The groups with order p^7 for odd prime p

E.A. O'Brien and M.R. Vaughan-Lee

Abstract

We determine product presentations for the nilpotent Lie rings with order p^7 where $p \geq 7$ is prime, and then use the Baker-Campbell-Hausdorff formula to construct power-commutator presentations for the corresponding groups. The number of such groups is a polynomial depending on p whose leading term is $3p^5$. We complete the determination of groups with order p^7 for $p = 3, 5$ using the p-group generation algorithm. We provide access to the resulting presentations for the groups via a database distributed with computer algebra systems.

1 Introduction

In collaboration with Newman [13], we recently determined the groups with order p^6 for p an odd prime,this using, amongst others, techniques for the construction of nilpotent Lie rings.

Recall that the Baker-Campbell-Hausdorff formula [9] and the Lazard correspondence [4] establish an isomorphism between the category of nilpotent Lie rings with order p^n and nilpotency class at most $p - 1$ and the category of finite p-groups with order p^n and class at most $p - 1$; in particular, since a group of order p^n has class at most $n - 1$, this isomorphism applies if $p \geq n$. Briefly, if we have a nilpotent Lie ring L with order p^n (for $p \geq n$), then we can define a group product on L in terms of the Lie addition and Lie multiplication, turning L into a group with order p^n. Similarly, if we have a group G with order p^n then we can define Lie addition and Lie multiplication on G in terms of the group product, turning G into a nilpotent Lie ring.

In [13] we developed the *Lie ring generation algorithm* to determine the nilpotent Lie rings with order p^n; this is an analogue of the p-group generation algorithm described in [14]. We applied this algorithm to determine the nilpotent Lie rings with order p^6 and then exploited the Lazard correspondence to obtain the p-groups with order p^6 for $p \geq 7$.

This work was supported by EPSRC grant GR/S86259/01 and the Marsden Fund of New Zealand via grant UOA124. 2000 *Mathematics Subject Classification.* Primary 20D15.

We now further develop and extend those ideas to determine the p-groups with order p^7 for $p \geq 7$; we also construct directly the groups with orders 3^7 and 5^7. The 2328 groups with order 2^7 were determined in [10]. For a detailed history of the determination of the groups with a given order, see Besche, Eick and O'Brien [1].

Our principal result is the following.

Theorem 1 *For $p > 5$ the number of groups with order p^7 is*

$$\begin{aligned}&3p^5 + 12p^4 + 44p^3 + 170p^2 + 707p + 2455\\ &+(4p^2 + 44p + 291)\gcd(p-1,3) + (p^2 + 19p + 135)\gcd(p-1,4)\\ &+(3p + 31)\gcd(p-1,5) + 4\gcd(p-1,7) + 5\gcd(p-1,8) + \gcd(p-1,9).\end{aligned}$$

There are 9310 groups with order 3^7 and 34297 groups with order 5^7.

Earlier Wilkinson [18] determined the groups with order p^7 and exponent $p > 5$. His published list has three errors:

1. Group 117 is redundant, and is isomorphic to 115 or 116 according to the value of the residue p mod 4.
2. There are two missing groups from the family 177, 178, 179 if $p = 3$ mod 4.
3. There are two missing groups from the family 183, 184, 185 if $p = 1$ mod 4.

These errors are not newly discovered; they were already identified by Newman in Zbl. 0651.20025. Hence the correct number of groups with order p^7 and exponent p is $7p + 174 + 2\gcd(p-1,3)$. We observe that the number of groups with order p^n and exponent p is first dependent on p for $n = 7$.

Our results agree with those of Blackburn [2, §4] for certain metabelian groups of maximal class. Our results for the prime 3 agree with independent computations performed by Newman (private communication) and confirm that there are 99 5-groups of maximal class and order 5^7 (see [11]).

We recall from [13] some notation and definitions. Let P be a p-group. The p-group generation algorithm uses the lower p-central series, defined recursively by $\mathcal{P}_1(P) = P$ and $\mathcal{P}_{i+1}(P) = [\mathcal{P}_i(P), P]\mathcal{P}_i(P)^p$ for $i \geq 1$. The p-class of P is the length of this series. Each p-group P, apart from the elementary abelian ones, is an *immediate descendant* of the quotient P/R where R is the last non-trivial term of the lower p-central series of P. Thus all the groups with order p^7, except the elementary abelian one, are immediate descendants of groups with order p^k for $k < 7$. All of the immediate descendants of P are quotients of a certain extension of P; the isomorphism problem for these descendants is equivalent to the problem of determining orbits of certain subgroups of this extension under an action of the automorphism group of P. Not all p-groups have immediate descendants, those that do are *capable*. If Q is an immediate descendant of P, then P is a *parent* of Q. If Q is a group of p-class c and $Q/\mathcal{P}_{c-2}(Q) \cong P$, then Q is a *grandchild* of P.

Following the ideas of [13], we used the Lie ring generation algorithm to determine all of the nilpotent Lie rings with order p^7 for all $p > 5$, and to obtain *product presentations* (see [7]) for them. We then applied the Baker-Campbell-Hausdorff formula to "translate" these presentations into group presentations.

In this way we obtained a list of presentations for the groups with order p^7 for $p > 5$. The algorithm also provided the 3-groups of p-class at most 2 and the 5-groups of p-class at most 4. To complete the classification of all groups with order p^7, we then constructed the remaining 3-groups and 5-groups using our implementation of the p-group generation algorithm.

A significant new feature arises in constructing nilpotent Lie rings with order p^7. While the nilpotent Lie rings with order p^6 all arise as immediate descendants of one of the 42 capable nilpotent Lie rings with order dividing p^5, some with order p^7 arise as descendants of *parameterized families* of nilpotent Lie rings with order p^6. In particular, the number of capable rings with order p^6 depends on p in eight of the 42 cases (see Table 2). In these cases, we process the family of capable Lie rings with order p^6 as uniformly as possible. We illustrate the resulting computations by presenting two examples in Section 3.

Recall Higman's long-standing PORC conjecture [8]: if, for a fixed fixed n, $f(p)$ is the number of isomorphism classes of groups with order p^n, then f is a polynomial on each residue class modulo some fixed number. Theorem 1 establishes this conjecture for the groups with order p^7. In light of Higman's work, we observe that the majority of groups with order p^k, for $k = 6, 7$ and all primes p, have p-class 3. This is no longer true for groups with order 2^8: of the 56092, a total of 30078 have p-class 2 (see, for example, [6]).

We have created a database of parametrised presentations for the groups with order p^7 for $p \geq 3$. The database is currently designed for use with Magma [3]; the data can readily be incorporated into other computer algebra systems.

We describe the database in Section 4, and in Section 5 discuss steps taken to verify the results.

2 The main result

In seeking to organise and present our work, we rely heavily on the organisation used in [13].

For $p \geq 5$, there are 42 groups with order p^k for $k < 6$ which have immediate descendants with order p^6.

In Theorem 2 we record a finite presentation for each such capable group (or *parent*). While these presentations have appeared in [13], we list them here since they are central to our claims.

The finite presentation and the listed p-class can be used to construct a power-commutator presentation. (For example it can be supplied with a specific prime p to the p-quotient algorithm [12].)

Theorem 2 [13, Theorem 2] *For $p \geq 5$, the groups with order dividing p^5 which have immediate descendants with order p^6 are the following where ω is a primitive root of unity mod p:*

1. $\langle a \mid \text{class } 5\rangle$
2. $\langle a, b \mid [b, a], \text{class } 2\rangle$
3. $\langle a, b \mid b^p, \text{class } 2\rangle$
4. $\langle a, b \mid b^p[b, a]^{-1}, \text{class } 2\rangle$
5. $\langle a, b \mid \text{class } 2\rangle$
6. $\langle a, b \mid a^p, b^p, \text{class } 3\rangle$
7. $\langle a, b \mid a^p[b, a, a]^{-1}, b^p, \text{class } 3\rangle$
8. $\langle a, b \mid a^p[b, a, b]^{-1}, b^p, \text{class } 3\rangle$
9. $\langle a, b \mid a^p[b, a, b]^{-\omega}, b^p, \text{class } 3\rangle$
10. $\langle a, b \mid a^p[b, a, a]^{-1}, b^p[b, a, b], \text{class } 3\rangle$
11. $\langle a, b \mid a^p[b, a, b], b^p[b, a, a]^{\omega}, \text{class } 3\rangle$
12. $\langle a, b \mid [b, a], b^{p^2}, \text{class } 3\rangle$
13. $\langle a, b \mid [b, a]a^{-p^2}, b^{p^2}, \text{class } 3\rangle$
14. $\langle a, b \mid [b, a, a], [b, a, b], b^p, \text{class } 3\rangle$
15. $\langle a, b \mid [b, a, b], a^{p^2}, b^p, \text{class } 3\rangle$
16. $\langle a, b \mid [b, a, b], a^{p^2}, b^p[b, a, a]^{-1}, \text{class } 3\rangle$
17. $\langle a, b \mid [b, a, b], a^{p^2}, b^p[b, a, a]^{-\omega}, \text{class } 3\rangle$
18. $\langle a, b \mid [b, a, a], a^{p^2}, b^p, \text{class } 3\rangle$
19. $\langle a, b \mid [b, a, a], b^p[b, a]^{-1}, \text{class } 3\rangle$
20. $\langle a, b \mid [b, a], b^p, \text{class } 4\rangle$
21. $\langle a, b \mid [b, a, b], a^p, b^p, \text{class } 4\rangle$

22. $\langle a, b \mid [b, a, b][b, a, a, a]^{-1}, a^p, b^p, \text{class } 4\rangle$

23. $\langle a, b, c \mid \text{class } 1\rangle$

24. $\langle a, b, c \mid [c, a], [c, b], a^p, b^p, c^p, \text{class } 2\rangle$

25. $\langle a, b, c \mid [b, a], [c, a], [c, b], c^p, \text{class } 2\rangle$

26. $\langle a, b, c \mid [c, a], [c, b], b^p, c^p, \text{class } 2\rangle$

27. $\langle a, b, c \mid [c, a], [c, b], b^p[b, a]^{-1}, c^p, \text{class } 2\rangle$

28. $\langle a, b, c \mid [c, a], [c, b], b^p, c^p[b, a]^{-1}, \text{class } 2\rangle$

29. $\langle a, b, c \mid [c, a], [c, b], a^p, b^p, \text{class } 2\rangle$

30. $\langle a, b, c \mid [c, a], [c, b], a^p[b, a]^{-1}, b^p, \text{class } 2\rangle$

31. $\langle a, b, c \mid [c, b], a^p, b^p, c^p, \text{class } 2\rangle$

32. $\langle a, b, c \mid [c, b], a^p[b, a]^{-1}, b^p, c^p, \text{class } 2\rangle$

33. $\langle a, b, c \mid [c, b], a^p, b^p[b, a]^{-1}, c^p, \text{class } 2\rangle$

34. $\langle a, b, c \mid [c, b], a^p, b^p[c, a]^{-1}, c^p, \text{class } 2\rangle$

35. $\langle a, b, c \mid [c, b], a^p[b, a]^{-1}, b^p[c, a]^{-1}, c^p, \text{class } 2\rangle$

36. $\langle a, b, c \mid [b, a], [c, a], [c, b], b^p, c^p, \text{class } 3\rangle$

37. $\langle a, b, c \mid [b, a, b], [c, a], [c, b], a^p, b^p, c^p, \text{class } 3\rangle$

38. $\langle a, b, c \mid [b, a, b], [c, a], [c, b][b, a, a]^{-1}, a^p, b^p, c^p, \text{class } 3\rangle$

39. $\langle a, b, c, d \mid \text{class } 1\rangle$

40. $\langle a, b, c, d \mid [b, a], [c, a], [d, a], [c, b], [d, b], [d, c], b^p, c^p, d^p, \text{class } 2\rangle$

41. $\langle a, b, c, d \mid [c, a], [c, b], [d, a], [d, b], [d, c], a^p, b^p, c^p, d^p, \text{class } 2\rangle$

42. $\langle a, b, c, d, e \mid \text{class } 1\rangle$

Theorem 3 *Let $p > 5$ be an odd prime. For each of the 42 groups with order dividing p^5 which have immediate descendants with order p^7, Table 1 lists the number of these descendants.*

#	Number of immediate descendants
3	4
5	$p^2 + 8p + 25$
6	$p + 6 + (p^2 + 3p + 10)\gcd(p-1,3)$
21	$2p^2 + p + 3 + 2(p+1)\gcd(p-1,3) + (2p+4)\gcd(p-1,4) + \gcd(p-1,8)$
22	$p^3 + p^2 + p - 2 + 2\gcd(p-1,3) + \gcd(p-1,4) + (p+1)\gcd(p-1,5)$
23	$p + 14$
25	$p + 8$
26	$4p^2 + 26p + 107 + 5\gcd(p-1,3) + (p+4)\gcd(p-1,4)$
27	$2p + 7$
29	$3p^2 + 17p + 53 + \gcd(p-1,3) + \gcd(p-1,4)$
31	$2p^5 + 7p^4 + 19p^3 + 49p^2 + 128p + 256 + (p^2 + 7p + 29)\gcd(p-1,3)$ $+(p^2 + 7p + 24)\gcd(p-1,4) + (p+3)\gcd(p-1,5)$
32	$3p^2 + 12p + 14 + (p+2)\gcd(p-1,4)$
33	$p^4 + 2p^3 + 5p^2 + 14p$
34	$3p^3 + 6p^2 + 6p + 11 + (p+7)\gcd(p-1,3) + (p+1)\gcd(p-1,4) + \gcd(p-1,5)$
39	$p^5 + 2p^4 + 7p^3 + 25p^2 + 88p + 270 + (p+4)\gcd(p-1,3) + \gcd(p-1,4)$
41	$p^4 + 5p^3 + 19p^2 + 64p + 140 + (p+6)\gcd(p-1,3) + (p+7)\gcd(p-1,4) + \gcd(p-1,5)$
42	$p^2 + 15p + 125$

Table 1: The immediate descendants with order p^7

Theorem 4 *Let $p > 5$ be an odd prime. For each of the 42 groups with order at most p^5, Table 2 records its number of immediate descendants with order p^6, and the number of these which are capable. For each group in turn, Table 3 lists the number of its grandchildren with order p^7.*

To obtain the complete list of groups with order p^7 we include the nine 6-generator groups of p-class 2 and the elementary abelian group with this order.

The statements of these theorems can be modified to provide partial results for the primes 3 and 5. In particular, the Baker-Campbell-Hausdorff formula applies when the corresponding p-groups are regular. Hence, with just two exceptions, the numbers of descendants given in Tables 1, 2 and 3 are valid when the prime p is greater than the p-class of these groups; for the prime 3, the number of immediate descendants of #39 with order 3^7 is 1361 and the corresponding number for #42 is 178. As we remarked in the introduction, we completed the classification of the remaining 7744 groups with order 3^7 and p-class at least 3, and the 1302 groups with order 5^7 and p-class at least 5, using the p-group generation algorithm.

Theorem 1 is now an immediate consequence. A detailed account of many of the calculations which underpin this theorem is available in [17]. We illustrate the approach in the next section.

#	Number of immediate descendants with order p^6	Number capable
1	1	1
2	2	2
3	$p+15$	16
4	1	1
5	$p+8$	2
6	$5+3\gcd(p-1,3)$	3
7	$p+\gcd(p-1,3)+1$	$p+\gcd(p-1,3)+1$
8	$1+\gcd(p-1,3)+\gcd(p-1,4)/2$	$1+\gcd(p-1,3)+\gcd(p-1,4)/2$
9	$1+\gcd(p-1,3)+\gcd(p-1,4)/2$	$1+\gcd(p-1,3)+\gcd(p-1,4)/2$
10	$p+1$	$p+1$
11	p	p
12	2	2
13	1	0
14	4	1
15	$2\gcd(p-1,3)+\gcd(p-1,4)+3$	$2\gcd(p-1,3)+2$
16	$3(p+1)/2$	$(p+1)/2$
17	$3(p+1)/2$	$(p+1)/2$
18	$2\gcd(p-1,3)+\gcd(p-1,4)+3$	$\gcd(p-1,4)+3$
19	2	1
20	2	1
21	$3\gcd(p-1,4)+2\gcd(p-1,3)+7$	2
22	$2p+2\gcd(p-1,3)+\gcd(p-1,4)+2\gcd(p-1,5)$	1
23	$3p+27$	$3p+27$
24	$3p^2+13p+37+\gcd(p-1,3)+\gcd(p-1,4)$	$5p+37+\gcd(p-1,4)$
25	4	2
26	23	9
27	5	1
28	4	2
29	12	3
30	$p+1$	1
31	35	3
32	$2p+13$	$2p+9$
33	$4p+8$	4
34	$2p+3\gcd(p-1,3)+\gcd(p-1,4)+13$	11
35	3	0
36	3	1
37	$4\gcd(p-1,3)+2\gcd(p-1,4)+11$	4
38	$2\gcd(p-1,3)+4$	1
39	$4p+48$	24
40	4	1
41	18	2
42	7	2

Table 2: Number of immediate descendants with order p^6 of the 42 parents

#	Number of grandchildren with order p^7 and parent with order p^6
1	1
2	4
3	$15p + 41 + 16\gcd(p-1,3) + 4\gcd(p-1,4)$
4	2
5	$5p + 10 + 2\gcd(p-1,3) + \gcd(p-1,4)$
6	$p^3 + 3p^2 + 8p + 18 + 5\gcd(p-1,3) + (p+5)\gcd(p-1,4)$ $+3\gcd(p-1,5) + 2\gcd(p-1,8) + \gcd(p-1,9)$
7	$3p^2 + 4p + (p+1)\gcd(p-1,3) + \gcd(p-1,4)$
8	$(p^2 + 2p + 1 + (p+5)\gcd(p-1,3) + (p+3)\gcd(p-1,4))/2$
9	$(p^2 + 2p + 1 + (p+5)\gcd(p-1,3) + (p+3)\gcd(p-1,4))/2$
10	$p + 3$
11	$p + 1$
12	3
13	0
14	4
15	$4p + 5 + (p+7)\gcd(p-1,3) + 3\gcd(p-1,4) + 2\gcd(p-1,5)$
16	$(p+1)/2$
17	$(p+1)/2$
18	$7p + 9 + 4\gcd(p-1,3) + 6\gcd(p-1,4) + 2\gcd(p-1,5)$
19	2
20	2
21	$4p + 3 + 2\gcd(p-1,3) + 4\gcd(p-1,5) + \gcd(p-1,7) + \gcd(p-1,8)$
22	$2p^2 + p + 2p\gcd(p-1,3) + p\gcd(p-1,5)$
23	$2p^2 + 63p + 362 + (p+19)\gcd(p-1,3) + 5\gcd(p-1,4) + \gcd(p-1,5)$
24	$p^4 + 4p^3 + 17p^2 + 39p + 72 + (p^2 + 9p + 47)\gcd(p-1,3)$ $+(2p+8)\gcd(p-1,4) + 2\gcd(p-1,5) + \gcd(p-1,7)$
25	6
26	$5p + 49 + 11\gcd(p-1,3) + 4\gcd(p-1,4)$
27	5
28	7
29	$2p + 20 + 7\gcd(p-1,3) + 3\gcd(p-1,4)$
30	$p + 1$
31	$p^2 + 9p + 36 + (p^2 + 5p + 29)\gcd(p-1,3) + (p+7)\gcd(p-1,4)$ $+\gcd(p-1,7) + \gcd(p-1,8)$
32	$10p + 16 + (2p+7)\gcd(p-1,3) + 2\gcd(p-1,4) + 2\gcd(p-1,5)$
33	$p^3 + 5p^2 + 13p + 6 + 3\gcd(p-1,3)$
34	$2p^2 + 14p + 10 + (2p+8)\gcd(p-1,3) + 7\gcd(p-1,4) + \gcd(p-1,5)$
35	0
36	3
37	$p^2 + 10p + 34 + (p+14)\gcd(p-1,3) + 13\gcd(p-1,4) + 6\gcd(p-1,5) + \gcd(p-1,7)$
38	$p^2 + 7p + 3 + 2\gcd(p-1,3) + 3\gcd(p-1,4) + \gcd(p-1,5)$
39	$p^3 + 13p^2 + 96p + 595 + (3p+21)\gcd(p-1,3) + (p+11)\gcd(p-1,4) + \gcd(p-1,5)$
40	4
41	$35 + (p+15)\gcd(p-1,3) + 4\gcd(p-1,4)$
42	30

Table 3: The number of grandchildren with order p^7 and parent with order p^6

3 Two illustrative examples

As we indicated in the introduction, some of the nilpotent Lie rings with order p^7 arise as descendants of parameterized families of nilpotent Lie rings with order p^6. We present two examples, which illustrate the resulting complexity. We refer the reader to [13] for a description of our method, and other sample calculations.

We recall that the lower p-central series of a Lie ring L is defined recursively by $L_1 = L$, and for $c > 1$ we set $L_{c+1} = L_c L + pL_c$. (Here $L_c L$ is $\langle ab \mid a \in L_c,\, b \in L\rangle$.) The ideal L_c consists of all linear combinations of terms of the form

$$a_1 a_2 \ldots a_c,\; pa_1 a_2 \ldots a_{c-1},\; p^2 a_1 a_2 \ldots a_{c-2}, \ldots,\; p^{c-1} a_1.$$

We say that L has p-class c if $L_{c+1} = \{0\}$, $L_c \neq \{0\}$. If L is a d-generator Lie ring, then its p-covering ring M is also d-generator and has a central elementary abelian ideal Z such that $M/Z \cong L$ and every immediate descendant of L is isomorphic to M/T for some $T \leq Z$.

3.1 Some grandchildren of #7

Consider the following 1-parameter family of nilpotent Lie rings with order p^6:

$$\langle a, b \mid pa - baa - \lambda babb,\; pb - babb,\; \text{class } 4\rangle \;(0 \leq \lambda < p).$$

These arise as immediate descendants of the Lie ring corresponding to group #7. The first step in computing the immediate descendants of these Lie rings is to compute their p-covering rings. Let

$$L = \langle a, b \mid pa - baa - \lambda babb,\; pb - babb,\; \text{class } 4\rangle$$

for $0 \leq \lambda < p$. Then L has order p^6. It is straightforward to see that L/L_2 has order p^2 and is generated by $a + L_2$, $b + L_2$, that L_2/L_3 has order p and is generated by $ba + L_3$, that L_3/L_4 has order p^2 and is generated by $baa + L_4$, $bab + L_4$, and that L_4 has order p and is generated by $babb$. The p-covering ring of L is the largest 2-generator Lie ring M having an ideal Z with $M/Z \cong L$, such that Z is contained in the centre of M, and such that $pZ = \{0\}$. It is easy to see that M has order p^9. If we let a, b denote the generators of M, then Z has order p^3 and is generated by $babba$, $pa - baa - \lambda babb$, $pb - babb$ and M_5 is generated by $babba$. The immediate descendants of L are of the form M/T for some *allowable* subring $T \leq Z$. This is a proper subring T of Z with the property that $T + M_5 = Z$. There is a natural action of the automorphism group of L on the set of allowable subrings of Z, and two immediate descendants, M/S and M/T, of L are isomorphic if and only if S and T lie in the same orbit under this action.

If T is an allowable subring of Z then T has order p^2 and is generated by $pa - baa - \lambda babb - \mu babba$, $pb - babb - \nu babba$ for some μ, ν. The corresponding immediate descendant of L has order p^7 and presentation

$$\{a, b \,|\, pa - baa - \lambda babb - \mu babba,\ pb - babb - \nu babba,\ \text{class } 5\}.$$

We now need to determine when two of these presentations give isomorphic Lie rings, and so we compute the automorphism group of L. This group has order p^8. If θ is an automorphism of L then $a\theta = a + c$, $b\theta = b + d$ for some $c, d \in L_2$, and if c, d are arbitrary elements in L_2 then there is an automorphism of L mapping a to $a + c$ and mapping b to $b + d$. We let

$$K = \langle a, b \,|\, pa - baa - \lambda babb - \mu babba,\ pb - babb - \nu babba,\ \text{class } 5\rangle,$$

and we consider elements $a', b' \in K$ where $a' = a + c$, $b' = b + d$ with $c, d \in K_2$. It is straightforward to check that

$$\begin{aligned} b'a'b'b'a' &= babba, \\ pb' - b'a'b'b' &= pb - babb, \end{aligned}$$

and so different values of the parameter ν give different algebras. But if we let $b' = b$, $a' = a + kbab$ then we have

$$pa' - b'a'a' - \lambda b'a'b'b' = pa - baa - \lambda babb + 2kbabba,$$

and taking $k = -\mu/2$ we have $pa' - b'a'a' - \lambda b'a'b'b' = 0$. It follows that for each value of λ we have p descendants with order p^7:

$$\langle a, b \,|\, pa - baa - \lambda babb,\ pb - babb - \nu babba,\ \text{class } 5\rangle\ (0 \le \nu < p).$$

As λ ranges over $0, 1, \ldots, p - 1$, we obtain a 2-parameter family of Lie rings.

3.2 Some grandchildren of #23

Consider the 1-parameter family

$$\langle a, b, c \,|\, pa - ca,\ pb - \mu cb,\ pc,\ \text{class } 2\rangle$$

where $0 \ne \mu \in \mathbb{Z}_p$ and μ, μ^{-1} define isomorphic Lie rings. For each value of μ we obtain a Lie ring of class 2 and order p^6.

These Lie rings are immediate descendants of the Lie ring corresponding to group #23. For such a ring L, the Frattini quotient L/L_2 has order p^3 and is generated by $a + L_2$, $b + L_2$, $c + L_2$, and L_2 has order p^3 and is generated by ba, ca, cb.

Then M, the p-covering ring of L, has order p^{12}, and the p-multiplicator Z has order p^6 and is generated by

$$baa,\ bab,\ cab,\ pa - ca,\ pb - \mu cb,\ pc.$$

The subring M_3 is generated by baa, bab and cab and we have

$$caa = 0,\ bac = \frac{\mu + 1}{\mu} cab,\ cac = 0,\ cba = -\frac{1}{\mu} cab,\ cbb = cbc = 0.$$

Every immediate descendant of L with order p^7 is isomorphic to M/T for some subring T of Z with order p^5 with $T + \langle baa, bab, bac \rangle = Z$. To compute the isomorphism classes of immediate descendants with order p^7, we have to compute the action of the automorphism group of L on the allowable subrings T of this form. Here the situation is more complicated than in the first example, since there are three different possibilities for the automorphism group of L, depending on the value of μ. Let θ be an automorphism of L, and suppose that $a\theta = a'$, $b\theta = b'$, $c\theta = c'$, where

$$\begin{aligned} a' &= \alpha a + \beta b + \gamma c, \\ b' &= \delta a + \varepsilon b + \eta c, \\ c' &= \rho a + \sigma b + \tau c \end{aligned}$$

modulo L_2. We have $pc' = 0$ and this implies that $\rho = \sigma = 0$. To ensure that $pa' = c'a'$ we need

$$\alpha(1 - \tau) = \beta(\mu - \tau) = 0,$$

and to ensure that $pb' = \mu c'b'$ we need

$$\delta(1 - \mu\tau) = \varepsilon(1 - \tau) = 0.$$

Hence, if $\mu = 1$ then we have

$$\begin{aligned} a' &= \alpha a + \beta b + \gamma c, \\ b' &= \delta a + \varepsilon b + \eta c, \\ c' &= c \end{aligned}$$

modulo L_2. But if $\mu = -1$ then we have

$$\begin{aligned} a' &= \alpha a + \gamma c, \\ b' &= \varepsilon b + \eta c, \\ c' &= c \end{aligned}$$

modulo L_2 or

$$\begin{aligned} a' &= \beta b + \gamma c, \\ b' &= \delta a + \eta c, \\ c' &= -c \end{aligned}$$

modulo L_2. If $\mu \neq \pm 1$ then we have

$$\begin{aligned} a' &= \alpha a + \gamma c, \\ b' &= \varepsilon b + \eta c, \\ c' &= c \end{aligned}$$

modulo L_2.

Setting $\mu = 1$ and $\mu = -1$, we obtain two Lie rings with order p^6; the number of immediate descendants with order p^7 is 5 and $6 + \gcd(p-1,3) + \gcd(p-1,4)/2$ respectively. The calculations are similar to those in [13].

We focus on the case $\mu \neq \pm 1$, and seek to construct uniformly the immediate descendants of the $(p-3)/2$ capable rings L with order p^6.

Let K be an immediate descendant with order p^7 of such an L. Then K_3 is generated by baa, bab and bac, with $cab = \frac{\mu}{\mu+1} bac$. If a', b', c' generate K and if $pa' - c'a'$, $pb' - \mu c'b'$, $pc' \in K_3$ then

$$\begin{aligned} a' &= \alpha a + \gamma c, \\ b' &= \varepsilon b + \eta c, \\ c' &= c \end{aligned}$$

modulo K_2 and

$$\begin{aligned} b'a'a' &= \alpha^2 \varepsilon baa + \frac{\mu+2}{\mu+1} \alpha\gamma\varepsilon bac, \\ b'a'b' &= \alpha\varepsilon^2 bab + \frac{2\mu+1}{\mu+1} \alpha\varepsilon\eta bac, \\ b'a'c' &= \alpha\varepsilon bac. \end{aligned}$$

First consider the situation when $bac \neq 0$. If $\mu \neq -2, -1/2$ then replacing a, b, c by suitable a', b', c', we can take $baa = bab = 0$. If $\mu = -2$ then we can take $bab = 0$ and $baa = 0$ or bac, and if $\mu = -1/2$ we can take $baa = 0$ and $bab = 0$ or bac.

If $bac = 0$ then we can take $baa = 0$ or $bab = 0$ or $bab = baa$.

3.2.1 Case 1

Let $baa = bab = 0$ and let K_3 be generated by bac. Adding suitable scalar multiples of ba to a, b, c we can take $pa - ca = pb - \mu cb = pc = 0$, so we have one Lie ring

$$\langle a, b, c \mid baa, bab, pa - ca,\ pb - \mu cb,\ pc,\ \text{class } 3 \rangle.$$

3.2.2 Case 2

Let $\mu = -2$ and let $bab = 0$, $bac = baa$ and let K_3 be generated by baa. Adding suitable scalar multiples of ba to a, b, c we can take $pa - ca = pb + 2cb = pc = 0$, so we have one Lie ring

$$\langle a, b, c \mid bab, bac - baa, pa - ca,\ pb + 2cb,\ pc, \text{ class } 3\rangle.$$

3.2.3 Case 3

The Lie ring with $\mu = -1/2$ is isomorphic to the Lie ring L with $\mu = -2$.

3.2.4 Case 4

Let $baa = bac = 0$ and let K_3 be generated by bab. Adding a suitable scalar multiple of ba to c we can take $pb - \mu cb = 0$. If a', b', c' generate K and $b'a'a' = b'a'c' = 0$ then

$$\begin{aligned} a' &= \alpha a + \gamma c, \\ b' &= \varepsilon b + \eta c, \\ c' &= c \end{aligned}$$

modulo K_2 and

$$\begin{aligned} b'a'b' &= \alpha\varepsilon^2 bab, \\ pa' - c'a' &= \alpha(pa - ca) + \gamma pc, \\ pc' &= pc \end{aligned}$$

so we have four Lie rings

$$\langle a, b, c \mid baa, bac, pa - ca,\ pb - \mu cb,\ pc, \text{ class } 3\rangle,$$

$$\langle a, b, c \mid baa, bac, pa - ca - bab,\ pb - \mu cb,\ pc, \text{ class } 3\rangle,$$

$$\langle a, b, c \mid baa, bac, pa - ca - \omega bab,\ pb - \mu cb,\ pc, \text{ class } 3\rangle,$$

$$\langle a, b, c \mid baa, bac, pa - ca,\ pb - \mu cb,\ pc - bab, \text{ class } 3\rangle,$$

where ω is a primitive element in $\mathbb{Z}_p$.

3.2.5 Case 5

Let $bab = bac = 0$ and let K_3 be generated by baa. Adding a suitable scalar multiple of ba to c we can take $pa - ca = 0$. If a', b', c' generate K and $b'a'b' = b'a'c' = 0$ then

$$\begin{aligned} a' &= \alpha a + \gamma c, \\ b' &= \varepsilon b + \eta c, \\ c' &= c \end{aligned}$$

modulo K_2 and

$$\begin{aligned} b'a'a' &= \alpha^2\varepsilon baa, \\ pb' - \mu c'b' &= \varepsilon(pb - \mu cb) + \eta pc, \\ pc' &= pc \end{aligned}$$

so we have four Lie rings

$$\langle a, b, c \,|\, bab, bac, pa - ca,\ pb - \mu cb,\ pc, \text{ class } 3\rangle,$$

$$\langle a, b, c \,|\, bab, bac, pa - ca,\ pb - \mu cb - baa,\ pc, \text{ class } 3\rangle,$$
$$\langle a, b, c \,|\, bab, bac, pa - ca,\ pb - \mu cb - \omega baa,\ pc, \text{ class } 3\rangle,$$
$$\langle a, b, c \,|\, bab, bac, pa - ca,\ pb - \mu cb,\ pc - baa, \text{ class } 3\rangle,$$

where ω is a primitive element in $\mathbb{Z}_p$.

3.2.6 Case 6

Finally, let $bac = 0$, $bab = baa$, and let K_3 be generated by baa. Adding a suitable scalar multiple of ba to c we can take $pa - ca = 0$. If a', b', c' generate K and $b'a'c' = 0$, $b'a'b' = b'a'a'$ then

$$\begin{aligned} a' &= \alpha a + \gamma c, \\ b' &= \alpha b + \eta c, \\ c' &= c \end{aligned}$$

modulo K_2 and

$$\begin{aligned} b'a'a' &= \alpha^3 baa, \\ pb' - \mu c'b' &= \alpha(pb - \mu cb) + \eta pc, \\ pc' &= pc \end{aligned}$$

so we have $3 + \gcd(p-1, 3)$ Lie rings

$$\langle a, b, c \,|\, bab - baa, bac, pa - ca,\ pb - \mu cb,\ pc, \text{ class } 3\rangle,$$

$$\langle a, b, c \,|\, bab - baa, bac, pa - ca,\ pb - \mu cb - baa,\ pc, \text{ class } 3\rangle,$$
$$\langle a, b, c \,|\, bab - baa, bac, pa - ca,\ pb - \mu cb - \omega baa,\ pc, \text{ class } 3\rangle,$$
$$\langle a, b, c \,|\, bab - baa, bac, pa - ca,\ pb - \mu cb,\ pc - baa, \text{ class } 3\rangle,$$
$$\langle a, b, c \,|\, bab - baa, bac, pa - ca,\ pb - \mu cb,\ pc - \omega baa, \text{ class } 3\rangle\ (p = 1 \bmod 3),$$
$$\langle a, b, c \,|\, bab - baa, bac, pa - ca,\ pb - \mu cb,\ pc - \omega^2 baa, \text{ class } 3\rangle\ (p = 1 \bmod 3)$$

where ω is a primitive element in $\mathbb{Z}_p$.

4 Providing access to the presentations

The groups with order 2^7 are already available in electronic form in the SmallGroups library described in Besche et al. [1]. They can be accessed through the computer algebra systems GAP [5] and Magma [3].

We have prepared a database for the groups with order p^7 for p odd based on our determination. The primary subdivision of the database is based on the capable Lie rings with order dividing p^5. If one of the 42 has a fixed number of capable descendants with order p^6, then, for each, there is a function which, given a prime $p > 5$, produces a list of explicit finite presentations for its immediate descendants with order p^7. For a parameterized family with order p^6, we usually provide a single function which constructs such a list for all of the groups in this family.

The presentations are usually obtained by running over a list of parameters: these include the prime, the set $\{1, \omega\}$ where ω is a (fixed) primitive root, and transversals of various powers in the multiplicative group of $\mathbb{Z}_p$. (Of course this implies that the explicit descriptions depend on "easy" computations in $\mathbb{Z}_p$.) Using the p-quotient algorithm, we construct a power-commutator presentation [16] for the group with order p^7 defined by such a finite presentation.

A user can construct each group in sequence, storing and investigating only one group at a time. Since the number of groups with order p^7 is already 113147 for $p = 7$, this is clearly both a desirable and necessary feature. It takes approximately 10 minutes to construct the list for $p = 7$ using Magma V2.11-8 on a Pentium IV 1.1 GHz processor.

On four occasions, we have not been able to write down a "concrete" solution for the set of immediate descendants with order p^7 of a given Lie ring. We consider one example in detail. In constructing the 4-generator Lie rings of p-class 2, we considered Lie rings L generated by a, b, c, d, subject to the relations $da = cb = 0$, $db = ca$. This is one of 13 subcases, partitioned according to the structure of $L^2 = \langle ab \,|\, a, b \in L\rangle$. Here L^2 is generated by ba, ca and dc, and $pL \leq L^2$. It is fairly easy to see that if a', b', c', d' generate L and satisfy $d'a' = c'b' = 0$, $d'b' = c'a'$, then (modulo L^2)

$$\begin{aligned}
a' &= \alpha\lambda a + \beta\lambda b + \beta\mu c - \alpha\mu d,\\
b' &= \gamma\lambda a + \delta\lambda b + \delta\mu c - \gamma\mu d,\\
c' &= \gamma\nu a + \delta\nu b + \delta\xi c - \gamma\xi d,\\
d' &= -\alpha\nu a - \beta\nu b - \beta\xi c + \alpha\xi d
\end{aligned}$$

with $\alpha\delta - \beta\gamma \neq 0$ and $\lambda\xi - \mu\nu \neq 0$. (We treat these scalars as elements of $\mathbb{Z}_p$.) It is straightforward to show that

$$\begin{pmatrix} b'a' \\ c'a' \\ d'c' \end{pmatrix} = (\alpha\delta - \beta\gamma) \begin{pmatrix} \lambda^2 & 2\lambda\mu & \mu^2 \\ \lambda\nu & \lambda\xi + \mu\nu & \mu\xi \\ \nu^2 & 2\nu\xi & \xi^2 \end{pmatrix} \begin{pmatrix} ba \\ ca \\ dc \end{pmatrix}.$$

Since $pL \leq L^2$ we need to give relations expressing pa, pb, pc, pd as linear combinations of ba, ca, dc. We can express these relations in the form

$$\begin{pmatrix} pa \\ pb \\ pc \\ pd \end{pmatrix} = A \begin{pmatrix} ba \\ ca \\ dc \end{pmatrix}$$

where A is a 4×3 matrix with entries in $\mathbb{Z}_p$. The isomorphism classes of 4-generator Lie rings of p-class 2 and order p^7 satisfying the relations $da = cb = 0$, $db = ca$, correspond to the orbits of 4×3 matrices A under transformations of the form

$$A \longmapsto (\alpha\delta - \beta\gamma)^{-1} \begin{pmatrix} \alpha\lambda & \beta\lambda & \beta\mu & -\alpha\mu \\ \gamma\lambda & \delta\lambda & \delta\mu & -\gamma\mu \\ \gamma\nu & \delta\nu & \delta\xi & -\gamma\xi \\ -\alpha\nu & -\beta\nu & -\beta\xi & \alpha\xi \end{pmatrix} A \begin{pmatrix} \lambda^2 & 2\lambda\mu & \mu^2 \\ \lambda\nu & \lambda\xi + \mu\nu & \mu\xi \\ \nu^2 & 2\nu\xi & \xi^2 \end{pmatrix}^{-1}.$$

We can prove that the number of orbits is 550 when $p = 3$ and

$$\begin{array}{ll} p^5 + p^4 + 4p^3 + 6p^2 + 18p + 19 & \text{if} \quad p = 1 \bmod 3, \\ p^5 + p^4 + 4p^3 + 6p^2 + 16p + 17 & \text{if} \quad p = 2 \bmod 3, \end{array}$$

but we were unable to write down an *explicit parameterised description valid for all primes* for the set of orbit representatives. Hence, when writing down the finite presentations for these immediate descendants with order p^7, we compute directly a set of representatives for the given p. While this computation is extremely fast for small primes, taking less than one second for the prime 3, the time taken to compute such a set of representatives grows rapidly with p.

5 Accuracy of results

We have taken various steps to ensure that the enumeration and the resulting database are accurate.

We used our implementations of the p-group generation algorithm and the enumeration algorithm of Eick & O'Brien [6] to confirm for various primes the numbers of descendants quoted in Tables 1 and 3. We confirmed the figures in Table 1 for #31 for $p \leq 19$ and for #41 for $p \leq 11$; and the figures in Table 3 for #23, #24, #34 and #39 for $p \leq 23$. In all other cases, we confirmed the claims for $p \leq 31$. Observe that the primes can be partitioned according to the values of the residues which occur in the formulae for the various number of descendants. Where possible, we considered additional larger representative primes.

We used invariant calculations and the isomorphism algorithm of O'Brien [15] to demonstrate that the database descriptions of the immediate descendants with order p^7 of 39 of the 42 capable groups with order dividing p^5 is complete and irredundant for $p \leq 13$; this calculation was completed only for $p \leq 7$ for each of #31, #39 and #41. In all cases, we demonstrated that this property holds for the database descriptions of grandchildren; in many cases, we established its veracity for $p \leq 59$.

Acknowledgements

We thank M.F. Newman for helpful conversations on aspects of this work, and useful comments on a draft of the paper.

References

[1] Hans Ulrich Besche, Bettina Eick, and E.A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12:623–644, 2002.

[2] N. Blackburn. On a special class of p-groups. *Acta Math.*, 100:45–92, 1958.

[3] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. *J. Symbolic Comput.*, 24:235–265, 1997.

[4] N. Bourbaki. *Éléments de mathématique. Fasc. XXXVII. Groupes et algèbres de Lie. Chapitre II: Algèbres de Lie libres. Chapitre III: Groupes de Lie.* Hermann, Paris, 1972. Actualités Scientifiques et Industrielles, No. 1349.

[5] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.3.* (`http://www.gap-system.org`), 2002.

[6] Bettina Eick and E.A. O'Brien. Enumerating p-groups. *J. Austral. Math. Soc. Ser. A*, 67:191–205, 1999.

[7] George Havas, M.F. Newman, and M.R. Vaughan-Lee. A nilpotent quotient algorithm for graded Lie rings. *J. Symbolic Comput.*, 9:653–664, 1990.

[8] G. Higman, Enumerating p-groups. II. Problems whose solution is PORC. *Proc. London Math. Soc.* (3) **10** (1960), 566–582.

[9] N. Jacobson, *Lie algebras*, Wiley-Interscience, New York, 1962.

[10] Rodney James, M.F. Newman, and E.A. O'Brien. The Groups of Order 128. *J. Algebra*, 129(1):136–158, 1990.

[11] M.F. Newman, Groups of prime-power order, *Groups—Canberra 1989*, 49–62, Lecture Notes in Math., **1456**, Springer, Berlin, 1990.

[12] M.F. Newman and E.A. O'Brien. Application of computers to questions like those of Burnside, II. *Internat. J. Algebra Comput.*, 6:593–605, 1996.

[13] M.F. Newman, E.A. O'Brien, and M.R. Vaughan-Lee, Groups and nilpotent Lie rings whose order is the sixth power of a prime, *J. Algebra*, **278**, 383-401, 2004.

[14] E.A. O'Brien. The p-group generation algorithm. *J. Symbolic Comput.*, 9:677–698, 1990.

[15] E.A. O'Brien. Isomorphism testing for p-groups. *J. Symbolic Comput.*, 17:133–147, 1994.

[16] Charles C. Sims. *Computation with finitely presented groups.* Cambridge University Press, 1994.

[17] E.A. O'Brien and M.R. Vaughan-Lee, Notes on the construction of the groups with order dividing p^7, (`www.math.auckland.ac.nz/~obrien/research/p7.html`), 2004.

[18] David Wilkinson, The groups of exponent p and order $p \geq 7$ (p any prime), *J. Algebra*, **118**, 109–119, 1988.

Department of Mathematics
University of Auckland
Auckland
New Zealand
obrien@math.auckland.ac.nz

Christ Church
University of Oxford
OX1 1DP
United Kingdom
michael.vaughan-lee@christ-church.oxford.ac.uk