Diagonally Cyclic Latin Squares

Ian Wanless

Monash University, Australia

Inc. joint work with Jack Allsop and Aleš Drápal

Diagonally Cyclic Latin Squares

A *Latin square* is a square matrix in which each row and column is a permutation of the same set of symbols.

$$\begin{bmatrix} 0 & 2 & 5 & 1 & 6 & 4 & 3 \\ 4 & 1 & 3 & 6 & 2 & 0 & 5 \\ 6 & 5 & 2 & 4 & 0 & 3 & 1 \\ 2 & 0 & 6 & 3 & 5 & 1 & 4 \\ 5 & 3 & 1 & 0 & 4 & 6 & 2 \\ 3 & 6 & 4 & 2 & 1 & 5 & 0 \\ 1 & 4 & 0 & 5 & 3 & 2 & 6 \end{bmatrix}$$

A Latin square is *diagonally cyclic* if the symbols occur in cyclic order along each broken diagonal parallel to the main diagonal.

Diagonally Cyclic Latin Squares

A DCLS is determined by its first row.

Diagonally Cyclic Latin Squares

A DCLS is determined by its first row.

0	1	2	3	4	$\cdots$
$\theta(0)$	$\theta(1)$	$\theta(2)$	$\theta(3)$	$\theta(4)$	$\cdots$

Diagonally Cyclic Latin Squares

A DCLS is determined by its first row.

0	1	2	3	4	$\cdots$
$\theta(0)$	$\theta(1)$	$\theta(2)$	$\theta(3)$	$\theta(4)$	$\cdots$

If I write down a permutation $x \mapsto \theta(x)$ will it produce a DCLS?

Diagonally Cyclic Latin Squares

A DCLS is determined by its first row.

0	1	2	3	4	$\cdots$
$\theta(0)$	$\theta(1)$	$\theta(2)$	$\theta(3)$	$\theta(4)$	$\cdots$

If I write down a permutation $x \mapsto \theta(x)$ will it produce a DCLS?

a		b
$\theta(a)$		$\theta(b)$
	$\ddots$	
	$\theta(a) + b - a$	

Diagonally Cyclic Latin Squares

A DCLS is determined by its first row.

0	1	2	3	4	$\cdots$
$\theta(0)$	$\theta(1)$	$\theta(2)$	$\theta(3)$	$\theta(4)$	$\cdots$

If I write down a permutation $x \mapsto \theta(x)$ will it produce a DCLS?

a		b
$\theta(a)$		$\theta(b)$
	$\ddots$	
	$\theta(a) + b - a$	

The only problem is if $\theta(a) + b - a = \theta(b)$ for some a and b.

Diagonally Cyclic Latin Squares

A DCLS is determined by its first row.

0	1	2	3	4	$\cdots$
$\theta(0)$	$\theta(1)$	$\theta(2)$	$\theta(3)$	$\theta(4)$	$\cdots$

If I write down a permutation $x \mapsto \theta(x)$ will it produce a DCLS?

a		b
$\theta(a)$		$\theta(b)$
	$\ddots$	
	$\theta(a) + b - a$	

The only problem is if $\theta(a) + b - a = \theta(b)$ for some a and b.

So we want $\theta(a) - a \neq \theta(b) - b$ for all a, b.

Orthomorphisms

An *orthomorphism* of an abelian group G is a permutation $\theta : G \mapsto G$ such that the map

$$x \mapsto \theta(x) - x$$

is also a permutation of G.

Orthomorphisms

An *orthomorphism* of an abelian group G is a permutation $\theta : G \mapsto G$ such that the map

$$x \mapsto \theta(x) - x$$

is also a permutation of G.

Eg. in $\mathbb{Z}_{13}$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\theta(x)$	0	2	10	6	8	12	4	9	1	5	7	3	11

Orthomorphisms

An *orthomorphism* of an abelian group G is a permutation $\theta : G \mapsto G$ such that the map

$$x \mapsto \theta(x) - x$$

is also a permutation of G.

Eg. in $\mathbb{Z}_{13}$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\theta(x)$	0	2	10	6	8	12	4	9	1	5	7	3	11

Orthomorphisms

An *orthomorphism* of an abelian group G is a permutation $\theta : G \mapsto G$ such that the map

$$x \mapsto \theta(x) - x$$

is also a permutation of G.

Eg. in $\mathbb{Z}_{13}$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\theta(x)$	0	2	10	6	8	12	4	9	1	5	7	3	11
$\theta(x) - x$	0	1	8	3	4	7	11	2	6	9	10	5	12

Orthomorphisms

An *orthomorphism* of an abelian group G is a permutation $\theta : G \mapsto G$ such that the map

$$x \mapsto \theta(x) - x$$

is also a permutation of G.

Eg. in $\mathbb{Z}_{13}$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\theta(x)$	0	2	10	6	8	12	4	9	1	5	7	3	11
$\theta(x) - x$	0	1	8	3	4	7	11	2	6	9	10	5	12

There is a DCLS with first row $[\theta(0), \theta(1), \ldots, \theta(n-1)]$ iff θ is an orthomorphism of $\mathbb{Z}_n$.

Generalisation to finite fields

Each Latin square can be written as a set of (row,column,symbol) triples.

Generalisation to finite fields

Each Latin square can be written as a set of (row,column,symbol) triples.

DCLS have a cyclic automorphism: $(r, c, s) \mapsto (r + 1, c + 1, s + 1)$

Generalisation to finite fields

Each Latin square can be written as a set of (row,column,symbol) triples.

DCLS have a cyclic automorphism: $(r, c, s) \mapsto (r + 1, c + 1, s + 1)$

Hence also $(r, c, s) \mapsto (r + a, c + a, s + a)$ for any fixed a.

Generalisation to finite fields

Each Latin square can be written as a set of (row,column,symbol) triples.

DCLS have a cyclic automorphism: $(r, c, s) \mapsto (r + 1, c + 1, s + 1)$

Hence also $(r, c, s) \mapsto (r + a, c + a, s + a)$ for any fixed a.

If we used the elements of a finite field to index the rows, columns and symbols, then this automorphism can be used to generalise DCLS.

Generalisation to finite fields

Each Latin square can be written as a set of (row,column,symbol) triples.

DCLS have a cyclic automorphism: $(r, c, s) \mapsto (r + 1, c + 1, s + 1)$

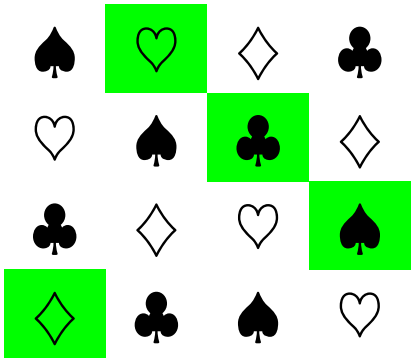
Hence also $(r, c, s) \mapsto (r + a, c + a, s + a)$ for any fixed a.

If we used the elements of a finite field to index the rows, columns and symbols, then this automorphism can be used to generalise DCLS.

Their structure is not so visually appealing but the theory works the same.

Transversals

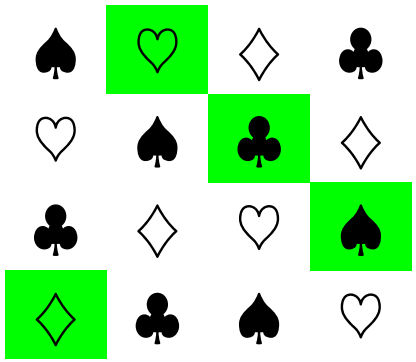
A *transversal* of a latin square is a set of entries which includes exactly one entry from each row and column and one of each symbol.



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

Transversals

A *transversal* of a latin square is a set of entries which includes exactly one entry from each row and column and one of each symbol.

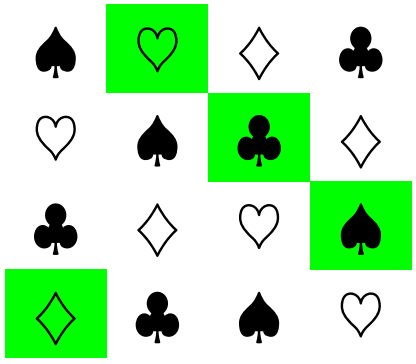


A	K	J	Q
Q	J	K	A
J	Q	A	K
K	A	Q	J

Theorem: [Euler] The addition table for $\mathbb{Z}_n$ has a transversal iff n is odd.

Transversals

A *transversal* of a latin square is a set of entries which includes exactly one entry from each row and column and one of each symbol.



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

Theorem: [Euler] The addition table for $\mathbb{Z}_n$ has a transversal iff n is odd.

A group has a transversal iff it has an orthomorphism:
Choose the triple $\big(x,\, \theta(x){-}x,\, \theta(x)\big)$ for each x.

Linear orthomorphisms

When will the map $x \mapsto \lambda x$ be an orthomorphism?

Linear orthomorphisms

When will the map $x \mapsto \lambda x$ be an orthomorphism?

We need $x \mapsto \lambda x$ and $x \mapsto (\lambda - 1)x$ to be permutations.

Linear orthomorphisms

When will the map $x \mapsto \lambda x$ be an orthomorphism?

We need $x \mapsto \lambda x$ and $x \mapsto (\lambda - 1)x$ to be permutations.

Over $\mathbb{Z}_n$, we need $\gcd(\lambda, n) = 1 = \gcd(\lambda - 1, n)$.
Over $\mathbb{F}_q$, we need $\lambda \notin \{0, 1\}$.

Cyclotomic orthomorphisms

A *cyclotomy class* of index k is a coset of a subgroup of index k in the multiplicative group $\mathbb{F}^*$.

Cyclotomic orthomorphisms

A *cyclotomy class* of index k is a coset of a subgroup of index k in the multiplicative group $\mathbb{F}^*$.

An orthomorphism θ is *cyclotomic of index k* if $\theta(0) = 0$ and $\theta(x)/x$ is constant on the cyclotomy classes of index k.

Cyclotomic orthomorphisms

A *cyclotomy class* of index k is a coset of a subgroup of index k in the multiplicative group $\mathbb{F}^*$.

An orthomorphism θ is *cyclotomic of index k* if $\theta(0) = 0$ and $\theta(x)/x$ is constant on the cyclotomy classes of index k.

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\theta(x)$	0	2	10	6	8	12	4	9	1	5	7	3	11
$\theta(x)/x$	–	2	5	2	2	5	5	5	5	2	2	5	2

Cyclotomic orthomorphisms

A *cyclotomy class* of index k is a coset of a subgroup of index k in the multiplicative group $\mathbb{F}^*$.

An orthomorphism θ is *cyclotomic of index k* if $\theta(0) = 0$ and $\theta(x)/x$ is constant on the cyclotomy classes of index k.

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\theta(x)$	0	2	10	6	8	12	4	9	1	5	7	3	11
$\theta(x)/x$	–	2	5	2	2	5	5	5	5	2	2	5	2

We use "linear", "quadratic", "cubic", "quartic", "quintic", ... to describe cyclotomic orthomorphisms of index 1, 2, 3, 4, 5, ...

Cyclotomic orthomorphisms

A *cyclotomy class* of index k is a coset of a subgroup of index k in the multiplicative group $\mathbb{F}^*$.

An orthomorphism θ is *cyclotomic of index k* if $\theta(0) = 0$ and $\theta(x)/x$ is constant on the cyclotomy classes of index k.

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\theta(x)$	0	2	10	6	8	12	4	9	1	5	7	3	11
$\theta(x)/x$	–	2	5	2	2	5	5	5	5	2	2	5	2

We use "linear", "quadratic", "cubic", "quartic", "quintic", ... to describe cyclotomic orthomorphisms of index 1, 2, 3, 4, 5, ...

Orthogonal cyclotomic orthomorphisms are the "best" way to construct mutually orthogonal latin squares.

The 16 card trick

Take the aces, kings, queens & jacks from a standard pack and arrange them in a 4×4 array so that each row and column contains one card of each suit and one card of each rank.

The 16 card trick

Take the aces, kings, queens & jacks from a standard pack and arrange them in a 4×4 array so that each row and column contains one card of each suit and one card of each rank.

$\spadesuit A$	$\heartsuit K$	$\diamondsuit J$	$\clubsuit Q$
$\heartsuit Q$	$\spadesuit J$	$\clubsuit K$	$\diamondsuit A$
$\clubsuit J$	$\diamondsuit Q$	$\heartsuit A$	$\spadesuit K$
$\diamondsuit K$	$\clubsuit A$	$\spadesuit Q$	$\heartsuit J$

The 16 card trick

Take the aces, kings, queens & jacks from a standard pack and arrange them in a 4×4 array so that each row and column contains one card of each suit and one card of each rank.

♠A	♡K	♢J	♣Q
♡Q	♠J	♣K	♢A
♣J	♢Q	♡A	♠K
♢K	♣A	♠Q	♡J

Each solution is the superposition of two latin squares

♠	♡	♢	♣
♡	♠	♣	♢
♣	♢	♡	♠
♢	♣	♠	♡

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

These squares are *orthogonal mates*.
When we overlay them each ordered pair of symbols occurs once.

Orthogonal DCLS

Two DCLS are orthogonal iff the difference between their orthomorphisms is itself a permutation.
eg Linear orthomorphisms $x \mapsto \lambda x$ and $x \mapsto \mu x$ are orthogonal provided $(\lambda - \mu)^{-1}$ exists.

Orthogonal DCLS

Two DCLS are orthogonal iff the difference between their orthomorphisms is itself a permutation.
eg Linear orthomorphisms $x \mapsto \lambda x$ and $x \mapsto \mu x$ are orthogonal provided $(\lambda - \mu)^{-1}$ exists.

In each finite field you can build a complete set of MOLS from the linear orthomorphisms (together with the LS with constant diagonals)

Orthogonal DCLS

Two DCLS are orthogonal iff the difference between their orthomorphisms is itself a permutation.
eg Linear orthomorphisms $x \mapsto \lambda x$ and $x \mapsto \mu x$ are orthogonal provided $(\lambda - \mu)^{-1}$ exists.

In each finite field you can build a complete set of MOLS from the linear orthomorphisms (together with the LS with constant diagonals)

For prime p, Evans ['92] showed how to build a maximal set of

$$\begin{cases} (p-1)/2 & \text{if } p \equiv 1 \mod 4 \\ (p-3)/2 & \text{if } p \equiv 3 \mod 4 \end{cases}$$

orthogonal LS using a quadratic orthomorphism and all the linear orthomorphisms orthogonal to it**.

Orthomorphism polynomials

Every function $\mathbb{F}_q \to \mathbb{F}_q$ can be represented by a polynomial of degree at most $q - 1$.

Orthomorphism polynomials

Every function $\mathbb{F}_q \to \mathbb{F}_q$ can be represented by a polynomial of degree at most $q-1$. If the function is a permutation, the degree is at most $q-2$ (and this is achieved by any transposition).

Orthomorphism polynomials

Every function $\mathbb{F}_q \to \mathbb{F}_q$ can be represented by a polynomial of degree at most $q-1$. If the function is a permutation, the degree is at most $q-2$ (and this is achieved by any transposition). If the function is an orthomorphism, the degree is at most $q-3$.

Orthomorphism polynomials

Every function $\mathbb{F}_q \to \mathbb{F}_q$ can be represented by a polynomial of degree at most $q-1$. If the function is a permutation, the degree is at most $q-2$ (and this is achieved by any transposition). If the function is an orthomorphism, the degree is at most $q-3$.

Theorem: [Allsop/W.'21] There exists an orthomorphism polynomial of degree $q-3$ over $\mathbb{F}_q$ if and only if $q \notin \{2, 3, 5, 8\}$.

Orthomorphism polynomials

Every function $\mathbb{F}_q \to \mathbb{F}_q$ can be represented by a polynomial of degree at most $q-1$. If the function is a permutation, the degree is at most $q-2$ (and this is achieved by any transposition). If the function is an orthomorphism, the degree is at most $q-3$.

Theorem: [Allsop/W.'21] There exists an orthomorphism polynomial of degree $q-3$ over $\mathbb{F}_q$ if and only if $q \notin \{2, 3, 5, 8\}$.

Theorem: There exist orthomorphisms f, g over $\mathbb{F}_q$ that differ on only 3 points in $\mathbb{F}_q$ if and only if $q \notin \{2, 5, 8\}$.

Orthomorphism polynomials

Every function $\mathbb{F}_q \to \mathbb{F}_q$ can be represented by a polynomial of degree at most $q-1$. If the function is a permutation, the degree is at most $q-2$ (and this is achieved by any transposition). If the function is an orthomorphism, the degree is at most $q-3$.

Theorem: [Allsop/W.'21] There exists an orthomorphism polynomial of degree $q-3$ over $\mathbb{F}_q$ if and only if $q \notin \{2,3,5,8\}$.

Theorem: There exist orthomorphisms f, g over $\mathbb{F}_q$ that differ on only 3 points in $\mathbb{F}_q$ if and only if $q \notin \{2,5,8\}$.

For such orthomorphisms $f-g$ has $q-3$ zeroes in $\mathbb{F}_q$, but is not identically zero. So $f-g$ has degree at least $q-3$.

Orthomorphism polynomials

Every function $\mathbb{F}_q \to \mathbb{F}_q$ can be represented by a polynomial of degree at most $q-1$. If the function is a permutation, the degree is at most $q-2$ (and this is achieved by any transposition). If the function is an orthomorphism, the degree is at most $q-3$.

Theorem: [Allsop/W.'21] There exists an orthomorphism polynomial of degree $q-3$ over $\mathbb{F}_q$ if and only if $q \notin \{2,3,5,8\}$.

Theorem: There exist orthomorphisms f, g over $\mathbb{F}_q$ that differ on only 3 points in $\mathbb{F}_q$ if and only if $q \notin \{2,5,8\}$.

For such orthomorphisms $f-g$ has $q-3$ zeroes in $\mathbb{F}_q$, but is not identically zero. So $f-g$ has degree at least $q-3$. Hence one (or both) of f or g must have degree $q-3$.

Orthomorphism polynomials

Every function $\mathbb{F}_q \to \mathbb{F}_q$ can be represented by a polynomial of degree at most $q-1$. If the function is a permutation, the degree is at most $q-2$ (and this is achieved by any transposition). If the function is an orthomorphism, the degree is at most $q-3$.

Theorem: [Allsop/W.'21] There exists an orthomorphism polynomial of degree $q-3$ over $\mathbb{F}_q$ if and only if $q \notin \{2,3,5,8\}$.

Theorem: There exist orthomorphisms f, g over $\mathbb{F}_q$ that differ on only 3 points in $\mathbb{F}_q$ if and only if $q \notin \{2,5,8\}$.

For such orthomorphisms $f-g$ has $q-3$ zeroes in $\mathbb{F}_q$, but is not identically zero. So $f-g$ has degree at least $q-3$. Hence one (or both) of f or g must have degree $q-3$.

Conjecture: Asymptotically almost all orthomorphisms have degree $q-3$.

Cyclotomic orthomorphisms as polynomials

A cyclotomic orthomorphism of index k corresponds to a polynomial of the form

$$\sum_{i=0}^{k-1} a_i X^{i(q-1)/k+1}$$

Cyclotomic orthomorphisms as polynomials

A cyclotomic orthomorphism of index k corresponds to a polynomial of the form

$$\sum_{i=0}^{k-1} a_i x^{i(q-1)/k+1}$$

e.g. quadratics are of the form $a_1 x^{(q+1)/2} + a_0 x$,
cubics have three equally spaced powers etc.

Cyclotomic orthomorphisms as polynomials

A cyclotomic orthomorphism of index k corresponds to a polynomial of the form

$$\sum_{i=0}^{k-1} a_i x^{i(q-1)/k+1}$$

e.g. quadratics are of the form $a_1 x^{(q+1)/2} + a_0 x$,
cubics have three equally spaced powers etc.

With Shallue (2013), we found all orthomorphism polynomials of degree $\leqslant 6$.

Subsquares

A *subsquare* is a submatrix that is itself a Latin square. For example here are a subsquare of order 3 and another of order 2.

$$\begin{bmatrix} 0 & 2 & 5 & 1 & 6 & 4 & 3 \\ 4 & 1 & 3 & 6 & 2 & 0 & 5 \\ 6 & 5 & 2 & 4 & 0 & 3 & 1 \\ 2 & 0 & 6 & 3 & 5 & 1 & 4 \\ 5 & 3 & 1 & 0 & 4 & 6 & 2 \\ 3 & 6 & 4 & 2 & 1 & 5 & 0 \\ 1 & 4 & 0 & 5 & 3 & 2 & 6 \end{bmatrix}$$

Subsquares

A *subsquare* is a submatrix that is itself a Latin square. For example here are a subsquare of order 3 and another of order 2.

$$\begin{bmatrix} 0 & 2 & 5 & 1 & 6 & 4 & 3 \\ 4 & 1 & 3 & 6 & 2 & 0 & 5 \\ 6 & 5 & 2 & 4 & 0 & 3 & 1 \\ 2 & 0 & 6 & 3 & 5 & 1 & 4 \\ 5 & 3 & 1 & 0 & 4 & 6 & 2 \\ 3 & 6 & 4 & 2 & 1 & 5 & 0 \\ 1 & 4 & 0 & 5 & 3 & 2 & 6 \end{bmatrix}$$

Theorem: [Maenhaut/Webb/W.'07] For all odd orders there exist Latin squares with no proper subsquares.

Subsquares

A *subsquare* is a submatrix that is itself a Latin square. For example here are a subsquare of order 3 and another of order 2.

$$\begin{bmatrix} 0 & 2 & 5 & 1 & 6 & 4 & 3 \\ 4 & 1 & 3 & 6 & 2 & 0 & 5 \\ 6 & 5 & 2 & 4 & 0 & 3 & 1 \\ 2 & 0 & 6 & 3 & 5 & 1 & 4 \\ 5 & 3 & 1 & 0 & 4 & 6 & 2 \\ 3 & 6 & 4 & 2 & 1 & 5 & 0 \\ 1 & 4 & 0 & 5 & 3 & 2 & 6 \end{bmatrix}$$

Theorem: [Maenhaut/Webb/W.'07] For all odd orders there exist Latin squares with no proper subsquares.

(The analogous problem for even orders is harder, and isn't completely resolved).

Row Cycles

2 rows of a LS define a permutation, which decomposes into cycles.

	0	2	5	1	6	4	3
	4	1	3	6	2	0	5
	6	5	2	4	0	3	1
$\rightarrow$	2	0	6	3	5	1	4
$\rightarrow$	5	3	1	0	4	6	2
	3	6	4	2	1	5	0
	1	4	0	5	3	2	6

Row Cycles

2 rows of a LS define a permutation, which decomposes into cycles.

	0	2	5	1	6	4	3
	4	1	3	6	2	0	5
	6	5	2	4	0	3	1
$\rightarrow$	2	0	6	3	5	1	4
$\rightarrow$	5	3	1	0	4	6	2
	3	6	4	2	1	5	0
	1	4	0	5	3	2	6

The rows marked with $\rightarrow$ form the permutation (254)(03)(61). Each of these 3 cycles gives us a *row cycle* (one of which is shown in green).

Row Cycles

2 rows of a LS define a permutation, which decomposes into cycles.

	0	2	5	1	6	4	3
	4	1	3	6	2	0	5
	6	5	2	4	0	3	1
$\rightarrow$	2	0	6	3	5	1	4
$\rightarrow$	5	3	1	0	4	6	2
	3	6	4	2	1	5	0
	1	4	0	5	3	2	6

The rows marked with $\rightarrow$ form the permutation (254)(03)(61). Each of these 3 cycles gives us a *row cycle* (one of which is shown in green).

A LS is *row-Hamiltonian* if every pair of rows forms a single cycle.

Row Cycles

2 rows of a LS define a permutation, which decomposes into cycles.

	0	2	5	1	6	4	3
	4	1	3	6	2	0	5
	6	5	2	4	0	3	1
$\rightarrow$	2	0	6	3	5	1	4
$\rightarrow$	5	3	1	0	4	6	2
	3	6	4	2	1	5	0
	1	4	0	5	3	2	6

The rows marked with $\rightarrow$ form the permutation (254)(03)(61). Each of these 3 cycles gives us a *row cycle* (one of which is shown in green).

A LS is *row-Hamiltonian* if every pair of rows forms a single cycle.

Similarly, we have column-Hamiltonian and symbol-Hamiltonian.

Hamiltonian LS

Cyclic groups of prime order are row-Hamiltonian, column-Hamiltonian and symbol-Hamiltonian.

Hamiltonian LS

Cyclic groups of prime order are row-Hamiltonian, column-Hamiltonian and symbol-Hamiltonian.

Quadratic orthomorphisms give us other examples of prime order, and even some of composite order!

Hamiltonian LS

Cyclic groups of prime order are row-Hamiltonian, column-Hamiltonian and symbol-Hamiltonian.

Quadratic orthomorphisms give us other examples of prime order, and even some of composite order!

Theorem: [Allsop/W.] For prime $p \equiv 3 \mod 8$, where $p \notin \{3, 19\}$, there exist LS of order p that are row-Hamiltonian and column-Hamiltonian but *not* symbol-Hamiltonian.

Hamiltonian LS

Cyclic groups of prime order are row-Hamiltonian, column-Hamiltonian and symbol-Hamiltonian.

Quadratic orthomorphisms give us other examples of prime order, and even some of composite order!

Theorem: [Allsop/W.] For prime $p \equiv 3 \mod 8$, where $p \notin \{3, 19\}$, there exist LS of order p that are row-Hamiltonian and column-Hamiltonian but *not* symbol-Hamiltonian.

-Hamiltonian LS correspond to perfect 1-factorisations of $K_{n,n}$.

Hamiltonian LS

Cyclic groups of prime order are row-Hamiltonian, column-Hamiltonian and symbol-Hamiltonian.

Quadratic orthomorphisms give us other examples of prime order, and even some of composite order!

Theorem: [Allsop/W.] For prime $p \equiv 3 \mod 8$, where $p \notin \{3, 19\}$, there exist LS of order p that are row-Hamiltonian and column-Hamiltonian but *not* symbol-Hamiltonian.

-Hamiltonian LS correspond to perfect 1-factorisations of $K_{n,n}$. They also have no proper subsquares.

Maximally non-associative quasigroups

If you write down the Cayley table of a finite group it produces a Latin square.

Maximally non-associative quasigroups

If you write down the Cayley table of a finite group it produces a Latin square. However, if you interpret a Latin square as the table for a binary operation what you typically get is a *quasigroup*.

Maximally non-associative quasigroups

If you write down the Cayley table of a finite group it produces a Latin square. However, if you interpret a Latin square as the table for a binary operation what you typically get is a *quasigroup*.

Quasigroups satisfy the cancellation laws

$$ax = ay \Longrightarrow x = y,$$

$$xa = ya \Longrightarrow x = y.$$

But in general they do not satisfy the associative law:
$(xy)z = x(yz)$.

Maximally non-associative quasigroups

If you write down the Cayley table of a finite group it produces a Latin square. However, if you interpret a Latin square as the table for a binary operation what you typically get is a *quasigroup*.

Quasigroups satisfy the cancellation laws

$$ax = ay \Longrightarrow x = y,$$

$$xa = ya \Longrightarrow x = y.$$

But in general they do not satisfy the associative law: $(xy)z = x(yz)$.

A quasigroup is *maximally non-associative* if $(xy)z = x(yz)$ only when $x = y = z$. Such quasigroups apparently have some application in cryptography.

Joint work with Aleš Drápal

Maximally non-associative quasigroups do not exist for orders $1, \ldots, 8$.

Joint work with Aleš Drápal

Maximally non-associative quasigroups do not exist for orders $1, \ldots, 8$.

Theorem: A maximally nonassociative quasigroup of order n exists for all $n \geqslant 9$, with the possible exception of $n \in \{11, 12, 15, 40, 42, 44, 56, 66, 77, 88, 90, 110\}$ and orders of the form $n = 2p_1$ or $n = 2p_1p_2$ for odd primes p_1, p_2 with $p_1 \leqslant p_2 < 2p_1$.

Joint work with Aleš Drápal

Maximally non-associative quasigroups do not exist for orders $1, \ldots, 8$.

Theorem: A maximally nonassociative quasigroup of order n exists for all $n \geqslant 9$, with the possible exception of $n \in \{11, 12, 15, 40, 42, 44, 56, 66, 77, 88, 90, 110\}$ and orders of the form $n = 2p_1$ or $n = 2p_1p_2$ for odd primes p_1, p_2 with $p_1 \leqslant p_2 < 2p_1$.

Theorem: For an odd prime power q the asymptotic proportion of quadratic orthomorphisms which produce maximally nonassociative quasigroups is

$$\begin{cases} \frac{953}{2^{15}} \approx 0.02908 & \text{for } q \equiv 1 \bmod 4, \\ \frac{825}{2^{16}} \approx 0.01259 & \text{for } q \equiv 3 \bmod 4. \end{cases}$$

That's all. Any questions?