# Deciding isomorphism of finite groups

Peter Brooksbank

Bucknell University

Linear Algebra and Matrix Theory:
connections, applications and computations
NUI Galway (December 5, 2012)

# The Group Isomorphism Problem

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

How might $G$ and $H$ be given?

1. As finitely presented groups (à la Dehn).
2. As finite groups.
   2.1 Listing elements of $G$ and $H$ and their multiplication tables.
   2.2 Specifying generating sets of permutations or matrices.

We will find it convenient to discuss the related problem:

AUTO: Given a group $G$, find generators for $\mathrm{Aut}(G)$.

# A Brute Force Approach

When $G$ and $H$, each of order $n$, are specified by multiplication tables, the following elementary approach (attributed to Tarjan) provides an upper bound on the complexity.

1. Pick a generating sequence $A$ of size $k$ for $G$.
2. For each $k$-sequence $B$ of elements of $H$, use the multiplication tables of $G$ and $H$ to decide whether or not the bijection $A \to B$ extends to an isomorphism.
3. There are $\binom{n}{k}k! < n^k$ such $k$-tuples $B$.
4. For each $k$-tuple, deciding whether the bijection extends requires $n^c$ checks (for some constant $c$).
5. Every group $G$ has a generating set of size at most $\log |G|$.
6. Thus the algorithm runs in time $n^{\log n + O(1)}$.

# Better Than Brute Force?

- Recent attempts have improved only very slightly on brute force, although significant improvements have been achieved for certain classes of group (such as abelian groups, and groups without abelian normal subgroups).

# Better Than Brute Force?

- Recent attempts have improved only very slightly on brute force, although significant improvements have been achieved for certain classes of group (such as abelian groups, and groups without abelian normal subgroups).
- There have been no measurable improvements even for nilpotent groups of class 2. In fact, it seems likely that these are among the hardest groups to handle. We study such groups in this lecture.

# Better Than Brute Force?

- Recent attempts have improved only very slightly on brute force, although significant improvements have been achieved for certain classes of group (such as abelian groups, and groups without abelian normal subgroups).
- There have been no measurable improvements even for nilpotent groups of class 2. In fact, it seems likely that these are among the hardest groups to handle. We study such groups in this lecture.
- There is perhaps more interest in practical isomorphism tests than in techniques to improve complexity bounds. For instance efforts to classify families of $p$-groups require such practical tests. It is not practical here to start by listing a multiplication table of the group.

# The Bimap of a Nilpotent Group

If $G$ is a nilpotent group of class 2, with centre $Z = Z(G)$, then

$$V := G/Z \text{ and } W := [G, G] \leqslant Z$$

are abelian groups. Associate to $G$ a function $\circ\colon V \times V \to W$

$$xZ \circ yZ \;:=\; [x, y] \text{ for all } x, y \in G.$$

# The Bimap of a Nilpotent Group

If $G$ is a nilpotent group of class 2, with centre $Z = Z(G)$, then

$$V := G/Z \text{ and } W := [G, G] \leqslant Z$$

are abelian groups. Associate to $G$ a function $\circ \colon V \times V \to W$

$$xZ \circ yZ \; := \; [x, y] \text{ for all } x, y \in G.$$

Writing operations in $V$ and $W$ additively, observe

$$\begin{aligned} u \circ (v + w) &= u \circ v + u \circ w \\ (u + v) \circ w &= u \circ w + v \circ w \end{aligned}$$

so $\circ$ is a bi-additive map (or simply a bimap). Notice $\circ$ is also alternating in that $u \circ u = 0$ for all $u \in V$.

# Isometries, Pseudo-Isometries, and Automorphisms

Let $G$ be a finite $p$-group of exponent $p$ and class 2. Then $V = G/Z$ and $W = [G, G] \leqslant Z$ are finite-dimensional vector spaces over $\mathbb{Z}/p$.

Let $\circ\colon V \times V \to W$ be the bimap associated to $G$, and let $\alpha$ be an automorphism of $G$. Let $\beta$ (resp. $\gamma$) be the automorphism of $V$ (resp. $W$) induced by $\alpha$. Then

$$u\beta \circ v\beta = (u \circ v)\gamma \text{ for all } u, v \in V.$$

Thus $\alpha$ induces the pseudo-isometry $(\beta, \gamma)$ of $\circ$.

# Isometries, Pseudo-Isometries, and Automorphisms

Let $G$ be a finite $p$-group of exponent $p$ and class 2. Then $V = G/Z$ and $W = [G, G] \leqslant Z$ are finite-dimensional vector spaces over $\mathbb{Z}/p$.

Let $\circ\colon V \times V \to W$ be the bimap associated to $G$, and let $\alpha$ be an automorphism of $G$. Let $\beta$ (resp. $\gamma$) be the automorphism of $V$ (resp. $W$) induced by $\alpha$. Then

$$u\beta \circ v\beta = (u \circ v)\gamma \ \text{ for all } u, v \in V.$$

Thus $\alpha$ induces the pseudo-isometry $(\beta, \gamma)$ of $\circ$. Define the group

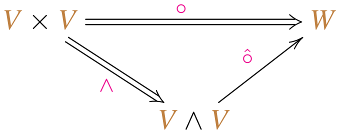
$$\Psi\mathrm{Isom}(\circ) = \{(g, h) \in \mathrm{Aut}(V) \times \mathrm{Aut}(W)\colon ug \circ vg = (u \circ v)h\},$$

of pseudo-isometries of $\circ$, and its normal subgroup of isometries,

$$\begin{aligned} \mathrm{Isom}(\circ) &= \{g \in \mathrm{Aut}(V)\colon ug \circ vg = u \circ v\} \\ &= \{g\colon (g, 1) \in \Psi\mathrm{Isom}(\circ)\}. \end{aligned}$$

# Computing Aut($G$) by Brute Force

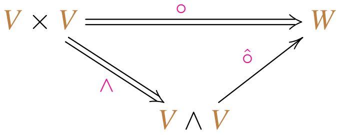
Let $G$ be a $p$-group of class 2, and $\circ\colon V \times V \to W$ its associated bimap. Then $\circ$ factors through the alternating tensor bimap:




Note, Aut($V$) acts on $V \wedge V$ via $(u \wedge v)^g = ug \wedge vg$, and $\Psi\mathrm{Isom}(\circ)$ is precisely the stabilizer under this action of Aut($V$) of $\ker \hat{\circ}$.

# Computing Aut($G$) by Brute Force

Let $G$ be a $p$-group of class 2, and $\circ\colon V \times V \to W$ its associated bimap. Then $\circ$ factors through the alternating tensor bimap:




Note, Aut($V$) acts on $V \wedge V$ via $(u \wedge v)^g = ug \wedge vg$, and $\Psi$Isom($\circ$) is precisely the stabilizer under this action of Aut($V$) of $\ker \hat{\circ}$.

Thus the problem of computing Aut($G$) reduces to that of computing the stabilizer of a subspace under the action of a group of matrices.

*we have exchanged one difficult problem for another!*

# Bimaps & Classical Groups

Let $\Phi_1, \ldots, \Phi_t$ be reflexive forms on a $k$-vector space $V$. Then

$$u \circ v = (u\,\Phi_1\,v, \ldots, u\,\Phi_t\,v).$$

is a bimap $\circ : V \times V \to k^t$, and

$$\mathrm{Isom}(\circ) = \mathrm{Isom}(\Phi_1) \cap \ldots \cap \mathrm{Isom}(\Phi_t).$$

Conversely, given an Hermitian bimap $\circ : V \times V \to W$, one obtains a corresponding list of forms by projection onto any spanning set of 1-dimensional subspaces of $W$.

*isometry groups of bimaps are intersections of classical groups*

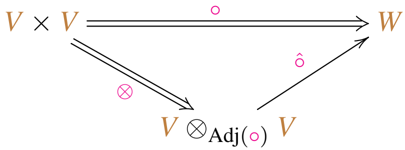
# The Adjoint Algebra of a Bimap

- Let $\circ \colon V \times V \to W$ be any bimap.
- Let $E = \mathrm{End}(V)$, and denote its opposite ring $E^{\mathrm{op}}$.
- View $V$ as a right $E$-module, and as a left $E^{\mathrm{op}}$-module.
- For $R$ subring of $E \times E^{\mathrm{op}}$, form the tensor product $V \otimes_R V$.
- Define the adjoint ring, $\mathrm{Adj}(\circ)$, to be the largest subring of $E \times E^{\mathrm{op}}$ for which $\circ$ factors through the tensor bimap:

$$\begin{array}{ccc} V \times V & \xrightarrow{\quad\circ\quad} & W \\ & {\scriptstyle\otimes}\searrow \quad \nearrow{\scriptstyle\hat{\circ}} & \\ & V \otimes_{\mathrm{Adj}(\circ)} V & \end{array}$$

# The Adjoint Algebra of a Bimap

- Let $\circ \colon V \times V \to W$ be any bimap.
- Let $E = \mathrm{End}(V)$, and denote its opposite ring $E^{\mathrm{op}}$.
- View $V$ as a right $E$-module, and as a left $E^{\mathrm{op}}$-module.
- For $R$ subring of $E \times E^{\mathrm{op}}$, form the tensor product $V \otimes_R V$.
- Define the adjoint ring, $\mathrm{Adj}(\circ)$, to be the largest subring of $E \times E^{\mathrm{op}}$ for which $\circ$ factors through the tensor bimap:




Here is an explicit description:

$$\mathrm{Adj}(\circ) = \{(x, y) \in E \times E^{\mathrm{op}} : ux \circ v = u \circ yv \ \ \forall u, v \in V\}.$$

# Adj($\circ$) as a $*$-algebra

1. Assume that $\circ : V \times V \to W$ is Hermitian: $\exists \theta \in \mathrm{Aut}(W)$ such that $u \circ v = (v \circ u)^\theta$ for all $u, v \in V$.
2. If $\circ$ is nondeg. and $(x, y) \in \mathrm{Adj}(\circ)$, then $y$ is uniquely determined by $x$ and $\mathrm{Adj}(\circ)$ is faithfully represented by projection onto $E$.
3. Hermitian $\Longrightarrow (x, y) \in \mathrm{Adj}(\circ)$ if and only if $(y, x) \in \mathrm{Adj}(\circ)$.

# Adj($\circ$) as a $*$-algebra

1. Assume that $\circ\colon V \times V \to W$ is Hermitian: $\exists \theta \in \mathrm{Aut}(W)$ such that $u \circ v = (v \circ u)^{\theta}$ for all $u, v \in V$.
2. If $\circ$ is nondeg. and $(x, y) \in \mathrm{Adj}(\circ)$, then $y$ is uniquely determined by $x$ and $\mathrm{Adj}(\circ)$ is faithfully represented by projection onto $E$.
3. Hermitian $\Longrightarrow$ $(x, y) \in \mathrm{Adj}(\circ)$ if and only if $(y, x) \in \mathrm{Adj}(\circ)$.
4. From 1 and 2, the map $x^* := y$ defines an involution on $\mathrm{Adj}(\circ)$.

# $\mathrm{Adj}(\circ)$ as a $*$-algebra

1. Assume that $\circ : V \times V \to W$ is Hermitian: $\exists \theta \in \mathrm{Aut}(W)$ such that $u \circ v = (v \circ u)^{\theta}$ for all $u, v \in V$.
2. If $\circ$ is nondeg. and $(x, y) \in \mathrm{Adj}(\circ)$, then $y$ is uniquely determined by $x$ and $\mathrm{Adj}(\circ)$ is faithfully represented by projection onto $E$.
3. Hermitian $\Longrightarrow (x, y) \in \mathrm{Adj}(\circ)$ if and only if $(y, x) \in \mathrm{Adj}(\circ)$.
4. From 1 and 2, the map $x^* := y$ defines an involution on $\mathrm{Adj}(\circ)$.
5. Consider the unitary group (or norm group) of $\mathrm{Adj}(\circ)$:

$$\mathrm{Adj}(\circ)^{\sharp} \quad = \quad \{x \in \mathrm{Adj}(\circ) : xx^* = 1 = x^*x\}$$

# $\mathrm{Adj}(\circ)$ as a $*$-algebra

1. Assume that $\circ\colon V \times V \to W$ is Hermitian: $\exists \theta \in \mathrm{Aut}(W)$ such that $u \circ v = (v \circ u)^{\theta}$ for all $u, v \in V$.
2. If $\circ$ is nondeg. and $(x, y) \in \mathrm{Adj}(\circ)$, then $y$ is uniquely determined by $x$ and $\mathrm{Adj}(\circ)$ is faithfully represented by projection onto $E$.
3. Hermitian $\Longrightarrow (x, y) \in \mathrm{Adj}(\circ)$ if and only if $(y, x) \in \mathrm{Adj}(\circ)$.
4. From 1 and 2, the map $x^* := y$ defines an involution on $\mathrm{Adj}(\circ)$.
5. Consider the unitary group (or norm group) of $\mathrm{Adj}(\circ)$:

$$\begin{aligned} \mathrm{Adj}(\circ)^{\sharp} &= \{x \in \mathrm{Adj}(\circ) : xx^* = 1 = x^*x\} \\ &= \{x \in \mathrm{Adj}(\circ) : x^* = x^{-1}\} \end{aligned}$$

# $\mathrm{Adj}(\circ)$ as a $*$-algebra

1. Assume that $\circ\colon V \times V \to W$ is Hermitian: $\exists\theta \in \mathrm{Aut}(W)$ such that $u \circ v = (v \circ u)^{\theta}$ for all $u, v \in V$.
2. If $\circ$ is nondeg. and $(x, y) \in \mathrm{Adj}(\circ)$, then $y$ is uniquely determined by $x$ and $\mathrm{Adj}(\circ)$ is faithfully represented by projection onto $E$.
3. Hermitian $\Longrightarrow (x, y) \in \mathrm{Adj}(\circ)$ if and only if $(y, x) \in \mathrm{Adj}(\circ)$.
4. From 1 and 2, the map $x^* := y$ defines an involution on $\mathrm{Adj}(\circ)$.
5. Consider the unitary group (or norm group) of $\mathrm{Adj}(\circ)$:

$$\begin{aligned}
\mathrm{Adj}(\circ)^{\sharp} &= \{x \in \mathrm{Adj}(\circ) : xx^* = 1 = x^*x\} \\
&= \{x \in \mathrm{Adj}(\circ) : x^* = x^{-1}\} \\
&= \{x \in \mathrm{Aut}(V) : ux \circ v = u \circ vx^{-1} \ \ \forall u, v \in V\}
\end{aligned}$$

# $\mathrm{Adj}(\circ)$ as a $*$-algebra

1. Assume that $\circ : V \times V \to W$ is Hermitian: $\exists \theta \in \mathrm{Aut}(W)$ such that $u \circ v = (v \circ u)^\theta$ for all $u, v \in V$.
2. If $\circ$ is nondeg. and $(x, y) \in \mathrm{Adj}(\circ)$, then $y$ is uniquely determined by $x$ and $\mathrm{Adj}(\circ)$ is faithfully represented by projection onto $E$.
3. Hermitian $\Longrightarrow (x, y) \in \mathrm{Adj}(\circ)$ if and only if $(y, x) \in \mathrm{Adj}(\circ)$.
4. From 1 and 2, the map $x^* := y$ defines an involution on $\mathrm{Adj}(\circ)$.
5. Consider the unitary group (or norm group) of $\mathrm{Adj}(\circ)$:

$$\begin{aligned}
\mathrm{Adj}(\circ)^\sharp &= \{x \in \mathrm{Adj}(\circ) : xx^* = 1 = x^*x\} \\
&= \{x \in \mathrm{Adj}(\circ) : x^* = x^{-1}\} \\
&= \{x \in \mathrm{Aut}(V) : ux \circ v = u \circ vx^{-1} \ \ \forall u, v \in V\} \\
&= \{x \in \mathrm{Aut}(V) : ux \circ vx = u \circ v \ \ \forall u, v \in V\} \\
&= \mathrm{Isom}(\circ)
\end{aligned}$$

# The Structure of Matrix Algebras

Let $A$ be a subalgebra of $\mathbb{M}_d(\mathbb{F}_q)$, where $\mathbb{F}_q$ is the field of $q$ elements.

1. The Jacobson radical, $J(A)$, is the unique largest nilpotent ideal of $A$, and $A = J(A) \oplus B$, where $B$ is a semisimple subring of $A$.
2. $B$ decomposes as a sum of minimal ideals $I_1 \oplus \ldots \oplus I_t$.
3. Each $I_j$ is a simple ring, and hence is isomorphic to $\mathbb{M}_{e_j}(K_j)$, where $K_j$ is a finite extension of $\mathbb{F}_q$.

# Algorithms for Matrix Algebras

- The algorithmic study of associative algebras was initiated by Rónyai in 1990.
- Methods were later refined for matrix algebras by Ivanyos and by Eberly & Giesbrecht in 2000.

# Algorithms for Matrix Algebras

- The algorithmic study of associative algebras was initiated by Rónyai in 1990.
- Methods were later refined for matrix algebras by Ivanyos and by Eberly & Giesbrecht in 2000.

## Theorem

*There is a Las Vegas, polynomial time algorithm which, given a subalgebra $A$ of $\mathbb{M}_d(\mathbb{F}_q)$, finds the following:*

*the Jacobson radical, $J(A)$, of $A$;*

*a ring decomposition $A = J(A) \oplus B$, where $B$ is semisimple;*

*a decomposition $B = I_1 \oplus \ldots \oplus I_t$ into minimal ideals; and*

*isomorphisms $\varphi_j \colon I_j \to \mathbb{M}_{e_j}(K_j)$ for field extensions $K_j$.*

# The Structure of Matrix $*$-Algebras

Let $A$ be a $*$-subalgebra of $\mathbb{M}_d(\mathbb{F}_q)$, where $q$ is odd.

1. $J(A)$ is a $*$-ideal (it is invariant under $*$), and $A = J(A) \oplus B$, where $B$ is a $*$-invariant semisimple subring of $A$. (Taft)

# The Structure of Matrix $*$-Algebras

Let $A$ be a $*$-subalgebra of $\mathbb{M}_d(\mathbb{F}_q)$, where $q$ is odd.

1. $J(A)$ is a $*$-ideal (it is invariant under $*$), and $A = J(A) \oplus B$, where $B$ is a $*$-invariant semisimple subring of $A$. (Taft)
2. $B$ decomposes as a sum of minimal $*$-ideals $I_1 \oplus \ldots \oplus I_t$.

# The Structure of Matrix $*$-Algebras

Let $A$ be a $*$-subalgebra of $\mathbb{M}_d(\mathbb{F}_q)$, where $q$ is odd.

1. $J(A)$ is a $*$-ideal (it is invariant under $*$), and $A = J(A) \oplus B$, where $B$ is a $*$-invariant semisimple subring of $A$. (Taft)
2. $B$ decomposes as a sum of minimal $*$-ideals $I_1 \oplus \ldots \oplus I_t$.
3. Each $I_j$ is a simple $*$-ring, and is isomorphic to one of the following:
   - $\mathbb{M}_{e_j}(K_j)$ with symplectic involution; $I_j^\sharp \cong \mathrm{Sp}(e_j, K_j)$.
   - $\mathbb{M}_{e_j}(K_j)$ with unitary involution; $I_j^\sharp \cong \mathrm{GU}(e_j, K_j)$.
   - $\mathbb{M}_{e_j}(K_j)$ with orthogonal involution; $I_j^\sharp \cong \mathrm{GO}^\epsilon(e_j, K_j)$.
   - $\mathbb{M}_{e_j}(K_j) \oplus \mathbb{M}_{e_j}(K_j)$ with exchange involution interchanging the two factors; $I_j^\sharp \cong \mathrm{GL}(e_j, K_j)$.

# Algorithms for Matrix $*$-Algebras

## Theorem (B & Wilson, 2012)

*There is a Las Vegas, polynomial time algorithm which, given a $*$-subalgebra $A$ of $\mathbb{M}_d(\mathbb{F}_q)$, where $|\mathbb{F}_q|$ is odd, finds the following:*

1. *a ring decomposition $A = J(A) \oplus B$, where $B$ is semisimple and $*$-invariant (based on original proof of Taft);*
2. *a decomposition $B = I_1 \oplus \ldots \oplus I_t$ into minimal $*$-ideals; and*
3. *isomorphisms $\varphi_j \colon I_j \to S_j$, where $S_j$ is the standard copy of the appropriate simple $*$-ring.*

Implementations of the algorithms for algebras and $*$-algebras are distributed with MAGMA as part of the `StarAlgebras` package.

# Constructing Isom($\circ$)

- Our next goal is to construct $\mathrm{Isom}(\circ)$ for any Hermitian bimap $\circ$.
- The strategy is to use the known structure of $\mathrm{Adj}(\circ)$ as a $*$-algebra to extract its norm group $\mathrm{Adj}(\circ)^\sharp = \mathrm{Isom}(\circ)$.
- We have $A = J(A) \oplus (I_1 \oplus \ldots \oplus I_t)$ with each $I_j$ simple.
- Finding each $I_j^\sharp$ is easy: one simply writes down generators for the appropriate classical group.
- Building norm 1 elements from the radical is trickier...

# Building Unipotent Generators

- A standard trick to build elements in a group from nilpotent elements of an algebra is to exponentiate: if $z^{n+1} = 0$, put

$$u = e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \ldots + \frac{z^n}{n!},$$

but this puts undesirable constraints on the characteristic of $\mathbb{F}_q$.

# Building Unipotent Generators

- A standard trick to build elements in a group from nilpotent elements of an algebra is to exponentiate: if $z^{n+1} = 0$, put

$$u = e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \ldots + \frac{z^n}{n!},$$

  but this puts undesirable constraints on the characteristic of $\mathbb{F}_q$.
- Instead, we use a different power series, namely for $z + \sqrt{1 + z^2}$.
- Put $J^- = \{z \in J(A) : z^* = -z\}$. Then,

$$J(A)^\sharp = \{z + \sqrt{1 + z^2} : z \in J^-\}.$$

# Results

**Theorem (B & Wilson, 2012)**

*There is a Las Vegas, polynomial time algorithm which, given an Hermitian bimap* $\circ : V \times V \to W$, *with* $|V|$ *and* $|W|$ *odd, constructs generators for, and explicitly determines the structure of* $\mathrm{Isom}(\circ)$.

# Results

## Theorem (B & Wilson, 2012)

*There is a Las Vegas, polynomial time algorithm which, given an Hermitian bimap* $\circ\colon V \times V \to W$*, with* $|V|$ *and* $|W|$ *odd, constructs generators for, and explicitly determines the structure of* $\mathrm{Isom}(\circ)$.

## Corollary

*There is a Las Vegas, polynomial time algorithm which, given a set of classical groups* $H_1, \ldots, H_n$ *defined on a common vector space of odd order, constructs a generating set for the intersection* $H_1 \cap \ldots \cap H_n$.

# Results

## Theorem (B & Wilson, 2012)

*There is a Las Vegas, polynomial time algorithm which, given an Hermitian bimap* $\circ\colon V \times V \to W$*, with* $|V|$ *and* $|W|$ *odd, constructs generators for, and explicitly determines the structure of* $\mathrm{Isom}(\circ)$.

## Corollary

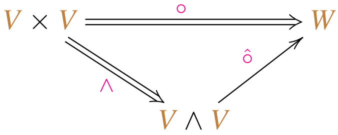
*There is a Las Vegas, polynomial time algorithm which, given a set of classical groups* $H_1, \ldots, H_n$ *defined on a common vector space of odd order, constructs a generating set for the intersection* $H_1 \cap \ldots \cap H_n$.

## Corollary

*There is a Las Vegas algorithm which, given a p-group* $G$ *of class 2 and exponent p* ($p > 2$)*, constructs the characteristic subgroup of* $\mathrm{Aut}(G)$ *consisting of automorphisms which centralize* $[G, G]$.

# Better Than Brute Force!

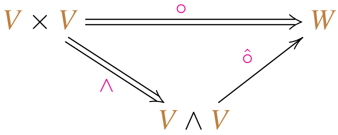
Recall that our principal objective is to construct $\Psi\mathrm{Isom}(\circ)$ for an alternating bimap $\circ$. A description of this group which is anything like as nice as $\mathrm{Isom}(\circ)$ has so far eluded us. Recall the situation:



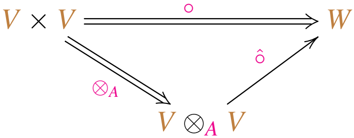

The orbit of $\ker \hat{\circ}$ is usually to large to list.

# Better Than Brute Force!

Recall that our principal objective is to construct $\Psi\mathrm{Isom}(\circ)$ for an alternating bimap $\circ$. A description of this group which is anything like as nice as $\mathrm{Isom}(\circ)$ has so far eluded us. Recall the situation:




The orbit of $\ker \hat{\circ}$ is usually to large to list. If $A = \mathrm{Adj}(\circ)$, then




In many situations $V \otimes_A V$ is of significantly smaller dimension than $V \wedge V$, the group that acts, namely $\Psi\mathrm{Isom}(\otimes_A)$, is much smaller than $\mathrm{Aut}(V)$, and we can construct this group [B-Wilson, 2012+].

# Work in Progress

The strategy just outlined works really well in certain situations.

## Theorem (B & Wilson, 2012+)

*There is an efficient algorithm which, given an alternating bimap* $\circ : V \times V \to \mathbb{F}_q^2$, *$q$ odd, constructs generators for* $\Psi\mathrm{Isom}(\circ)$.

Thus, if a $p$-group $G$ of exponent $p$ and class 2 has co-rank 2 then we can determine $\mathrm{Aut}(G)$ efficiently.

# Work in Progress

The strategy just outlined works really well in certain situations.

## Theorem (B & Wilson, 2012+)

*There is an efficient algorithm which, given an alternating bimap* $\circ : V \times V \to \mathbb{F}_q^2$*, q odd, constructs generators for* $\Psi\mathrm{Isom}(\circ)$.

Thus, if a $p$-group $G$ of exponent $p$ and class 2 has co-rank 2 then we can determine $\mathrm{Aut}(G)$ efficiently.

There is a comprehensive strategy to attack $\Psi\mathrm{Isom}(\circ)$ for arbitrary alternating $\circ$ using a mélange of linear and combinatorial methods. [B-O'Brien-Wilson, 201?]