 are *fixed points*. All other cycles are *non-trivial*.

Theorem: Whether (α, β, γ) is in $\mathrm{atp}(n)$ depends only on the cycle structures of α, β, and γ.

So the fact that
$\big((123)(4)(567), (123)(4)(567), (123)(4)(567)\big) \in \mathrm{atp}(7)$
implies that
$\big((142)(356)(7), (1)(234)(567), (213)(4)(675)\big) \in \mathrm{atp}(7)$.

Cycle structures

By the *cycle structure* of a permutation I mean a sorted list of the lengths of its cycles.

So (123)(4)(567) has cycle structure [3,3,1] (which we might abbreviate to $[3^2, 1]$).
and (12345) has cycle structure [5].

Cycles of length 1 are *fixed points*. All other cycles are *non-trivial*.

Theorem: Whether (α, β, γ) is in $\mathrm{atp}(n)$ depends only on the cycle structures of α, β, and γ.

So the fact that
$\big((123)(4)(567), (123)(4)(567), (123)(4)(567)\big) \in \mathrm{atp}(7)$
implies that
$\big((142)(356)(7), (1)(234)(567), (213)(4)(675)\big) \in \mathrm{atp}(7)$.

And the fact that $\big((123456), \varepsilon, (123456)\big) \in \mathrm{atp}(6)$, implies that $\big((142536), (231546), \varepsilon\big) \in \mathrm{atp}(6)$.

Number of possible cycle structures

n	3 diff	2 diff	$\#\mathrm{aut}(n)$	$\#\mathrm{atp}(n)$
1			1	1
2		1	1	2
3		1	3	4
4		5	4	9
5		1	5	6
6	1	11	6	18
7		1	9	10
8		25	12	37
9		10	13	23
10	1	23	14	38
11		1	18	19
12	7	113	26	146
13		1	24	25
14	1	37	24	62
15	1	34	39	74
16		151	50	201
17		1	38	39

Number of possible cycle structures

n	3 diff	2 diff	$\#\mathrm{aut}(n)$	$\#\mathrm{atp}(n)$	
1			1	1	
2		1	1	2	⟵
3		1	3	4	⟵
4		5	4	9	
5		1	5	6	⟵
6	1	11	6	18	
7		1	9	10	⟵
8		25	12	37	
9		10	13	23	
10	1	23	14	38	
11		1	18	19	⟵
12	7	113	26	146	
13		1	24	25	⟵
14	1	37	24	62	
15	1	34	39	74	
16		151	50	201	
17		1	38	39	⟵

Computer meets theory

In the process of compiling the data for the previous table we uncovered many theoretical results.

Computer meets theory

In the process of compiling the data for the previous table we uncovered many theoretical results.

We would look for a Latin square with a particular autotopism and if the computer found there isn't one, we'd ask "Why?".

Computer meets theory

In the process of compiling the data for the previous table we uncovered many theoretical results.

We would look for a Latin square with a particular autotopism and if the computer found there isn't one, we'd ask "Why?". Usually the result was a new theorem.

Computer meets theory

In the process of compiling the data for the previous table we uncovered many theoretical results.

We would look for a Latin square with a particular autotopism and if the computer found there isn't one, we'd ask "Why?". Usually the result was a new theorem.

Theorem: Suppose 2^a is the largest power of 2 dividing n, where $a \geqslant 1$. If the length of each cycle in α, β and γ is divisible by 2^a then $(\alpha, \beta, \gamma) \notin \mathrm{atp}(n)$.

Computer meets theory

In the process of compiling the data for the previous table we uncovered many theoretical results.

We would look for a Latin square with a particular autotopism and if the computer found there isn't one, we'd ask "Why?". Usually the result was a new theorem.

Theorem: Suppose 2^a is the largest power of 2 dividing n, where $a \geqslant 1$. If the length of each cycle in α, β and γ is divisible by 2^a then $(\alpha, \beta, \gamma) \notin \mathrm{atp}(n)$.

By the end, our theory was sufficient to rule out every example that doesn't exist for $n \leqslant 17$,

Computer meets theory

In the process of compiling the data for the previous table we uncovered many theoretical results.

We would look for a Latin square with a particular autotopism and if the computer found there isn't one, we'd ask "Why?". Usually the result was a new theorem.

Theorem: Suppose 2^a is the largest power of 2 dividing n, where $a \geqslant 1$. If the length of each cycle in α, β and γ is divisible by 2^a then $(\alpha, \beta, \gamma) \notin \mathrm{atp}(n)$.

By the end, our theory was sufficient to rule out every example that doesn't exist for $n \leqslant 17$, with one exception.

Computer meets theory

In the process of compiling the data for the previous table we uncovered many theoretical results.

We would look for a Latin square with a particular autotopism and if the computer found there isn't one, we'd ask "Why?". Usually the result was a new theorem.

Theorem: Suppose 2^a is the largest power of 2 dividing n, where $a \geqslant 1$. If the length of each cycle in α, β and γ is divisible by 2^a then $(\alpha, \beta, \gamma) \notin \mathrm{atp}(n)$.

By the end, our theory was sufficient to rule out every example that doesn't exist for $n \leqslant 17$, with one exception. We had no way to rule out cycle structure ([1,1,4],[2,4],[2,4]).

Computer meets theory

In the process of compiling the data for the previous table we uncovered many theoretical results.

We would look for a Latin square with a particular autotopism and if the computer found there isn't one, we'd ask "Why?". Usually the result was a new theorem.

Theorem: Suppose 2^a is the largest power of 2 dividing n, where $a \geqslant 1$. If the length of each cycle in α, β and γ is divisible by 2^a then $(\alpha, \beta, \gamma) \notin \mathrm{atp}(n)$.

By the end, our theory was sufficient to rule out every example that doesn't exist for $n \leqslant 17$, with one exception. We had no way to rule out cycle structure ([1,1,4],[2,4],[2,4]).

We also had theorems giving general constructions for many cases. In particular, we categorised all automorphisms with three or fewer non-trivial cycles.

Automorphisms with three nontrivial cycles

Theorem: Suppose $\alpha \in \mathcal{S}_n$ has precisely three nontrivial cycles of lengths $d_1 \geqslant d_2 \geqslant d_3$, as well as d_∞ fixed points.

Automorphisms with three nontrivial cycles

Theorem: Suppose $\alpha \in \mathcal{S}_n$ has precisely three nontrivial cycles of lengths $d_1 \geqslant d_2 \geqslant d_3$, as well as d_∞ fixed points.

Then $\alpha \in \mathrm{aut}(n)$ iff one of the following holds:

1. $d_1 = d_2 = d_3$ and (a) $d_\infty \leqslant 3d_1$ and (b) if d_1 is even then $d_\infty \geqslant 1$,
2. $d_1 > d_2 = d_3$ and (a) $d_1 \geqslant 2d_2 + d_\infty$, (b) d_2 divides d_1, (c) $d_\infty \leqslant 2d_2$, and (d) if d_2 is even and d_1/d_2 is odd then $d_\infty > 0$,
3. $d_1 = d_2 > d_3$ and (a) d_3 divides d_1, (b) $d_\infty \leqslant d_3$, and (c) if d_3 is even then $d_\infty > 0$,
4. $d_1 > d_2 > d_3$ and (a) $d_1 = \mathrm{lcm}(d_2, d_3)$, (b) $d_3 \geqslant d_\infty$, and (c) if d_1 is even then $d_\infty > 0$,
5. $d_1 > d_2 > d_3$ and (a) d_3 divides d_2 which divides d_1, (b) $d_3 \geqslant d_\infty$, and (c) if d_3 is even then $d_\infty > 0$.

The order of an autotopism

The *order* of an autotopism (α, β, γ) is the smallest power m for which $(\alpha, \beta, \gamma)^m = (\varepsilon, \varepsilon, \varepsilon)$. (This is just the least common multiple of all of the cycle lengths in α, β and γ).

The order of an autotopism

The *order* of an autotopism (α, β, γ) is the smallest power m for which $(\alpha, \beta, \gamma)^m = (\varepsilon, \varepsilon, \varepsilon)$. (This is just the least common multiple of all of the cycle lengths in α, β and γ).

Horoševskiĭ [1974] proved that for Latin squares that are group tables, the order of an automorphism is never more than n, the order of the Latin square.

The order of an autotopism

The *order* of an autotopism (α, β, γ) is the smallest power m for which $(\alpha, \beta, \gamma)^m = (\varepsilon, \varepsilon, \varepsilon)$. (This is just the least common multiple of all of the cycle lengths in α, β and γ).

Horoševskiĭ [1974] proved that for Latin squares that are group tables, the order of an automorphism is never more than n, the order of the Latin square.

Is the same true more generally?

The order of an autotopism

The *order* of an autotopism (α, β, γ) is the smallest power m for which $(\alpha, \beta, \gamma)^m = (\varepsilon, \varepsilon, \varepsilon)$. (This is just the least common multiple of all of the cycle lengths in α, β and γ).

Horoševskiĭ [1974] proved that for Latin squares that are group tables, the order of an automorphism is never more than n, the order of the Latin square.

Is the same true more generally?

Theorem: Let L be any Latin square of order n. The order of any autotopism of L is no more than $n^2/4$.

The order of an autotopism

The *order* of an autotopism (α, β, γ) is the smallest power m for which $(\alpha, \beta, \gamma)^m = (\varepsilon, \varepsilon, \varepsilon)$. (This is just the least common multiple of all of the cycle lengths in α, β and γ).

Horoševskiĭ [1974] proved that for Latin squares that are group tables, the order of an automorphism is never more than n, the order of the Latin square.

Is the same true more generally?

Theorem: Let L be any Latin square of order n. The order of any autotopism of L is no more than $n^2/4$.

[In particular this means most permutations aren't automorphisms.]

The order of an autotopism

The *order* of an autotopism (α, β, γ) is the smallest power m for which $(\alpha, \beta, \gamma)^m = (\varepsilon, \varepsilon, \varepsilon)$. (This is just the least common multiple of all of the cycle lengths in α, β and γ).

Horoševskiĭ [1974] proved that for Latin squares that are group tables, the order of an automorphism is never more than n, the order of the Latin square.

Is the same true more generally?

Theorem: Let L be any Latin square of order n. The order of any autotopism of L is no more than $n^2/4$.

[In particular this means most permutations aren't automorphisms.]

By computer we found that there are no Latin squares of order $n \leqslant 1000$ that have an automorphism of order $m > n$.

No small examples

Method: Hypothesise m.

No small examples

Method: Hypothesise m. You then know the possible cycle lengths.

No small examples

Method: Hypothesise m. You then know the possible cycle lengths. Construct a linear program whose variables are n, and a variable to count the number of cycles of each possible length.

No small examples

Method: Hypothesise m. You then know the possible cycle lengths. Construct a linear program whose variables are n, and a variable to count the number of cycles of each possible length. There are many restrictions on them, which can be coded as linear constraints.

No small examples

Method: Hypothesise m. You then know the possible cycle lengths. Construct a linear program whose variables are n, and a variable to count the number of cycles of each possible length. There are many restrictions on them, which can be coded as linear constraints. In most cases there are no feasible solutions.

No small examples

Method: Hypothesise m. You then know the possible cycle lengths. Construct a linear program whose variables are n, and a variable to count the number of cycles of each possible length. There are many restrictions on them, which can be coded as linear constraints. In most cases there are no feasible solutions.

For each feasible solution, construct a new linear program describing the *block diagram*.

No small examples

Method: Hypothesise m. You then know the possible cycle lengths. Construct a linear program whose variables are n, and a variable to count the number of cycles of each possible length. There are many restrictions on them, which can be coded as linear constraints. In most cases there are no feasible solutions.

For each feasible solution, construct a new linear program describing the *block diagram*. This divides the Latin square into blocks defined by the cycles acting on the rows and on the columns.

No small examples

Method: Hypothesise m. You then know the possible cycle lengths. Construct a linear program whose variables are n, and a variable to count the number of cycles of each possible length. There are many restrictions on them, which can be coded as linear constraints. In most cases there are no feasible solutions.

For each feasible solution, construct a new linear program describing the *block diagram*. This divides the Latin square into blocks defined by the cycles acting on the rows and on the columns. Now count, with a variable, the number of symbols from each cycle that occur within each block.

No small examples

Method: Hypothesise m. You then know the possible cycle lengths. Construct a linear program whose variables are n, and a variable to count the number of cycles of each possible length. There are many restrictions on them, which can be coded as linear constraints. In most cases there are no feasible solutions.

For each feasible solution, construct a new linear program describing the *block diagram*. This divides the Latin square into blocks defined by the cycles acting on the rows and on the columns. Now count, with a variable, the number of symbols from each cycle that occur within each block. The ensuing constraints cannot be satisfied for $n \leqslant 1000$.

No small examples

Method: Hypothesise m. You then know the possible cycle lengths. Construct a linear program whose variables are n, and a variable to count the number of cycles of each possible length. There are many restrictions on them, which can be coded as linear constraints. In most cases there are no feasible solutions.

For each feasible solution, construct a new linear program describing the *block diagram*. This divides the Latin square into blocks defined by the cycles acting on the rows and on the columns. Now count, with a variable, the number of symbols from each cycle that occur within each block. The ensuing constraints cannot be satisfied for $n \leqslant 1000$.

But they are satisfied when $n = 28009$ by an automorphism of order $m = 45045$ (with cycle type [9009,6435,5005,4095,3465]). Indeed, we managed to build an example with these parameters!

No small examples

Method: Hypothesise m. You then know the possible cycle lengths. Construct a linear program whose variables are n, and a variable to count the number of cycles of each possible length. There are many restrictions on them, which can be coded as linear constraints. In most cases there are no feasible solutions.

For each feasible solution, construct a new linear program describing the *block diagram*. This divides the Latin square into blocks defined by the cycles acting on the rows and on the columns. Now count, with a variable, the number of symbols from each cycle that occur within each block. The ensuing constraints cannot be satisfied for $n \leqslant 1000$.

But they are satisfied when $n = 28009$ by an automorphism of order $m = 45045$ (with cycle type [9009,6435,5005,4095,3465]). Indeed, we managed to build an example with these parameters!

The only problem is it's a bit big to include in the paper!

Prime orders

For prime orders $p \leqslant 17$ all autotopisms (α, β, γ) have

(a) α, β, γ with the same cycle structure;

Prime orders

For prime orders $p \leqslant 17$ all autotopisms (α, β, γ) have

(a) α, β, γ with the same cycle structure; or

(b) Two of α, β, γ are p-cycles and the other is the identity.

Prime orders

For prime orders $p \leqslant 17$ all autotopisms (α, β, γ) have

(a) α, β, γ with the same cycle structure; or

(b) Two of α, β, γ are p-cycles and the other is the identity.

Let $\mathcal{C}(\alpha, k)$ be the #points that appear in cycles of α for which the cycle length is divisible by k.

Prime orders

For prime orders $p \leqslant 17$ all autotopisms (α, β, γ) have

(a) α, β, γ with the same cycle structure; or

(b) Two of α, β, γ are p-cycles and the other is the identity.

Let $\mathcal{C}(\alpha, k)$ be the #points that appear in cycles of α for which the cycle length is divisible by k.

Theorem: Suppose L is a Latin square of order n and that (α, β, γ) is an autotopism of L of order m. If k is a prime power divisor of m then

(a) $\mathcal{C}(\alpha, k) = \mathcal{C}(\beta, k) = \mathcal{C}(\gamma, k) \geqslant \frac{1}{2}n$; or

(b) Two of $\mathcal{C}(\alpha, k)$, $\mathcal{C}(\beta, k)$, $\mathcal{C}(\gamma, k)$ are equal to n.

Prime orders

For prime orders $p \leqslant 17$ all autotopisms (α, β, γ) have

(a) α, β, γ with the same cycle structure; or

(b) Two of α, β, γ are p-cycles and the other is the identity.

Let $\mathcal{C}(\alpha, k)$ be the #points that appear in cycles of α for which the cycle length is divisible by k.

Theorem: Suppose L is a Latin square of order n and that (α, β, γ) is an autotopism of L of order m. If k is a prime power divisor of m then

(a) $\mathcal{C}(\alpha, k) = \mathcal{C}(\beta, k) = \mathcal{C}(\gamma, k) \geqslant \frac{1}{2}n$; or

(b) Two of $\mathcal{C}(\alpha, k)$, $\mathcal{C}(\beta, k)$, $\mathcal{C}(\gamma, k)$ are equal to n.

This is a strong restriction. For prime $n \leqslant 29$ it only leaves

$n = 23$, $[6^2, 3, 2, 1^6]$ and $2 \times [6, 3^3, 2^4]$

$n = 29$, $[6^2, 3, 2^4, 1^6]$ and $2 \times [6, 3^3, 2^7]$

$n = 29$, $[6^3, 3, 2, 1^6]$ and $2 \times [6^2, 3^3, 2^4]$

Prime orders

For prime orders $p \leqslant 17$ all autotopisms (α, β, γ) have

(a) α, β, γ with the same cycle structure; or

(b) Two of α, β, γ are p-cycles and the other is the identity.

Let $\mathcal{C}(\alpha, k)$ be the #points that appear in cycles of α for which the cycle length is divisible by k.

Theorem: Suppose L is a Latin square of order n and that (α, β, γ) is an autotopism of L of order m. If k is a prime power divisor of m then

(a) $\mathcal{C}(\alpha, k) = \mathcal{C}(\beta, k) = \mathcal{C}(\gamma, k) \geqslant \frac{1}{2}n$; or

(b) Two of $\mathcal{C}(\alpha, k)$, $\mathcal{C}(\beta, k)$, $\mathcal{C}(\gamma, k)$ are equal to n.

This is a strong restriction. For prime $n \leqslant 29$ it only leaves

$n = 23$, $[6^2, 3, 2, 1^6]$ and $2 \times [6, 3^3, 2^4]$ $\leftarrow$ doesn't exist.

$n = 29$, $[6^2, 3, 2^4, 1^6]$ and $2 \times [6, 3^3, 2^7]$ $\leftarrow$ doesn't exist.

$n = 29$, $[6^3, 3, 2, 1^6]$ and $2 \times [6^2, 3^3, 2^4]$ $\leftarrow$ does exist!

Prime orders

For prime orders $p \leqslant 17$ all autotopisms (α, β, γ) have

(a) α, β, γ with the same cycle structure; or

(b) Two of α, β, γ are p-cycles and the other is the identity.

Let $\mathcal{C}(\alpha, k)$ be the #points that appear in cycles of α for which the cycle length is divisible by k.

Theorem: Suppose L is a Latin square of order n and that (α, β, γ) is an autotopism of L of order m. If k is a prime power divisor of m then

(a) $\mathcal{C}(\alpha, k) = \mathcal{C}(\beta, k) = \mathcal{C}(\gamma, k) \geqslant \frac{1}{2}n$; or

(b) Two of $\mathcal{C}(\alpha, k)$, $\mathcal{C}(\beta, k)$, $\mathcal{C}(\gamma, k)$ are equal to n.

This is a strong restriction. For prime $n \leqslant 29$ it only leaves

$n = 23$, $[6^2, 3, 2, 1^6]$ and $2 \times [6, 3^3, 2^4]$ $\leftarrow$ doesn't exist.

$n = 29$, $[6^2, 3, 2^4, 1^6]$ and $2 \times [6, 3^3, 2^7]$ $\leftarrow$ doesn't exist.

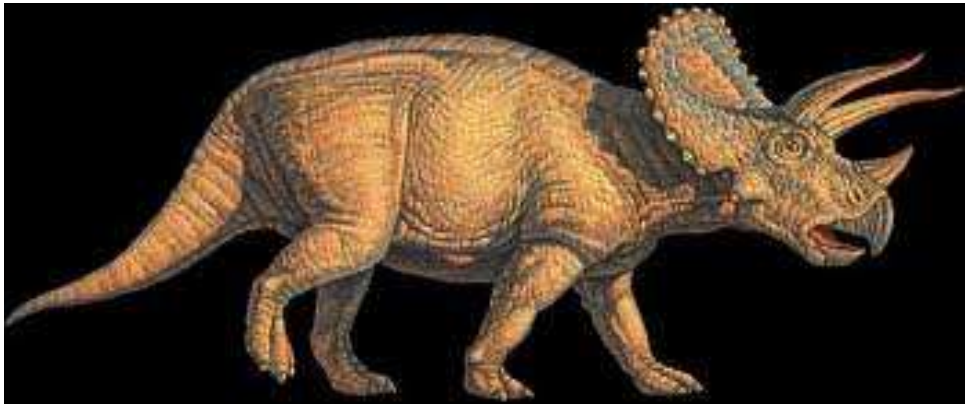
$n = 29$, $[6^3, 3, 2, 1^6]$ and $2 \times [6^2, 3^3, 2^4]$ $\leftarrow$ does exist!

Is it possible for prime order to have 3 different cycle structures?

An autotopism consisting of 3 permutations with different cycle structures shall henceforth be known as a

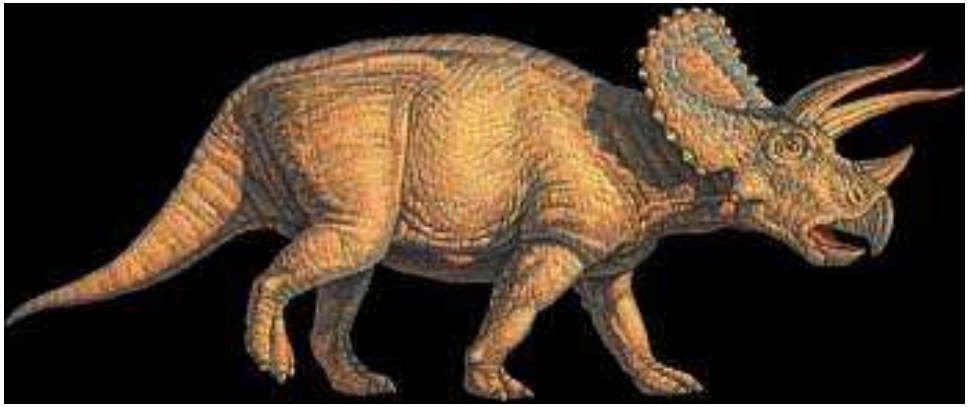
Triceratopisms

An autotopism consisting of 3 permutations with different cycle structures shall henceforth be known as a *triceratopism*.



Triceratopisms

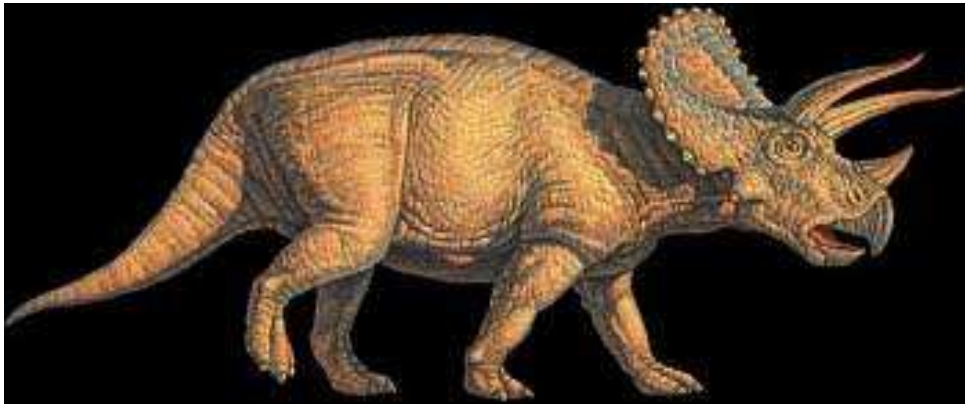
An autotopism consisting of 3 permutations with different cycle structures shall henceforth be known as a *triceratopism*.



Such creatures do exist. The smallest Latin square of prime order that possesses a triceratopism, has order 131.

Triceratopisms

An autotopism consisting of 3 permutations with different cycle structures shall henceforth be known as a *triceratopism*.



Such creatures do exist. The smallest Latin square of prime order that possesses a triceratopism, has order 131.

The cycle structures of the three permutations are
$[30^1, 15^2, 10^3, 6^6, 5^1]$,
$[30^2, 10^3, 6^1, 5^1, 3^{10}]$ and
$[30^2, 15^2, 6^1, 5^1, 2^{15}]$.

References

D. S. Stones, P. Vojtěchovský and I. M. Wanless,
Cycle structure of autotopisms of quasigroups and Latin squares,
J. Combin. Des., **20** (2012), 227–263.

B. D. McKay, I. M. Wanless and X. Zhang,
The order of automorphisms of quasigroups,
preprint.

Also related:

J. Browning, D. S. Stones and I. M. Wanless,
Bounds on the number of autotopisms and subsquares of a Latin square, *Combinatorica*, to appear.

... gives $n^{O(\log n)}$ bounds on the number of different autotopisms a single Latin square of order n can have.

McKay, Meynert and Myrvold 2007

Theorem: Let L be a Latin square of order n and let (α, β, γ) be a nontrivial autotopism of L. Then either

(a) α, β and γ have the same cycle structure with at least 1 and at most $\left\lfloor \frac{1}{2}n \right\rfloor$ fixed points, or

(b) one of α, β or γ has at least 1 fixed point and the other two permutations have the same cycle structure with no fixed points, or

(c) α, β and γ have no fixed points.

McKay, Meynert and Myrvold 2007

Theorem: Let L be a Latin square of order n and let (α, β, γ) be a nontrivial autotopism of L. Then either

(a) α, β and γ have the same cycle structure with at least 1 and at most $\left\lfloor \frac{1}{2} n \right\rfloor$ fixed points, or

(b) one of α, β or γ has at least 1 fixed point and the other two permutations have the same cycle structure with no fixed points, or

(c) α, β and γ have no fixed points.

Corollary: Suppose Q is a quasigroup of order n and that $\alpha \in \mathrm{aut}(Q)$ with $\alpha \neq \varepsilon$.

1. If α has a cycle of length $c > n/2$, then $\mathrm{ord}(\alpha) = c$.
2. If p^a is a prime power divisor of $\mathrm{ord}(\alpha)$ then $\mathcal{C}(\alpha, p^a) \geqslant \frac{1}{2} n$.

(Here $\mathcal{C}(\alpha, k)$ is #points that appear in cycles of α for which the cycle length is divisible by k.)

Some simple cases

Autotopisms where one component is the identity ε:

Theorem: $(\alpha, \beta, \varepsilon) \in \mathrm{atp}(n)$ iff both α and β consist of n/d cycles of length d, for some divisor d of n.

Some simple cases

Autotopisms where one component is the identity ε:
Theorem: $(\alpha, \beta, \varepsilon) \in \mathrm{atp}(n)$ iff both α and β consist of n/d cycles of length d, for some divisor d of n.

Automorphisms with all nontrivial cycles of the same length:
Theorem: Suppose $\alpha \in \mathcal{S}_n$ has precisely m nontrivial cycles, each of length d.

Some simple cases

Autotopisms where one component is the identity ε:
Theorem: $(\alpha, \beta, \varepsilon) \in \mathrm{atp}(n)$ iff both α and β consist of n/d cycles of length d, for some divisor d of n.

Automorphisms with all nontrivial cycles of the same length:
Theorem: Suppose $\alpha \in \mathcal{S}_n$ has precisely m nontrivial cycles, each of length d.
If α has at least one fixed point, then $\alpha \in \mathrm{aut}(n)$ iff $n \leqslant 2md$.

Some simple cases

Autotopisms where one component is the identity ε:
Theorem: $(\alpha, \beta, \varepsilon) \in \mathrm{atp}(n)$ iff both α and β consist of n/d cycles of length d, for some divisor d of n.

Automorphisms with all nontrivial cycles of the same length:
Theorem: Suppose $\alpha \in \mathcal{S}_n$ has precisely m nontrivial cycles, each of length d.
If α has at least one fixed point, then $\alpha \in \mathrm{aut}(n)$ iff $n \leqslant 2md$.
If α has no fixed points, then $\alpha \in \mathrm{aut}(n)$ iff d is odd or m is even.

Some simple cases

Autotopisms where one component is the identity ε:
Theorem: $(\alpha, \beta, \varepsilon) \in \mathrm{atp}(n)$ iff both α and β consist of n/d cycles of length d, for some divisor d of n.

Automorphisms with all nontrivial cycles of the same length:
Theorem: Suppose $\alpha \in \mathcal{S}_n$ has precisely m nontrivial cycles, each of length d.
If α has at least one fixed point, then $\alpha \in \mathrm{aut}(n)$ iff $n \leqslant 2md$.
If α has no fixed points, then $\alpha \in \mathrm{aut}(n)$ iff d is odd or m is even.

Corollary: Suppose 2^a is the largest power of 2 dividing n, where $a \geqslant 1$. Suppose each cycle in α, β and γ has length divisible by 2^a. Then $(\alpha, \beta, \gamma) \notin \mathrm{atp}(n)$.

lcm conditions

Let (α, β, γ) be an autotopism of a Latin square L. If i belongs to an a-cycle of α and j belongs to a b-cycle of β, then L_{ij} belongs to a c-cycle of γ, where

lcm conditions

Let (α, β, γ) be an autotopism of a Latin square L. If i belongs to an a-cycle of α and j belongs to a b-cycle of β, then L_{ij} belongs to a c-cycle of γ, where

$$\mathrm{lcm}(a, b) = \mathrm{lcm}(b, c) = \mathrm{lcm}(a, c) = \mathrm{lcm}(a, b, c).$$

lcm conditions

Let (α, β, γ) be an autotopism of a Latin square L. If i belongs to an a-cycle of α and j belongs to a b-cycle of β, then L_{ij} belongs to a c-cycle of γ, where

$$\mathrm{lcm}(a, b) = \mathrm{lcm}(b, c) = \mathrm{lcm}(a, c) = \mathrm{lcm}(a, b, c).$$

Let Λ be a fixed integer, and let R_Λ, C_Λ and S_Λ be the sets of all rows, columns and symbols in cycles whose length *divides* Λ.

lcm conditions

Let (α, β, γ) be an autotopism of a Latin square L. If i belongs to an a-cycle of α and j belongs to a b-cycle of β, then L_{ij} belongs to a c-cycle of γ, where

$$\mathrm{lcm}(a, b) = \mathrm{lcm}(b, c) = \mathrm{lcm}(a, c) = \mathrm{lcm}(a, b, c).$$

Let Λ be a fixed integer, and let R_Λ, C_Λ and S_Λ be the sets of all rows, columns and symbols in cycles whose length *divides* Λ.

Theorem: If at least two of R_Λ, C_Λ and S_Λ are nonempty, then

lcm conditions

Let (α, β, γ) be an autotopism of a Latin square L. If i belongs to an a-cycle of α and j belongs to a b-cycle of β, then L_{ij} belongs to a c-cycle of γ, where

$$\mathrm{lcm}(a, b) = \mathrm{lcm}(b, c) = \mathrm{lcm}(a, c) = \mathrm{lcm}(a, b, c).$$

Let Λ be a fixed integer, and let R_Λ, C_Λ and S_Λ be the sets of all rows, columns and symbols in cycles whose length *divides* Λ.

Theorem: If at least two of R_Λ, C_Λ and S_Λ are nonempty, then $|R_\Lambda| = |C_\Lambda| = |S_\Lambda|$ and there is a Latin subsquare M on the rows R_Λ, columns C_Λ and symbols S_Λ.

lcm conditions

Let (α, β, γ) be an autotopism of a Latin square L. If i belongs to an a-cycle of α and j belongs to a b-cycle of β, then L_{ij} belongs to a c-cycle of γ, where

$$\mathrm{lcm}(a, b) = \mathrm{lcm}(b, c) = \mathrm{lcm}(a, c) = \mathrm{lcm}(a, b, c).$$

Let Λ be a fixed integer, and let R_Λ, C_Λ and S_Λ be the sets of all rows, columns and symbols in cycles whose length *divides* Λ.

Theorem: If at least two of R_Λ, C_Λ and S_Λ are nonempty, then $|R_\Lambda| = |C_\Lambda| = |S_\Lambda|$ and there is a Latin subsquare M on the rows R_Λ, columns C_Λ and symbols S_Λ. Moreover, M admits an autotopism that is a restriction of the original autotopism.