Short Two-Variable Identities for Finite Groups

David P. Cargo
Department of Defense, 9800 Savage Rd
Fort George G. Meade
Maryland 20755-6565, USA

Warwick de Launey
Center for Communications Research
4320 Westerra Court
La Jolla CA92121, USA

Martin W. Liebeck
Department of Mathematics
Imperial College
London SW7 2AZ, UK

Richard M. Stafford
Department of Defense, 9800 Savage Rd
Fort George G. Meade
Maryland 20755-6565, USA

October 16, 2007

Abstract

In this paper, we consider finite groups G satisfying identities of the form

$$x^{e_1}y^{f_1}x^{e_2}y^{f_2}\dots x^{e_r}y^{f_r}=1\,.$$

We focus on identities with r small, $\sum_i e_i=\sum_i f_i=0$, and all e_i, f_i coprime to the order of G. We show that for $r=2,3$ and 5, G must be nilpotent. We also classify for $r=4,6$ and 7, the special identities which can hold in non-nilpotent groups. Finally, we show that for $r<30$, the group G must be solvable.

1 Introduction

In this paper, we consider two-variable identities for finite groups. Let $e_1, e_2, \ldots, e_r,\ f_1, f_2, \ldots, f_r$ denote integers. We study finite groups G in which the identity

$$x^{e_1} y^{f_1} x^{e_2} y^{f_2} \ldots x^{f_r} y^{f_r} = 1 \tag{1}$$

holds for all $x, y \in G$. We say such a group G satisfies the identity (1).

Some cases of such identities have been studied, for example in [1, 2]. Also in [3], the authors presented a recursive algorithm for deciding whether a non-nilpotent (respectively non-solvable) group can satisfy an n-variable identity $w(x_1, \ldots, x_n) = 1$.

In this paper we study identities of the form (1) with an emphasis on relatively small r. We give precise results concerning which identities are satisfied by non-nilpotent groups for $r \leq 7$, and show that, under natural conditions described in Section 2, no identity with $r < 30$ can be satisfied by any non-solvable group.

The rest of this paper is organized as follows. Section 2 covers some preliminary comments which refine the question. Section 3 states the results obtained. Sections 4 and 5 contain the proofs for the results regarding nilpotency and solvability. Finally, Section 6 poses several open problems which follow on from our work.

2 Preliminaries

Firstly we identify a special case where there is a nilpotent group of class two satisfying (1). Let

$$E = \sum_i e_i \qquad F = \sum_i f_i \qquad K = \sum_{i \leq j} e_i f_j \ .$$

Proposition 2.1. *If* $\gcd(E, F, K) \neq 1$*, then there is a nilpotent two-generator group of class two satisfying* (1)*. In particular, this is the case when* $E = F = 0$ *and* $K \neq \pm 1$.

Proof. The group $G = \langle a, b \mid a^E = b^F = [a,b]^K = 1, [a,b] \text{ central } \rangle$ satisfies (1). If p is a prime dividing $\gcd(E, F, K)$, then G has as a homomorphic image the group $Q = \langle a, b \mid a^p = b^p = [a,b]^p = 1, [a,b] \text{ central } \rangle$ which is a class two group of order p^3. $\square$

We next introduce some constraints on the exponents e_i and f_i appearing in (1). Suppose that E is not zero. Then setting $y = 1$ in (1) yields $x^E = 1$.

Therefore the exponent $\exp(G)$ of G must divide E, and one can add or subtract multiples of $\exp(G)$ from the exponents e_i to obtain a new relation for G with E equal to zero. Therefore we restrict our attention to identities with exponents e_i, f_i obeying the equations

$$E = \sum_i e_i = 0 \qquad F = \sum_i f_i = 0\,. \tag{2}$$

Note that when (2) holds, Proposition 2.1 shows that usually there is a nilpotent group of class two satisfying (1).

Next observe that if for some i, we have $\gcd(|G|, e_i) > 1$ or $\gcd(|G|, f_i) > 1$, then the identity (1) is somewhat degenerate for G, since one of the terms in the identity ranges over a restrictive subset of the elements of G. Therefore we impose the coprimality constraint

$$\gcd(e_i, |G|) = \gcd(f_i, |G|) = 1 \qquad \text{for all } i \tag{3}$$

This constraint avoids a host of somewhat uninteresting identities imposed by global properties of the group. For example, if H is a normal subgroup of index n in G, then $x^{ne_1}y^{nf_1}\dots x^{ne_r}y^{nf_r} = 1$ holds in G whenever (1) holds in H. Moreover, if the possible orders for an element in G are $n_1, n_2, \dots, n_s$, then $[\dots[[x, y^{n_1}], y^{n_2}], \dots, y^{n_s}] = 1$ holds in G.

The implications of the coprimality condition (3) can be surprising. The following result shows that the dihedral groups, which are rather close to being abelian, cannot have short identities with exponents obeying (3).

Lemma 2.2. *Let $D_{2n} = \langle\, a, b \mid a^2 = b^n = 1, b^a = b^{-1}\,\rangle$. If (1) holds in D_{2n} for exponents satisfying the coprime condition (3), then n divides r.*

Proof. Since $\exp(G)$ is even, the exponents e_i and f_i are odd. Put $x = a$ and $y = ab$. Then x and y are both involutions, and (1) reduces to $b^r = 1$. Since b has order n, n must divide r. □

The analog of condition (3) for infinite groups G is that x^{e_i} and y^{f_i} each range uniformly over G if x and y do. Equivalently,

$$\{x^{e_i} \mid x \in G\} = G \qquad \text{and} \qquad \{x^{f_i} \mid x \in G\} = G \tag{4}$$

Proposition 2.3. *Let $G = D_\infty = \langle a, b \mid a^2 = 1, b^a = b^{-1}\rangle$. No identity of the form (1) with exponents satisfying (4) can hold in G.*

Proof. For all n, the group G has D_{2n} as a homomorphic image. Therefore, n divides r for all natural numbers n - a contradiction. □

We now discuss two kinds of minimal groups. If (1) holds in a group G, then it holds in all subgroups and homomorphic images of G. Therefore, if (1) holds in a non-nilpotent group, then it holds also in some minimal non-nilpotent group - that is, a non-nilpotent group all of whose proper subgroups and homomorphic images are nilpotent. Such minimal non-nilpotent groups are well understood. The following elementary result is equivalent to a result proved in [3].

Theorem 2.4. *Let G be a finite minimal non-nilpotent group. Then there exist two primes p and q and a natural number k such that G is a Frobenius group of order $q^k p$. Specifically,*

1. *q has multiplicative order equal to k modulo p,*
2. *$G = PQ$ is a semidirect product of subgroups P and $Q \triangleleft G$ of respective orders p and q^k,*
3. *Q may be regarded as the additive group $(\mathrm{GF}(q^k), \oplus)$,*
4. *P is the subgroup of order p of the multiplicative group $(\mathrm{GF}(q^k)^*, \cdot)$,*
5. *$x \in P$ acts on $u \in Q$ by field multiplication: i.e., $x^{-1}ux = u^x = x \cdot u = u \cdot x$.*

Remark 2.5. The exponent of the group G in Theorem 2.4 is pq. Let $x, y \in P$ and $u, v \in Q$. Then $u^x v^y = x{\cdot}u \oplus y{\cdot}v = y{\cdot}v \oplus x{\cdot}u = v^y u^x$. We use the field addition and multiplication in $\mathrm{GF}(q^k)$ to keep track of the action of the elements of P on the elements of Q. One has $u^x u^y = x{\cdot}u \oplus y{\cdot}u = (x \oplus y){\cdot}u = u^{x \oplus y}$, and $(u^x)^y = (x \cdot u)^y = y \cdot (x \cdot u) = (y \cdot x) \cdot u = (x \cdot y) \cdot u = u^{x \cdot y}$. In the exponent, we will use the usual notation for multiplication and addition in $\mathrm{GF}(q^k)$. So we write u^{x+y} for $u^{x \oplus y}$ and u^{xy} for $u^{x \cdot y}$. Using this notation, for any integer k, one has

$$(xu)^k = x^k u^{x^{k-1} + x^{k-2} + \cdots + 1} , \tag{5}$$

where for negative k, the exponent of u is a sum of decreasing powers of x down to nearest multiple of p. In particular all elements of PQ not in Q have order p.

We will also need a corresponding result for minimal non-solvable groups: those non-solvable groups whose subgroups and homomorphic images are all solvable. The following characterization is derived in [3] from the celebrated N-group theorem of Thompson.

Theorem 2.6. *Let G be a finite minimal non-solvable group. Then G is one of the following simple groups, where p denotes an odd prime: $PSL(2,p)$ (for $p \geq 5$), $PSL(2,2^p)$, $PSL(2,3^p)$, $\mathrm{Sz}(2^p)$, and $PSL(3,3)$.*

3 Results

In section 5 we prove

Theorem 3.1. *Suppose G is a finite group satisfying the identity (1) with exponents e_i and f_i obeying the coprime condition (3). If $r < 30$, then G is solvable.*

The bound of 30 in this theorem is best possible, since there is an obvious identity of type (1) with $r = 30$ for the non-solvable group A_5, namely $(xy)^{30} = 1$. However in the proof we shall obtain some much stronger lower bounds on the possible lengths r of identities for various types of simple groups, such as $PSL(2,q)$ and $Sz(q)$.

In section 4 we prove classification results regarding nilpotency for $r \leq 7$. Our methods could be applied for any r; however, the number of cases to consider grows rapidly with r. The answers we obtain for $r \leq 7$ suggest that for larger r there are more direct arguments. Nevertheless, the overall principle seems to be that satisfying a randomly selected identity almost always forces the group to be nilpotent.

We now present our nilpotency results.

Theorem 3.2. *If $r = 2, 3$ or 5, and (2) and (3) hold, then any finite group satisfying (1) is nilpotent.*

Theorem 3.3. *Suppose $r = 4$, and that (2) and (3) hold. Then there is a non-nilpotent group G satisfying (1) if and only if there is an odd prime p such that*

$$e_1 + e_2 \equiv e_2 + e_3 \equiv f_1 + f_2 \equiv f_2 + f_3 \equiv 0 \pmod p$$

and $(e_i, 2p) = (f_i, 2p) = 1$ for all i.

Theorem 3.4. *Suppose $r = 6$, and that (2) and (3) hold. Then there is a non-nilpotent group G satisfying (1) if and only if one of the following four possibilities holds.*

1. *There is a prime* $p \neq 3$ *such that*

$$\begin{aligned}
&e_1 + e_2 \equiv e_2 + e_3 \equiv e_3 + e_4 \equiv e_4 + e_5 \equiv 0 \pmod p, \\
&f_1 + f_2 \equiv f_2 + f_3 \equiv f_3 + f_4 \equiv f_4 + f_5 \equiv 0 \pmod p, \\
&e_1 - e_3 \equiv e_2 - e_4 \equiv e_3 - e_5 \equiv e_4 - e_6 \pmod 3 \\
&f_1 - f_3 \equiv f_2 - f_4 \equiv f_3 - f_5 \equiv f_4 - f_6 \pmod 3
\end{aligned}$$

   and $(e_i, 3p) = (f_i, 3p) = 1$ *for all* i.

2. *There is a prime* $p \neq 2$ *such that*

$$\begin{aligned}
&e_1 - e_4 \equiv e_2 - e_5 \equiv e_3 - e_6 \equiv 0 \pmod p, \\
&f_1 - f_4 \equiv f_2 - f_5 \equiv f_3 - f_6 \equiv 0 \pmod p
\end{aligned}$$

   and $(e_i, 2p) = (f_i, 2p) = 1$ *for all* i.

3. *There are distinct primes* p, q *such that*

$$\begin{aligned}
&e_1 + e_2 \equiv e_2 + e_3 \equiv e_3 + e_4 \equiv e_4 + e_5 \equiv 0 \pmod p, \\
&e_1 + e_4 \equiv e_2 + e_5 \equiv 0 \pmod q, \\
&f_1 + f_2 + f_3 \equiv f_2 + f_3 + f_4 \equiv f_3 + f_4 + f_5 \equiv 0 \pmod p, \\
&f_1 + f_3 + f_5 \equiv 0 \pmod q
\end{aligned}$$

   and $(e_i, pq) = (f_i, pq) = 1$ *for all* i.

4. *The previous case holds with each pair* e_i, f_i *interchanged.*

For specific values of q, the Frobenius groups PQ of order $q^k p$ as in the conclusion of Theorem 2.4 provide minimal examples of the non-nilpotent G in Theorems 3.3 and 3.4. In Theorem 3.3, $q = 2$; in parts (1) and (2) of Theorem 3.4, $q = 3, 2$, respectively; and in parts (3) and (4) $q \neq p$ is arbitrary.

In each of the above examples, the identity (1) reduces to simple forms. For the examples in Theorem 3.3, the identity becomes

$$[x^{e_1}, y^{f_1}]^2 = 1\,.$$

In Theorem 3.4 part (1), the identity reduces to

$$(x^{e_1} y^{f_1} x^{e_2} y^{f_2})^3 = 1\,.$$

In Theorem 3.4 part (2), the identity reduces to

$$([x^{-e_1}, y^{-f_1}][y^{-f_1}, x^{-e_1-e_2}][x^{-e_1-e_2}, y^{-f_1}])^2 = 1$$

for $x, y \in PQ\backslash Q$, and to

$$(x^{e_1} y x^{-e_2} y x^{-e_1-e_2} y)^2 = 1$$

for $x \in PQ\backslash Q, y \in Q$. And in Theorem 3.4 part (3), the identity reduces to

$$[x^{-e_1}, y^{-f_1}][y^{-f_1-f_2}, x^{-e_1}][y^{-f_1}, x^{-e_1}][x^{-e_1}, y^{-f_1-f_2}] = 1$$

for $x, y \in PQ\backslash Q$.

We now consider identities with $r = 7$ satisfied by non-nilpotent groups. First we describe a way to get many such identities for which (2) and (3) hold. Let G be a non-nilpotent group with $G'' = 1$. (Note that the Frobenius group $G = PQ$ as in Theorem 2.4 is such a group.) Let e_1, e_3, and f_1, f_2 be any integers. Then for all $x, y \in G$, we have

$$[y^{f_1}, x^{-e_1}][y^{-f_2}, x^{-e_3}][x^{-e_1}, y^{f_1}][x^{-e_3}, y^{-f_2}] = 1\,.$$

Conjugating by y^{-f_1} gives the following identity with $r = 7$:

$$x^{e_1} y^{f_1} x^{-e_1} y^{f_2} x^{e_3} y^{-f_2} x^{e_1-e_3} y^{-f_1} x^{-e_1} y^{f_1} x^{e_3} y^{f_2} x^{-e_3} y^{-f_1-f_2} = 1\,. \qquad (6)$$

Notice that since e_1, e_3 and $e_1 - e_3$ cannot all be odd, we must have G of odd order if the above identity satisfies the coprime condition (3). Finally, observe that we may obtain six further identities by *cycling the exponents* in (6). For example, the first such identity is

$$x^{-e_1} y^{f_2} x^{e_3} y^{-f_2} x^{e_1-e_3} y^{-f_1} x^{-e_1} y^{f_1} x^{e_3} y^{f_2} x^{-e_3} y^{-f_1-f_2} x^{e_1} y^{f_1} = 1\,.$$

The following result shows that these are the only identities satisfied by minimal non-nilpotent groups.

Theorem 3.5. *Let $r = 7$. There is a non-nilpotent group satisfying* (1) *(with* (2) *and* (3) *holding) if and only if there is a Frobenius group PQ of odd order pq^k as in Theorem 2.4 in which the identity takes the form* (6)*, up to cycling exponents.*

The necessary and sufficient condition in Theorem 3.5 is equivalent to existence of primes p and q such that up to cycling of exponents

$$\begin{aligned}
e_1 \equiv -e_2 \equiv -e_5, \quad e_3 \equiv e_6 \equiv -e_7, \quad e_4 \equiv e_1 - e_3 \quad &\pmod p\\
f_1 \equiv -f_4 \equiv f_5, \quad f_2 \equiv -f_3 \equiv f_6, \quad f_7 \equiv -f_1 - f_2 \quad &\pmod p\\
e_2 + e_4 + e_6 \equiv e_1 + e_5 \equiv e_3 + e_7 \quad &\pmod q\\
f_7 + f_2 + f_5 \equiv f_1 + f_4 \equiv f_3 + f_6 \quad &\pmod q
\end{aligned}$$

When combined with the above results, our final theorem shows that 2,3 and 5 are the only values of r which force all groups satisfying (1), (2), (3) to be nilpotent.

Theorem 3.6. *For $r = 4$ or $r \geq 6$, there is an identity* (1)*, and a finite non-nilpotent group G satisfying* (1)*, such that* (2)*,* (3) *hold.*

4 Proofs of Theorems on Nilpotency

Suppose G is a finite group satisfying the identity (1) and that $(2),(3)$ hold. We first obtain some polynomial constraints which hold if and only if there is a non-nilpotent such G, and then we determine when these constraints are satisfied.

4.1 Polynomial Constraints

Suppose G is minimal non-nilpotent. Then there are primes p, q such that $G = PQ$ is as in the conclusion of Theorem 2.4.

For $x, y \in P$ and $u, v \in Q$ the identity (1) gives

$$(xu)^{e_1}(yv)^{f_1}(xu)^{e_2}(yv)^{f_2}\cdots(xu)^{e_r}(yv)^{f_r} = 1. \tag{7}$$

By (5), we have $(xu)^m = x^m u^{x^{m-1}+x^{m-2}+\cdots+1}$. Hence (7) becomes

$$\begin{array}{l} u^{(x^{e_1-1}+\cdots+1)x^{e_2+\cdots+e_r}y^{f_1+\cdots+f_r}}v^{(y^{f_1-1}+\cdots+1)x^{e_2+\cdots+e_r}y^{f_2+\cdots+f_r}}\times \\ u^{(x^{e_2-1}+\cdots+1)x^{e_3+\cdots+e_r}y^{f_2+\cdots+f_r}}v^{(y^{f_2-1}+\cdots+1)x^{e_3+\cdots+e_r}y^{f_3+\cdots+f_r}}\times\cdots \\ \cdots\times u^{(x^{e_r-1}+\cdots+1)y^{f_r}}v^{y^{f_r-1}+\cdots+1} = 1 \end{array} \tag{8}$$

for all $x, y \in P$, $u, v \in Q$. Now put

$$E_i = e_i + e_{i+1} + \cdots + e_r \qquad F_i = f_i + f_{i+1} + \cdots + f_r \qquad (\text{for } i = 1, 2, \ldots, r)$$

Note that $E_1 = F_1 = 0$. Next set

$$\begin{array}{rcl} w &=& (x^{e_1-1}+\cdots+1)x^{E_2}y^{F_1} + (x^{e_2-1}+\cdots+1)x^{E_3}y^{F_2} \\ && +\cdots+(x^{e_r-1}+\cdots+1)x^{E_1}y^{F_r} \\ z &=& (y^{f_1-1}+\cdots+1)x^{E_2}y^{F_2} + (y^{f_2-1}+\cdots+1)x^{E_3}y^{F_3} \\ && +\cdots+(y^{f_r-1}+\cdots+1)x^{E_1}y^{F_1} \end{array}$$

Then, by Remark 2.5, (8) becomes

$$u^w v^z = 1\,.$$

Since this holds for all u and v, one must have $w = z = 0$ for all $x, y \in P$. Putting first $x = 1$, then $y = 1$, and then $x, y \neq 1$, in the expressions for w and z, one obtains the following three polynomial equations over $\mathrm{GF}(q^k)$ which must hold for all x and y in the multiplicative subgroup P of order p in $\mathrm{GF}(q^k)^*$:

$$
\begin{aligned}
e_1 y^{F_1} + e_2 y^{F_2} + \cdots + e_{r-1} y^{F_{r-1}} + e_r y^{F_r} &= 0 \quad (9)\\
f_r x^{E_1} + f_1 x^{E_2} + \cdots + f_{r-2} x^{E_{r-1}} + f_{r-1} x^{E_r} &= 0 \quad (10)\\
(x^{e_1} - 1) x^{E_2} y^{F_1} + (x^{e_2} - 1) x^{E_3} y^{F_2} + \cdots + (x^{e_r} - 1) x^{E_1} y^{F_r} &= 0 \quad (11)
\end{aligned}
$$

4.2 An Associated Graph

We continue with the assumptions and notation of the previous subsection. We now introduce a graph which is a useful aid to analyzing the polynomial constraints (9) and (10). By the coprimeness hypothesis (3), we have

$$(e_i, pq) = (f_i, pq) = 1 \qquad (\text{for } i = 1, 2, \ldots, r)$$

In particular all the coefficients e_i and f_i in equations (9), (10) are nonzero modulo q. Since the left hand side reduces to zero, the r exponents

$$E_1, E_2, \ldots, E_{r-1}, E_r \tag{12}$$

appearing in (10) must partition into subsets of size at least 2, such that each subset in the partition consists of E_i's which are pairwise congruent modulo p. We suppose this partition is maximal in the sense that E_i's in different subsets are not congruent modulo p. Since $e_i \not\equiv 0 \pmod{p}$ the exponents E_i and E_{i+1} cannot appear in the same subset of the partition. Analogous remarks apply to the r exponents

$$F_1, F_2, \ldots, F_{r-1}, F_r \tag{13}$$

appearing in (9). Let A (respectively, B) denote the partition on the set $\{E_i \mid i = 1, 2 \ldots, r\}$ (respectively, $\{F_i \mid i = 1, 2, \ldots, r\}$).

Now let Γ_r denote a graph on the vertices $E_1, E_2, \ldots, E_r, F_1, F_2, \ldots, F_r$ with edges $\{E_i, E_j\}, \{F_i, F_j\}$, for all i and j such that $j \not\equiv i, i-1, i+1 \pmod{r}$. Then the above partitions A and B comprise a set of vertex-disjoint cliques of Γ_r such that

1. each clique contains at least two vertices,
2. each vertex in Γ_r appears in exactly one clique.

We call a set of vertex-disjoint cliques of Γ_r satisfying the above two conditions a *clique decomposition* of Γ_r. Any clique decomposition of Γ_r yields congruences modulo p on the e_i's and f_i's, and hence also, via (9) and (10), congruences modulo q.

4.3 The Proofs

Proof of Theorem 3.2. For $r = 2$ and 3, Γ_r contains no edges; so there are no cliques of size two or more. Therefore there is no clique decomposition of Γ_r for $r = 2$ or 3. For $r = 5$, the edges of Γ_5 are $\{E_1, E_3\}, \{E_1, E_4\}, \{E_2, E_4\}$, $\{E_2, E_5\}, \{E_3, E_5\}, \{F_1, F_3\}$, $\{F_1, F_4\}, \{F_2, F_4\}, \{F_2, F_5\}, \{F_3, F_5\}$. In this case, any clique decomposition must contain vertex-disjoint cliques of size 2 and 3. Since Γ_5 contains no triangle, there are no such clique decompositions of Γ_5. This completes the proof of Theorem 3.2. □

Proof of Theorem 3.3. For $r = 4$. The only clique decomposition of Γ_4 has $A = \{E_1, E_3\}, \{E_2, E_4\}$, and $B = \{F_1, F_3\}, \{F_2, F_4\}$. Hence we must have

$$E_1 \equiv E_3 \pmod{p}, \quad E_2 \equiv E_4 \pmod{p},$$
$$F_1 \equiv F_3 \pmod{p}, \quad F_2 \equiv F_4 \pmod{p}.$$

So $e_1 + e_2 \equiv e_2 + e_3 \equiv 0 \pmod{p}$ and $f_1 + f_2 \equiv f_2 + f_3 \equiv 0 \pmod{p}$. Then the third polynomial constraint (11) reduces to the equation

$$2(x^{e_1} - 1)(y^{f_1} - 1) = 0\,.$$

This implies that $q = 2$. Hence p is odd, and all e_i, f_i are odd. Indeed,

$$e_2 \equiv -e_1 \pmod{pq} \quad \text{and} \quad f_2 \equiv -f_1 \pmod{pq}\,.$$

Thus, for elements $x, y \in PQ$, the left hand side of the identity (1) becomes $[x^{-e_1}, y^{-f_1}]^2$, which is equal to 1 (since all commutators in PQ lie in Q which has exponent 2). Hence (1) certainly holds in the group PQ with $q = 2$. All parts of Theorem 3.3 are now proved. □

Proof of Theorem 3.4. For $r = 6$, the possible A and B partitions are

$A_1 : \{E_1, E_3, E_5\}$, $\{E_2, E_4, E_6\}$	$B_1 : \{F_1, F_3, F_5\}$, $\{F_2, F_4, F_6\}$
$A_2 : \{E_1, E_3\}$, $\{E_2, E_5\}$, $\{E_4, E_6\}$	$B_2 : \{F_1, F_3\}$, $\{F_2, F_5\}$, $\{F_4, F_6\}$
$A_3 : \{E_1, E_4\}$, $\{E_2, E_5\}$, $\{E_3, E_6\}$	$B_3 : \{F_1, F_4\}$, $\{F_2, F_5\}$, $\{F_3, F_6\}$
$A_4 : \{E_1, E_4\}$, $\{E_2, E_6\}$, $\{E_3, E_5\}$	$B_4 : \{F_1, F_4\}$, $\{F_2, F_6\}$, $\{F_3, F_5\}$
$A_5 : \{E_1, E_5\}$, $\{E_2, E_4\}$, $\{E_3, E_6\}$	$B_5 : \{F_1, F_5\}$, $\{F_2, F_4\}$, $\{F_3, F_6\}$

Each of the 25 possible choices for the pair $\{A, B\}$ implies a set of equalities and non-equalities modulo p among the E_i's and F_i's.

Example 4.1. The choice $\{A, B\} = \{A_3, B_3\}$ implies the constraints

$$E_1 \equiv E_4 \pmod p \quad E_2 \equiv E_5 \pmod p \quad E_3 \equiv E_6 \pmod p$$

and

$$F_1 \equiv F_4 \pmod p \quad F_2 \equiv F_5 \pmod p \quad F_3 \equiv F_6 \pmod p$$

The constraints (9), (10), (11) become

$$\begin{aligned}
(e_1 + e_4)y^{F_1} + (e_2 + e_5)y^{F_2} + (e_3 + e_6)y^{F_3} &= 0 \pmod q \\
(f_6 + f_3)x^{E_1} + (f_1 + f_4)x^{E_2} + (f_2 + f_5)x^{E_3} &= 0 \pmod q \\
2(y^{F_1}x^{E_1} - y^{F_1}x^{E_2} + y^{F_2}x^{E_2} - y^{F_2}x^{E_3} + y^{F_3}x^{E_3} - y^{F_3}x^{E_4}) &= 0 \pmod q
\end{aligned}$$

Since E_1, E_2 and E_3 are distinct modulo p and F_1, F_2 and F_3 are distinct modulo p, the third equation implies that $q = 2$. The coprimeness constraint (3) then implies that e_i and f_i are odd, and then we see that the first two constraints are satisfied. Thus for $q = 2$ and any odd prime p, there is a solution to the constraints (9), (10), (11) with $\{A, B\} = \{A_3, B_3\}$.

In principle, we may examine each of the other 24 possibilities for $\{A, B\}$. However, it is convenient to employ two symmetries on the set of solutions for (9), (10), (11). Observe that the identity (1) holds in G if and only if the identity

$$a^{f_6}b^{e_1}a^{f_1}b^{e_2}\cdots a^{f_5}b^{e_6} = 1$$

holds, and also if and only if the identity

$$a^{-f_6}b^{-e_6}a^{-f_5}b^{-e_5}\cdots a^{-f_1}b^{-e_1} = 1$$

holds. Hence the invertible operations

$$\begin{aligned}
&\rho: \ e_1 \to f_6 \to e_6 \to f_5 \to \cdots \to e_2 \to f_1 \to e_1 \\
&\sigma: \ e_1 \leftrightarrow -f_6,\ e_2 \leftrightarrow -f_5, \cdots, e_6 \leftrightarrow -f_1
\end{aligned}$$

preserve the collection of 12-tuples $(e_1, e_2, \ldots, e_r, f_1, f_2, \ldots, f_6)$ of exponents in identities (1) holding in G. ρ moves E_1 to $F_6 - f_6, E_2$ to $F_1 - f_6$, E_3 to $F_2 - f_6$, $\ldots$, E_6 to $F_5 - f_6$, and F_i to E_i for $i = 1, 2, \ldots, 6$. Thus ρ maps congruences of the form $E_i \equiv E_j \pmod p$ $(i \neq j)$ to congruences of the form $F_k \equiv F_\ell \pmod p$ $(k \neq \ell)$ and vice versa. Hence ρ induces an action on the set $\{A_1, A_2, \ldots, A_5, B_1, B_2, \ldots, B_5\}$. Using the cycle permutation notation, ρ acts as $(A_1, B_1)(A_2, B_4, A_4, B_5, A_5, B_2)(A_3, B_3)$. In a similar manner, σ acts as $(A_1, B_1)(A_2, B_5)(A_3, B_3)(A_4, B_4)(A_5, B_2)$. Using the shorthand ij

for the pair $\{A_i, B_j\}$, the orbits of the induced action of $\langle \rho, \sigma \rangle$ on the set $\{ij \mid i, j = 1, 2, \ldots, 5\}$ are

$$\begin{aligned} &\{11\}, \{12, 21, 51, 14, 15, 41\}, \{13, 31\}, \{22, 24, 55, 44, 45, 52\}, \\ &\{23, 34, 35, 43, 53, 32\}, \{25, 54, 42\}, \{33\} \end{aligned} \tag{14}$$

Thus to analyze the initial 25 possibilities it is sufficient to consider the seven orbit representatives $11, 21, 31, 22, 32, 42, 33$. We will show that, of the original 25 cases, only the cases $11, 31, 13$ and 33 yield solutions to the polynomial constraints (9), (10) and (11).

We first show that we cannot have $A = A_2$ or $B = B_2$. If $B = B_2$, then (11) becomes

$$\begin{aligned} y^{F_1}\left\{(x^{e_1}-1)x^{E_2} + (x^{e_3}-1)x^{E_4}\right\} + y^{F_2}\left\{(x^{e_2}-1)x^{E_3} + (x^{e_5}-1)x^{E_6}\right\} \\ + y^{F_4}\left\{(x^{e_4}-1)x^{E_5} + (x^{e_6}-1)x^{E_1}\right\} = 0\,. \end{aligned}$$

Since F_1, F_2 and F_4 are distinct modulo p, this is equivalent to the condition

$$\begin{aligned} x^{E_1} + x^{E_3} &= x^{E_2} + x^{E_4} \\ x^{E_2} + x^{E_5} &= x^{E_3} + x^{E_6} \\ x^{E_4} + x^{E_6} &= x^{E_5} + x^{E_1} \end{aligned}$$

Since this must hold for all $x \in \mathrm{GF}(q^k)$ of order p, the first equation can only hold if the list of residues E_1, E_3 modulo p is the same as the list E_2, E_4, or $q = 2$ and $E_1 \equiv E_3 \pmod p$ and $E_2 \equiv E_4 \pmod p$. Referring to the possibilities for A, we see that the first case is not possible. Hence the latter holds and we have $q = 2$ and $A = A_1$. Now the coprimeness condition (3) implies that the exponents e_i and f_i are odd (since $q = 2$). But then (10) holds only if $f_6 + f_2 + f_6 \equiv f_1 + f_3 + f_5 \equiv 0 \pmod 2$ - an impossibility since f_i is odd. Hence $B \neq B_2$.

Examination of (11) similarly reveals that $A = A_2$ implies $q = 2$ and $B = B_1$, and hence via (3) and then (9) the contradiction $1 \equiv e_1 + e_3 + e_5 \equiv e_2 + e_4 + e_6 \equiv 0 \pmod 2$. Since each of the orbits in (14) except $\{11\}, \{13, 31\}$ and $\{33\}$, have an element with $A = A_2$ or $B = B_2$, we have proved that the only possibilities for the partition pair (A, B) are $11, 13, 31$ or 33 as claimed.

We now examine each of these cases separately.

Case $\mathbf{A = A_1, B = B_1}$ Here (11) reduces to

$$3(x^{e_2} - 1)x^{E_1} \equiv 0 \pmod q$$

Therefore $q = 3$, and we must have $p \neq 3$ prime. Now $A = A_1$ implies that $e_1 + e_2 \equiv e_2 + e_3 \equiv e_3 + e_4 \equiv e_4 + e_5 \equiv e_5 + e_6 \equiv 0 \pmod p$ and hence from (10) that $f_1 + f_3 + f_5 \equiv f_2 + f_4 + f_6 \equiv 0 \pmod 3$. The coprimeness condition (3) in fact implies that $f_1 \equiv f_3 \equiv f_5 \pmod 3$ and $f_2 \equiv f_4 \equiv f_6 \pmod 3$. Similarly, $B = B_1$ implies the above conditions with e_i and f_i interchanged. We now have all the congruences listed in part 1 of Theorem 3.4. Moreover, we have shown that these congruences imply that (9), (10) and (11) hold. Hence the identity (1) holds in the Frobenius group PQ.

Case $\mathbf{A} = \mathbf{A_1}, \mathbf{B} = \mathbf{B_3}$ In this case, the modulo p constraints are

$$\begin{aligned} f_1 - f_4 \equiv f_2 - f_5 \equiv f_3 - f_6 \equiv 0 &\pmod p \\ e_1 \equiv -e_2 \equiv e_3 \equiv -e_4 \equiv e_5 \equiv -e_6 &\pmod p \end{aligned}$$

and the modulo q constraints (required to cause (9) and (10) to hold) are

$$\begin{aligned} e_1 + e_4 \equiv e_2 + e_5 \equiv e_3 + e_6 \equiv 0 &\pmod q \\ f_1 + f_3 + f_5 \equiv f_2 + f_4 + f_6 \equiv 0 &\pmod q \end{aligned}$$

Finally, in this case, (11) holds without condition on p or q. This case corresponds to part 3 of Theorem 3.4.

Case $\mathbf{A} = \mathbf{A_3}, \mathbf{B} = \mathbf{B_1}$ This case is the same as the above case with the exponents e_i and f_i interchanged. This corresponds to the last part of Theorem 3.4.

Case $\mathbf{A} = \mathbf{A_3}, \mathbf{B} = \mathbf{B_3}$ This case was covered in Example 4.1. In this case, we require $q = 2$ and p to be an odd prime. The modulo p conditions on the exponents e_i $(i = 1, 2 \ldots, 6)$ are equivalent to $e_1 + e_2 + e_3 \equiv e_2 + e_3 + e_4 \equiv e_3 + e_4 + e_5 \equiv 0 \pmod p$ which is equivalent to $e_4 \equiv e_1 \pmod p, e_5 \equiv e_2 \pmod p, e_6 \equiv e_3 \pmod p$. Analogous constraints hold for the exponents f_i. This case corresponds to part 2 of Theorem 3.4.

This concludes the proof of Theorem 3.4. □

Proof of Theorem 3.5. The clique decompositions of Γ_7 are $P_i = (i, i+2, i+5 : i+1, i+3 : i+4, i+6)$ and $P_i' = (i, i+2, i+5 : i+1, i+4 : i+3, i+6)$, where $1 \leq i \leq 7$. By cycling exponents, we may suppose that the partition A is P_1 or P_1'. Suppose the former, then (11) reduces to

$$\begin{aligned} 0 = x^{E_1}&(y^{F_1} + y^{F_3} + y^{F_6} - y^{F_2} - y^{F_5} + y^{F_7}) \\ &+ x^{E_2}(y^{F_2} + y^{F_4} - y^{F_1} - y^{F_3}) + x^{E_5}(y^{F_5} + y^{F_7} - y^{F_4} - y^{F_6}) \end{aligned}$$

Since F_2 cannot be congruent to F_1 or F_3 modulo p, we see from the coefficient of x^{E_2} that $y^{F_2} = y^{F_4}, y^{F_1} = y^{F_3}$ and $q = 2$. But there is a clique of size 3 and hence (10) implies that $f_7 + f_2 + f_5 \equiv 0 \pmod 2$ contradicting the coprime condition (3).

Hence $A = P_1'$, and (11) implies that $B = P_4'$. Consequently, the congruences among the exponents e_i, f_i are as listed after Theorem 3.5. □

Proof of Theorem 3.6. We prove two lemmas which together with Theorem 3.5 imply that Theorem 3.6 holds for $r = 6, 7, 8, 9, 10, 11$. Then concatenating with identities provided by Theorem 3.4 gives Theorem 3.6 for all $r \geq 12$.

Lemma 4.2. *Theorem* 3.6 *holds when r is not prime.*

Proof. Suppose that r is not prime, and let s be the smallest prime divisor of r. Write $r = st$. Consider the identity

$$((xy)^{s-1}x^{-s+1}y^{-s+1})^t = 1. \tag{15}$$

Choose a prime q dividing t. By choice of s, we know that q does not divide $s-1$. Let p be another prime, distinct from q and not dividing $s-1$, and let $G = PQ$ be a Frobenius group of order $q^k p$ as in Theorem 2.4. Then for $x, y \in G$, the element $(xy)^{s-1}x^{-s+1}y^{-s+1}$ lies in $G' = Q$. Hence G satisfies the identity (15) of length $r = st$, and this identity satisfies (2) and (3). □

Lemma 4.3. *Theorem 3.6 holds for $r = 11$.*

Proof. The identity

$$[x^{a_1}, y^{b_1}][x^{a_2}, y^{b_2}][x^{a_3}, y^{b_3}] = [x^{a_3}, y^{b_3}][x^{a_1}, y^{b_1}][x^{a_2}, y^{b_2}]$$

holds in any group G with $G'' = 1$. This reduces to

$$x^{a_3-a_1}y^{b_1}x^{a_1}y^{b_1}x^{-a_2}y^{-b_2}x^{a_2}y^{b_2}x^{-a_3}y^{-b_3}\times \\ x^{a_3}y^{b_3-b_2}x^{-a_2}y^{b_2}x^{a_2}y^{-b_1}x^{-a_1}y^{b_1}x^{a_1}y^{-b_3}x^{-a_3}y^{b_3} = 1$$

which is an identity with $r = 11$. □

This completes the proof of Theorem 3.6. □

5 Proof of Solvability Theorem 3.1

Suppose G is a minimal finite, non-solvable group. Then G must be one of the groups listed in Theorem 2.6. Suppose that the identity (1) holds in G with e_i and f_i satisfying the coprime condition (3). The following lemma gives large lower bounds on r. Indeed, since $(xy)^e = 1$, where $e = \exp(G)$, is an identity with exponents $e_i = f_i = 1$ satisfying conditions (2) and (3), some of the bounds are sharp.

We would like to thank Steve Schibell for his assistance with the computational work in proving part (v) of the next lemma.

Lemma 5.1. *Let G be a group which satisfies an identity* (1) *such that* (3) *holds.*

(i) *If $G = PSL(2,q)$ (q any prime power), then r is divisible by $(q^2-1)/(4,q^2-1)$.*

(ii) *If $G = PSL(2,p)$ with $p \equiv 1 \bmod 4$, then r is divisible by $p(p^2-1)/4 = \exp(G)$.*

(iii) *If $G = PSL(2,2^p)$, then r is divisible by $2(2^{2p}-1) = \exp(G)$.*

(iv) *If $G = Sz(2^p)$, then r is divisible by $2(2^p-1)(2^{2p}+1) = \frac{1}{2}\exp(G)$.*

(v) *If $G = PSL(2,7)$ or $PSL(3,3)$, then r is divisible by 12 and is at least* 36.

Proof. Each of the above groups contains various dihedral groups. So we may use Lemma 2.2 to obtain constraints on r.

Now $PSL(2,q)$ contains dihedral subgroups D_{2k} for $k = (q-1)/(2,q-1)$ and $k = (q+1)/(2,q-1)$, and the least common multiple of these numbers is $(q^2-1)/(4,q^2-1)$. Part (i) follows.

Next, if $p \equiv 1 \bmod 4$, then $PSL(2,p)$ also contains a dihedral subgroup of order $2p$, giving part (ii). And $PSL(2,2^p)$ contains a pair of (commuting) involutions with product of order 2, which gives (iii).

By [4], the Suzuki group $Sz(q)$, $q = 2^p$, contains dihedral subgroups of order $2k$ for $k = q-1$, $k = q+\sqrt{2q}+1$, $k = q-\sqrt{2q}+1$ and $k = 2$, from which (iv) follows.

Finally, the groups in part (v) are small enough to handled computationally using MAGMA. As above, r is divisible by 12 for these groups, so the possibilities for r less than 30 are 12 and 24. Evaluating proposed identities on elements x and y of small order, we showed that no identities with $r = 12$ or 24 exist. $\square$

Remark In our MAGMA computations for part (v) of the above lemma, we found some "near identities" on G = PSL(2, 7). Define functions P and $Q = Q_1Q_2$ as follows:

$$\begin{array}{rl} P(x,y) = & (x^{-1}yxy^{-1}x^{-1}y^{-1}xy^{-1}x^{-1}yxy^{-1}x^{-1}y^{-1}xy)^3, \\ Q_1(x,y) = & x^{29}y^{67}x^{19}y^{41}x^{65}y^{23}x^{43}y^{65}x^{41}y^{61}x^{19}y^{83}x^{17}y^{17}\times \\ & x^{31}y^{31}x^{17}y^{73}x^{55}y^{23}x^{5}y^{71}x^{67}y^{59}, \\ Q_2(x,y) = & x^{17}y^{67}x^{55}y^{41}x^{65}y^{59}x^{55}y^{25}x^{53}yx^{79}y^{83}x^{29}y^{17}\times \\ & x^{67}y^{59}x^{41}y^{61}x^{31}y^{23}x^{53}y^{71}x^{55}y^{55}. \end{array}$$

Then P evaluates to the identity on 18480 of the 28224 pairs of elements in PSL(2, 7). This is about 65% of the space. The partial identity $Q(x, y) = 1$ holds for 19152 of the 28224 pairs of elements in PSL(2, 7).

Theorem 3.1 follows quickly from the lemma. Consider G as in (i)-(v) above. If $G = PSL(2, q)$ as in (i)-(iii) then r is divisible by $(q^2-1)/(4, q^2-1)$ by Lemma 5.1(i), and so $r \geq 30$ provided $q \geq 8$. The remaining possible values for q are 5 and 7, and for these we have $r \geq 30$ by Lemma 5.1(ii),(v). If $G = Sz(q)$, $q = 2^p \geq 8$, then r is divisible by $2(q-1)(q^2+1)$ by Lemma 5.1(iv), so certainly $r \geq 30$. This leaves $G = PSL(3, 3)$ as the only remaining possibility, and this is covered by Lemma 5.1(v). This completes the proof of the theorem.

6 Concluding Remarks

This paper shows that short identities (where $r = 4, 6$) can hold in a non-nilpotent group G, but that such identities are very special. On the other hand, short identities (where $r < 30$) cannot hold in a non-solvable group. Our results are indicative of a relationship between the behavior of derived or lower central series of a group G and the least possible value for r obtained by an identity satisfied by that group. Our next goal should be to refine our understanding of this relationship both when the series in question terminates in the trivial group 1, and when it doesn't. In this section, we pose some problems whose solution would in part serve this need.

The examples listed after the Theorem 3.4 of non-nilpotent groups satisfying identities with $r = 4$ or 6 are solvable of derived length two. It seems likely that r would have to be larger for identities in solvable non-nilpotent groups with longer derived series.

Problem 1. *Amongst the identities* (1)*, satisfying* (2) *and* (3)*, holding for some finite, solvable, non-nilpotent group with derived series length k, what is the least value $r_{min}(k)$ of r?*

Our results show that $r_{min}(2) = 4$.

The identities (1) with $r = 2, 3$ or 5 seem to offer particular interest, since Theorem 3.2 shows that (under the assumptions (2), (3)), all finite groups satisfying these identites are necessarily nilpotent. For $r = 2$, the groups are abelian; and for $r = 3$, Larry Wilson (personal communication) has shown that the groups have class at most 3. So we pose

Problem 2. *For $r = 5$, is there a finite bound on the nilpotency class of the finite groups satisfying an identity of the form* (1) *with exponents obeying* (3)*?*

Notice that the groups satisfying such an identity include the finite Burnside groups of exponent 5 (take $e_i = f_i = 1$ for $i = 1, 2, \ldots, 5$).

The next problem is related to Problem 2. We know by Proposition 2.1 that for every choice of exponents e_i and f_i, there is a nilpotency class two group satisfying (1) whenever $\gcd(E, F, K) \neq 1$. So given an identity (1), it would be interesting to find techniques for solving the following problem.

Problem 3. *For a given choice of exponents e_i and f_i in* (1) *and positive integer k, is there a finite nilpotent group of class k satisfying* (1)*?*

Finally we pose a problem for non-solvable groups. We know that any identity (1) (with (2), (3)) which is satisfied by a non-solvable group, must have $r \geq 30$. Moreover, for various classes of non-abelian simple groups, we showed in Lemma 5.1 that such identities must be much longer. We pose the following problem for simple groups.

Problem 4. *For each finite simple group G, determine the minimum $r(G)$ of the values of r in identities* (1) *(with* (2)*,* (3) *holding) satisfied by G.*

For example, Lemma 5.1 shows that for $G = PSL(2, p)$ ($p \equiv 1 \pmod 4$) or $PSL(2, 2^p)$ (p prime), we have $r(G) = \exp(G)$.

References

[1] N.D. Gupta and H. Heineken, Groups with a two-variable commutator identity, *Math. Z.* **95** (1967), 276–287.

[2] H. Heineken and F. Levin, Varieties of groups satisfying one two-variable law, *Publ. Math. Debrecen* **14** (1967), 211–225.

[3] H. Heineken and P. M. Neumann, Identical relations and decision procedures for groups, *J. Austral. Math. Soc.*, **7**, No. I (1967), 39–47.

[4] M. Suzuki, On a class of doubly transitive groups, *Annals of Math.* **75** (1962), 105–145.