THEORY OF COMPUTING, Volume 11 (15), 2015, pp. 395–401
www.theoryofcomputing.org

NOTE

Groups with Identical k-Profiles

George Glauberman   Łukasz Grabowski

Received June 16, 2013; Revised November 30, 2015; Published December 23, 2015

Abstract: We show that for $1 \le k \le \sqrt{2\log_3 n} - (5/2)$, the multiset of isomorphism types of k-generated subgroups does not determine a group of order at most n. This answers a question raised by Tim Gowers in connection with the Group Isomorphism problem.

ACM Classification: F.2.2

AMS Classification: 68Q17, 20D15, 20F69, 68Q25

Key words and phrases: group theory, nilpotent groups, p-groups, group isomorphism problem, algorithms, lower bounds, k-generated group, k-profile of groups

1 Introduction

We say that a group is k-generated if it has a set of at most k generators. Let $\mathcal{G}_k$ be the set of isomorphism types[1] of all k-generated finite groups. Let G be a finite group. Following Gowers [3], we say that the k-*profile* of G is the function $f_G : \mathcal{G}_k \to \mathbb{N}$ defined by letting $f_G(H)$ be the number of subgroups of G isomorphic to H ($H \in \mathcal{G}_k$).

Tim Gowers raised the question [3], for which k does the k-profile determine a group of order n? Such a k yields a simple isomorphism test[2] in time $n^{O(k)}$ for groups of order n given by their Cayley tables (see Section 3).

[1] Two groups belong to the same *isomorphism type* if and only if they are isomorphic.

[2] Regarding the significance of the Group Isomorphism problem to the Graph Isomorphism problem we refer the reader to Section 13 of [1] and especially to footnote 9 in that section.

DOI: 10.4086/toc.2015.v011a015

Theorem 1.1. *If p is an odd prime, k and n are positive integers, and*

$$1 \le k \le \sqrt{2\log n/\log p} - (5/2)\,,$$

then there exist nonisomorphic p-groups of order at most n with identical k-profiles.

Remark 1.2. In particular, setting $p = 3$, we see that if k and n are positive integers such that $1 \le k \le \sqrt{2\log_3 n} - (5/2)$, then there exist nonisomorphic groups of order at most n with identical k-profiles.

Our examples are p-groups of class 2 and exponent p.

Theorem 1.3. *For any odd prime p and positive integer k there exist nonisomorphic p-groups of class 2, exponent p, and order p^N, where $N = (k+2)(k+3)/2$, with identical k-profiles.*

2 The proof

Recall that a nilpotent group G is of *class 2* if $G' \le Z(G)$, where G' denotes the commutator subgroup $G' = [G,G]$ and $Z(G)$ denotes the center of G. For an odd prime p, a *relatively free* p-group P of class 2 and exponent p with m generators can be obtained from a free group with m generators by factoring out all elements u^p and all commutators $[[u,v],w]$.

Fact 2.1. *For real numbers m and k such that $m \ge k+2$, we have*

$$m(m-1)/2 \ge 1 + mk - (k^2+k)/2\,.$$

Proof. Let $x = m-k-2$, so $x \ge 0$ and we wish to show that $f(x) \ge 0$ where

$$f(x) = (k+2+x)(k+1+x) - 2(k+2+x)k + k^2 + k - 2\,.$$

But then $f(x) = x^2 + 3x \ge 0$, as desired. □

Fact 2.2. *For an odd prime p and a positive integer k we have*

$$(p^k-1)(p^k-p)\cdots(p^k-p^{k-1}) > (1/2)p^{k^2}\,.$$

Proof.

$$\frac{\prod_{i=0}^{k-1}(p^k-p^i)}{p^{k^2}} = \prod_{j=1}^{k}\left(1-\frac{1}{p^j}\right) > 1 - \sum_{j=1}^{\infty}\frac{1}{p^j} = 1 - \frac{1}{p-1} \ge \frac{1}{2}\,.$$ □

Hypothesis 2.3.

(i) *p is an odd prime,*

(ii) *m is a positive integer, and*

(iii) *P is a relatively free group with m generators, class two, and exponent p.*

Lemma 2.4. *Assume Hypothesis 2.3. Suppose k is a positive integer such that $m \geq k+2$. Then there exists an element of P' that does not lie in Q' for any k-generated subgroup Q of P.*

Note. This is false for $k = 2$ and $m = k+1 = 3$.

Proof. In this situation, $P' = Z(P), |P/P'| = p^m$, and $|P'| = p^{m(m-1)/2}$.

We claim that for every k-generated subgroup Q of P, there exists a k-generated subgroup R of P such that $R' \geq Q'$ and $|R/(R \cap P')| = p^k$.

Indeed, let Q be a k-generated subgroup of P and $p^i = |Q/(Q \cap P')| = |QP'/P'|$. Let $s_1, \ldots, s_i$ be elements of Q such that $Q \cap P'$ together with $s_1, \ldots, s_i$ generate Q. Let $S = \langle s_1, \ldots, s_i \rangle$. Then $i \leq k$. If $i = k$, let $R = S$. If $i < k$ then there exist elements $s_{i+1}, \ldots, s_k$ such that $|RP'/P'| = p^k$ for $R = \langle s_1, \ldots, s_k \rangle$. In both cases, $|RP'/P'| = p^k$, $|R'| = p^{k(k-1)/2}$, $Q = S(Q \cap P') \leq SP' \leq RP'$, and $Q' \leq (RP')' = R'$. This proves the claim.

The number of distinct subgroups of the form RP' is the same as the number of k-dimensional subspaces of an m-dimensional vector space over the prime field $\mathbb{F}_p$. Call this number $N(m,k)$. Then

$$N(m,k) = \frac{(p^m - 1)(p^m - p) \ldots (p^m - p^{k-1})}{(p^k - 1)(p^k - p) \ldots (p^k - p^{k-1})}\,. \tag{1}$$

Clearly, the numerator of $N(m,k)$ is less than p^{mk}. By Fact 2.2, the denominator is greater than $(1/2)p^{k^2}$. Therefore, $N(m,k) < 2p^{mk-k^2}$. Since $p \geq 3$, we have $N(m,k) < p^{mk-k^2+1}$.

Now we count the elements of P' that lie in Q' for some k-generated subgroup Q of P. Each such element lies in $(RP')'$ for some subgroup RP' as above. So we obtain the upper bound

$$p^{k(k-1)/2} N(m,k) < p^{e+1} \tag{2}$$

for $e = (k^2 - k)/2 + mk - k^2 = mk - (k^2 + k)/2$.

We saw above that $|P'| = p^{m(m-1)/2}$. Fact 2.1 shows that

$$m(m-1)/2 \geq e+1\,.$$

This gives the desired conclusion. □

Lemma 2.5. *Assume Hypothesis 2.3 for a group P_1 in place of P. Let d be a positive integer such that $m \geq d+2$. Let $P_2 = \langle w \rangle$ be a cyclic group of order p and $P = P_1 \times P_2$. Then there exists an element v of P_1' such that*

(a) $|\langle v, w \rangle| = p^2$,

(b) $P/\langle v \rangle$ is not isomorphic to $P/\langle w \rangle$, and

(c) for every d-generated subgroup Q of P we have $Q' \cap \langle v, w \rangle = 1$.

Proof. By Lemma 2.4, P_1' has an element v that does not lie in Q' for any d-generated subgroup Q of P. Then (a) is obvious. We obtain (b) because

$$(P/\langle v \rangle)' = P_1'/\langle v \rangle \quad \text{and} \quad (P/\langle w \rangle)' \cong P_1'\,. \tag{3}$$

To obtain (c), let $s_1,\dots,s_d$ be d elements of P. Set $R=\langle s_1,\dots,s_d\rangle$. Then there exist unique elements $u_1,\dots,u_d$ of P_1 such that $u_i^{-1}s_i\in\langle w\rangle$ for each i, and $R'=Q'$ where $Q=\langle u_1,\dots,u_d\rangle$. By the choice of v, we see that $v\notin R'$. As $R'\le P_1$, we have $R'\cap\langle v,w\rangle=1$. □

Lemma 2.6. *Assume the hypothesis and notation of Lemma 2.5. Then there exists a bijection between the set of all d-generated subgroups of $P/\langle v\rangle$ and the set of all d-generated subgroups of $P/\langle w\rangle$ such that corresponding subgroups are isomorphic.*

Proof. Consider a d-generated subgroup Q of $P/\langle v\rangle$. Then $Q=Q^*/\langle v\rangle$ for a subgroup Q^* of P that contains v, and $Q^*=\langle Q_0,v\rangle$ for some d-generated subgroup Q_0 of P. Let $Q^{**}=\langle Q^*,w\rangle=\langle Q_0,v,w\rangle$. Recall that v and w are in $Z(P)$. So

$$(Q^{**})'=(Q^*)'=(Q_0)'. \tag{4}$$

By Lemma 2.5 we infer $(Q^{**})'\cap\langle v,w\rangle=1$.

For a d-generated subgroup R of $P/\langle w\rangle$, we obtain analogous subgroups R^*, R_0, R^{**} of P. Note that Q and R uniquely determine Q^{**} and R^{**}.

Now consider the family of all subgroups S of P such that

(i) v and w are in S, and

(ii) $S=\langle S_0,v,w\rangle$ for some d-generated subgroup S_0 of S.

The analysis above shows that to prove Lemma 2.6, it suffices to obtain, for each subgroup S as above, a bijection between

- the set of all d-generated subgroups Q of $P/\langle v\rangle$ for which $Q^{**}=S$ and
- the set of all d-generated subgroups R of $P/\langle w\rangle$ for which $R^{**}=S$

such that corresponding subgroups Q and R are isomorphic.

For each subgroup S, we have $S'\cap\langle v,w\rangle=S_0'\cap\langle v,w\rangle=1$ by Lemma 2.5.

Since P has exponent p and S/S' is abelian, there exists a complement S_1/S' to $\langle S',v,w\rangle/S'$ in S/S'. Since S', v, and w are central, we have $S=S_1\times\langle v,w\rangle$. Therefore, there exists a unique automorphism of S that induces the identity on S_1 and switches v and w. This establishes the desired bijection. □

Proof of Theorem 1.3. The result is contained in Lemma 2.6. Let $m=k+2$. Then

$$|P|=p^{1+m(m+1)/2}=p^{1+(k+2)(k+3)/2}.$$

The groups $P/\langle v\rangle$ and $P/\langle w\rangle$ have order $|P|/p$. □

Proof of Theorem 1.1. The condition $k\le\sqrt{2\log n/\log p}-(5/2)$ means

$$n\ge p^{(k+(5/2))^2/2}>p^{(k+2)(k+3)/2}=p^N.$$

By Theorem 1.3, there exist nonisomorphic groups of order p^N with identical k-profiles. □

Remark 2.7. We comment on the case $k = 1$. It is obvious that p-groups of exponent p of equal order have the same 1-profile. In particular, for every odd prime p there exist nonisomorphic p-groups of order p^3 with the same 1-profile. Moreover, for all primes p there exists a nonabelian group of order p^4 with a cyclic subgroup of order p^3 called $M_4(p)$, which has the same 1-profile as the direct product of a cyclic group of order p^3 and the cyclic group of order p. (For the definition of $M_4(p)$ see the classification of p-groups with a cyclic subgroup of index p in [2, pp. 192–193].) In particular, $M_4(2)$ has order 16, improving Remark 1.2 for $k = 1$.

3 The isomorphism test

We describe the isomorphism test based on k-profiles suggested by Gowers [3].

Proposition 3.1. *Let k,n be positive integers and suppose the groups of order n are determined, up to isomorphism, by their k-profiles. Then isomorphism of two groups of order n, given by their Cayley tables, can be decided in time $n^{2k+O(1)}$.*

Proof. Let G,H be two groups of order n. By our assumption, G and H are isomorphic if and only if their k-profiles agree, so we only need to show how to compare the k-profiles of the two groups. This can be done by computing the following equivalence relation on the disjoint union $X := G^k \dot\cup H^k$. We say that two k-tuples $(x_1,\dots,x_k) \in X$ and $(y_1,\dots,y_k) \in X$ are equivalent if the correspondence $x_i \mapsto y_i$ extends to an isomorphism of the subgroups generated by these k-tuples. This can be checked in polynomial time per instance, so $n^{2k+O(1)}$ total time. Now the k-profiles of G and H agree if and only if each equivalence class is evenly divided between G^k and H^k. $\square$

Remark 3.2. While our result shows that the comparison of k-profiles alone will not solve the Group Isomorphism problem in polynomial time, it does not rule out a role for this algorithm in improving the state of the art in this area. Indeed, Group Isomorphism is not currently known to be testable in time $n^{o(\log n)}$ (cf. [4, 6, 5, 7]). Therefore, if our bound on k is not very far from being tight, say the result stated in Remark 1.2 would fail if we replace $\sqrt{2\log_3 n}$ by $O((\log n)^{0.99})$, this would mean progress on the complexity of the Group Isomorphism problem.

Acknowledgments

The first author wishes to thank Youming Qiao for bringing this problem to his attention and László Babai for suggestions that strengthened the main results. The second author thanks Nikolai Nikolov for helpful conversations and EPSRC for financial support.

References

[1] LÁSZLÓ BABAI: Graph isomorphism in quasipolynomial time. Technical report, 2015. [arXiv:1512.03547] 395

[2] DANIEL GORENSTEIN: *Finite Groups*. AMS Chelsea Publ., 1980. 2nd ed. 399

[3] TIM GOWERS: Comment on Dick Lipton's blog entry "The Group isomorphism Problem: A Possible Polymath Problem?". Blog entry started November 7, 2011. Comment cited: November 12, 2011. http://rjlipton.wordpress.com/2011/11/07/the-group-isomorphism-problem-a-possible-polymath-problem/. 395, 399

[4] EUGENE M. LUKS: Group isomorphism with fixed subnormal chains. Technical report, 2015. [arXiv:1511.00151] 399

[5] DAVID ROSENBAUM: Bidirectional collision detection and faster algorithms for isomorphism problems. Technical report, 2013. [arXiv:1304.3935] 399

[6] DAVID ROSENBAUM: Breaking the $n^{\log n}$ barrier for solvable-group isomorphism. In *Proc. 24th ACM–SIAM Symp. Discrete Algorithms (SODA'13)*, pp. 1054–1073, 2013. [doi:10.1137/1.9781611973105.76, arXiv:1205.0642] 399

[7] DAVID ROSENBAUM AND FABIAN WAGNER: Breaking the generator-enumeration bound for p-group isomorphism. *Theoret. Comput. Sci.*, pp. 16–25, 2015. [doi:10.1016/j.tcs.2015.05.036, arXiv:1312.1755] 399

AUTHORS

George Glauberman
Professor
University of Chicago
gg@math.uchicago.edu
`http://www.math.uchicago.edu/~gg/`

Łukasz Grabowski
Research associate
University of Warwick
graboluk@gmail.com
`http://homepages.warwick.ac.uk/~masmbh/`

ABOUT THE AUTHORS

GEORGE GLAUBERMAN received his Ph. D. in 1965 from the University of Wisconsin–Madison under the supervision of Richard H. Bruck, with additional help from Helmut Wielandt and John Thompson. His work has been in the theory of finite groups, especially their local analysis. He is also an avid baseball fan (the famed Jewish pitcher Sandy Koufax is one of his heroes) and played catcher on the Math–Stat graduate student softball team 1996–2010, wearing a replica of Jackie Robinson's uniform. Since retiring from softball because of an injury, his hobby has been to learn about fusion systems.

ŁUKASZ GRABOWSKI graduated from the University of Göttingen in 2011 under the supervision of Andreas Thom and Thomas Schick. He is currently a research associate at the University of Warwick, working in combinatorics and group theory. His aim for this year is to be a little bit like Stephen Curry.