Associative triples and quadratic orthomorphisms

Ian Wanless

Monash University, Australia

Inc. joint work with Aleš Drápal and Jack Allsop

Diagonally Cyclic Latin Squares

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

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

Diagonally Cyclic Latin Squares

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

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

A DCLS is determined by its first row.

Diagonally Cyclic Latin Squares

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

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

A DCLS is determined by its first row.
But which first rows work?

Diagonally Cyclic Latin Squares

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

Diagonally Cyclic Latin Squares

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

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

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

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?

$$\begin{array}{cc} a & b \\ \hline \theta(a) & \theta(b) \\ \ddots & \\ & \theta(a)+b-a \end{array}$$

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.

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

Cyclotomic orthomorphisms

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

Cyclotomic orthomorphisms

A *cyclotomy class* of index k is a coset of the 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 the 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.

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

Cyclotomic orthomorphisms

A *cyclotomy class* of index k is a coset of the 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.

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

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

Cyclotomic orthomorphisms

A *cyclotomy class* of index k is a coset of the 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.

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

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

Cyclotomic orthomorphisms

A *cyclotomy class* of index k is a coset of the 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.

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

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
$\theta(x)/x$	–	2	5	2	2	5	5	5	5	2	2	5	2

Cyclotomic orthomorphisms

A *cyclotomy class* of index k is a coset of the 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.

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

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
$\theta(x)/x$	–	2	5	2	2	5	5	5	5	2	2	5	2

So θ is a *quadratic orthomorphism*.

Cyclotomic maps

Let γ be a primitive element of the finite field $\mathbb{F}$. For $0 \leqslant j \leqslant k-1$ define the *cyclotomy class* $C_j = \{\gamma^{ki+j} : 0 \leqslant i \leqslant m-1\}$ to be a coset of the unique subgroup C_0 of index k in $\mathbb{F}^*$. A *cyclotomic map* $\phi = \phi_\gamma[a_0, \ldots, a_{k-1}]$ of index k can then be defined by

$$\phi(x) = \begin{cases} 0 & \text{if } x = 0, \\ a_i x & \text{if } x \in C_i, \end{cases}$$

where $a_0, \ldots, a_{k-1} \in \mathbb{F}$.

Cyclotomic maps

Let γ be a primitive element of the finite field $\mathbb{F}$. For $0 \leqslant j \leqslant k-1$ define the *cyclotomy class* $C_j = \{\gamma^{ki+j} : 0 \leqslant i \leqslant m-1\}$ to be a coset of the unique subgroup C_0 of index k in $\mathbb{F}^*$. A *cyclotomic map* $\phi = \phi_\gamma[a_0, \ldots, a_{k-1}]$ of index k can then be defined by

$$\phi(x) = \begin{cases} 0 & \text{if } x = 0, \\ a_i x & \text{if } x \in C_i, \end{cases}$$

where $a_0, \ldots, a_{k-1} \in \mathbb{F}$.

Such ϕ will be a permutation iff $C_j \mapsto a_j C_j$ permutes the cyclotomy classes.

Quadratic quasigroups $Q_{a,b}$

In general, a quadratic orthomorphism has the form

$$\theta(x) = \begin{cases} ax & \text{if } x \text{ is a square,} \\ bx & \text{if } x \text{ is a nonsquare,} \end{cases}$$

Quadratic quasigroups $Q_{a,b}$

In general, a quadratic orthomorphism has the form

$$\theta(x) = \begin{cases} ax & \text{if } x \text{ is a square,} \\ bx & \text{if } x \text{ is a nonsquare,} \end{cases}$$

From it, we can build a quasigroup $(Q_{a,b}, *)$ by

$$x * y = x + \theta(y - x)$$

for $x, y \in Q_{a,b}$.

Quadratic quasigroups $Q_{a,b}$

In general, a quadratic orthomorphism has the form

$$\theta(x) = \begin{cases} ax & \text{if } x \text{ is a square,} \\ bx & \text{if } x \text{ is a nonsquare,} \end{cases}$$

From it, we can build a quasigroup $(Q_{a,b}, *)$ by

$$x * y = x + \theta(y - x)$$

for $x, y \in Q_{a,b}$.

[We need odd characteristic, and both ab and $(a-1)(b-1)$ to be nonzero squares]

Maximally non-associative quasigroups

Recall: A quasigroup is *maximally non-associative* if $(xy)z = x(yz)$ only when $x = y = z$. Such quasigroups apparently have some application in cryptography for designing second pre-image resistant hash functions.

$Q_{2,5}$

*	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	2	10	6	8	12	4	9	1	5	7	3	11
1	12	1	3	11	7	9	0	5	10	2	6	8	4
2	5	0	2	4	12	8	10	1	6	11	3	7	9
3	10	6	1	3	5	0	9	11	2	7	12	4	8
4	9	11	7	2	4	6	1	10	12	3	8	0	5
5	6	10	12	8	3	5	7	2	11	0	4	9	1
6	2	7	11	0	9	4	6	8	3	12	1	5	10
7	11	3	8	12	1	10	5	7	9	4	0	2	6
8	7	12	4	9	0	2	11	6	8	10	5	1	3
9	4	8	0	5	10	1	3	12	7	9	11	6	2
10	3	5	9	1	6	11	2	4	0	8	10	12	7
11	8	4	6	10	2	7	12	3	5	1	9	11	0
12	1	9	5	7	11	3	8	0	4	6	2	10	12

$Q_{2,5}$

*	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	2	10	6	8	12	4	9	1	5	7	3	11
1	12	1	3	11	7	9	0	5	10	2	6	8	4
2	5	0	2	4	12	8	10	1	6	11	3	7	9
3	10	6	1	3	5	0	9	11	2	7	12	4	8
4	9	11	7	2	4	6	1	10	12	3	8	0	5
5	6	10	12	8	3	5	7	2	11	0	4	9	1
6	2	7	11	0	9	4	6	8	3	12	1	5	10
7	11	3	8	12	1	10	5	7	9	4	0	2	6
8	7	12	4	9	0	2	11	6	8	10	5	1	3
9	4	8	0	5	10	1	3	12	7	9	11	6	2
10	3	5	9	1	6	11	2	4	0	8	10	12	7
11	8	4	6	10	2	7	12	3	5	1	9	11	0
12	1	9	5	7	11	3	8	0	4	6	2	10	12

is the smallest MNQ built from a quadratic orthomorphism.

Characterisation of quadratic MNQs

$Q_{a,b}$ is an MNQ iff

(1) $a^2 \neq b$ or $a \neq 2b - b^2$,

(2) at least one of -1, $a - 1$ or a is nonsquare,

(3) at least one of b, $(1-a)(a^2-b)$ or $\sigma(a-1)$ is square,

(4) at least one of $a\nu$, $1 - b$ or $a\tau$ is square,

(5) -1 is nonsquare or $\sigma a(b-1)$ is square or $\tau a(b-1)$ is square,

(6) -1 is square or $b - 1$ is nonsquare or $(ab - a + b)b$ is nonsquare,

(7) $(b - a^2)\mu$ is square or $b\mu(ab - 2a + 1)$ is nonsquare or $(a-1)(ab-a+b)\mu$ is square,

(8) -1 is square or $a - 1$ is square or b is nonsquare,

(9) at least one of -1, a or $(ab - 2a + 1)(b - 1)$ is square, and

(10) conditions $(1) - (9)$ all apply when a and b are interchanged.

Here $\mu = b^2 - 2b + a$, $\nu = a^2 - 2a + b$, $\sigma = a^2 b - a^2 - ab + b$, and $\tau = a^2 b - ab - a + b$.

How many quadratic orthomorphisms give MNQs?

Using Weil bounds we were able to show that these conditions are satisfied in all large fields (of odd characteristic).

How many quadratic orthomorphisms give MNQs?

Using Weil bounds we were able to show that these conditions are satisfied in all large fields (of odd characteristic).

We also found MNQs from orthomorphisms of these groups:

$\mathbb{Z}_{21}, \mathbb{Z}_{33}, \mathbb{Z}_{35}, \mathbb{Z}_{55},$

$\mathbb{Z}_2 \times \mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_{10}, \mathbb{Z}_2 \times \mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_{14}, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4.$

How many quadratic orthomorphisms give MNQs?

Using Weil bounds we were able to show that these conditions are satisfied in all large fields (of odd characteristic).

We also found MNQs from orthomorphisms of these groups:

$\mathbb{Z}_{21}, \mathbb{Z}_{33}, \mathbb{Z}_{35}, \mathbb{Z}_{55}$,

$\mathbb{Z}_2 \times \mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_{10}, \mathbb{Z}_2 \times \mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_{14}, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$.

Theorem: MNQ exist for $n \geqslant 9$, 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 $p_1 \leqslant p_2 < 2p_1$.

How many quadratic orthomorphisms give MNQs?

Theorem: For odd prime powers q the asymptotic proportion of quadratic orthomorphisms which produce MNQs is

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

How many quadratic orthomorphisms give MNQs?

Theorem: For odd prime powers q the asymptotic proportion of quadratic orthomorphisms which produce MNQs is

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

Hence it is viable to find large MNQs “randomly”.

How many quadratic orthomorphisms give MNQs?

Theorem: For odd prime powers q the asymptotic proportion of quadratic orthomorphisms which produce MNQs is

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

Hence it is viable to find large MNQs "randomly".

We currently do not have a corresponding density result for the near-field construction that Aleš talked about yesterday. Drápal and Lisonek conjecture an asymptotic density of ≈ 0.29.

Orthomorphisms of higher index

Applications of orthomorphisms of higher index to the construction of maximally nonassociative quasigroups have not been developed;

Orthomorphisms of higher index

Applications of orthomorphisms of higher index to the construction of maximally nonassociative quasigroups have not been developed; ...with one exception:

Orthomorphisms of higher index

Applications of orthomorphisms of higher index to the construction of maximally nonassociative quasigroups have not been developed; ...with one exception:

Drápal and Hora [2020] built a loop of order 20 by prolonging a cubic quasigroup of order 19. Their loop had $1160 = 3n^2 - 2n$ associative triples, which is the fewest possible for involutory loops.

Orthomorphisms of higher index

Applications of orthomorphisms of higher index to the construction of maximally nonassociative quasigroups have not been developed; ...with one exception:

Drápal and Hora [2020] built a loop of order 20 by prolonging a cubic quasigroup of order 19. Their loop had $1160 = 3n^2 - 2n$ associative triples, which is the fewest possible for involutory loops.
For all primes $p \geqslant 13$ except $p = 19$ they had been able to find an involutory loop of order $n = p + 1$ with only $3n^2 - 2n$ associative triples by prolonging a quadratic quasigroup.

Automorphisms of quadratic quasigroups

Theorem: Let $Q_{a,b}$ and $Q_{c,d}$ be quadratic quasigroups over $\mathbb{F}$. Then $Q_{a,b}$ is isomorphic to $Q_{c,d}$ if and only if there exists $\alpha \in \mathrm{aut}(\mathbb{F})$ such that $\{a, b\} = \{\alpha(c), \alpha(d)\}$.

Automorphisms of quadratic quasigroups

Theorem: Let $Q_{a,b}$ and $Q_{c,d}$ be quadratic quasigroups over $\mathbb{F}$. Then $Q_{a,b}$ is isomorphic to $Q_{c,d}$ if and only if there exists $\alpha \in \mathrm{aut}(\mathbb{F})$ such that $\{a, b\} = \{\alpha(c), \alpha(d)\}$.

Open question: The corresponding result with "isotopic" in place of "isomorphic".

Automorphisms of quadratic quasigroups

Theorem: Let $Q_{a,b}$ and $Q_{c,d}$ be quadratic quasigroups over $\mathbb{F}$. Then $Q_{a,b}$ is isomorphic to $Q_{c,d}$ if and only if there exists $\alpha \in \mathrm{aut}(\mathbb{F})$ such that $\{a, b\} = \{\alpha(c), \alpha(d)\}$.

Open question: The corresponding result with "isotopic" in place of "isomorphic".

Theorem: Let $Q = Q_{a,b}$ be a quadratic quasigroup over $\mathbb{F}$ with $a \neq b$. Denote by $\mathbb{K}$ the least subfield of $\mathbb{F}$ that contains $\{a, b\}$. The automorphism group of Q consists of all affine semilinear mappings $x \mapsto \lambda\alpha(x) + \mu$, where λ is a square in $\mathbb{F}^*$, $\mu \in \mathbb{F}$ and $\alpha \in \mathrm{Gal}(\mathbb{F} \mid \mathbb{K})$, except:

(i) If $b = a^\gamma$ and $\gamma^2 = |\mathbb{K}|$, then we also have automorphisms $x \mapsto \lambda\alpha(x^\gamma) + \mu$, where λ is a nonsquare.

(ii) If $|\mathbb{F}| = 7$ and $\{a, b\} = \{3, 5\}$, then $\mathrm{aut}(Q) \cong \mathrm{PSL}_2(7)$.

Quadratic quasigroups in certain varieties

Theorem: Let $Q = Q_{a,b}$ be a quadratic quasigroup upon $\mathbb{F}$. Then

(i) Q is medial (i.e. fulfils the law $xy \cdot uv = xu \cdot yv$) if and only if $a = b$;

(ii) Q is left distributive (i.e. fulfils the law $x \cdot yz = xy \cdot xz$) if and only if $a = b$;

(iii) Q is right distributive (i.e. fulfils the law $xy \cdot z = xz \cdot yz$) if and only if $a = b$;

(iv) Q is commutative if and only if $a + b = 1$ and either $|\mathbb{F}| \equiv 3 \bmod 4$ or $a = b$.

(v) Q is flexible (i.e. fulfils the law $x \cdot yx = xy \cdot x$) if and only if $a = b$ or $\chi(a) = \chi(1 - a) = 1$ or both $a + b = 1$ and $|\mathbb{F}| \equiv 3 \bmod 4$;

(vi) Q is semisymmetric (i.e. fulfils the law $xy \cdot x = y$) if and only if $a^2 - a + 1 = 0$ and either $a = b$ or $a + b = 1$.

(vii) Q is a Steiner quasigroup (i.e. idempotent, commutative and semisymmetric) if and only if either $\mathbb{F}$ has characteristic 3 and $a = b = -1$, or $\mathbb{F}$ has characteristic > 3, $a + b = ab = 1$, and $\chi(a) = \chi(-1) = -1$. In the latter case, $a \neq b$.

(viii) Q is isotopic to a group if and only if $a = b$.

Snow Design

Perfect 1-factorisations

A *1-factor* of a graph is a set of edges covering every vertex exactly once.

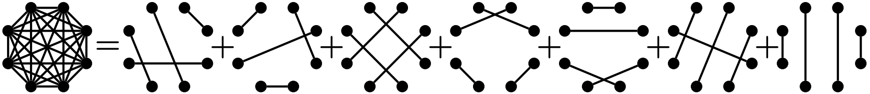
Perfect 1-factorisations

A 1-*factor* of a graph is a set of edges covering every vertex exactly once.

A 1-*factorisation* is a decomposition of a graph into 1-factors.

Perfect 1-factorisations

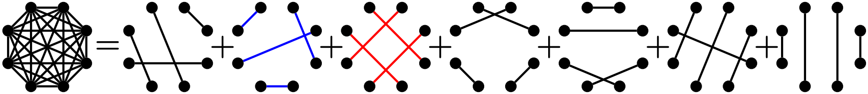
A *1-factor* of a graph is a set of edges covering every vertex exactly once.
A *1-factorisation* is a decomposition of a graph into 1-factors.



Perfect 1-factorisations

A *1-factor* of a graph is a set of edges covering every vertex exactly once.

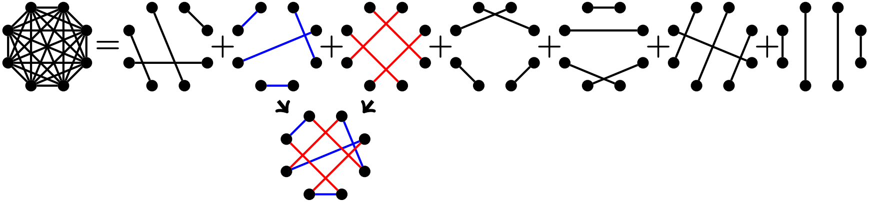
A *1-factorisation* is a decomposition of a graph into 1-factors.



Perfect 1-factorisations

A *1-factor* of a graph is a set of edges covering every vertex exactly once.

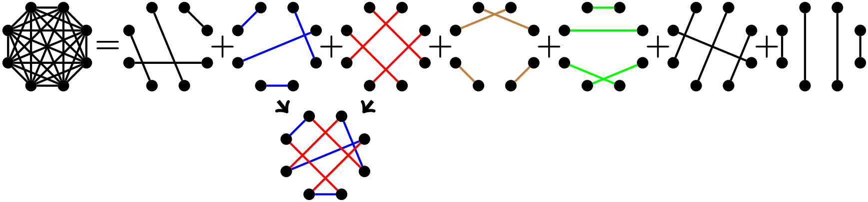
A *1-factorisation* is a decomposition of a graph into 1-factors.



Perfect 1-factorisations

A *1-factor* of a graph is a set of edges covering every vertex exactly once.

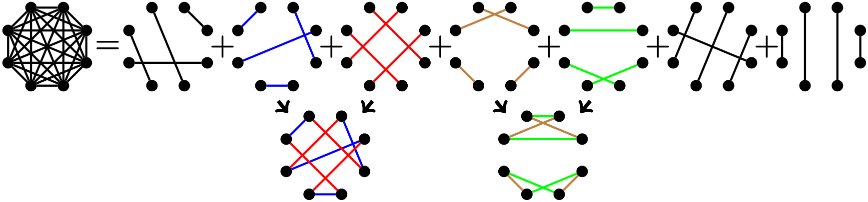
A *1-factorisation* is a decomposition of a graph into 1-factors.



Perfect 1-factorisations

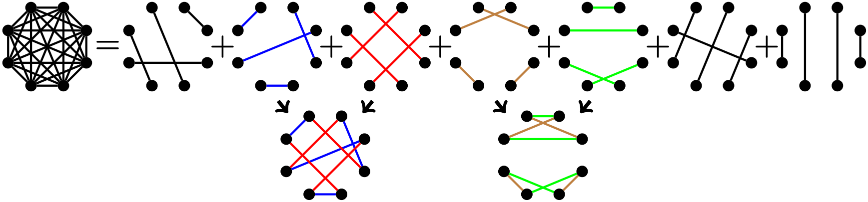
A *1-factor* of a graph is a set of edges covering every vertex exactly once.

A *1-factorisation* is a decomposition of a graph into 1-factors.



Perfect 1-factorisations

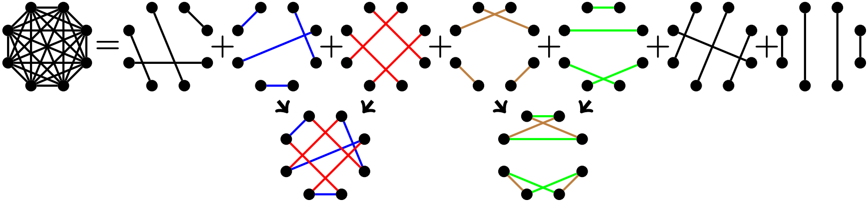
A *1-factor* of a graph is a set of edges covering every vertex exactly once.
A *1-factorisation* is a decomposition of a graph into 1-factors.



A *perfect 1-factorisation (P1F)* is a 1-factorisation for which every pair of 1-factors form a Hamiltonian cycle.

Perfect 1-factorisations

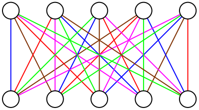
A *1-factor* of a graph is a set of edges covering every vertex exactly once.
A *1-factorisation* is a decomposition of a graph into 1-factors.



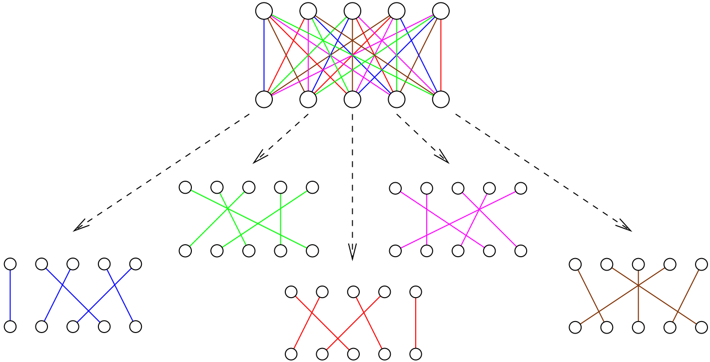
A *perfect 1-factorisation (P1F)* is a 1-factorisation for which every pair of 1-factors form a Hamiltonian cycle.

Today I will talk about P1Fs of the complete bipartite graph $K_{n,n}$ (n odd or $n = 2$).

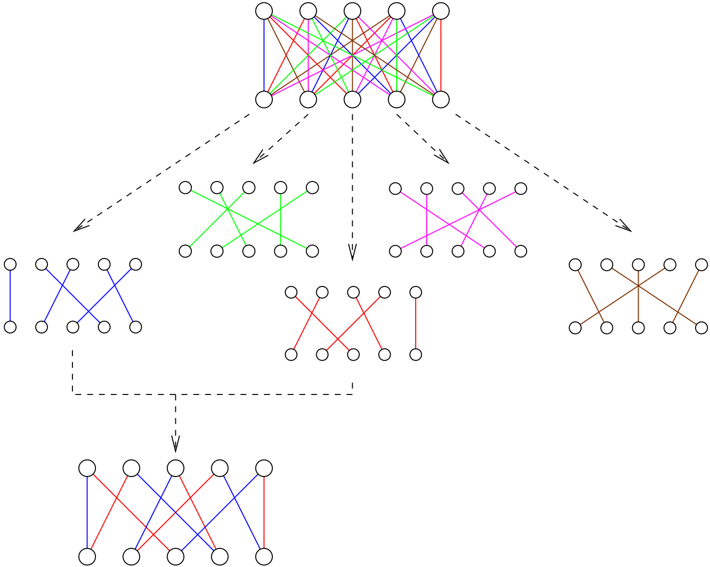
A 1-factorisation of $K_{5,5}$



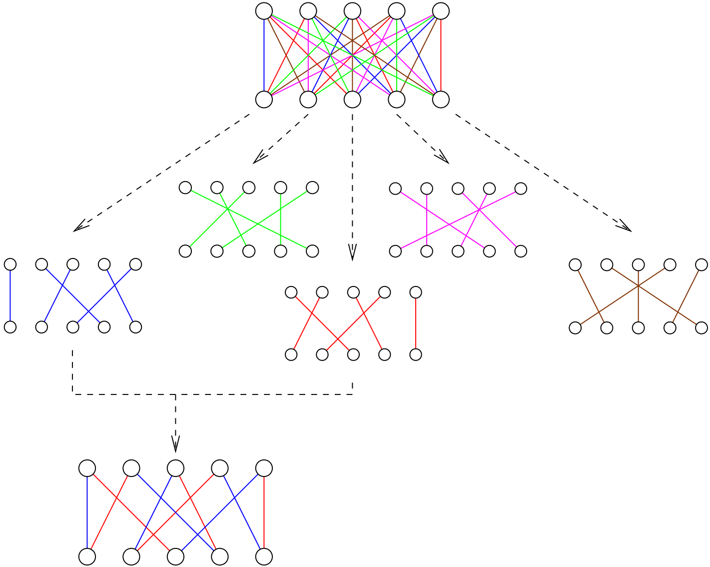
A 1-factorisation of $K_{5,5}$



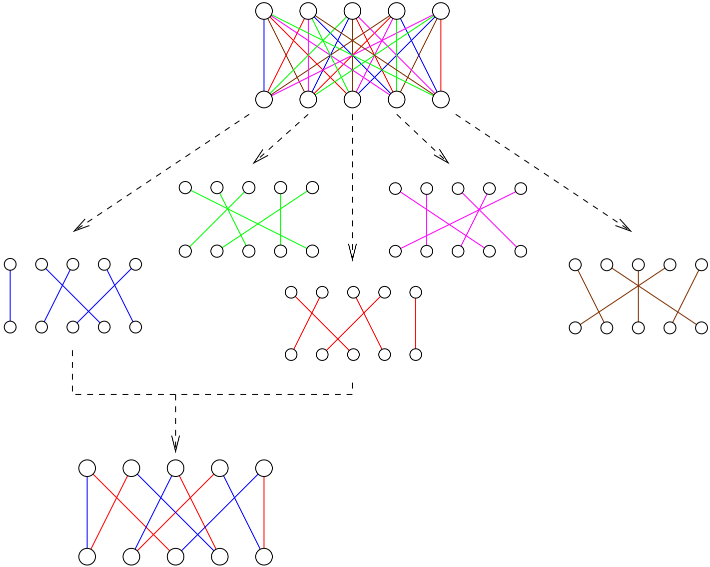
A 1-factorisation of $K_{5,5}$



A perfect 1-factorisation of $K_{5,5}$



A perfect 1-factorisation of $K_{5,5}$



Row Cycles

Two 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

Two 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

Two 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).

Each row cycle corresponds to a cycle of the permutation $L_y \circ L_x^{-1}$ where

$$L_x : Q \rightarrow Q, \qquad L_x(z) = x \cdot z.$$

Similarly, there are *column cycles*, corresponding to cycles of $R_y \circ R_x^{-1}$, where

$$R_x : Q \rightarrow Q, \qquad R_x(z) = z \cdot x.$$

Hamiltonian LS

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

Hamiltonian LS

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

Let $\nu(L)$ denote the number of parastrophes of L which are row-Hamiltonian.

Hamiltonian LS

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

Let $\nu(L)$ denote the number of parastrophes of L which are row-Hamiltonian.

It's easy to see that $\nu(L) \in \{0, 2, 4, 6\}$.

Hamiltonian LS

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

Let $\nu(L)$ denote the number of parastrophes of L which are row-Hamiltonian.

It's easy to see that $\nu(L) \in \{0, 2, 4, 6\}$.

All previously known families of row-Hamiltonian LS have $\nu(L) \in \{2, 6\}$.

Hamiltonian LS

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

Let $\nu(L)$ denote the number of parastrophes of L which are row-Hamiltonian.

It's easy to see that $\nu(L) \in \{0, 2, 4, 6\}$.

All previously known families of row-Hamiltonian LS have $\nu(L) \in \{2, 6\}$.

We call L *atomic* if $\nu(L) = 6$.

Hamiltonian LS

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

Let $\nu(L)$ denote the number of parastrophes of L which are row-Hamiltonian.

It's easy to see that $\nu(L) \in \{0, 2, 4, 6\}$.

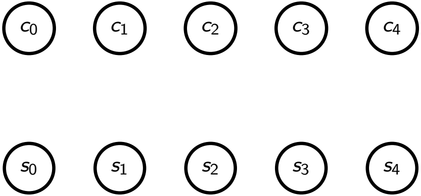
All previously known families of row-Hamiltonian LS have $\nu(L) \in \{2, 6\}$.

We call L *atomic* if $\nu(L) = 6$.

We have 5 families of atomic Latin squares but all are for prime orders only. There are some sporadic orders up to 39601 known, but they are all for prime power orders.

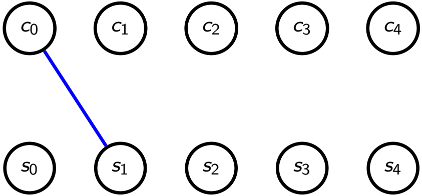
1-factorisations from Latin squares

1	2	4	0	3
3	1	0	2	4
4	3	2	1	0
0	4	1	3	2
2	0	3	4	1



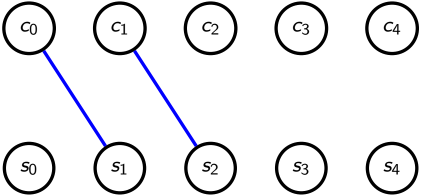
1-factorisations from Latin squares

1	2	4	0	3
3	1	0	2	4
4	3	2	1	0
0	4	1	3	2
2	0	3	4	1



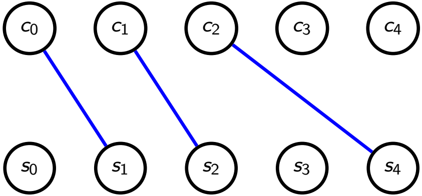
1-factorisations from Latin squares

1	*2*	4	0	3
3	1	0	2	4
4	3	2	1	0
0	4	1	3	2
2	0	3	4	1



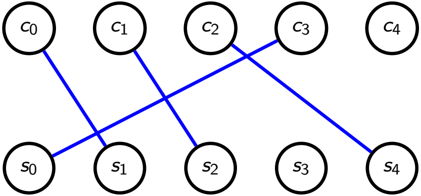
1-factorisations from Latin squares

1	*2*	*4*	0	3
3	1	0	2	4
4	3	2	1	0
0	4	1	3	2
2	0	3	4	1



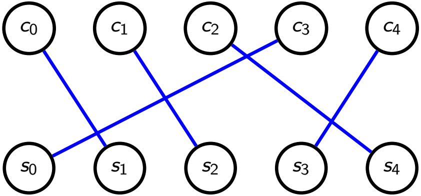
1-factorisations from Latin squares

1	*2*	*4*	*0*	3
3	1	0	2	4
4	3	2	1	0
0	4	1	3	2
2	0	3	4	1



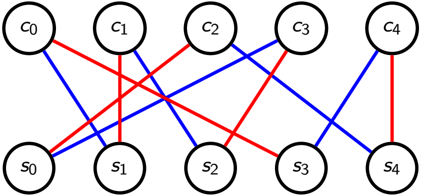
1-factorisations from Latin squares

1	*2*	*4*	*0*	*3*
3	1	0	2	4
4	3	2	1	0
0	4	1	3	2
2	0	3	4	1



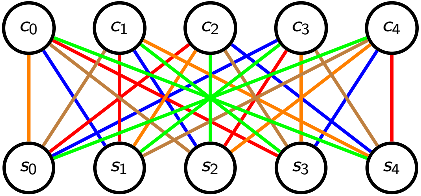
1-factorisations from Latin squares

1	*2*	*4*	*0*	*3*
3	1	0	2	4
4	3	2	1	0
0	4	1	3	2
2	0	3	4	1



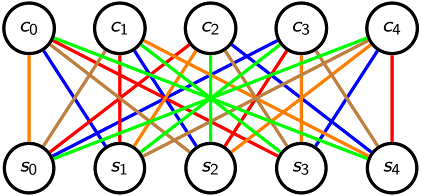
1-factorisations from Latin squares

1	*2*	*4*	*0*	*3*
3	1	0	2	4
4	3	2	1	0
0	4	1	3	2
2	0	3	4	1



1-factorisations from Latin squares

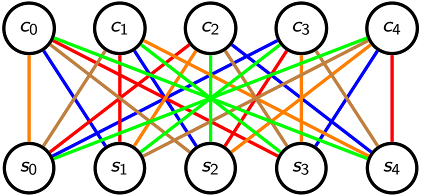
1	*2*	*4*	*0*	*3*
3	1	0	2	4
4	3	2	1	0
0	4	1	3	2
2	0	3	4	1



$n \times n$ Latin squares correspond to 1-factorisations of $K_{n,n}$.

1-factorisations from Latin squares

1	*2*	*4*	*0*	*3*
3	1	0	2	4
4	3	2	1	0
0	4	1	3	2
2	0	3	4	1

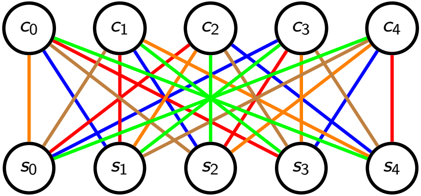


$n \times n$ Latin squares correspond to 1-factorisations of $K_{n,n}$.

$n \times n$ row-Hamiltonian Latin squares correspond to P1Fs of $K_{n,n}$.

1-factorisations from Latin squares

1	*2*	*4*	*0*	*3*
3	1	0	2	4
4	3	2	1	0
0	4	1	3	2
2	0	3	4	1



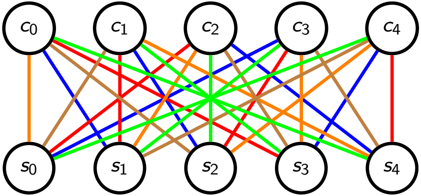
$n \times n$ Latin squares correspond to 1-factorisations of $K_{n,n}$.

$n \times n$ row-Hamiltonian Latin squares correspond to P1Fs of $K_{n,n}$.

Conjecture: [Kotzig'64] There exists a P1F of $K_{n,n}$ for all odd n.

1-factorisations from Latin squares

1	*2*	*4*	*0*	*3*
3	1	0	2	4
4	3	2	1	0
0	4	1	3	2
2	0	3	4	1



$n \times n$ Latin squares correspond to 1-factorisations of $K_{n,n}$.

$n \times n$ row-Hamiltonian Latin squares correspond to P1Fs of $K_{n,n}$.

Conjecture: [Kotzig'64] There exists a P1F of $K_{n,n}$ for all odd n.

Only proved for some sporadic orders and $K_{p,p}$, $K_{2p-1,2p-1}$ and K_{p^2,p^2} where p is an odd prime.

Enumeration

n	All 1F of $K_{n,n}$	P1F
2	1	1
3	1	1
4	2	-
5	2	1
6	17	-
7	324	2
8	842227	-
9	57810418543	37
10	104452188344901572	-
11	6108088657705958932053657	

Counted by

6	Clausen 1842??, Tarry 1900	
9		W. 1999
10	McKay/Meynert/Myrvold 2007	
11	Hulpke/Kaski/Östergård 2011	

Use a quadratic orthomorphism!

You don't need to check much to see if $Q_{a,b}$ is row-Hamiltonian, since it has such a large automorphism group.

Use a quadratic orthomorphism!

You don't need to check much to see if $Q_{a,b}$ is row-Hamiltonian, since it has such a large automorphism group.

If $p \equiv 3 \bmod 4$ there is a single orbit on unordered pairs of rows.

Use a quadratic orthomorphism!

You don't need to check much to see if $Q_{a,b}$ is row-Hamiltonian, since it has such a large automorphism group.

If $p \equiv 3 \bmod 4$ there is a single orbit on unordered pairs of rows.

If $p \equiv 1 \bmod 4$ there are two orbits on unordered pairs of rows.

Use a quadratic orthomorphism!

You don't need to check much to see if $Q_{a,b}$ is row-Hamiltonian, since it has such a large automorphism group.

If $p \equiv 3 \bmod 4$ there is a single orbit on unordered pairs of rows.

If $p \equiv 1 \bmod 4$ there are two orbits on unordered pairs of rows.

Let p be a prime where $p \equiv 1, 3 \bmod 8$ and let $\mathcal{L}_p = Q_{-1,\frac{1}{2}}$.

Use a quadratic orthomorphism!

You don't need to check much to see if $Q_{a,b}$ is row-Hamiltonian, since it has such a large automorphism group.

If $p \equiv 3 \bmod 4$ there is a single orbit on unordered pairs of rows.
If $p \equiv 1 \bmod 4$ there are two orbits on unordered pairs of rows.

Let p be a prime where $p \equiv 1, 3 \bmod 8$ and let $\mathcal{L}_p = Q_{-1,\frac{1}{2}}$.

I conjectured in 2010 that $\mathcal{L}_p$ is row-Hamiltonian.

Use a quadratic orthomorphism!

You don't need to check much to see if $Q_{a,b}$ is row-Hamiltonian, since it has such a large automorphism group.

If $p \equiv 3 \bmod 4$ there is a single orbit on unordered pairs of rows.

If $p \equiv 1 \bmod 4$ there are two orbits on unordered pairs of rows.

Let p be a prime where $p \equiv 1, 3 \bmod 8$ and let $\mathcal{L}_p = Q_{-1,\frac{1}{2}}$.

I conjectured in 2010 that $\mathcal{L}_p$ is row-Hamiltonian. Then in 2021 my student Jack Allsop found Beck's Theorem, which allows you to show a permutation consists of a single cycle by showing that a certain matrix is non-singular over $\mathbb{Z}_2$.

Use a quadratic orthomorphism!

You don't need to check much to see if $Q_{a,b}$ is row-Hamiltonian, since it has such a large automorphism group.

If $p \equiv 3 \bmod 4$ there is a single orbit on unordered pairs of rows.
If $p \equiv 1 \bmod 4$ there are two orbits on unordered pairs of rows.

Let p be a prime where $p \equiv 1, 3 \bmod 8$ and let $\mathcal{L}_p = Q_{-1,\frac{1}{2}}$.

I conjectured in 2010 that $\mathcal{L}_p$ is row-Hamiltonian. Then in 2021 my student Jack Allsop found Beck's Theorem, which allows you to show a permutation consists of a single cycle by showing that a certain matrix is non-singular over $\mathbb{Z}_2$.

Theorem: $\mathcal{L}_p$ is row-Hamiltonian for all $p \equiv 1, 3 \bmod 8$.

Use a quadratic orthomorphism!

You don't need to check much to see if $Q_{a,b}$ is row-Hamiltonian, since it has such a large automorphism group.

If $p \equiv 3 \bmod 4$ there is a single orbit on unordered pairs of rows.

If $p \equiv 1 \bmod 4$ there are two orbits on unordered pairs of rows.

Let p be a prime where $p \equiv 1, 3 \bmod 8$ and let $\mathcal{L}_p = Q_{-1,\frac{1}{2}}$.

I conjectured in 2010 that $\mathcal{L}_p$ is row-Hamiltonian. Then in 2021 my student Jack Allsop found Beck's Theorem, which allows you to show a permutation consists of a single cycle by showing that a certain matrix is non-singular over $\mathbb{Z}_2$.

Theorem: $\mathcal{L}_p$ is row-Hamiltonian for all $p \equiv 1, 3 \bmod 8$.
It has no Hamiltonian column cycles unless $p \in \{3, 19\}$.

Example $p = 11$

$$\begin{array}{c|cccccccccc}
 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
2 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
3 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
4 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
5 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
6 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
7 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\
8 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
9 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
10 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{array}$$

Example $p = 11$

	1	2	3	4	5	6	7	8	9	10
1	0	0	0	0	0	0	0	0	0	1
2	0	0	1	1	0	1	1	1	1	1
3	0	1	0	0	0	1	1	1	0	1
4	0	1	0	0	0	1	1	1	1	1
5	0	0	0	0	0	1	1	1	1	1
6	0	1	1	1	1	0	1	1	0	1
7	0	1	1	1	1	1	0	1	0	1
8	0	1	1	1	1	1	1	0	0	1
9	0	1	0	1	1	0	0	0	0	1
10	1	1	1	1	1	1	1	1	1	0

Example $p = 11$

	1	2	3	4	5	6	7	8	9	10
1	0	0	0	0	0	0	0	0	0	1
2	0	0	1	1	0	1	1	1	1	1
3	0	1	0	0	0	1	1	1	0	1
4	0	1	0	0	0	1	1	1	1	1
5	0	0	0	0	0	1	1	1	1	1
6	0	1	1	1	1	0	1	1	0	1
7	0	1	1	1	1	1	0	1	0	1
8	0	1	1	1	1	1	1	0	0	1
9	0	1	0	1	1	0	0	0	0	1
10	1	1	1	1	1	1	1	1	1	0

Phase 1

	1	2	3	4	5	6	7	8	9	10
1	0	0	0	0	0	0	0	0	0	1
2	0	0	1	1	0	1	1	1	1	1
3	0	1	0	0	0	1	1	1	0	1
4	0	1	0	0	0	1	1	1	1	1
5	0	0	0	0	0	1	1	1	1	1
6	0	1	1	1	1	0	1	1	0	1
7	0	1	1	1	1	1	0	1	0	1
8	0	1	1	1	1	1	1	0	0	1
9	0	1	0	1	1	0	0	0	0	1
10	1	1	1	1	1	1	1	1	1	0

Phase 1

$$\begin{array}{c c} & \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 9 & 10 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 9 \\ 10 \end{array} & \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Phase 2

	1	2	3	4	5	6	9	10
1	0	0	0	0	0	0	0	1
2	0	0	1	1	0	1	1	1
3	0	1	0	0	0	1	0	1
4	0	1	0	0	0	1	1	1
5	0	0	0	0	0	1	1	1
6	0	1	1	1	1	0	0	1
9	0	1	0	1	1	0	0	1
10	1	1	1	1	1	1	1	0

Phase 2

$$
\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 9 \\ 10 \end{array}
\begin{array}{c}
\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 9 & 10 \end{array} \\
\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{pmatrix}
\end{array}
$$

Phase 2

$$
\begin{array}{c|cccccc}
 & 1 & 3 & 5 & 6 & 9 & 10 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 & 1 \\
3 & 0 & 0 & 0 & 1 & 0 & 1 \\
5 & 0 & 0 & 0 & 1 & 1 & 1 \\
6 & 0 & 1 & 1 & 0 & 0 & 1 \\
9 & 0 & 0 & 1 & 0 & 0 & 1 \\
10 & 1 & 1 & 1 & 1 & 1 & 0
\end{array}
$$

Phase 2

	1	3	5	6	9	10
1	0	0	0	0	0	1
3	0	0	0	1	0	1
5	0	0	0	1	1	1
6	0	1	1	0	0	1
9	0	0	1	0	0	1
10	1	1	1	1	1	0

Phase 2

	1	3	5	6	9	10
1	0	0	0	0	0	1
3	0	0	0	1	0	1
5	0	0	0	1	1	1
6	0	1	1	0	0	1
9	0	0	1	0	0	1
10	1	1	1	1	1	0

Phase 2

$$\begin{array}{c} \\ 1 \\ 5 \\ 9 \\ 10 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 5 & 9 & 10 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Phase 3

	1	5	9	10
1	0	0	0	1
5	0	0	1	1
9	0	1	0	1
10	1	1	1	0

Phase 3

	1	5	9	10
1	0	0	0	1
5	0	0	1	1
9	0	1	0	1
10	1	1	1	0

The end game

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Not atomic

$\mathcal{L}_p$ has a autoparastrophy mapping its rows to symbols, so $\nu(\mathcal{L}_p) \geqslant 4$.

Not atomic

$\mathcal{L}_p$ has a autoparastrophy mapping its rows to symbols, so $\nu(\mathcal{L}_p) \geqslant 4$.

If there exists $x \in \mathbb{Z}_p$ such that

$$x, x+1, x+\frac{1}{2} \in \Box \quad \text{and} \quad -\frac{x}{2}-\frac{3}{4}, \frac{1}{4}-\frac{x}{2} \notin \Box$$

Not atomic

$\mathcal{L}_p$ has a autoparastrophy mapping its rows to symbols, so $\nu(\mathcal{L}_p) \geqslant 4$.

If there exists $x \in \mathbb{Z}_p$ such that

$$x, x+1, x+\frac{1}{2} \in \Box \quad \text{and} \quad -\frac{x}{2}-\frac{3}{4}, \frac{1}{4}-\frac{x}{2} \notin \Box$$

then $\mathcal{L}_p$ has a column cycle of length 3.

Not atomic

$\mathcal{L}_p$ has a autoparastrophy mapping its rows to symbols, so $\nu(\mathcal{L}_p) \geqslant 4$.

If there exists $x \in \mathbb{Z}_p$ such that

$$x, x+1, x+\frac{1}{2} \in \square \quad \text{and} \quad -\frac{x}{2}-\frac{3}{4}, \frac{1}{4}-\frac{x}{2} \notin \square$$

then $\mathcal{L}_p$ has a column cycle of length 3.

Such an x exists for all large p by Weil's theorem, and all small p can be checked by computer.

Not atomic

$\mathcal{L}_p$ has a autoparastrophy mapping its rows to symbols, so $\nu(\mathcal{L}_p) \geqslant 4$.

If there exists $x \in \mathbb{Z}_p$ such that

$$x, x+1, x+\frac{1}{2} \in \Box \quad \text{and} \quad -\frac{x}{2}-\frac{3}{4}, \frac{1}{4}-\frac{x}{2} \notin \Box$$

then $\mathcal{L}_p$ has a column cycle of length 3.

Such an x exists for all large p by Weil's theorem, and all small p can be checked by computer.

$\mathcal{L}_p$ is atomic for $p \in \{3, 19\}$, but otherwise $\nu(\mathcal{L}_p) = 4$.

Varieties

Let E be a set of identities. The *loop variety* defined by E is the set of loops satisfying all identities in E.

Varieties

Let E be a set of identities. The *loop variety* defined by E is the set of loops satisfying all identities in E.

e.g. The loop variety defined by the associative identity,

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z,$$

is the set of groups.

Varieties

Let E be a set of identities. The *loop variety* defined by E is the set of loops satisfying all identities in E.

e.g. The loop variety defined by the associative identity,

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z,$$

is the set of groups.

We call a variety *anti-associative* if the only group it contains is the trivial group.

Varieties

Let E be a set of identities. The *loop variety* defined by E is the set of loops satisfying all identities in E.

e.g. The loop variety defined by the associative identity,

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z,$$

is the set of groups.

We call a variety *anti-associative* if the only group it contains is the trivial group.

We call a loop variety *isotopically-closed* if it is closed under taking loop isotopes.

Varieties

Let E be a set of identities. The *loop variety* defined by E is the set of loops satisfying all identities in E.

e.g. The loop variety defined by the associative identity,

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z,$$

is the set of groups.

We call a variety *anti-associative* if the only group it contains is the trivial group.

We call a loop variety *isotopically-closed* if it is closed under taking loop isotopes.

Question: [Falconer'70] Does there exist a non-trivial, anti-associative, isotopically-closed loop variety?

Solving Falconer's problem

Recall

$$L_x : Q \to Q, \qquad L_x(z) = x \cdot z,$$
$$R_x : Q \to Q, \qquad R_x(z) = z \cdot x.$$

Solving Falconer's problem

Recall

$$L_x : Q \to Q, \qquad L_x(z) = x \cdot z,$$

$$R_x : Q \to Q, \qquad R_x(z) = z \cdot x.$$

Consider the variety defined by

$$(L_y \circ L_x^{-1})^p(z) = z, \tag{1}$$

$$(R_y \circ R_x^{-1})^{\mathrm{lcm}(1,2,\ldots,p-1)}(z) = z. \tag{2}$$

Solving Falconer's problem

Recall

$$L_x : Q \to Q, \quad L_x(z) = x \cdot z,$$

$$R_x : Q \to Q, \quad R_x(z) = z \cdot x.$$

Consider the variety defined by

$$(L_y \circ L_x^{-1})^p(z) = z, \tag{1}$$

$$(R_y \circ R_x^{-1})^{\mathrm{lcm}(1,2,\ldots,p-1)}(z) = z. \tag{2}$$

(1) $\leftrightarrow$ row-Hamiltonian $\leftrightarrow$ every element of every loop isotope has left order dividing p.

(2) $\leftrightarrow$ no column cycle a p-cycle $\leftrightarrow$ every element of every loop isotope has right order coprime to p.

Solving Falconer's problem

Recall

$$L_x : Q \to Q, \qquad L_x(z) = x \cdot z,$$

$$R_x : Q \to Q, \qquad R_x(z) = z \cdot x.$$

Consider the variety defined by

$$(L_y \circ L_x^{-1})^p(z) = z, \tag{1}$$

$$(R_y \circ R_x^{-1})^{\mathrm{lcm}(1,2,\ldots,p-1)}(z) = z. \tag{2}$$

(1) $\leftrightarrow$ row-Hamiltonian $\leftrightarrow$ every element of every loop isotope has left order dividing p.

(2) $\leftrightarrow$ no column cycle a p-cycle $\leftrightarrow$ every element of every loop isotope has right order coprime to p.

Theorem: There are infinitely many Falconer varieties.

Loose ends

Question: When is $Q_{a,b}$ isotopic to $Q_{c,d}$?

Loose ends

Question: When is $Q_{a,b}$ isotopic to $Q_{c,d}$?

Question: What is the asymptotic proportion of MNQ built via the nearfield construction?

Loose ends

Question: When is $Q_{a,b}$ isotopic to $Q_{c,d}$?

Question: What is the asymptotic proportion of MNQ built via the nearfield construction?

Question: Do there exist MNQs for all sufficiently large orders?

Loose ends

Question: When is $Q_{a,b}$ isotopic to $Q_{c,d}$?

Question: What is the asymptotic proportion of MNQ built via the nearfield construction?

Question: Do there exist MNQs for all sufficiently large orders?

Question: Do there exist atomic LS of orders that aren't prime powers?

Loose ends

Question: When is $Q_{a,b}$ isotopic to $Q_{c,d}$?

Question: What is the asymptotic proportion of MNQ built via the nearfield construction?

Question: Do there exist MNQs for all sufficiently large orders?

Question: Do there exist atomic LS of orders that aren't prime powers?

Question: Do there exist infinitely many atomic LS of composite order?

Loose ends

Question: When is $Q_{a,b}$ isotopic to $Q_{c,d}$?

Question: What is the asymptotic proportion of MNQ built via the nearfield construction?

Question: Do there exist MNQs for all sufficiently large orders?

Question: Do there exist atomic LS of orders that aren't prime powers?

Question: Do there exist infinitely many atomic LS of composite order?

Question: For which (a, b, n) do there exist quasigroups of order n in which every row cycle has length a and every column cycle has length b?

That's all. Any questions?

- J. Allsop and I. M. Wanless, Row-Hamiltonian Latin squares and Falconer varieties, arXiv:2211.13826.
- A. Drápal and I. M. Wanless, Isomorphisms of quadratic quasigroups, arXiv:2211.09472.
- A. Drápal and I. M. Wanless, On the number of quadratic orthomorphisms that produce maximally nonassociative quasigroups, *J. Aust. Math. Soc.*, to appear.
- A. Drápal and I. M. Wanless, Maximally nonassociative quasigroups via quadratic orthomorphisms, *Algebr. Comb.* **4** (2021), 501–515.