Group Isomorphism is tied up in knots.

James B. Wilson
Colorado State University

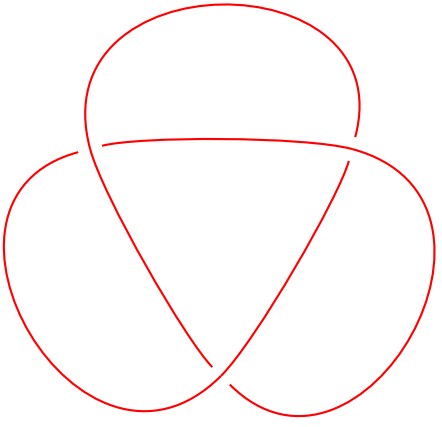
Some tapas of group isomorphism

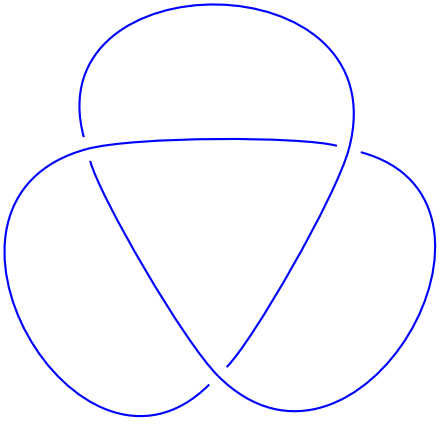
(1) An historic introduction.
(2) How to input groups and the effect on the complexity.
(3) Undecideable cases: when it happens and how to avoid it.
(4) Group isomorphism is hard, but not uniformly hard.
(5) Lessons from counting isomorphism classes.
(6) Modern algorithms.
(7) The main obstruction.
(8) Filters – a flexible way to mingle strategies.
(9) Locating new structure to break up the problem.
(10) Open problems.

An historic introduction.

(List – Next)

Early history of group isomorphism





$\stackrel{?}{=}$

Theorem (Dehn 1909). The closed knot tied under-over cannot be deformed continuously to the closed knot tied over-under.

Proof. A continuous deformation of one knot K_1 to another K_2 will make an orientation preserving isomorphism of the two knot groups $G_i = \{[S^1 \to \mathbb{R}^3 \backslash K_i]\}$.

The knot groups are generated by two loops: one wrapped over a single string, the second weaved through the knot.

Bummer: $G_1 \cong G_2$.

But wait! The obvious isomorphism is orientation reversing.

There are infinitely many isomorphisms to check. Instead, compute a finite generating set of the automorphism group. These all preserve orientation.

All isomorphisms between G_1 and G_2 are orientation reversing. $\square$

Moral: Group isomorphism is a powerful calculation capable of describing huge diversity between objects in a humble set of generators.

The Group Isomorphism Problem (Dehn 1911).
Is this calculation actually possible?

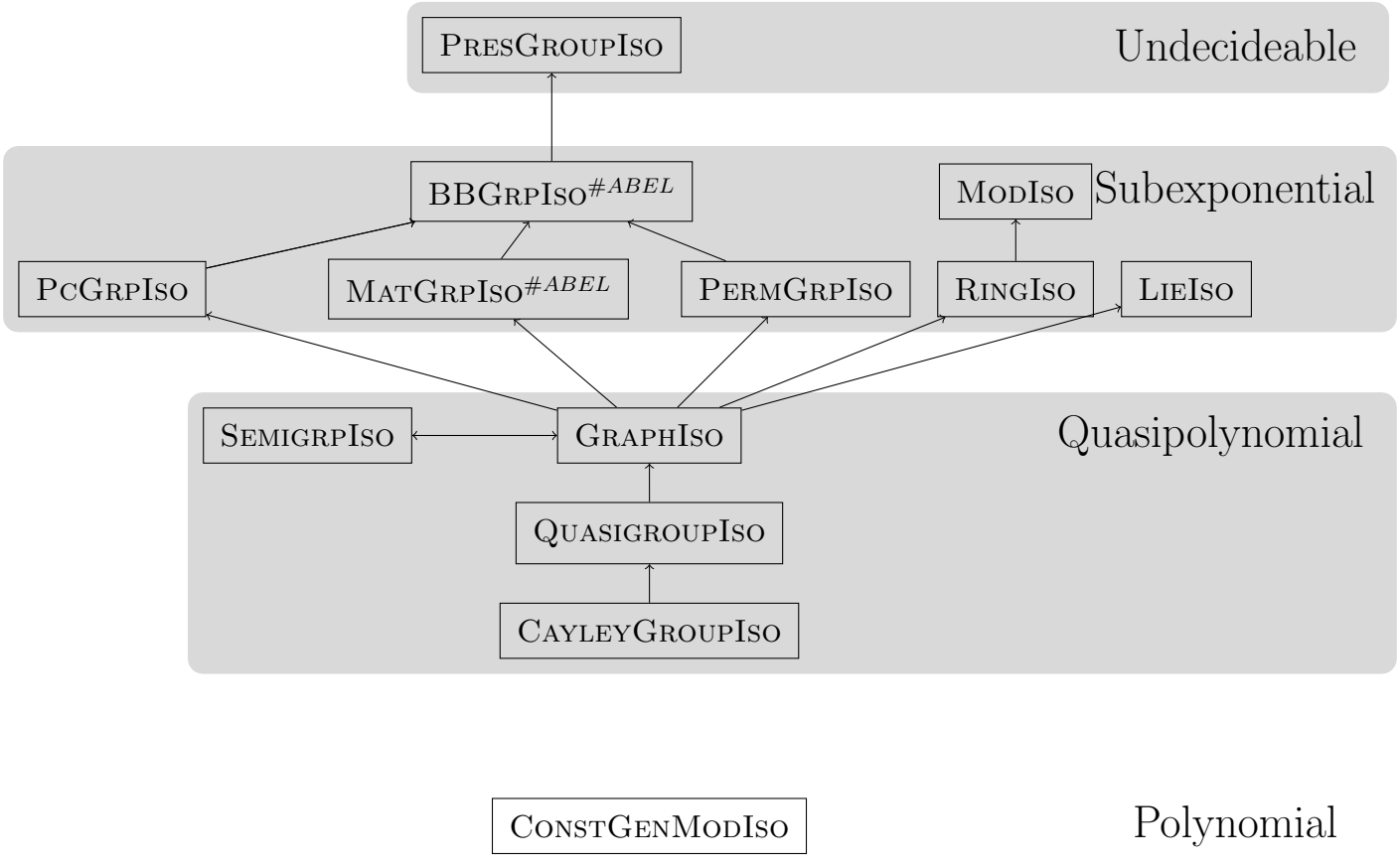
How to input groups and the effect on the complexity.

(Previous – List – Next)

Sensible input models for groups vary greatly.

- A generating set of functions (permutaitons or matrices).
  E.g. problems of symmetry in combinatorics, geometry and molecular models.
- Products on equivalence classes (black-box).
  E.g. fundamental groups, points on elliptic curve.
- Formal generators and relations (presentation).
  E.g. classification projects, building counter-examples from required properties.
- Geometry with group coordinates (Cayley table).
  E.g. Moufang sets related by triality to a group, Kantor families, Difference sets, etc.

Complexity of Isomorphism problems in algebra.



A second look at Group Iso complexity

- Complexity is as a function of input size.
- The same problem input another way has a different complexity ON THE SAME ALGORITHM.
- How can we judge improvement? Will some data structures over measureable advantages?

Options (with Brooksbank-Miyazaki)

- Time against Kolmogorov complexity $t = t(G)$ of input of a group G.
  Thm. $t \in \Theta((\log |G|)^3)$.
  (Uniform, but loose any use of data structure.)

- **Fact.** NP problems have canonical brute-force (exhaust certificates).
  Improve the ratio to canonical brute-force.

Undecideable cases: when it happens and how to avoid it.

(Previous – List – Next)

Adian 1955, Rabin 1957. Group isomorphism for groups given as

$$G = \langle x_1, \ldots, x_n | r_1, \ldots, r_m \rangle$$

is undecidable.[1]

Proof. Novikov '52/Boone '54 create groups $G_0 = \langle \mathtt{X} | \mathtt{R} \rangle$ and a word w such that $w \equiv 1$ in G_0 is undecidable.

Rabin: for every such w there is a group $T(G, w)$ where $w \equiv 1$ in G implies $T \cong 1$; otherwise $G \hookrightarrow T$.

Let $H = \langle \mathtt{Y} | \mathtt{S} \rangle \ncong 1$. Set

$$G = T(H * G_0, w).$$

If $w \equiv 1$ in G_0 then $G \cong 1$; else, $1 \neq H \leq H * G_0 \leq G$. So $w \equiv 1$ in G_0 iff $G \cong 1$. We cannot decide this.

Also, for any group K,

$$K * G \cong K \Leftrightarrow G \cong 1.$$

So $(K, K*G)$ is a pair for which group isomorphism is undecideable. □

[1] $\mathtt{IsIso}(G, H)$ modeled as $f : \mathbb{N} \to \{0, 1\}$ is non-recursive. Recursive is rare – their are only countably many programs; yet, $2^{\mathbb{N}}$ is uncountable.

Ouch. Cannot decide if groups are finite, abelian, solvable, or indecomposable.

Proof. Fix a property $\mathcal{P}$ that transfers to all subgroups (e.g. trivial, finite, abelian solvable, etc.). Let H and K be groups, H with $\mathcal{P}$ and K without. Set

$$G = H * T(K * G_0, w).$$

Cannot decide $\mathcal{P}$ for G.

If H be directly indecomposable and G a group that we cannot decide is trivial. Then cannot decide if $H \times G$ is indecomposable. □

Outside of algebra. Cannot decide if spaces are homotopic.

Proof. Consider Ellenberg-MacLane spaces. □

Reality check.

- Groups you find come with more than $\langle \mathtt{X} | \mathtt{R} \rangle$.
- Gromov style "random" groups $\langle \mathtt{X} | \mathtt{R} \rangle$ have a solvable word problem (they are hyperbolic.)
- Rabin. Isomorphism types are recursively enumerable.

Moral: Ask the question where at least brute-force exists.

Enumerable Group Isomorphism (EGI): Given two *enumerable* groups, how hard is it to solve group isomorphism?

Isomorphism testing is not uniformly hard.

(Previous – List – Next)

Def. The *generator degree* of a group G is the cardinal:[2]

$$d(G) = \min\{|\mathtt{X}| : G = \langle \mathtt{X} \rangle\}.$$

Fact. If $d(G) \neq |G|$ then $2^{d(G)} \leq |G| \leq \aleph_0$.

Fact. For enumerable groups G of size n brute-force isomorphism testing takes time $O(n^{d(G)})$, $d(G) \leq \log n$.

Proof. Homomorphisms

$$f : G = \langle \mathtt{X} \rangle \to H$$

are set $f : \mathtt{X} \to H$. So

$$|\hom(G, H)| \leq |H|^{d(X)}.$$

□

Open Problem.
Decide EGI in time better than brute-force.

Who opened this problem?
Cayley 1854, v. Dyck 1889, Felsch-Neubüser '68, Tarjan '7x, Miller '77, Lipton-Synder-Zalcstein '78.

Good questions should be asked more than once.

[2] If $\mathbb{Q} = \langle \mathtt{X} \rangle$, then $\forall x \in \mathtt{X}$, $\mathbb{Q} = \langle \mathtt{X} - \{x\} \rangle$. So $d(G)$ cannot be ordinal.

Isomorphism for unbiased order is usually easy!

Theorem. Hölder 1895.
Groups of square free order are $\mathbb{Z}_a \rtimes \mathbb{Z}_b$, $(a, b) = 1$.

Theorem. Slattery '04,
Groups of order $n = p_1 \cdots p_s$ have $O((\log n)^c)$-time isomorphism tests.*

Theorem. Dietrich-Eick 2005
Same for cube-free.*

*Needs oracle for factoring n.

Theorem (W.) $\forall \varepsilon > 0, \exists d$ such that group isomorphism can be decided in time $O(n^d)$ for a set of finite cardinals of density $(1 - \varepsilon)$.

(E.g. $O(n^8)$ covers 99.6% of all group orders.)

Proof. Guralnick '89, Luccchini 2000, show if $n = p_1^{e_1} \cdots p_s^{e_s}$, p_i prime, then

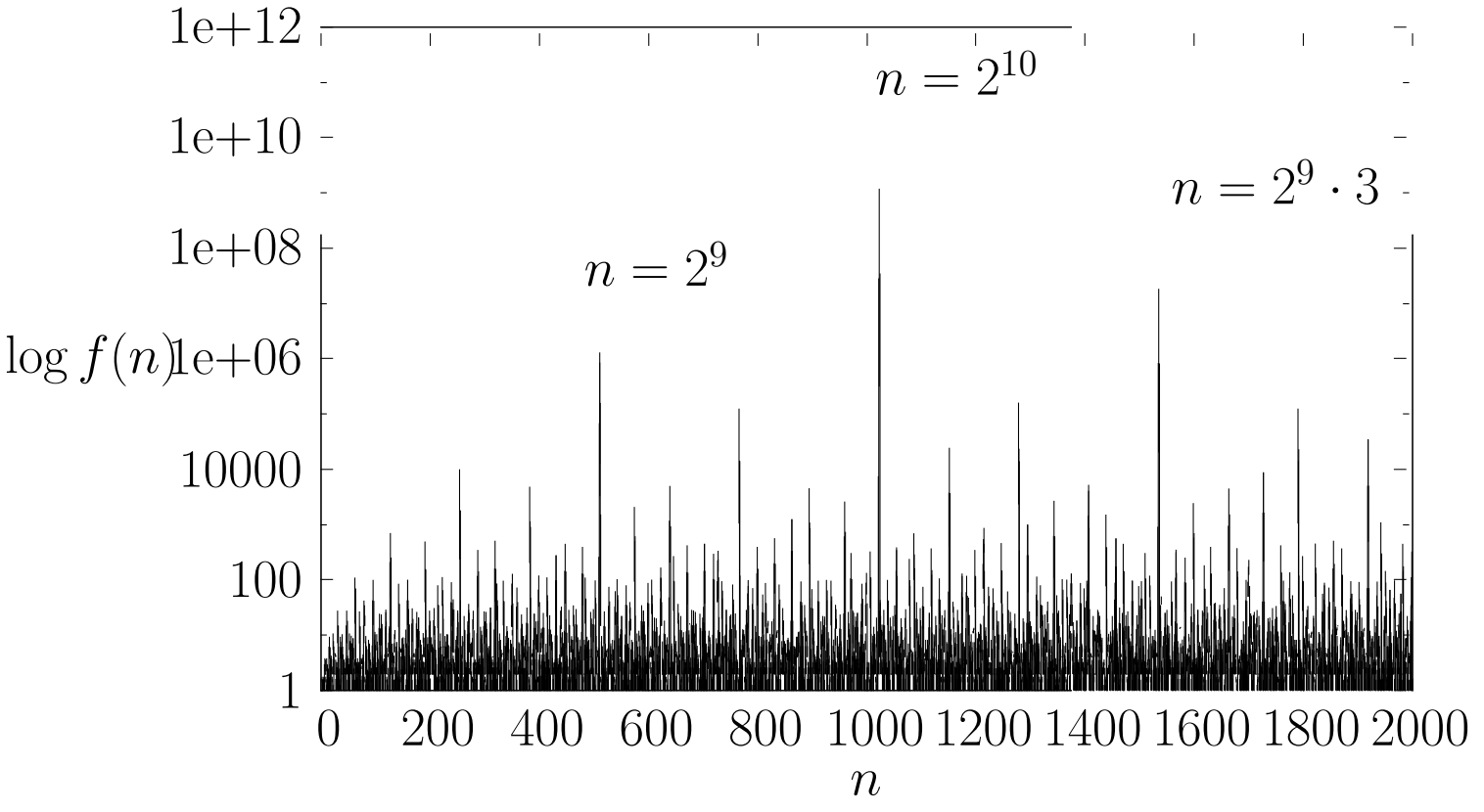
$$d(G) \leq \mu(N) := \max\{e_i\}.$$

The number of integers n with $\mu(n) < d$ tends to $1/\zeta(d)$. $\square$

Lessons from counting isomorphism classes.

(Previous – List – Next)

Besche-Eick-O'Brien 2000.



A log-scale plot of the number $f(n)$ of the groups of order n.

(Probably) most finite groups order 2^k, $2^k 3$, 3^k....

Conjecture. Erdős
Up to isomorphism most groups of size $\leq n$ have order 2^m.

Theorem. Higman 60; Sims 65
The number $f(p^m)$ of groups of order p^m is

$$p^{2m^3/27+\Omega(m^2)\cap O(m^{3-\epsilon})}$$

for a some $\epsilon > 0$.

Theorem. Pyber 93 The number $f(n)$ of groups order at n satisfies

$$f(n) \leq n^{2\mu(n)^2/27+D\mu(n)^{2-\epsilon}}.$$

Fact. The number of graphs on n vertices is

$$2^{\Theta(n^2)}.$$

Fact. The number of semigroups of order n vertices is

$$2^{\Theta(n^2 \log n)}.$$

Groups do not grow like combinatorics. The rare prime power sized sets are by far the most complex.

What grows like groups?

Theorem. Kruse-Price-70
The number of finite rings of order p^m is

$$p^{4m^3/27+\Omega(m^2)\cap O(m^{3-\epsilon})}$$

.

Theorem. Neretin-87
The dimension of the variety of algebras is

$$\frac{2}{27}n^3 + D_1 m^{3-\epsilon_1}$$

for commutative or Lie,

$$\frac{4}{27}m^3 + D_2 m^{3-\epsilon_2}$$

for associative.

Theorem. Poonen-08
The number of commutative rings of order p^m is

$$p^{2m^3/27+\Omega(m^2)\cap O(m^{3-\epsilon})}$$

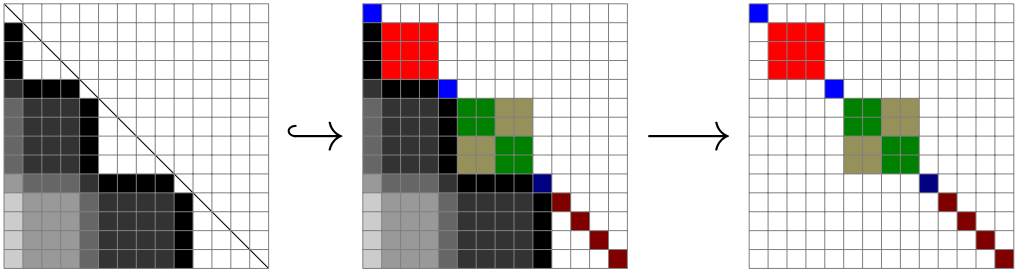
Why so similar to groups? Hint.
Groups have a second product

$$[x, y] = x^{-1}x^y = x^{-1}y^{-1}xy$$

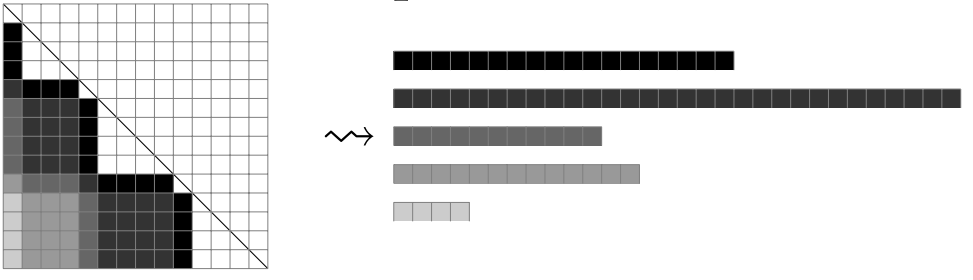
and it nearly distributes:

$$[xy, z] = [x, z]^y[y, z].$$

Step one: separate nilpotent from reductive

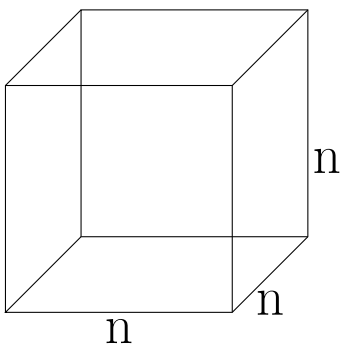


Step two: Break nilpotent into abelian sections



Where is the complexity in "triangular matrices"?

A. Nonassociative products need 3-dimensional array of parameters. Entropy of $\Theta(m^3)$.

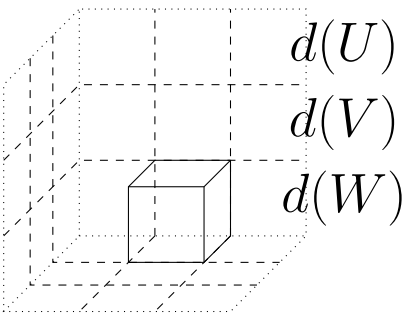


B. Matrix type groups

$$\begin{bmatrix} s & u & w \\ 0 & s & v \\ 0 & 0 & s \end{bmatrix} \begin{bmatrix} s' & u' & w' \\ 0 & s' & v' \\ 0 & 0 & s' \end{bmatrix} =$$

$$\begin{bmatrix} ss' & us'+su' & ws'+u*v'+sw' \\ 0 & ss' & vs'+sv' \\ 0 & 0 & ss' \end{bmatrix}$$

need only $* : U \times V \rightarrowtail W$.

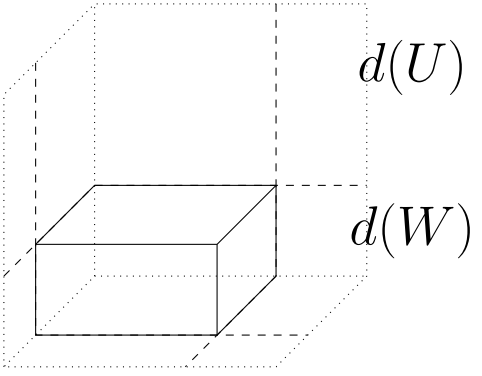


$$d(U)d(V)d(W) \leq m^3/27$$

C. Cut to diagonal embedding

$$\left\{ \begin{bmatrix} s & u & w \\ 0 & s & \pm u\theta \\ 0 & 0 & s \end{bmatrix} : \begin{array}{c} u \in U, \\ w \in W \end{array} \right\}$$

now use $* : U \times U \rightarrowtail W$.



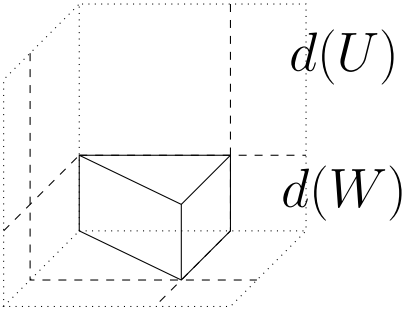
$$d(U)^2(m - d(U)) \leq 4m^3/27.$$

D. Add symmetry

$$\left\{ \begin{bmatrix} s & u & w \\ 0 & s & \pm u\theta \\ 0 & 0 & s \end{bmatrix} : u \in U, w \in W \right\}$$

need $\pm\theta$-Hermitian

$$* : U \times U \rightarrowtail W.$$



$$\tfrac{1}{2}d(U)^2(n - d(U)) \leq 2n^3/27.$$

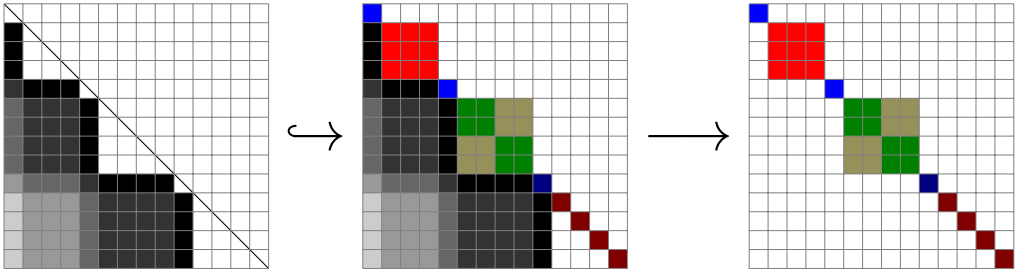
Moral: Isomorphism of your groups might be easy. But most groups are made the same way as rings and algebras. It is all about bilinear maps $* : U \times V \rightarrowtail W$ and the Hermitian ones.

Open problem: Decide if two bimaps are isotopic/pseudo-isometric.

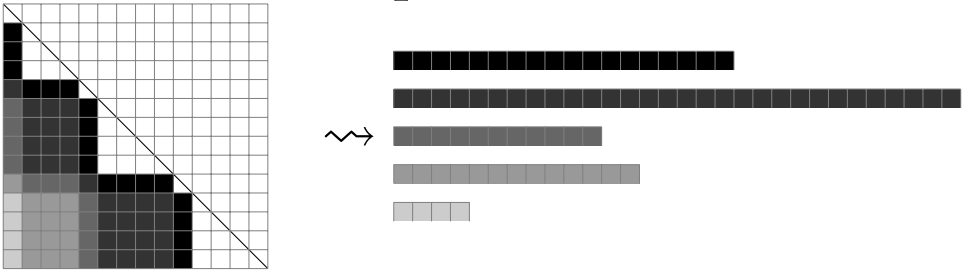
Modern algorithms

(Previous – List – Next)

Recall all group break up something like this...



Step two: Break nilpotent into abelian sections

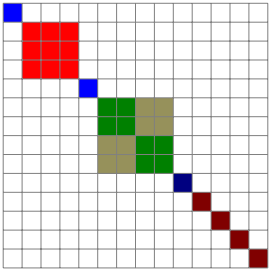


Modern algorithms work by...

(1) Decide on bases case with special strategies, e.g. abelian groups, simple groups.
(2) Describe the cohomology of the extension.
(3) Recursively compute the isomorphisms of the quotient and subgroup of the extension
(4) Search both sets for compatible pairs.
(5) That action can be recored as a group acting on subsets of vector space

Brutal summary of delicate work of Higman, Cannon, Newmann, Robinson, O'Brien, Leedham-Green, Eick, Holt, and others.

What about these as a base case?



(Grochow-Qiao) The reductive case

Theorem. Babai-Codenotti-Qiao
Groups with no radical have an $O(n^c)$ isomorphism-test.

Proof. Fitting, Beals-Babai give structure theorem. Here groups are products of simples extended by outer automorphisms and permutations.

Simples benefit from classification. The rest lends itself to a problem of nonabelian code-equivalence. A small one compared to the size of the group. Dynamic programming is enough umph. □

Theorem. Grochow-Qiao
Groups with abelian radical have an $O(n^{\log\log n})$ isomorphism-test.

Proof. Nonabelian group cohomology bounds reduce to a code equivalence problem of smaller size. □

The main bottleneck

(Previous – List – Next)

Many have wondered if these methods reduce isomorphism testing to p-groups.
I don't believe that they do, but already they leave use with one simple to state problem.

Thm. Cayley group isomorphism reduces to subspace transporter (general module isomorphism) in polynomial time.

Conjecture. This is true also for permutation groups.

How hard could that be?

Thm. Most (a proportion tending to 1) of all group isomorphism instances for groups of size at most n take time

$$2^{2/9\mu(n)^2+O(\mu(n))}$$

(and by current methods this is also a lower bound).

Proof. $d = d(G) = 2\mu(n)/3$ maximize the number of d-generated groups of order n. The asymptotic is exponential so it has proportion $\to 1$ as $n \to \infty$. The subspace transporter problem has $\mathrm{GL}(d,2)$ acting on subspaces of $\mathbb{Z}_2^{d^2/2}$. By LU-decomposition listing this takes time $\sqrt{|\mathrm{GL}(d,2)|}$. $\square$

Filters, a flexible way to mingle ideas.

(Previous – List – Next)

Filters (with Maglione)

M a monoid.

$$\phi : M \to 2^G$$

$$[\phi_s, \phi_t] \leq \phi_{s+t} \leq \phi_s \cap \phi_t.$$

Thm [W.] Every filter determines a Lie algebra

$$L(\phi) = \bigoplus_{s \neq 0} \phi_s / \partial\phi_s$$

$\partial\phi_s = \langle \phi_{s+t} : t \neq 0 \rangle$.

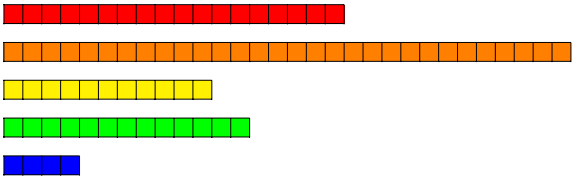
E.g. Lower central series determines the usual Lie algebra.

Thm [W.] Under suitable hypothesis, given a filter $\phi : M \to 2^G$ and normals subgroups $\{N_1, \ldots, N_t\}$, there is a unique filter $M \times \mathbb{N} \to 2^G$ generated by these groups.

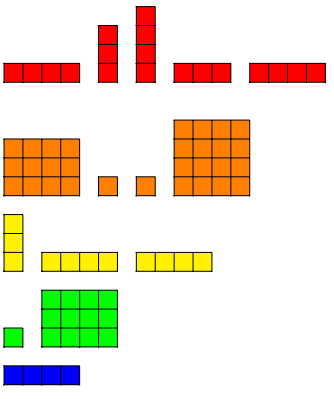
Filters can be updated as often as we like, even on the fly, and they keep a Lie algebra (linear algebra).

$$G = \langle a_1, \ldots, a_{76} : [a_1, a_2] = a_3^* \cdots a_{76}^*, \ldots, a_1^p = a_2^* \cdots a_{76}^*, \ldots \rangle$$

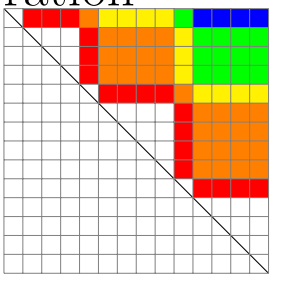
Naive lower central series.



Refinement breaks into smaller and structured parts.



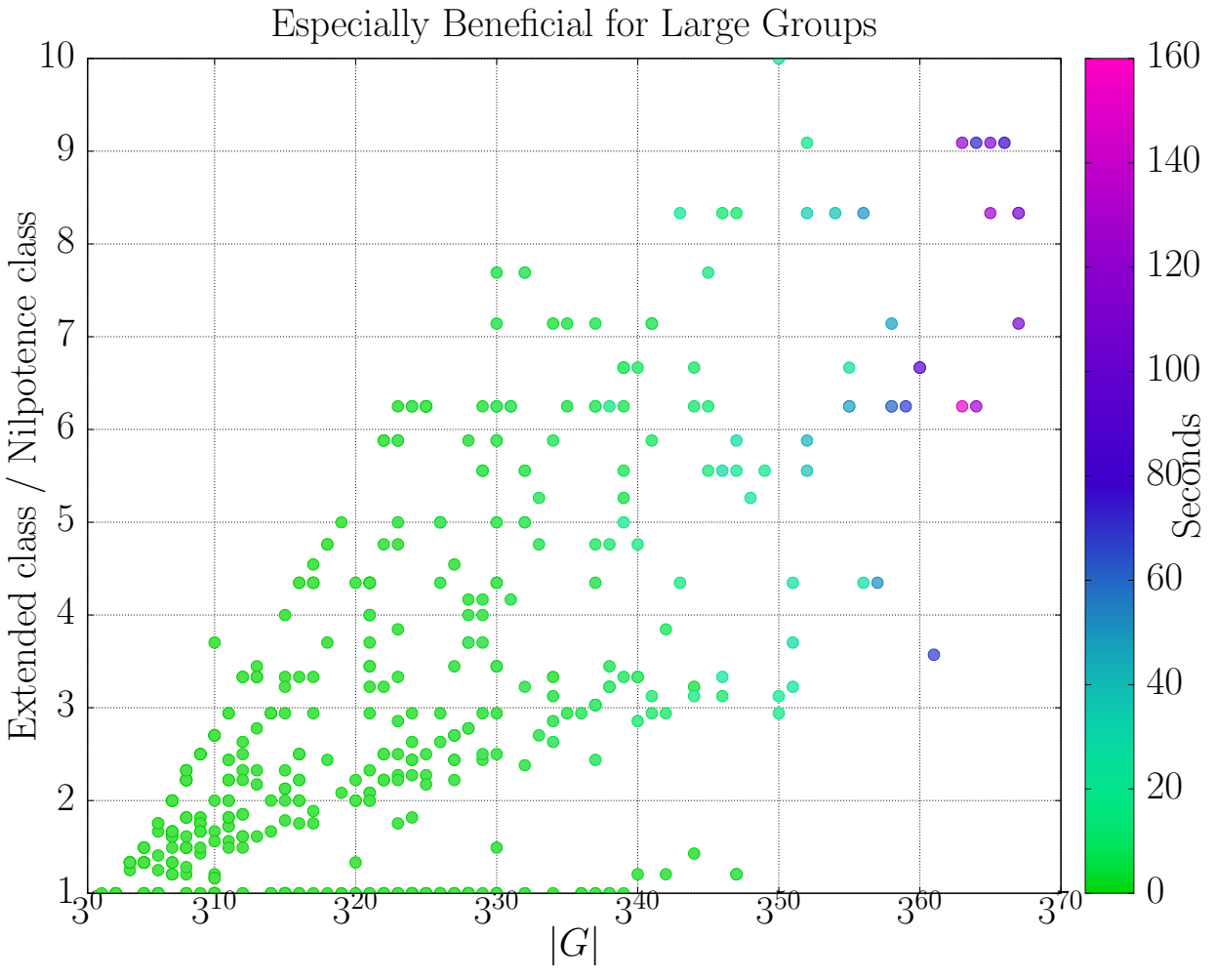
Rediscovered "matrix" configuration



Theorem. W.
A positive logarithmic proportion of all finite groups admit proper refinements.

Theorem. Maglione
There is a polynomial-time algorithm to compute this filter.

Survey. Maglione-W.
Of the 11 million groups of order $\leq$ 1000, over 81% admit a proper decomposition by the refinements we know so far.


Especially Beneficial for Large Groups
Extended class / Nilpotence class
10
9
8
7
6
5
4
3
2
1
3^{0}
3^{10}
3^{20}
3^{30}
3^{40}
3^{50}
3^{60}
3^{70}
$|G|$
Seconds
160
140
120
100
80
60
40
20
0

Refining filters.

(Previous – List – Next)

(Brooksbank-W.) The adjoint-tensor attack

Theorem. W.-Lewis.
Quotients of Heisenberg groups over fields have $O((\log n)^6)$-time isomorphism tests, this despite having no known group theoretic differences.

Theorem. Brooksbank-W.
Central products of quotients of Heisenberg groups over cyclic rings have $O((\log n)^6)$-time isomorphism tests.

In both cases these handle p^{cm^2} many groups.

Proof. Fix $* : U \times V \rightarrowtail W$.

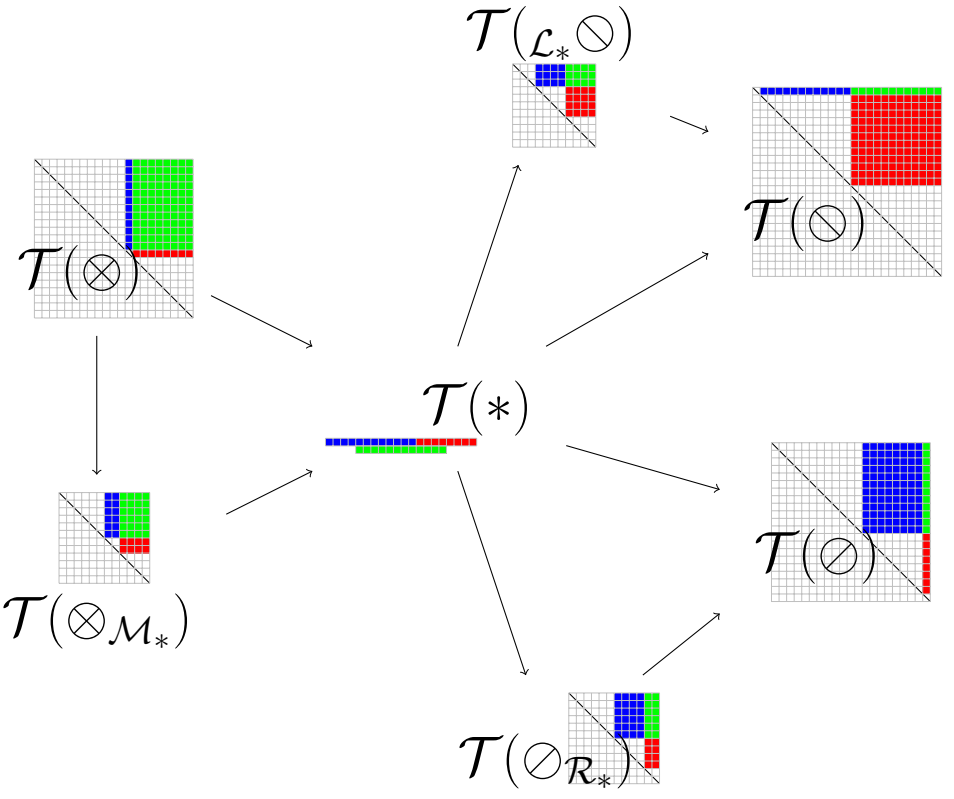
$\mathcal{M}_* = \{(f, g) : uf*v = u*gv\}$.

Fact. $*$ factors through $\otimes_{\mathcal{M}_*}$ and this is the smallest possible tensor product for $*$.

$\mathrm{Aut}(*)$ is a stabilizer in $\mathrm{Aut}(\otimes_{\mathcal{M}_*})$ and $\mathrm{Aut}(\otimes_{\mathcal{M}_*})$ is the normalizer of $\mathcal{M}_*$.

If the rings $\mathcal{M}_*$ are semisimple then computed efficiently. $\square$

(W.) Triality attack.



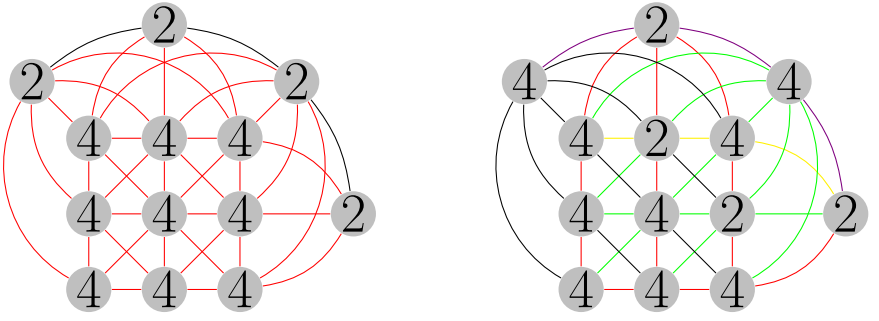
Theorem. W.
Every group (and every ring/algebra) can be given a filter where the homogeneous products

$$* : H_i \times H_j \rightarrowtail H_{i+j}$$

each have $\mathcal{LMR}_*$ semisimple.

When linear algebra runs out. (with Brooksbank-O'Brien)

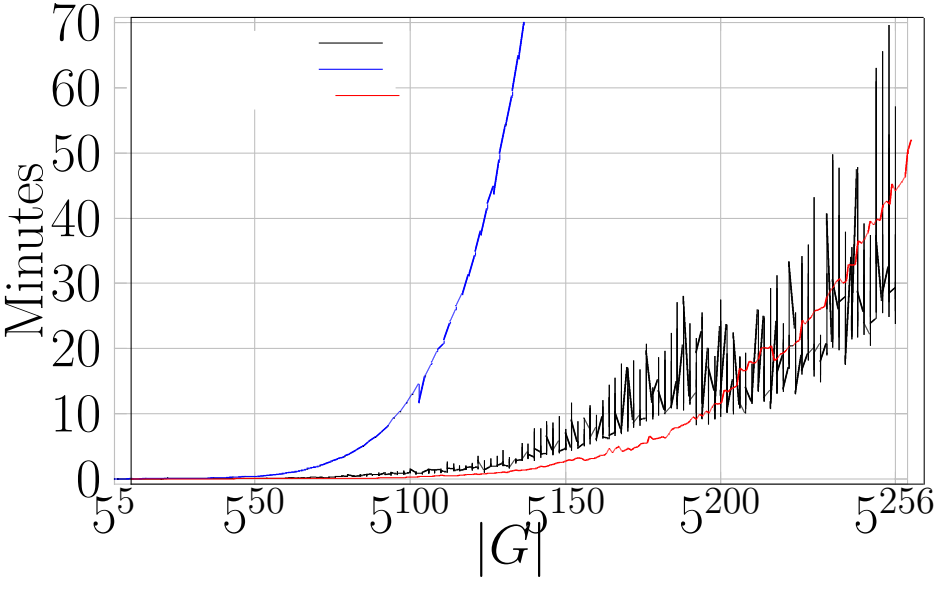
Label and color the projective geometry of the search space with tensor invariants. Perform a graph isomorphism computation.



(1) No isomorphism as graphs implies no isomorphism as groups.
(2) Yes isomorphism, then build orbits to create a new refinement.
(3) Left with primitive case.

Where to get the labels

Theorem. Brooksbank-Malgione-W.
Quadratic time isomorphism of groups of genus 2!



Competes in real life with the speed of matrix multiplication... in fact it went so fast our test could handle groups bigger than Magma could allow.

Open problems.

(Previous – List –)

(1) Find an isomorphism test that improves on brute force, in any input model. "Improve" ideally means a double log scale has 0 ratio.
(2) Describe what oracles you would need to add to permutation groups so that if Caley Group iso is in P then so is permutation group iso subject to the oracles. As a guess: add integer factorization, discrete log, and graph isomorphism on $O(\log n)$ sized graphs.
(3) Solve subspace transporter efficiently.
(4) Build invariants to the subspace transporter problems not related to tensors.
(5) Prove a dichotemy theorem for primitive case of the Brooksbank-O'Brien-W. method.