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

In 1911, Burnside [Bu1, Note B] asked the question: Are there groups $G$
such that $\text{Out}_c(G) \neq 1$? Only two years later, Burnside himself settled the
question [Bu2]: for each prime $p \equiv \pm 3 \pmod{8}$, there is a group $G_p$ of order
$p^6$ and nilpotency class 2 with $\text{Out}_c(G_p) \neq 1$.

Since Burnside’s initial discovery, the problem has been revisited on many
occasions, and new families of groups $G$ with $\text{Out}_c(G) \neq 1$ 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 $\mathcal{H} = \{H_j\}_{j=1}^\infty$, where
$H_j$ is a 4-generator 2-group of order $2^{5+j}$ and nilpotency class $j+1$ such that
$\text{Out}_c(H_j) \neq 1$.

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

---

*Project sponsored by the National Security Agency under Grant Number H98230-11-1-0146. The United States Government is authorized to reproduce and distribute reprints not-withstanding any copyright notation herein.

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

2010 Mathematics Subject Classification: 20D15, 20D45, 20E45.
the group orders. This is because $H_{j+1}$ is built as a central extension of $H_j$ by $\mathbb{Z}/2$. Indeed, each $H$ may be constructed algorithmically using the $p$-group generation algorithm [O’B]; 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 $G(2,4)$ (cf. [EL]).

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

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

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

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

In 1992, Malinowska exhibited, for each prime $p > 5$ and each $r > 2$, a $p$-group $G$ of nilpotency class $r$ such that $\text{Out}_c(G) \neq 1$ [Ma]. 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 [FS, Section C]: if $G$ is a finite simple group then $\text{Out}_c(G) = 1$.

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

$$G = \gamma_1(G) \supseteq \gamma_2(G) \supseteq \ldots$$
where $\gamma_{i+1}(G) = [G, \gamma_i(G)]$. A group $G$ is nilpotent if $\gamma_i(G) = 1$ for some $i \geq 1$, 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 poly-cyclic generating sequence [HEO, 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 $X = \{x_1, \ldots, x_n\} \subset G$ be such that if $P_i = \langle x_i, \ldots, x_n \rangle$ ($i = 1, \ldots, n$), then $P_i/P_{i+1}$ has order $p$, and $G = P_1 > P_2 > \ldots > P_n > 1$ refines the lower central series in Equation (1). If $G$ has nilpotency class $r$, we define a weighting, $w: X \to \{1, \ldots, r\}$, where $w(x_i) = k$ if $x_i \in \gamma_{k-1}(G)/\gamma_k(G)$. Evidently, $w(x_i) \geq w(x_j)$ whenever $i \geq j$. 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

$$
\begin{align*}
&x_i^p = \prod_{k=i+1}^n x_k^{b(i,k)}; & \text{where } 0 \leq b(i,k) < p, 1 \leq i \leq n, \\
&x_j x_i x_j^{-1} = x_j^{x_i}; & \text{where } 0 \leq b(i,j,k) < p, 1 \leq i < j \leq n
\end{align*}
$$

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 $x_i^p = 1$, and an omitted relation $x_j x_i x_j^{-1}$ 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 $G = P_1 > \ldots > P_n > 1$ refines a related series called the exponent p-central series [HEO, 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 $x_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$, where $0 \leq a_i < p$. Given $g \in G$ as a word in $x_1, \ldots, x_n$, a normal form may be obtained by repeatedly applying the relations in Equation (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 $X = \{x_1, \ldots, x_n\}$, 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 [HEO, 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 $\lbrace x_1, \ldots, x_n \rbrace$ is consistent if the following pairs of words in the generators
have the same normal form (the products in parentheses are collected first):

\[
\begin{align*}
(x_k x_j) x_i & \text{ and } x_k (x_j x_i) \quad 1 \leq i < j < k \leq n \text{ and } i \leq d, \ w(x_i) + w(x_j) + w(x_k) \leq r; \\
(x_j x_i) x_i & \text{ and } x_j (x_i x_i) \quad 1 \leq i < j \leq n \text{ and } i \leq d, \ w(x_i) + w(x_j) < r; \\
(x_j x_i) x_i & \text{ and } x_j (x_i x_i) \quad 1 \leq i < j \leq n, \ w(x_i) + w(x_j) < r; \text{ and} \\
(x_i x_i) x_i & \text{ and } x_i (x_i x_i) \quad 1 \leq i \leq n, \ 2w(x_i) < r.
\end{align*}
\]

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 \( X_n = \{x_1, x_2, x_3, x_4, z, y_1, \ldots, y_n\} \), with the group minimally generated by \( \{x_1, x_2, x_3, x_4\} \). The commutator relations for each family are identical, namely

\[
\begin{align*}
C_n = \left\{ [x_2, x_1] = [x_3, x_2] = [x_4, x_1] = z, \ [x_3, x_1] = y_1, \right. \\
& \left. [x_1, y_i] = [x_3, y_i] = y_{i+1} \ (i = 1, \ldots, n - 1) \right\}
\end{align*}
\]

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

\[
P_n^\epsilon = \left\{ x_2^2 = z^{\epsilon_j} \ (j = 1, \ldots, 4), \ z^2 = 1, \ y_1^2 = 1, \ y_i^2 = y_{i+1} y_{i+2} \ (i = 1, \ldots, n - 2), \ y_{n-1}^2 = y_n \right\}
\]

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 \( H_n^\epsilon \), 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 \( H_n^\epsilon \). 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 \( \langle y_s \rangle \), \( s = 1, \ldots, n \) is abelian).
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 $H_n^\varepsilon$.

\[
\begin{align*}
\gamma_1(H_n^\varepsilon) &= H_n^\varepsilon \\
\gamma_2(H_n^\varepsilon) &= \langle z, y_i : 1 < i < n \rangle \\
\gamma_3(H_n^\varepsilon) &= \langle y_i : j - 1 < i < n \rangle \text{ for } j = 3, \ldots, n + 1 \\
\gamma_{n+2}(H_n^\varepsilon) &= 1.
\end{align*}
\]

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

Proposition 3.1 suggests that there are 16 families $H^\varepsilon$, 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 $\{H_n^\varepsilon : \varepsilon \in \{0, 1\}^4\}$.

**Proof.** Each group $H = H_n^\varepsilon$ determines a quadratic map $q = q^\varepsilon$ (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 $q : V \to W$ and $b : V \times V \to W$, where $q(xA) = x^2B$ and $b(xA, yA) = [x, y]B$ for all $x, y \in H$. Using additive notation in $V$ and $W$, one easily checks that

\[b(u, v) = q(u + v) + q(u) + q(v) \quad \text{for all } u, v \in V,\]

so $b$ is the symmetric bilinear map associated to $q$ in the familiar sense.

If $H_n^\varepsilon$ and $H_n^{\varepsilon'}$ are isomorphic groups, and $\alpha : H_n^\varepsilon \to H_n^{\varepsilon'}$ is any isomorphism, then $\alpha$ induces isomorphisms $\beta : V^\varepsilon \to V^{\varepsilon'}$ and $\gamma : W^\varepsilon \to W^{\varepsilon'}$ such that

<table>
<thead>
<tr>
<th>Triple $(a, b, c)$</th>
<th>Conditions</th>
<th>Normal form of $a(bc)$ and $(ab)c$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(x_3, x_2, x_1)$</td>
<td></td>
<td>$x_1x_2x_3y_1$</td>
</tr>
<tr>
<td>$(x_4, x_2, x_1)$</td>
<td></td>
<td>$x_1x_2x_4$</td>
</tr>
<tr>
<td>$(x_4, x_3, x_1)$</td>
<td></td>
<td>$x_1x_3x_4y_1$</td>
</tr>
<tr>
<td>$(x_5, x_3, x_2)$</td>
<td>$s \leq n - 2$</td>
<td>$x_1x_2zysy_{s+1}$</td>
</tr>
<tr>
<td>$(y_5, x_2, x_1)$</td>
<td>$s \leq n - 2$</td>
<td>$x_1x_3y_1y_5$</td>
</tr>
<tr>
<td>$(y_5, x_3, x_1)$</td>
<td>$s \leq n - 2$</td>
<td>$x_2x_3zy_{s}y_{s+1}$</td>
</tr>
<tr>
<td>$(y_5, x_4, x_1)$</td>
<td>$s \leq n - 2$</td>
<td>$x_2x_4y_5$</td>
</tr>
<tr>
<td>$(y_5, x_4, x_2)$</td>
<td>$s \leq n - 2$</td>
<td>$x_3x_4y_{s+1}$</td>
</tr>
<tr>
<td>$(x_j, x_j, x_i)$</td>
<td>$1 \leq i &lt; j \leq 4$</td>
<td>$x_iz^{\varepsilon_j}$</td>
</tr>
<tr>
<td>$(y_j, y_s, x_i)$</td>
<td>$s \leq n - 2$, $i = 1, 3$</td>
<td>$x_1y_5$</td>
</tr>
<tr>
<td>$(x_j, x_i, x_i)$</td>
<td>$1 \leq i &lt; j \leq 4$</td>
<td>$x_iz^{\varepsilon_j}$</td>
</tr>
<tr>
<td>$(y_j, x_i, x_i)$</td>
<td>$s \leq n - 2$, $i \leq 4$</td>
<td>$z^{\varepsilon_j}y_5$</td>
</tr>
<tr>
<td>$(x_i, x_i, x_i)$</td>
<td>$i \leq 4$</td>
<td>$x_i^{z^{\varepsilon_j}}$</td>
</tr>
</tbody>
</table>
preserving automorphism of each group $H$ to an isomorphism if and only if there exists $g$, $b$ and the matrix representing the associated bilinear map $v$ is easily computed. Extend $A$ representing $q$, $Q$ can easily test for pseudo-isometry as follows. Let $q$, Equation (5) and a finite induction, we see that $q$, and $Q$ matrix maps associated to the families $H$, denote the image of $q$, $\delta$, defined by an isomorphism $H^\epsilon / A^\epsilon \rightarrow H^\delta / A^\delta$ induced by an isomorphism $H^\epsilon \rightarrow H^\delta$, then the induced isomorphism $A^\epsilon / B^\epsilon \rightarrow A^\delta / B^\delta$ is uniquely determined by $g$, and its matrix $h \in GL(2, 2)$ is easily computed. Extend $h$ entry-wise to a map $M_4(W^\epsilon) \rightarrow M_4(W^\delta)$, and denote the image of $X \in M_4(W^\epsilon)$ by $X^h$. Then $q^\epsilon$ and $q^\delta$ are pseudo-isometric if and only if there exists $g \in GL(4, 2)$ such that

$$gB^\delta g^{tr} = (B^\epsilon)^h$$ and $$v_i(gQ^\delta g^{tr})v_i^{tr} = v_i(Q^\epsilon)^hv_i^{tr},$$

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 $H^\epsilon$ is an elementary matrix calculation in $GL(4, 2)$, which is easily carried out using a computer algebra system such as MAGMA [BCP]. Those classes are represented by

$$Q^\epsilon$$ 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 $Q^\epsilon \rightarrow Q^\delta$ lifts to an isomorphism $H^\epsilon \rightarrow H^\delta$. Thus, for each $n$, there are precisely four isomorphism classes of group $H_n^\epsilon$, 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 $H_n^\epsilon$ that is not inner.
Fix \( n \geq 1, \epsilon \in \{0,1\}^4 \), and put \( H = H_n^\epsilon \). Define \( \theta : H \to H \) on generators, sending

\[
x \mapsto \begin{cases} x_4z & \text{if } x = x_4 \\ x & \text{if } x \in X_n \setminus \{x_4\} \end{cases}
\]

One easily verifies (by replacing \( x_4 \) with \( x_4z \) in each pc-relation involving \( x_4 \) and evaluating) that \( \theta \in \text{Aut}(H) \).

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

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

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

\[
hx_4 = x_1h \cdot \left( z^{a_2+a_4}y_1^{a_3} \prod_{j=2}^{n} y_j^{c_j-1} \right).
\]

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

\[
x_3h = x_1^{x_2}x_3^{x_4}x_4 = y_1^{a_1+c_1} \prod_{j=2}^{n} y_j^{c_j} \quad \text{while}
\]

\[
hx_3 = x_1^{x_2}x_3^{x_4}x_4 = y_1^{a_1+c_1} \prod_{j=2}^{n} y_j^{c_j-1}.
\]

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

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

\[
h = \prod_{i=1}^{4} x_i^{a_i} \cdot z^b \cdot \prod_{j=1}^{n} y_j^{c_j}, \quad \text{as in Equation (7). If } a_4 = 0, \text{ then } h = h^t = h \text{ and } t(h) = 1 \text{ works. Thus, we may assume that } a_4 = 1, \text{ and hence that } h = h \text{.}
\]

**Claim:** If \( h = h^t = hz \) or \( h^{x_1x_3} = hz \).

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 \( y_j^{x_1x_3} = (y_jy_+)^{x_3} = y_jy_1^{y_j^{x_1x_3}} \). Using the relations (and a finite induction) one sees that \( y_j^{x_1x_3} = y_1^{x_1x_3} = 1 \). It is easy to see that \( y_n^{x_1x_3} = y_n \) 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,

\[
h^{x_2} = (x_1^{a_1}x_2^{a_2}x_3^{a_3})^{x_2} = x_1^{x_2^{a_1}}x_2^{a_2}x_3^{a_3}x_1 = hz^{a_1+a_2}.
\]

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 \( x_2^{x_1x_3} = x_2^{x_2} = x_2 \). Finally, if
\(a_1 = a_3 = 1\), then either \(h = x_1 x_3\) or \(h = x_1 x_2 x_3\); clearly \(x_1 x_3\) commutes with itself, and
\[
(x_1 x_2 x_3)^{x_1 x_3} = (x_1 (x_2 z)(x_3 y_1))^{x_3} = (x_1 y_1^{-1})(x_2 z)x_3(y_1 y_2) = x_1 x_2 y_1^{-1} x_3 y_1 y_2 = x_1 x_2 x_3.
\]
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**


Peter A. Brooksbank
Department of Mathematics
Bucknell University
Lewisburg, PA 17837
email: pbrooks@bucknell.edu

Matthew S. Mizuhara
Department of Mathematics
Bucknell University
Lewisburg, PA 17837
email: msm030@bucknell.edu