

# Unique decompositions of large unipotent groups

James B. Wilson

The Ohio State University

July 2009

# What is $\text{Aut } P$ ?

$$P = \left\{ \begin{bmatrix} 1 & . & a & b & c & d & e & f & g & h \\ . & 1 & b\omega & a & i & j & k & l & m & n \\ . & . & 1 & . & . & . & o & p' & . & . \\ . & . & . & 1 & . & . & p'\omega & o & . & . \\ . & . & . & . & 1 & . & . & . & q & . \\ . & . & . & . & . & 1 & . & . & . & q\omega \\ . & . & . & . & . & . & 1 & . & . & . \\ . & . & . & . & . & . & . & 1 & . & . \\ . & . & . & . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & . & . & . & 1 \end{bmatrix} \in \text{GL}(10, p) \right\}.$$

# Motivation: group isomorphism.

## Folklore

$\text{GroupIsomorphism} \leq_P \text{GraphIsomorphism}$

- As a complexity problem,  $\text{GroupIsomorphism}$  assumes as input the Cayley table for the group!
- Some hope one or both of these problems is not in  $P$  ( $\Rightarrow P \neq NP$ ).

## Babai (private communication)

$\text{GroupIsomorphism} \leq_P \text{GroupAutomorphism}$

# $N^{\log N}$ -problems

## The Tarjan-Miller test

If every object  $G$  in a concrete category  $\mathcal{C}$  can be generated by a subset  $S$  of size  $f(|G|)$ , then isomorphism testing in  $\mathcal{C}$  uses at most  $|G|^{f(|G|)+O(1)}$  steps, (also applies to generating  $\text{Aut } G$ ).

**Proof:** Compare all  $f(|G|)$ -tuples in one object to those in the other.  $\square$

## Corollary

Isomorphism testing of groups of order  $N$  requires at most  $N^{\log N+O(1)}$  steps.

# A broad view of group isomorphism schemes

[Besche, Eick, Havas, Holt, Leedham-Green, Newman, O'Brien, et.al.] (Now assume as input generators, not a Cayley table.)

- 1 Construct a characteristic subgroup  $N$  of  $G$ .
- 2 Recursively compute  $\text{Aut}(G/N)$  (and sometimes  $\text{Aut}(N)$ ).
- 3 Create  $\text{Aut}(G)$  from  $\text{Aut}(G/N)$ 
  - A. Look at orbits of  $\text{Aut}(N) \times \text{Aut}(G/N)$  on appropriate cohomology groups.
  - B. Write  $G = G^*/M$  and describe an action of  $\text{Aut}(G/N)$  on  $G^*$ . Find the stabilizer in  $\text{Aut}(G/N)$  of  $N/M$ .
- 4 Base cases
  - A.  $G$  is a semi-almost-quasi-umpa-lumpa-simple group. (Done; thank you all).
  - B.  $G$  elementary abelian (Done; thank you Gauss).

# Complexity and real-life experience.

- Polynomial-time if orbits in the cohomology and/or stabilizer domains are bounded.
- That requires at least that  $O_\infty(G)$  have a characteristic series whose factors have bounded size (bounded ranks are not usually enough).
- For groups of order  $p^n$  (without nice structure) leads to listing orbits of size

$$p^{\binom{n-o(1)}{2}} \in p^{\frac{n^2}{2}+O(1)} = N^{1/2 \cdot \log N + O(1)}, \quad N = p^n.$$

# Why might this always be hard?

- (Heinken-Leibeck) Every group can be a quotient of the automorphism group by its central automorphisms.
- Every linear group can be the quotient of  $\text{Aut } P$  for some  $P$  (i.e., acts on  $P/\Phi(P)$  as a prescribed linear group.
- (Higman, Sims, Pyber) Most groups are likely to be  $p$ -groups, so if  $p$ -groups are hard then on average group isomorphism is hard.

# How to go further

- P. Hall's influence is to study **vertical** decompositions:  
$$P = P_1 \geq P_2 \geq P_3 \geq \dots$$
- We get stuck when there are no long chains of characteristic subgroups (class 2 groups for example).
- Why not consider O. Hölder's ideas and study **horizontal** decompositions  $P = P_1 P_2 P_3 \dots$ ?

# Issues with horizontal decompositions.

- 1 Can we actually find them?
- 2 Which ones are unique?
- 3 What does this leave as a new base case?

Our main results begin to handle some of these issues.

# Direct product theorems.

## Theorem (W. 2008)

There is a polynomial-time algorithm which returns a Remak decomposition of  $G$ , i.e. a direct product decomposition of maximum size.

## Theorem (Wedderburn 1905, Remak 1911, Schmidt 1913)

Remak decompositions of finite groups are conjugate in  $G \rtimes C_{\text{Aut } G}(\text{Inn } G)$ .

(The uniqueness proof is algorithmic.)

# How often do we encounter a directly indecomposable?

## Theorem (Higman)

There  $p^{2n^3/27+O(n^2)}$  groups of order  $p^n$  and class 2.

## Theorem (W. 2008)

- There are  $p^{2n^3/27+O(n^2)}$  directly **decomposable** groups of order  $p^n$  and class 2 (obvious, e.g.  $Q \times \mathbb{Z}_p$  with  $|Q| = p^{n-1}$ ).
- There are  $p^{2n^3/27+O(n^2)}$  directly **indecomposable** groups of order  $p^n$  and class 2 (not that obvious).

Individually each is insightful, together they are meaningless.

## For the remainder please assume:

- Let  $p > 2$  and  $P \leq \mathrm{GL}(d, p)$  be a unipotent group with  $P' \leq Z(P)$ .
- Alternatively, allow any  $p$ -group of class 2 and phrase the theorems up to *isoclinism*.
- Watch for the role of

$$\mathrm{Inn} P \leq C_{\mathrm{Aut} P}(Z(P)) \leq \mathrm{Aut} P.$$

# Coordinatization type theorems

## Theorem (W. 2007)

There is a polynomial-time algorithm which returns a fully refined central decomposition of  $P$  which also identifies its semi-refinement and the types of of the centrally indecomposable factors.

## Theorem (W. 2007)

Semi-refined central decompositions of  $P$  are conjugate in  $P \rtimes C_{\text{Aut } G}(Z(P))$ .

# Base cases: centrally indecomposables

## Theorem (W. 2007)

The sets of centrally decomposable and indecomposable groups of order  $p^n$  have size  $p^{2n^3/27+O(n^2)}$ .

There are four families of centrally indecomposables: if

$$G = C_{\text{Aut } P}(Z(P))/O_p(C_{\text{Aut } P}(Z(P))), \text{ then we have}$$

- 1 Orthogonal type  $G \cong O(1, p^e)$ ,
- 2 Unitary type  $G \cong U(1, p^e)$ ,
- 3 Exchange type  $G \cong GL(1, p^e)$ , and
- 4 Symplectic type  $G \cong Sp(2, p^e)$ .

# Wedderburn-Artin type theorems for $p$ -groups

Theorem I (W. 2009).

If

$$R(P) = \{x \in P : \forall \varphi \in O_p(C_{\text{Aut } P}(Z(P))), x\varphi \equiv x \pmod{Z(P)}\};$$

then there exists  $[R(P), P] \leq A \leq R(P)$  and  $Q \leq P$  such that

- 1  $R(P) = A \times Z(Q)$ ,
- 2  $R(Q) = Z(Q)$ , and
- 3  $P = A \rtimes Q$ .

Finally, all such  $(A, Q)$  are conjugate in  $P \rtimes O_p(C_{\text{Aut } P}(Z(P)))$ .

$C_{\text{Aut } P}(Z(P))$  is enormously informative, yet tractible

Theorem [Brooksbank-W. 2009]

There is a Las Vegas polynomial-time algorithm which returns generators for  $C_{\text{Aut } P}(Z(P))$ . Furthermore, the generators exhibit the following structure:

$$O_p(C_{\text{Aut } P}(Z(P))) \rtimes (G_1 \times \cdots \times G_t)$$

with  $G_i$  a classical group for all  $1 \leq i \leq t$ .

# Case study

$$P = \left\{ \begin{bmatrix} 1 & . & a & b & c & d & e & f & g & h \\ . & 1 & b\omega & a & i & j & k & l & m & n \\ . & . & 1 & . & . & . & o & p' & . & . \\ . & . & . & 1 & . & . & p'\omega & o & . & . \\ . & . & . & . & 1 & . & . & . & q & . \\ . & . & . & . & . & 1 & . & . & . & q\omega \\ . & . & . & . & . & . & 1 & . & . & . \\ . & . & . & . & . & . & . & 1 & . & . \\ . & . & . & . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & . & . & . & 1 \end{bmatrix} \in \text{GL}(10, p) \right\}.$$

# Linearize via bimap $\text{Bi}(P)$ of commutation in $P$

$b = \text{Bi}(P) : P/Z(P) \times P/Z(P) \rightarrow P'$  where  $b(u, v) = uBv^t$  and

$$B = \begin{matrix} \hat{a} \\ \hat{b} \\ \hat{c} \\ \hat{d} \\ \hat{i} \\ \hat{j} \\ \hat{o} \\ \hat{p}' \\ \hat{q} \end{matrix} \begin{bmatrix} 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \hat{e} & \hat{f} & \cdot \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot & \hat{f} & \omega\hat{e} & \cdot \\ \cdot & \cdot & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \hat{g} \\ \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & \cdot & \omega\hat{h} \\ \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & \hat{m} \\ \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \omega\hat{n} \\ -\hat{e} & -\hat{f} & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot \\ -\hat{f} & -\omega\hat{e} & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \cdot \\ \cdot & \cdot & -\hat{g} & -\omega\hat{h} & -\hat{m} & -\omega\hat{n} & \cdot & \cdot & 0 \end{bmatrix} .$$

( $\hat{a}$  is matrix in  $P$  and  $a = 1$  and all other variables set to 0.)

Compute the centroid  $C(\text{Bi}(P)) \cong GF(p^2) \oplus GF(p)$

$$C(\text{Bi}(P)) = \left\{ \begin{bmatrix} \alpha & \beta & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \beta\omega & \alpha & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \gamma & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \gamma & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \gamma & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \gamma & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha & \beta & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \beta\omega & \alpha & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \gamma \end{bmatrix} \in M_9(\mathbb{Z}_p) \right\}$$

Find a primitive idempotent of  
 $C(\text{Bi}(P)) \cong GF(p^2) \oplus GF(p)$

$$E = \begin{bmatrix} 1 & . & . & . & . & . & . & . & . \\ . & 1 & . & . & . & . & . & . & . \\ . & . & 0 & . & . & . & . & . & . \\ . & . & . & 0 & . & . & . & . & . \\ . & . & . & . & 0 & . & . & . & . \\ . & . & . & . & . & 0 & . & . & . \\ . & . & . & . & . & . & 1 & . & . \\ . & . & . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & . & . & 0 \end{bmatrix}$$

# Use the idempotent to define direct factors of $P$

$$P = P_E \oplus \mathbb{Z}_p^2 \oplus P_{1-E} = \left\{ \begin{bmatrix} 1 & . & a & b & c & d & e & f & g & h \\ & 1 & b\omega & a & i & j & k & l & m & n \\ & & 1 & . & . & . & o & p' & . & . \\ & & & 1 & . & . & p'\omega & o & . & . \\ & & & & 1 & . & . & . & . & . \\ & & & & & 1 & . & . & q & . \\ & & & & & & 1 & . & . & q\omega \\ & & & & & & & 1 & . & . \\ & & & & & & & & 1 & . \\ & & & & & & & & & 1 \end{bmatrix} \right\}.$$

## By product: extract scalars

- Note that  $EC(L(P))E = GF(p^2)$ .
- This indicates that  $P_E$  is a  $GF(p^2)$ -powered group, i.e.

$$P_E = (p^{1+2} \otimes GF(p^2)).$$

- So  $\text{Aut } P_E = \text{Sp}(2, p^2). \Gamma L(1, p^2)$ .

Also look at  $Q = P_{1-E}$  with other decompositions

- $O_p(C_{\text{Aut } Q}(Z(Q))) \neq 1$  and its fixed points give us:

$$Q = \mathbb{Z}_p^8 \rtimes \mathbb{Z}_p$$

- 

$$\text{Aut } Q = \mathbb{Z}_p^{20} \cdot \text{GL}(4, p) \cdot \Gamma L(1, p)$$

$$Q = P_{1-E} = \mathbb{Z}_p^8 \rtimes \mathbb{Z}_p = \left\{ \begin{bmatrix} 1 & & & & c & d & & & g & h \\ & 1 & & & i & j & & & m & n \\ & & 1 & & & & & & & \\ & & & 1 & & & & & & \\ & & & & 1 & & & & & \\ & & & & & 1 & & & q & \\ & & & & & & 1 & & & q\omega \\ & & & & & & & 1 & & \\ & & & & & & & & 1 & \\ & & & & & & & & & 1 \end{bmatrix} \right\}.$$

# Finally.



$$\text{Aut } P \cong \mathbb{Z}_p^e \cdot (\text{Sp}(2, p^2) \cdot \Gamma L(1, p^2) \times \text{GL}(4, p) \cdot \Gamma L(1, p)).$$

- Using these methods one can distinguish any group of class 2 and order  $p^6$  using linear algebra in  $\mathbb{Z}_p$ , i.e. in time  $O(\log p)$  (compared with  $p^{O(1)}$  methods).
- This scales well (has handled some  $p^{200}$ 's) but of course is not enough for all  $p$ -groups.
- I have similar results using Jordan pairs, associative pairs, and various Lie algebras. So more decompositions are out there.