2-GROUPS OF ALMOST MAXIMAL CLASS

RODNEY JAMES

1. Introduction

Let G be a group of order 2^n and $x, y \in G$. We define the *commutator* $[x, y]$ as $x^{-1}y^{-1}xy$. Similarly, if X, Y are subsets of G, then $[X, Y]$ denotes the subgroup generated by all commutators of the form $[x, y]$ where $x \in X$, $y \in Y$. Using this, we may define the *lower central series* of G inductively by

$$\gamma_2(G) = [G, G], \quad \gamma_{i+1}(G) = [\gamma_i(G), G], \quad (i \geq 2).$$

The following results are well known.

THEOREM 1.1. *Let G be a group of order 2^n. Then*

(a) *there exists a positive integer c (known as the class of G) such that $\gamma_i(G) = 1$ (the identity group) if and only if $i > c$.*

(b) *$c < n$ (and so we can speak of a group of maximal class in the case $c = n-1$).*

(c) *If $n > 3$, there are precisely three groups of maximal class (to within isomorphism).* *

The purpose of this paper is to find all the groups of "almost maximal" class, i.e. when the class is $n-2$. The main result is

THEOREM 1.2. *The number of groups of order 2^n and class $n-2$ for $n > 4$ is:**

(a) 15 *when $n = 5$*

(b) 22 *when $n = 6$*

(c) 26 *when n $= 7$*

(d) $24 + 4(n, 2)$ *when $n > 7$, where $(n, 2) = 1$ for n odd and $(n, 2) = 2$ for n even.*

Incidentally, theorem 4.3 also lists the groups in the class $\text{ECF}(m, n, 2)$ of groups described by Blackburn (1958).

_____

* Throughout this paper, "number of groups" is to be understood to mean "number of isomorphism classes of groups".

2. Preliminaries

Most of the concepts and results of this paper may be found in the paper by Blackburn (1958) and the interested reader is referred to that paper. All groups in this paper will be assumed to be finite 2-groups (groups of order 2^n for some integer n).

The notation C_r will be used for the abstract cyclic group of order r and if G, H are two groups $G \times H$ will denote the direct product of G and H. In particular, an *elementary abelian 2-group* is one of the form $C_2 \times C_2 \times \cdots \times C_2$. If G is a group, we will write $|G|$ for the order G, $H \leq G$ to denote that H is a subgroup of G, $H < G$ to denote that H is a proper subgroup of G ($H \neq G$) and $H \lhd G$ to denote that H is a proper normal subgroup of G. Also if $x, y, x_1, x_2, \cdots x_n \in G$, $X \subseteq G$, $H \leq G$ and $N \lhd G$, then

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

$$[x_1, x_2, \cdots, x_n] = [[x_1, x_2, \cdots, x_{n-1}], x_n] \text{ for } n > 2$$

$\langle x_1, x_2, \cdots, x_n \rangle$ (or $\langle X \rangle$) is the subgroup generated by $x_1, x_2, \cdots, x_n$ (or X)

$$\mathscr{C}(x) = \{z \in G \mid xz = zx\} \text{ is the } centralizer \text{ of } x$$

$$\mathscr{C}(X) = \{z \in G \mid xz = zx \text{ for all } x \in X\}$$

$$G - X = \{g \in G \mid g \notin X\}$$

$$|G:H| = \text{number of right cosets of } H \text{ in } G$$

$$G/N \text{ is the group whose elements are the cosets of } N$$

Finally, $\Phi(G)$ denotes the *Frattini subgroup* of G (the intersection of the maximal subgroups of G) and $Z_i(G)$ denotes the i-th term of the *upper central series* defined inductively by

$$Z_1(G) = Z(G) = \mathscr{C}(G), \quad Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)) \quad i \geq 1$$

The following results will be used throughout this paper.

THEOREM 2.1. *Let G be a group generated by a set X of elements. If $\gamma_i(G) = \langle Y, \gamma_{i+1}(G) \rangle$, then $\gamma_{i+1}(G) = \langle [X, Y], \gamma_{i+2}(G) \rangle$ for all $i \geq 1$ (where $\gamma_1(G)$ is interpreted to mean G for this theorem only).*

PROOF. See Hall (1933), Theorem 2.81.

THEOREM 2.2. *Let G be a group and x, y, $z \in G$. Then*
(a) $[xy, z] = [x, z]^y [y, z]$, $[x, yz] = [x, z][x, y]^z$
(b) $[x^{-1}, y] = [y, x]^{x^{-1}}$, $[x, y^{-1}] = [y, x]^{y^{-1}}$
(c) $[x, y^2] = [x, y]^2[x, y, y]$, $[x^2, y] = [x, y]^2[x, y, x][[x, y, x], [x, y]]$
(d) $(xy)^2 = x^2 y^2 [y, x][y, x, y]$

THEOREM 2.3. *Let G be a group and $x, y, z \in G$. Then*

$$[x, y, z] = [z, x]^w [z, y]^{xw} [x, z]^y [y, z] \text{ where } w = [x, y]$$

PROOF. $[w, z] = [x^{-1} xw, z] = [x^{-1}, z]^{xw} [y^{-1} xy, z]$

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

$$= [z, x]^w [z, y]^{xw} [x, z]^y [y, z] \text{ by theorem 2.2.(b).}$$

COROLLARY. *If $\gamma_2(G)$ is abelian, $[x, y, z] = [z, y, x][x, z, y]$*

THEOREM 2.4. *Let G be a group of order 2^n and class $n-1$. Then G has a cyclic subgroup $\langle s_1 \rangle$ of index 2 such that $\gamma_i(G) = \langle s_1^{2^{i-1}} \rangle$ for all $i > 1$. If $n > 3$, there are three choices for G with generators s, s_1 and the defining relations (where $u = s_1^{2^{n-2}}$):*

(i) $u^2 = s_1^2 [s_1, s] = s^2 = 1$,   *denoted D_n*
(ii) $u^2 = s_1^2 [s_1, s] = 1, \ s^2 = u$,   *denoted Q_n*
(iii) $u^2 = s^2 = 1, \ s_1^2 [s_1, s] = u$,   *denoted S_n*

If $n = 3$, (iii) defines an abelian group and so there are only two choices for G in this case.

PROOF. See Hall and Senior (1964), page 9.

For the next theorem, we need two more concepts. If G and H are two groups whose centres are isomorphic, we may construct a group (called a *central product* of G and H) consisting of all formal products gh with $g \in G$, $h \in H$ where elements in $Z(G)$ and $Z(H)$ which correspond under the above isomorphism are regarded as the same and where $(gh)(g'h') = (gg')(hh')$ for all $g, g' \in G$ and $h, h' \in H$. Also a 2-group G of class 2 with $G/\gamma_2(G)$ elementary abelian and $|Z(G)| = |y_2(G)| = 2$ is called an *extra-special* 2-group.

THEOREM 2.5. (a) *An extra-special 2-group is isomorphic to the central product of several copies of D_3 and at most one copy of Q_3.*

(b) *A 2-group G of class $c > 2$ with $|Z(G)| = 2$ is the central product of an extra special 2-group and a group L with $|Z(L)| = 2$ and $Z_2(L)$ abelian.*

PROOF. See Hall and Senior (1964), Theorems 4.1 and 4.2. Their proof of (b) for $c = 3$ is easily adapted to the general case.

3. CF $(m, n, 2)$

A useful set of groups of order 2^n is the set $CF(m, n, 2)$ of groups G whose class is $m - 1$ and

$$\left| \gamma_i(G): \gamma_{i+1}(G) \right| = 2 \qquad i \geqq 2$$

If $G \in CF(m, n, 2)$ and $m > 3$ we define a subgroup $\gamma_1(G)$ of G by the property that $\gamma_1(G)/\gamma_4(G)$ is the centraliser in $G/\gamma_4(G)$ of $\gamma_2(G)/\gamma_4(G)$.

THEOREM 3.1. (Blackburn (1958)). *Let* $G \in CF(m, n, 2)$ *and* $m > 3$. *Then*
(a) $G > \gamma_1(G) > Z_{m-2}(G) \geqq \gamma_2(G)$ *and* $\left| G : \gamma_1(G) \right| = \left| \gamma_1(G) : Z_{m-2}(G) \right| = 2$,
(b) *If* r *is the smallest positive integer such that there exists* $s \in G - \gamma_1(G)$ *with* $s^{2^r} \in \gamma_2(G)$, *then* $\gamma_2(G)$ *can be generated by less than* 2^r *elements*.

If s is an element of G with $s \notin \gamma_1(G)$ and $s \notin \mathscr{C}(\gamma_{m-2}(G))$, and $s_1 \in \gamma_1(G) - Z_{m-2}(G)$, we may define elements inductively by

$$s_{i+1} = [s_i, s] \qquad i = 1, 2, \cdots$$

THEOREM 3.2. *Let* $G \in CF(m, n, 2)$ *with* $m \geqq 5$ *and* s, s_i *as above. Then* $\mathscr{C}(s) \cap \gamma_2(G) \leqq \gamma_4(G)$ *and* $\gamma_i(G) = \langle s_i, \gamma_{i+1}(G) \rangle$, $i = 2, 3, 4$.

PROOF. By Theorem 2.1, $\gamma_2(G) = \langle s_2, \gamma_3((G) \rangle$, and, since $[\gamma_1(G), \gamma_2(G)]$ $\leqq \gamma_4(G)$, we get $\gamma_3(G) = \langle s_3, \gamma_4(G) \rangle$, ⸢and so $\gamma_4(G) = \langle [s_3, \gamma_1(G)]$, $s_4, [s_3, \gamma_1(G)], \gamma_5(G) \rangle$. However, if $v \in \gamma_1(G)$, then

$$[s_3, v] = [s_2, s, v] \equiv [s_2, v, s][v, s, s_2] \pmod{\gamma_5(G)}$$

$$\equiv [v, s, s_2] \pmod{\gamma_5(G)} \text{ since } [s_2, v] \in \gamma_4(G)$$

But $[v, s] \in \langle s_2, \gamma_3(G) \rangle$ and so

$$[v, s, s_2] \in [\gamma_3(G), \gamma_2(G)] \leqq \gamma_5(G).$$

Thus $[s_3, v] \in \gamma_5(G)$ and so $\gamma_4(G) = \langle s_4, \gamma_5(G) \rangle$. If $m \geqq 5$, $s_4 \notin \gamma_5(G)$ and so $s_3 \notin \mathscr{C}(s)$, giving the results.

The above result may be improved if we assume a condition of commutativity on $\gamma_1(G)$:

THEOREM 3.3. (Blackburn (1958)). *Let* $G \in CF(m, n, 2)$ *with* $m > 3$ *and suppose* $[\gamma_1(G), \gamma_i(G)] \leqq \gamma_{i+2}(G)$ *for* $i = 1, 2, \cdots m-3$. *If* s, s_i *are defined as above then*
(a) $\gamma_i(G) = \langle s_i, \gamma_{i+1}(G) \rangle$, $i = 2, 3, \cdots m-1$
(b) $\mathscr{C}(s) \cap \gamma_2(G) = \gamma_{m-1}(G)$
(c) *There exists a set* T *of elements of* $\mathscr{C}(s)$ *such that* $Z_{m-2}(G) = \langle T, \gamma_2(G) \rangle$ *and* $[t, u] \in \gamma_{m-1}(G)$ *for all* $t, u \in T$.

COROLLARY 1. $\left| \mathscr{C}(s) \right| = 2^{n-m+2}$.

COROLLARY 2. *The conjugacy class containing* s *is* $s\gamma_2(G)$.
Since we will be assuming that $G/\gamma_2(G)$ has exponent 2 or 4, we shall consider that case now.

THEOREM 3.4. *Let* $G \in CF(m, n, 2)$ *with* $m > 3$ *and suppose* $G/\gamma_2(G)$ *has exponent* 2^r *with* $r \leqq 2$. *If* s, s_i *are defined as above, then*

(a) $[\gamma_1(G), \gamma_i(G)] \leqq \gamma_{i+2}(G)$ *for* i *odd*

(b) $\gamma_i(G) = \langle s_i, \gamma_{i+1}(G) \rangle$, $i = 2, 3, \cdots m-1$

(c) $\mathscr{C}(s) \cap \gamma_2(G) = \gamma_{m-1}(G)$

(d) *If* $\gamma_2(G)$ *may be generated by* 2 *elements,* G *satisfies the conditions of theorem* 3.3.

PROOF. By theorem 3.1, $\gamma_2(G)$ has at most three generators. Since $\Phi(\gamma_2(G)) \lhd G$, $\Phi(\gamma_2(G)) = \gamma_{2+d}(G)$ where d is the number of generators of $\gamma_2(G)$.

If $d \leqq 2$, then by theorem 2 of Blackburn (1957), $\gamma_3(G) \leqq Z(\gamma_2(G))$ and so $\gamma_2(G)$ is abelian. By the corollary to theorem 2.10 of Blackburn (1958), G then satisfies the conditions of theorem 3.3, proving all parts of this theorem for this case.

If $d = 3$, we have $\Phi(\gamma_2(G)) = \gamma_5(G)$ and so $s_2^2, s_3^2, s_4^2 \in \gamma_5(G)$. Writing $\bar{G}$ for $G/\gamma_6(G)$, theorem 3.2 tells us that $\bar{G}$ satisfies the condition for theorem 3.3 and so (b) is true for $i \leqq 5$. Also since $s_2^2, s_3^2 \in \gamma_5(G)$ and $s^4 \in \mathscr{C}(s) \cap \gamma_2(G) \leqq \gamma_5(G)$, we get (working modulo $\gamma_6(G)$)

$$s_4^2 \equiv s_5^2 \equiv 1,$$

$$s_3^2[s_3, s_2] \equiv [s_2^2, s] \equiv 1,$$

$$1 \equiv [s_1, s^4] \equiv [s_1, s^2]^2 [s_1, s^2, s^2]$$

$$\equiv (s_2^2 s_3)^2 [s_3, s^2] \equiv s_3^2 s_5$$

and, for $v \in \gamma_1(G)$, $[s_4, v] = [s_3, s, v]$

$$= [v, s_3]^{s_4}[v, s]^{s_3 s_4}[s_3, v]^s[s, v] \equiv [v, s, s_3]$$

i.e. $s_3^2 \equiv [s_3, s_2] \equiv [s_4, s_1] \equiv s_5 \pmod{\gamma_6(G)}$

and

$$[s_4, v] \equiv \begin{cases} s_5 & \text{if } [v, s] \notin \gamma_3(G) \\ 1 & \text{if } [v, s] \in \gamma_3(G) \end{cases}$$

We now prove (by induction) the following:

(i) $[s_{2j}, s_1] \equiv s_{2j+1} \pmod{\gamma_{2j+2}(G)}$, $[s_{2j-1}, s_1] \in \gamma_{2j+1}(G)$ $j \geqq 2$

(ii) $s_i \equiv s_{i-2}^2 \pmod{\gamma_{i+1}(G)}$ $i \geqq 5$.

Since these results have been proved for $j = 2$ and $i = 5$, we will assume them for $2 \leqq j' \leqq j, 5 \leqq i' \leqq i$. Then $s_{i+1} = [s_i, s] \equiv [s_{i-2}^2, s] \equiv s_{i-1}^2 \pmod{\gamma_{i+2}(G)}$, proving (ii). Also

$$[s_{2(j+1)}, s_1] \equiv [s_{2j}^2, s_1] \equiv [s_{2j}, s_1]^2 \equiv s_{2j+1}^2 \equiv s_{2j+3} \pmod{\gamma_{2j+4}(G)}$$

and similarly $[s_{2j+1}, s_1] \in \gamma_{2j+3}(G)$, proving (i).

Using these results, we may show in a similar way that, for $v \in \gamma_1(G)$, $[s_{2j+1}, v] \in \gamma_{2j+3}(G)$ yielding (a), and $[v, s_{2j}] \equiv s_{2j+1}$ or $1 \pmod{\gamma_{2j+2}}$. Thus, if $\gamma_i(G) = \langle s_i, \gamma_{i+1}(G) \rangle$, then

$$\gamma_{i+1}(G) = \langle s_{i+1}, [s_i, \gamma_1(G)], \gamma_{i+2}(G) \rangle$$

$$= \langle s_{i+1}, \gamma_{i+2}(G) \rangle$$

proving (b).

Finally, (c) follows from (b) which tells us that $[s_i, s] \neq 1$ and so $s_i \notin \mathscr{C}(s)$ for $i = 2, 3, \cdots m-2$.

COROLLARY. *If* $s^2 \in \gamma_2(G)$, *then* $\langle s, \gamma_2(G) \rangle$ *is a group of maximal class for* $m > 3$ *and* $s_i^2 s_{i+1} = 1$ *for* $i = 2, 3, \cdots m-2$.

PROOF. $\langle s, \gamma_2(G) \rangle$ has order 2^{m-1} and class $m-2$. Clearly $s^2 \in \mathscr{C}(s) \cap \gamma_2(G)$ $= \gamma_{m-1}(G) \leqq Z(G)$ and so $1 = [s_j, s^2] = [s_j, s]^2 [s_j, s, s] = s_{j+1}^2 s_{j+2}$ for $j = 1, 2,$ $\cdots m - 2$.

4. ECF $(m, n, 2)$

Following Blackburn, we say that a group G belongs to the class ECF$(m,n,2)$ if $G \in$ CF$(m, n, 2)$ and $G/\gamma_2(G)$ is elementary abelian. In this paragraph we will determine all the groups of ECF$(m, n, 2)$ for any values of m, n with $m > 2$. In particular, it is clear that ECF$(n, n, 2)$ consists of the groups of order 2^n and maximal class and that the cyclic subgroup of index 2 in theorem 2.4 is the subgroup $\gamma_1(G)$.

Since ECF$(m, n, 2) \subset$ CF$(m,n,2)$, we may use the results of the previous section. Thus if $G \in$ ECF$(m, n, 2)$ then $\gamma_2(G)$ is cyclic by Theorem 3.1(b) and so (by theorem 3.4(d)) there exist elements $s \in G - \gamma_1(G)$, $s_1 \in \gamma_1(G) - Z_{m-2}(G)$ and a set $T \subset \mathscr{C}(s)$ such that $G = \langle s, \gamma_1(G) \rangle$, $\gamma_1(G) = \langle s_1, Z_{m-2}(G) \rangle$, $Z_{m-2}(G) = \langle T, \gamma_2(G) \rangle$ and $\gamma_i(G) = \langle s_i, \gamma_{i+1}(G) \rangle$ where $s_i = [s_{i-1}, s]$ for $i = 2, 3, \cdots m-1$. Also, if we write G_1 for $\langle s, s_1 \rangle$ then it is clear that $\gamma_i(G_1) = \gamma_i(G)$ for $i = 2, 3, \cdots m-1$, and G_1 is a group of order 2^m and class $m-1$. By theorem 2.4, we can see that

(1) $s_i^2 s_{i+1} = [s_i, s_j] = 1$ for all $i \geqq 2, j \geqq 1$

and that we may assume

(2) $s^2 = s_{m-1}^\alpha, \quad s_1^2 s_2 = s_{m-1}^\beta$

where $\alpha, \beta = 0$ or 1 and α, β are not both equal to 1.

LEMMA. *If* $m > 3$, $Z_2(G) = \langle T, \gamma_{m-2}(G) \rangle$ *and* $t^2 \in \gamma_{m-1}(G)$ *for all* $t \in T$.

PROOF. Let $t \in T$. As in the case of G_1, we may show that $\langle s, s_1 t \rangle$ is a group of maximal class and so for $i \geq 2$, $1 = [s_i, s_1 t] = [s_i, t][s_i, s_1]$. Since $[s_i, s_1] = 1$ and $T \subset \mathscr{C}(s)$,

(3) $[T, \gamma_2(G)] = [T, s] = 1$

To find $[s_1, t]$, we note that $s_1^2 \in \gamma_2(G)$ and so

$$1 = [t, s_1^2] = [t, s_1]^2 [t, s_1, s_1] = [t, s_1]^2.$$

Since $\gamma_2(G)$ is cyclic, $\gamma_{m-1}(G)$ is the only subgroup of order 2 and so $[t, s_1] \in \gamma_{m-1}(G)$ Using Theorem 3.3(c) and the fact that $[t, s] = 1$, we see that $[T, G] \leqq \gamma_{m-1}(G)$ $\leqq Z(G)$, and so $\langle T, \gamma_{m-2}(G) \rangle \leqq Z_2(G)$. The equality follows from the facts that

$$Z_2(G) \leqq Z_{m-2}(G) = \langle T, \gamma_2(G) \rangle \text{ and } Z_2(G) \cap \gamma_2(G) \leqq \gamma_{m-2}(G).$$

Finally, since $G/\gamma_2(G)$ is elementary Abelian, $t^2 \in \gamma_2(G) \cap \mathscr{C}(s) = \gamma_{m-1}(G)$.

If we write $T = \{t_1, t_2, \cdots t_{n-m}\}$, where the t_i are independent, and

(4) $t_j^2 = s_{m-1}^{\gamma_j}, \quad [s_1, t_j] = s_{m-1}^{\delta_j} \qquad (j = 1, 2, \cdots n - m)$

then the groups G of $\mathrm{ECF}(m, n, 2)$ will be determined by the equations (1) to (4), the parameters $\alpha, \beta, \gamma_j, \delta_j$ and the commutators of elements of T. The argument proceeds as in paragraph 4 of Blackburn (1958) or the paper by James and Cannon (1969).

THEOREM 4.1. *The number of groups G of $\mathrm{ECF}(m, n, 2)$ with $Z_2(G)$ abelian and $|Z(G)| = 2$ is 2 if $n = m + 1 > 4$, 3 if $n = m \neq 3$, and 0 otherwise.*

PROOF. Since $Z_2(G)$ is abelian, we have

$$[t_i, t_j] = [s, t_j] = 1 \quad i, j = 1, 2, \cdots n - m.$$

Since $|Z(G)| = 2$, we must have $[s_1, t] = s_{m-1}$ for all $t \in T$. However, if $[s_1, t_1] = [s_1, t_2] = s_{m-1}$, then $[s_1, t_1 t_2] = 1$ and so $t_1 t_2 \in Z(G)$ which is impossible. Thus $n = m$ or $m + 1$.

If $n = m$, then G has maximal class and so the result follows. If $n = m + 1$ then

$$G = \langle s, s_1, t, \gamma_2(G) \rangle \text{ where } [s_1, t] = s_{m-1}, t^2 = s_{m-1}^{\gamma}.$$

By replacing s by $ss_1^{\gamma+1}$ and t by $ts_{m-2}^{\gamma+1}$, we may suppose $t^2 = s_{m-1}$. Then, by replacing s by st^α, we may suppose $s^2 = 1$. The two choices for $s_1^2 s_2$ clearly yield non-isomorphic groups.

If $m = 3$, there are no such groups since $Z_2(G) = G$ is not abelian.

THEOREM 4.2. *The number of groups G of $\mathrm{ECF}(m, n, 2)$ with $|Z(G)| = 2$ is 2 if $m = 3$ and $n - m$ even or $m \neq 3$ and $n - m$ odd; 3 if $m \neq 3$ and $n - m$ even; and 0 if $m = 3$ and $n - m$ odd.*

PROOF. By Theorem 2.5, G is the central product of groups G_1 and C where G_1 is a group of the previous theorem and C is extra special (in the case where $m \neq 3$).

(a) If $n - m$ is even, then G_1 is a group of maximal class and $C = \langle t_1, \cdots, t_{n-m} \rangle$ where $[t_1, t_2] = [t_3, t_4] = \cdots = [t_{n-m-1}, t_{n-m}] = s_{m-1}, \quad [t_i, t_j] = 1$ otherwise and

$$t_1^2 = s_{m-1}^{\gamma}, \quad t_2^2 = t_3^2 = \cdots = t_{n-m}^2 = s_{m-1}.$$

By replacing t_1 by $t_1 s_{m-2}^{\gamma+1}$ and s by $s t_2^{\gamma+1}$, we may suppose $t_1^2 = s_{m-1}$. Since $\mathscr{C}(Z_2(G)) = \langle s_1 \rangle$ is characteristic in G, we may only replace s_1 by a power of itself and so the two values for $s_1^2 s_2$ yield non-isomorphic groups. If we replace s by $s s_1^\xi t$ where ξ is a non-negative integer and $t \in Z_2(G) - Z(G)$, then we must also replace t' by $t' s_{m-2}$ (where t' is an element of $Z_2(G) - Z(G)$ with $[t, t'] = s_{m-1}$) thus changing the value of t'^2. Hence, if the above values for $t_i^2 \ (t_i \in T)$ are fixed, the only elements which may replace s are of the form $s s_1^\xi$, yielding three groups with the relations

$$s_1^2 s_2 = s_{m-1} \qquad 1 \qquad 1$$

$$s^2 = 1 \qquad s_{m-1} \qquad 1$$

(b) If $n - m$ is odd, then G_1 is the other group of theorem 4.1 and $C = \langle t_2, t_3, \cdots t_{n-m} \rangle$ where

$$[t_2, t_3] = [t_4, t_5] = \cdots = [t_{n-m-1}, t_{n-m}] = s_{m-1}, \quad [t_i, t_j] = 1$$

otherwise, and

$$t_2^2 = s_{m-1}^\gamma, \ t_1^2 = t_3^2 = t_4^2 = \cdots = t_{n-m}^2 = s_{m-1}$$

Again, by replacing t_2 by $t_2 s_{m-2}^{\gamma+1}$ and s by $s t_3^{\gamma+1}$, we may suppose $t_2^2 = s_{m-1}$ and it is again easy to show that the resultant two groups (with $s^2 = 1$) are not isomorphic.

If $m = 3$, G is extra-special and the result follows from theorem 2.5(a).

THEOREM 4.3. *The number of groups in* ECF$(m, n, 2)$ *is*

$$[\tfrac{1}{2}(3n - 5)] \quad \text{for} \quad m = 3, \ n \geqq 3$$

$$3(n - m + 1) + [\tfrac{1}{2}(n-m)] \quad \text{for} \quad m > 3, \ n \geqq m$$

where $[\tfrac{1}{2}r] = \tfrac{1}{2}r$ *for* r *even and* $[\tfrac{1}{2}r] = \tfrac{1}{2}(r-1)$ *for* r *odd.*

PROOF. Let G be a group in ECF$(m, n, 2)$ and use the notation above. Then

$$Z_2(G) = \langle t_1, t_2, \cdots t_{n-m}, \gamma_{m-2}(G) \rangle$$

and, by suitably ordering the t_i, we may write

$$Z(G) = \langle t_{l+1}, \cdots, t_{n-m}, s_{m-1} \rangle \text{ and so}$$

$$G = \langle G_2, t_{l+1}, \cdots t_{n-m} \rangle$$

where $G_2 \in$ ECF$(m, m + l, 2)$ and $|Z(G_2)| = 2$. Thus G_2 is one of groups of theorem 4.2.

If $Z(G)$ has an element of order 4, we may take $t_{l+1}^2 = s_{m-1}$. By replacing s by $s t_{l+1}^\alpha$, s_1 by $s_1 t_{l+1}^\beta$ and t_j by $t_j t_{l+1}^{\gamma_j} \ (j = l + 2, \cdots, n - m)$, we may suppose

$$s^2 = s_1^2 s_2 = t_{l+2}^2 = t_{l+3}^2 = \cdots = t_{n-m}^2 = 1$$

and

$$t_1^2 = t_2^2 = \cdots = t_l^2 = s_{m-1}$$

yielding one group for each value of $l = 0, 1, \cdots n - m - 1$ (none for $m = 3$ and l odd).

If $Z(G)$ does not have an element of order 4, it is elementary abelian, and

$$G = G_2 \times \langle t_{l+1} \rangle \times \cdots \times \langle t_{n-m} \rangle$$

yielding three groups (two for $m = 3$) for each even value of $l = 0, 2, \cdots, n-m$ and two groups (none for $m = 3$) for each odd value of $l = 1, 3, \cdots, n-m$.

5. Groups of order 2^n and class $n-2$

In this paragraph, we will use the preceding results to obtain the 2-groups of almost maximal class. The following lemma (the proof of which may be found in Blackburn (1958), page 74) and its corollary will be useful in what follows.

LEMMA. *If G is a 2-group with $\left| G : \gamma_2(G) \right| = 4$, then G is a group of maximal class.*

COROLLARY. *If G is a group of order 2^n and class $n-2$, then $G \in CF(n-1, n, 2)$.*

PROOF. Since $\left| \gamma_i(G) : \gamma_{i+1}(G) \right| \geq 2$ for $i = 2, 3, \cdots n-2$, we must have $\left| \gamma_2(G) \right| \geq 2^{n-3}$ and so $\left| G : \gamma_2(G) \right| \leq 8$. By the lemma, $\left| G : \gamma_2(G) \right| \neq 4$ and so $\left| \gamma_2(G) \right| = 2^{n-3}$. Thus $\left| \gamma_i(G) : \gamma_{i+1}(G) \right| = 2$ for each i, forcing G to be in $CF(n-1, n, 2)$.

Since the groups of order 2^n ($n \leq 4$) are well known, we will consider only the groups G of order 2^n and class $n-2$ with $n > 4$. In such a group, $\left| \gamma_1(G) : \gamma_2(G) \right| = 4$ and $G/\gamma_2(G)$ is either of the form $C_2 \times C_2 \times C_2$ or $C_4 \times C_2$. In the first case, $G \in ECF(n-1, n, 2)$ and so Theorem 4.3 yields:

THEOREM 5.1. *There are precisely 6 groups G of order 2^n and class $n-2$ ($n > 4$) with $G/\gamma_2(G)$ elementary abelian.*

In the second case, we have two possibilities depending on whether $\gamma_1(G)/\gamma_2(G)$ is cyclic or elementary abelian.

THEOREM 5.2. *The number of groups G of order 2^n and class $n-2$ with $\gamma_1(G)/\gamma_2(G)$ cyclic is 3 if $n = 5$ and 6 if $n > 5$.*

PROOF. Since $G \in CF(n-1, n, 2)$, we may use the results of paragraph 3 and so we may write $G = \langle s, s_1 \rangle$ where $\gamma_1(G) = \langle s_1, \gamma_2(G) \rangle$ $s_1^2 \notin \gamma_2(G)$ and $s_1^4 \in \gamma_2(G)$. Since $G/\gamma_2(G)$ is of the form $C_4 \times C_2$, we may choose $s \notin \gamma_1(G)$ such that $s^2 \in \gamma_2(G)$. By theorem 3.4 and its corollary, we have $\gamma_i(G) = \langle s_i, \gamma_{i+1}(G) \rangle$ where

(1) $s_{i+1} = [s_i, s] = s_i^{-2}$ for $i = 2, 3, \cdots n-2$

To evaluate $[s_1, s_i]$, we note that $[s_1, s_2] \in \gamma_4(G)$. If r is an integer with $r \geq 4$ such that $[s_1, s_2] \in \gamma_r(G) - \gamma_{r+1}(G)$, then $[s_1, s_2] \equiv s_r \pmod{\gamma_{r+1}(G)}$ and so

$$[s_1, s_3] = [s_1, s_2^{-2}] \equiv s_r^{-2} \equiv s_{r+1} \pmod{\gamma_{r+2}(G)}.$$

However $[s_1^2, s] = [s_1, s]^2[s_1, s, s_1] \equiv s_2^2 s_r \equiv s_3 \pmod{\gamma_4(G)}$ and so $[s_1^4, s] = [s_1^2, s]^2[s_1^2, s, s_1^2] \equiv s_3^2 \equiv s_4 \pmod{\gamma_5(G)}$. But $s_1^4 \in \gamma_2(G)$ and so $s_1^4 \equiv s_3 \pmod{\gamma_4(G)}$. Combining these result,

$$s_{r+1} \equiv [s_1, s_3] \equiv [s_1, s_1^4] \equiv 1 \pmod{\gamma_{r+2}(G)}$$

which is impossible unless $r \geq n-2$. Thus

(2) $[s_1, s_2] = s_{n-2}$ or 1, $[s_1, s_i] = 1$ for $i > 2$

Finally, using this result in the above, we get $[s_1^4, s] = s_4$ and so $s_1^4 s_3^{-1} \in \mathscr{C}(s) \cap \gamma_2(G) = \gamma_{n-2}(G)$, and so

(3) $s^2 = s_{n-2}$ or 1, $s_1^4 = s_3 s_{n-2}$ or s_3

The equations (1), (2) and (3) are the defining relations for G and it is easy to check (when $n > 4$) that a group of order 2^n exists with the given defining relations (with $[s_1, s_2] = 1$ for $n = 5$). If $s_1^4 s_3^{-1} = s_{n-2}[s_1, s_2]$ and $s^2 = s_{n-2}$ then (by replacing s by ss_1^2) we may suppose $s^2 = 1$. Since $(ss_1^2)^2 = s^2 s_1^4 [s_1^2, s] = s^2 s_1^4 s_3^{-1}[s_1, s_2]$, we may write the defining relations:

$[s_1, s_2]$	$= 1$	1	1	s_{n-2}	s_{n-2}	s_{n-2}
$s_1^4 s_3^{-1}$	$= 1$	1	s_{n-2}	1	s_{n-2}	s_{n-2}
s^2	$= 1$	s_{n-2}	1	1	1	s_{n-2}
$(ss_1^2)^2$	$= 1$	s_{n-2}	s_{n-2}	s_{n-2}	1	s_{n-2}

In the first three cases $|Z(G)| = 4$ whereas in the last three cases $|Z(G)| = 2$ and so none of the first three is isomorphic to any of the last three. In fact, by counting the number of elements of order 2, we can see that each of the above cases yields a distinct group. Thus we obtain three groups for $n = 5$ (the groups $\Gamma_8 c_1$, $\Gamma_8 c_2$ and $\Gamma_8 e$ of Hall and Senior (1964)) and six groups for $n > 5$.

THEOREM 5.3. *The number of groups G of order 2^n and class $n-2$ with $G/\gamma_2(G)$ of exponent 4, $\gamma_1(G)/\gamma_2(G)$ elementary abelian and with $\gamma_2(G)$ having 1 or 2 generators is 6 for $n = 5$, 8 for $n = 6$ and 10 for $n > 6$.*

PROOF. Again we use the notation of paragraph 3, noting that $\gamma_1(G) = \langle s_1, s^2, \gamma_2(G) \rangle$. By Theorem 3.4 (d), Theorem 3.3 applies and $\gamma_i(G) = \langle s_i, \gamma_{i+1}(G) \rangle$ for $i = 2, 3, \cdots, n-2$ and $s^4 \in \mathscr{C}(s) \cap \gamma_2(G) = \gamma_{n-2}(G) \leqq Z(G)$.

(a) Suppose $\gamma_2(G)$ is cyclic and so $\gamma_2(G) = \langle s_2 \rangle$. If $s_1^2 \in \gamma_3(G), s_2^2 = [s_1^2, s] \in \gamma_4(G)$ contradicting our assumption and so $s_2 \equiv s_1^2 \pmod{\gamma_3(G)}$. Thus $s^{-1} s_1 s = s_1^\alpha$

where $\alpha \equiv 3 \pmod 4$. Since $s^4 \in Z(G)$, $s_1 = s^{-4} s_1 s^4 = s_1^{\alpha^4}$ and so $\alpha^4 \equiv 1 \pmod{2^{n-2}}$. Solving these congruences, we get $\alpha \equiv 3$ or $7 \pmod 8$ when $n = 5$ and $\alpha \equiv -1$, $2^{n-3} - 1$, $2^{n-4} - 1$ or $2^{n-4} + 2^{n-3} - 1 \pmod{2^{n-2}}$ for $n > 5$. Again it is easy to check that groups of order 2^n exist with defining relations $s^4 = 1$ or s_{n-2}, $s^{-1} s_1 s = s_1^\alpha$ (α as above). The latter may be written:

$$
\begin{array}{llll}
s_1^2 s_2 = 1 & s_{n-2} & s_{n-3} & s_{n-3} s_{n-2} \\
[s_1, s^2] = 1 & 1 & s_{n-2} & s_{n-2}
\end{array}
$$

where only the first two cases exist for $n = 5$. In the last case, by replacing s by s^{-1}, we may suppose $s_1^2 s_2 = s_{n-3}^{-1} s_{n-2}^{-1} = s_{n-3}$; also if $s^4 = s_{n-2}$ we may suppose (by replacing s by ss_1) that $s^4 = 1$. Thus the last two cases yield one group which is not isomorphic to those defined by the first two cases since it has no abelian subgroup of index 2. In the second case, if $s^4 = s_{n-2}$ we may suppose (by replacing s_1 by $s_1 s^2$) that $s_1^2 s_2 = 1$, and this group is not isomorphic to those with $s^4 = 1$ since it has only one normal subgroup of order 2. Finally, in the case where $s^4 = 1$ and $s_1^2 s_2 \in \gamma_{n-2}(G)$, if we replace s_1 by s_1^ξ we do not affect the value of $s_1^2 s_2$, showing that the two groups are not isomorphic. Thus we obtain three groups for $n = 5$ and four groups for $n > 5$.

(b) Suppose $\gamma_2(G)$ has 2 generators and so $s_2^2, s_3^2 \in \gamma_4(G)$. If $s_3^2 \equiv s_4 \pmod{\gamma_5(G)}$, then the above argument for s_1^2 shows that $s_2^2 \equiv s_3 \pmod{\gamma_4(G)}$ and so $\gamma_2(G)$ is cyclic. Thus we must suppose $s_2^2 \equiv s_4 \pmod{\gamma_5(G)}$. Proceeding by induction, we obtain

(1) $s_i^2 \equiv s_{i+2} \ (i = 2, 3, \cdots n-4), \ s_{n-3}^2 = s_{n-2}^2 = 1$

In particular, if $x \in \gamma_i(G)$, then $x^2 \in \gamma_{i+2}(G)$.

Write $s_2^2 = s_4 s_5 x$ and so $s_3^2 = [s_4 s_5 x, s] = s_5 s_6 [x, s]$. Since

$$s^4 \in Z(G), 1 = [s_1, s^4] = [s_1, s^2]^2 [s_1, s^2, s^2] = s_2^4 s_3^6 s_4^4 s_5$$

$$= (s_4 s_5 x)^2 s_5 s_6 [x, s] s_3^4 s_4^4 s_5 = s_3^4 s_4^6 s_5^4 s_6 x^2 [x, s]$$

$$= [s_2, s^4] x^2 [x, s] = x^2 [x, s]$$

and so $x \in \gamma_{n-2}(G)$. Proceeding by induction, we get

(2) $s_2^2 = s_4 s_5 s_{n-2}^\delta, \quad s_i^2 = s_{i+2} s_{i+3} \quad (i = 3, 4, \cdots n-4)$

To find s_1^2 and $[s_1, s_i]$, we note that

$$[s_2, s_1 s^2] = [s_2, s^2][s_2, s_1]^{s^2} \equiv s_4[s_2, s_1] \pmod{\gamma_5(G)}$$

and so (by replacing s_1 by $s_1 s^2$ if necessary) we may suppose that $[s_2, s_1] \equiv s_4 \pmod{\gamma_5(G)}$ and similarly $[s_i, s_1] \equiv s_{i+2} \pmod{\gamma_{i+3}(G)}$ for $i \geq 2$. Thus, if $s_1^2 \equiv s_r \pmod{\gamma_{r+1}(G)}$, then

$$s_{r+2} \equiv [s_r, s_1] \equiv [s_1^2, s_1] \equiv 1 \pmod{\gamma_{r+3}(G)}$$

and so $r \geqq n-3$. Noting that $s^4 \in \gamma_{n-2}(G)$, we get

(3) $$s^4 = s_{n-2}^\alpha, \; s_1^2 = s_{n-3}^\beta s_{n-2}^\gamma$$

Thus $[s_2, s_1]s_2^2 = [s_1^2, s] = s_{n-2}^\beta$ and again, by induction, we get

(4) $$[s_1, s_2] = s_4 s_5 s_{n-2}^{\beta+\delta}, \; [s_1, s_i] = s_{i+2} s_{i+3} \quad \text{for } i = 3, 4, \cdots n-4$$

The equations (1) to (4), together with the fact that $\gamma_2(G)$ is abelian, are the defining relations for G and it is easy to check that (for $n \geqq 5$) a group of order 2^n with the given defining relations does exist.

When $n = 5$, $s_2^2 = [s_1, s_2] = 1$ and so $\beta = \delta = 0$. If $s^4 = 1$, then $(s_1 s^2)^2 = s_1^2 s^4 s_2^2 s_3 = s_1^2 s_3$ and so we may suppose $s_1^2 = 1$, yielding the 3 stem groups of Γ_7 (see Hall and Senior (1964)).

When $n = 6$, $s_2^2 = s_4$ and so $\delta = 0$. Replacing s_1 by $s_1 s^{2\beta}$, we may suppose $s_1^2 = s_4^\gamma$ and $[s_1, s_2] = 1$, yielding the 4 stem groups of Γ_{23} in Hall and Senior (1964).

When $n \geqq 7$, replace s_1 by $s_1 s_{n-5}^\delta$ and s_2 by $s_2 s_{n-4}^\delta$. Since $(s_2 s_{n-4}^\delta)^2 = s_2^2 s_{n-2}^\delta$, we may suppose $\delta = 0$. To find the isomorphism classes for these groups, we replace s by $s^* = s^{1+2\xi} s_1^\zeta u$ and s_1 by $s_1^* = s_1 s^{2\eta} v$ (as in Theorem 5.2) where $u, v \in \gamma_2(G)$. Thus

$$s_2^* = [s_1 s^{2\eta} v, s^{1+2\xi} s_1^\zeta u] \equiv s_2 \pmod{\gamma_3(G)}.$$

$$[s_1^*, s_2^*] \equiv [s_1 s^{2\eta}, s_2] \equiv [s_1, s_2] s_4^\eta \equiv s_4^{1+\eta} \pmod{\gamma_5(G)}$$

As we have supposed that $[s_1, s_2] \notin \gamma_5(G)$, we must take $\eta = 0$. Also

$$\begin{aligned}(s^{1+2\xi} s_1^\zeta)^2 &= s^{2+4\xi} s_1^{2\zeta}[s_1, s^{1+2\xi}]^\zeta \equiv s^2[s_1, s^{2\xi}]^\zeta[s_1, s]^\zeta[s_1, s, s^{2\xi}]^\zeta \\ &\equiv s^2(s_2^2 s_3)^{\xi\zeta} s_2^\zeta(s_3^2 s_4)^{\xi\zeta} \equiv s^2 s_2^\zeta s_3^{\xi\zeta} \pmod{\gamma_{n-2}(G)}\end{aligned}$$

By Corollary 2 of Theorem 3.3, s^* is conjugate to $s^{1+2\xi} s_1^\zeta$ and so

$$\begin{aligned}s^{*4} &= (s^{1+2\xi} s_1^\zeta)^4 = (s^2 s_2^\zeta s_3^{\xi\zeta})^2 \\ &= s^4(s_2 s_3^\xi)^{2\zeta}(s_3 s_4^\xi)^{2\zeta}(s_4 s_5^\xi)^\zeta = s^4\end{aligned}$$

Similarly, since $\mathscr{C}(s_1) = \langle s_1, \gamma_{n-3}(G) \rangle$ has order 8, the conjugacy class of s_1 is $s_1 \gamma_2(G)$ and so $s_1^{*2} = (s_1 v)^2 = (s_1^*)^2 = (s_1^2)^x$ for some $x \in G$. If $s_1^2 \in \gamma_{n-2}(G)$, then clearly $s_1^{*2} = s_1^2$ yielding 4 groups. If $s_1^2 = s_{n-3} s_{n-2}^\gamma$, take $x = s^\gamma$ and so we may suppose $s_1^2 = s_{n-3}$, yielding 2 groups.

THEOREM 5.4. *The number of groups G of order 2^n and class $n-2$ with $G/\gamma_2(G)$ of exponent 4 and $\gamma_1(G)/\gamma_2(G)$ elementary abelian is 6 when $n = 5$, 10 when $n = 6$, 14 when $n = 7$, 16 when $n > 7$ and n odd, and 20 when $n > 7$ and n is even.*

PROOF. Once again, we use the notation of paragraph 3. By theorem 3.4. $\gamma_i(G) = \langle s_i, \gamma_{i+1}(G)\rangle$ for $i = 2, 3, \cdots n-2$ and $s^4 \in \mathscr{C}(s) \cap \gamma_2(G) = \gamma_{n-2}(G) \leqq Z(G)$. By theorem 3.1, $\gamma_2(G)$ may be generated by 3 elements and, since the groups G where $\gamma_2(G)$ has 1 or 2 generators were considered in theorem 5.3, we will assume here that $\Phi(\gamma_2(G)) = \gamma_5(G)$.

As in the reasoning for Theorem 3.4, we can show that $s_i \equiv s_{i-2}^2$ (mod $\gamma_{i+1}(G)$) for $i \geq 5$ and so $G_1 = \langle s, \gamma_2(G)\rangle$ is a group of order 2^{n-1} which satisfies the conditions of theorem 5.3 with $\gamma_i(G_1) = \gamma_{i+1}(G)$ for $i = 1, 2, \cdots n-3$. By noting that, since $s_2^2 \in \gamma_5(G)$, $1 \equiv [s_2^2, s] \equiv s_3^2 [s_3, s_2] \equiv s_5[s_3, s_2]$ (mod $\gamma_6(G)$) and so $[s_3, s_2] \equiv s_5$ (mod $\gamma_5(G_1)$), we may use that theorem to obtain

(1)
$$\begin{cases} s^4 = s_{n-2}^\alpha, \ s_2^2 = s_{n-3}^\beta s_{n-2}^\gamma, \ [s_2, s_3] = s_5 s_6 s_{n-2}^\beta \\ [s_2, s_i] = s_i^2 = s_{i+2}s_{i+3} \ (i > 3), \ s_3^2 = s_5 s_6 \end{cases}$$

Also (as in theorem 3.4) we may show that

$$[s_{2j}, s_1] \equiv s_{2j+1} \pmod{\gamma_{2j+2}(G)}, \ [s_{2j-1}, s_1] \in \gamma_{2j+1}(G) \text{ for } j \geqq 2.$$

Thus $s_{2j} \notin \mathscr{C}(s_1)$ and so $s_1^2 \equiv s_{2r+1} \pmod{\gamma_{2r+2}(G)}$ for some r. However, since

and
$$(s^2 s_1)^2 = s^4 s_1^2[s_1, s^2] \equiv s_1^2 s_3 \pmod{\gamma_4(G)}$$

$$(s_1 s_{2r})^2 \equiv s_1^2 s_{2r}^2[s_{2r}, s_1] \equiv s_1^2 s_{2r+1} \pmod{\gamma_{2r+2}(G)} \text{ for } r > 2,$$

we may suppose $s_1^2 \in \gamma_{n-2}(G)$, and so

(2)
$$s_1^2 = s_{n-2}^\delta \text{ (where } \delta = 0 \text{ if } n \text{ is odd)}$$

To find $[s_i, s_1]$, we note that $s_1^2 \in Z(G)$ and so

$$1 = [s_1^2, s] = s_2^2[s_2, s_1][s_2, s_1, s_2]$$

$$\equiv [s_2, s_1][s_2, s_1, s_2] \pmod{\gamma_{n-3}(G)}$$

Thus $[s_2, s_1] \in \gamma_{n-3}(G)$ and so $[s_2, s_1, s_2] = 1$, yielding

(3)
$$[s_2, s_1] = s_2^2 = s_{n-3}^\beta s_{n-2}^\gamma$$

By theorem 2.3 $[s_3, s_1] = [s_1, s_2]^{s_3} s_2[s_2, s_2 s_3][s_2, s_1]^s s_2^{-1}$

$$= s_{n-3}^\beta s_{n-2}^\gamma s_2 s_5 s_6 s_{n-3}^\beta s_{n-2}^\gamma s_2^{-1}$$

$$= s_2(s_5 s_6)s_2^{-1} = s_5 s_6[s_5 s_6, s_2^{-1}]$$

$$= s_5 s_6[s_5 s_6, s_2^{-2} s_2] = s_5 s_6(s_5 s_6)^{-2} = s_5^{-1} s_6^{-1}$$

Similarly, by repeated application of theorem 2.3, we obtain

(4)
$$\begin{cases} [s_{4j-1}, s_1] = s_{4j+1}^{-1} s_{4j+2}^{-1}, \ [s_{4j}, s_1] = s_{4j+1}s_{4j+2} \\ [s_{4j+1}, s_1] = 1, \ [s_{4j+2}, s_1] = s_{4j+3} \text{ for } j \geqq 1 \end{cases}$$

Once again the equations (1) to (4), together with the fact that $\gamma_3(G)$ is Abelian, may be shown to define a group of order 2^n when $n > 5$.

When $n = 6$, we have $s_s^2 = s_3^2 = s_4^2 = 1$, $[s_i, s_j] = 1$ for $i, j = 1, 2, 3, 4$, $s^4 = s_4^\alpha$ and $s_1^2 = s_4^\delta$. Since $(ss_1)^4 = s^4 s_2^2[s_2, s^2] = s^4 s_4$ we may suppose (by replacing s by ss_1) that $\alpha = 0$ giving the 2 stem groups of Γ_{22} in Hall and Senior (1964).

When $n = 7$, we must have $s_2^2 \in \gamma_5(G)$, and so

$$s^4 = s_5^\alpha, \; s_1^2 \doteq s_4^2 = s_5^2 = 1, s_2^2 = [s_2, s_1] = s_5^\gamma,$$

$$s_3^2 = [s_3, s_2] = [s_3, s_1] = [s_4, s_1] = s_5.$$

By theorem 5.3, we cannot reduce this any further unless we replace s by $ss_1 t$ where $t \in \langle s^2, \gamma_2(G) \rangle = K$. However $(ss_1 t)^2 = s^2 (s_1 t)^2 [s_1 t, s]$

$$= s^2 s_1^2 t^2 [t, s_1] s_2 [s_2, t] [t, s] \equiv s_2 s^2 \pmod{\gamma_3(G)}$$

Since $\gamma_3(G)^2$ and $[\gamma_3(G), K] \leqq \gamma_5(G)$, this yields $(ss_1 t)^4 \equiv s^4 s_2^2[s_2, s^2] \equiv s_4$ $(\text{mod } \gamma_5(G))$, contradicting (1) and so we may not replace s by $ss_1 t$. Thus there are 4 isomorphism classes of groups in this case.

When $n > 7$, we may show (as in Theorem 5.3) that s_2^2 may be taken to be s_{n-3}, s_{n-2} or 1, and (as in the case when $n = 7$) that different values of s^4 yield non-isomorphic groups. In the case where $s_2^2 = s_{n-3}$, by replacing s_1 by $s_1 s_2^\delta s_3^\delta s_4^\delta$, we may replace s_1^2 by $s_1^2 s_3^{2\delta}[s_3, s_2]^\delta = 1$. In the case where $s_2^2 \in \gamma_{n-2}(G)$ and n is even, we have $s_1^2 = s_{n-2}^\delta$ ($\delta = 0$ or 1). If we replace s_1 by $s_1^* = s_1 w$ with $w \in \gamma_3(G)$, then $s_1^{*2} = (s_1 w)^2 = s_1^2 w^2 [w, s_1]$. Since $\gamma_3(G)$ is generated by $s_3 s_4$ and s_3, we may write $w = (s_3 s_4)^\omega s_3^\tau$ for some ω, τ and so $w^2 = s_5^{-\omega + \tau} s_6^\tau$, $[w, s_1] = s_5^{-\tau} s_6^{-\tau}$ and $s_1^{*2} = s_1^2 s_5^{-\omega}$. Since $s_1^{*2} \in \gamma_{n-2}(G)$, $\omega = 0$ and so $s_1^{*2} = s_1^2$. If we replace s_1 by $s_1^* = s_1 s_2 w$, then

$$s_1^{*2} = (s_1 s_2)^2 w^2 [w, s_1 s_2] = s_1^2 s_2^2 [s_2, s_1] w^2 [w, s_2] [w, s_1] [w, s_1, s_2]$$

$$= s_1^2 [w, s_1] [w, s_1, s_2] \text{ by (3) and (4)}$$

$$= s_1^2 [w, s_1] \text{ since } [w, s_1] \in \gamma_{n-2}(G)$$

$$= s_1^2 s_5^{-\tau} s_6^{-\tau}$$

Again $s_1^{*2} \in \gamma_{n-2}(G) \Rightarrow \tau = 0 \Rightarrow s_1^{*2} = s_1^2$ and so the two values for δ give non-isomorphic groups.

Thus, when $n > 7$ and n is odd the six groups are given by $s^4 = s_{n-2}$ or 1, $s_1^2 = 1$ and $s_2^2 = s_{n-3}, s_{n-2}$ or 1; when $n > 7$ and n is even the ten groups are given by $s^4 = s_{n-2}$ or 1 and

$s_2^2 = s_{n-3}$	s_{n-2}	s_{n-2}	1	1
$s_1^2 = 1$	s_{n-2}	1	s_{n-2}	1

The results of theorems 5.1 to 5.4 yield the results of theorem 1.2.

References

N. Blackburn (1958), 'On a special class of p-groups', *Acta Math.* **100,** 45–92.

N. Blackburn (1957), 'On prime-power groups in which the derived group has two generators', *Proc. Camb. Phil. Soc.* **53,** 19–27.

M. Hall and J. K. Senior (1964), *The Groups of Order* a^n; $(n \leqq 6)$, (The Macmillan Company, New York, 1964).

P. Hall (1933), 'A Contribution to the theory of groups of prime-power order', *Proc. Lond. Matk. Soc.* (2) **36,** 29–95.

R. James and J. Cannon (1969), 'Computation of isomorphism classes of p-groups', *Maths. of Computation* **23,** 135–140.

The University of New South Wales
Sydney, Australia