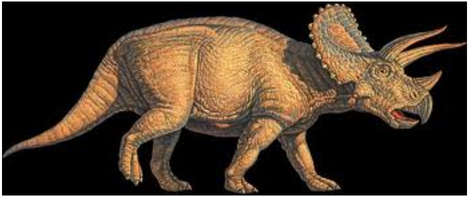
Triceratopisms of Latin Squares

Ian Wanless



Joint work with Brendan McKay 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.

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

is a Latin square of order 4.

The Cayley table of a finite (quasi-)group is a Latin square.

Autotopisms and Automorphisms

Let $\mathcal{S}_n$ be the symmetric group on n letters.
There is a natural action of $\mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$ on Latin squares,

Autotopisms and Automorphisms

Let $\mathcal{S}_n$ be the symmetric group on n letters.

There is a natural action of $\mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$ on Latin squares, where (α, β, γ) applies

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

Autotopisms and Automorphisms

Let $\mathcal{S}_n$ be the symmetric group on n letters.
There is a natural action of $\mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$ on Latin squares, where (α, β, γ) applies

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

...The stabiliser of a Latin square is its *autotopism group*.

Autotopisms and Automorphisms

Let $\mathcal{S}_n$ be the symmetric group on n letters.
There is a natural action of $\mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$ on Latin squares, where (α, β, γ) applies

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

...The stabiliser of a Latin square is its *autotopism group*.

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

Autotopisms and Automorphisms

Let $\mathcal{S}_n$ be the symmetric group on n letters.
There is a natural action of $\mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$ on Latin squares, where (α, β, γ) applies

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

...The stabiliser of a Latin square is its *autotopism group*.

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

$\mathrm{aut}(n)$ is the subset of $\mathcal{S}_n$ consisting of all α such that $(\alpha, \alpha, \alpha) \in \mathrm{atp}(n)$. (Such α are *automorphisms*).

Autotopisms and Automorphisms

Let $\mathcal{S}_n$ be the symmetric group on n letters.
There is a natural action of $\mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$ on Latin squares, where (α, β, γ) applies

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

...The stabiliser of a Latin square is its *autotopism group*.

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

$\mathrm{aut}(n)$ is the subset of $\mathcal{S}_n$ consisting of all α such that $(\alpha, \alpha, \alpha) \in \mathrm{atp}(n)$. (Such α are *automorphisms*).

Whether (α, β, γ) is in $\mathrm{atp}(n)$ depends only on

- The multiset $\{\alpha, \beta, \gamma\}$.

Autotopisms and Automorphisms

Let $\mathcal{S}_n$ be the symmetric group on n letters.
There is a natural action of $\mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$ on Latin squares, where (α, β, γ) applies

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

...The stabiliser of a Latin square is its *autotopism group*.

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

$\mathrm{aut}(n)$ is the subset of $\mathcal{S}_n$ consisting of all α such that $(\alpha, \alpha, \alpha) \in \mathrm{atp}(n)$. (Such α are *automorphisms*).

Whether (α, β, γ) is in $\mathrm{atp}(n)$ depends only on

- The multiset $\{\alpha, \beta, \gamma\}$.
- The cycle structure of α, β, γ.

Number of possible cycle structures

n	3 diff	2 diff	$\#\text{aut}(n)$	$\#\text{atp}(n)$
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

Stones' questions

Q1. If $(\alpha, \beta, \gamma) \in \mathrm{atp}(n)$ for some prime n,

Stones' questions

Q1. If $(\alpha, \beta, \gamma) \in \mathrm{atp}(n)$ for some prime n, but α, β, γ don't all have the same cycle structure, must one of them be the identity?

Stones' questions

Q1. If $(\alpha, \beta, \gamma) \in \mathrm{atp}(n)$ for some prime n, but α, β, γ don't all have the same cycle structure, must one of them be the identity?

The answer is yes for $n \leqslant 23$.

Stones' questions

Q1. If $(\alpha, \beta, \gamma) \in \mathrm{atp}(n)$ for some prime n, but α, β, γ don't all have the same cycle structure, must one of them be the identity?

The answer is yes for $n \leqslant 23$.

Q2. If $\theta \in \mathrm{atp}(n)$ then is the order of θ at most n?

Stones' questions

Q1. If $(\alpha, \beta, \gamma) \in \mathrm{atp}(n)$ for some prime n, but α, β, γ don't all have the same cycle structure, must one of them be the identity?

The answer is yes for $n \leqslant 23$.

Q2. If $\theta \in \mathrm{atp}(n)$ then is the order of θ at most n?

Horoševskiĭ [1974] proved the answer is yes for groups.

Stones' questions

Q1. If $(\alpha, \beta, \gamma) \in \mathrm{atp}(n)$ for some prime n, but α, β, γ don't all have the same cycle structure, must one of them be the identity?

The answer is yes for $n \leqslant 23$.

Q2. If $\theta \in \mathrm{atp}(n)$ then is the order of θ at most n?

Horoševskiĭ [1974] proved the answer is yes for groups.

Conjecture: For almost all $\alpha \in \mathcal{S}_n$ there are no $\beta, \gamma \in \mathcal{S}_n$ such that $(\alpha, \beta, \gamma) \in \mathrm{atp}(n)$.

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 $\lfloor \frac{1}{2}n \rfloor$ 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 $\psi(\alpha, p^a) \geqslant \frac{1}{2}n$.

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

The result

Theorem: Suppose Q is a quasigroup of order n. Then

1. $\mathrm{ord}(\alpha) \leqslant n^2/4$ for all $\alpha \in \mathrm{aut}(Q)$.

The result

Theorem: Suppose Q is a quasigroup of order n. Then

1. $\mathrm{ord}(\alpha) \leqslant n^2/4$ for all $\alpha \in \mathrm{aut}(Q)$.
2. $\mathrm{ord}(\theta) \leqslant n^4/16$ for all $\theta \in \mathrm{atp}(Q)$.

The result

Theorem: Suppose Q is a quasigroup of order n. Then

1. $\mathrm{ord}(\alpha) \leqslant n^2/4$ for all $\alpha \in \mathrm{aut}(Q)$.
2. $\mathrm{ord}(\theta) \leqslant n^4/16$ for all $\theta \in \mathrm{atp}(Q)$.
3. $\mathrm{ord}(\phi) \leqslant 3n^4/16$ for all $\phi \in \mathrm{par}(Q)$.

The result

Theorem: Suppose Q is a quasigroup of order n. Then

1. $\mathrm{ord}(\alpha) \leqslant n^2/4$ for all $\alpha \in \mathrm{aut}(Q)$.
2. $\mathrm{ord}(\theta) \leqslant n^4/16$ for all $\theta \in \mathrm{atp}(Q)$.
3. $\mathrm{ord}(\phi) \leqslant 3n^4/16$ for all $\phi \in \mathrm{par}(Q)$.

Corollary: A random permutation is not an automorphism of a quasigroup,

The result

Theorem: Suppose Q is a quasigroup of order n. Then

1. $\mathrm{ord}(\alpha) \leqslant n^2/4$ for all $\alpha \in \mathrm{aut}(Q)$.
2. $\mathrm{ord}(\theta) \leqslant n^4/16$ for all $\theta \in \mathrm{atp}(Q)$.
3. $\mathrm{ord}(\phi) \leqslant 3n^4/16$ for all $\phi \in \mathrm{par}(Q)$.

Corollary: A random permutation is not an automorphism of a quasigroup, Steiner triple system,

The result

Theorem: Suppose Q is a quasigroup of order n. Then

1. $\mathrm{ord}(\alpha) \leqslant n^2/4$ for all $\alpha \in \mathrm{aut}(Q)$.
2. $\mathrm{ord}(\theta) \leqslant n^4/16$ for all $\theta \in \mathrm{atp}(Q)$.
3. $\mathrm{ord}(\phi) \leqslant 3n^4/16$ for all $\phi \in \mathrm{par}(Q)$.

Corollary: A random permutation is not an automorphism of a quasigroup, Steiner triple system, or 1-factorisation of K_n;

The result

Theorem: Suppose Q is a quasigroup of order n. Then

1. $\mathrm{ord}(\alpha) \leqslant n^2/4$ for all $\alpha \in \mathrm{aut}(Q)$.
2. $\mathrm{ord}(\theta) \leqslant n^4/16$ for all $\theta \in \mathrm{atp}(Q)$.
3. $\mathrm{ord}(\phi) \leqslant 3n^4/16$ for all $\phi \in \mathrm{par}(Q)$.

Corollary: A random permutation is not an automorphism of a quasigroup, Steiner triple system, or 1-factorisation of K_n; nor is it a component of an autotopism,

The result

Theorem: Suppose Q is a quasigroup of order n. Then

1. $\mathrm{ord}(\alpha) \leqslant n^2/4$ for all $\alpha \in \mathrm{aut}(Q)$.
2. $\mathrm{ord}(\theta) \leqslant n^4/16$ for all $\theta \in \mathrm{atp}(Q)$.
3. $\mathrm{ord}(\phi) \leqslant 3n^4/16$ for all $\phi \in \mathrm{par}(Q)$.

Corollary: A random permutation is not an automorphism of a quasigroup, Steiner triple system, or 1-factorisation of K_n; nor is it a component of an autotopism, autoparatopism or

The result

Theorem: Suppose Q is a quasigroup of order n. Then

1. $\mathrm{ord}(\alpha) \leqslant n^2/4$ for all $\alpha \in \mathrm{aut}(Q)$.
2. $\mathrm{ord}(\theta) \leqslant n^4/16$ for all $\theta \in \mathrm{atp}(Q)$.
3. $\mathrm{ord}(\phi) \leqslant 3n^4/16$ for all $\phi \in \mathrm{par}(Q)$.

Corollary: A random permutation is not an automorphism of a quasigroup, Steiner triple system, or 1-factorisation of K_n; nor is it a component of an autotopism, autoparatopism or triceratopism of a latin square.

Prime orders

Theorem: Suppose Q is a quasigroup of order n and that $\theta = (\alpha, \beta, \gamma)$ is an autotopism of Q. If k is a prime power divisor of $\mathrm{ord}(\theta)$ and k does not divide n then

$$\psi(\alpha, k) = \psi(\beta, k) = \psi(\gamma, k) \geqslant \tfrac{1}{2}n.$$

Prime orders

Theorem: Suppose Q is a quasigroup of order n and that $\theta = (\alpha, \beta, \gamma)$ is an autotopism of Q. If k is a prime power divisor of $\mathrm{ord}(\theta)$ and k does not divide n then

$$\psi(\alpha, k) = \psi(\beta, k) = \psi(\gamma, k) \geqslant \tfrac{1}{2} n.$$

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

Theorem: Suppose Q is a quasigroup of order n and that $\theta = (\alpha, \beta, \gamma)$ is an autotopism of Q. If k is a prime power divisor of $\mathrm{ord}(\theta)$ and k does not divide n then

$$\psi(\alpha, k) = \psi(\beta, k) = \psi(\gamma, k) \geqslant \tfrac{1}{2}n.$$

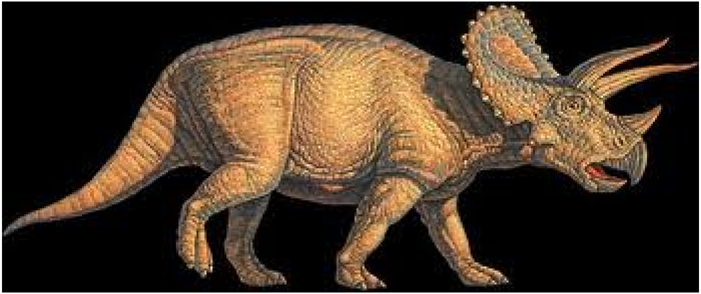
This is a strong restriction. For prime $n \leqslant 29$ it only leaves

$n = 23$, $(6^2, 3, 2, 1^6)$ 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 $2 \times (6^2, 3^3, 2^4)$.

But is it possible for prime order to have three different cycle structures?

Triceratopisms

An autotopism consisting of 3 permutations with different cycle structures is a *triceratopism*.



References

D. S. Stones, P. Vojtěchovský and I. M. Wanless,
Cycle structure of autotopisms of quasigroups and Latin squares,
J. Combin. Des., 2012.

R. M. Falcón,
Cycle structures of autotopisms of the Latin squares of order up to 11,
Ars Combin., to appear.

B. L. Kerby and J. D. H. Smith,
Quasigroup automorphisms and the Norton-Stein complex,
Proc. Amer. Math. Soc. **138** (2010), 3079–3088.

B. D. McKay, A. Meynert and W. Myrvold,
Small Latin squares, quasigroups and loops,
J. Combin. Des., **15** (2007), 98–119.

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

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

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.