Hardness of equations over finite solvable groups under the exponential time hypothesis

Armin Weiß
Universität Stuttgart, Institut für Formale Methoden der Informatik (FMI), Germany
armin.weiss@fmi.uni-stuttgart.de

Abstract

Goldmann and Russell (2002) initiated the study of the complexity of the equation satisfiability problem in finite groups by showing that it is in P for nilpotent groups while it is NP-complete for non-solvable groups. Since then, several results have appeared showing that the problem can be solved in polynomial time in certain solvable groups of Fitting length two. In this work, we present the first lower bounds for the equation satisfiability problem in finite solvable groups: under the assumption of the exponential time hypothesis, we show that it cannot be in P for any group of Fitting length at least four and for certain groups of Fitting length three. Moreover, the same hardness result applies to the equation identity problem.

2012 ACM Subject Classification Theory of computation → Problems, reductions and completeness

Keywords and phrases equations in groups, solvable groups, exponential time hypothesis

Funding *Armin Weiß*: Funded by DFG project DI 435/7-1.

Acknowledgements I am grateful to Moses Ganardi for bringing my attention to the AND-weakness conjecture and pointing out the relation to the exponential time hypothesis. I am also thankful to David A. Mix Barrington for an interesting email exchange concerning the AND-weakness conjecture and the idea to include steps of the lower central series in Proposition 8 to get a more refined upper bound. Finally, I want to thank Caroline Mattes and Jan Philipp Wächter for many helpful discussions.

1 Introduction

The study of equations over algebraic structures has a long history in mathematics. Some of the first explicit decidability results in group theory are due to Makanin [29], who showed that equations over free groups are decidable. Subsequently several other decidability and undecidability results as well as complexity results on equations over infinite groups emerged (see [11, 13, 28, 33] for a random selection). For a fixed group G, the equation satisfiability problem EQN-SAT is as follows: given an expression $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$ where $\mathcal{X}$ is some set of variables, the question is whether there exists some assignment $\sigma : \mathcal{X} \to G$ such that $\sigma(\alpha) = 1$ (here σ is extended to expressions in the natural way – $\mathcal{X}^{-1}$ is a disjoint copy of $\mathcal{X}$ representing the inverses of $\mathcal{X}$). Likewise EQN-ID is the problem, given an expression, decide whether it evaluates to 1 under *all* assignments.

Henceforth, all groups we consider are finite. In this case, equation satisfiability and related questions are clearly decidable by an exhaustive search. Still the complexity is an interesting topic of research: its study has been initiated by Goldmann and Russell [14], who showed that satisfiability of systems of equations can be decided in P if and only if the group is abelian (assuming $\mathsf{P} \neq \mathsf{NP}$) – otherwise, the problem is NP-complete. They also obtained some results for single equations: EQN-SAT is NP-complete for non-solvable groups, while for nilpotent groups it is in P. This left the case of solvable but non-nilpotent groups open. Indeed, Burris and Lawrence raised the question whether EQN-ID$(G) \in \mathsf{P}$ for all finite solvable groups G [9, Problem 1]. Moreover, Horváth [16] conjectured a positive answer.

Contribution. In this work we give a negative answer to this question assuming the exponential time hypothesis by showing the following result:

▶ **Corollary A.** *Let G be finite solvable group and assume that either*
- *the Fitting length of G is at least four, or*
- *the Fitting length of G is three and there is no Fitting-length-two normal subgroup whose index is a power of two.*

Then EQN-SAT(G) *and* EQN-ID(G) *are not in* P *under the exponential time hypothesis.*

To the best of our knowledge, this constitutes the first hardness results for EQN-SAT(G) and EQN-ID(G) if G is solvable. The Fitting length of a group G is the minimal d such that there is a sequence $1 = G_0 \trianglelefteq \cdots \trianglelefteq G_d = G$ with all quotients G_{i+1}/G_i nilpotent.

Moreover, we show that if S is a semigroup with a group divisor meeting the requirements of Corollary A, EQN-SAT(S) (here the input consists of two expressions) is also not in P under the exponential time hypothesis. Finally, we give an upper bound of $2^{\mathcal{O}(n^{1/(d-1)})}$ for the length of the shortest G-program (definition see below) for the n-input AND function in a finite solvable group of Fitting length $d \geq 2$.

General approach. The complexity of EQN-SAT is closely related to the complexity of the satisfiability problem for G-programs (denoted by ProgramSAT – for a definition see Section 3). Indeed, [5] gives a reduction from EQN-SAT to ProgramSAT (be aware that in infinite groups this is *not* true, in general). Moreover, also ProgramSAT is in P for nilpotent groups and NP-complete for non-solvable groups [6].

In order to show hardness of these problems, one usually reduces some NP-complete problem like 3SAT or C-Coloring to them. Typically, this requires to encode big logical conjunctions into the group G. Therefore, the complexity of these problems is linked to the length of the shortest G-program for the AND function. Indeed, [5, Theorem 4] shows that, if the AND function can be computed by G-programs of polynomial length, then ProgramSAT in $G \wr C_k$ for $k \geq 4$ is NP-complete (here C_k denotes the cyclic group of order k). Thus, if there exists a solvable group with polynomial length G-programs for the AND function, then there is a solvable group with an NP-complete ProgramSAT problem.

It is well-known that G-programs describe the circuit complexity class CC^0 [30] with the depth of the circuit relating to the Fitting length of the group. One can make a depth size trade-off for the AND function using a divide-and-conquer approach: Assume there is a circuit of depth two and size 2^n for the n-input AND (which is the case by [3]). Since the n-input AND can be decomposed as $\sqrt{n}$-input AND of $\sqrt{n}$ many $\sqrt{n}$-input ANDs, we obtain a CC^0 circuit of depth 4 and size roughly $2^{\sqrt{n}}$.

This observation plays a crucial role for our results: it allows us to reduce an m-edge C-Coloring instance to an equation of size roughly $2^{\sqrt{m}}$. We compare this to the exponential time hypothesis (ETH), which conjectures that n-variable 3SAT cannot be solved in time $2^{o(n)}$. ETH implies that C-Coloring cannot be solved in time $2^{o(m)}$, which gives us a quasipolynomial lower bound on EQN-SAT and EQN-ID. Notice that in the literature there are several other quasipolynomial lower bounds building on the exponential time hypothesis – see [1, 7, 8] for some examples.

Outline. In Section 2, we fix our notation and state some basic results on inducible and atomically universally definable subgroups. Some of these observations are well-known, while others, to the best of our knowledge, have not been stated explicitly. Section 3 gives a little excursion to the complexity of the AND-function in terms of G-programs over finite solvable groups deriving an upper bound $2^{\mathcal{O}(n^{1/(d-1)})}$ if $d \geq 2$ is the Fitting length of G.

Section 4 and Section 5 are the main part of our paper: we reduce the C-Coloring problem to EQN-SAT and EQN-ID. For the reduction, we need some special requirements on the group G. In Section 5 we show that actually the requirements of Corollary A are enough using the concept of inducible and atomically universally definable subgroups. Finally, in Corollary 21 we examine consequences to EQN-SAT in semigroups.

Related work on equations. Since the work of Goldman and Russell [14] and Barrington et. al. [5], a long list of literature has appeared investigating EQN-ID and EQN-SAT in groups and other algebraic structures. In [9] it is shown that EQN-ID is in P for nilpotent groups as well as for dihedral groups D_k where k is odd. Horváth [17, 20] extended these results by showing, in particular, that EQN-SAT(G) is in P for $G = C_n \rtimes B$ with B abelian, $n = p^k$ or $n = 2p^k$ for some prime p. Moreover, EQN-ID is in P for semidirect products $G = C_{n_1} \rtimes (C_{n_2} \rtimes \cdots \rtimes (C_{n_k} \rtimes (A \rtimes B)))$ with A, B abelian. Finally, in [12] it is proved that EQN-SAT(G) $\in \mathsf{P}$ for so-called semipattern groups. Notice that all these groups have in common that their Fitting length is at most two.

In [18, 19] the EQN-SAT and EQN-ID problems for generalized terms are introduced. Here a generalized term means an expression which may also use commutators or even more complicated terms inside the input expression. Using commutators is a more succinct representation, which allows for showing that EQN-SAT is NP-complete and EQN-ID is coNP-complete in the alternating group A_4 [19]. In [27] this result is extended by showing that, with commutators and the generalized term $w(x, y_1, y_2, y_3) = x^8[x, y_1, y_2, y_3]$, EQN-SAT is NP-complete and EQN-ID is coNP-complete for all non-nilpotent groups.

There is also extensive literature on equations in other algebraic structures – for instance, [2, 5, 22, 23, 24, 25, 34, 35, 36] in semigroups. We only mention two of them explicitly: [23] showed that identity checking (EQN-ID without constants in the input) in semigroups is coNP complete. Moreover, among other results, [2] reduces the identity checking problem in the direct product of maximal subgroups to identity checking in some semigroup.

2 Preliminaries

The set of words over some alphabet Σ is denoted by Σ^*. The length of a word $w \in \Sigma^*$ is denoted by $|w|$. We denote the interval of integers $\{ i, \ldots, j \}$ by $[i \,..\, j]$.

Complexity. We use standard notation from complexity theory. In several cases we use the notion of AC^0 many-one reductions (denoted by $\leq_{\mathrm{m}}^{\mathsf{AC}^0}$) meaning that the reducing function can be computed in AC^0 (i.e., by a polynomial-size, constant-depth Boolean circuit). The reader unfamiliar with this terminology may think about logspace or polynomial time reductions. Also be aware that in order to obtain AC^0 many-one reductions in most cases we need the presence of neutral letters for padding reasons.

Exponential time hypothesis. The exponential time hypothesis (ETH) is the conjecture that there is some $\delta > 0$ such that every algorithm for 3SAT needs time $\Omega(2^{\delta n})$ in the worst case where n is the number of variables of the given 3SAT instance. By the sparsification lemma [21, Thm. 1] this is equivalent to the existence of some $\epsilon > 0$ such that every algorithm for 3SAT needs time $\Omega(2^{\epsilon(m+n)})$ in the worst case where m is the number of clauses of the given 3SAT instance (see also [10, Thm. 14.4]). In particular, under ETH there is no algorithm for 3SAT running in time $2^{o(n+m)}$.

C-Coloring. A C-coloring for $C \in \mathbb{N}$ of a graph $\Gamma = (V, E)$ is a map $\chi : V \to [1 \,..\, C]$. A coloring χ is called *valid* if $\chi(u) \neq \chi(v)$ whenever $\{ u, v \} \in E$. The problem C-Coloring is

as follows: given an undirected graph $\Gamma = (V, E)$, the question is whether there is a valid C-coloring of Γ. The C-Coloring problem is one of the classical NP-complete problems for $C \geq 3$. Moreover, by [10, Thm. 14.6], 3-Coloring cannot be solved in time $2^{o(|V|+|E|)}$ unless ETH fails. Since 3-Coloring can be reduced to C-Coloring for fixed $C \geq 3$ by introducing only a linear number of additional edges and a constant number of vertices, it follows that also C-Coloring cannot be solved in time $2^{o(|V|+|E|)}$ unless ETH fails for any $C \geq 3$.

Commutators and Fitting series. Throughout, we only consider finite groups G. We use notation similar to [32]. We write $[x, y] = x^{-1}y^{-1}xy$ for the commutator and $x^y = y^{-1}xy$ for the conjugation. Moreover, we write $[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$ for $n \geq 3$. We also write g^H for the set $\{ g^h \mid h \in H \}$ (be aware that here we differ from [32]).

As usual for subsets $X, Y \subseteq G$, we write $\langle X \rangle$ for the subgroup generated by X and we define $[X, Y] = \langle [x, y] \mid x \in X, y \in Y \rangle$ and $[X_1, \ldots, X_k] = [[X_1, \ldots, X_{k-1}], X_k]$ for $X_1, \ldots, X_k \subseteq G$. In contrast, we write $[X, Y]_{\text{set}} = \{ [x, y] \mid x \in X, y \in Y \}$ (thus, $[X, Y] = \langle [X, Y]_{\text{set}} \rangle$) and $[X_1, \ldots, X_k]_{\text{set}} = [[X_1, \ldots, X_{k-1}]_{\text{set}}, X_k]_{\text{set}}$.

▶ **Lemma 1.** *If $X_i^G = X_i \subseteq G$ for $i = 1, \ldots, k$, then*

$$[\langle X_1 \rangle, \ldots, \langle X_k \rangle] = \langle [X_1, \ldots, X_k]_{\text{set}} \rangle .$$

Proof. By [32, 5.1.7], we have $[\langle X \rangle, \langle Y \rangle] = [X, Y]^{\langle X \rangle \langle Y \rangle}$ for arbitrary $X, Y \subseteq G$. Thus, if $X = X^G$ and $Y = Y^G$, we have $[\langle X \rangle, \langle Y \rangle] = [X, Y]$. Now a straightforward induction shows the lemma. ◀

For $x, y \in G$, we write $[x, {}_k\ y] = [x, \underbrace{y, \ldots, y}_{k \text{ times}}]$ and likewise for $X, Y \subseteq G$, we write $[X, {}_k\ Y] = [X, \underbrace{Y, \ldots, Y}_{k \text{ times}}]$ and $[{}_k\ Y] = [\underbrace{Y, \ldots, Y}_{k \text{ times}}]$.

Since G is finite, there is some $M \in \mathbb{N}$ such that $[X, {}_M\ Y] = [X, {}_i\ Y]$ for all $i \geq M$ and all $X, Y \subseteq G$ with $X^G = X$ and $Y^G = Y$ (notice that $[X, {}_i\ Y] \leq [X, {}_j\ Y]$ for $j \leq i$ due to the normality of $[X, Y]$). We fix this M throughout.

The k-th term of the lower central series is $\gamma_k G = [G, {}_k\ G]$. The *nilpotent residual* of G is defined as $\gamma_\infty G = \gamma_M G$ where M is as above (i.e., $\gamma_\infty G = \gamma_i G$ for every $i \geq M$).

▶ **Lemma 2.** *For all $X, Y \subseteq G$ with $X^G = X$ we have $[X, {}_M\ Y] = [[X, G], {}_M\ Y]$.*

Proof. We have $[X, G] \leq \langle X \rangle$ because $[x, g] = x^{-1}x^g \in X$. Thus, the inclusion right to left follows. The other inclusion is because $[X, {}_M\ Y] = [X, {}_{M+1}\ Y] \leq [X, G, {}_M Y] = [[X, G], {}_M\ Y]$. ◀

The *Fitting* subgroup $\mathrm{Fit}(G)$ is the union of all nilpotent normal subgroups. Let G be a finite solvable group. The *upper Fitting series*

$$1 = \mathcal{U}_0 G \lhd \mathcal{U}_1 G \lhd \cdots \lhd \mathcal{U}_k G = G$$

is defined by $\mathcal{U}_{i+1}G/\mathcal{U}_i G = \mathrm{Fit}(G/\mathcal{U}_i G)$. The *lower Fitting series*

$$1 = \mathcal{L}_d G \lhd \cdots \lhd \mathcal{L}_1 G \lhd \mathcal{L}_0 G = G$$

The following facts are also well-known:

▶ **Lemma 3.** *Let $H \trianglelefteq G$ be a normal subgroup. Then for all i, we have $\mathcal{U}_i H = \mathcal{U}_i G \cap H$. In particular,*

(i) *if $\mathrm{FitLen}(H) = i$, then $H \leq \mathcal{U}_i G$,*

(ii) *if $g \in \mathcal{U}_i G \setminus \mathcal{U}_{i-1} G$, then $\mathrm{FitLen}(\langle g^G \rangle) = i$.*

Equations in groups. An *expression* (also called a *polynomial* in [35, 20, 27]) over a group G is a word α over the alphabet $G \cup \mathcal{X} \cup \mathcal{X}^{-1}$ where $\mathcal{X}$ is a set of variables. Here $\mathcal{X}^{-1}$ denotes a formal set of inverses of the variables. Since we are dealing with finite groups only, a variable $X^{-1} \in \mathcal{X}^{-1}$ for $X \in \mathcal{X}$ can be considered as an abbreviation for $X^{|G|-1}$. Sometimes we write $\alpha(X_1, \dots, X_n)$ for an expression α to indicate that the variables occurring in α are from the set $\{ X_1, \dots, X_n \}$. Moreover, if $\beta_1, \dots, \beta_n$ are other expressions, we write $\alpha(\beta_1, \dots, \beta_n)$ for the expression obtained by substituting each occurrence of a variable X_i by the expression β_i.

An assignment for an expression α is a mapping $\sigma : \mathcal{X} \to G$ – here σ is canonically extended by $\sigma(X^{-1}) = \sigma(X)^{-1}$ and $\sigma(g) = g$ for $g \in G$. An assignment σ is *satisfying* if $\sigma(\alpha) = 1$ in G. The problems EQN-SAT(G) and EQN-ID(G) are as follows: for both of them the input is an expression α. For EQN-SAT(G) the question is whether there *exists* a satisfying assignment, for EQN-ID(G) the question is whether *all* assignments are satisfying.

Notice that in the literature EQN-SAT is also denoted by POL-SAT [35, 20] or Eq [27], while EQN-ID is also referred to as POL-EQ (e.g. in [35, 20, 24]) or Id [27].

If $\mathcal{X} = \mathcal{Y} \cup \mathcal{Z}$ with $\mathcal{Y} \cap \mathcal{Z} = \emptyset$ and we are given assignments $\sigma_1 : \mathcal{Y} \to G$ and $\sigma_2 : \mathcal{Z} \to G$, we obtain a new assignment $\sigma_1 \cup \sigma_2$ defined by $(\sigma_1 \cup \sigma_2)(X) = \sigma_1(X)$ if $X \in \mathcal{Y}$ and $(\sigma_1 \cup \sigma_2)(X) = \sigma_2(X)$ if $X \in \mathcal{Z}$. We write $[X \mapsto g]$ for the assignment $\{ X \} \to G$ mapping X to g.

Inducible and atomically universally definable subgroups. According to [14], we call a subset $S \subseteq G$ *inducible* if there is some expression $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$ such that $S = \{ \sigma(\alpha) \mid \sigma \colon \mathcal{X} \to G \}$. In this case we say that α *induces* S. Notice that in a finite group every verbal subgroup is inducible. This shows the first three points of the following lemma (for $\gamma_1 G$, see also [14, Lemma 5]):

▶ **Lemma 4.** *Let G be a finite group. Then*

(i) *for every $k \in \mathbb{N}$, the subgroup generated by all k-th powers is inducible,*

(ii) *every term $\gamma_k G$ of the lower central series is inducible,*

(iii) *every term $\mathcal{L}_k G$ of the lower Fitting series is inducible,*

(iv) *if $K \leq H \leq G$ and K is inducible in H and H inducible in G, then K is also inducible in G,*

(v) *if $H \leq G$ with $H = [G, H]$, then H is inducible.*

The fourth point follows simply by "plugging in" an expression for H inside an expression for K. The last point follows from the proof of [27, Lemma 9]. Be aware that the terms of the upper Fitting series are not inducible in general. Therefore, we introduce a similar notion:

We call a subset $S \subseteq G$ *atomically universally definable* if there is some word $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$ where $\mathcal{X} = \{ X \} \cup \{ Y_1, Y_2, \dots \}$ such that

$$S = \{ g \in G \mid (\sigma \cup [X \mapsto g])(\alpha) = 1 \text{ for all } \sigma \colon \{ Y_1, Y_2, \dots \} \to G \}.$$

In this case we say that α *atomically universally defines* S. (Notice that *universally definable* usually is defined analogously but instead of a single equation α one allows a Boolean formula of equations.)

It is clear that the center $Z(G)$ of a group is atomically universally definable by the expression $[X, Y]$. This generalizes as follows:

▶ **Lemma 5.** *Let G be a finite group.*

- *The Fitting group* $\mathrm{Fit}(G)$ *is atomically universally definable.*

- *If $N \leq H \leq G$ and N is normal in G and H/N is atomically universally definable in G/N and N is atomically universally definable in G, then H is atomically universally definable in G.*
- *All terms $\mathcal{U}_i G$ of the upper Fitting series are atomically universally definable.*
- *If $H \leq G$ is inducible, then the centralizer $C_G(H) = \{ g \in G \mid gh = hg \text{ for all } h \in H \}$ is atomically universally definable.*

Proof. By Lemma 3, the normal subgroup $\langle g^G \rangle$ generated by $g \in G$ is nilpotent if and only if $g \in \mathrm{Fit}(G)$. Therefore, $g \in \mathrm{Fit}(G)$ if and only if $\left[_M \ \langle g^G \rangle\right] = 1$, which, by Lemma 1, is the case if and only if $\left[_M \ g^G\right]_{\mathrm{set}} = 1$. Hence, the expression $[X^{Y_1}, \ldots, X^{Y_M}]$ atomically universally defines $\mathrm{Fit}(G)$.

Now, suppose that $\beta \in (G \cup \mathcal{X}_\beta \cup \mathcal{X}_\beta^{-1})^*$ with $\mathcal{X}_\beta = \{ X, Y_1, \ldots, Y_k \}$ atomically universally defines H/N in G/N and that $\alpha \in (G \cup \mathcal{X}_\alpha \cup \mathcal{X}_\alpha^{-1})^*$ with $\mathcal{X}_\alpha = \{ Z, Y_{k+1}, \ldots, Y_m \}$ atomically universally defines N in G. Thus, $g \in H$ if and only if $\beta(g, Y_1, \ldots, Y_k) \in N$ for all $Y_1, \ldots, Y_k \in G$ and $h \in N$ if and only if $\alpha(h, Y_{k+1}, \ldots, Y_m) = 1$ for all $Y_{k+1}, \ldots, Y_m \in G$. Hence, $\alpha(\beta(g, Y_1, \ldots, Y_k), Y_{k+1}, \ldots, Y_m) = 1$ for all $Y_1, \ldots, Y_m \in G$ if and only if $g \in H$ and so H is atomically universally definable.

The third point follows by induction from the first and second point. The fourth point is essentially due to [18, Lemma 10]. ◀

The following facts are also straightforward (see [14, Lemma 8] or [18, Lemma 9 and 10]):

▶ **Lemma 6.** *Let $H \leq G$ be an inducible subgroup. Then*

- $\text{EQN-SAT}(H) \leq_{\mathrm{m}}^{\mathsf{AC}^0} \text{EQN-SAT}(G)$*, and*
- $\text{EQN-ID}(H) \leq_{\mathrm{m}}^{\mathsf{AC}^0} \text{EQN-ID}(G)$*.*
- *If, moreover, H is normal in G, then* $\text{EQN-SAT}(G/H) \leq_{\mathrm{m}}^{\mathsf{AC}^0} \text{EQN-SAT}(G)$*.*

Notice that if $G = H \rtimes Q$, then we always have $\text{EQN-SAT}(Q) \leq_{\mathrm{m}}^{\mathsf{AC}^0} \text{EQN-SAT}(G)$ – even without H being inducible. This is because every solution in G projects to one in Q and every solution in Q embeds to one in G. Moreover, even if G is finite but not a semidirect product, $\text{EQN-SAT}(G/H)$ always reduces to $\text{EQN-SAT}(G)$ via disjunctive truth table reductions by the proof of [5, Theorem 9] – be aware that this relies on the fact that we are dealing with finite groups.

The situation for reducing $\text{EQN-ID}(G/H)$ to $\text{EQN-ID}(G)$ is slightly more complicated. For this we need an atomically universally definable subgroup.

▶ **Lemma 7.** *Let $H \trianglelefteq G$ be an atomically universally definable normal subgroup. Then*

$$\text{EQN-ID}(G/H) \leq_{\mathrm{m}}^{\mathsf{AC}^0} \text{EQN-ID}(G).$$

Proof. Denote $Q = G/H$. Let $\beta \in (G \cup \mathcal{X}_\beta \cup \mathcal{X}_\beta^{-1})^*$ with $\mathcal{X}_\beta = \{ Z, Y_1, \ldots, Y_k \}$ atomically universally define H and let $\alpha \in (Q \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$ be an instance for $\text{EQN-ID}(Q)$ (with $\mathcal{X} \cap \mathcal{X}_\beta = \emptyset$). Let $\tilde{\alpha}$ denote the expression obtained from α by replacing every constant of Q by an arbitrary preimage in G. Then $\sigma(\alpha) = 1$ in Q for all assignments $\sigma : \mathcal{X} \to Q$ if and only if $\tilde{\sigma}(\tilde{\alpha}) \in H$ for all assignments $\tilde{\sigma} : \mathcal{X} \to G$. By the choice of β, the latter is the case if and only if $\hat{\sigma}(\beta(\tilde{\alpha}, Y_1, \ldots, Y_k)) = 1$ for all assignments $\hat{\sigma} : \mathcal{X} \cup \{ Y_1, \ldots, Y_k \} \to G$. ◀

3 G-programs and AND-weakness

Let G be a finite group. An n-input G-program of length ℓ with variables from $\{ X_1, \ldots, X_n \}$ is a sequence

$$P = \langle X_{i_1}, a_1, b_1 \rangle \langle X_{i_2}, a_2, b_2 \rangle \cdots \langle X_{i_\ell}, a_\ell, b_\ell \rangle \in (\{ X_1, \ldots, X_n \} \times G \times G)^*.$$

For a mapping $\sigma : \{ X_1, \dots, X_n \} \to \{0,1\}$ (called an assignment) we define $\sigma(P) \in G$ as the group element $c_1 c_2 \cdots c_\ell$, where $c_j = a_j$ if $X_{i_j} = 0$ and $c_j = b_j$ if $X_{i_j} = 1$ for all $1 \leq j \leq \ell$. We say that an n-input G-program P *computes* a function $f : \{0,1\}^n \to \{0,1\}$ if P is over the variables $X_1, \dots, X_n$ and there is some $S \subseteq G$ such that $\sigma(P) = S$ if and only if $f(\sigma) = 1$.

ProgramSAT is the following problem: given a G-program P with variables $X_1, \dots, X_n$, decide whether there is an assignment $\sigma : \{ X_1, \dots, X_n \} \to G$ such that $\sigma(P) = 1$.

The AND-weakness conjecture. In [6], Barrington, Straubing and Thérien conjectured that, if G is finite and solvable, every G-program computing the n-input AND requires length exponential in n. This is called the AND-*weakness conjecture*.

Unfortunately, the term "exponential" seems to be a source of a possible misunderstanding: while often it means $2^{\Omega(n)}$, in other occasions it is used for $2^{n^{\Omega(1)}}$. Indeed, in [14, 5], the conjecture is restated as its *strong version* : "every G-program over a solvable group G for the n-input AND requires length $2^{\Omega(n)}$." However, already in the earlier paper [4], it is remarked that the n-input AND can be computed by depth-k CC^0 circuits of size $2^{\mathcal{O}(n^{1/(k-1)})}$ for every $k \geq 2$ (a CC^0 circuit is a circuit consisting only of MOD_m gates for some $m \in \mathbb{N}$). For a recent discussion about the topic also referencing the cases where the conjecture actually is proved, we refer to [26].

In this section we provide a more detailed upper bound on the length of G-programs for the AND function in terms of the Fitting length of G. We can view our upper bound as a refined version of the $2^{\mathcal{O}(n^{1/(k-1)})}$ upper bound for depth-k CC^0 circuits. This is because every depth-k CC^0 circuit can be transformed into a G-program of polynomial length over a group G of Fitting length k (indeed, of derived length k) by [30, Theorem 2.8].

The easiest variant to disprove the strong version of the AND-weakness conjecture is a divide-and-conquer approach: Assume we can compute the n-input AND by a CC^0-circuit of size 2^n and depth 2 (which is true by [3]). Since we can decompose the n-input AND as $\sqrt{n}$-input AND of $\sqrt{n}$ many $\sqrt{n}$-input ANDs, we obtain a CC^0 circuit of depth 4 and size roughly $2^{2\sqrt{n}}$ – or, more generally, a CC^0 circuit of depth $2k$ and size roughly $2^{k\sqrt[k]{n}}$. The proof of Proposition 8 uses a similar divide-and-conquer approach:

▶ **Proposition 8.** *Consider a strictly ascending series $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_m = G$ of normal subgroups where $H_i = \gamma_{k_i}(H_{i+1})$ with $k_i \in \mathbb{N} \cup \{\infty\}$ for $i \in [1\,..\,m-1]$ and $k_0 = \infty$. Denote $c = \{ i \in [1\,..\,m-1] \mid k_i = \infty \}$ and $C = \prod_{k_i < \infty}(k_i + 1)$.*

Then the n-input AND *function can be computed by a G-program of length $\mathcal{O}(2^{Dn^{1/c}})$ where $D = \frac{c}{C^{1/c}}$. More precisely, for every $n \in \mathbb{N}$ there is some $1 \neq g \in G$ and a G-program Q_n of length $\mathcal{O}(2^{Dn^{1/c}})$ such that*

$$\sigma(Q_n) = \begin{cases} g & \text{if } \sigma(X_1) = \cdots = \sigma(X_n) = 1, \\ 1 & \text{otherwise.} \end{cases}$$

Clearly we have $c \leq d - 1$ if d is the Fitting length of G. The lower Fitting series is the special example of such a series where $H_i = \mathcal{L}_{d-i}G$ and $k_i = \infty$ for all $i \in \{0, \dots, d\}$. Thus, we get the following corollary:

▶ **Corollary 9.** *Let G be a finite solvable group of Fitting length $d \geq 2$. Then the n-input* AND *function can be computed by a G-program of length $2^{\mathcal{O}(n^{1/(d-1)})}$.*

▶ **Example 10.** The symmetric group on four elements S_4 has Fitting length 3 with $S_4 \geq A_4 \geq C_2 \times C_2 \geq 1$ being both the upper and lower Fitting series. Therefore, we obtain a length-$\mathcal{O}(2^{2\sqrt{n}})$ program for the n-input AND by Proposition 8. In particular, the strong

version of the AND-weakness conjecture does not hold for the group S_4. Note that according to [6], S_4 is the smallest group for which the $2^{\Omega(n)}$ lower bound from [6] does not apply.

On the other hand, consider the group $G = (C_3 \times C_3) \rtimes D_4$ where D_4 (the dihedral group of order eight) acts faithfully on $C_3 \times C_3$[1]. It has Fitting length two. Moreover, its derived subgroup $G' = (C_3 \times C_3) \rtimes C_2$ still has Fitting length two. Hence, we have a series $H_3 = G$, $H_2 = G' = \gamma_1 G$, $H_1 = \gamma_\infty G' = C_3 \times C_3$, and $H_0 = 1$. Therefore, we get an upper bound of $\mathcal{O}(2^{n/2})$ for the length of a program for the n-input AND.

Proof of Proposition 8. We choose $K = (n/C)^{1/c}$. For simplicity, let us first assume that K is an integer. Moreover, we assume that K is large enough such that $H_i = [_K\ H_{i+1}]$ holds whenever $k_i = \infty$ and that $K \geq k_i + 1$ for all $k_i < \infty$.

We define sets $A_i \subseteq G$ inductively by $A_m = G$ and $A_i = [_K\ A_{i+1}]_{\text{set}}$ if $k_i = \infty$ and $A_i = [_{k_i+1}\ A_{i+1}]_{\text{set}}$ if $k_i < \infty$. By Lemma 1 and induction it follows that $H_i = \langle A_i \rangle$ for all $i \in 0, \ldots, m$. Since $H_1 \neq 1$, we find a non-trivial element $g \in A_1$. We can decompose g recursively. For this, we need some more notation: for $\ell \in [1\,..\,m]$ consider the set of words

$$V_\ell = \left\{ v = v_1 \cdots v_{\ell-1} \in [1\,..\,K]^{\ell-1} \;\middle|\; v_i \leq k_i + 1 \text{ for all } i \in [1\,..\,\ell-1] \right\}.$$

We have $|V_m| = C \cdot K^c = n$, so we can fix a bijection $\kappa\colon V_m \to [1\,..\,n]$.

Now, we can describe the recursive decomposition of $g = g_\epsilon$:

- g_v for $v \in V_m$ are arbitrary element from G, and
- $g_v = [g_{v1}, \ldots, g_{vK}]$ for $v \in V_\ell$ with $k_\ell = \infty$, and
- $g_v = [g_{v1}, \ldots, g_{v(k_\ell+1)}]$ for $v \in V_\ell$ with $k_\ell < \infty$.

For $v \in V_\ell$ we have $|g_v| \leq \sum_{i=1}^{K} 2^{K+1-i} |g_{vi}| \leq 2^{K+1} \max_i |g_{vi}|$ whenever $k_\ell = \infty$ and $|g_v| \leq 2^{k_\ell+2} \max_i |g_{vi}|$ if $k_\ell < \infty$. Therefore, setting $D = \frac{c}{C^{1/c}}$ we obtain by induction

$$|g_\varepsilon| \leq 2^{\sum_{k_\ell<\infty}(k_\ell+2)} (2^{K+1})^c \in \mathcal{O}(2^{Dn^{1/c}}).$$

In order to obtain a G-program for the n-input AND, we define G-programs P_v for $v \in \bigcup_{\ell \leq m} V_\ell$. In the commutators we need also programs for inverses: for a G-program $P = \langle X_{i_1}, a_1, b_1 \rangle \langle X_{i_2}, a_2, b_2 \rangle \cdots \langle X_{i_\ell}, a_\ell, b_\ell \rangle$ we set $P^{-1} = \langle X_{i_\ell}, a_\ell^{-1}, b_\ell^{-1} \rangle \cdots \langle X_{i_1}, a_1^{-1}, b_1^{-1} \rangle$. Clearly $(\sigma(P))^{-1} = \sigma(P^{-1})$ for all assignments σ.

- for $v \in V_m$ we set $P_v = \langle X_{\kappa(v)}, 1, g_v \rangle$,
- for $v \in V_\ell$ with $1 \leq \ell < m$ we set $P_v = [P_{v1}, \ldots, P_{vK}]$ if $k_\ell = \infty$, and
- for $v \in V_\ell$ with $1 \leq \ell < m$ we set $P_v = [P_{v1}, \ldots, P_{v(k_\ell+1)}]$ if $k_\ell < \infty$.

For $v \in V_\ell$ let $V(v)$ denote the set of those words $w \in V_m$ having v as a prefix. By induction we see that

$$\sigma(P_v) = \begin{cases} g_v & \text{if } \sigma(X_{\kappa(w)}) = 1 \text{ for all } w \in V(v), \\ 1 & \text{otherwise.} \end{cases}$$

This shows the correctness of our construction.

It remains to consider the case that $(n/C)^{1/c}$ is not an integer. Then we set $K = \lceil (n/C)^{1/c} \rceil$. It follows that $|V_{m-1}| = C \cdot K^c \geq n$, so we can fix a bijection $\kappa\colon U \to [1\,..\,n]$ for some subset $U \subseteq V_{m-1}$. We still have $|g_\varepsilon| \leq 2^{\sum_{k_i<\infty}(k_i+1)} (2^{K+1})^c \in \mathcal{O}(2^{cK}) = \mathcal{O}(2^{Dn^{1/c}})$ with D as above. This concludes the proof of Proposition 8. ◀

[1] This group can be found in the GAP small group library under the index [72, 40]. It was suggested as an example by Barrington (private communication).

▶ Remark 11. In the light of Proposition 8 it is natural to ask for a refined version of the AND weakness conjecture. A natural candidate would be to conjecture that every G-program for the n-input AND has length $2^{\Omega(n^{1/(d-1)})}$ where d is the Fitting length of G.

However, this is also wrong! Indeed, in [4, Section 2.4] Barrington, Beigel and Rudich show that the n-input AND can be computed by circuits using only MOD_m gates of depth 3 and size $2^{\mathcal{O}(n^{1/r}\log n)}$ where r is the number of different prime factors of m. Translating the circuit into a G-program yields a group G of Fitting length 3. Since there is no bound on r, we see that there is no lower bound on the exponent δ such that there are G-programs of length $2^{\mathcal{O}(n^\delta)}$ for the n-input AND in groups of Fitting length 3. While this does not yield smaller CC^0 circuits or shorter G-programs than the approach of Proposition 8 allows, it shows that the divide-and-conquer technique on which Proposition 8 relies is not always the best way for constructing small programs for AND.

In [15] it is shown that the AND function can be computed by probabilistic CC^0 circuits using only a logarithmic number of random bits, which "may be viewed as evidence contrary to the conjecture" [15]. In the light of this, we do not feel confident to judge which form of the AND-weakness conjecture might be true. The following version seems at least possible.

▶ **Conjecture 1** (AND-weakness [6]). *Let G be finite solvable. Then every G-program for the n-input* AND *has length $2^{n^{\Omega(1)}}$.*

Notice that [5, Theorem 2] (if G is AND-weak, ProgramSAT over G can be decided in quasi-polynomial time) still holds with this version of the AND-weakness conjecture.

4 Reducing C-Coloring to equations

In this section we describe the reduction of C-Coloring to EQN-SAT(G) and EQN-ID(G) in the spirit of [14, 27]. For this, we rely on the fact that G has some normal subgroups meeting some special requirements. In Section 5, we show that all sufficiently complicated finite solvable groups meet the requirements of Theorem 14.

For a normal subgroup $H \trianglelefteq G$ and $g \in G$, we define $\eta_g(H) = \left[H\,,_M\, g^G\right]$. Since H is normal, we have $\eta_g(H) \leq H$ and $\eta_g(H)$ is normal in G.

▶ **Lemma 12.** *Let $H \trianglelefteq G$ be a normal subgroup and $g \in G$. Then*

(i) $\eta_g(\eta_g(H)) = \eta_g(H)$, *and*

(ii) $\eta_{gh}(H) \leq \eta_g(H)\eta_h(H)$, *and*

(iii) $\mathrm{FitLen}(\eta_{gh}(H)) \leq \max\{\,\mathrm{FitLen}(\eta_g(H)), \mathrm{FitLen}(\eta_h(H))\,\}$.

Proof. We use the fact that M is chosen such that $[X\,,_M\, Y] = [X\,,_i\, Y]$ for all $i \geq M$ and all $X, Y \subseteq G$ with $X^G = G$ and $Y^G = Y$:

$$\eta_g(H) = \left[H\,,_M\, g^G\right] = \left[H\,,_{2M}\, g^G\right] = \left[\left[H\,,_M\, g^G\right]\,,_M\, g^G\right] = \eta_g(\eta_g(H)).$$

The second point follows with the same kind of argument:

$$\begin{aligned}\eta_{gh}(H) &= [H,\,{}_{2M}(gh)^G] \leq [H,\,{}_{2M}\langle g^G \cup h^G\rangle] \\ &= \langle [H,\,{}_{2M} g^G \cup h^G]_{\mathrm{set}}\rangle \qquad \text{(by Lemma 1)} \\ &\leq \eta_g(H)\eta_h(H).\end{aligned}$$

The last step is because any of the commutators in $[H,\,{}_{2M}g^G \cup h^G]_{\mathrm{set}}$ either contains at least M terms from g^G and, thus, is in $\eta_g(H)$ or it contains at least M terms from h^G.

The third point is an immediate consequence of the second point and Lemma 3. ◀

▶ **Lemma 13.** *Suppose that $K \trianglelefteq G$ is a normal subgroup satisfying $\eta_g(K) = K$ for some $g \in G$. Then K is inducible.*

Proof. Because $\eta_g(K) = K$ for some $g \in G$ implies that $K = [K, G]$, it follows from Lemma 4 that K is inducible. ◀

▶ **Theorem 14.** *Let G be a finite solvable group of Fitting length three and assume there are normal subgroups $K \trianglelefteq H \trianglelefteq G$ such that* $\mathrm{FitLen}(K) = 2$, *$\mathcal{U}_2 G \leq H$, and $|G/H| \geq 3$. Moreover, assume that*

- *for all $g \in G \setminus H$ we have $\eta_g(K) = K$,*
- *for all $h \in H$ we have* $\mathrm{FitLen}(\eta_h(K)) \leq 1$.

Then EQN-SAT(G) *and* EQN-ID(G) *cannot be decided in deterministic time $2^{o(\log^2 N)}$ under ETH where N is the length of the input expression. In particular,* EQN-SAT(G) *and* EQN-ID(G) *are not in* P *under ETH.*

Proof. We reduce the C-Coloring problem to EQN-SAT (resp. EQN-ID). Notice that we have a size blow-up so that a graph with n vertices and m edges is reduced to an equation of length $2^{\mathcal{O}(\sqrt{n+m})}$. For the number of colors we use $C = |G/H|$. Thus, since we assumed $|G/H| \geq 3$, under ETH C-Coloring cannot be solved in time $2^{o(n+m)}$. Hence, a $2^{o(\log^2 N)}$ time algorithm for EQN-SAT (resp. EQN-ID) would contradict ETH if N denotes the input length for EQN-SAT (resp. EQN-ID).

Let us describe how the C-Coloring problem for a given graph $\Gamma = (V, E)$ is reduced to an instance of EQN-SAT (resp. EQN-ID). We denote $V = \{ v_1, \ldots, v_n \}$. For every vertex v_i we introduce a variable X_i and we set $\mathcal{X} = \{ X_1, \ldots, X_n \}$. By fixing a bijection $|G/H| \to [1 \,..\, C]$, we obtain a correspondence between assignments $\mathcal{X} \to G$ and colorings $V \to [1 \,..\, C]$ (be aware that it is *not* one-to-one). During the construction we will also introduce a set $\mathcal{Y}$ of auxiliary variables. The idea is that an assignment $\mathcal{X} \to G$ represents a valid coloring if and only if there is an assignment to the auxiliary variables under which the equation evaluates to a non-identity element.

For each edge $\{ v_i, v_j \} \in E$, we introduce one edge gadget $X_i X_j^{-1}$ (it does not matter which one is the positive variable). Now, we group these gadgets into μ batches of μ elements each (if the number of gadgets is not a square, we duplicate some gadgets) – i.e., we choose $\mu = \lceil \sqrt{m} \rceil$. How the gadgets exactly are grouped together does not matter.

For $k \in [1 \,..\, \mu]$ and $i \in [1 \,..\, |K|]$ let $\alpha_{k,i}$ be an expression which induces K. Such an expression exists by Lemma 13. Let the variables of $\alpha_{k,i}$ be $Y_{k,i,\iota}$ for $\iota \in [1 \,..\, \nu]$ for some $\nu \in \mathbb{N}$. Moreover, we introduce more auxiliary variables $Z_{k,i,j,\ell}$ for $k \in [1 \,..\, \mu]$, $i \in [1 \,..\, |K|]$, $j \in [1 \,..\, \mu]$, and $\ell \in [1 \,..\, M]$ (recall that M is chosen such that $[H_1 \,,_M\, H_2] = [H_1 \,,_{M+1}\, H_2]$ for arbitrary normal subgroups H_1, H_2 of G) and we set

$$\mathcal{Y}'_k = \left\{ Z_{k,i,j,\ell},\ Y_{k,i,\iota} \;\middle|\; i \in [1 \,..\, |K|], j \in [1 \,..\, \mu], \ell \in [1 \,..\, M], \iota \in [1 \,..\, \nu] \right\}.$$

Let $\beta_{k,1}, \ldots, \beta_{k,\mu}$ be the gadgets of the k-th batch for some $k \in [1 \,..\, \mu]$. We define

$$\gamma_k = \prod_{i=1}^{|K|} \left[\alpha_{k,i}, \beta_{k,1}^{Z_{k,i,1,1}}, \ldots, \beta_{k,1}^{Z_{k,i,1,M}}, \ldots, \beta_{k,\mu}^{Z_{k,i,\mu,1}}, \ldots, \beta_{k,\mu}^{Z_{k,i,\mu,M}} \right]. \tag{1}$$

We do this for every batch of gadgets. Moreover, for every set of auxiliary variables $\mathcal{Y}'_k$ we add M disjoint copies, which we call $\mathcal{Y}_k^{(i)}$ for $i \in [1 \,..\, M]$. We write $\gamma_k^{(i)}$ for the copy of γ_k where the variables of $\mathcal{Y}'_k$ are substituted by the corresponding ones in $\mathcal{Y}_k^{(i)}$ (the variables $\mathcal{X}$ are shared over all $\gamma_k^{(i)}$). We set

$$\delta = \left[\gamma_1^{(1)}, \ldots, \gamma_1^{(M)}, \ldots, \gamma_\mu^{(1)}, \ldots, \gamma_\mu^{(M)} \right].$$

Finally, fix some $\tilde{h} \in K \setminus 1$ with $\tilde{h} \in [{}_{M\mu}\ K]_{\text{set}}$. Our equation is $\delta\tilde{h}^{-1}$ for the reduction of C-Coloring to EQN-SAT(G) and δ for the reduction to EQN-ID(G). It remains to show the following points:

- The length of δ is in $2^{\mathcal{O}(\sqrt{m+n})}$,
- δ can be computed in time polynomial in its length,
- $\delta = \tilde{h}$ is satisfiable if and only if Γ has a valid C-coloring, and
- $\delta = 1$ is universal if and only if Γ does not have a valid C-coloring.

For the first point observe that the length of γ_k is $\mathcal{O}(2^{M\mu})$ for all k. Thus, the length of δ is $\mathcal{O}(2^{M\mu}) \cdot \mathcal{O}(2^{M\mu}) \subseteq 2^{\mathcal{O}(\mu)} = 2^{\mathcal{O}(\sqrt{m})}$ as desired. The second point is straightforward from the construction of δ. The third and fourth point follow from the next lemma.

Here, we write $\mathcal{Y} = \bigcup_{k,i} \mathcal{Y}_k^{(i)}$. We fix a bijection $\xi : G/H \to [1\,..\,C]$. For an assignment $\sigma : \mathcal{X} \to G$, we define a corresponding coloring $\chi_\sigma : V \to [1\,..\,C]$ by $\chi_\sigma(v_i) = \xi(\sigma(X_i)H)$.

▶ **Lemma 15.** *Let $\sigma : \mathcal{X} \to G$ be an assignment. Then*

- *if χ_σ is valid, then there is an assignment $\sigma' : \mathcal{Y} \to G$ such that $(\sigma \cup \sigma')(\delta) = \tilde{h} \neq 1$,*
- *if χ_σ is* not *valid, then for all assignments $\sigma' : \mathcal{Y} \to G$ we have $(\sigma \cup \sigma')(\delta) = 1$.*

In order to see Lemma 15, we first prove another lemma:

▶ **Lemma 16.** *Let $\sigma\colon \mathcal{X} \to G$ be an assignment.*

(i) *Let $k \in [1\,..\,\mu]$. If $\sigma(\beta_{k,i}) \in G \setminus H$ for all i, then*

$$\{\, (\sigma \cup \sigma')(\gamma_k) \mid \sigma' : \mathcal{Y}'_k \to G \,\} = K,$$

Otherwise,

$$\{\, (\sigma \cup \sigma')(\gamma_k) \mid \sigma' : \mathcal{Y}'_k \to G \,\} \leq \mathcal{U}_1 K.$$

(ii) *If $\sigma(\beta_{k,i}) \in G \setminus H$ for all k and i, then there is some assignment $\sigma'\colon \mathcal{Y} \to G$ such that $(\sigma \cup \sigma')(\delta) = \tilde{h}$. Otherwise $(\sigma \cup \sigma')(\delta) = 1$ for all $\sigma'\colon \mathcal{Y} \to G$.*

Proof. By construction, we have $(\sigma \cup \sigma')(\alpha_{k,i}) \in K$ for all k and i and all assignments σ and σ'. Since K is normal, it follows that $(\sigma \cup \sigma')(\gamma_k) \in K$ for all assignments σ and σ'. Consider the case that $g_i \coloneqq \sigma(\beta_{k,i}) \in G \setminus H$ for all $i \in [1\,..\,\mu]$. By assumption, we have $K = \eta_{g_1}(K) = \eta_{g_2}(\eta_{g_1}(K)) = \cdots = \eta_{g_\mu} \ldots \eta_{g_2}(\eta_{g_1}(K)) \cdots)$. By Lemma 1, it follows that $K = \left\langle [K,\, {}_M g_1^G, \ldots,\, {}_M g_\mu^G]_{\text{set}} \right\rangle$. Since $1 \in [K,\, {}_M g_1^G, \ldots,\, {}_M g_\mu^G]_{\text{set}}$ and every element in K can be written as a product of length at most $|K|$ over any generating set, we conclude $K = \left([K,\, {}_M g_1^G, \ldots,\, {}_M g_\mu^G]_{\text{set}}\right)^{|K|}$. This is exactly the form how γ_k was defined in Equation (1) (recall that $\alpha_{k,i}$ can evaluate to every element of K). Therefore, for each $h \in K$, there is an assignment $\sigma'\colon \mathcal{Y}'_k \to G$ such that $(\sigma \cup \sigma')(\gamma_k) = h$.

On the other hand, if $g_i \coloneqq \sigma(\beta_{k,i}) \in H$ for some i, then $(\sigma \cup \sigma')(\gamma_k) \in \eta_{g_i}(K)$. Since $\text{FitLen}(\eta_{g_i}(K)) \leq 1$, we have $(\sigma \cup \sigma')(\gamma_k) \in \mathcal{U}_1 K$ by Lemma 3.

The second part of the lemma follows from the first one: if for some $\sigma'\colon \mathcal{Y} \to G$ there is a k with $(\sigma \cup \sigma')(\gamma_k^{(i)}) \in \mathcal{U}_1 K$ for all $i \in [1\,..\,M]$, then $(\sigma \cup \sigma')(\delta) \in [{}_M\ \mathcal{U}_1 K] = 1$. Finally, if $\sigma(\beta_{k,i}) \in G \setminus H$ for all k and i, then by part (i), $\left\{(\sigma \cup \sigma')(\gamma_k^{(i)}) \,\middle|\, \sigma' : \mathcal{Y}_k^{(i)} \to G\right\} = K$ for all k and i. Hence, since we chose the auxiliary variables $\mathcal{Y}_k^{(i)}$ to be all disjoint, we obtain

$$\tilde{h} \in [{}_{M\mu}\ K]_{\text{set}} \subseteq \left\{ (\sigma \cup \sigma')(\delta) \;\middle|\; \sigma' : \mathcal{Y}_k^{(i)} \to G \right\}. \qquad \blacktriangleleft$$

Proof of Lemma 15. Let χ_σ be a valid coloring. First, observe that the gadgets all evaluate to some element outside of H under σ. This is because, if there is a gadget $X_i X_j^{-1}$ that means that $\{ v_i, v_j \} \in E$ and so $\chi_\sigma(v_i) \neq \chi_\sigma(v_j)$; hence, $\sigma(X_i) \neq \sigma(X_j)$ in G/H (since ξ is a bijection). Therefore, by part (ii) of Lemma 16, it follows that δ evaluates to $\tilde{h}$ under some proper assignment for $\mathcal{Y}$.

On the other hand, if χ_σ is not a valid coloring, then there is an edge $\{ v_i, v_j \} \in E$ with $\chi_\sigma(v_i) = \chi_\sigma(v_j)$. Then we will have $\sigma(X_i)H = \sigma(X_j)H$. Hence, by Lemma 16 (ii), we obtain that $(\sigma_\chi \cup \sigma')(\delta) = 1$ in G for any $\sigma' : \mathcal{Y} \to G$. ◀

This concludes the proof of Theorem 14. ◀

5 Consequences

In this section we derive our main result Corollary A. We start again with a lemma.

▶ **Lemma 17.** *For every finite solvable, non-nilpotent group G of Fitting length d, there are proper normal subgroups $K \trianglelefteq H \lhd G$ with $\mathrm{FitLen}(K) = d - 1$ and $\mathcal{U}_{d-1}G \leq H$ such that*

- *for all $g \in G \setminus H$ we have $\eta_g(K) = K$,*
- *for all $h \in H$ we have $\mathrm{FitLen}(\eta_h(K)) < \mathrm{FitLen}(K)$.*

The construction for Lemma 17 resembles the ones in Lemmas 5 and 6 of [27]. However, while in [27] a minimal normal subgroup N of a quotient G/K is constructed such that r_g with $r_g(x) = [x, g]$ is an automorphism of N (and N is abelian), in our case this is not enough since we need to apply commutator constructions to our analog of N in the spirit of the divide-and-conquer approach of Proposition 8. While our construction is rather easier than [27], it cannot cope with the case that $G/\mathcal{U}_{d-1}G$ is a 2-group.

Proof. Let $g_1 \in G \setminus \mathcal{U}_{d-1}G$ where d is the Fitting length of G. We construct a sequence of normal subgroups $K_1, K_2, \ldots$ of G as follows: we set $K_1 = \eta_{g_1}(G)$. By Lemma 2, $K_1 = \gamma_\infty \langle g_1^G \rangle$, so it has Fitting length $d - 1$.

Now, while there is some $g_i \in G$ such that $\eta_{g_i}(K_{i-1}) < K_{i-1}$ and $\mathrm{FitLen}(\eta_{g_i}(K_{i-1})) = \mathrm{FitLen}(K_{i-1})$, we set $K_i = \eta_{g_i}(K_{i-1})$ and continue. Since K_i is a proper subgroup of K_{i-1}, this process eventually terminates. We call the last term K. We claim that K satisfies the statement of Lemma 17. By construction for every $g \in G$ one of the two cases

- $\eta_g(K) = K$ or
- $\mathrm{FitLen}(\eta_g(K)) < \mathrm{FitLen}(K)$

applies. Moreover, since $K = \eta_g(K')$ for some $K' \leq G$ and some $g \in G$, we have $K = \eta_g(K') = \eta_g(\eta_g(K')) = \eta_g(K)$ by Lemma 12 (i). By Lemma 12 (iii), the elements $\{ h \in G \mid \mathrm{FitLen}(\eta_h(K)) < \mathrm{FitLen}(K) \}$ form a subgroup H of G. Clearly H is normal (by the definition of η_h) and $\mathcal{U}_{d-1}G \leq H$ because $\mathrm{FitLen}([K, {}_M\, \mathcal{U}_{d-1}G]) = \mathrm{FitLen}(K) - 1$. Since there is some $g \in G$ with $K = \eta_g(K)$, we have $H \neq G$. ◀

Be aware that K depends on the order the g_i were chosen. Indeed, if G is a direct product of two groups G_1 and G_2 of equal Fitting length, then K will either be contained in G_1 or in G_2 – in which factor depends on the choice of the g_i.

▶ **Theorem 18** (Corollary A). *Let G be a finite solvable group meeting one of the following conditions:*

(i) $\mathrm{FitLen}(G) = 3$ *and $|G/\mathcal{U}_2G|$ has a prime divisor 3 or greater (i.e., $G/\mathcal{U}_2G$ is not a 2-group),*

(ii) $\mathrm{FitLen}(G) \geq 4$.

Then EQN-SAT(G) *and* EQN-ID(G) *cannot be decided in deterministic time* $2^{o(\log^2 N)}$ *under ETH. In particular,* EQN-SAT(G) *and* EQN-ID(G) *are not in* P *under ETH.*

Proof. Consider the case that G has Fitting length 3 and $|G/\mathcal{U}_2G|$ has a prime divisor 3 or greater. Let 2^ν for some $\nu \in \mathbb{N}$ be the greatest power of two dividing $|G/\mathcal{U}_2G|$. Then, the subgroup $\widetilde{G}$ generated by all 2^ν-th powers is normal and it is not contained in $\mathcal{U}_2G$. Therefore, by Lemma 3 it has Fitting length 3 as well. Also, by Lemma 3, we know that $\mathcal{U}_2\widetilde{G} = \widetilde{G} \cap \mathcal{U}_2G$. Hence, $\widetilde{G}/\mathcal{U}_2\widetilde{G}$ is a subgroup of $G/\mathcal{U}_2G$. Moreover, since $\widetilde{G}$ is generated by 2^ν-th powers, the generators of $\widetilde{G}$ have odd order in $\widetilde{G}/\mathcal{U}_2\widetilde{G}$. Since $\widetilde{G}/\mathcal{U}_2\widetilde{G}$ is nilpotent, it follows that $|\widetilde{G}/\mathcal{U}_2\widetilde{G}|$ is odd (recall that a nilpotent group is a direct product of p-groups).

Since $\widetilde{G}$ is inducible in G, by Lemma 6, it suffices to show that $\widetilde{G}$ satisfies the requirements of Theorem 14. For this, we use Lemma 17, which gives us normal subgroups $K \trianglelefteq H \lhd \widetilde{G}$ with $\mathcal{U}_2\widetilde{G} \leq H$, $\mathrm{FitLen}(K) = 2$ and such that for all $g \in \widetilde{G} \setminus H$ we have $\eta_g(K) = K$, and for all $h \in H$ we have $\mathrm{FitLen}(\eta_h(K)) \leq 1$.

It only remains to show that $|\widetilde{G}/H| \geq 3$. Nevertheless, since $H \neq \widetilde{G}$ and $|\widetilde{G}/H|$ is odd, this holds trivially. Thus, both EQN-SAT(G) and EQN-ID(G) are not in P under ETH if G has Fitting length 3 and $|G/\mathcal{U}_2G|$ a prime divisor 3 or greater.

The second case can be reduced to the first case as follows: Assume that G has Fitting length $d \geq 4$. If $|G/\mathcal{U}_{d-1}G|$ has a prime factor 3 or greater, we can apply the Fitting length 3 case to $G/\mathcal{L}_3G$ for EQN-SAT and to $G/\mathcal{U}_{d-3}G$ for EQN-ID. By Lemma 4 and Lemma 6 this implies the corollary for EQN-SAT. For EQN-ID, the statement follows form Lemma 5 and Lemma 7.

On the other hand, if $|G/\mathcal{U}_{d-1}G| = 2^\nu$ for some $\nu \geq 1$, as in the first case, we consider the subgroup $\widetilde{G}$ generated by all 2^ν-th powers. Then the index of $\widetilde{G}$ in G is again a power of two (since the order of every element in $G/\widetilde{G}$ is a power of two). Moreover, $\widetilde{G} \leq \mathcal{U}_{d-1}G$ and, by Lemma 3, we have

$$\widetilde{G}/\mathcal{U}_{d-2}\widetilde{G} = \widetilde{G}/(\mathcal{U}_{d-2}G \cap \widetilde{G}) \cong (\widetilde{G} \cdot \mathcal{U}_{d-2}G)/\mathcal{U}_{d-2}G \leq \mathcal{U}_{d-1}G/\mathcal{U}_{d-2}G.$$

Now, $|\mathcal{U}_{d-1}G/\mathcal{U}_{d-2}G|$ cannot be a power of two because, otherwise, $G/\mathcal{U}_{d-2}G$ would be a 2-group and, thus, nilpotent – contradicting the fact that the upper Fitting series is a shortest Fitting series. Since the index of $\widetilde{G}$ in $\mathcal{U}_{d-1}G$ is a power of two, we see that $\widetilde{G} \not\subseteq \mathcal{U}_{d-2}G$ and that the index of $\mathcal{U}_{d-2}\widetilde{G}$ in $\widetilde{G}$ has a prime factor other than 2. Therefore, we can apply the Fitting length 3 case to $\widetilde{G}/\mathcal{L}_3\widetilde{G}$ (resp. $\widetilde{G}/\mathcal{U}_{d-3}\widetilde{G}$). ◀

Consequences for ProgramSAT. It is well-known that for finite groups EQN-SAT $\leq_{\mathrm{m}}^{\mathsf{AC}^0}$ ProgramSAT [5, Lem. 1] (while not explicitly stated, it is clear that the reduction described there is an AC^0-reduction). Thus, by Theorem 14, ProgramSAT is not in P under ETH if G is of Fitting length at least 4 or G is of Fitting length 3 and $G/\mathcal{U}_2G$ is not a 2-group.

Small groups for which Theorem 18 gives a lower bound. In [17] lists of groups are given where the complexity of EQN-SAT and EQN-ID is unknown. The paper refers to a more comprehensive list available on the author's website `http://math.unideb.hu/horvath-gabor/research.html`. We downloaded the lists of groups and ran tests in GAP for which of these groups Theorem 18 provides lower bounds. In the list with unknown complexity for EQN-ID there are 2331 groups of order less than 768 out of which 1559 are of Fitting length three or greater. Theorem 18 applies to 22 of them: 3 groups of Fitting length 4 and 19 groups G of Fitting length 2 where $G/\mathcal{U}_2G$ is not a 2-group. A list of the groups for which we could prove lower bounds can be found in Table 1.

Table 1 Groups up to order 767 for which Theorem 18 gives lower bounds.

Index in Small Groups Library	Fitting length	GAP Structure description
[168, 43]	3	(C2 x C2 x C2) : (C7 : C3)
[216, 153]	3	((C3 x C3) : Q8) : C3
[324, 160]	3	((C3 x C3 x C3) : (C2 x C2)) : C3
[336, 210]	3	C2 x ((C2 x C2 x C2) : (C7 : C3))
[432, 734]	4	(((C3 x C3) : Q8) : C3) : C2
[432, 735]	3	C2 x (((C3 x C3) : Q8) : C3)
[504, 52]	3	(C2 x C2 x C2) : (C7 : C9)
[504, 158]	3	C3 x ((C2 x C2 x C2) : (C7 : C3))
[600, 150]	3	(C5 x C5) : SL(2,3)
[648, 531]	3	C3 . (((C3 x C3) : Q8) : C3) = (((C3 x C3) : C3) : Q8) . C3
[648, 532]	3	(((C3 x C3) : C3) : Q8) : C3
[648, 533]	3	(((C3 x C3) : C3) : Q8) : C3
[648, 534]	3	((C3 x C3) : Q8) : C9
[648, 641]	3	((C3 x C3 x C3) : Q8) : C3
[648, 702]	3	C3 x (((C3 x C3) : Q8) : C3)
[648, 703]	4	(((C3 x C3 x C3) : (C2 x C2)) : C3) : C2
[648, 704]	4	(((C3 x C3 x C3) : (C2 x C2)) : C3) : C2
[648, 705]	3	(S3 x S3 x S3) : C3
[648, 706]	3	C2 x (((C3 x C3 x C3) : (C2 x C2)) : C3)
[672, 1049]	3	C4 x ((C2 x C2 x C2) : (C7 : C3))
[672, 1256]	3	C2 x C2 x ((C2 x C2 x C2) : (C7 : C3))
[672, 1257]	3	(C2 x C2 x C2 x C2 x C2) : (C7 : C3)

5.1 Equations in finite semigroups

For a semigroup S, the problems EQN-SAT(S) and EQN-ID(S) both receive two expressions as input. The questions is whether the two expressions evaluate to the same element under some (resp. all) assignments. For semigroups R, S we say that R *divides* S if R is a quotient of a subsemigroup of S. The following lemmas are straightforward to prove using basic semigroup theory. For the proofs, we need Green's relations $\mathcal{H}$ and $\mathcal{J}$. For a definition, we refer to [31, Appendix A]. For a semigroup S we write S^1 for S with an identity adjoined if there is none.

▶ **Lemma 19.** *Let G be a maximal subgroup of a finite semigroup S. Then* EQN-SAT(G) $\leq_{\mathrm{m}}^{\mathsf{AC}^0}$ EQN-SAT(S).

Proof. Let $e \in G$ denote the identity of G. Clearly, $G = eGe \leq eSe$ and eSe is a submonoid of S with identity e. The reduction simply replaces every variable X by eXe (and likewise for constants). Let $\tilde{\alpha}$ denote the equation we obtain from an input equation α this way. Now the question is whether $\tilde{\alpha} = e$ in S.

Clearly, if α has a solution in G, the resulting equation $\tilde{\alpha}$ will have a solution in S. On the other hand, if $\tilde{\alpha}$ has a solution in S, we obtain a solution of $\alpha = e$ in S where every variable takes values in eSe.

Assume we have $\sigma(X) = x \notin G$ for a satisfying assignment σ and some variable X of α. Since $\sigma(\alpha) = e$, we have that e is in the two-sided ideal S^1xS^1 generated by $x = exe$. By point 2. of [31, Exercise A.2.2] it follows that $x \in H_e = G$ where H_e denotes the $\mathcal{H}$-class of e under Green's relations (for a definition, we refer to [31]) and G agrees with H_e because G is a maximal subgroup. ◀

▶ **Lemma 20.** *If a group G divides a semigroup S, then G divides already one of the maximal subgroups (i.e., regular $\mathcal{H}$-classes) of S.*

Proof. Let $U \leq S$ a subsemigroup and $\varphi : U \to G$ a surjective semigroup homomorphism. Pick some arbitrary element $s \in U$ and let $e = s^\omega$ be the idempotent generated by s. Clearly, we have $\varphi(e) = 1$. Now, the subsemigroup $eUe \leq U$ still maps surjectively onto G under φ: by assumption for every $g \in G$ there is some $u_g \in U$ with $\varphi(u_g) = g$; hence, $g = 1g1 = \varphi(e)\varphi(u_g)\varphi(e) \in \varphi(eUe)$.

If eUe is not contained in a maximal subgroup, then by point 2. of [31, Exercise A.2.2], there is some $t \in eUe$ which is not $\mathcal{J}$-equivalent to e. Now, we can repeat the above process starting with t. This will decrease the size of U, so it eventually terminates. ◀

▶ **Corollary 21.** *Let S be a finite semigroup and G a group dividing S. If* $\mathrm{FitLen}(G) \geq 4$ *or* $\mathrm{FitLen}(G) = 3$ *and $G/\mathcal{U}_2G$ is not a 2-group, then* EQN-SAT(S) *is not in* P *under ETH.*

Proof. If G with $\mathrm{FitLen}(G) \geq 4$ or $\mathrm{FitLen}(G) = 3$ and $G/\mathcal{U}_2G$ divides S, then it follows from Lemma 20 that there is a group $\widetilde{G}$ with the same properties and which is a maximal subgroup of S. Hence, the statement follows from Lemma 19. ◀

[2, Theorem 1] states that identity checking over $\widetilde{G}$ reduces to identity checking over S where $\widetilde{G}$ is the direct product of all maximal subgroups of S. However, be aware that in this context the identity checking problem does not allow constants. Since the proof of Theorem 14 essentially relies on the fact that the subgroup K is inducible and this can be only shown using constants, this does not allow us to show hardness of EQN-ID(S).

6 Conclusion

We have shown that assuming the exponential time hypothesis there are solvable groups with equation satisfiability problem not decidable in polynomial time. Thus, under standard assumptions from complexity theory this means a negative answer to [9, Problem 1] (also conjectured in [16]). Theorem 18 yields a quasipolynomial time lower bound under ETH. Thus, a natural weakening of [9, Problem 1] is as follows:

▶ **Conjecture 2.** *If G is a finite solvable group, then* EQN-SAT(G) *and* EQN-ID(G) *are decidable in quasipolynomial time.*

Notice that a quasipolynomial time algorithm for EQN-SAT(G) is also conjectured in [14] if G is AND-weak.

Theorem 18 proves lower bounds on EQN-SAT and EQN-ID for all sufficiently complicated finite solvable groups. Possible further research might attack the question to which other groups of Fitting length three or even two our lower bounds might be extended.

References

1 Scott Aaronson, Russell Impagliazzo, and Dana Moshkovitz. AM with multiple merlins. In *IEEE 29th Conference on Computational Complexity, CCC 2014, Vancouver, BC, Canada, June 11-13, 2014*, pages 44–55. IEEE Computer Society, 2014. doi:10.1109/CCC.2014.13.

2 Jorge Almeida, M. V. Volkov, and S. V. Goldberg. Complexity of the identity checking problem for finite semigroups. *Journal of Mathematical Sciences*, 158(5):605–614, 2009. doi:10.1007/s10958-009-9397-z.

3 David A. Mix Barrington. Width-3 permutation branching programs. Technical Report TM-293, MIT Laboratory for Computer Science, 1985.

4 David A. Mix Barrington, Richard Beigel, and Steven Rudich. Representing Boolean functions as polynomials modulo composite numbers. *Computational Complexity*, 4:367–382, 1994. doi:10.1007/BF01263424.

5 David A. Mix Barrington, Pierre McKenzie, Cristopher Moore, Pascal Tesson, and Denis Thérien. Equation satisfiability and program satisfiability for finite monoids. In *Mathematical Foundations of Computer Science 2000, 25th International Symposium, MFCS 2000, Proceedings*, volume 1893 of *Lecture Notes in Computer Science*, pages 172–181. Springer, 2000. doi:10.1007/3-540-44612-5_13.

6 David A. Mix Barrington, Howard Straubing, and Denis Thérien. Non-uniform automata over groups. *Inf. Comput.*, 89(2):109–132, 1990. doi:10.1016/0890-5401(90)90007-5.

7 Mark Braverman, Young Kun-Ko, Aviad Rubinstein, and Omri Weinstein. ETH hardness for densest-k-subgraph with perfect completeness. In Philip N. Klein, editor, *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2017, Barcelona, Spain, Hotel Porta Fira, January 16-19*, pages 1326–1341. SIAM, 2017. doi:10.1137/1.9781611974782.86.

8 Mark Braverman, Young Kun-Ko, and Omri Weinstein. Approximating the best nash equilibrium in $n^{o(\log n)}$-time breaks the exponential time hypothesis. In Piotr Indyk, editor, *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2015, San Diego, CA, USA, January 4-6, 2015*, pages 970–982. SIAM, 2015. doi:10.1137/1.9781611973730.66.

9 Stanley Burris and J. Lawrence. Results on the equivalence problem for finite groups. *Algebra Universalis*, 52(4):495–500 (2005), 2004. doi:10.1007/s00012-004-1895-8.

10 Marek Cygan, Fedor V. Fomin, Lukasz Kowalik, Daniel Lokshtanov, Dániel Marx, Marcin Pilipczuk, Michal Pilipczuk, and Saket Saurabh. *Parameterized Algorithms*. Springer, 2015. doi:10.1007/978-3-319-21275-3.

11 Volker Diekert and Murray Elder. Solutions of twisted word equations, EDT0L languages, and context-free groups. In *ICALP 2017, Proceedings*, volume 80 of *LIPIcs*, pages 96:1–96:14, Dagstuhl, Germany, 2017. URL: http://drops.dagstuhl.de/opus/volltexte/2017/7397, doi:10.4230/LIPIcs.ICALP.2017.96.

12 Attila Földvári. The complexity of the equation solvability problem over semipattern groups. *IJAC*, 27(2):259, 2017. doi:10.1142/S0218196717500126.

13 Albert Garreta, Alexei Miasnikov, and Denis Ovchinnikov. Diophantine problems in solvable groups. *Bulletin of Mathematical Sciences*, 01 2020. doi:10.1142/S1664360720500058.

14 Mikael Goldmann and Alexander Russell. The complexity of solving equations over finite groups. *Inf. Comput.*, 178(1):253–262, 2002. doi:10.1006/inco.2002.3173.

15 Kristoffer Arnsfelt Hansen and Michal Koucký. A new characterization of ACC^0 and probabilistic CC^0. *Computational Complexity*, 19(2):211–234, 2010. doi:10.1007/s00037-010-0287-z.

16 Gábor Horváth. The complexity of the equivalence and equation solvability problems over nilpotent rings and groups. *Algebra Universalis*, 66(4):391–403, 2011. doi:10.1007/s00012-011-0163-y.

17 Gábor Horváth. The complexity of the equivalence and equation solvability problems over meta-Abelian groups. *J. Algebra*, 433:208–230, 2015. doi:10.1016/j.jalgebra.2015.03.015.

18 Gábor Horváth and Csaba Szabó. The extended equivalence and equation solvability problems for groups. *Discrete Math. Theor. Comput. Sci.*, 13(4):23–32, 2011.

19 Gábor Horváth and Csaba Szabó. Equivalence and equation solvability problems for the alternating group $\mathbf{A}_4$. *J. Pure Appl. Algebra*, 216(10):2170–2176, 2012. doi:10.1016/j.jpaa.2012.02.007.

20 Gábor Horváth and Csaba A. Szabó. The complexity of checking identities over finite groups. *IJAC*, 16(5):931–940, 2006. doi:10.1142/S0218196706003256.

21 Russell Impagliazzo, Ramamohan Paturi, and Francis Zane. Which problems have strongly exponential complexity? *J. Comput. Syst. Sci.*, 63(4):512–530, 2001. doi:10.1006/jcss.2001.1774.

22 Marcel Jackson and Ralph McKenzie. Interpreting graph colorability in finite semigroups. *IJAC*, 16(1):119–140, 2006. doi:10.1142/S0218196706002846.

23 Andrzej Kisielewicz. Complexity of semigroup identity checking. *IJAC*, 14(4):455–464, 2004. doi:10.1142/S0218196704001840.

24 Ondrej Klíma, Pascal Tesson, and Denis Thérien. Dichotomies in the complexity of solving systems of equations over finite semigroups. *Theory Comput. Syst.*, 40(3):263–297, 2007. doi:10.1007/s00224-005-1279-2.

25 Ondřej Klíma. Complexity issues of checking identities in finite monoids. *Semigroup Forum*, 79(3):435–444, 2009. doi:10.1007/s00233-009-9180-y.

26 Michael Kompatscher. CC-circuits and the expressive power of nilpotent algebras. *CoRR*, abs/1911.01479, 2019. URL: http://arxiv.org/abs/1911.01479, arXiv:1911.01479.

27 Michael Kompatscher. Notes on extended equation solvability and identity checking for groups. *Acta Math. Hungar.*, 159(1):246–256, 2019. doi:10.1007/s10474-019-00924-7.

28 Markus Lohrey and Géraud Sénizergues. Theories of HNN-extensions and amalgamated products. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *ICALP*, volume 4052 of *Lecture Notes in Computer Science*, pages 504–515. Springer, 2006. doi:10.1007/11787006_43.

29 Gennadiĭ Semyonovich Makanin. The problem of solvability of equations in a free semigroup. *Math. Sbornik*, 103:147–236, 1977. English transl. in Math. USSR Sbornik 32 (1977).

30 Pierre McKenzie, Pierre Péladeau, and Denis Thérien. NC^1: The automata-theoretic viewpoint. *Computational Complexity*, 1:330–359, 1991. doi:10.1007/BF01212963.

31 John L. Rhodes and Benjamin Steinberg. *The* q*-theory of finite semigroups.* Springer Monographs in Mathematics. Springer, 2009.

32 Derek J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996. doi:10.1007/978-1-4419-8594-1.

33 Vitaly Roman'kov. Equations in free metabelian groups. *Siberian Mathematical Journal*, 20, 05 1979. doi:10.1007/BF00969959.

34 Steve Seif. The Perkins semigroup has co-NP-complete term-equivalence problem. *Internat. J. Algebra Comput.*, 15(2):317–326, 2005. doi:10.1142/S0218196705002293.

35 Steve Seif and Csaba Szabó. Computational complexity of checking identities in 0-simple semigroups and matrix semigroups over finite fields. *Semigroup Forum*, 72(2):207–222, 2006. doi:10.1007/s00233-005-0510-4.

36 Csaba Szabó and Vera Vértesi. The complexity of checking identities for finite matrix rings. *Algebra Universalis*, 51(4):439–445, 2004. doi:10.1007/s00012-004-1873-1.