Testing isomorphism of p-groups of genus 2

Peter Brooksbank

Bucknell University

Algorithms for Linear Groups

Banff International Research Station

November 16–21, 2014

Group Isomorphism

(joint work with J. Maglione and J. Wilson)

Group Isomorphism

(joint work with J. Maglione and J. Wilson)

ISO *Given two groups, G and H, decide whether or not $G \cong H$.*

Group Isomorphism

(joint work with J. Maglione and J. Wilson)

ISO *Given two groups, G and H, decide whether or not $G \cong H$.*

- Computational model?

Group Isomorphism

(joint work with J. Maglione and J. Wilson)

ISO *Given two groups, G and H, decide whether or not $G \cong H$.*

- Computational model? We assume that G and H are specified concisely (e.g. permutation group, matrix group, PC-group).

Group Isomorphism

(joint work with J. Maglione and J. Wilson)

ISO *Given two groups, G and H, decide whether or not $G \cong H$.*

- Computational model? We assume that G and H are specified concisely (e.g. permutation group, matrix group, PC-group).
- Efficiency?

Group Isomorphism

(joint work with J. Maglione and J. Wilson)

ISO *Given two groups, G and H, decide whether or not $G \cong H$.*

- Computational model? We assume that G and H are specified concisely (e.g. permutation group, matrix group, PC-group).
- Efficiency? We desire algorithms that are (close to) polynomial in $\log |G|$, and that are also practical.

Group Isomorphism

(joint work with J. Maglione and J. Wilson)

ISO *Given two groups, G and H, decide whether or not $G \cong H$.*

- Computational model? We assume that G and H are specified concisely (e.g. permutation group, matrix group, PC-group).
- Efficiency? We desire algorithms that are (close to) polynomial in $\log |G|$, and that are also practical.

AUTO *Given a finite group G, construct (generators for)* $\mathrm{Aut}(G)$.

Some Remarks

1. In the *Cayley Model* (where the full multiplication table is given), isomorphism of groups of order N can be tested in time $N^{\log N}$.

Some Remarks

1. In the *Cayley Model* (where the full multiplication table is given), isomorphism of groups of order N can be tested in time $N^{\log N}$.
2. Isomorphism of simple groups decided in polynomial time ...

Some Remarks

1. In the *Cayley Model* (where the full multiplication table is given), isomorphism of groups of order N can be tested in time $N^{\log N}$.
2. Isomorphism of simple groups decided in polynomial time ...
3. ... but the hard stuff lies at the other end of the spectrum:
   - Abelian groups are handled easily.
   - Extraspecial p-groups are fine too.
   - Certain very large families of "indistinguishable" p-groups can be handled in polynomial time [LW-2012] and [BW-2015+].

Some Remarks

1. In the *Cayley Model* (where the full multiplication table is given), isomorphism of groups of order N can be tested in time $N^{\log N}$.
2. Isomorphism of simple groups decided in polynomial time ...
3. ... but the hard stuff lies at the other end of the spectrum:
   - Abelian groups are handled easily.
   - Extraspecial p-groups are fine too.
   - Certain very large families of "indistinguishable" p-groups can be handled in polynomial time [LW-2012] and [BW-2015+].
   - **However, the isomorphism problem for arbitrary p-groups of class 2 is thought to be as hard as the general problem.**

The Baer Correspondence

Throughout, k will be a finite field.

The Baer Correspondence

Throughout, k will be a finite field.

A k-**bimap** is a function $\circ\colon k^d \times k^d \rightarrowtail k^e$ s.t. $\forall u, v, w \in k^d$, $\forall \alpha \in k$,

$$(u + \alpha v) \circ w = u \circ w + \alpha(v \circ w),$$
$$u \circ (v + \alpha w) = u \circ v + \alpha(u \circ w).$$

The Baer Correspondence

Throughout, k will be a finite field.

A k-**bimap** is a function $\circ\colon k^d \times k^d \rightarrowtail k^e$ s.t. $\forall u, v, w \in k^d$, $\forall \alpha \in k$,

$$(u + \alpha v) \circ w = u \circ w + \alpha(v \circ w),$$
$$u \circ (v + \alpha w) = u \circ v + \alpha(u \circ w).$$

If G is a finite p-group of class 2 and exponent p, then

$$xZ(G) \circ yZ(G) := [x, y]$$

is an alternating $(\mathbb{Z}/p)$-bimap $\circ = \circ(G)\colon G/Z(G) \times G/Z(G) \rightarrowtail G'$. Conversely, given a $(\mathbb{Z}/p)$-bimap, $\circ$, one can build a p-group G whose associated bimap is $\circ$. This is known as the **Baer Correspondence**.

Isometries and Pseudo-Isometries

Automorphisms of G correspond to **pseudo-isometries** of $\circ(G)$:

$$\Psi\mathrm{Isom}(\circ) = \{(h, \hat{h}) \in \mathrm{GL}(d,k) \times \mathrm{GL}(e,k) : uh \circ vh = (u \circ v)\hat{h}\}.$$

- $\Psi\mathrm{Isom}(G)$ is faithfully represented on k^d; this is its **inner action**. The projection onto $\mathrm{GL}(e,k)$ is referred to as its **outer action**.

Isometries and Pseudo-Isometries

Automorphisms of G correspond to **pseudo-isometries** of $\circ(G)$:

$$\Psi\mathrm{Isom}(\circ) = \{(h, \hat{h}) \in \mathrm{GL}(d,k) \times \mathrm{GL}(e,k) : uh \circ vh = (u \circ v)\hat{h}\}.$$

- $\Psi\mathrm{Isom}(G)$ is faithfully represented on k^d; this is its **inner action**. The projection onto $\mathrm{GL}(e,k)$ is referred to as its **outer action**.
- $\Psi\mathrm{Isom}(\circ)$ has a more familiar-looking normal subgroup, namely its group of **isometries**:

$$\mathrm{Isom}(\circ) = \{h \in \mathrm{GL}(d,k) : uh \circ vh = u \circ v\}.$$

Adjoints

To each bimap $\circ\colon k^d \times k^d \rightarrowtail k^e$ we associate a ring

$$A(\circ) = \{(x, y) \in \mathbb{M}_d(k) \times \mathbb{M}_d(k) \colon ux \circ v = u \circ yv\},$$

called the **adjoint ring** of $\circ$.

Adjoints

To each bimap $\circ\colon k^d \times k^d \rightarrowtail k^e$ we associate a ring

$$A(\circ) = \{(x, y) \in \mathbb{M}_d(k) \times \mathbb{M}_d(k) \colon ux \circ v = u \circ yv\},$$

called the **adjoint ring** of $\circ$.

- $A(\circ)$ is a $*$**-ring**. It is represented faithfully represented on k^d, and $x^* := y$ is an involution on $A(\circ)$.

Adjoints

To each bimap $\circ\colon k^d \times k^d \rightarrowtail k^e$ we associate a ring

$$A(\circ) = \{(x, y) \in \mathbb{M}_d(k) \times \mathbb{M}_d(k) \colon ux \circ v = u \circ yv\},$$

called the **adjoint ring** of $\circ$.

- $A(\circ)$ is a $*$**-ring**. It is represented faithfully represented on k^d, and $x^* := y$ is an involution on $A(\circ)$.
- $A(\circ)$ is the unique largest ring $B \subset \mathbb{M}_d(k)$ such that $\circ$ factors through the tensor bimap $k^d \times k^d \rightarrowtail k^d \otimes_B k^d$.

Adjoints

To each bimap $\circ\colon k^d \times k^d \rightarrowtail k^e$ we associate a ring

$$A(\circ) = \{(x, y) \in \mathbb{M}_d(k) \times \mathbb{M}_d(k) \colon ux \circ v = u \circ yv\},$$

called the **adjoint ring** of $\circ$.

- $A(\circ)$ is a $*$**-ring**. It is represented faithfully represented on k^d, and $x^* := y$ is an involution on $A(\circ)$.
- $A(\circ)$ is the unique largest ring $B \subset \mathbb{M}_d(k)$ such that $\circ$ factors through the tensor bimap $k^d \times k^d \rightarrowtail k^d \otimes_B k^d$.
- The $*$-ring structure of $A(\circ)$ mirrors group structure of $\mathrm{Isom}(\circ)$.

Adjoints

To each bimap $\circ\colon k^d \times k^d \rightarrowtail k^e$ we associate a ring

$$A(\circ) = \{(x, y) \in \mathbb{M}_d(k) \times \mathbb{M}_d(k) \colon ux \circ v = u \circ yv\},$$

called the **adjoint ring** of $\circ$.

- $A(\circ)$ is a **$*$-ring**. It is represented faithfully represented on k^d, and $x^* := y$ is an involution on $A(\circ)$.
- $A(\circ)$ is the unique largest ring $B \subset \mathbb{M}_d(k)$ such that $\circ$ factors through the tensor bimap $k^d \times k^d \rightarrowtail k^d \otimes_B k^d$.
- The $*$-ring structure of $A(\circ)$ mirrors group structure of $\mathrm{Isom}(\circ)$.

[BW-2012a] *Given an alternating bimap* $\circ\colon k^d \times k^d \rightarrowtail k^e$, *in polynomial-time we can:*
(a) construct a k-basis for $A(\circ)$*; and*
(b) if k is finite, $\mathrm{char}\, k > 2$, *construct generators for* $\mathrm{Isom}(\circ)$.

Perp Decompositions

We say that a direct sum decomposition $V = U_1 \oplus \ldots \oplus U_n$ is a **$\perp$-decomposition** of $\circ : V \times V \rightarrowtail W$ if $U_i \circ U_j = 0$ for all $i \neq j$.

Perp Decompositions

We say that a direct sum decomposition $V = U_1 \oplus \ldots \oplus U_n$ is a **$\perp$-decomposition** of $\circ\colon V \times V \rightarrowtail W$ if $U_i \circ U_j = 0$ for all $i \neq j$.

If the restriction of $\circ$ to U_i is $\perp$-indecomposable for all i, then we say that the decomposition of **fully refined**.

Such decompositions correspond to *frames* of primitive, self-adjoint idempotents in $A(\circ)$.

Perp Decompositions

We say that a direct sum decomposition $V = U_1 \oplus \ldots \oplus U_n$ is a **$\perp$-decomposition** of $\circ\colon V \times V \rightarrowtail W$ if $U_i \circ U_j = 0$ for all $i \neq j$.

If the restriction of $\circ$ to U_i is $\perp$-indecomposable for all i, then we say that the decomposition of **fully refined**.

Such decompositions correspond to *frames* of primitive, self-adjoint idempotents in $A(\circ)$.

[Wi-2009] *There is a polynomial-time algorithm which, given a $*$-ring R, returns a frame of primitive, self-adjoint idempotents of R.*

Perp Decompositions

We say that a direct sum decomposition $V = U_1 \oplus \ldots \oplus U_n$ is a **$\perp$-decomposition** of $\circ\colon V \times V \rightarrowtail W$ if $U_i \circ U_j = 0$ for all $i \neq j$.

If the restriction of $\circ$ to U_i is $\perp$-indecomposable for all i, then we say that the decomposition of **fully refined**.

Such decompositions correspond to *frames* of primitive, self-adjoint idempotents in $A(\circ)$.

[Wi-2009] *There is a polynomial-time algorithm which, given a $*$-ring R, returns a frame of primitive, self-adjoint idempotents of R.*

All of these algorithms are distributed with MAGMA as part of the package `StarAlgebras`.

Genus 2

For the remainder of the talk we focus on alternating bimaps $\circ : k^d \times k^d \rightarrowtail k^2$, which we refer to as **genus 2**. They correspond to p-groups G of class 2 and exponent p for which $Z(G)$ has order p^2.

Genus 2

For the remainder of the talk we focus on alternating bimaps $\circ\colon k^d \times k^d \rightarrowtail k^2$, which we refer to as **genus 2**. They correspond to p-groups G of class 2 and exponent p for which $Z(G)$ has order p^2.

- We specify $\circ$ for computation via a **basis** $[X, Y]$ of matrices.
- We say that $\circ$ is **sloped** if there exists $\pi\colon k^2 \to k$ such that the form $\bullet\colon k^d \times k^d \rightarrowtail k$, where $u \bullet v = (u \circ v)\pi$, is nondegenerate.
- If $\circ$ is sloped, we may assume that X, say, is nonsingular. We refer to $\sigma := YX^{-1}$ as a **slope** of $\circ$. Here, $A(\circ) = C_{\mathbb{M}_d(k)}(\sigma)$. By a change of basis, we may assume that

$$X = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & \tau \\ -\tau^{\mathrm{tr}} & 0 \end{bmatrix} \quad \text{and} \quad YX^{-1} = \begin{bmatrix} \tau & 0 \\ 0 & \tau^{\mathrm{tr}} \end{bmatrix}.$$

Genus 2

For the remainder of the talk we focus on alternating bimaps $\circ\colon k^d \times k^d \rightarrowtail k^2$, which we refer to as **genus 2**. They correspond to p-groups G of class 2 and exponent p for which $Z(G)$ has order p^2.

- We specify $\circ$ for computation via a **basis** $[X, Y]$ of matrices.
- We say that $\circ$ is **sloped** if there exists $\pi\colon k^2 \to k$ such that the form $\bullet\colon k^d \times k^d \rightarrowtail k$, where $u \bullet v = (u \circ v)\pi$, is nondegenerate.
- If $\circ$ is sloped, we may assume that X, say, is nonsingular. We refer to $\sigma := YX^{-1}$ as a **slope** of $\circ$. Here, $A(\circ) = C_{\mathbb{M}_d(k)}(\sigma)$. By a change of basis, we may assume that

$$X = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & \tau \\ -\tau^{\mathrm{tr}} & 0 \end{bmatrix} \quad \text{and} \quad YX^{-1} = \begin{bmatrix} \tau & 0 \\ 0 & \tau^{\mathrm{tr}} \end{bmatrix}.$$

- If $\circ$ is not sloped, we say that it is **flat**.

Genus 2

For the remainder of the talk we focus on alternating bimaps $\circ\colon k^d \times k^d \rightarrowtail k^2$, which we refer to as **genus 2**. They correspond to p-groups G of class 2 and exponent p for which $Z(G)$ has order p^2.

- We specify $\circ$ for computation via a **basis** $[X, Y]$ of matrices.
- We say that $\circ$ is **sloped** if there exists $\pi\colon k^2 \to k$ such that the form $\bullet\colon k^d \times k^d \rightarrowtail k$, where $u \bullet v = (u \circ v)\pi$, is nondegenerate.
- If $\circ$ is sloped, we may assume that X, say, is nonsingular. We refer to $\sigma := YX^{-1}$ as a **slope** of $\circ$. Here, $A(\circ) = C_{\mathbb{M}_d(k)}(\sigma)$. By a change of basis, we may assume that

$$X = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & \tau \\ -\tau^{\mathrm{tr}} & 0 \end{bmatrix} \quad \text{and} \quad YX^{-1} = \begin{bmatrix} \tau & 0 \\ 0 & \tau^{\mathrm{tr}} \end{bmatrix}.$$

- If $\circ$ is not sloped, we say that it is **flat**.
- See [BW-2012b] for more details.

Pseudo-Isometries, Automorphisms, Isomorphisms

THEOREM

There are **two** Las Vegas algorithms which, given alternating

$$\circ : \mathrm{GF}(p^e)^d \times \mathrm{GF}(p^e)^d \rightarrowtail \mathrm{GF}(p^e)^2,$$

constructs generators for $\Psi\mathrm{Isom}(\circ)$:

(i) the first uses $O(d^6 + (pe)^3 d^4)$ operations in $\mathrm{GF}(p^e)$, and

(ii) the second runs in time $O((de)^6)$, assuming the group permuting isotypic components of τ has comp. factors of bounded degree.

Pseudo-Isometries, Automorphisms, Isomorphisms

THEOREM

There are **two** Las Vegas algorithms which, given alternating

$$\circ : \mathrm{GF}(p^e)^d \times \mathrm{GF}(p^e)^d \rightarrowtail \mathrm{GF}(p^e)^2,$$

constructs generators for $\Psi\mathrm{Isom}(\circ)$:

(i) the first uses $O(d^6 + (pe)^3 d^4)$ operations in $\mathrm{GF}(p^e)$, and

(ii) the second runs in time $O((de)^6)$, assuming the group permuting isotypic components of τ has comp. factors of bounded degree.

COR 1

Given a p-group G of genus 2, one can efficiently construct $\mathrm{Aut}(G)$.

COR 2

Given p-groups G and H of genus 2, one can efficiently decide whether $G \cong H$ and, if so, construct an isomorphism $G \to H$.

Overview of Algorithms

$\Psi\mathrm{Isom}(\circ : k^d \times k^d \rightarrowtail k^2)$

{Given: a nondegenerate bimap $\circ : k^d \times k^d \rightarrowtail k^2$}

{Find: (generators for) $\Psi\mathrm{Isom}(\circ)$}

Overview of Algorithms

$\Psi\mathrm{Isom}(\circ : k^d \times k^d \rightarrowtail k^2)$

{Given: a nondegenerate bimap $\circ : k^d \times k^d \rightarrowtail k^2$}

{Find: (generators for) $\Psi\mathrm{Isom}(\circ)$}

1. Decompose $\circ = \circ_1 \perp \ldots \perp \circ_n$ into indecomposables.
2. Write $\circ = \diamond \perp \bullet$ where $\diamond$ and $\bullet$ are flat and sloped summands.
3. Construct $H^{\diamond} := \Psi\mathrm{Isom}(\diamond)$.
4. Construct $H^{\bullet} := \Psi\mathrm{Isom}(\bullet)$. ** here the two methods differ */*
5. Glue together $H^{\diamond}$ and $H^{\bullet}$ to obtain $H = \Psi\mathrm{Isom}(\circ)$.

The Polynomial Method

- Based on two papers by Vishnevetskiĭ [Vi-1980], [Vi-1985].

The Polynomial Method

- Based on two papers by Vishnevetskiĭ [Vi-1980], [Vi-1985].
- It uses the original decomposition $\circ_1 \perp \ldots \perp \circ_n$ into sloped indecomposables.
- It associates to each indecomposable summand a homogeneous polynomial $f_i(s,t)$ of degree d.
- For $\hat{h} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{GL}(2,k)$, define $f_i^{\hat{h}}(s,t) = f_i(\alpha s + \beta t, \gamma s + \delta t)$. Then $\hat{h}$ lifts to a pseudo-isometry iff $\exists (c_1, \ldots, c_n) \in k^n$ such that

$$\{c_1 {f_1}^{\hat{h}}, \ldots, c_n {f_n}^{\hat{h}}\} = \{f_1, \ldots, f_n\} \qquad \text{(as multisets)}.$$

Nilpotent Quotient Algorithms

When computing the automorphism group of p-group G of class 2, *nilpotent quotient algorithms* arrive at the following situation:

- We have $\circ = \circ(G) \colon V \times V \rightarrowtail W$.
- As $\circ$ is alternating, it factors through the exterior square $V \wedge V$.
- There is a unique map $\hat{\circ} \colon V \wedge V \to W$ such that

$$u \circ v \;=\; (u \wedge v)\hat{\circ} \quad \text{for all } u, v \in V.$$

Nilpotent Quotient Algorithms

When computing the automorphism group of p-group G of class 2, *nilpotent quotient algorithms* arrive at the following situation:

- We have $\circ = \circ(G) \colon V \times V \rightarrowtail W$.
- As $\circ$ is alternating, it factors through the exterior square $V \wedge V$.
- There is a unique map $\hat{\circ} \colon V \wedge V \to W$ such that

$$u \circ v \;=\; (u \wedge v)\hat{\circ} \quad \text{for all } u, v \in V.$$

- $\mathrm{Aut}(G)$ corresponds to the stabilizer of $\ker \hat{\circ}$ under the natural action of $\Psi\mathrm{Isom}(\wedge)$ on $V \wedge V$.
- Note that $\dim(V \wedge V) = \binom{d}{2}$, and $\Psi\mathrm{Isom}(\wedge) \cong \mathrm{GL}(d, p)$.

Nilpotent Quotient Algorithms

When computing the automorphism group of p-group G of class 2, *nilpotent quotient algorithms* arrive at the following situation:

- We have $\circ = \circ(G) \colon V \times V \rightarrowtail W$.
- As $\circ$ is alternating, it factors through the exterior square $V \wedge V$.
- There is a unique map $\hat{\circ} \colon V \wedge V \to W$ such that

$$u \circ v \;=\; (u \wedge v)\hat{\circ} \quad \text{for all } u, v \in V.$$

- $\mathrm{Aut}(G)$ corresponds to the stabilizer of $\ker \hat{\circ}$ under the natural action of $\Psi\mathrm{Isom}(\wedge)$ on $V \wedge V$.
- Note that $\dim(V \wedge V) = \binom{d}{2}$, and $\Psi\mathrm{Isom}(\wedge) \cong \mathrm{GL}(d, p)$.

... the orbits of $\ker \hat{\circ}$ quickly become unmanageably large.

A Refinement: The Adjoint-Tensor Method

Idea: Factor $\circ$ through tensor over a larger ring.

A Refinement: The Adjoint-Tensor Method

Idea: Factor $\circ$ through tensor over a larger ring.

Recall: $A = A(\circ)$ *is the largest such ring!*

A Refinement: The Adjoint-Tensor Method

Idea: Factor $\circ$ through tensor over a larger ring.

Recall: $A = A(\circ)$ *is the largest such ring!* Now, we have:

- $\hat{\circ}\colon V \otimes_A V \to W$;
- $\Psi\mathrm{Isom}(\otimes)$ acts naturally on $V \otimes_A V$; and
- we require the stabilizer of $\ker \hat{\circ}$ in this action.

A Refinement: The Adjoint-Tensor Method

Idea: Factor $\circ$ through tensor over a larger ring.

Recall: $A = A(\circ)$ *is the largest such ring!* Now, we have:

- $\hat{\circ}\colon V \otimes_A V \to W$;
- $\Psi\mathrm{Isom}(\otimes)$ acts naturally on $V \otimes_A V$; and
- we require the stabilizer of $\ker \hat{\circ}$ in this action.

The method works best when:

- $V \otimes_A V$ is small (significantly smaller than $V \wedge V$);
- we can readily build the group $\Psi\mathrm{Isom}(\otimes)$; and
- we can compute stabilizers under the action of $\Psi\mathrm{Isom}(\otimes)$ using techniques that are better than brute force.

These ideas are discussed more fully in [BW-2014].

$\Psi\mathrm{Isom}(\otimes_A)$

Given $\circ : k^d \times k^d \rightarrowtail k^2$ specified by $X = \left[\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right]$ and $Y = \left[\begin{smallmatrix} 0 & \tau \\ -\tau^{\mathrm{tr}} & 0 \end{smallmatrix}\right]$.

- Put $\sigma := YX^{-1} = \left[\begin{smallmatrix} \tau & 0 \\ 0 & \tau^{\mathrm{tr}} \end{smallmatrix}\right]$. Then $A = A(\circ) = C(\sigma) \cong \mathbb{M}_2(k[\tau])$.

$\Psi\mathrm{Isom}(\otimes_A)$

Given $\circ : k^d \times k^d \rightarrowtail k^2$ specified by $X = \left[\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right]$ and $Y = \left[\begin{smallmatrix} 0 & \tau \\ -\tau^{\mathrm{tr}} & 0 \end{smallmatrix}\right]$.

- Put $\sigma := YX^{-1} = \left[\begin{smallmatrix} \tau & 0 \\ 0 & \tau^{\mathrm{tr}} \end{smallmatrix}\right]$. Then $A = A(\circ) = C(\sigma) \cong \mathbb{M}_2(k[\tau])$.
- Put $R := k[\tau]$. Then $k^d \otimes_A k^d \cong R$ as a k-module, and

$$\otimes = \otimes_A : R^2 \times R^2 \rightarrowtail R \quad \text{is an } R\text{-form.}$$

$\Psi\mathrm{Isom}(\otimes_A)$

Given $\circ : k^d \times k^d \rightarrowtail k^2$ specified by $X = \left[\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right]$ and $Y = \left[\begin{smallmatrix} 0 & \tau \\ -\tau^{\mathrm{tr}} & 0 \end{smallmatrix}\right]$.

- Put $\sigma := YX^{-1} = \left[\begin{smallmatrix} \tau & 0 \\ 0 & \tau^{\mathrm{tr}} \end{smallmatrix}\right]$. Then $A = A(\circ) = C(\sigma) \cong \mathbb{M}_2(k[\tau])$.
- Put $R := k[\tau]$. Then $k^d \otimes_A k^d \cong R$ as a k-module, and

$$\otimes \;= \otimes_A : R^2 \times R^2 \rightarrowtail R \quad \text{is an } R\text{-form.}$$

- $\Psi\mathrm{Isom}(\otimes)$ acts on R with kernel $\mathrm{Isom}(\otimes) = \mathrm{Isom}(\circ)$, and

$$\Psi\mathrm{Isom}(\otimes)/\mathrm{Isom}(\otimes) \cong R^\times \rtimes N(R) = \Pi.\Sigma,$$

where Π permutes the isotypic factors of τ, and Σ is soluble.

$\Psi\mathrm{Isom}(\otimes_A)$

Given $\circ : k^d \times k^d \rightarrowtail k^2$ specified by $X = \left[\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right]$ and $Y = \left[\begin{smallmatrix} 0 & \tau \\ -\tau^{\mathrm{tr}} & 0 \end{smallmatrix}\right]$.

- Put $\sigma := YX^{-1} = \left[\begin{smallmatrix} \tau & 0 \\ 0 & \tau^{\mathrm{tr}} \end{smallmatrix}\right]$. Then $A = A(\circ) = C(\sigma) \cong \mathbb{M}_2(k[\tau])$.
- Put $R := k[\tau]$. Then $k^d \otimes_A k^d \cong R$ as a k-module, and

$$\otimes \; = \otimes_A : R^2 \times R^2 \rightarrowtail R \quad \text{is an } R\text{-form.}$$

- $\Psi\mathrm{Isom}(\otimes)$ acts on R with kernel $\mathrm{Isom}(\otimes) = \mathrm{Isom}(\circ)$, and

$$\Psi\mathrm{Isom}(\otimes)/\mathrm{Isom}(\otimes) \cong R^\times \rtimes N(R) = \Pi.\Sigma,$$

  where Π permutes the isotypic factors of τ, and Σ is soluble.
- Using methods of Luks [Lu-1992] for soluble matrix groups together with some linear algebra tricks we can compute subspace stabilizers under the action of $\Psi\mathrm{Isom}(\otimes)$ efficiently.

Testing Isomorphism

`IsIsomorphic` (G_1 , G_2)
{Given: genus 2 groups G_1 and G_2}
{Decide: Is $G_1 \cong G_2$?}

Testing Isomorphism

`IsIsomorphic` (G_1 , G_2)
{Given: genus 2 groups G_1 and G_2}
{Decide: Is $G_1 \cong G_2$?}

1. Write down the bimaps $\circ_i : k^d \times k^d \rightarrowtail k^2$ associated to G_i.
2. Compute the adjoint algebras $A_i = A(\circ_i) \leqslant \mathbb{M}_d(k)$.

Testing Isomorphism

`IsIsomorphic` (G_1 , G_2)
{Given: genus 2 groups G_1 and G_2}
{Decide: Is $G_1 \cong G_2$?}

1. Write down the bimaps $\circ_i : k^d \times k^d \rightarrowtail k^2$ associated to G_i.
2. Compute the adjoint algebras $A_i = A(\circ_i) \leqslant \mathbb{M}_d(k)$.
3. Find $g \in \mathrm{GL}(d,k)$ with $A_2^g = A_1$ (if such exists). [BW-2015]

Testing Isomorphism

`IsIsomorphic` (G_1 , G_2)
{Given: genus 2 groups G_1 and G_2}
{Decide: Is $G_1 \cong G_2$?}

1. Write down the bimaps $\circ_i : k^d \times k^d \rightarrowtail k^2$ associated to G_i.
2. Compute the adjoint algebras $A_i = A(\circ_i) \leqslant \mathbb{M}_d(k)$.
3. Find $g \in \mathrm{GL}(d,k)$ with $A_2^g = A_1$ (if such exists). [BW-2015]
3. Use g to change basis of $\circ_2$; form tensor product $k^d \otimes_{A_1} k^d$.
4. Decide isomorphism, as before, by testing whether $\ker \hat{\circ}_1$ and $\ker \hat{\circ}_2$ are in the same $\Psi\mathrm{Isom}(\otimes)$-orbit.

Implementation & Performance

Versions of both algorithms have been implemented in MAGMA.

Implementation & Performance

Versions of both algorithms have been implemented in MAGMA.

- *Outside-In*
  The polynomial approach lists the "outer action", and determines which elements can be lifted to "inner" pseudo-isometries.
  This always involves a loop over p^3 elements.
- *Inside-Out*
  The adjoint-tensor approach finds a good over-estimate of the "inner" pseudo-isometries, and then chops it down to size.
  Almost always this can be done very quickly but sometimes we must loop over quite large permutation groups.

References

[BW-2012a] B, J.B. Wilson, *Computing isometry groups of Hermitian maps*, TAMS, 2012.

[BW-2012b] B, J.B. Wilson, *Intersecting two classical groups*, J. Algebra, 2012.

[BW-2014] B, J.B. Wilson, *Groups acting on tensor products*, J. Pure Appl. Algebra, 2014.

[BW-2015] B, J.B. Wilson, *The module isomorphism problem reconsidered*, J. Algebra, 2015.

[BW-2015+] B, J.B. Wilson, *On the futility of group isomorphism testing*, preprint.

[LW-2012] M. Lewis, J.B. Wilson, *Isomorphism in expanding families of indistinguishable groups*, Groups Complex. Cryptol., 2012.

[Lu-1992] E.M. Luks, *Computing in solvable matrix groups*, IEEE, 1992.

[Wi-2009] J.B. Wilson, *Finding central decompositions of p-groups*, J. Algebra, 2009.

[Vi-1980] A.L. Vishnevetskiĭ, *Groups of class 2 and exponent p with commutant of order p^2*, Dokl. Akad. Nauk. Ukraine, 1980.

[Vi-1985] A.L. Vishnevetskiĭ, *A system of invariants of certain groups of class 2 with commutator subgroup of rank 2*, Ukrain. Mat. Zh., 1985.

Thank You, Ákos