Automorphisms of Quadratic Quasigroups

Ian Wanless

Monash University

Joint work with Aleš Drápal, Charles University

The wikipedia theorem

https://en.wikipedia.org/wiki/Gordon_Royle

Evil sudoku with 17 initial values 00:59

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

Check my Sudoku

Evil sudoku with 17 initial values 01:00

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

Check my Sudoku

Orthomorphisms

Throughout $\mathbb{F}$ will be a finite field of odd order.

Orthomorphisms

Throughout $\mathbb{F}$ will be a finite field of odd order.

An *orthomorphism* of $\mathbb{F}$ is a permutation $\theta : \mathbb{F} \mapsto \mathbb{F}$ such that the map

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

is also a permutation of $\mathbb{F}$.

Orthomorphisms

Throughout $\mathbb{F}$ will be a finite field of odd order.

An *orthomorphism* of $\mathbb{F}$ is a permutation $\theta : \mathbb{F} \mapsto \mathbb{F}$ such that the map

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

is also a permutation of $\mathbb{F}$.

A *quadratic orthomorphism* is a map of the form

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

Orthomorphisms

Throughout $\mathbb{F}$ will be a finite field of odd order.

An *orthomorphism* of $\mathbb{F}$ is a permutation $\theta : \mathbb{F} \mapsto \mathbb{F}$ such that the map

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

is also a permutation of $\mathbb{F}$.

A *quadratic orthomorphism* is a map of the form

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

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

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

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

Orthomorphisms

Throughout $\mathbb{F}$ will be a finite field of odd order.

An *orthomorphism* of $\mathbb{F}$ is a permutation $\theta : \mathbb{F} \mapsto \mathbb{F}$ such that the map

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

is also a permutation of $\mathbb{F}$.

A *quadratic orthomorphism* is a map of the form

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

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

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

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

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

Applications of quadratic quasigroups

Quadratic quasigroups have been used to build

Applications of quadratic quasigroups

Quadratic quasigroups have been used to build

- large sets of mutually orthogonal Latin squares.

Applications of quadratic quasigroups

Quadratic quasigroups have been used to build

- large sets of mutually orthogonal Latin squares.
- atomic Latin squares (whose indivisible structure mimics that of the cyclic groups of prime order).

Applications of quadratic quasigroups

Quadratic quasigroups have been used to build

- large sets of mutually orthogonal Latin squares.
- atomic Latin squares (whose indivisible structure mimics that of the cyclic groups of prime order).
- perfect 1-factorisations of certain complete graphs and complete bipartite graphs.

Applications of quadratic quasigroups

Quadratic quasigroups have been used to build

- large sets of mutually orthogonal Latin squares.
- atomic Latin squares (whose indivisible structure mimics that of the cyclic groups of prime order).
- perfect 1-factorisations of certain complete graphs and complete bipartite graphs.
- anti-perfect 1-factorisations.

Applications of quadratic quasigroups

Quadratic quasigroups have been used to build

- large sets of mutually orthogonal Latin squares.
- atomic Latin squares (whose indivisible structure mimics that of the cyclic groups of prime order).
- perfect 1-factorisations of certain complete graphs and complete bipartite graphs.
- anti-perfect 1-factorisations.
- maximally non-associative quasigroups (where $x(yz) \neq (xy)z$ except when $x = y = z$).

Applications of quadratic quasigroups

Quadratic quasigroups have been used to build

- large sets of mutually orthogonal Latin squares.
- atomic Latin squares (whose indivisible structure mimics that of the cyclic groups of prime order).
- perfect 1-factorisations of certain complete graphs and complete bipartite graphs.
- anti-perfect 1-factorisations.
- maximally non-associative quasigroups (where $x(yz) \neq (xy)z$ except when $x = y = z$).
- Falconer varieties (non-trivial, anti-associative, isotopically-closed loop varieties)

Applications of quadratic quasigroups

Quadratic quasigroups have been used to build

- large sets of mutually orthogonal Latin squares.
- atomic Latin squares (whose indivisible structure mimics that of the cyclic groups of prime order).
- perfect 1-factorisations of certain complete graphs and complete bipartite graphs.
- anti-perfect 1-factorisations.
- maximally non-associative quasigroups (where $x(yz) \neq (xy)z$ except when $x = y = z$).
- Falconer varieties (non-trivial, anti-associative, isotopically-closed loop varieties)

Our results: Isomorphism

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

Our results: Isomorphism

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

The automorphism group

Let $\mathbb{K}$ be the least subfield of $\mathbb{F}$ that contains $\{a, b\}$.

The automorphism group

Let $\mathbb{K}$ be the least subfield of $\mathbb{F}$ that contains $\{a, b\}$.

Let $\mathrm{A}\Gamma^2\mathrm{L}_1(\mathbb{F}\,|\,\mathbb{K})$ be the group of all *affine semilinear mappings* $x \mapsto \lambda\alpha(x) + \mu$, where $\chi(\lambda) = 1$, $\mu \in \mathbb{F}$ and $\alpha \in \mathrm{aut}(\mathbb{F})$ fixes every element of $\mathbb{K}$ (in other words, $\alpha \in \mathrm{Gal}(\mathbb{F}\,|\,\mathbb{K})$).

The automorphism group

Let $\mathbb{K}$ be the least subfield of $\mathbb{F}$ that contains $\{a, b\}$.

Let $\mathrm{A}\Gamma^2\mathrm{L}_1(\mathbb{F}\,|\,\mathbb{K})$ be the group of all *affine semilinear mappings* $x \mapsto \lambda\alpha(x) + \mu$, where $\chi(\lambda) = 1$, $\mu \in \mathbb{F}$ and $\alpha \in \mathrm{aut}(\mathbb{F})$ fixes every element of $\mathbb{K}$ (in other words, $\alpha \in \mathrm{Gal}(\mathbb{F}\,|\,\mathbb{K})$).

Theorem: The automorphism group of $Q_{a,b}$ is $\mathrm{A}\Gamma^2\mathrm{L}_1(\mathbb{F}\,|\,\mathbb{K})$, up to these exceptions:

The automorphism group

Let $\mathbb{K}$ be the least subfield of $\mathbb{F}$ that contains $\{a, b\}$.

Let $\mathrm{A\Gamma^2L_1}(\mathbb{F} \,|\, \mathbb{K})$ be the group of all *affine semilinear mappings* $x \mapsto \lambda\alpha(x) + \mu$, where $\chi(\lambda) = 1$, $\mu \in \mathbb{F}$ and $\alpha \in \mathrm{aut}(\mathbb{F})$ fixes every element of $\mathbb{K}$ (in other words, $\alpha \in \mathrm{Gal}(\mathbb{F} \,|\, \mathbb{K})$).

Theorem: The automorphism group of $Q_{a,b}$ is $\mathrm{A\Gamma^2L_1}(\mathbb{F} \,|\, \mathbb{K})$, up to these exceptions:

(i) If $a = b$, then $\mathrm{aut}(Q_{a,b}) \cong \mathrm{AGL}_k(\mathbb{K})$, where $k = [\mathbb{F} : \mathbb{K}]$.
The automorphisms are all mappings $x \mapsto \sigma(x) + \mu$, where $\mu \in \mathbb{F}$ and $\sigma \colon \mathbb{F} \to \mathbb{F}$ is a $\mathbb{K}$-linear bijection.

The automorphism group

Let $\mathbb{K}$ be the least subfield of $\mathbb{F}$ that contains $\{a, b\}$.

Let $\mathrm{A}\Gamma^2\mathrm{L}_1(\mathbb{F} \,|\, \mathbb{K})$ be the group of all *affine semilinear mappings* $x \mapsto \lambda\alpha(x) + \mu$, where $\chi(\lambda) = 1$, $\mu \in \mathbb{F}$ and $\alpha \in \mathrm{aut}(\mathbb{F})$ fixes every element of $\mathbb{K}$ (in other words, $\alpha \in \mathrm{Gal}(\mathbb{F} \,|\, \mathbb{K})$).

Theorem: The automorphism group of $Q_{a,b}$ is $\mathrm{A}\Gamma^2\mathrm{L}_1(\mathbb{F} \,|\, \mathbb{K})$, up to these exceptions:

(i) If $a = b$, then $\mathrm{aut}(Q_{a,b}) \cong \mathrm{AGL}_k(\mathbb{K})$, where $k = [\mathbb{F} : \mathbb{K}]$.
The automorphisms are all mappings $x \mapsto \sigma(x) + \mu$, where $\mu \in \mathbb{F}$ and $\sigma\colon \mathbb{F} \to \mathbb{F}$ is a $\mathbb{K}$-linear bijection.

(ii) If there is an integer γ such that $b = a^\gamma$ and $\gamma^2 = |\mathbb{K}|$, then there are extra automorphisms of the form $x \mapsto \lambda\alpha(x^\gamma) + \mu$, where $\chi(\lambda) = -1$.

The automorphism group

Let $\mathbb{K}$ be the least subfield of $\mathbb{F}$ that contains $\{a, b\}$.

Let $\mathrm{A}\Gamma^2\mathrm{L}_1(\mathbb{F}\,|\,\mathbb{K})$ be the group of all *affine semilinear mappings* $x \mapsto \lambda\alpha(x) + \mu$, where $\chi(\lambda) = 1$, $\mu \in \mathbb{F}$ and $\alpha \in \mathrm{aut}(\mathbb{F})$ fixes every element of $\mathbb{K}$ (in other words, $\alpha \in \mathrm{Gal}(\mathbb{F}\,|\,\mathbb{K})$).

Theorem: The automorphism group of $Q_{a,b}$ is $\mathrm{A}\Gamma^2\mathrm{L}_1(\mathbb{F}\,|\,\mathbb{K})$, up to these exceptions:

(i) If $a = b$, then $\mathrm{aut}(Q_{a,b}) \cong \mathrm{AGL}_k(\mathbb{K})$, where $k = [\mathbb{F} : \mathbb{K}]$.
The automorphisms are all mappings $x \mapsto \sigma(x) + \mu$, where $\mu \in \mathbb{F}$ and $\sigma\colon \mathbb{F} \to \mathbb{F}$ is a $\mathbb{K}$-linear bijection.

(ii) If there is an integer γ such that $b = a^\gamma$ and $\gamma^2 = |\mathbb{K}|$, then there are extra automorphisms of the form $x \mapsto \lambda\alpha(x^\gamma) + \mu$, where $\chi(\lambda) = -1$.

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

Various varieties

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

(a) $Q_{a,b}$ is commutative iff $a + b = 1$ and either $|\mathbb{F}| \equiv 3 \bmod 4$ or $a = b$.

Various varieties

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

(a) $Q_{a,b}$ is commutative iff $a + b = 1$ and either $|\mathbb{F}| \equiv 3 \bmod 4$ or $a = b$.

(b) $Q_{a,b}$ is semisymmetric (i.e. fulfils the law $xy \cdot x = y$) iff $a^2 - a + 1 = 0$ and either $a = b$ or $a + b = 1$.

Various varieties

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

(a) $Q_{a,b}$ is commutative iff $a+b=1$ and either $|\mathbb{F}| \equiv 3 \bmod 4$ or $a=b$.

(b) $Q_{a,b}$ is semisymmetric (i.e. fulfils the law $xy \cdot x = y$) iff $a^2 - a + 1 = 0$ and either $a=b$ or $a+b=1$.

(c) $Q_{a,b}$ is a Steiner quasigroup (i.e. idempotent, commutative and semisymmetric)

Various varieties

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

(a) $Q_{a,b}$ is commutative iff $a+b=1$ and either $|\mathbb{F}| \equiv 3 \bmod 4$ or $a=b$.

(b) $Q_{a,b}$ is semisymmetric (i.e. fulfils the law $xy \cdot x = y$) iff $a^2-a+1=0$ and either $a=b$ or $a+b=1$.

(c) $Q_{a,b}$ is a Steiner quasigroup (i.e. idempotent, commutative and semisymmetric) iff either

- $\mathrm{char}(\mathbb{F}) = 3$ and $a=b=-1$, or

Various varieties

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

(a) $Q_{a,b}$ is commutative iff $a+b=1$ and either $|\mathbb{F}| \equiv 3 \bmod 4$ or $a=b$.

(b) $Q_{a,b}$ is semisymmetric (i.e. fulfils the law $xy \cdot x = y$) iff $a^2 - a + 1 = 0$ and either $a = b$ or $a + b = 1$.

(c) $Q_{a,b}$ is a Steiner quasigroup (i.e. idempotent, commutative and semisymmetric) iff either

- $\mathrm{char}(\mathbb{F}) = 3$ and $a = b = -1$, or
- $\mathrm{char}(\mathbb{F}) > 3$, $a \neq b$, $a + b = ab = 1$, and $\chi(a) = \chi(-1) = -1$.

Various varieties

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

(a) $Q_{a,b}$ is commutative iff $a+b=1$ and either $|\mathbb{F}| \equiv 3 \bmod 4$ or $a=b$.

(b) $Q_{a,b}$ is semisymmetric (i.e. fulfils the law $xy \cdot x = y$) iff $a^2-a+1=0$ and either $a=b$ or $a+b=1$.

(c) $Q_{a,b}$ is a Steiner quasigroup (i.e. idempotent, commutative and semisymmetric) iff either

- $\mathrm{char}(\mathbb{F})=3$ and $a=b=-1$, or
- $\mathrm{char}(\mathbb{F})>3$, $a \neq b$, $a+b=ab=1$, and $\chi(a)=\chi(-1)=-1$.

(d) $Q_{a,b}$ is isotopic to a group iff $a=b$.

Minimal subquasigroups

Minimal subquokkagroups

Minimal subquokkagroups

In Steiner quasigroups every pair of elements generates a (minimal) subquasigroup of order 3.

Minimal subquokkagroups

In Steiner quasigroups every pair of elements generates a (minimal) subquasigroup of order 3.

So suppose $Q_{a,b}$ is a quadratic quasigroup over $\mathbb{F}$ that is not Steiner. Let $\mathbb{K}$, $\mathbb{K}_0$ and $\mathbb{K}_1$ be the subfields of $\mathbb{F}$ generated by $\{a, b\}$, $\{a\}$ and $\{b\}$, respectively.

Minimal subquokkagroups

In Steiner quasigroups every pair of elements generates a (minimal) subquasigroup of order 3.

So suppose $Q_{a,b}$ is a quadratic quasigroup over $\mathbb{F}$ that is not Steiner. Let $\mathbb{K}$, $\mathbb{K}_0$ and $\mathbb{K}_1$ be the subfields of $\mathbb{F}$ generated by $\{a, b\}$, $\{a\}$ and $\{b\}$, respectively.

Theorem: Suppose that each subquasigroup of $Q_{a,b}$ that is generated by two distinct elements is minimal. There are two possibilities:

(i) $\mathbb{K}$ contains an element that is a nonsquare in $\mathbb{F}$, and $\mathbb{K} = \mathbb{K}_0 = \mathbb{K}_1$. The minimal subquasigroups of $Q_{a,b}$ are exactly the sets $\lambda\mathbb{K} + \mu$, where $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$.

(ii) All elements of $\mathbb{K}_0 \cup \mathbb{K}_1$ are squares in $\mathbb{F}$. If $\zeta \in \mathbb{F}$ is a nonsquare, then the minimal subquasigroups of $Q_{a,b}$ are exactly the sets $\lambda\zeta^i\mathbb{K}_i + \mu$, where $i \in \{0, 1\}$, $\lambda \in \mathbb{F}^*$ is a square, and $\mu \in \mathbb{F}$.

Minimal subquokkagroups

Theorem: Suppose there is a 2-generated subquasigroup of $Q_{a,b}$ that is *not* minimal.

Minimal subquokkagroups

Theorem: Suppose there is a 2-generated subquasigroup of $Q_{a,b}$ that is *not* minimal. Then all such subquasigroups are exactly the sets $\lambda\mathbb{K} + \mu$, where $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$.

Minimal subquokkagroups

Theorem: Suppose there is a 2-generated subquasigroup of $Q_{a,b}$ that is *not* minimal. Then all such subquasigroups are exactly the sets $\lambda\mathbb{K} + \mu$, where $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$. Furthermore, each of -1, a, b, $1 - a$ and $1 - b$ is a square in $\mathbb{F}$.

Minimal subquokkagroups

Theorem: Suppose there is a 2-generated subquasigroup of $Q_{a,b}$ that is *not* minimal. Then all such subquasigroups are exactly the sets $\lambda\mathbb{K} + \mu$, where $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$. Furthermore, each of -1, a, b, $1 - a$ and $1 - b$ is a square in $\mathbb{F}$. There are two possibilities:

Minimal subquokkagroups

Theorem: Suppose there is a 2-generated subquasigroup of $Q_{a,b}$ that is *not* minimal. Then all such subquasigroups are exactly the sets $\lambda\mathbb{K} + \mu$, where $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$. Furthermore, each of -1, a, b, $1 - a$ and $1 - b$ is a square in $\mathbb{F}$. There are two possibilities:

(i) $\mathbb{K}_1$ consists of squares only and $\mathbb{K}_0$ contains a nonsquare. In this case $\mathbb{K}$ is generated, as a subquasigroup, by $\{0, 1\}$. The minimal subquasigroups of $Q_{a,b}$ are exactly the sets $\zeta\mathbb{K}_1 + \mu$, where $\mu, \zeta \in \mathbb{F}$ and $\chi(\zeta) = -1$.

Minimal subquokkagroups

Theorem: Suppose there is a 2-generated subquasigroup of $Q_{a,b}$ that is *not* minimal. Then all such subquasigroups are exactly the sets $\lambda\mathbb{K} + \mu$, where $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$. Furthermore, each of -1, a, b, $1-a$ and $1-b$ is a square in $\mathbb{F}$. There are two possibilities:

(i) $\mathbb{K}_1$ consists of squares only and $\mathbb{K}_0$ contains a nonsquare. In this case $\mathbb{K}$ is generated, as a subquasigroup, by $\{0, 1\}$. The minimal subquasigroups of $Q_{a,b}$ are exactly the sets $\zeta\mathbb{K}_1 + \mu$, where $\mu, \zeta \in \mathbb{F}$ and $\chi(\zeta) = -1$.

(ii) $\mathbb{K}_0$ consists of squares only and $\mathbb{K}_1$ contains a nonsquare. In this case $\mathbb{K}$ is generated, as a subquasigroup, by $\{0, \zeta\}$ where $\zeta \in \mathbb{K}$ and $\chi(\zeta) = -1$. The minimal subquasigroups of $Q_{a,b}$ are exactly the sets $s\mathbb{K}_0 + \mu$, where $\mu, s \in \mathbb{F}$ and $\chi(s) = 1$.

The original application

Theorem: For odd prime powers q the asymptotic proportion of quadratic orthomorphisms which produce maximally non-associative quasigroups is

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

The original application

Theorem: For odd prime powers q the asymptotic proportion of quadratic orthomorphisms which produce maximally non-associative quasigroups is

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

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

The original application

Theorem: For odd prime powers q the asymptotic proportion of quadratic orthomorphisms which produce maximally non-associative quasigroups is

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

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

Thanks to our new theorem, we also know that (most) different choices give non-isomorphic results.

Future work

You could ask all the same questions for quasigroups built from cubic orthomorphisms, quartic orthomorphisms, etc.

Future work

You could ask all the same questions for quasigroups built from cubic orthomorphisms, quartic orthomorphisms, etc.

Future work

You could ask all the same questions for quasigroups built from cubic orthomorphisms, quartic orthomorphisms, etc.

A. Drápal and I. M. Wanless, Isomorphisms of quadratic quasigroups, to appear

Future work

You could ask all the same questions for quasigroups built from cubic orthomorphisms, quartic orthomorphisms, etc.

A. Drápal and I. M. Wanless, Isomorphisms of quadratic quasigroups, to appear (Proc Edinburgh Math. Soc.)

Future work

You could ask all the same questions for quasigroups built from cubic orthomorphisms, quartic orthomorphisms, etc.

A. Drápal and I. M. Wanless, Isomorphisms of quadratic quasigroups, to appear (Proc Edinburgh Math. Soc.)

`https://www.youtube.com/watch?v=ui3Kz8-Z0t0`

Future work

You could ask all the same questions for quasigroups built from cubic orthomorphisms, quartic orthomorphisms, etc.

A. Drápal and I. M. Wanless, Isomorphisms of quadratic quasigroups, to appear (Proc Edinburgh Math. Soc.)

`https://www.youtube.com/watch?v=ui3Kz8-Z0t0`

Happy $\sim 1^{\text{st}}$ birthday Gordon