On Groups with a Class-Preserving Outer Automorphism

Peter A. Brooksbank
Bucknell University, pbrooksb@bucknell.edu

involve
a journal of mathematics

On groups with a class-preserving outer automorphism

Peter A. Brooksbank and Matthew S. Mizuhara

msp

2014 vol. 7, no. 2

INVOLVE 7:2 (2014)
dx.doi.org/10.2140/involve.2014.7.171

On groups with a class-preserving outer automorphism

Peter A. Brooksbank and Matthew S. Mizuhara

(Communicated by Nigel Boston)

Four infinite families of 2-groups are presented, all of whose members possess an outer automorphism that preserves conjugacy classes. The groups in these families are central extensions of their predecessors by a cyclic group of order 2. For each integer $r > 1$, there is precisely one 2-group of nilpotency class r in each of the four families. All other known families of 2-groups possessing a class-preserving outer automorphism consist entirely of groups of nilpotency class 2.

1. Introduction

Let G be a group, $\mathrm{Aut}(G)$ the automorphism group of G, and $\mathrm{Inn}(G)$ the subgroup of inner automorphisms. Then $\mathrm{Aut}(G)$ acts naturally on the set of conjugacy classes of G, and we denote the kernel of this action by $\mathrm{Aut}_c(G)$. We refer to the elements of $\mathrm{Aut}_c(G)$ as *class-preserving automorphisms*. Evidently $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}_c(G)$, and the elements of $\mathrm{Out}_c(G) = \mathrm{Aut}_c(G)/\mathrm{Inn}(G)$ will be referred to as *class-preserving outer automorphisms.*

Over a century ago, William Burnside [1911, Note B, p. 463] asked the question: *Are there groups G such that* $\mathrm{Out}_c(G) \neq 1$? He himself settled the question soon thereafter [Burnside 1913]: *for each prime $p \equiv \pm 3 \pmod 8$, there is a group G_p of order p^6 and nilpotency class* 2 *with* $\mathrm{Out}_c(G_p) \neq 1$.

Since Burnside's initial discovery, the problem has been revisited on many occasions, and new families of groups G with $\mathrm{Out}_c(G) \neq 1$ have been found. Until fairly recently, however, most of those families consisted of p-groups of nilpotency class 2. The object of this paper is to prove the following result.

Theorem 1.1. *There are four distinct infinite families $\mathscr{H} = \{H_j\}_{j=1}^{\infty}$, where H_j is a* 4*-generator* 2*-group of order 2^{5+j} and nilpotency class $j+1$ such that* $\mathrm{Out}_c(H_j) \neq 1$.

MSC2010: 20D15, 20D45, 20E45.

Keywords: p-groups, class-preserving automorphisms, polycyclic groups.

Project sponsored by the National Security Agency under Grant Number H98230-11-1-0146.

It is evident from the statement of Theorem 1.1 that the nilpotency class of the groups H_j in each family grows in an elementary way as a function of the group orders. This is because H_{j+1} is built as a central extension of H_j by $\mathbb{Z}/2$. Indeed, each $\mathcal{H}$ may be constructed algorithmically using the p-group generation algorithm [O'Brien 1990]; this is precisely how the families were discovered and studied. Furthermore, the groups in all four families have coclass 4, so we have shown that they are all "mainline groups" in the coclass graph $\mathcal{G}(2, 4)$ (see [Eick and Leedham-Green 2008]).

Readers interested in the history and applications of Burnside's problem are referred to the recent comprehensive survey of Yadav [2011]; we restrict ourselves here to a brief summary of those results pertaining directly to Theorem 1.1.

Wall [1947] showed that, for each integer m divisible by 8, the general linear group $\mathrm{GL}(1, \mathbb{Z}/m)$ (i.e., the group of linear permutations $x \mapsto \sigma x + \tau$ on integers modulo m with σ, τ integral) has a class-preserving automorphism that is not inner. This family includes the smallest group G such that $\mathrm{Out}_c(G) \neq 1$, namely $\mathrm{GL}(1, \mathbb{Z}/8)$ of order 32 (there, in fact, are two nonisomorphic groups of order 32 having this property). The 2-groups in Wall's family, namely $\mathrm{GL}(1, \mathbb{Z}/2^k)$, have nilpotency class 2.

Heineken [1979] constructed, for each odd prime p, an infinite family of p-groups of nilpotency class 2, *all* of whose automorphisms are class-preserving. As far as we are aware, these are the only known infinite families of groups G for which $\mathrm{Aut}_c(G) = \mathrm{Aut}(G)$.

Hertweck [2001] constructed a family of Frobenius groups as subgroups of affine semilinear groups $A\Gamma(F)$, where F is a finite field, which possess class-preserving automorphisms that are not inner.

Malinowska [1992] exhibited, for each prime $p > 5$ and each $r > 2$, a p-group G of nilpotency class r such that $\mathrm{Out}_c(G) \neq 1$. Unlike the groups in our families, however, it is not clear how the order of G relates to r.

We remark that the absence of simple groups in the above summary is explained by Feit and Seitz [1989, Section C]: *if G is a finite simple group then* $\mathrm{Out}_c(G) = 1$.

Briefly, the paper is organized as follows. In Section 2 we summarize the necessary background on p-groups. The families $\mathcal{H}$ in Theorem 1.1 are introduced in Section 3; they are naturally parametrized by vectors $\epsilon \in \{0, 1\}^4$, but there only four distinct families. The proof of Theorem 1.1 is given in Section 4.

2. Preliminaries

Our notation and terminology is standard. For elements x, y of a group, we write $x^y = y^{-1}xy$ and $[x, y] = x^{-1}x^y$. For subsets X and Y of a group, we denote by $[X, Y]$ the subgroup generated by all commutators $[x, y]$, where $x \in X$ and $y \in Y$.

The *lower central series* of a group G is the series

$$G = \gamma_1(G) \geqslant \gamma_2(G) \geqslant \cdots, \tag{1}$$

where $\gamma_{i+1}(G) = [G, \gamma_i(G)]$. A group G is *nilpotent* if $\gamma_i(G) = 1$ for some $i \geqslant 1$, in which case the smallest r such that $\gamma_{r+1}(G) = 1$ is called the *nilpotency class* (or simply *class*) of G. A finite group G is a *p-group* if $|G| = p^n$ for some prime p. All p-groups are nilpotent, and if G has class r, then G has *coclass* $n - r$. A p-group minimally generated by d elements is called a *d-generator* group.

Each nilpotent group (more generally, each soluble group) possesses a *polycyclic generating sequence* [Holt et al. 2005, Chapter 8]. This in turn gives rise to a *power-conjugate presentation* (or simply *pc-presentation*), an extremely efficient model for computing with soluble groups. We describe these presentations specifically for p-groups.

Fix a p-group G. Let $X = [x_1, \dots, x_n] \subset G$ be such that if $P_i = \langle x_i, \dots, x_n\rangle$ $(i = 1, \dots, n)$, then P_i/P_{i+1} has order p, and $G = P_1 > P_2 > \cdots > P_n > 1$ refines the lower central series in (1). If G has nilpotency class r, we define a *weighting*, $w\colon X \to \{1, \dots, r\}$, where $w(x_i) = k$ if $x_i \in \gamma_{k-1}(G) \setminus \gamma_k(G)$. Evidently, $w(x_i) \geqslant w(x_j)$ whenever $i \geqslant j$. Any such sequence X satisfies the conditions needed to serve as the generating sequence of a *weighted pc-presentation* of G. The relations, R, in such a presentation all have the form

$$\begin{aligned} &x_i^p = \prod_{k=i+1}^{n} x_k^{b(i,k)}, &&\text{where } 0 \leqslant b(i,k) < p,\ 1 \leqslant i \leqslant n,\\ &\text{or} && \\ &x_j^{x_i} = x_j \prod_{k=j+1}^{n} x_k^{b(i,j,k)}, &&\text{where } 0 \leqslant b(i,j,k) < p,\ 1 \leqslant i < j \leqslant n. \end{aligned} \tag{2}$$

We write $\langle X \mid R\rangle$ to denote the p-group defined by such a presentation. We adopt the usual convention that an omitted relation x_i^p implies that $x_i^p = 1$, and an omitted relation $x_j^{x_i}$ implies that x_i and x_j commute. We will often find it convenient to write a conjugate relation $x_j^{x_i} = x_j w$ as a commutator relation $[x_j, x_i] = w$.

Remark 2.1. In general, one requires that $G = P_1 > \cdots > P_n > 1$ refines a related series called the *exponent p-central series* [Holt et al. 2005, p. 355]. For the families of p-groups we consider here, however, the two series coincide.

A critical feature of a pc-presentation for a p-group is that elements of the group inherit a *normal form* $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, where $0 \leqslant a_i < p$. Given $g \in G$ as a word in $x_1, \dots, x_n$, a normal form may be obtained by repeatedly applying the relations in (2) in a process known as *collection*. If each element of G has a unique normal form, the pc-presentation is said to be *consistent*. Clearly if G has a consistent pc-presentation on $X = [x_1, \dots, x_n]$, then $|G| = p^n$.

We conclude this section with a useful test for consistency. We state it just for 2-groups — since this is all we need — and refer the reader to [Holt et al. 2005, Theorem 9.22] for the more general version.

Proposition 2.2. *A weighted pc-presentation of a d-generator 2-group of class r on $[x_1, \dots, x_n]$ is consistent if the following pairs of words in the generators have the same normal form (the products in parentheses are collected first):*

$$(x_k x_j)x_i \text{ and } x_k(x_j x_i), \quad 1 \leqslant i < j < k \leqslant n \text{ and } i \leqslant d,\ w(x_i)+w(x_j)+w(x_k) \leqslant r;$$
$$(x_j x_j)x_i \text{ and } x_j(x_j x_i), \quad 1 \leqslant i < j \leqslant n \text{ and } i \leqslant d,\ w(x_i)+w(x_j) < r;$$
$$(x_j x_i)x_i \text{ and } x_j(x_i x_i), \quad 1 \leqslant i < j \leqslant n,\ w(x_i)+w(x_j) < r;$$
$$(x_i x_i)x_i \text{ and } x_i(x_i x_i), \quad 1 \leqslant i \leqslant n,\ 2w(x_i) < r.$$

3. The families $\mathcal{H}^\epsilon$

In this section we introduce four infinite families of 4-generator 2-groups of fixed coclass 4. In the next section we will show that each family consists of groups that have a class-preserving outer automorphism, thus proving Theorem 1.1.

We will define the groups in each family by giving consistent pc-presentations. It is convenient to denote the ordered list of pc-generators of the n-th group in each family by $X_n = \{x_1, x_2, x_3, x_4, z, y_1, \dots, y_n\}$, with the group minimally generated by $\{x_1, x_2, x_3, x_4\}$. The commutator relations for each family are identical, namely

$$C_n = \big\{[x_2, x_1] = [x_3, x_2] = [x_4, x_1] = z,\ \ [x_3, x_1] = y_1,\\ [x_1, y_i] = [x_3, y_i] = y_{i+1}\ (i = 1, \dots, n-1)\big\}. \quad (3)$$

For each $\epsilon = (\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4) \in \{0, 1\}^4$, define

$$P_n^\epsilon = \big\{x_j^2 = z^{\epsilon_j}\ (j = 1, \dots, 4),\ \ z^2 = 1,\\ y_n^2 = 1,\ \ y_i^2 = y_{i+1}y_{i+2}\ (i = 1, \dots, n-2),\ \ y_{n-1}^2 = y_n.\big\}. \quad (4)$$

Let $R_n^\epsilon = C_n \cup P_n^\epsilon$, define $H_n^\epsilon = \langle X_n \mid R_n^\epsilon \rangle$, and put $\mathcal{H}^\epsilon = \{H_n^\epsilon\}_{n=1}^\infty$. Note that the pc-presentations for the n-th group in each family differ only in the power relations of the generators x_i.

Proposition 3.1. *Let n be a positive integer, and $\epsilon \in \{0, 1\}^4$. Then $H_n^\epsilon = \langle X_n \mid R_n^\epsilon \rangle$ has order 2^{n+5} and class $n + 1$ (hence coclass 4).*

Proof. To confirm the order of H_n^ϵ, it suffices to check that their defining pc-presentations are consistent, for which we use Proposition 2.2. Although there are $O(n^3)$ computations involved in that test, the lion's share of these may be treated uniformly for the groups H_n^ϵ. The following table lists all of the triples that must be checked, together with their normal forms. Triples involving z are omitted (since z is central), as are triples involving two or more y_s generators (since $\langle y_s : s = 1, \ldots, n\rangle$ is abelian).

Triple (a, b, c)	Conditions	Normal form of $a(bc)$ and $(ab)c$
(x_3, x_2, x_1)		$x_1x_2x_3y_1$
(x_4, x_2, x_1)		$x_1x_2x_4$
(x_4, x_3, x_1)		$x_1x_3x_4zy_1$
(x_4, x_3, x_2)		$x_2x_3x_4z$
(y_s, x_2, x_1)	$s \leqslant n-2$	$x_1x_2zy_sy_{s+1}$
(y_s, x_3, x_1)	$s \leqslant n-2$	$x_1x_3y_1y_s$
(y_s, x_4, x_1)	$s \leqslant n-2$	$x_1x_4zy_sy_{s+1}$
(y_s, x_3, x_2)	$s \leqslant n-2$	$x_2x_3zy_sy_{s+1}$
(y_s, x_4, x_2)	$s \leqslant n-2$	$x_2x_4y_s$
(y_s, x_4, x_3)	$s \leqslant n-2$	$x_3x_4y_sy_{s+1}$
(x_j, x_j, x_i)	$1 \leqslant i < j \leqslant 4$	$x_iz^{e_j}$
(y_s, y_s, x_i)	$s \leqslant n-2,\ i = 1, 3$	x_iy_{s+1}
(x_j, x_i, x_i)	$1 \leqslant i < j \leqslant 4$	$x_jz^{e_i}$
(y_s, x_i, x_i)	$s \leqslant n-2,\ i \leqslant 4$	$z^{e_i}y_s$
(x_i, x_i, x_i)	$i \leqslant 4$	$x_iz^{e_i}$

Routine calculations using the pc-relations are all that is needed to verify the normal forms listed in the table. It remains to compute the lower central series of H_n^ϵ:

$$\begin{aligned}
\gamma_1(H_n^\epsilon) &= H_n^\epsilon,\\
\gamma_2(H_n^\epsilon) &= \langle z, y_i : 1 \leqslant i \leqslant n\rangle,\\
\gamma_j(H_n^\epsilon) &= \langle y_i : j-1 \leqslant i \leqslant n\rangle \quad \text{for } j = 3, \ldots, n+1,\\
\gamma_{n+2}(H_n^\epsilon) &= 1.
\end{aligned}$$

This shows that H_n^ϵ has class $n+1$, as stated. □

Proposition 3.1 suggests that there are 16 families $\mathcal{H}^\epsilon$, but the following result shows that there is some duplication.

Proposition 3.2. *For each positive integer n, there are four isomorphism classes among the groups $\{H_n^\epsilon : \epsilon \in \{0, 1\}^4\}$.*

Proof. Each group $H = H_n^\epsilon$ determines a quadratic map $\boldsymbol{q} = \boldsymbol{q}^\epsilon$ (independent of n) as follows. Let V denote the largest elementary abelian quotient of H, namely $V = H/A \cong (\mathbb{Z}/2)^4$, where $A = \langle z, y_1, \ldots, y_n\rangle$. Let W denote the largest elementary abelian quotient of A, namely $W = A/B \cong (\mathbb{Z}/2)^2$, where $B = \langle y_2, \ldots, y_n\rangle$. Define maps $\boldsymbol{q}\colon V \to W$ and $\boldsymbol{b}\colon V \times V \to W$, where $\boldsymbol{q}(xA) = x^2B$ and $\boldsymbol{b}(xA, yA) =$

$[x, y]B$ for all $x, y \in H$. Using additive notation in V and W, one easily checks that

$$\boldsymbol{b}(u, v) = \boldsymbol{q}(u+v) + \boldsymbol{q}(u) + \boldsymbol{q}(v) \text{ for all } u, v \in V, \tag{5}$$

so $\boldsymbol{b}$ is the symmetric bilinear map associated to $\boldsymbol{q}$ in the familiar sense.

If H_n^ϵ and H_n^δ are isomorphic groups, and $\alpha\colon H_n^\epsilon \to H_n^\delta$ is any isomorphism, then α induces isomorphisms $\beta\colon V^\epsilon \to V^\delta$ and $\gamma\colon W^\epsilon \to W^\delta$ such that $\boldsymbol{q}^\delta(v\beta) = \boldsymbol{q}^\epsilon(v)\gamma$ for all $v \in V^\epsilon$. Thus α induces a *pseudo-isometry* between $\boldsymbol{q}^\epsilon$ and $\boldsymbol{q}^\delta$.

Fixing a basis $\{v_i\}$ for V, one can represent a quadratic map $\boldsymbol{q}$ as a 4×4 matrix $\boldsymbol{Q} = [[q_{ij}]]$ with entries in W, where $q_{ii} = \boldsymbol{q}(v_i)$, $q_{ij} = \boldsymbol{b}(v_i, v_j)$ if $i < j$, and $q_{ij} = 0$ of $i > j$. Given $v \in V$, write $v = \sum \lambda_i v_i$ with $\lambda_i \in \mathbb{Z}/2$. Using (5) and a finite induction, we see that $\boldsymbol{q}(v) = \sum_i \sum_{j \geqslant i} \lambda_i \lambda_j q_{ij}$. An easy matrix calculation then shows that $\boldsymbol{q}(v) = v\boldsymbol{Q}v^{\text{tr}}$ for all $v \in V$.

Using the basis $\{x_i A\}$ for V, and identifying A/B on basis $\{zB, y_1 B\}$ with the additive group of the ring $(\mathbb{Z}/2)[t]/(t^2)$ on the usual basis $\{1, t\}$, the matrix representing $\boldsymbol{q} = \boldsymbol{q}^\epsilon$, where $\epsilon = (\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$, is

$$\boldsymbol{Q} = \begin{bmatrix} \epsilon_1 & 1 & t & 1 \\ 0 & \epsilon_2 & 1 & 0 \\ 0 & 0 & \epsilon_3 & 0 \\ 0 & 0 & 0 & \epsilon_4 \end{bmatrix},$$

and the matrix representing the associated bilinear map $\boldsymbol{b}$ is $\boldsymbol{B} = \boldsymbol{Q} + \boldsymbol{Q}^{\text{tr}}$.

Given maps $\boldsymbol{q}^\epsilon$ and $\boldsymbol{q}^\delta$ representing groups H^ϵ and H^δ ($\epsilon, \delta \in \{0, 1\}^4$), one can easily test for pseudo-isometry as follows. Let $\boldsymbol{Q}^\epsilon$ and $\boldsymbol{Q}^\delta$ be matrices representing $\boldsymbol{q}^\epsilon$ and $\boldsymbol{q}^\delta$. If $g \in \mathrm{GL}(4, 2)$ represents an isomorphism $H^\epsilon/A^\epsilon \to H^\delta/A^\delta$ induced by an isomorphism $H^\epsilon \to H^\delta$, then the induced isomorphism $A^\epsilon/B^\epsilon \to A^\delta/B^\delta$ is uniquely determined by g, and its matrix $h \in \mathrm{GL}(2, 2)$ is easily computed. Extend h entry-wise to a map $\mathbb{M}_4(W^\epsilon) \to \mathbb{M}_4(W^\delta)$, and denote the image of $X \in \mathbb{M}_4(W^\epsilon)$ by X^h. Then $\boldsymbol{q}^\epsilon$ and $\boldsymbol{q}^\delta$ are pseudo-isometric if and only if there exists $g \in \mathrm{GL}(4, 2)$ such that

$$g\boldsymbol{B}^\delta g^{\text{tr}} = (\boldsymbol{B}^\epsilon)^h \quad \text{and} \quad v_i(g\boldsymbol{Q}^\delta g^{\text{tr}})v_i^{\text{tr}} = v_i(\boldsymbol{Q}^\epsilon)^h v_i^{\text{tr}},$$

as v_i runs over a basis for $(\mathbb{Z}/2)^4$.

Thus, the determination of the pseudo-isometry classes of the quadratic maps associated to the families $\mathcal{H}^\epsilon$ is an elementary matrix calculation in $\mathrm{GL}(4, 2)$, which is easily carried out using a computer algebra system such as MAGMA [Bosma et al. 1997]. Those classes are represented by

$$\boldsymbol{Q}^\epsilon \quad \text{for } \epsilon \in \{(0,0,0,0), (0,0,1,1), (1,1,0,0), (1,1,1,1)\}.$$

Finally, it is not difficult to verify that any pseudo-isometry $\boldsymbol{Q}^\epsilon \to \boldsymbol{Q}^\delta$ lifts to an isomorphism $H^\epsilon \to H^\delta$. Thus, for each n, there are precisely four isomorphism classes of group H_n^ϵ, as claimed. □

4. Proof of Theorem 1.1

In this section we complete the proof of Theorem 1.1 by exhibiting a class-preserving automorphism of each group H_n^ϵ that is not inner.

Proof of Theorem 1.1. Fix $n \geqslant 1$, $\epsilon \in \{0, 1\}^4$, and put $H = H_n^\epsilon$. Define $\theta\colon H \to H$ on generators, sending

$$x \mapsto \begin{cases} x_4 z & \text{if } x = x_4, \\ x & \text{if } x \in X_n \setminus \{x_4\}. \end{cases} \tag{6}$$

One easily verifies (by replacing x_4 with $x_4 z$ in each pc-relation involving x_4 and evaluating) that $\theta \in \mathrm{Aut}(H)$.

First, suppose that θ is an inner automorphism. Then there exists $h \in H$ commuting with x_1 and x_3, but not with x_4. Writing

$$h = \prod_{i=1}^{4} x_i^{a_i} \cdot z^b \cdot \prod_{j=1}^{n} y_j^{c_j} \quad (a_i, b, c_j \in \{0, 1\}) \tag{7}$$

and using the defining commutator relations of H, we see that

$$hx_1 = x_1 h \cdot \Big(z^{a_2+a_4} y_1^{a_3} \prod_{j=2}^{n} y_j^{c_{j-1}} \Big).$$

Hence $h \in C_H(x_1)$ if and only if $a_2 = a_4$ and $0 = a_3 = c_1 = \cdots = c_{n-1}$. Also,

$$x_3 h = x_1^{a_1} x_2^{a_2} x_3^{1+a_3} x_4^{a_4} z^{a_2+b} y_1^{a_1+c_1} \prod_{j=2}^{n} y_j^{c_j},$$

while

$$hx_3 = x_1^{a_1} x_2^{a_2} x_3^{1+a_3} x_4^{a_4} z^{b} y_1^{c_1} \prod_{j=2}^{n} y_j^{c_j} \prod_{j=2}^{n} y_j^{c_{j-1}},$$

so that $h \in C_H(x_3)$ if and only if $0 = a_1 = a_2 = c_1 = \cdots = c_{n-1}$. It follows that $C_H(x_1) \cap C_H(x_3) = \langle z, y_n \rangle = Z(H)$. Hence θ is not inner.

We next show that θ is class-preserving. To that end, we must show that, for each $h \in H$, there exists $t = t(h) \in H$ with $h^t = h\theta$. Fix $h \in H$, and write

$$h = \prod_{i=1}^{4} x_i^{a_i} \cdot z^b \cdot \prod_{j=1}^{n} y_j^{c_j},$$

as in (7). If $a_4 = 0$, then $h\theta = h$ and $t(h) = 1$ works. Thus, we may assume that $a_4 = 1$, and hence that $h\theta = hz$.

Claim. *If $h\theta = hz$, then either $h^{x_2} = hz$ or $h^{x_1 x_3} = hz$.*

It is clear from the pc-relations that x_2 commutes with every y_j. This is true also of x_1x_3. For, if $j < n-1$, then $y_j^{x_1x_3} = (y_j y_{j+1})^{x_3} = y_j y_{j+1}^2 y_{j+2}$. Using the relations (and a finite induction) one sees that $y_{j+1}^2 y_{j+2} = y_{n-1}^2 y_n = y_n^2 = 1$. It is easy to see that $y_{n-1}^{x_1x_3} = y_{n-1}$ and that $y_n^{x_1x_3} = y_n$.

Next, observe that x_2 commutes with x_4, while $x_4^{x_1x_3} = (x_4z)^{x_3} = x_4z$. Thus, it suffices to show that, if $h = x_1^{a_1}x_2^{a_2}x_3^{a_3}$ with $(a_1, a_2, a_3) \in \{0, 1\}^3$, then either $h^{x_2} = hz$, or $h^{x_1x_3} = h$. First,

$$h^{x_2} = (x_1^{a_1}x_2^{a_2}x_3^{a_3})^{x_2} = x_1^{a_1}x_2^{a_2}x_3^{a_3}z^{a_1+a_3} = hz^{a_1+a_3}.$$

Hence, if $a_1 \neq a_3$, then $h^{x_2} = hz$, as required. It remains to show that x_1x_3 commutes with h whenever $a_1 = a_3$. If $a_1 = a_3 = 0$, then either $h = 1$ or $h = x_2$; clearly x_1x_3 commutes with 1, and $x_2^{x_1x_3} = x_2z^2 = x_2$. Finally, if $a_1 = a_3 = 1$, then either $h = x_1x_3$ or $h = x_1x_2x_3$; clearly x_1x_3 commutes with itself, and

$$\begin{aligned}(x_1x_2x_3)^{x_1x_3} &= (x_1(x_2z)(x_3y_1))^{x_3}\\ &= (x_1y_1^{-1})(x_2z)zx_3(y_1y_2)\\ &= x_1x_2y_1^{-1}x_3y_1y_2\\ &= x_1x_2x_3y_2^{-1}y_1^{-1}y_1y_2 \;=\; x_1x_2x_3.\end{aligned}$$

This establishes our claim, and completes the proof of Theorem 1.1. □

Acknowledgments

The authors would like to thank R. Quinlan for bringing this problem to their attention, and the anonymous referee for some helpful suggestions.

References

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3–4 (1997), 235–265. MR 1484478 Zbl 0898.68039

[Burnside 1911] W. Burnside, *Theory of groups of finite order*, 2nd ed., Cambridge Univ. Press, New York, 1911. Reprinted Dover, New York, 1955. MR 16,1086c Zbl 0064.25105

[Burnside 1913] W. Burnside, "On the outer isomorphisms of a group", *Proc. London Math. Soc.* **S2-11**:1 (1913), 40–42. MR 1577234 JFM 43.0198.03

[Eick and Leedham-Green 2008] B. Eick and C. Leedham-Green, "On the classification of prime-power groups by coclass", *Bull. Lond. Math. Soc.* **40**:2 (2008), 274–288. MR 2009b:20030 Zbl 1168.20007

[Feit and Seitz 1989] W. Feit and G. M. Seitz, "On finite rational groups and related topics", *Illinois J. Math.* **33**:1 (1989), 103–131. MR 90a:20016 Zbl 0701.20005

[Heineken 1979] H. Heineken, "Nilpotente Gruppen, deren sämtliche Normalteiler charakteristisch sind", *Arch. Math.* (*Basel*) **33**:6 (1979), 497–503. MR 81h:20023 Zbl 0413.20017

[Hertweck 2001] M. Hertweck, "Class-preserving automorphisms of finite groups", *J. Algebra* **241**:1 (2001), 1–26. MR 2002e:20047 Zbl 0993.20017

[Holt et al. 2005] D. F. Holt, B. Eick, and E. A. O'Brien, *Handbook of computational group theory*, Chapman & Hall, Boca Raton, FL, 2005. MR 2006f:20001 Zbl 1091.20001

[Malinowska 1992] I. Malinowska, "On quasi-inner automorphisms of a finite p–group", *Publ. Math. Debrecen* **41**:1–2 (1992), 73–77. MR 93g:20069 Zbl 0792.20019

[O'Brien 1990] E. A. O'Brien, "The p–group generation algorithm", *J. Symbolic Comput.* **9**:5–6 (1990), 677–698. MR 91j:20050 Zbl 0736.20001

[Wall 1947] G. E. Wall, "Finite groups with class-preserving outer automorphisms", *J. London Math. Soc.* **22** (1947), 315–320. MR 10,8g Zbl 0030.00901

[Yadav 2011] M. K. Yadav, "Class preserving automorphisms of finite p–groups: a survey", pp. 569–579 in *Groups St Andrews 2009* (Bath, 2009), vol. II, edited by C. M. Campbell et al., London Math. Soc. Lecture Note Ser. **388**, Cambridge Univ. Press, 2011. MR 2012j:20061 Zbl 1231.20024

Received: 2012-08-04 Revised: 2012-11-07 Accepted: 2012-11-17

pbrooksb@bucknell.edu *Department of Mathematics, Bucknell University, 380 Olin Science Building, Lewisburg, PA 17837, United States*

msm030@bucknell.edu *Department of Mathematics, Bucknell University, 380 Olin Science Building, Lewisburg, PA 17837, United States*

involve

msp.org/involve

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2014 is US $120/year for the electronic version, and $165/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2014 vol. 7 no. 2