Some Remarks on Isomorphism Testing

G. Eric Moorhouse

Department of Mathematics
University of Wyoming

RMAC Seminar—6 March 2015

Isomorphism Invariants

Let $\mathcal{C}$ be a category.

An *isomorphism invariant* on $\mathcal{C}$ is a map f taking objects $C \in \mathcal{C}$ to objects $f(C) \in \mathcal{D}$ (for some category $\mathcal{D}$) such that

$$C_1 \cong C_2 \Rightarrow f(C_1) \cong f(C_2).$$

f is a *complete isomorphism invariant* if

$$C_1 \cong C_2 \Leftrightarrow f(C_1) \cong f(C_2).$$

In order for f to be useful,

- f should be efficiently computable; and
- isomorphism should be more readily testable in $\mathcal{D}$ than in $\mathcal{C}$.

The map f is not usually functorial. But…

Isomorphism Invariants

Let $\mathcal{C}$ be a category.

An *isomorphism invariant* on $\mathcal{C}$ is a map f taking objects $C \in \mathcal{C}$ to objects $f(C) \in \mathcal{D}$ (for some category $\mathcal{D}$) such that

$$C_1 \cong C_2 \;\Rightarrow\; f(C_1) \cong f(C_2).$$

f is a *complete isomorphism invariant* if

$$C_1 \cong C_2 \;\Leftrightarrow\; f(C_1) \cong f(C_2).$$

In order for f to be useful,

- f should be efficiently computable; and
- isomorphism should be more readily testable in $\mathcal{D}$ than in $\mathcal{C}$.

The map f is not usually functorial. But…

Isomorphism Invariants

Let $\mathcal{C}$ be a category.

An *isomorphism invariant* on $\mathcal{C}$ is a map f taking objects $C \in \mathcal{C}$ to objects $f(C) \in \mathcal{D}$ (for some category $\mathcal{D}$) such that

$$C_1 \cong C_2 \;\Rightarrow\; f(C_1) \cong f(C_2).$$

f is a *complete isomorphism invariant* if

$$C_1 \cong C_2 \;\Leftrightarrow\; f(C_1) \cong f(C_2).$$

In order for f to be useful,

- f should be efficiently computable; and
- isomorphism should be more readily testable in $\mathcal{D}$ than in $\mathcal{C}$.

The map f is not usually functorial. But…

Isomorphism Invariants

Let $\mathcal{C}$ be a category.

An *isomorphism invariant* on $\mathcal{C}$ is a map f taking objects $C \in \mathcal{C}$ to objects $f(C) \in \mathcal{D}$ (for some category $\mathcal{D}$) such that

$$C_1 \cong C_2 \;\Rightarrow\; f(C_1) \cong f(C_2).$$

f is a *complete isomorphism invariant* if

$$C_1 \cong C_2 \;\Leftrightarrow\; f(C_1) \cong f(C_2).$$

In order for f to be useful,

- f should be efficiently computable; and
- isomorphism should be more readily testable in $\mathcal{D}$ than in $\mathcal{C}$.

The map f is not usually functorial. But. . .

A *loop* is a set L with a binary operation satisfying

- There exists $1 \in L$ satisfying $1x = x1 = x$ for all $x \in L$; and
- For all $a \in L$, both of the maps $x \mapsto ax$ and $x \mapsto xa$ are bijective on L.

Bol identity $((xy)z)y = x((yz)y)$ $\Rightarrow$ *Moufang identity* $x(y(zy)) = ((xy)z)y$ $\Rightarrow$ *associativity* $(xy)z = x(yz)$ (group)

Loops

A *loop* is a set L with a binary operation satisfying

- There exists $1 \in L$ satisfying $1x = x1 = x$ for all $x \in L$; and
- For all $a \in L$, both of the maps $x \mapsto ax$ and $x \mapsto xa$ are bijective on L.

Bol identity $((xy)z)y = x((yz)y)$ $\Rightarrow$ *Moufang identity* $x(y(zy)) = ((xy)z)y$ $\Rightarrow$ *associativity* $(xy)z = x(yz)$ *(group)*

Loops

Classification of Bol loops of small order:

n	# groups	# proper Moufang loops	# proper Bol loops	total # Bol loops
8	5	0	6	11
12	5	1	3	8
15	1	0	2	3
16	14	5	2038*	2052*

All Bol loops of orders $n \leqslant 16$ not appearing in this table are associative (i.e. groups).

(*) Classification of Bol loops of order 16 due to M. (2002).

Loops

Given a loop $L = \{g_1{=}1,\ g_2,\ g_3,\ \dots\ , g_n\}$, define a graph $\Gamma(L)$ having $n^2 + 3n$ vertices

$$\textbf{Cell}_{ij},\ \textbf{Row}_i,\ \textbf{Col}_j,\ \textbf{Entry}_k \quad (i, j, k = 1, 2, \dots, n)$$

where vertex $\textbf{Cell}_{ij}$ is joined to vertices $\textbf{Row}_i$, $\textbf{Col}_j$, $\textbf{Entry}_k$ whenever $g_i g_j = g_k$.

Regard $\Gamma(L)$ as a graph with 4 colours of vertices; and graph morphisms are required to preserve the vertex colouring. Then $\Gamma(L)$ is a complete isomorphism invariant of L.

Better yet, add three more colours: one each for $\textbf{Row}_1$, $\textbf{Col}_1$, $\textbf{Entry}_1$.

Even better:

Loops

Given a loop $L = \{g_1{=}1,\ g_2,\ g_3,\ \ldots\ ,g_n\}$, define a graph $\Gamma(L)$ having $n^2 + 3n$ vertices

$$\textbf{Cell}_{ij},\ \textbf{Row}_i,\ \textbf{Col}_j,\ \textbf{Entry}_k \quad (i, j, k = 1, 2, \ldots, n)$$

where vertex $\textbf{Cell}_{ij}$ is joined to vertices $\textbf{Row}_i$, $\textbf{Col}_j$, $\textbf{Entry}_k$ whenever $g_i g_j = g_k$.

Regard $\Gamma(L)$ as a graph with 4 colours of vertices; and graph morphisms are required to preserve the vertex colouring. Then $\Gamma(L)$ is a complete isomorphism invariant of L.

Better yet, add three more colours: one each for $\textbf{Row}_1$, $\textbf{Col}_1$, $\textbf{Entry}_1$.

Even better:

Loops

Given a loop $L = \{g_1{=}1,\ g_2,\ g_3,\ \ldots\ ,g_n\}$, define a graph $\Gamma(L)$ having $n^2 + 3n$ vertices

$$\mathbf{Cell}_{ij},\ \mathbf{Row}_i,\ \mathbf{Col}_j,\ \mathbf{Entry}_k \quad (i, j, k = 1, 2, \ldots, n)$$

where vertex $\mathbf{Cell}_{ij}$ is joined to vertices $\mathbf{Row}_i$, $\mathbf{Col}_j$, $\mathbf{Entry}_k$ whenever $g_i g_j = g_k$.

Regard $\Gamma(L)$ as a graph with 4 colours of vertices; and graph morphisms are required to preserve the vertex colouring. Then $\Gamma(L)$ is a complete isomorphism invariant of L.

Better yet, add three more colours: one each for $\mathbf{Row}_1$, $\mathbf{Col}_1$, $\mathbf{Entry}_1$.

Even better:

Loops

Use two shades of red for **Row**$_i$, according as row i is an even or odd permutation of L, i.e. according to the parity of the permutation $g \mapsto g_i g$.

Use two shades of green for **Col**$_j$, according as column j is an even or odd permutation of L, i.e. according to the parity of the permutation $g \mapsto g g_j$.

Use two shades of brown for **Entry**$_k$, according to the parity of permutation $x \mapsto y$ defined by $xy = g_k$.

Now $\Gamma(L)$ is a complete isomorphism invariant, taken to be in the category of 10-coloured graphs.

Loops

Use two shades of red for **Row**$_i$, according as row i is an even or odd permutation of L, i.e. according to the parity of the permutation $g \mapsto g_i g$.

Use two shades of green for **Col**$_j$, according as column j is an even or odd permutation of L, i.e. according to the parity of the permutation $g \mapsto g g_j$.

Use two shades of brown for **Entry**$_k$, according to the parity of permutation $x \mapsto y$ defined by $xy = g_k$.

Now $\Gamma(L)$ is a complete isomorphism invariant, taken to be in the category of 10-coloured graphs.

Loops

Use two shades of red for **Row**$_i$, according as row i is an even or odd permutation of L, i.e. according to the parity of the permutation $g \mapsto g_i g$.

Use two shades of green for **Col**$_j$, according as column j is an even or odd permutation of L, i.e. according to the parity of the permutation $g \mapsto g g_j$.

Use two shades of brown for **Entry**$_k$, according to the parity of permutation $x \mapsto y$ defined by $xy = g_k$.

Now $\Gamma(L)$ is a complete isomorphism invariant, taken to be in the category of 10-coloured graphs.

Loops

Use two shades of red for $\textbf{Row}_i$, according as row i is an even or odd permutation of L, i.e. according to the parity of the permutation $g \mapsto g_i g$.

Use two shades of green for $\textbf{Col}_j$, according as column j is an even or odd permutation of L, i.e. according to the parity of the permutation $g \mapsto g g_j$.

Use two shades of brown for $\textbf{Entry}_k$, according to the parity of permutation $x \mapsto y$ defined by $xy = g_k$.

Now $\Gamma(L)$ is a complete isomorphism invariant, taken to be in the category of 10-coloured graphs.

Two-Graphs and Skew Two-Graphs

Let X be a set, and $\binom{X}{k}$ the collection of all k-subsets of X.

A *two-graph on X* is a subset $\Delta \subseteq \binom{X}{3}$ such that every 4-subset $S \subseteq X$ contains an even number (i.e. 0, 2 or 4) triples in Δ.

The *degree* of a pair $\{x, y\} \in \binom{X}{2}$ is the number of triples in Δ containing $\{x, y\}$. The *degree sequence* of Δ is the multiset of degrees of pairs in X. It is an isomorphism invariant of Δ.

Let $\mathrm{Alt}_3 X$ the collection of all 3-cycles of X. A *skew two-graph on X* is a subset $\nabla \subseteq \mathrm{Alt}_3 X$ such that for every 4-subset $\{x,y,z,w\} \subseteq X$, an even number (i.e. 0, 2 or 4) of the 3-cycles

$$(xyz), (xzw), (xwy), (ywz)$$

are in ∇.

Two-Graphs and Skew Two-Graphs

Let X be a set, and $\binom{X}{k}$ the collection of all k-subsets of X.

A *two-graph on X* is a subset $\Delta \subseteq \binom{X}{3}$ such that every 4-subset $S \subseteq X$ contains an even number (i.e. 0, 2 or 4) triples in Δ.

The *degree* of a pair $\{x, y\} \in \binom{X}{2}$ is the number of triples in Δ containing $\{x, y\}$. The *degree sequence* of Δ is the multiset of degrees of pairs in X. It is an isomorphism invariant of Δ.

Let $\mathrm{Alt}_3\, X$ the collection of all 3-cycles of X. A *skew two-graph on X* is a subset $\nabla \subseteq \mathrm{Alt}_3\, X$ such that for every 4-subset $\{x,y,z,w\} \subseteq X$, an even number (i.e. 0, 2 or 4) of the 3-cycles

$$(xyz),\ (xzw),\ (xwy),\ (ywz)$$

are in ∇.

Two-Graphs and Skew Two-Graphs

Let X be a set, and $\binom{X}{k}$ the collection of all k-subsets of X.

A *two-graph on X* is a subset $\Delta \subseteq \binom{X}{3}$ such that every 4-subset $S \subseteq X$ contains an even number (i.e. 0, 2 or 4) triples in Δ.

The *degree* of a pair $\{x, y\} \in \binom{X}{2}$ is the number of triples in Δ containing $\{x, y\}$. The *degree sequence* of Δ is the multiset of degrees of pairs in X. It is an isomorphism invariant of Δ.

Let $\mathrm{Alt}_3\, X$ the collection of all 3-cycles of X. A *skew two-graph on X* is a subset $\nabla \subseteq \mathrm{Alt}_3\, X$ such that for every 4-subset $\{x,y,z,w\} \subseteq X$, an even number (i.e. 0, 2 or 4) of the 3-cycles

$$(xyz), (xzw), (xwy), (ywz)$$

are in ∇.

Let X be a set, and $\binom{X}{k}$ the collection of all k-subsets of X.

A *two-graph on X* is a subset $\Delta \subseteq \binom{X}{3}$ such that every 4-subset $S \subseteq X$ contains an even number (i.e. 0, 2 or 4) triples in Δ.

The *degree* of a pair $\{x, y\} \in \binom{X}{2}$ is the number of triples in Δ containing $\{x, y\}$. The *degree sequence* of Δ is the multiset of degrees of pairs in X. It is an isomorphism invariant of Δ.

Let $\mathrm{Alt}_3 X$ the collection of all 3-cycles of X. A *skew two-graph on X* is a subset $\nabla \subseteq \mathrm{Alt}_3 X$ such that for every 4-subset $\{x,y,z,w\} \subseteq X$, an even number (i.e. 0, 2 or 4) of the 3-cycles

$$(xyz),\ (xzw),\ (xwy),\ (ywz)$$

are in ∇.

Two-Graphs and Skew Two-Graphs

Let X be a set, and $\binom{X}{k}$ the collection of all k-subsets of X.

A *two-graph on X* is a subset $\Delta \subseteq \binom{X}{3}$ such that every 4-subset $S \subseteq X$ contains an even number (i.e. 0, 2 or 4) triples in Δ.

The *degree* of a pair $\{x, y\} \in \binom{X}{2}$ is the number of triples in Δ containing $\{x, y\}$. The *degree sequence* of Δ is the multiset of degrees of pairs in X. It is an isomorphism invariant of Δ.

Let $\mathrm{Alt}_3\, X$ the collection of all 3-cycles of X. A *skew two-graph on X* is a subset $\nabla \subseteq \mathrm{Alt}_3\, X$ such that for every 4-subset $\{x,y,z,w\} \subseteq X$, an even number (i.e. 0, 2 or 4) of the 3-cycles

$$(xyz),\ (xzw),\ (xwy),\ (ywz)$$

are in ∇.

Two-Graphs and Skew Two-Graphs

Let X be a set, and $\binom{X}{k}$ the collection of all k-subsets of X.

A *two-graph on X* is a subset $\Delta \subseteq \binom{X}{3}$ such that every 4-subset $S \subseteq X$ contains an even number (i.e. 0, 2 or 4) triples in Δ.

The *degree* of a pair $\{x, y\} \in \binom{X}{2}$ is the number of triples in Δ containing $\{x, y\}$. The *degree sequence* of Δ is the multiset of degrees of pairs in X. It is an isomorphism invariant of Δ.

Let $\mathrm{Alt}_3\, X$ the collection of all 3-cycles of X. A *skew two-graph on X* is a subset $\nabla \subseteq \mathrm{Alt}_3\, X$ such that for every 4-subset $\{x,y,z,w\} \subseteq X$, an even number (i.e. 0, 2 or 4) of the 3-cycles

$$(xyz),\ (xzw),\ (xwy),\ (ywz)$$

are in ∇.

Two-Graphs and Skew Two-Graphs

Let X be a set, and $\binom{X}{k}$ the collection of all k-subsets of X.

A *two-graph on X* is a subset $\Delta \subseteq \binom{X}{3}$ such that every 4-subset $S \subseteq X$ contains an even number (i.e. 0, 2 or 4) triples in Δ.

The *degree* of a pair $\{x, y\} \in \binom{X}{2}$ is the number of triples in Δ containing $\{x, y\}$. The *degree sequence* of Δ is the multiset of degrees of pairs in X. It is an isomorphism invariant of Δ.

Let $\mathrm{Alt}_3 X$ the collection of all 3-cycles of X. A *skew two-graph on X* is a subset $\nabla \subseteq \mathrm{Alt}_3 X$ such that for every 4-subset $\{x,y,z,w\} \subseteq X$, an even number (i.e. 0, 2 or 4) of the 3-cycles

$$(xyz),\ (xzw),\ (xwy),\ (ywz)$$

are in ∇.

Spread Sets/Translation Planes

A *spread set in $GL_n(q)$* is a set of q^n+1 matrices

$$\Sigma = \{M_0, M_1, M_2, \ldots, M_{q^n}\}$$

such that $M_i - M_j$ is invertible whenever $i \neq j$.

If $q^n \equiv 1 \mod 4$, then Σ yields an invariant two-graph $\Delta(\Sigma)$ on $\{0, 1, 2, \ldots, q^n\}$ consisting of those triples $\{i, j, k\}$ such that

$$\det((M_i - M_j)(M_j - M_k)(M_k - M_i)) \text{ is a square in } \mathbb{F}_q.$$

The degree sequence of $\Delta(\Sigma)$ is an isomorphism invariant of the translation plane associated to Σ. It is the best practical isomorphism invariant known for spreads; but it does not easily adapt to general theoretical results.

Spread Sets/Translation Planes

A *spread set in $GL_n(q)$* is a set of q^n+1 matrices

$$\Sigma = \{M_0, M_1, M_2, \ldots, M_{q^n}\}$$

such that $M_i - M_j$ is invertible whenever $i \neq j$.

If $q^n \equiv 1 \mod 4$, then Σ yields an invariant two-graph $\Delta(\Sigma)$ on $\{0, 1, 2, \ldots, q^n\}$ consisting of those triples $\{i, j, k\}$ such that

$$\det\big((M_i - M_j)(M_j - M_k)(M_k - M_i)\big) \text{ is a square in } \mathbb{F}_q.$$

The degree sequence of $\Delta(\Sigma)$ is an isomorphism invariant of the translation plane associated to Σ. It is the best practical isomorphism invariant known for spreads; but it does not easily adapt to general theoretical results.

Spread Sets/Translation Planes

A *spread set in $GL_n(q)$* is a set of q^n+1 matrices

$$\Sigma = \{M_0, M_1, M_2, \ldots, M_{q^n}\}$$

such that $M_i - M_j$ is invertible whenever $i \neq j$.

If $q^n \equiv 1 \mod 4$, then Σ yields an invariant two-graph $\Delta(\Sigma)$ on $\{0, 1, 2, \ldots, q^n\}$ consisting of those triples $\{i, j, k\}$ such that

$$\det\big((M_i - M_j)(M_j - M_k)(M_k - M_i)\big) \text{ is a square in } \mathbb{F}_q.$$

The degree sequence of $\Delta(\Sigma)$ is an isomorphism invariant of the translation plane associated to Σ. It is the best practical isomorphism invariant known for spreads; but it does not easily adapt to general theoretical results.

A *spread set in $GL_n(q)$* is a set of q^n+1 matrices

$$\Sigma = \{M_0, M_1, M_2, \ldots, M_{q^n}\}$$

such that $M_i - M_j$ is invertible whenever $i \neq j$.

If $q^n \equiv 3 \mod 4$, then Σ yields an invariant skew two-graph $\nabla(\Sigma)$ consisting of those 3-cycles $(i\,j\,k)$ such that

$$\det\big((M_i - M_j)(M_j - M_k)(M_k - M_i)\big) \text{ is a square in } \mathbb{F}_q.$$

This is an isomorphism invariant of the associated translation plane; but a less useful one.

There exist non-isomorphic (and non-polar) translation planes with the same skew two-graph. Moreover, no information about $\nabla(\Sigma)$ is provided by degree sequences.

Spread Sets/Translation Planes

A *spread set in $GL_n(q)$* is a set of q^n+1 matrices

$$\Sigma = \{M_0, M_1, M_2, \ldots, M_{q^n}\}$$

such that $M_i - M_j$ is invertible whenever $i \neq j$.

If $q^n \equiv 3 \mod 4$, then Σ yields an invariant skew two-graph $\nabla(\Sigma)$ consisting of those 3-cycles $(i\,j\,k)$ such that

$$\det\big((M_i - M_j)(M_j - M_k)(M_k - M_i)\big) \text{ is a square in } \mathbb{F}_q.$$

This is an isomorphism invariant of the associated translation plane; but a less useful one.

There exist non-isomorphic (and non-polar) translation planes with the same skew two-graph. Moreover, no information about $\nabla(\Sigma)$ is provided by degree sequences.

Spread Sets/Translation Planes

A *spread set in $GL_n(q)$* is a set of q^n+1 matrices

$$\Sigma = \{M_0, M_1, M_2, \ldots, M_{q^n}\}$$

such that $M_i - M_j$ is invertible whenever $i \neq j$.

If $q^n \equiv 3 \mod 4$, then Σ yields an invariant skew two-graph $\nabla(\Sigma)$ consisting of those 3-cycles $(i\,j\,k)$ such that

$$\det\big((M_i - M_j)(M_j - M_k)(M_k - M_i)\big) \text{ is a square in } \mathbb{F}_q.$$

This is an isomorphism invariant of the associated translation plane; but a less useful one.

There exist non-isomorphic (and non-polar) translation planes with the same skew two-graph. Moreover, no information about $\nabla(\Sigma)$ is provided by degree sequences.

A *spread set in $GL_n(q)$* is a set of q^n+1 matrices

$$\Sigma = \{M_0, M_1, M_2, \dots, M_{q^n}\}$$

such that $M_i - M_j$ is invertible whenever $i \neq j$.

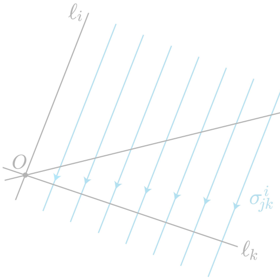
If $q^n \equiv 3 \mod 4$, then Σ yields an invariant skew two-graph $\nabla(\Sigma)$ consisting of those 3-cycles $(i\,j\,k)$ such that

$$\det\big((M_i - M_j)(M_j - M_k)(M_k - M_i)\big) \text{ is a square in } \mathbb{F}_q.$$

This is an isomorphism invariant of the associated translation plane; but a less useful one.

There exist non-isomorphic (and non-polar) translation planes with the same skew two-graph. Moreover, no information about $\nabla(\Sigma)$ is provided by degree sequences.

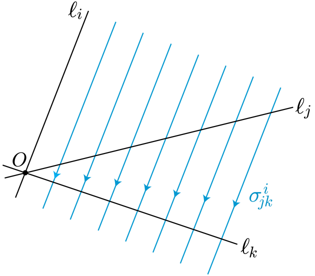
Let $\mathcal{A}$ be an *affine plane of order $n \geqslant 2$*, with a distinguished point O. We describe an invariant of the pair $(\mathcal{A}, O)$. (This may be adapted to an invariant of $\mathcal{A}$ or of a projective plane.)



Let $\ell_0, \ell_1, \ell_2, \ldots, \ell_n$ be the lines through O. Lines parallel to ℓ_i define a bijection on points $\sigma^i_{jk} : \ell_j \to \ell_k$. We obtain a two-graph $\Delta(\mathcal{A}, O)$ on $\{0, 1, 2, \ldots, n\}$ consisting of those triples $\{i, j, k\}$ such that the permutation $\sigma^j_{ki} \circ \sigma^i_{jk} \circ \sigma^k_{ij} \in Sym\,\ell_i$ is odd.

Affine Planes (Conway's invariant)

Let $\mathcal{A}$ be an *affine plane of order $n \geqslant 2$*, with a distinguished point O. We describe an invariant of the pair $(\mathcal{A}, O)$. (This may be adapted to an invariant of $\mathcal{A}$ or of a projective plane.)



Let $\ell_0, \ell_1, \ell_2, \ldots, \ell_n$ be the lines through O. Lines parallel to ℓ_i define a bijection on points $\sigma^i_{jk} : \ell_j \to \ell_k$. We obtain a two-graph $\Delta(\mathcal{A}, O)$ on $\{0, 1, 2, \ldots, n\}$ consisting of those triples $\{i, j, k\}$ such that the permutation $\sigma^j_{ki} \circ \sigma^i_{jk} \circ \sigma^k_{ij} \in Sym\,\ell_i$ is odd.

Ovoids

Consider a finite orthogonal space of type $O_{2n}^{+}(q)$ with associated bilinear form B. An *ovoid* is a set $\mathcal{O}$ consisting of $q^{n-1}+1$ singular points, no two of which are perpendicular with respect to B.

Assume q is odd. The triples of points $\langle u\rangle$, $\langle v\rangle$, $\langle w\rangle$ in $\mathcal{O}$ such that

$$B(u,v)B(v,w)B(w,u) \text{ is a square in } \mathbb{F}_q$$

form an invariant two-graph $\Delta(\mathcal{O})$.

In $O_6^{+}(q)$, $\Delta(\mathcal{O})$ coincides with the invariant of the spread set in $GL_2(q)$ associated to $\mathcal{O}$ by the Klein correspondence.

Ovoids

Consider a finite orthogonal space of type $O^+_{2n}(q)$ with associated bilinear form B. An *ovoid* is a set $\mathcal{O}$ consisting of $q^{n-1}+1$ singular points, no two of which are perpendicular with respect to B.

Assume q is odd. The triples of points $\langle u\rangle$, $\langle v\rangle$, $\langle w\rangle$ in $\mathcal{O}$ such that

$$B(u,v)B(v,w)B(w,u) \text{ is a square in } \mathbb{F}_q$$

form an invariant two-graph $\Delta(\mathcal{O})$.

In $O^+_6(q)$, $\Delta(\mathcal{O})$ coincides with the invariant of the spread set in $GL_2(q)$ associated to $\mathcal{O}$ by the Klein correspondence.

Ovoids

Consider a finite orthogonal space of type $O_{2n}^{+}(q)$ with associated bilinear form B. An *ovoid* is a set $\mathcal{O}$ consisting of $q^{n-1}+1$ singular points, no two of which are perpendicular with respect to B.

Assume q is odd. The triples of points $\langle u\rangle$, $\langle v\rangle$, $\langle w\rangle$ in $\mathcal{O}$ such that

$$B(u,v)B(v,w)B(w,u) \text{ is a square in } \mathbb{F}_q$$

form an invariant two-graph $\Delta(\mathcal{O})$.

In $O_6^{+}(q)$, $\Delta(\mathcal{O})$ coincides with the invariant of the spread set in $GL_2(q)$ associated to $\mathcal{O}$ by the Klein correspondence.

Ovoids

The invariant $\Delta(\mathcal{O})$, or its degree sequence, is the best available invariant for ovoids. It is extremely effective at distinguishing nonisomorphic ovoids, or finding explicit isomorphisms when there is one. But:

Conway, Kleidman and Wilson (1988) showed that there is at least one ovoid in $O_8^+(p)$ for every prime p.

M. (1993) found additional families of ovoids in $O_8^+(p)$ the number of which seems to $\to \infty$ as $p \to \infty$. This is an open question which our invariants seem unsuited to resolve.

Ovoids

The invariant $\Delta(\mathcal{O})$, or its degree sequence, is the best available invariant for ovoids. It is extremely effective at distinguishing nonisomorphic ovoids, or finding explicit isomorphisms when there is one. But:

Conway, Kleidman and Wilson (1988) showed that there is at least one ovoid in $O_8^+(p)$ for every prime p.

M. (1993) found additional families of ovoids in $O_8^+(p)$ the number of which seems to $\to \infty$ as $p \to \infty$. This is an open question which our invariants seem unsuited to resolve.

Ovoids

The invariant $\Delta(\mathcal{O})$, or its degree sequence, is the best available invariant for ovoids. It is extremely effective at distinguishing nonisomorphic ovoids, or finding explicit isomorphisms when there is one. But:

Conway, Kleidman and Wilson (1988) showed that there is at least one ovoid in $O_8^+(p)$ for every prime p.

M. (1993) found additional families of ovoids in $O_8^+(p)$ the number of which seems to $\to \infty$ as $p \to \infty$. This is an open question which our invariants seem unsuited to resolve.

Skew Hadamard Matrices

A *Hadamard matrix of order n* is an $n \times n$ matrix H with entries ± 1 satisfying $HH^T = nI$. Hadamard matrices H_1, H_2 are *equivalent* if $MH_1N = H_2$ for some ± 1-monomial matrices M, N.

Ding and Yuan (2006) constructed a family of difference sets in the additive group of $\mathbb{F}_q$, $q = 3^{2r+1}$ given by

$$\mathcal{D} = \{x^{10} - x^6 - x^2 \; : \; 0 \neq x \in \mathbb{F}_q\}$$

resulting in a family of skew Hadamard matrices of order $q+1$ given by $H = \left[h_{xy}\right]_{x,y \in \mathbb{F}_q \cup \{\infty\}}$ where

$$h_{xy} = \begin{cases} 1, & \text{if } x = y; \\ 1, & \text{if } x = \infty \neq y \;\text{ or }\; x \in y + \mathcal{D}; \\ -1, & \text{if } x \neq \infty = y \;\text{ or }\; y \in x + \mathcal{D}. \end{cases}$$

Skew Hadamard Matrices

A *Hadamard matrix of order n* is an $n \times n$ matrix H with entries ± 1 satisfying $HH^T = nI$. Hadamard matrices H_1, H_2 are *equivalent* if $MH_1N = H_2$ for some ± 1-monomial matrices M, N.

Ding and Yuan (2006) constructed a family of difference sets in the additive group of $\mathbb{F}_q$, $q = 3^{2r+1}$ given by

$$\mathcal{D} = \{x^{10} - x^6 - x^2 \,:\, 0 \neq x \in \mathbb{F}_q\}$$

resulting in a family of skew Hadamard matrices of order $q + 1$ given by $H = \left[h_{xy}\right]_{x,y \in \mathbb{F}_q \cup \{\infty\}}$ where

$$h_{xy} = \begin{cases} 1, & \text{if } x = y; \\ 1, & \text{if } x = \infty \neq y \;\text{ or }\; x \in y + \mathcal{D}; \\ -1, & \text{if } x \neq \infty = y \;\text{ or }\; y \in x + \mathcal{D}. \end{cases}$$

Skew Hadamard Matrices

Ding, Wang and Xiang (2007) constructed another infinite family of skew Hadamard matrices of the same order $q+1$, $q = 3^{2r+1}$ from the difference sets

$$\widetilde{\mathcal{D}} = \{x^{2\sigma+3} + \varepsilon x^{\sigma} - x \,:\, 0 \neq x \in \mathbb{F}_q\}\,,\ \sigma = 3^{r+1},\ \varepsilon = \pm 1.$$

Conjecturally, the resulting skew Hadamard matrices $\widetilde{H}$ coincide with the Ding-Yuan construction only for $q = 3$.

Ding, Wang and Xiang (2007) constructed another infinite family of skew Hadamard matrices of the same order $q+1$, $q=3^{2r+1}$ from the difference sets

$$\widetilde{\mathcal{D}} = \{x^{2\sigma+3} + \varepsilon x^{\sigma} - x \,:\, 0 \neq x \in \mathbb{F}_q\}\,,\ \sigma = 3^{r+1},\ \varepsilon = \pm 1.$$

Conjecturally, the resulting skew Hadamard matrices $\widetilde{H}$ coincide with the Ding-Yuan construction only for $q=3$.

DRGs Related to Generalized Preparata Codes

Let $q = 2^{2t-1}$, $\sigma = 2^e$ where $\gcd(e, 2t-1) = 1$. Consider the graph $\Gamma_{q,\sigma}$ with vertex set $\mathbb{F}_q \times \mathbb{F}_2 \times \mathbb{F}_q$ and adjacency

$$(a, i, \alpha) \sim (b, j, \beta) \;\Leftrightarrow\; \alpha + \beta = a^\sigma b + ab^\sigma + (i+j)(a^{\sigma+1} + b^{\sigma+1}).$$

Theorem (de Caen, Mathon, M. (1995))

(a) $\Gamma_{q,\sigma}$ is an antipodal distance regular graph of diameter 3, a q-fold cover of K_{2q} via $(a, i, \alpha) \mapsto (a, i)$.

(b) $\Gamma_{q,\sigma} \cong \Gamma_{q,\sigma'} \Leftrightarrow \sigma' = \sigma^{\pm 1}$, resulting in $\frac{1}{2}\phi(2t-1)$ nonisomorphic such covers.

The full automorphism group of $\Gamma_{q,\sigma}$ is determined, together with the nonisomorphism result (b), by using walks on the graph $\Gamma_{q,\sigma}$ to construct binary codes; then showing that these are generalized Preparata codes; and finally using Kantor's determination of automorphisms/isomorphisms of generalized Preparata codes (1983).

DRGs Related to Generalized Preparata Codes

Let $q = 2^{2t-1}$, $\sigma = 2^e$ where $\gcd(e, 2t-1) = 1$. Consider the graph $\Gamma_{q,\sigma}$ with vertex set $\mathbb{F}_q \times \mathbb{F}_2 \times \mathbb{F}_q$ and adjacency

$$(a, i, \alpha) \sim (b, j, \beta) \;\Leftrightarrow\; \alpha + \beta = a^\sigma b + ab^\sigma + (i+j)(a^{\sigma+1}+b^{\sigma+1}).$$

Theorem (de Caen, Mathon, M. (1995))

(a) $\Gamma_{q,\sigma}$ *is an antipodal distance regular graph of diameter 3, a q-fold cover of* K_{2q} *via* $(a, i, \alpha) \mapsto (a, i)$.

(b) $\Gamma_{q,\sigma} \cong \Gamma_{q,\sigma'} \Leftrightarrow \sigma' = \sigma^{\pm 1}$, *resulting in* $\frac{1}{2}\phi(2t-1)$ *nonisomorphic such covers.*

The full automorphism group of $\Gamma_{q,\sigma}$ is determined, together with the nonisomorphism result (b), by using walks on the graph $\Gamma_{q,\sigma}$ to construct binary codes; then showing that these are generalized Preparata codes; and finally using Kantor's determination of automorphisms/isomorphisms of generalized Preparata codes (1983).

DRGs Related to Generalized Preparata Codes

Let $q = 2^{2t-1}$, $\sigma = 2^e$ where $\gcd(e, 2t-1) = 1$. Consider the graph $\Gamma_{q,\sigma}$ with vertex set $\mathbb{F}_q \times \mathbb{F}_2 \times \mathbb{F}_q$ and adjacency

$$(a, i, \alpha) \sim (b, j, \beta) \ \Leftrightarrow \ \alpha + \beta = a^\sigma b + ab^\sigma + (i+j)(a^{\sigma+1} + b^{\sigma+1}).$$

Theorem (de Caen, Mathon, M. (1995))

(a) $\Gamma_{q,\sigma}$ *is an antipodal distance regular graph of diameter 3, a q-fold cover of* K_{2q} *via* $(a, i, \alpha) \mapsto (a, i)$.

(b) $\Gamma_{q,\sigma} \cong \Gamma_{q,\sigma'} \Leftrightarrow \sigma' = \sigma^{\pm 1}$*, resulting in* $\frac{1}{2}\phi(2t-1)$ *nonisomorphic such covers.*

The full automorphism group of $\Gamma_{q,\sigma}$ is determined, together with the nonisomorphism result (b), by using walks on the graph $\Gamma_{q,\sigma}$ to construct binary codes; then showing that these are generalized Preparata codes; and finally using Kantor's determination of automorphisms/isomorphisms of generalized Preparata codes (1983).

Thank You!

Questions?