Autotopisms of Latin Squares

Ian Wanless

Monash University

Joint work with Doug Stones and Petr Vojtěchovský

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. $\begin{array}{|cccc} \hline 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{array}$ is a Latin square of order 4.

Hence a Latin square is a 2 dimensional permutation.

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, 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*).

What is $\mathrm{atp}(n)$?

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

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

In particular, whether $\alpha \in \mathrm{aut}(n)$ depends only on the cycle structure of α.

I'll use "nontrivial cycle" for any cycle that is not a fixed point.

Our results are sufficient to determine $\mathrm{atp}(n)$ for $n \leqslant 17$, except they fail to show that $\mathrm{atp}(6)$ contains no autotopism with cycle structure $(4 \cdot 2, 4 \cdot 2, 4 \cdot 1^2)$.

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

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

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.

Automorphisms with two nontrivial cycles

Theorem: Suppose $\alpha \in \mathcal{S}_n$ consists of a d_1-cycle, a d_2-cycle and d_∞ fixed points.

If $d_1 = d_2$ then $\alpha \in \mathrm{aut}(n)$ iff $0 \leqslant d_\infty \leqslant 2d_1$.

If $d_1 > d_2$ then $\alpha \in \mathrm{aut}(n)$ iff

(a) d_2 divides d_1,

(b) $d_2 \geqslant d_\infty$, and

(c) if d_2 is even then $d_\infty > 0$.

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 $d_\infty > 0$.

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

Open? 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 $n \leqslant 23$ (but we have a counterexample for a larger value of n).

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 $(\alpha, \beta, \gamma) \in \mathrm{atp}(n)$.

That's all!

All results from today's talk appear in

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

See also:

R. M. Falcón,
Cycle structures of autotopisms of the Latin squares of order up to 11,
Ars Combin., (2012), 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.