Journal of Algebra 322 (2009) 791–801

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

On counterexamples to the Hughes conjecture

George Havas [a,*,1], Michael Vaughan-Lee [b]

[a] *ARC Centre for Complex Systems, School of Information Technology and Electrical Engineering, The University of Queensland, Queensland 4072, Australia*
[b] *Christ Church, Oxford OX1 1DP, United Kingdom*

ARTICLE INFO

Article history:
Received 5 January 2009
Available online 29 April 2009
Communicated by Eamonn O'Brien

Dedicated to John Cannon and Derek Holt in recognition of distinguished contributions to mathematics

Keywords:
Hughes conjecture
p-Groups
Counterexamples
Power-commutator presentations
Lie rings

ABSTRACT

In 1957 D.R. Hughes published the following problem in group theory. Let G be a group and p a prime. Define $H_p(G)$ to be the subgroup of G generated by all the elements of G which do not have order p. Is the following conjecture true: either $H_p(G) = 1$, $H_p(G) = G$, or $[G : H_p(G)] = p$? After various classes of groups were shown to satisfy the conjecture, G.E. Wall and E.I. Khukhro described counterexamples for $p = 5, 7$ and 11. Finite groups which do not satisfy the conjecture, anti-Hughes groups, have interesting properties. We give explicit constructions of a number of anti-Hughes groups via power-commutator presentations, including relatively small examples with orders 5^{46} and 7^{66}. It is expected that the conjecture is false for all primes larger than 3. We show that it is false for $p = 13, 17$ and 19.

1. Introduction

Hughes [11] published the following problem in group theory.

Let G be a group and p a prime. Define $H_p(G)$ to be the subgroup of G generated by all the elements of G which do not have order p. Is the following conjecture true: either $H_p(G) = 1$, $H_p(G) = G$, or $[G : H_p(G)] = p$?

$H_p(G)$ is called the Hughes subgroup. For finite groups this conjecture has become known as the Hughes conjecture, and all groups in this paper are finite unless otherwise stated.

* Corresponding author.
E-mail addresses: havas@itee.uq.edu.au (G. Havas), vlee@maths.ox.ac.uk (M. Vaughan-Lee).
[1] Partially supported by the Australian Research Council.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2009.04.011

Initial positive results about the conjecture include the following. In 1956, before publication of the conjecture and perhaps as partial justification for it, Hughes [10, Lemma 4] proved the conjecture for $p = 2$ for all (finite or infinite) groups. Next, in 1958 Straus and Szekeres [21] proved it for $p = 3$ for all (finite or infinite) groups. Then, in 1959 Hughes and Thompson [12] proved that the Hughes conjecture is true for any finite group that is not a p-group, and focus shifted to finite p-groups.

Later work culminated in some positive results about finite p-groups with specific structural properties. The conjecture was proved for metabelian groups in 1969 by Hogan and Kappe [8] and for groups with nilpotency class less than $2p - 1$ in 1971 by Macdonald [19] (who earlier [18] showed the same for 2-generator groups with class less than $2p$). But these results followed the discovery of the first counterexamples. (Later counterexamples prove that Macdonald's class bounds are tight in the situations for which we have counterexamples.)

In 1967, G.E. Wall [23] found a counterexample for $p = 5$. Wall's counterexample relies on the existence of a Lie relator of weight 9 which holds in the associated Lie rings of Burnside groups of exponent 5, but is not a consequence of the 4-Engel identity. In fact Wall found a Lie relator of weight $2p - 1$ which holds in the associated Lie rings of groups of exponent p, and conjectured that if $p \geqslant 5$ then this Lie relator is not a consequence of the $(p - 1)$-Engel identity in characteristic p. (It has been known since the 1950's that the associated Lie rings of groups of exponent p have characteristic p and satisfy the $(p - 1)$-Engel identity.) Wall confirmed his conjecture for $p = 5$ by hand calculation in related associative rings. John Cannon [3] used a computer to confirm Wall's conjecture for $p = 5$ and 7. Cannon's work on this is described in more detail [2, Chapter VI] in his doctoral thesis which was supervised by Wall, and the result was extended to $p = 11$. Wall amplified his proof in [24]. It follows from Wall's and Cannon's work that there are 3-generator counterexamples to the Hughes conjecture for $p = 5, 7$ and 11.

Later, in 1981 and 1982, E.I. Khukhro [13,14] found further counterexamples. Khukhro's 1981 counterexample is a 3-generator 5-group of order 5^{917} and class 9 with Hughes subgroup of index 25, and his 1982 counterexample is a 2-generator 7-group of order 7^{1075} and class 14 with Hughes subgroup of index 49. Khukhro's 3-generator 5-group example relies on the existence of Wall's new Lie relator for $p = 5$. His 2-generator 7-group example is slightly more subtle. An important instance of Wall's new relator has multiweight $(p - 1, p - 1, 1)$ in three variables x, y, z. If we write this relator as $f_p(x, y, z)$, then $f_p(x, y, [x, y])$ has multiweight (p, p) in two variables x and y. So the associated Lie ring of the Burnside group $B(2, 7)$ satisfies the relation $f_7(x, y, [x, y]) = 0$. Khukhro showed that $f_7(x, y, [x, y]) = 0$ is *not* a consequence of the 6-Engel identity, and deduced the existence of his 2-generator 7-group counterexample to the Hughes conjecture.

When $p = 5$ the corresponding relation $f_5(x, y, [x, y]) = 0$ of weight 10 *is* a consequence of the 4-Engel identity. This is why there is no 2-generator 5-group counterexample with class 10. In fact there is no 2-generator counterexample for $p = 5$ at all. This can be confirmed by an analogous computation to the one we use later in Section 2. We compute Q, the largest nilpotent quotient of the 2-generator 5-group with the fifth powers of all elements outside its derived group trivial. It turns out that Q actually has exponent 5, so Q is the same as the restricted Burnside group $R(2, 5)$. (This is the basis for the result for $p = 5$ in [16, Corollary 2].)

Having proved the existence of some anti-Hughes groups, Khukhro proved more. In [15] he showed that almost all p-groups satisfy the Hughes conjecture, in a well defined sense. He went on to show that the existence of a d-generator anti-Hughes group for a prime p implies the existence of a largest such group, so that all d-generator anti-Hughes groups for that prime are quotients of it. Nice overviews of his and other results on the Hughes' problem appear in [16,17].

As pointed out by Macdonald [18], 2-generator anti-Hughes groups provide counterexamples to various conjectures about p-groups. Indeed this work was motivated in part by a request from R.K. Dennis for small counterexamples. Dennis was investigating problems about the exponents of generating sets of finite groups and anti-Hughes groups provide interesting case studies for p-groups. In particular, our 2-generator anti-Hughes groups are groups with exponent p^2 in which all elements of any minimal generating set have order p.

This makes it worthwhile for us to be able to compute with anti-Hughes groups. Calculations with p-groups can be carried out effectively with the use of power-commutator presentations (PCPs). Such computations can be done using the p-quotient algorithm as implemented in Magma [1], and

as a share package in GAP [4]. Detailed descriptions of these presentations, their algorithms, some applications and further references are provided in [9,20]. Suffice it to say, we can efficiently answer very many interesting questions about p-groups if we have PCPs for them.

Although Khukhro gave precise definitions of his groups, it seems that up till now nobody has actually constructed power-commutator presentations for them. This is not surprising, since computing PCPs for the groups is a non-trivial exercise. We construct PCPs for Khukhro's two counterexamples, and we also construct quotient groups of order 5^{46} and 7^{66} (among many others), which are quite small counterexamples to the Hughes conjecture. They are very much smaller than previously known, but we have no reason to believe that these are the smallest counterexamples.

Supplementary materials, including some MAGMA programs which compute anti-Hughes groups, are available at our websites [6], together with their outputs. These outputs give some further details on our anti-Hughes groups and also provide information on computer resource usage.

Using the same types of ideas, we have constructed PCPs for a 3-generator 7-group of class 13 and order 7^{2631} which is an anti-Hughes group, and for a 2-generator counterexample of class 22 and order 11^{2408}.

Our group constructions are independent of the theory of Lie relators in Burnside groups, but Khukhro has shown that 3-generator, class $2p-1$, counterexamples to the Hughes conjecture exist if and only if there is a new Lie relator of weight $2p-1$. Similarly he has shown that 2-generator, class $2p$, counterexamples exist if and only if the relation $f_p(x, y, [x, y]) = 0$ is not a consequence of the $(p-1)$-Engel identity. So our group constructions give independent verification of the existence of these new relators for $p = 5, 7$ and 11.

We have also carried out Lie algebra calculations to show that the relation

$$f_p\big(x, y, [x, y]\big) = 0$$

is not a consequence of the $(p-1)$-Engel identity for $p = 13, 17$ and 19. So 2-generator counterexamples to the Hughes conjecture also exist for $p = 13, 17$ and 19, though it is not easy to construct them. We have some hope of eventually constructing a PCP for a 2-generator 13-group of class 26 which is a counterexample, but the computations are taking months of computer time and are far from complete. The theory of Lie relators in Burnside groups is rather tricky, and we do not explore this subject here. Some details may be found in [22] where Theorem 2.5.1 gives a sequence of multilinear identities $K_n = 0$ $(n \geqslant 2)$ which hold in the associated Lie rings of Burnside groups of prime power exponent p^k. Wall's identity is equivalent to $K_{2p-1} = 0$, which is multilinear in $2p-1$ variables. So we have (modulo constants)

$$f_p(x, y, z) = K_{2p-1}(\underbrace{x, x, \ldots, x}_{p-1}, \underbrace{y, y, \ldots, y}_{p-1}, z),$$

and

$$f_p\big(x, y, [x, y]\big) = K_{2p-1}\big(\underbrace{x, x, \ldots, x}_{p-1}, \underbrace{y, y, \ldots, y}_{p-1}, [x, y]\big).$$

It seems very likely that the relation $f_p(x, y, [x, y]) = 0$ is not a consequence of the $(p-1)$-Engel identity for any prime $p > 5$, but we have no idea how one might prove this general result.

In each of our anti-Hughes groups the Hughes subgroup has index p^2. In 1986 Wall [25] showed that if, for a prime p, for all $j = 1, \ldots, n$ the law $K_{j(p-1)+1}$ is not a consequence of the K_i with smaller indices, then there is a counterexample where the index of the Hughes subgroup is p^n. This criterion does not hold for $n = 3$ and $p = 5$, so Wall's theory does not yield a 5-group with Hughes subgroup of index 5^3. The question of whether Wall's criterion holds for $n = 3$ and $p = 7$ seems to be beyond the range of direct computational investigation.

Our anti-Hughes groups have class $2p-1$ or $2p$ because these are the lowest possible classes. The restricted Burnside groups $R(3,5)$ and $R(2,7)$ are known to have classes 17 and 28, respectively, so corresponding counterexamples exist with classes at least as big as those.

It is worth noting that the existence of a d-generator anti-Hughes p-group G implies the existence of n-generator anti-Hughes p-groups for all $n \geqslant d$. This follows from consideration of $K = G \times C_p$. Clearly $H_p(K) = H_p(G) \times C_p$.

2. Khukhro's 7-group

Following Khukhro [14] we let F be the free group of rank 2, and we let N be the normal subgroup of F generated by $\{g^7 \mid g \notin F'\}$. We consider the nilpotent quotients of F/N, looking for a quotient which does not have exponent 7. Khukhro's theoretical work guarantees that such a quotient exists. As he proved, the class 13 quotient of F/N has exponent 7, but the class 14 quotient does not. In fact the class 14 quotient of $B(2,7)$ has order 7^{1074}, but the class 14 quotient of F/N has order 7^{1075}. Let this class 14 quotient be H, and let H be generated by a and b. Then $[b,a]$ has order 49. Also $\gamma_3(H)$ has exponent 7 and H' has class 6. It follows that $([b,a]g)^7 = [b,a]^7$ for all $g \in \gamma_3(H)$, and this implies that all the elements $[b,a]g$ $(g \in \gamma_3(H))$ have order 49. So the Hughes subgroup $\langle g \in H \mid g^7 \neq 1\rangle = H'$, which has index 49.

The difficulty with computing a PCP for this group is finding a sufficiently small generating set for the normal subgroup N. The p-quotient algorithm, as implemented in Magma and as a share package in GAP, incorporates very sophisticated techniques for finding relatively small test sets of words for enforcing exponent p, but this is precisely what we do *not* want to do. However these same techniques are also appropriate for finding a relatively small set of generators for N.

We construct H as follows (using the Magma program [6, `gettestwords.m`] followed by the start of [6, `p7g2r1075.m`]). First we construct the class 13 quotient of $B(2,7)$ (which we denote by $B(2,7:13)$), and then we construct the p-covering group [9, pp. 357–360] of this class 13 quotient. Call this p-covering group Q. It has order 7^{1258}. Suppose that Q is generated by a and b. Let $G = Q/N$, where N is the normal subgroup of Q generated by $\{g^7 \mid g \notin Q'\}$. This is Khukhro's counterexample to the Hughes conjecture of order 7^{1075} and class 14.

Finding a reasonably small set of 7th powers which generate N requires a certain amount of thought! Every element outside the derived group of Q is a power of an element from the set

$$S = \{ag \mid g \in Q'\} \cup \left\{a^i bg \;\middle|\; 0 \leqslant i \leqslant 6,\ g \in Q'\right\}.$$

Now N is contained in the centre of Q, since Q is the p-covering group of a group of exponent 7. In fact $N \leqslant M$, where M is the p-multiplicator [9, p. 364] of $B(2,7:13)$. Also S is a normal subset of Q, and S is a union of conjugacy classes of Q. So if we let T be a set of representatives for these conjugacy classes, then N is generated by $\{t^7 \mid t \in T\}$. Since M is central in Q and of exponent 7, it is only necessary to compute these conjugacy classes modulo M. But even so, this set T is huge. However we can reduce the set of 7th power relations significantly. It will be helpful in what follows if we can assume that $\gamma_3(Q)$ has exponent 7. This is easy to check. Since Q has class 14 it follows that $\gamma_3(Q)$ has class at most 4, so it is only necessary to check that the elements from a set of generators of $\gamma_3(Q)$ all have order 7. Now $\gamma_3(Q)$ is the normal closure of $[b,a,a]$ and $[b,a,b]$, and so it is only necessary to check that $[b,a,a]^7 = [b,a,b]^7 = 1$. This is easily done.

The first major reduction is the following lemma which implies that we only need to compute a set of representatives for the conjugacy classes of S modulo $\gamma_9(Q)M$.

Lemma 1. *If $g \in Q$ and $h \in \gamma_9(Q)$ then $(gh)^7 = g^7$.*

Proof. The Hall collection process implies that $(gh)^7 = g^7 h^7 u v$, where u is a product of 7th powers of elements in the derived group of $\langle g,h\rangle$, and where v lies in the 7th term of the lower central series of $\langle g,h\rangle$. Since $\gamma_3(Q)$ has exponent 7, it follows that $h^7 = u = 1$. And since $h \in \gamma_9(Q)$, it follows that $v \in \gamma_{15}(Q) = \{1\}$. □

So we need to compute the conjugacy classes of S modulo $\gamma_9(Q)M$. Since

$$Q/\gamma_9(Q)M \cong B(2,7:8),$$

this is equivalent to computing conjugacy classes in $B(2,7:8)$. In principle, MAGMA can compute these conjugacy classes with a single command. But, as we shall see, S is a union of 8×7^{23} conjugacy classes modulo $\gamma_9(Q)M$. Since the MAGMA command would attempt to store representatives for all these classes, MAGMA would quickly run out of memory. So we compute a set of representatives "by hand" — we are able to do this symbolically, without storing representatives for each individual class. Let G be the class 8 quotient of $B(2,7)$, and (with some abuse of notation) let a and b be the generators of G. We let $S_1 = \{ag \mid g \in \gamma_2(G)\}$ and we let $S_2 = \{a^i bg \mid 0 \leqslant i \leqslant 6,\ g \in \gamma_2(G)\}$. We want to compute representatives for the conjugacy classes of S_1 and S_2.

First consider the set S_1. Working modulo $\gamma_3(G)$ we see that a is conjugate to $a[b,a]^k$ for all $k = 0, 1, \ldots, 6$. So all the elements of S_1 are conjugate to ag for some $g \in \gamma_3(G)$. Working modulo $\gamma_4(G)$, we see that $\gamma_3(G)$ is generated by $[b,a,a]$ and $[b,a,b]$. (These are PCP generators $G.4$ and $G.5$ of G.) If $g \in \gamma_3(G)$ then

$$(ag)^{[b,a]^k} = ag[b,a,a]^{-k} \quad \text{modulo } \gamma_4(G),$$

and so a complete set of representatives for the conjugacy classes of S_1 modulo $\gamma_4(G)$ is $a[b,a,b]^k$ $(0 \leqslant k \leqslant 6)$.

Working modulo $\gamma_5(G)$ we see that $\gamma_4(G)$ is generated by $[b,a,a,a]$, $[b,a,a,b]$ and $[b,a,b,b]$. (These are PCP generators $G.6$, $G.7$ and $G.8$ of G.) If $g \in \gamma_3(G)$ then

$$(ag)^{[b,a,a]^r[b,a,b]^s} = ag[b,a,a,a]^{-r}[b,a,a,b]^{-s} \quad \text{modulo } \gamma_5(G),$$

and so a complete set of representatives for the conjugacy classes of S_1 modulo $\gamma_5(G)$ is

$$a[b,a,b]^r[b,a,b,b]^s \quad (0 \leqslant r, s \leqslant 6).$$

Next we notice that $\gamma_5(G)$ is an elementary abelian subgroup of G, and that $[a,\gamma_4(G)]$ is a subgroup of $\gamma_5(G)$. We let K be a complement for $[a,\gamma_4(G)]$ in $\gamma_5(G)$, so that $[a,\gamma_4(G)] \cap K = \{1\}$ and $[a,\gamma_4(G)]K = \gamma_5(G)$. Fortunately we are able to choose the complement K so that it is also a complement for all the groups $[a[b,a,b]^r[b,a,b,b]^s, \gamma_4(G)]$ for all $0 \leqslant r, s \leqslant 6$. So a complete set of representatives for the conjugacy classes of S_1 is

$$a[b,a,b]^r[b,a,b,b]^s k \quad (0 \leqslant r, s \leqslant 6,\ k \in K).$$

Similarly we see that a complete set of representatives for the conjugacy classes of S_2 modulo $\gamma_5(G)$ is

$$a^i b[b,a,a]^r[b,a,a,a]^s \quad (0 \leqslant i, r, s \leqslant 6).$$

We are similarly able to find a single complement L in $\gamma_5(G)$ for all the subgroups

$$\left[a^i b[b,a,a]^r[b,a,a,a]^s, \gamma_4(G)\right].$$

So a complete set of representatives for the conjugacy classes of S_2 is

$$a^i b[b,a,a]^r[b,a,a,a]^s k \quad (0 \leqslant i, r, s \leqslant 6,\ k \in L).$$

We compute K and L using [6, `gettestwords.m`]. The subgroup K is generated by $G.10$, $G.12$, $G.14$, $G.19$, $G.22$, $G.23$, $G.27$, $G.31$, $G.32$, $G.35$, $G.37$, $G.39$, $G.43$, $G.45$, $G.47$, $G.49$, $G.51$, $G.53$, $G.54$,

$G.56$, $G.58$, and the subgroup L is generated by $G.9$, $G.11$, $G.13$, $G.15$, $G.17$, $G.20$, $G.25$, $G.28$, $G.30$, $G.33$, $G.36$, $G.38$, $G.40$, $G.42$, $G.44$, $G.46$, $G.48$, $G.50$, $G.52$, $G.55$, $G.57$. It is not clear from the method of constructing these sets of representatives that they are irredundant sets, but in fact they are. MAGMA shows that the centraliser of a in G has order 7^{25}, which implies that the conjugacy class of a has size 7^{33}. Since G is relatively free, all the elements ag $(g \in G')$ have conjugacy classes of size 7^{33}, and since there is a total of 7^{56} elements of the form ag this implies that there are 7^{23} conjugacy classes. The same considerations apply to the elements $a^i bg$ $(g \in G')$.

We now lift these representatives for the conjugacy classes of S_1 and S_2 to preimages in Q. The preimage of K is generated by $Q.10, Q.12, \ldots, Q.58$ modulo $\gamma_9(Q)$, and the preimage of L is generated by $Q.9, Q.11, \ldots, Q.57$ modulo $\gamma_9(Q)$.

The most significant reduction in the set of generators for $N = \langle g^7 \mid g \notin Q' \rangle$ comes from an application of Higman's Lemma [7] (see also [20, pp. 562–563]). Higman shows that if $x_1, x_2, \ldots, x_m$ are elements of a group G, then $(x_1 x_2 \ldots x_m)^n = uv$, where u lies in the subgroup generated by elements of the form $(x_i x_j \ldots x_k)^n$ where $1 \leqslant i < j < \cdots < k \leqslant m$ and where $\{i, j, \ldots, k\}$ is a proper subset of $\{1, 2, \ldots, m\}$, and where v is a product of commutators of weight at least m, each involving all of the generators $x_1, x_2, \ldots, x_m$. We apply this lemma to the 7th power of one of our representatives. Let

$$w = a[b, a, b]^r [b, a, b, b]^s (Q.10)^{\alpha_{10}} (Q.12)^{\alpha_{12}} \ldots (Q.58)^{\alpha_{58}}.$$

The PCP generators of Q all have weights reflecting the terms of the lower central series of Q which they lie in. Thus a has weight 1, $[b, a, b]$ has weight 3, $[b, a, b, b]$ has weight 4, $Q.10$ has weight 5, …, and $Q.58$ has weight 8. We define the weight of w to be

$$1 + 3r + 4s + 5\alpha_{10} + \cdots + 8\alpha_{58}.$$

We also define the exponent length of w to be $1 + r + s + \alpha_{10} + \cdots + \alpha_{58}$. We show that we need only impose relations $w^7 = 1$ for words of weight at most 14 (because 14 is the nilpotency class of Q).

So suppose that w has weight $k > 14$. By a *subword* of w we mean a word of the form

$$w' = a^\beta [b, a, b]^{r'} [b, a, b, b]^{s'} (Q.10)^{\beta_{10}} (Q.12)^{\beta_{12}} \ldots (Q.58)^{\beta_{58}}$$

where $\beta \leqslant 1$, $r' \leqslant r$, $s' \leqslant s$, $\beta_{10} \leqslant \alpha_{10}$, …, $\beta_{58} \leqslant \alpha_{58}$, and where the exponent length of w' is less than the exponent length of w. We apply Higman's Lemma, with m equal to the exponent length of w, and $n = 7$. We then substitute a for x_1, substitute $[b, a, b]$ for $x_2, x_3, \ldots, x_{r+1}$, substitute $[b, a, b, b]$ for $x_{r+2}, x_{r+3}, \ldots, x_{r+s+1}$, and so on. Higman's Lemma implies that $w^7 = uv$, where u lies in the subgroup generated by elements of the form $(w')^7$ with w' a subword of w, and where v is a product of commutators each of which lie in $\gamma_k(Q)$ where k is the weight of w. Note that if w' is a subword of w then either w' is another of our representatives for the conjugacy classes of S_1 with lower weight than w, or $w' \in \gamma_3(Q)$ which implies that $(w')^7 = 1$. So if $k > 14$, then by repeated application of Higman's Lemma we see that w^7 lies in the subgroup generated by the elements $(w')^7$ where $w' \in S_1$ is a subword of w of weight at most 14.

There is a further reduction we can make. Suppose that w has weight at most 14, and also suppose that w has exponent length greater than 1 but less than 7. As we mentioned above, the Hall collection process implies that if g, h are elements of a group, then $(gh)^7 = g^7 h^7 w_1 w_2$, where w_1 is a product of 7th powers of commutators involving g and h, and where w_2 is a product of commutators in g and h of weight at least 7. We combine this result with the proof of Higman's Lemma. We let m be the exponent length of w, and we apply this result to the word $(x_1 x_2 \ldots x_m)^7$, taking $g = x_1 x_2 \ldots x_{m-1}$ and $h = x_m$. So

$$(x_1 x_2 \ldots x_m)^7 = (x_1 x_2 \ldots x_{m-1})^7 x_m^7 w_1 w_2$$

where w_1 is a product of 7th powers of commutators with at least one entry x_m, and w_2 is a product of commutators each of which has weight at least 7 and each of which has at least one entry x_m.

Expanding these commutators, we may assume that all the entries in the commutators in the products w_1 and w_2 lie in the set $\{x_1, x_2, \ldots, x_m\}$. So we have

$$w_1^{-1} x_m^{-7} (x_1 x_2 \ldots x_{m-1})^{-7} (x_1 x_2 \ldots x_m)^7 = w_2.$$

Using Higman's Lemma again, we see that this implies that $(x_1 x_2 \ldots x_m)^7 = uv$ where

- u lies in the subgroup generated by elements of the form $(x_i x_j \ldots x_k)^7$ where $1 \leqslant i < j < \cdots < k \leqslant m$ and where $\{i, j, \ldots, k\}$ is a proper subset of $\{1, 2, \ldots, m\}$ and by elements of the form c^7 where c is a commutator with at least one entry x_m, and
- v is a product of commutators of weight at least 7 each involving all of the generators $x_1, x_2, \ldots, x_m$.

We now substitute PCP generators of Q for the elements $x_1, x_2, \ldots, x_m$ as above. There are two key points to note.

1) Elements of the form c^7 where c is a commutator with at least one entry x_m become trivial under the substitution since $\gamma_3(Q)$ has exponent 7.
2) Since $m < 7$, commutators of weight at least 7 involving all of the generators $x_1, x_2, \ldots, x_m$ must have repeated entries. In particular, they become trivial under the substitution if $k + 7 - m > 14$ where k is the weight of w.

So if $k + 7 - m > 14$ then we see that w^7 lies in the subgroup generated by elements $(w')^7$, where w' is a subword of w.

The combined effect of all this is that the subgroup generated by the elements $(ag)^7$ $(g \in Q')$ is generated by the elements w^7 where w has the form

$$w = a[b, a, b]^r [b, a, b, b]^s (Q.10)^{\alpha_{10}} (Q.12)^{\alpha_{12}} \ldots (Q.58)^{\alpha_{58}}, \tag{1}$$

and where if w has weight k and exponent length m then $k \leqslant 14$ and $k + 7 - m \leqslant 14$.

We now consider the subgroup generated by the elements $(a^i bg)^7$ $(g \in Q')$. As we showed above, this subgroup is generated by elements w^7 where w has the form

$$w = a^i b[b, a, a]^r [b, a, a, a]^s (Q.9)^{\alpha_9} (Q.11)^{\alpha_{11}} \ldots (Q.57)^{\alpha_{57}}. \tag{2}$$

Using the same argument as above, we see that if this word has weight k and exponent length m where $k > 14$ or $k + 7 - m > 14$, then w^7 lies in the subgroup generated by elements $(w')^7$ where w' is a subword of w. Such a subword w' has one of three types. It could be a word of the same form as w (which is fine), or we could have $w' \in \gamma_3(Q)$ (which is fine, since $\gamma_3(Q)$ has exponent 7), or we could have

$$w' = a^{i'} [b, a, a]^{r'} [b, a, a, a]^{s'} (Q.9)^{\beta_9} (Q.11)^{\beta_{11}} \ldots (Q.57)^{\beta_{57}}$$

for some i', r', s', β_9, …, β_{57}. In this last case $(w')^7$ lies in the subgroup generated by 7th powers of elements of the form (1). So the subgroup $\langle g^7 \mid g \notin Q' \rangle$ is generated by elements of the form (1) and (2) which have weight k and exponent length m satisfying $k \leqslant 14$, $k + 7 - m \leqslant 14$. There is a total of 272 of these words.

3. Khukhro's 5-group

The construction of Khukhro's 3-generator 5-group is very similar to the construction of his 2-generator 7-group, as shown in [6, `p5g3r917.m`]. We first construct the 5-covering group Q of the class 8 quotient of $B(3, 5)$. Denote the generators of Q by a, b, c. Then we let N be the normal

subgroup of Q generated by $\{g^5 \mid g \notin \langle c\rangle Q'\}$. We let $H = Q/N$. Then H is a group of order 5^{917}, whereas $B(3,5:9)$ has order 5^{916}. The element $cN \in H$ has order 25. If g is any element of Q' then there is an automorphism of H mapping aN to aN, bN to bN, and mapping cN to cgN, and so all the elements cgN have order 25. This implies that the Hughes subgroup of H has index 25.

Once again, the main difficulty in carrying out this computation is in finding a relatively small number of 5th powers which generate N. Using similar arguments to those above, we see that N is generated by the 5th powers of conjugacy class representatives of the following:

$$a[c,b]^r k \quad (0 \leqslant r \leqslant 4,\ k \in K_1), \tag{3}$$

$$a^i b[c,a]^r k \quad (0 \leqslant i, r \leqslant 4,\ k \in K_2), \tag{4}$$

$$a^i b^j c[b,a]^r k \quad (0 \leqslant i, j, r \leqslant 4,\ i+j \neq 0,\ k \in K_3), \tag{5}$$

where K_1, K_2 and K_3 are certain sets of size 5^{29} consisting of products of PCP generators of Q of weights 3, 4 and 5. It is easy to check that Q' has exponent 5, so using the same arguments as above we see that the subgroup generated by 5th powers of elements of type (3) and (4) is generated by words of type (3) and (4) with weight k and exponent length m, where $k \leqslant 9$ and $k+5-m \leqslant 9$. However there is a problem with words of type (5). We use Higman's Lemma to show that if w has weight k and exponent length m where $k > 9$ or $k+5-m > 9$, then w^5 lies in the subgroup generated by elements $(w')^5$ where w' is a subword of w. The problem is that $a^i b^j c[b,a]^r k$ has subwords of the form $c[b,a]^r k$, and we do *not* want to include 5th powers of these words as relations. The "work around" to this problem is as follows. If $j > 0$ we write

$$a^i b^j c[b,a]^r k = a^i b^{j-1}(bc)[b,a]^r k$$

and if $j = 0$ but $i > 0$ then we write

$$a^i c[b,a]^r k = a^{i-1}(ac)[b,a]^r k.$$

Then we redefine the weight and exponent length of the word by letting (bc) (or (ac)) contribute only one to the weight and one to the exponent length. Thus the redefined weight and exponent length are both one less than the original weight and exponent length. If $w = a^i b^{j-1}(bc)[b,a]^r k$, and if the redefined exponent length is m, then when we apply Higman's Lemma, we substitute a for $x_1, x_2, \ldots, x_i$, substitute b for $x_{i+1}, x_{i+2}, \ldots, x_{i+j-1}$, substitute bc for x_{i+j}, and then carry on as before. This has the effect that a subword of $x_1 x_2 \ldots x_m$ either maps to a subword of w of type (5) under the substitution, or to a conjugate of a power of an element of type (3) or (4), or to an element of Q'. We treat words of the form $a^{i-1}(ac)[b,a]^r k$ similarly. So modifying the definitions of weight and exponent length for words of type (5) in this way we see that N is generated by the 5th powers of words of type (3), (4) and (5) with weight k and exponent length m with $k \leqslant 9$ and $k+5-m \leqslant 9$. There are 1201 of these words.

4. Constructing smaller counterexamples

It is easy to obtain quotient groups of the two groups constructed above which are still counterexamples to the Hughes conjecture. Consider our 2-generator 7-group of order 7^{1075}; its centre has order 7^{407}. The element $[b,a]^7$ lies in the centre of H, but we can factor out a subgroup of the centre of order 7^{406} which does not contain $[b,a]^7$. This gives us a counterexample to the Hughes conjecture of order 7^{669}. We can continue iterating this procedure until we obtain a quotient group with centre of order 7. In this way we obtain counterexamples with order as small as 7^{117}, see [6, `p7g2r1075.m`].

There is a vast amount of choice in picking subgroups of the centre to factor out in this way, so there is no reason to suppose that 7^{117} is the smallest group you could obtain with such a procedure. A simple method is to look at the PCP generators which have nonzero exponent in the evaluation

of $[b,a]^7$. For each such PCP generator (there are 222 of these), we construct complements and factor them out as above, yielding final anti-Hughes groups with orders ranging from 7^{117} to 7^{121}, see [6, `p7exp.m`].

Applying an analogous procedure to Khukhro's example of order 5^{917} we obtain an anti-Hughes group of order 5^{99}, see [6, `p5g3r917.m`].

We also tried another approach. The underlying theory implies that there is a 2-generator anti-Hughes 7-group of class 14 in which the normal closures of the generators both have class 7. The MAGMA implementation of the p-quotient algorithm has a facility (via the `MaxOccurrence` parameter) which enables you to force the normal closures of the generators to have specified classes. Using this we obtain an anti-Hughes group of order 7^{597}. Factoring out subgroups of the centre as above, the smallest anti-Hughes quotient we found this way has order 7^{119}, see [6, `p7g2mo.m`]. This computation is much faster (compared with `p7exp.m`) because it starts with a smaller group (but leads to a larger reduced group after factoring out subgroups of the centre).

Next we tried adding defining relators to our group. After some experimentation we found that if we start with the group generated by a and b, with relators

$$[b,a,a,a,a,b], \qquad [b,a,a,a,a,a,b], \qquad [b,a,a,a,a,a,a,b],$$

$$[a,b,b,b,b,a], \qquad [a,b,b,b,b,b,a], \qquad [a,b,b,b,b,b,b,a],$$

and impose the condition that the normal closures of a and b are nilpotent of class 7, then we can construct a counterexample of order 7^{159} and class 14. Repeatedly factoring out complements to $[b,a]^7$ in the centre of this group we obtain an example of order 7^{71}, see [6, `p7g2qmo.m`]. In this case, relaxing the conditions on the normal closures of a and b leads to a larger starting group, order 7^{165}, but not a smaller final group, see [6, `p7g2q6.m`].

For faster computation we replaced the three relators

$$[a,b,b,b,b,a], \qquad [a,b,b,b,b,b,a], \qquad [a,b,b,b,b,b,b,a]$$

by

$$[b,a,b,b,b,a], \qquad [b,a,b,b,b,b,a], \qquad [b,a,b,b,b,b,b,a]$$

and then systematically added as relators PCP generators which did not kill off $[b,a]^7$. The addition of five such relators gives us a 2-generator anti-Hughes 7-group of class 14 and order 7^{97} which satisfies 11 commutator defining relators and in which the normal closures of both generators have class 7. Then repeatedly factoring out complements to $[b,a]^7$ in the centre leads to 2-generator anti-Hughes 7-group of class 14 and order 7^{66}, see [6, `p7g2q11mo.m`]. This is the smallest 2-generator anti-Hughes group that we have found.

Similarly, there is a 3-generator 5-group counterexample to the Hughes conjecture generated by a,b,c where the normal closures of a and b are nilpotent of class 4 and the normal closure of c is abelian. (In this example we should also have the Hughes subgroup equal to $\langle c\rangle G'$.) We first construct the largest class 8 group of exponent 5 in which the normal closures of the three generators have classes $4,4,1$ respectively. Then we construct the p-covering group of this group, while maintaining the restriction on the normal closures of the generators. This gives us a group of order 5^{171}. Then we factor out the subgroup generated by the 5th powers of elements outside the subgroup $\langle c\rangle G'$, and this gives us a counterexample of order 5^{123}. Reducing this example in the same way as above gives us an example of order 5^{54}, see [6, `p5g3mo.m`].

We now add defining commutator relators to the 5-group. With relators $[c,a,b]$ and $[c,b,b,b,a]$ we obtain an example of order 5^{50}, see [6, `p5g3q.m`]; then, with those relators and with the normal closures of a and b having class 4 [6, `p5g3qmo.m`] we obtain an example of order 5^{48}. Further experimenting reveals that we can add 6 more defining relators and retain the anti-Hughes property, leading to an example of order 5^{46} [6, `p5g3q8mo.m`]. This is the smallest 3-generator anti-Hughes group that we have found.

A similar approach allows us to construct a PCP for Wall's 3-generator 5-group defined in [23]. It has order 5^{167} and class 11. Its largest class 9 quotient has order 5^{151} and is also an anti-Hughes group. Repeated factoring out of complements leads to an anti-Hughes group with order 5^{56}, see [6, `wallcl9.m`]; with the normal closures of a and b having class 4 we obtain an example of order 5^{54}.

5. Further examples

As demonstrated by the outputs on [6], our computations thus far can be done quite easily. The timings and memory usages shown in the outputs are for runs done on a Dell XPS M1330 laptop with 2.4 GHz Intel Core 2 Duo cpus. When going on to consider larger examples we used a standalone implementation of the p-quotient algorithm. We wrote special new code to enforce pth power relations, which runs considerably faster than the previous code. We also distributed the power checking over several processors.

We constructed a 3-generator 7-group with Hughes subgroup of index 49. We first constructed the largest class 12 group of exponent 7 generated by three elements a, b, c where the normal closures of a and b have class 6 and the normal closure of c is abelian. This group has order 7^{2078}. We next constructed the p-covering group of this group, while maintaining the restriction that the normal closures of a, b, c have class $6, 6, 1$ respectively. This gave us a group G of order 7^{2875}. We then factored out the normal subgroup generated by 7th powers of elements outside the subgroup $\langle c\rangle G'$. This gave us a group of order 7^{2631}, with Hughes subgroup of index 49.

Our success in constructing examples with extra defining relators suggested that it might be possible to construct a 2-generator 11-group of class 22 as a counterexample to the Hughes conjecture. In the end we imposed the relators

$$[b, \underbrace{a, a, \ldots, a}_{k}, b] \quad \text{for } k = 4, 5, 6, 7, 8, 9, 10, 11,$$

$$[b, a, \underbrace{b, b, \ldots, b}_{k}, a] \quad \text{for } k = 3, 4, 5, 6, 7, 8, 9, 10,$$

$$[b, a, a, a, b, b], \qquad [b, a, a, a, b, a, a, b, a], \qquad [b, a, a, b, a, b, b, b, b, b],$$

as well as imposing the conditions that the normal closures of a and b have class 11. This gave us a 2-generator example of order 11^{2408} and class 22.

6. Lie algebra calculations

In principle, to show that $f_p(x, y, [x, y]) = 0$ is not a consequence of the $(p-1)$-Engel identity, one could compute the class $2p$ quotient of the free $(p-1)$-Engel Lie algebra over GF(p) on two generators a, b, and then verify that $f_p(a, b, [a, b]) \neq 0$. Such calculations can readily be done with the program described in [5]. However even for $p = 13$ this would be a massive computation. Our idea was to add extra relations to the Lie algebra, the trick being to add enough extra relations to make the dimension of the algebra manageable but without adding in so many extra relations that the resulting algebra did satisfy $f_p(a, b, [a, b]) = 0$.

After some experimenting we settled on the following extra relations. First, we added in the relations $w = 0$ for every Lie product $w(a, b)$ with multiweight (r, s) in a and b where $r > p$, or $s > p$, or $|r - s| \geqslant 3$. We also added in the relation $[b, a, a, a] = 0$, as well as the $(p-1)$-Engel identity. For $p = 11, 13, 17$ and 19 this gave Lie algebras of class $2p$ and dimensions 471, 1809, 22816 and 29131. In each case it was straightforward to check that $f_p(a, b, [a, b]) \neq 0$. For $p = 7$ the Lie algebra defined above has class 12 and dimension 37, but if we omit the relation $[b, a, a, a] = 0$ (but keep the other relations), then we obtain a Lie algebra of class 14 and dimension 153 in which $f_7(a, b, [a, b]) \neq 0$.

References

[1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput. 24 (1997) 235–265. See also http://magma.maths.usyd.edu.au/magma/.
[2] J.J. Cannon, Computation in finite algebraic structures, PhD thesis, The University of Sydney, 1969.
[3] J.J. Cannon, Some combinatorial and symbol manipulation programs in group theory, in: Computational Problems in Abstract Algebra, Proc. Conf., Oxford, 1967, Pergamon, Oxford, 1970, pp. 199–203.
[4] The GAP Group, GAP – groups, algorithms, and programming, Version 4.4.12, http://www.gap-system.org/, 2008.
[5] G. Havas, M.F. Newman, M.R. Vaughan-Lee, A nilpotent quotient algorithm for graded Lie rings, J. Symbolic Comput. 9 (1990) 655–664.
[6] G. Havas, M.R. Vaughan-Lee, Anti-Hughes groups; supplementary materials, http://www.itee.uq.edu.au/~havas/hughes, http://users.ox.ac.uk/~vlee/hughes, 2009.
[7] G. Higman, Some remarks on varieties of groups, Quart. J. Math. Oxford Ser. 2 10 (1959) 165–178.
[8] G.T. Hogan, W.P. Kappe, On the H_p-problem for finite p-groups, Proc. Amer. Math. Soc. 20 (1969) 450–454.
[9] D.F. Holt, B. Eick, E.A. O'Brien, Handbook of Computational Group Theory, Chapman & Hall/CRC, 2005.
[10] D.R. Hughes, Partial difference sets, Amer. J. Math. 78 (1956) 650–677.
[11] D.R. Hughes, A problem in group theory, Bull. Amer. Math. Soc. 63 (1957) 209.
[12] D.R. Hughes, J.G. Thompson, The H-problem and the structure of H-groups, Pacific J. Math. 9 (1959) 1097–1101.
[13] E.I. Khukhro, On the connection between the Hughes conjecture and relations in finite groups of prime exponent, Mat. Sb. 116 (1981) 253–264 (in Russian); translation in: Math. USSR Sbornik 44 (1983) 227–237.
[14] E.I. Khukhro, On the associated Lie ring of a free 2-generator group of prime exponent and the Hughes conjecture for 2-generator p-groups, Mat. Sb. 118 (1982) 567–575 (in Russian); translation in: Math. USSR Sbornik 46 (1983) 571–579.
[15] E.I. Khukhro, On Hughes' problem for finite p-groups, Algebra Logika 26 (1987) 642–646, 650 (in Russian); translation in: Algebra Logic 26 (1988) 398–401.
[16] E.I. Khukhro, On finite p-groups not satisfying the Hughes conjecture, Sibirsk. Mat. Zh. 35 (1994) 221–227 (in Russian); translation in: Siberian Math. J. 35 (1994) 202–207.
[17] E.I. Khukhro, Generalizations of the restricted Burnside problem for groups with automorphisms, in: Groups St. Andrews 1997 in Bath, II, in: London Math. Soc. Lecture Note Ser., vol. 261, Cambridge Univ. Press, Cambridge, 1999, pp. 474–491.
[18] I.D. Macdonald, The Hughes problem and others, J. Aust. Math. Soc. 10 (1969) 475–479.
[19] I.D. Macdonald, Solution of the Hughes problem for finite p-groups of class $2p-2$, Proc. Amer. Math. Soc. 27 (1971) 39–42.
[20] C.C. Sims, Computation with Finitely Presented Groups, Cambridge Univ. Press, 1994.
[21] E.G. Straus, G. Szekeres, On a problem of D.R. Hughes, Proc. Amer. Math. Soc. 9 (1958) 157–158.
[22] M.R. Vaughan-Lee, The Restricted Burnside Problem, second ed., Oxford University Press, 1993.
[23] G.E. Wall, On Hughes' H_p-problem, in: Proc. Internat. Conf. Theory of Groups, Canberra, 1965, Gordon and Breach, New York, 1967, pp. 357–362.
[24] G.E. Wall, On the Lie ring of a group of prime exponent, in: Proceedings of the Second International Conference on the Theory of Groups, Canberra, 1973, in: Lecture Notes in Math., vol. 372, Springer, Berlin, 1974, pp. 667–690.
[25] G.E. Wall, On the multilinear identities which hold in the Lie ring of a group of prime-power exponent, J. Algebra 104 (1986) 1–22.