The Complexity of Solving Equations over Finite Groups

Mikael Goldmann
Numerical Analysis and Computer Science
Royal Institute of Technology
Stockholm, Sweden
migo@nada.kth.se

Alexander Russell*
Computer Science Division
University of California, Berkeley
Berkeley, CA 94720
acr@cs.berkeley.edu

Abstract

We study the computational complexity of solving systems of equations over a finite group. An equation *over a group G is an expression of the form*

$$w_1 \cdot w_2 \cdot \cdots \cdot w_k = \mathbf{id}$$

where each w_i is either a variable, an inverted variable, or group constant and **id** *is the identity element of G. A solution to such an equation is an assignment of the variables (to values in G) which realizes the equality. A* system *of equations is a collection of such equations; a solution is then an assignment which simultaneously realizes each equation.*

We demonstrate that the problem of determining if a (single) equation has a solution is NP*-complete for all non-solvable groups G. For nilpotent groups, this same problem is shown to be in* P*. The analogous problem for systems of such equations is shown to be* NP*-complete if G is non-Abelian, and in* P *otherwise. Finally, we observe some connections between these languages and the theory of non-uniform automata.*

1. Introduction

Many natural computational problems can be viewed as problems about the solvability of certain equations over a finite group. One immediately thinks of QUADRATIC RESIDUES or, if considering the problem of actually producing a solution, the discrete log problem. In both cases, the size of the group in question grows with the input length and, in fact, a complete enough understanding of the group involved effectively solves the problem. (For QUADRATIC RESIDUES in $\mathbb{Z}_n^*$, for example, with a decomposition of $\mathbb{Z}_n^*$ into cyclic groups (which is enough to factor n), the problem can be solved in RP.) Recent work of Håstad [4] on the non-approximability of k-SAT has focused on the scenario where the group is *fixed*; the input consists only of the equations to be solved. We adopt this second perspective, studying conditions on the group G which allow the problem of solving equations over G to be neatly classified.

An *expression* over a group G is given by a function $\ell : G^s \to G$, where $\ell : (v_1, \ldots, v_s) \mapsto w_1 w_2 \ldots w_t$, each w_i being a constant from the group, a variable v_i, or an inverted variable v_i^{-1}. Observe that a given variable may occur many times. An *equation* over G is simply an equality $\ell(v_1, \ldots, v_s) = \gamma$ for some constant γ in G.

Naturally, a *system* of equations over a group G is a collection of expressions $\{\ell_i \,|\, i \in [n]\}$ (assumed of the same arity, s) and group constants $\{\gamma_i \,|\, i \in [n]\}$. (Here $[n]$ denotes the set $\{1, \ldots, n\}$.) A *solution* to such a system is a vector of group constants $\vec{a} = (a_1, \ldots, a_s)$ for which $\ell_i(a_1, \ldots, a_s) = \gamma_i$ for each $i \in [n]$.

For example, the system of equations

$$\langle x\gamma x^{-1}\gamma^{-1} = \mathbf{id} \rangle_{\gamma \in G},$$

where **id** is the group identity element, is solved by any x in the center of G.

For a finite group G, we shall focus on the following two languages:

$$\mathrm{EQN}_G \stackrel{\text{def}}{=} \{\langle \ell, \gamma \rangle \,|\, \exists \vec{a} \in G^s, \ell(\vec{a}) = \gamma\}, \text{ and}$$

$$\mathrm{EQN}_G^* \stackrel{\text{def}}{=} \left\{ \left\langle (\ell_1, \gamma_1), \ldots, (\ell_n, \gamma_n) \right\rangle \,\middle|\, \begin{array}{l} \exists \vec{a} \in G^s, \\ \forall i, \ell_i(\vec{a}) = \gamma_i \end{array} \right\}.$$

When G is Abelian, it is not hard to show that EQN_G^*, and hence EQN_G, can be recognized in polynomial time (see §2.1, below). For any non-Abelian group G, EQN_G^* is NP-complete, making a tidy boundary; this is the subject of §2.

The situation for a single equation (that is, EQN_G) seems to be more complicated. §3.1 is devoted to demonstrating that for non-solvable groups G, EQN_G is NP-complete.

*Supported by NSF NYI Grant No. CCR-9457799 and a David and Lucile Packard Fellowship for Science and Engineering.

Curiously, applying machinery from the theory of non-uniform automata, it is shown in §3.2 that for nilpotent groups G, EQN_G can be recognized in polynomial time. This gap between nilpotent groups and non-solvable groups seems to be the same as that which manifests itself in the study of non-uniform automata (cf. [2]) and the fine structure of NC^1.

2. Systems of Equations over Finite Groups

We begin by studying the complexity of solving *systems* of equations. For completeness, we recall that over an Abelian group, systems can be solved in polynomial time.

2.1. Abelian Groups

Theorem 1. *For G a finite Abelian group,* $\mathrm{EQN}^*_G \in \mathrm{P}$.

Proof. Since G is Abelian, we may write

$$G \cong \mathbb{Z}/q_1 \oplus \cdots \oplus \mathbb{Z}/q_k,$$

(see, for example, [5, II.§7]). With this decomposition, a system of equations over G may be viewed as k independent systems of equations, each over a cyclic group $\mathbb{Z}/q_i$. The original system has a solution exactly when each of these k systems has a solution so that we may assume, without loss of generality, that G is cyclic. The group operation in an Abelian group we write additively. Then any expression $\ell : (v_1, \ldots, v_s) \mapsto w_1 w_2 \ldots w_t$ may be expressed

$$\ell : (v_1, \ldots, v_s) \mapsto c_1 v_1 + \cdots + c_s v_s + \delta$$

where each $c_i \in \mathbb{Z}$ and $\delta \in G$. Collecting constants, a system of equations (ℓ_i, γ_i) may be rewritten so that $\ell_i(v_1, \ldots, v_s) \mapsto c_{i1} v_1 + \cdots + c_{is} v_s$. For convenience, we collect these c_{ij} together into a matrix C and may express our problem as

$$\exists \vec{a}, C\vec{a} = \vec{\gamma}.$$

It is easy to check that the existence of a solution to such a system is invariant under elementary row and column operations. (An *elementary* row (column) operation consists of adding a multiple of one row (column) to *another* row (column).) Elementary row operations, of course, have a corresponding result on the target values γ_i. With such operations the matrix C can be diagonalized in polynomial time, and the existence of a solution can then be determined by inspection. □

2.2. Non-Abelian Groups

We shall say that a group G is *expressive* if EQN^*_G is NP-complete. Our goal, in this section, is to prove the following:

Theorem 2. *Every finite non-Abelian group is expressive.*

2.2.1. A Special Case: S_3

Before presenting the proof of Theorem 2, we consider the special case of S_3, which involves some of the ideas in the general argument.

Theorem 3. *Let S_3 be the group of permutations of three elements.* $\mathrm{EQN}^*_{\mathrm{S}_3}$ *is expressive.*

Proof. The proof is a reduction from GRAPH 6-COLORING to $\mathrm{EQN}^*_{\mathrm{S}_3}$.

With each vertex i in G we associate a variable x_i; an assignment of group elements to these variables will correspond to a coloring of G.

For each edge (i, j) in G we introduce a variable $z_{i,j}$ and the equation

$$z_{i,j} x_i x_j^{-1} z_{i,j}^{-1} x_j x_i^{-1} = (1\,2\,3).$$

Note that if for any edge (i, j), $x_i = x_j$ then the corresponding equation cannot be satisfied as the left hand side will be the identity of S_3 regardless of $z_{i,j}$. Evidently, a solution to the system of equations corresponds to a legal 6-coloring of the graph.

It remains to show that if G is 6-colorable, then the system of equations has a solution. Assume that there is a legal 6-coloring of the graph and let each color correspond to an element of S_3. Assign x_v the color of v; since the coloring is legal, for every edge (i, j) the product $x_i x_j^{-1}$ is not the identity. It is now easy to check that the equation

$$z_{i,j} \alpha z_{i,j}^{-1} \alpha^{-1} = (1\,2\,3) \tag{1}$$

has a solution if and only if α is not the identity. □

2.2.2. A Proof of the General Result

As in the case of $\mathrm{EQN}_{\mathrm{S}_3}$, we use a reduction from GRAPH k-COLORING (for some $k \geq 3$) to prove Theorem 2. Developing a direct analogue of the proof of Theorem 3 in the general case seems difficult as there is no immediate method for distinguishing elements in center of G from each other. (Recall that the *center* of a group G is the subgroup $Z(G) = \{g \in G \mid \forall h \in G, gh = hg\}$.) Indeed, we shall use the cosets of $Z(G)$ to color the elements. We begin with some definitions.

Definition 1. *A subset S of a group G is called* inducible *if there is an expression $\ell : G^s \to G$ so that*

$$S = \mathbf{im}\, \ell = \{g \mid \exists \vec{a} \in G^s, \ell(\vec{a}) = g\}.$$

Our proof of Theorem 2 proceeds by induction on the size of the group. In preparation for this, we observe that the property of expressivity respects subgroup and group quotient structure:

Lemma 4. *Let H be an inducible subgroup of G.*

1. *If H is expressive, then G is expressive.*
2. *If H is normal in G and G/H is expressive, then G is expressive.*

Proof. Part 1 is easy. Part 2 is done by rewriting an equation $\mathcal{E}$ of form

$$w_1 H \cdot w_2 H \cdot \cdots \cdot w_k H = \gamma H$$

(where each w_i is a variable or constant), first as

$$\exists h \in H : w_1 \cdot w_2 \cdot \cdots \cdot w_k \cdot h = \gamma$$

and finally as

$$w_1 \cdot w_2 \cdot \cdots \cdot w_k \cdot \ell_H = \gamma$$

where ℓ_H is an expression that induces H. □

Definition 2. *A commutator of G is an element of form $\alpha\beta\alpha^{-1}\beta^{-1}$, denoted $[\alpha, \beta]$, for some $\alpha, \beta \in G$. For two subsets A and B of G, we extend this notation, defining*

$$[A, B] \stackrel{def}{=} \left\{ \alpha\beta\alpha^{-1}\beta^{-1} \,\middle|\, \alpha \in A, \beta \in B \right\}.$$

*Then the commutator subgroup G' of a group G is the smallest subgroup containing $[G, G]$. In general, for subsets A and B, the (A, B)-*commutator subgroup*, denoted (A, B), is the smallest subgroup containing $[A, B]$.*

It is worth noting that G is Abelian if and only if $G' = \{\mathbf{id}\}$. The commutator subgroup is always normal and, in fact, the group G/G' is the largest Abelian quotient of the group G. In this sense, the commutator subgroup can be seen as a measure of the non-commutativity of the group.

Lemma 5. *G' is inducible.*

Proof. Any element of G' can be formed by a finite product of elements in $[G, G]$. Now $[\alpha, \alpha] = e_G$, so that there is a constant $d_G \geq 1$ for which

$$G' = \{[\alpha_1, \beta_1] \cdots [\alpha_{d_G}, \beta_{d_G}] \mid \alpha_i, \beta_i \in G\},$$

and this gives an easy recipe for inducing G'. □

The proof of Theorem 2 focuses on subgroups of G' of form $(\{\gamma\}, G)$ for an element $\gamma \notin Z(G)$. Such subgroups are inducible and, in fact, normal:

Lemma 6. *For every $\gamma \in G$,*

1. *$(\{\gamma\}, G) \subseteq G'$,*
2. *$(\{\gamma\}, G)$ is inducible, and*
3. *$(\{\gamma\}, G)$ is normal in G.*

Proof. Part 1 is immediate. Observing that for any $\gamma \in G$, $\gamma^{-1} = \gamma^k$ for some $k \geq 1$, the proof of part 2 is analogous to the proof that G' is inducible. In preparation for the proof of part 3, observe the equality:

$$\alpha[\gamma, \beta]\alpha^{-1} = [\gamma, \alpha]^{-1}[\gamma, \alpha\beta]. \tag{2}$$

Then, any element $\delta \in (\{\gamma\}, G)$ can be written $\delta = \prod_{i=1}^{t} [\gamma, \beta_i]$ and for any $\alpha \in G$ we have

$$\begin{aligned} \alpha\delta\alpha^{-1} &= \prod_{i=1}^{t} \alpha[\gamma, \beta_i]\alpha^{-1} \\ &= \prod_{i=1}^{t} [\gamma, \alpha]^{-1}[\gamma, \alpha\beta_i] \in (\{\gamma\}, G) \end{aligned}$$

by equation (2) above. Hence, $(\{\gamma\}, G)$ is normal in G. □

Definition 3. *We call G* commutator simple *if for all $\gamma \notin Z(G)$ we have $G' = (\{\gamma\}, G)$.*

Next we establish that if G is non-Abelian and commutator simple, then G is expressive.

Lemma 7. *Let G be a finite and non-Abelian commutator simple group. Then G is expressive.*

Proof. It is easy to show that if G is non-Abelian, then the quotient group $G/Z(G)$ cannot be cyclic, and thus contains at least 4 elements. Let $k = |G/Z(G)|$. We reduce GRAPH k-COLORING to EQN$^*_G$. An instance (V, E) of GRAPH k-COLORING is mapped to a system of equations in the following way. We shall have a variable x_v for every $v \in V$. Intuitively, the coset of $Z(G)$ in which x_v lies is the "color" of v. Recall that $x_u x_v^{-1} \in Z(G)$ iff x_u and x_v lie in the same coset of $Z(G)$. Now, we would like to include, for each edge, an equation satisfied only when $x_u x_v^{-1} \notin Z(G)$ (that is, when they lie in different cosets). Fortunately, when G is commutator simple, there is a convenient property satisfied by elements outside of the center: if $\gamma \notin Z(G)$, then every element $\alpha \in G'$ can be written as a product

$$\alpha = \prod_{i=1}^{d_G} [\gamma, \beta_i],$$

for some $\beta_i \in G$, where d_G is a constant depending only on G. So fix once and for all an element $\kappa \in G' \setminus \{\mathbf{id}\}$. For each edge $(u, v) \in E$, we include an equation of form

$$\kappa = [x_u x_v^{-1}, s_1] \cdots [x_u x_v^{-1}, s_{d_G}],$$

for (new) variables s_i. It is then easy to see that the graph has a legal k-coloring iff this system has a solution. □

Combining the above Lemma with induction on group order proves Theorem 2.

Proof of Theorem 2. The proof proceeds by induction on the size of the group. The smallest non-Abelian group is S_3, for which the theorem is true. There are no other non-Abelian groups of order 6, so the theorem is true for all non-Abelian groups of order 6 or less. Assuming the theorem for all non-Abelian groups of size $n-1$ or less, let us consider a non-Abelian group G of order n. If G is commutator simple, we are done, so assume that there is $\gamma \in G \setminus Z(G)$ for which $(\{\gamma\}, G) \neq G'$.

Since $\gamma \notin Z(G)$, $(\{\gamma\}, G)$ is non-trivial. Also, since $(\{\gamma\}, G)$ is a proper subset of G', $G/(\{\gamma\}, G)$ is non-Abelian (see [5, Theorem 7.8]). Applying Lemma 4, part 2, and the induction hypothesis to this smaller group finishes the proof. □

3. Single Equations over Finite Groups

Let us now shift our attention to the language EQN_G, that is, the problem of determining if a single equation over G has a solution. We begin by showing that if G has a rich enough structure, (i.e., G is non-solvable), then even solving a single equation over G is NP-complete. For a discussion of solvable and nilpotent groups, see [5].

3.1. Non-Solvable Groups

Definition 4. *A group G is called* singly expressive *if* EQN_G *is* NP*-complete.*

As before, single expressivity respects subgroup and group quotient structure.

Lemma 8. *Let H be an inducible subgroup of G.*

1. *If H is singly expressive, then G is singly expressive.*
2. *If H is normal in G and G/H is singly expressive, then G is singly expressive.*

The proof proceeds as does that of Lemma 4.

Definition 5. *Let G be a non-solvable group, and define $G^{(1)} = G' = (G, G)$ and $G^{(i+1)} = \left(G^{(i)}, G^{(i)}\right)$. These subgroups make the* derived series *for G,*

$$G > G^{(1)} > \cdots > G^{(k)} = H,$$

which terminates in a subgroup H for which $H' = H$. This subgroup, which we shall label $G^{(*)}$, is actually normal in G. (See [5, II.7.13].) Observe, also, that $G^{(*)}$ is inducible.

The following lemma proves that a certain variety of non-solvable groups are singly expressive. It will serve as a base case in an inductive proof of the general result.

Lemma 9. *Let G be a finite non-solvable group such that $G = G'$ and G is commutator simple. Then G is singly expressive.*

Proof. Initially, the proof follows that of Lemma 7. For $k = |G/Z(G)|$, we shall reduce GRAPH k-COLORABILITY to EQN_G. As before, $k \geq 4$. An instance (V, E) is mapped to an equation in the following way. Every vertex v in V shall be associated with a variable x_v. As before, the coset of $Z(G)$ in which x_v lies will correspond to the color assigned v. Then, for every edge $e = (u, v)$ in E, $x_u x_v^{-1} \notin Z(G)$ iff x_u and x_v lie in different cosets of $Z(G)$. Since G is commutator simple and $G' = G$, there is a constant d_G so that whenever $x_u x_v^{-1} \notin Z(G)$,

$$G = \left\{ \prod_{i=1}^{d_G} [x_u x_v^{-1}, \beta_i] \;\middle|\; \beta_i \in G \right\}.$$

Let $\mathcal{E}_e(\beta_1, \ldots, \beta_{d_G}) = \prod_{i=1}^{d_G} [x_u x_v^{-1}, \beta_i]$ denote this function. Then, when $x_u x_v^{-1} \in Z(G)$, $\mathcal{E}_e = \mathbf{id}$ for all $\beta_1, \ldots, \beta_{d_G}$ and when $x_u x_v^{-1} \notin Z(G)$, every element of G can be induced from some setting of $\beta_1, \ldots, \beta_{d_G}$. Now we use an idea of Barrington's [1] to patch these equations together. Specifically, let $\mathcal{E}_1(\vec{\alpha})$ and $\mathcal{E}_2(\vec{\beta})$ be two functions, over disjoint sets of variables, each of which induces $\{\mathbf{id}\}$ or G. Then there is a constant d'_G, for which the function

$$\mathcal{E} = \prod_{i=1}^{d'_G} [\mathcal{E}_1(\vec{\alpha}_i), \mathcal{E}_2(\vec{\beta}_i)]$$

induces G exactly when both $\mathcal{E}_1$ and $\mathcal{E}_2$ induced G, and $\{\mathbf{id}\}$, otherwise. Repeatedly applying this construction in a balanced manner results in a function $\mathcal{E}$ which induces G when every edge has been colored with different cosets, and $\{\mathbf{id}\}$, otherwise. Selecting an element $\kappa \in G \setminus \{\mathbf{id}\}$, the equation $\mathcal{E} = \kappa$, has the desired properties.

To see that $\mathcal{E}$ has polynomial size, notice that as a function of the number of compounded equations (the $\mathcal{E}_e$), the length $L(k)$ of $\mathcal{E}$ satisfies $L(k) = O(1)L(k/2)$, so that $L(k) \leq n^{O(1)}$, as desired. □

Theorem 10. *If G is a finite non-solvable group, then G is singly expressive.*

Proof. We assume that G is non-solvable and proceed by induction on the order of G. Since $G^{(*)}$ is inducible, it is enough to show that $G^{(*)}$ is expressive.

If $|G^{(*)}| < |G|$ we are done by induction, since $G^{(*)}$ is non-solvable. If $G = G^{(*)}$ and G is commutator-simple, then we are done by the above lemma. Finally, if $G = G^{(*)}$ and G is *not* commutator-simple, we argue as follows. There is $\gamma \in G \setminus Z(G)$ for which $G \not\subset (\{\gamma\}, G)$. Since $\gamma \notin Z(G)$, $(\{\gamma\}, G)$ is non-trivial. Notice, also, that $(\{\gamma\}, G)$ is inducible. Recall the following standard result from the theory of solvable groups:

Fact 11. *Let H be a normal subgroup of G, with both H and G/H solvable. Then G is solvable.*

In our case, $(\{\gamma\}, G)$ is normal in G, so either $(\{\gamma\}, G)$ or $G/(\{\gamma\}, G)$ is non-solvable. Then Lemma 8 coupled with the induction hypothesis finishes the proof. Notice that the proof covers the base case, too. □

3.2. Nilpotent Groups and the Connection with Non-Uniform Finite Automata

So far, we see that for rich enough groups, the language EQN_G is NP-complete. It is natural to wonder if the above theorem can be improved somehow to show that for any non-Abelian group, EQN_G is NP-complete. It turns out that this is not the case (unless P = NP): applying the non-uniform finite automata machinery of Péladeau and Thérien [6], we show that for nilpotent groups N, $\text{EQN}_N \in \text{P}$. This also suggests that the ambient AND introduced when one considers a *system* of equations (that is, the requirement that each equation be satisfied) is quite powerful. Indeed, there are impossibility results for "computing the AND function" over nilpotent groups. (In fact, Lemmas 14 and 15 offer a result of this sort; see also [1]).

Definition 6. *A* non-uniform deterministic finite automaton *over a group G on n inputs is defined by a sequence of* instructions*; each instruction is an element of $[n] \times G^{\{0,1\}}$. Computation proceeds as follows: for an element $w \in \{0,1\}^n$, the automaton $A = (i_1, \delta_1)(i_2, \delta_2)\cdots(i_l, \delta_l)$* yields *the group element $\gamma \in G$ if*

$$\delta_1(w_{i_1}) \cdot \delta_2(w_{i_2}) \cdot \cdots \cdot \delta_l(w_{i_l}) = \gamma.$$

In general, the automaton defines a function $f_A : \{0,1\}^n \to G$. We say that the automaton can recognize $L \subset \{0,1\}^n$ if there is a subset $S \subset G$ for which $L = f_A^{-1}(S)$.

The theory of such automata has been admirably developed, motivated both by their connection with the fine structure of NC^1 and the satisfying algebraic perspective they offer the theory of finite automata. (See [2].)

For a fixed group $G = \{g_1, \ldots, g_k\}$, observe now that an equation

$$w_1 w_2 \cdots w_l = \gamma$$

over variables $v_1, \ldots, v_n$ may be transformed into an automaton program, with the property that there is an input accepted by the program if and only if there is a solution to the equation. The transformation proceeds as follows:

The product $w_1 w_2 \cdots w_l$ is translated into a sequence of instructions by translating each w_i into a short sequence of instructions and concatenating the result. For notational convenience we introduce a short-hand for instructions: let $\delta_{g_0,g_1}(y)$ correspond to an instruction that depends on the variable y and maps 0 to g_0 and 1 to g_1.

With each variable x_i of the equation we associate $k = |G|$ variables $(y_{i,j})_{j\in[k]}$. We also introduce a dummy variable z which is used when w_i is a constant.

If $w_i = g \in G$, then w_i is transformed into the instruction $\delta_{g,g}(z)$.

If $w_i = x_j$, then w_i is transformed into the sequence:

$$x_j \longrightarrow \delta_{e,g_1}(y_{j,1}), \delta_{e,g_2}(y_{j,2}), \ldots, \delta_{e,g_k}(y_{j,k})$$

If $w_i = x_j^{-1}$, then w_i is transformed into the sequence:

$$x_j^{-1} \longrightarrow \delta_{e,g_k^{-1}}(y_{j,k}), \ldots, \delta_{e,g_2^{-1}}(y_{j,2}), \delta_{e,g_1^{-1}}(y_{j,1})$$

Finally, let $\{\gamma\}$ be the set S of Definition 6.

It is straight-forward to transform a solution to the equation into an input accepted by the NUDFA, and vice versa. Also, the transformation can be done in polynomial time. Thus, if we, given an NUDFA A over G and $S \subset G$, can decide in polynomial time $f_A^{-1}(S) \neq \emptyset$, then we can decide in polynomial time if a given equation over G is solvable. We call this decision problem NUDFA-SAT_G.

Using methods from [6], we show the following.

Theorem 12. *If G is a finite nilpotent group, then NUDFA-SAT_G can be decided in polynomial time.*

As noted above, this yields the desired result:

Corollary 13. *If G is a finite nilpotent group, then EQN_G can be decided in polynomial time.*

Before describing the proof, we set down some notation. For a ring R with unit 1_R, the ring of n-variate polynomials over R is denoted $R[x_1, \ldots, x_n]$. Let $N \subset R[x_1, \ldots, x_n]$ be the ideal generated by the set $\left\{ x_i^2 - x_i \,\middle|\, i = 1, \ldots, n \right\}$. Then every element $p \in R[x_1, \ldots, x_n]/N$ may be represented as a multi-linear polynomial over R, and gives rise to a function $\mathbf{p} : \{0,1\}^n \to R$ by evaluation. We say that $p \in R[x_1, \ldots, x_n]/N$ *recognizes* the language $L \subset \{0,1\}^n$, if for some subset $S \subset R$,

$$L = \mathbf{p}^{-1}(S).$$

The proof of Theorem 12 depends on the following two lemmas.

Lemma 14. *Let L be a subset of $\{0,1\}^n$ recognized by an NUDFA over a finite nilpotent group G. There exists a finite, commutative ring $R = R(G)$ with unit and an element $r \in R[X]/N$ of degree $d = d(G)$ such that L is recognized by r. Furthermore, given an NUDFA, the corresponding polynomial is constructible in polynomial time.*

Lemma 14 is stated and proved in [6][1]. Note in particular that neither the ring R, nor the degree d depend on n.

For $w \in \{0,1\}^n$, let $\sigma(w) = \{i \mid w_i = 1\}$.

Lemma 15. *If R is a finite ring and d is a positive integer, then there is a constant $m = m(R,d)$ with the following property.*

If $r \in R[x_1, \ldots, x_n]/N$ is a polynomial of degree at most d, then

$$\mathbf{r}(\{0,1\}^n) = \left\{ \mathbf{r}(w) \;\middle|\; w \in \{0,1\}^n, |\sigma(w)| \leq m \right\}.$$

Or, in other words, if $\mathbf{r}(w) = \alpha$ for some $w \in \{0,1\}^n$, then $\mathbf{r}(u) = \alpha$ for some u where $|\sigma(u)| \leq m$. This is the key to proving Theorem 12.

Proof of Theorem 12. By Lemma 14 we can reduce NUDFA-SAT$_G$ to the problem of determining if a given polynomial r of degree at most d over a fixed ring R has a zero. By Lemma 15 we know that if $\mathbf{r}(w) = 0$ for some $w \in \{0,1\}^n$, then there is $u \in \{0,1\}^n$ with $|\sigma(u)| \leq m$ such that $\mathbf{r}(u) = 0$.

All we need to do is to run over all

$$u \in \{v \in \{0,1\}^n \mid |\sigma(v)| \leq m\}.$$

As this set has size $\Theta\left(\binom{n}{m} 2^m\right)$, and m is independent of n, this can be done in polynomial time. □

Theorem 12 shows that EQN$_G$ is in P when G is nilpotent. However, the time grows essentially like n^m, where m depends on the group G. In fact, as we shall see, m can be quite large even for small groups.

Lemma 15 follows from the proof of Lemma 2 in [6], but unfortunately the proof given there is not completely correct. The proof presented here uses the main ideas from [6], and can be used to fix the proof of Lemma 2 in [6].

Proof of Lemma 15. Let $w \in \{0,1\}^n$ be arbitrary. It suffices to show that there is a constant m such that, if $|\sigma(w)| > m$, then we can find some u for which $\sigma(u) \subsetneq \sigma(w)$ and $f(u) = f(w)$.

Write r as $r(x_1, \ldots, x_n) = \sum_{|S| \leq d} \lambda_S \left(\prod_{j \in S} x_j\right)$.

For a set $I \subseteq \sigma(w)$ we define

$$\Lambda(I) = \sum_{\substack{I \subseteq S \subseteq \sigma(w) \\ |S| \leq d}} \lambda_S .$$

Note that if $i \in \sigma(w)$ and we reset w_i to 0, then the value of $\mathbf{r}$ changes by $\Lambda(\{i\})$.

Let $t = |R|$ and let q be the smallest integer such that $qx = 0$ for all $x \in R$. By Ramsey's theorem (see e.g., [3, Theorem 2]) there is an integer $m = m(q,t,d) = m(R,d)$ with the following property: if $\sigma(w) > m$, then there exists a set $J \subseteq \sigma(w)$ of cardinality $qd!$ such that for $i = 1, 2, \ldots, d$ the quantities $\Lambda(I)$ associated with subsets $I \subset J$ of size i all have the same value, denoted by Λ_i.

If $\sigma(w) > m$ then construct $u \in \{0,1\}^n$ as follows. Find $J \subseteq \sigma(w)$ with the property described above. Let $u_i = w_i$ if $i \notin J$, and let $u_i = 0$ if $i \in J$.

Obviously $\sigma(u) \subsetneq \sigma(w)$. It remains to see that $\mathbf{r}(u) = \mathbf{r}(w)$.

$$\mathbf{r}(u) = \mathbf{r}(w) - \sum_{\substack{I \cap J \neq \emptyset, I \subseteq \sigma(w), \\ |I| \leq d}} \lambda_I .$$

And by inclusion-exclusion we have

$$\begin{aligned} \mathbf{r}(y) &= \mathbf{r}(w) - \sum_{\{j\} \subset J} \Lambda(\{j\}) + \sum_{\{j_1, j_2\} \subset J} \Lambda(\{j_1, j_2\}) - \cdots \\ &= \mathbf{r}(w) - \sum_{s=1}^{d} (-1)^s \binom{qd!}{s} \Lambda_s \\ &= \mathbf{r}(w). \end{aligned}$$

The last equality follows because q divides each binomial coefficient in the sum. □

4. Open Problems

An outstanding open problem is that of the complexity of EQN$_G$ for groups G which are solvable but not nilpotent. (A example is S_3.) There are lower bounds for the computational power of NUDFAs over some of these groups (like S_3), and it would be interesting to see if these could be used to understand the complexity of EQN$_G$.

5. Acknowledgments

We thank David Barrington for originally suggesting the connection between NUDFAs and group equations. The second author thanks Marcos Kiwi for several illuminating discussion. Both authors would especially like to thank Denis Thérien for teaching them about NUDFAs and inviting them to McGill.

References

[1] D. A. Barrington. *Bounded-Width Branching Programs*. PhD thesis, Massachusetts Institute of Technology, 1986.

[2] D. A. M. Barrington, H. Straubing, and D. Thérien. Non-uniform automata over groups. *Information and Computation*, 89(2):109–132, Dec. 1990.

[1] Polynomial-time constructibility is not explicitly stated in [6], but it is easy to conclude from the proof given there.

[3] R. L. Graham, B. L. Rothschild, and J. H. Spencer. *Ramsey Theory*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley and Sons, 1990.

[4] J. Håstad. Some optimal inapproximability results. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pages 1–10, El Paso, Texas, 4–6 May 1997.

[5] T. W. Hungerford. *Algebra*. Springer-Verlag, 1974.

[6] P. Péladeau and D. Thérien. Sur les langages reconnus par des groupes nilpotents. *C. R. Acad. Sci. Paris Sér. I Math.*, 306(2):93–95, 1988.