SOME NOTES ON EXTENDED EQUATION SOLVABILITY AND IDENTITY CHECKING FOR GROUPS

MICHAEL KOMPATSCHER

Abstract. Every finite non-nilpotent group can be extended by a term operation such that solving equations in the resulting algebra is NP-complete and checking identities is co-NP-complete. This result was firstly proven by Horváth and Szabó; the term constructed in their proof depends on the underlying group. In this paper we provide a uniform term extension that induces hardness. In doing so we also characterize a big class of solvable, non-nilpotent groups for which extending by the commutator operation suffices.

1. Introduction

The equation solvability problem $\text{Eq}(A)$ of a finite algebra $A$ is the computational problem of deciding whether for two polynomials $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_n)$ over $A$ the equation $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ has a solution in $A$ or not. The identity checking problem $\text{Id}(A)$ (also known as the equivalence problem) is the dual problem that asks whether for all assignments of the variables $x_1, \ldots, x_n$ the equation $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ holds.

Many results regarding the complexity of these problems are known for finite groups. If the group $G$ is nilpotent both $\text{Id}(G)$ and $\text{Eq}(G)$ are in P (see [GR02], [BL05], [Hor11], [Föl18]). More general, so called semipattern groups induce problems that are in P [Föl17]. By [HMSL07] the equation solvability problem of a non-solvable group is NP-complete and its identity checking problem is co-NP-complete. However the complexity of both problems still remains unclassified for general solvable, non-nilpotent groups, with the smallest group for which it is unknown being the symmetric group $S_4$ (see Problem 1 in [HS12]).

Taking a different approach one might ask whether adding additional definable operations to the signature of the group has an influence on the complexity of the problem. Non-solvable groups induce hard problems, thus also extension by terms induce hard problems. By [Hor11] extensions of nilpotent groups still induce problems that are in P (and the same is true in the more general setting of supernilpotent Mal’cev algebras [Kom18]). In the terminology of [GK11] the problems are representation-independent for those algebras.

However for solvable, non-nilpotent groups the complexity may differ: It was shown in [HS12] that for the alternating group $A_4$ and the commutator operation $[x, y] = x^{-1} y^{-1} xy$, $\text{Id}(A_4; [,])$ is co-NP-complete and $\text{Eq}(A_4; [,])$ is NP-complete, while both problems for $(A_4; \cdot)$ are in P. The reason for this phenomenon is that some operation can be defined in a more concise way in the extended group. For example, the length of $[\ldots [[x_1, x_2], x_3], \ldots, x_n]$ is linear in $n$ if expressed using the commutator, but $O(2^n)$ just using the group multiplication.

By [HS11] every finite solvable, non-nilpotent group $(G; \cdot)$ has an extension by a term operation $f(x_1, \ldots, x_n)$ such that $\text{Eq}(G; : f(x_1, \ldots, x_n))$ is NP-complete and $\text{Id}(G; : f(x_1, \ldots, x_n))$ is co-NP-complete. However, the term $f$ constructed in [HS11] and also its arity depend on $G$.

Date: August 24, 2018.
The first contribution of this paper is to give a uniform extension: We are going to show that the extension of a solvable, non-nilpotent groups by its commutator operation \([x, y] = x^{-1}y^{-1}xy\) and the additional 4-ary function defined by \(w(x, y_1, y_2, y_3) = x^8[[[x, y_1], y_2], y_3]\) always induces NP-hard equation solvability and co-NP-hard identity checking problems.

Secondly we prove that many cases are covered by the commutator operation alone, while for all other the extension by \(w\) suffices. In doing so we proceed on answering Problem 1 of [HS11], which asks for a complete classification of the equation solvability and identity checking problem for groups extended by their commutator. Our main result states as follows:

**Theorem 1.** Let \(G\) be a finite solvable, non-nilpotent group and \(L\) be the smallest group of the derived series of \(G\) that is not nilpotent. By \(F(L)\) we denote the Fitting subgroup of \(L\). Furthermore we define the operations \([x, y] = x^{-1}y^{-1}xy\) and \(w(x, y_1, y_2, y_3) = x^8[[[x, y_1], y_2], y_3]\).

1. If \(\exp(L/F(L)) > 2\) then \(\text{Eq}(G, [\cdot, \cdot])\) is NP-complete and \(\text{Id}(G, [\cdot, \cdot])\) is co-NP-complete.
2. If \(\exp(L/F(L)) = 2\) then \(\text{Eq}(G, [\cdot, \cdot], w)\) is NP-complete and \(\text{Id}(G, [\cdot, \cdot], w)\) is co-NP-complete.

We remark that (1) generalizes the hardness result for \(A_4\) and the class of groups studied in Section 8.5 of [Hor88]. A complete classification of the complexity for groups extended by their commutator is still open. But - as a consequence of our proof - it would suffice to prove that non-nilpotent dihedral groups induce hard problems in order to show hardness for all groups in (2). We discuss this in more detail in Section 5 at the end of the paper.

In Section 2 we introduce notation and recall standard definitions from group theory. In Section 3 we use some complexity reduction to prove that it is enough to consider a very specific subclass of solvable, non-nilpotent groups in the proof of Theorem 1. Section 4 contains the proof of Theorem 1.

### 2. Preliminaries

An *algebra* \(A = (A; (f^A)_{f \in \tau})\) (of type \(\tau\)) consists of a set \(A\) (its *domain*) and a set of finitary operations \(f^A : A^{ar(f)} \to A\) for every function symbol \(f\) with arity \(ar(f)\) in \(\tau\). Often we are not going to distinguish between function symbols and their corresponding operation, but this should not cause any confusion. In this paper we only consider finite algebras, i.e. algebra of both finite domain and finite type.

A *term* \(t(x_1, \ldots, x_n)\) over \(A\) is an expression built using variables \(x_1, x_2, \ldots\) and function symbols in \(\tau\). The *term operation* \(t^A\) is the operation \(A^n \to A\) that we obtain if we interpret every function symbol as its corresponding operation in \(A\). *Polynomials* over \(A\) are terms, in whose construction we are additionally allowed to use constants from \(A\). By the *extension* of the algebra \(A = (A; f_1^A, \ldots, f_n^A)\) by the term \(t(x_1, \ldots, x_n)\) we denote the algebra \((A, t) = (A; f_1^A, \ldots, f_n^A, t^A)\).

As defined in the introduction the *equation solvability problem* \(\text{Eq}(A)\) of a finite algebra \(A\) is defined as the computational problem of deciding whether for two polynomials \(f(x_1, \ldots, x_n), g(x_1, \ldots, x_n)\) it holds that \(A \models \exists x_1, \ldots, x_n f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)\) or not. The *identity checking problem* \(\text{Eq}(A)\) of a finite algebra \(A\) asks whether for two polynomials \(f(x_1, \ldots, x_n), g(x_1, \ldots, x_n)\) it holds that \(A \models \forall x_1, \ldots, x_n f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)\) or not.

Here a polynomial is encoded by a string defining it, which in a finite algebra is proportional to its *length* (see e.g. [AMO17] for a precise definition). We remark that in the literature one
can also find other ways of encoding polynomials, which might result in different complexities (e.g. by circuits in \[IK17\], or certain normal forms like in \[HLW15\]).

In this paper we are going to study finite groups \( G = (G; e, e^{-1}) \) and their term extensions. In particular \((G, [\cdot, \cdot])\) will denote extension of the group by the commutator term \([x, y] = x^{-1}y^{-1}xy\). For simplicities sake we are going to abuse notation and sometimes use the symbol \(G\) both for the group and its underlying domain.

The exponent \(\exp(G)\) of a group is the smallest positive integer \(n\) such that \(g^n = e\) holds for all \(g \in G\). For an element \(a \in G\) we define \((a)\) to be the smallest normal subgroup of \(G\) containing \(a\), i.e. the group generated by \(a\) and all of its conjugated elements. For two subsets \(V, W\) of a group \([V, W]\) will denotes the subgroup generated by all elements of the form \([v, w]\), where \(v \in V\) and \(w \in W\). By \(G'\) we are going to denote the commutator subgroup of \(G\), i.e. \(G' = [G, G]\). The centralizer of a subset \(V \subseteq G\) is defined by \(C_G(V) = \{x \in G : \forall v \in V xv = vx\}\). The centralizer \(C_G(G)\) is called the center of \(G\).

The derived series of a group \(G\) is defined by \(G^{(1)} = G'\) and \(G^{(i+1)} = [G^{(i)}, G^{(i)}]\). A group is called solvable if there is a \(k\) such that \(G^{(k)} = \{e\}\). The lower central series of \(G\) is defined by \(G_1 = G\) and \(G_{i+1} = [G_i, G]\). The upper central series of \(G\) is defined by \(Z_1 = C_G(G)\) and \(Z_{i+1} = C_G(G/Z_i)\). A group is nilpotent if there is a \(k\) such that \(G_k = \{e\}\), or equivalently \(Z_k = G\).

The Fitting subgroup \(F(G)\) of \(G\) is the biggest nilpotent normal subgroup of \(G\). It is well known \[Bae57\] that in finite groups \(F(G)\) is equal to the set of all left Engel elements, i.e. elements \(g \in G\) such that for all \(h \in G\) there is an \(n \in N\) with \([\cdots [h, g], g], \ldots, g] = e.\)

### 3. Some complexity reductions

In this section we are going to show that in the proof of Theorem \[1\] it suffices to consider groups \(G\) that posses a nilpotent commutator subgroup, and a minimal normal subgroup \(N\) of \(G\) with \([G, N] = N\). The reductions we use in proving this statement slightly differ for the equation solvability problem and the identity checking problem, we are going to provide them in Lemma \[3\] and \[5\].

Before we start let us recall the following facts about the commutator:

**Lemma 2.** Let \(G\) be a group and \(N\) a normal subgroup of \(G\). Then

1. For all \(f, g, h \in G\): \([f^{-1}g, f^{-1}h, f] = f^{-1}[g, h]f\)
2. For all \(f \in G, g \in C_G(N), n \in N\): \([n, f] = [n, fg] = [n, gf]\)
3. If \(N\) is abelian, for all \(n, m \in N, b \in G\): \([n, b][m, b] = [nm, b]\)

**Proof.** All 3 statements follow from easy computations. \(\square\)

Let us call a subgroup \(V\) of \(G\) verbal if it is the range of some term \(p_V(x_1, \ldots, x_n)\) of \(G\). Then the following (many-to-one) reductions hold:

**Lemma 3.** Let \(V\) be a verbal subgroup of \(G\) and \(f\) be a term in the language of groups. Then

1. \(\text{Eq}(V, f)\) reduces to \(\text{Eq}(G, f)\) in polynomial time.
2. \(\text{Id}(V, f)\) reduces to \(\text{Id}(G, f)\) in polynomial time.

If \(V\) is a normal subgroup of \(G\), let \(H = G/V, K = G/C_G(V)\). Then

3. \(\text{Eq}(H, f)\) reduces to \(\text{Eq}(G, f)\) in polynomial time.
4. \(\text{Id}(K, f)\) reduces to \(\text{Id}(G, f)\) in polynomial time.
Proof. Lemma 9 and 10 of [HS11]. □

Note that the commutator subgroup of $G$ (and more general $[V,W]$ for verbal group $V$ and arbitrary $W$) is a verbal subgroup of $G$. Lemma 3(1) and (2) thus imply that for every element of the derived series $L = G^{(i)}$, $\text{Id}(L, f)$ reduces to $\text{Id}(G, f)$ and $\text{Id}(L, f)$ reduces to $\text{Id}(G, f)$ in polynomial time. In particular this implies that in proving Theorem 1 it is enough to consider the unique element of the derived series $L = G^{(i)}$ such that $L$ is not nilpotent, but $L'$ is. If we want to proceed further, we have to use the reductions Lemma 3(3) and (4) respectively.

Lemma 4. Let $G$ be a finite solvable, non-nilpotent group and $L$ be the last non-nilpotent element of the derived series of $G$. Then there exists an element $K$ of the lower central series of $L$ such that $H = L/K$ has a minimal normal subgroup $N$ with $[H, N] = N$ and $[H', N] = \{e\}$. Furthermore $N$ can be chosen such that $|H/C_H(N)| > 2$ if and only if $\exp(L/F(L)) > 2$.

Proof. Let $L$ be the last non-nilpotent element of the derived series. Since $L'$ is nilpotent and $L$ is not we have $L' \leq F(L) < L$. Let $g \in L \setminus F(L)$ and let us define the map $r_g : x \mapsto [x, g]$. Since $g \in L \setminus F(L)$, there is an element $a \in L$ such that $r_g^n(a) \neq e$ for all $n \in \mathbb{N}$. By the finiteness of $L$ we can without loss of generality assume that there is an $m$ such that $r_g^m(a) = a$. As $L'$ is nilpotent its lower central series is eventually equal to $\{e\}$. Let $K$ be the first element of this lower central series such that $a \notin K$. We set $H = L/K$. The normal subgroup $\langle a \rangle$ generated by $a$ in $H$ is abelian and satisfies $[H', \langle a \rangle] = \{e\}$, because it is contained in the last non-trivial element of the lower central series of $H'$. Lemma 2(3) implies that the map $r_g$ is an endomorphism of $\langle a \rangle$.

An easy calculation using Lemma 2(1) shows $[x^{-1}ax, g] = x^{-1}[a, x^{-1}, g^{-1}g]x$. As $H'$ lies in the centralizer of $a$, we have $r_g(x^{-1}ax) = x^{-1}r_g(a)x$. Since $a$ and all of its conjugates generate $\langle a \rangle$ and $r_g^m(a) = a$, $r_g$ has to be an automorphism of $\langle a \rangle$. Without loss of generality we can assume that $N = \langle a \rangle$ is a minimal normal subgroup - otherwise we take such minimal normal subgroup contained in $\langle a \rangle$. This concludes the proof of the first part of the Lemma.

For the second part suppose that $\exp(L/F(L)) > 2$; in other words there is a $g \in L$ such that $g, g^2 \in L \setminus F(L)$. As above we can construct the group $H$ and a minimal normal subgroup $N = \langle a \rangle$ of $H$ such that $r_{g^2} : x \mapsto [x, g^2]$ is an automorphism of $N$. We claim that also $r_g$ is an automorphism of $N$. Otherwise $r_g(m) = [m, g] = e$ would hold for some $m \neq e$. But $N$ is minimal and thus generated by $m$. This in turn implies that $N$ centralizes $g$ and consequently also $g^2$ - contradiction.

In order to prove the opposite direction suppose that $\exp(L/F(L)) = 2$, i.e. for all $g \in L$ we have that $g^2 \in F(L)$. Let $K$, $H$ and $N$ as above. As $K$ is nilpotent it is a subgroup of $F(L)$ and thus $L/F(L)$ is isomorphic to $H/(F(L)/K)$. Since $(F(L)/K)$ is nilpotent, it is a subgroup of $F(H)$ which implies that $\exp(H/F(H)) = 2$. By the nilpotency of $F(H)$ and minimality of $N$ we have that $[F(H), N] = \{e\}$. Therefore, for every $g \notin F(L)$ and all $a \in N$ we have $[a, g^2] = e$. An easy calculation shows $[a, g^2] = [a, g]g^{-1}[a, g]g$ which is equal to $[ag^{-1}ag, g]$ by Lemma 2. As $r_g$ is an automorphism of $N$, $[a, g^2] = e$ implies $g^{-1}ag = a^{-1}$. Now let $h, g \in L \setminus C(N)$. By what we showed $h^{-1}g^{-1}agh = a$ holds for all $a \in N$, hence $gh \in C(N)$. This concludes the proof that $|H/C_H(N)| = 2$. □

Lemma 5. Let $G$ be a finite solvable, non-nilpotent group and $L$ be the last non-nilpotent element of the derived series. Let $H_0 = L$ and $H_{i+1} = H_i/C_{H_i}(H')$. Then there is an $i$ such that $H_i$ has a minimal normal subgroup $N$ with $[H, N] = N$ and $[H', N] = \{e\}$. Furthermore $N$ can be chosen such that $|H/C_H(N)| > 2$ if and only if $\exp(L/F(L)) > 2$. 

Proof. Let $L$ be the last non-nilpotent element of the derived series of $G$. For $g \in L \setminus F(L)$ let us define the map $r_g : x \mapsto [x,g]$. As $g \in L \setminus F(L)$ there is an element $a \in L$ such that $r_g^n(a) \neq e$ for all $n \in \mathbb{N}$. By the finiteness of $L$ we can furthermore assume that there is an integer $m$ with $r_g^m(a) = a$. Let $H_0 = L$ and $H_{i+1} = H_i/C_{H_i}(H_i')$. As $L'$ is nilpotent and $a \in L'$ there is an index $i$ such that $aH_{i-1} \subseteq C_{H_i}(H_i') \setminus \{e\}$. We set $H = H_i$. The normal subgroup $\langle a \rangle$ generated by $a$ in $H$ is abelian, as it is contained in the center of $H'$. Lemma 2 (3) implies that the map $r_g$ is an endomorphism of $\langle a \rangle$. As in the proof of Lemma 4 we can show that $r_g$ is actually an automorphism of $\langle a \rangle$. Furthermore we can assume that $N = \langle a \rangle$ is a minimal normal subgroup of $H$ - otherwise we take such minimal normal subgroup contained in $\langle a \rangle$. This concludes the proof of the first part of the Lemma.

The proof of the second part is also analogous to the proof of Lemma 4 (using the fact that $C_{H_i}(H_i')$ is always nilpotent, as $[[C_{H_i}(H_i'), C_{H_i}(H_i')], C_{H_i}(H_i')] \subseteq [H_i', C_{H_i}(H_i')] = \{e\}$).

Remark 6. We remark that the group $H$ constructed in Lemma 4 and 5 might differ for the same $G$, even using the same elements $g, a \in G$. Further note that forming the quotients in Lemma 4 and 5 is indeed a necessary step in proving the existence of a minimal normal subgroup $N$ with $[H, N] = N$: An example of a group without this property is the special linear group $SL(2,3)$. It is not nilpotent and its commutator subgroup is the (nilpotent) quaternion group, but its only minimal normal subgroup $\mathbb{Z}_2$ is equal to its center.

Both Lemma 4 and 5 reduce the task of proving Theorem 1 to a very specific subclass of solvable, not nilpotent groups. In the following lemma we list some of the properties of such groups that were partially already proven in Lemma 4.

Lemma 7. Let $G$ be a finite solvable group and $N$ a minimal normal subgroup, such that $[G, N] = N$ and $[G', N] = \{e\}$. Then

1. $N$ is elementary abelian.
2. For all $b \in G \setminus C_G(N)$ the map $r_b : n \mapsto [n, b]$ is an automorphism of $N$.
3. If $|G/C_G(N)| = 2$, then for all $b \in G \setminus C_G(N)$ and $n \in N$ we have $b^{-1}nb = n^{-1}$.

This implies further that $N$ is a cyclic group of odd prime order.

Proof. (1) is a well-known fact that holds for all minimal normal subgroups in all finite solvable groups. (2) is analogous to the proof step of Lemma 4 in which we show that $r_g$ is an automorphism of $N$. To show that $b^{-1}nb = n^{-1}$ in (3) we can also argue as in the proof of Lemma 4. If $\exp(N) = 2$ this would imply $b^{-1}nb = n$, thus $b$ commutes with $N$ - contradiction! So by (1) $\exp(N)$ has to be equal to some odd prime $p$. Since for all $b \in G \setminus C_G(N)$ $[n, b] = n^{-2}$, the commutator group $N = [G, \{n\}]$ just consists of powers of $n$, i.e it is cyclic.

4. Proof of the main theorem

We are now ready to prove Theorem 1. Depending on the index of $C_G(N)$ in $G$ we do a case distinction.

Lemma 8. Let $G = (G; e, e^{-1})$ be a finite solvable and non-nilpotent group. Furthermore assume that there is a non-trivial minimal normal subgroup $N$ such that $C_G(N) \cong G'$ and $|G/C_G(N)| > 2$. Then $\text{Eq}(G, [\cdot, \cdot])$ is NP-complete and $\text{Id}(G, [\cdot, \cdot])$ is co-NPcomplete.

Proof. We prove the statement by constructing terms in $(G; [\cdot, \cdot])$ that allow us to reduce the $|G/C_G(N)|$-graph-coloring problem to $\text{Eq}(G, [\cdot, \cdot])$ and its complement to $\text{Id}(G, [\cdot, \cdot])$. Reductions of similar type were already used in [HS12] and [IK17].
Let us define the sequence of terms
\[ t_1(x, y_1) = [x, y_1] \]
\[ t_{k+1}(x, y_1, \ldots, y_k, y_{k+1}) = [t_k(x, y_1, \ldots, y_k), y_{k+1}] \].

Note that the length of \( t_k \) in \((G, [\cdot, \cdot])\) grows linearly in \( k \). Furthermore, if for every \( j = 1, \ldots, k \) we have \( b_j \in G \setminus C_G(N) \), then \( x \mapsto t_k(x, b_1, \ldots, b_k) \) is an automorphism of \( N \) by Lemma 7 (2). If there is a \( j \) with \( b_j \in C_G(N) \), then \( t_k(x, b_1, \ldots, b_k) = e \) for all \( x \in N \).

Now let \((V; E)\) be an undirected graph, i.e. an input of the \(|G/C_G(N)|\)-coloring problem. Then we define the term
\[ r(x, (y_v)_{v \in V}) = t_{|E|}(x, (y_v^{-1})(v_1, v_2)_{v \in E}). \]

By the properties of \( t_{|E|}, t(x, (b_v)_{v \in V}) \), for \( x \in N \) is equal to \( e \) if there is an edge \((v_1, v_2) \in E\), such that \( b_1, b_2^{-1} \in C_G(N) \). If however, for all edges \((v_1, v_2) \in E\) the elements \( b_1 \) and \( b_2 \) are in different cosets of \( C_G(N) \), then \( x \mapsto r(x, (b_v)_{v \in V}) \) is a permutation of \( N \). Note also, that for \( x \in N \) the value of \( r(x, (b_v)_{v \in V}) \) only depends on the \( C_G(N)\)-cosets of the elements \( b_v \).

Thus if the equation \( r(x, (y_v)_{v \in V}) = n \) for some \( n \in N \setminus \{e \} \) has a solution with \( x \in N \), then the graph is \(|G/C_G(N)|\)-colorable: just color the vertices by the corresponding elements of the \( C_G(N)\)-cosets of the solution to the equation. Conversely a proper \(|G/C_G(N)|\)-coloring of the graph gives rise to a solution of the equation, by assigning representatives of the \( C_G(N)\)-classes to the \(|G/C_G(N)|\)-many colors. Analogously the identity \( r(x, (y_v)_{v \in V}) = e \) holds for all \( x \in N \) if there is no proper \(|G/C_G(N)|\)-coloring of the graph \((V; E)\).

At last notice that we can restrict ourselves to solutions with \( x \in N \), since \( N \) is verbal. By \([N, G] = N\) every element of \( N \) can be written as the product of commutator expressions \([n, g]\), \( n \in N \). Thus there is a polynomial of the form \( s_N(z_1, \ldots, z_k) = [n_1, z_1] \cdot [n_2, z_2] \cdots [n_k, z_k] \) with \( n_1, \ldots, n_k \in N \) such that \( N \) is its range. When substituting \( x = s_N(z) \) in \( r \), the resulting term is still polynomial in the size of the graph \((V; E)\). Thus the \(|G/C_G(N)|\)-coloring problem reduces to \( \text{Eq}(G) \) and its complement reduces to \( \text{Id}(G) \). This concludes the proof. \( \square \)

It is left to consider the case where \(|G/C_G(N)| = 2\); we show that then \((G, w)\) induces hard problems.

**Lemma 9.** Let \( G \) be a finite solvable, non-nilpotent group and let \( w(x, y_1, y_2, y_3) = x^8([x, y_1], [y_2], y_3]) \). Furthermore assume that there is a non-trivial minimal normal subgroup \( N \) such that \( C_G(N) \supseteq G' \) and \(|G/C_G(N)| = 2\). Then \( \text{Eq}(G, w) \) is NP-complete and \( \text{Id}(G, w) \) is co-NP-complete.

**Proof.** By Lemma 7(3) we have for \( b \notin C_G(N), x \in N \) we have \( b^{-1}xb = x^{-1} \) and consequently \([x, b] = x^{-2}\). We are going to prove the NP-hardness of \( \text{Eq}(G, w) \) by encoding 3-SAT. For that observe that, by the above
\[ w(e, y_1, y_2, y_3) = e \]
\[ w(x, y_1, y_2, y_3) = e \] if \( x \in N \) and \( \forall \ i : y_i \notin C_G(N) \)
\[ w(x, y_1, y_2, y_3) = x^8 \] if \( x \in N \) and \( \exists \ i : y_i \in C_G(N) \)

Thus if one of the elements \( b_1, b_2, b_3 \) lies \( C_G(N) \), the map \( x \mapsto w(x, b_1, b_2, b_3) \) is an automorphism of \( N \). Otherwise it is constant and equal to \( e \). Now let us define recursively the terms
\[ w_1(x, y_1, y_2, y_3) = w(x, y_1, y_2, y_3), \]
\[ w_{n+1}(x, y_1, y_2, \ldots, y_{3n+3}) = w(w_n(x, y_1, y_2, \ldots, y_{3n}), y_{3n+1}, y_{3n+2}, y_{3n+3}). \]
Then $x \mapsto w_n(x, b_1, \ldots, b_{3n})$ is an automorphism of $N$, if in every triple $(b_{3i}, b_{3i+1}, b_{3i+2})$ at least one entry is from $C_G(N)$, otherwise it is constant and equal to $e$ (on $N$).

This allows us to encode an input of 3-SAT as an input of $\operatorname{Eq}(G, w)$. Let $(l_1 \lor l_2 \lor l_3) \land \cdots \land (l_{3n} \lor l_{3n+1} \lor l_{3n+2})$ be a 3-CNF formula in variables $z_1, \ldots, z_k$ with the $l_i$ being the literals in variables $z_{ij}$. Then let us form the polynomial $w_{n+1}(x, l'_1, l'_2, \ldots, l'_{3n+3})$ in variables $z'_1, \ldots, z'_k$ with $l'_i = z'_i$ if $l_i = z_i$ and $l'_i = bz'_i$ if $l_i = \neg z_i$, where $b$ is an element of $G \setminus C_G(N)$.

Let $n \in N \setminus \{e\}$. Then it is not hard to see that the equation $n = w_{n+1}(x, l'_1, l'_2, \ldots, l'_{3n+3})$ has a solution with $x \in N$ if and only if the instance of 3-SAT is satisfiable. Moreover $w_{n+1}(x, l'_1, l'_2, \ldots, l'_{3n+3})$ is constantly equal to $e$ for $x \in N$, if and only if the instance of 3-SAT is unsatisfiable.

$N$ is verbal, so as in the proof of Lemma 5 we can restrict us to $x \in N$, by substituting $x$ by a polynomial with range $N$. Thus 3-SAT reduces to $\operatorname{Eq}(G, w)$ and its complement reduces to $\operatorname{ld}(G, w)$ in polynomial time. We conclude that $\operatorname{Eq}(G, w)$ is NP-complete, and $\operatorname{ld}(G, w)$ is co-NP-complete.

We remark that a proof of Lemma 9 for the special case $G = S_3$ due to Idziak already appeared in [GK11]. We are now ready to sum up the proof of Theorem 1.

**Proof of Theorem 1** Let $G$ be a finite solvable, non-nilpotent group and let $L$ be the last non-nilpotent element of its derived series. By Lemma 3 (1),(3) and Lemma 4 there is a group $H$ such that

- For every term $f$, $\operatorname{Eq}(H, f)$ reduces to $\operatorname{Eq}(G, f)$ in polynomial time.
- $H$ has a non-trivial minimal normal subgroup $N$ with $[H, N] = N$ and $[H', N] = \{e\}$.
- $N$ can be picked such that $|H/C_H(N)| > 2$ if and only if $\exp(L/F(L)) > 2$.

If $|H/C_H(N)| > 2$ it follows from Lemma 5 that $\operatorname{Eq}(H, \cdot, \cdot)$ is NP-hard. If $|H/C_H(N)| = 2$, it follows from Lemma 5 that $\operatorname{Eq}(H, w)$ is NP-hard. The proof for the identity checking problem is analogous, using the reduction from Lemma 6 (2),(4) and Lemma 6 instead.

Note that the inversion $^-1$ is actually not needed, since in any input we can substitute $(xy)^-1 = y^-1x^-1$ and $x^-1 = x^{|G|-1}$.  

5. DISCUSSION

Theorem 1 does not complete the complexity classification of $\operatorname{Eq}(G, [\cdot, \cdot])$ and $\operatorname{ld}(G, [\cdot, \cdot])$ for all finite groups $G$, as asked for in Problem 1 of [HS11]. However the class $C$ of groups for which the complexity is still unknown consists only of groups $G$ satisfying $G' \leq F(G) < G$ and $\exp(G/F(G)) = 2$ (and groups containing such $G$ in their derived series).

By Lemma 4 and Lemma 3 it would suffice to show hardness only for all those $G \in C$ that additionally have a minimal normal subgroup $N$ with $|G/C_G(N)| = 2$ in order to prove hardness for all $G \in C$. By Lemma 1 (3) the elements of $G \setminus C_G(N)$ then act on $N$ as by inversion; furthermore $N$ is a cyclic group of order $p$ for some odd prime $p$. Thus the semidirect product of $G/C_G(N)$ and $N$ is equal to the dihedral group $D_{2p}$. This naturally leads to the question:

**Question 10.** Let $p$ be an odd prime. What is the computational complexity of $\operatorname{Eq}(D_{2p}, [\cdot, \cdot])$ and $\operatorname{ld}(D_{2p}, [\cdot, \cdot])$ for the dihedral group $D_{2p}$? In particular, what is the complexity for the symmetric group on 3 elements $D_6 = S_3$? (cf. Problem 1 in [HS11]).

If $\operatorname{Eq}(D_{2p}, [\cdot, \cdot])$ was NP-complete (respectively $\operatorname{ld}(D_{2p}, [\cdot, \cdot])$ co-NP-complete) the proof would most likely rely on the action of $D_{2p}/\mathbb{Z}_p$ on $\mathbb{Z}_p$ and thus (using similar arguments
as in Lemma 9) lift to all non-nilpotent groups with exp\((G/F(G)) = 2\). But also other possible answers to Question 10 would be of central importance in getting a better understanding the expressive power of the commutator operation in finite groups.

References

[AMO17] Erhard Aichinger, Nebojša Mudrinski, and Jakub Opršal. Complexity of term representations of finitary functions. arXiv preprint arXiv:1709.01759, 2017.

[Bae57] Reinhold Baer. Engelsche Elemente Noetherscher Gruppen. Mathematische Annalen, 133(3):256–270, 1957.

[BL05] Stanley Burris and John Lawrence. Results on the equivalence problem for finite groups. Algebra Universalis, 52(4):495–500, 2005.

[Föl17] Attila Földvári. The complexity of the equation solvability problem over semipattern groups. International Journal of Algebra and Computation, 27(02):259–272, 2017.

[Föl18] Attila Földvári. The complexity of the equation solvability problem over nilpotent groups. Journal of Algebra, 495:289–303, 2018.

[GMK11] Tomasz Gorazd and Jacek Krzaczkowski. The complexity of problems connected with two-element algebras. Reports on Mathematical Logic, 2011(46):91–108, 2011.

[GR02] Mikael Goldmann and Alexander Russell. The complexity of solving equations over finite groups. Information and Computation, 178(1):253–262, 2002.

[HGW11] Gábor Horváth, John Lawrence, and Ross Willard. The complexity of the equation solvability problem over finite rings. preprint on http://real.mtak.hu/28210/, 2015.

[HMSL07] Gábor Horváth, László Mérai, Csaba Szabó, and John Lawrence. The complexity of the equivalence problem for nonsolvable groups. Bulletin of the London Mathematical Society, 39(3):433–438, 2007.

[Hor08] Gábor Horváth. Functions and Polynomials over Finite Groups from the Computational Perspective. PhD thesis, University of Hertfordshire, 2008.

[Hor11] Gábor Horváth. The complexity of the equivalence and equation solvability problems over nilpotent rings and groups. Algebra universalis, 66(4):391–403, 2011.

[HS11] Gábor Horváth and Csaba Szabó. The extended equivalence and equation solvability problems for groups. Discrete Mathematics & Theoretical Computer Science, 13(4):23–32, 2011.

[HS12] Gábor Horváth and Csaba Szabó. Equivalence and equation solvability problems for the alternating group \(A_4\). J. Pure Appl. Algebra, 2012.

[IK17] Paweł Idziak and Jacek Krzaczkowski. Satisfiability in multi-valued circuits. To appear in the proceedings of LICS 2018; arXiv preprint arXiv:1710.08163, 2017.

[Kom18] Michael Kompatscher. The equation solvability problem over nilpotent Mal’cev algebras. arXiv preprint; arXiv:1710.03083, to appear in the International Journal of Algebra and Computation, 2018.