Submitted exclusively to the London Mathematical Society
doi:10.1112/S0000000000000000

THE COMPLEXITY OF THE EQUIVALENCE PROBLEM FOR NONSOLVABLE GROUPS

GÁBOR HORVÁTH, JOHN LAWRENCE, LÁSZLÓ MÉRAI AND CSABA SZABÓ

ABSTRACT

The equivalence problem for a group G is the problem of deciding which equations hold in G. It is know that for finite nilpotent groups and certain other solvable groups, the equivalence problem has polynomial time complexity. We prove that the equivalence problem for a finite nonsolvable group G is co-NP-complete by reducing the k-coloring problem for graphs to the equivalence problem, where k is the cardinality of G.

1. *Introduction*

A *group* G is a set with a multiplication operation $\cdot$ and an inverse operation $^{-1}$. *Terms* for groups are expressions $t(x_1, \dots, x_n)$ built up from the two operation symbols in the usual manner; to each term $t(x_1, \dots, x_n)$ and each group G one has a naturally associated *term function* $t^G : G^n \to G$. A group G *satisfies* an equation $s(\vec{x}) \approx t(\vec{x})$ if the corresponding term functions s^G and t^G are the same function.

The *(term) equivalence problem* for a group G is the problem of deciding which equations $s \approx t$ are satisfied by G. Since $G \models s \approx t$ if and only if $G \models s \cdot t^{-1} \approx 1$, we can view the equivalence problem for groups as the problem of deciding which equations $t \approx 1$ are satisfied by G.

Early investigations into the equivalence problem for various finite algebraic structures were carried out by computer scientists, in particular at Syracuse University where the terminology *the term equivalence problem* was introduced. In particular they considered finite commutative rings and finite lattices. In the early 1990s it was known by Hunt and Stearns (see [**4**]) that the equivalence problem of a finite commutative ring has either polynomial time complexity or it is co-NP-complete. Later Burris and Lawrence proved in [**2**] that the same holds for rings in general.

THEOREM 1.1. *Let R be a finite ring. The equivalence problem for R is in P if R is nilpotent, and it is co-NP-complete otherwise.*

The equivalence problem for finite groups has proved to be a far more challenging topic than that for finite rings. In 2004 Burris and Lawrence [**1**] proved that if G is nilpotent or $G \simeq D_n$, the dihedral group for odd n-s, then the equivalence problem

---

2000 *Mathematics Subject Classification* 20F10.

The research of the Hungarian authors was supported by the Hungarian National Foundation for Scientific Research, Grant F32325 and T038059. The first author was partly supported by a PhD studentship of the Algorithms Research Group, School of Comupter Science, University of Hertfordshire, U.K.

for G is in P. Later Horváth and Szabó [**5**] presented an other method for meta-abelian groups and, for example, they proved that if $G \simeq A \rtimes B$, where A and B are abelian groups, such that the exponent of A is squarefree and $(|A|, |B|) = 1$, then the equivalence problem for G is in P.

Interest in the computational complexity of the equivalence problem of a finite algebraic structure has been steadily increasing since that time. There are many results about the equivalence problem of finite monoids [**7**], [**12**],[**13**]. Their initial approach came from the complexity of recognizing formal languages. The first hardness result for semigroups was proved by Popov and Volkov [**9**], and several results were proved in Seif, Szabó [**11**]. For commutative semigroups the topic was thoroughly investigated in Kisielewicz [**6**].

In this paper we prove the following:

THEOREM 1.2. *The equivalence problem for a finite nonsolvable group G is co-NP-complete.*

We would like to eventually show that the equivalence problem for any finite group has either polynomial time complexity or it is co-NP-complete, but much remains to be done on this project.

2. *Preliminaries*

This section contains some definitions and easy observations about commutators and solvable groups (for more details see [**10**]).

DEFINITION 1.

a The commutator $[x, y]$ is a group term defined by

$$[x, y] := x^{-1}y^{-1}xy.$$

b Define the commutator terms $c_r\big(x_1, \ldots, x_{2^r}\big)$ by induction: $c_1(x_1, x_2) = [x_1, x_2]$ and for $r > 1$ let c_r be of arity 2^r:

$$c_r(x_1, x_2, \ldots, x_{2^r}) = \big[c_{r-1}(x_1, \ldots, x_{2^{r-1}}), c_{r-1}(x_{2^{r-1}+1}, \ldots, x_{2^r})\big].$$

c G is *solvable* if and only if for some $r \geq 1$, $G \models c_r \approx 1$. The smallest possible r is called the solvable length of G.

d For $a \in G$ let

$$[a, G] \;:=\; \big\langle \big\{ [a, g] : g \in G \big\} \big\rangle .$$

LEMMA 2.1.

a *If $N \trianglelefteq G$ with both N and G/N are solvable then G is also solvable.*

b *If N_1, N_2 are two normal solvable subgroups of G then the product $N_1 \cdot N_2$ is also a normal solvable subgroup of G.*

c *$[a, G]$ is a normal subgroup of G.*

d *If G is a non-abelian simple group then*

$$[a, G] \;=\; \begin{cases} 1 & \text{if } a = 1 \\ G & \text{if } a \neq 1 \end{cases}.$$

Here are some notations and claims about the verbal subgroups of a group (see [**8**]).

DEFINITION 2.

a Given a set T of group terms and let

$$T(G) \;:=\; \bigcup_{t\in T} \mathsf{Range}(t^G)$$

the union of the ranges of the term functions t^G.

b The subgroup generated by $T(G)$, which we denote by

$$T^*(G) \;:=\; \langle T(G)\rangle$$

is called a *verbal* subgroup of G.

c $\{1\}$ and G are verbal subgroups of G. If these are the only verbal subgroups of G then we say G is *verbally simple*.

d Given two terms $s(x_1,\dots,x_m)$ and $t(x_1,\dots,x_n)$, we define the term s_t by

$$s_t\big(x_1,\dots,x_{mn}\big) \;:=\; s\big(t(x_1,\dots,x_n),t(x_{n+1},\dots,x_{2n}),\dots,t(x_{mn-n+1},\dots,x_{mn})\big).$$

e For a finite group G let d_G be a positive integer such that for any set X of generators of G we have

$$G \;=\; \bigcup_{0\le k\le d_G} X^k.$$

f Given a term $s(x_1,\dots,x_m)$ and a finite group G define the term s_G by

$$s_G\big(x_1,\dots,x_{md_G}\big) \;:=\; \underbrace{s(x_1,\dots,x_m)\cdot s(x_{m+1},\dots,x_{2m})\cdots}_{\text{a product of } d_G \text{ terms } s(\cdots),\text{ with distinct variables}}.$$

LEMMA 2.2.

a *Every verbal subgroup of G is normal in G.*

b *A finite group G has a largest solvable verbal subgroup.*

c *Suppose G is finite. If $T=\{t_1,\dots,t_k\}$ let $t=t_1\cdots t_k$. Then*

$$T^*(G) \;=\; t_G(G).$$

d *Thus for a finite G, every verbal subgroup V of G is the range of a single term function.*

The length of a term is important in our investigations.

DEFINITION 3.

We define the length of a term function inductively: the length of a variable or its inverse is 1, and if s and t are terms with length a and b, then the length of the product term st is $a+b$.

LEMMA 2.3.

a *The length of s_t is the product of the length of t and the length of s.*

b *The length of s_G is the product of d_G and the length of s.*

The following proposition will play a crucial role in the proof of Theorem 1.2.

PROPOSITION 2.4. *Given a finite group G*

a *For a verbal subgroup V let s be a term with $s(G) = V$. For all terms t we have*

$$V \models t \approx 1 \quad \text{if and only if} \quad G \models t_s \approx 1.$$

b *Suppose G is nonsolvable but every proper verbal subgroup of G is solvable. Let V be the largest solvable verbal subgroup of G, denote its solvable length by r. Then for all terms t we have*

$$G/V \models t \approx 1 \quad \text{if and only if} \quad G \models c_{rt_G} \approx 1.$$

c *If G is verbally simple and N is a proper normal subgroup of G then for all terms t we have*

$$G \models t \approx 1 \quad \text{if and only if} \quad G/N \models t \approx 1.$$

Proof.

a Let t be n-ary and s be m-ary. Let $\vec{y}_i = (y_{i1}, \dots, y_{im})$ for $i = 1, \dots, n$, and we consider the terms $t(x_1, \dots, x_n)$ and $t_s\big(y_{11}, \dots, y_{nm}\big) = t\big(s(\vec{y}_1), \dots, s(\vec{y}_n)\big)$. While $\vec{y}_i$ run through all tuples from G, the values of $s(\vec{y}_i)$ attain every element of V. Thus if $t \neq 1$ at some evaluation $(h_1, \dots, h_n) \in V^n$, then we can choose the tuples $\vec{y}_i$ such that $s(\vec{y}_i) = h_i$. Thus there is an evaluation of t_s such that $t_s \neq 1$.
On the other hand, if $t_s \not\approx 1$ over G, then there is an evaluation $\vec{y}_1, \dots, \vec{y}_k$ such that $t_s \neq 1$. Now, for the elements $h_i = s(\vec{y}_i)$ we have $t(h_1, \dots, h_n) \neq 1$, hence $t \not\approx 1$ over V.

b Let m be the arity of t_G. If $t \approx 1$ over G/V, then $t_G(G) \leq V$, hence $t_G(G)$ is solvable and $c_{rt_G} \approx 1$ over G. On the other hand, if $t \not\approx 1$ over G/V then $t_G(G)$ is non-solvable and $t_G(G) = G$. As there are some elements $g_1, \dots g_{2^r} \in G$ such that $c_r(\vec{g}) \neq 1$, and there are m-tuples $\vec{y}^i$ such that $t_G(\vec{y}^i) = g_i$, we have $c_{rt_G}(\vec{y}^1, \dots, \vec{y}^{2^r}) \neq 1$. Hence $c_{rt_G} \not\approx 1$ over G.

c If $t \approx 1$ over G then clearly $t \approx 1$ over G/N. Now, if $t \approx 1$ over G/N, then $t_G(G) \leq N$. As $t_G(G)$ is verbal, $t_G(G) = \{1\}$, hence $t \approx 1$ over G.

□

3. *Proving Co-NP-Completeness*

Our leading reference on computational complexity will be [**3**]. The equivalence problem of any finite group G is clearly in co-NP: to check if an equation $t(\vec{x}) \approx 1$ fails in G one only needs one instance $\vec{g}$ where $t^G(\vec{g}) \neq 1$, and given such an instance $\vec{g}$ one can find the value of $t^G(\vec{g})$ in polynomial time. Thus to prove the theorem we will exhibit an NP-complete problem that polynomially reduces to the equivalence problem of G. The most elegant choice we have found is to use the NP-completeness of the k-coloring problem where k is the size of the group G when G is a simple non-Abelian group. Then we use induction for non-solvable groups in general.

THEOREM 3.1. *Let G be a finite, simple, non-Abelian group. Then the equivalence problem for G is co-NP-complete.*

Proof. Let $k = |G|$. The group G is non-Abelian and simple, hence $k \geq 60$. We polynomially reduce GRAPH k-COLORING to the equivalence problem of G. Let $\Gamma = (V, E)$ be an arbitrary simple graph with no loops, or multiple edges, $V = \{v_1, \ldots, v_n\}$ and $E = \{e_1, \ldots, e_m\}$. We shall color the vertices of Γ by the elements of G. The color of v_i will be g_i. We exhibit a term function t over G such that $t(g_1, \ldots, g_n) \neq 1$ if and only if the appropriate coloring is a k-coloring.

By Lemma 2.1/d we have $[g, G] = G$ for every $g \neq 1$. Let d_G be the constant defined in Definition 2/e. This constant is depending only on G and for every $g \in G$

$$G = [g, G] = \prod_1^{d_G} [g, y_i]$$

holds. Let

$$S(x, y_1, \ldots, y_{d_G}) = S(x, \bar{y}) = \prod_{k=1}^{d_G} [x, y_k].$$

Every vertex v_i in V will be associated to a variable x_i. Then for every edge $e = (v_i, v_j)$ we define

$$S_{i,j}(\bar{y}) = S(x_i x_j^{-1}, \bar{y}).$$

Thus $S_{i,j}(G) = 1$ if we substitute $x_i = x_j$ and $S_{i,j}(G) = G$ if we substitute $x_i \neq x_j$. The length of $S_{i,j}$ depends only on G: each commutator contains 3 variables, repeated twice and we multiply d_G of them, so the length of this term fuction is $6d_G$. We are ready to define t. Let $e = (v_i, v_j)$ be an edge of Γ. Let

$$t_e(\bar{y}) = S_{i,j}(\bar{y}) = S(x_i x_j^{-1}, \bar{y}).$$

Let $e_1, e_2, \ldots, e_m$ be the list of edges of Γ and r such that $2^{r-1} < m \leq 2^r$. Moreover let

$$t = c_r(t_{e_1}, t_{e_2}, \ldots, t_{e_m}, t_{e_m}, \ldots, t_{e_m}).$$

Here we repeat t_{e_m} enough many ($2^r - m$ many) times in order to match the arity of c_r. In the terms t_{e_i} the variables of $\bar{y}$ are all distinct. So there are altogether $d_G 2^r$ many 'y'-s and their inverses. The length of t is $6d_G \cdot 4^r \leq 6d_G(2m)^2 = 24d_G m^2$ hence polynomial in the size of Γ. We claim that $t \not\approx 1$ over G if and only if Γ is k-colorable. Firstly, let us assume that Γ is k-colorable by the elements of G, and let g_i be the color of v_i. Now, substituting $x_i = g_i$, for every edge e of Γ we have $t_e(G) = G$. Since G is not solvable, $c_r \not\approx 1$ over G and so $t \not\approx 1$, either. Secondly, if G is not k-colorable, then at any assignment of the variables we have a monochromatic edge, e. Then $t_e = 1$ at every substitution, hence $t = 1$ at every substitution, thus $t \approx 1$. □

The first step of the induction is about verbal subgroups.

LEMMA 3.2. *Let V be a verbal subgroup of G. If the equivalence problem for V is co-NP-complete, then the equivalence problem for G is co-NP-complete.*

Proof. We give a polynomial reduction from the equivalence problem of V to the equivalence problem of G. For every term function $t(x_1, \ldots, x_k)$ over V we present a term function t' over G such that $t \approx 1$ over V if and only if $t' \approx 1$ over G. As V

is verbal, there is a term $s(x_1, \ldots, x_n)$ over G such that $s(G) = V$. Let $t' = t_s$ as in Proposition 2.4/a. Now $t \approx 1$ over V if and only if $t' \approx 1$ over G.

The reduction is polynomial in the length of t because the length of t' is the product of the length of t and the length of s. The latter depends only on the group G. □

Now, we prove Theorem 1.2.

Proof of Theorem 1.2 . We proceed by induction on the order of G.

Case 1: There exists a non-trivial, non-solvable verbal subgroup V of G. Now, $|V| < |G|$ and the equivalence problem for V is co-NP-complete by the assumption. Thus the equivalence problem for G is co-NP-complete by Lemma 3.2.

Case 2: There are no nontrivial nonsolvable verbal subgroups of G but there is a non-trivial solvable verbal subgroup of G. Let V be the largest solvable verbal subgroup and r denote its solvable length. The quotient group G/V is non-solvable. Now, the equivalence problem for G/V is co-NP-complete by the assumption, as $|G/V| < |G|$. We give a polynomial reduction from the equivalence problem for G/V to the equivalence problem for G.

Let t be a term over G/V. Then we know by Proposition 2.4/b that $t \approx 1$ over G/V if and only if $c_{rt_G} \approx 1$ over G. The length of c_{rt_G} is the product of the length of c_r and the length of t_G, which is the product of t and d_G. The latter and the length of c_r depend only on the group G, hence the reduction is polynomial.

Case 3: There are no verbal subgroups in G. If G is simple, we are done by Theorem 3.1. Let N be a normal subgroup of G and t be a term function. By Proposition 2.4/c we know that $t \approx 1$ over G if and only if $t \approx 1$ over G/N. The factor group G/N is non-solvable, because G' is verbal and so $G' = G$. Thus by induction the equivalence problem for G is co-NP-complete. □

4. *Problems*

There are lots of work left to be done. The best possible result would be one similar to Theorem 1.1.

PROBLEM 1. Give an algebraic characterization of the class of finite groups with a polynomial time equivalence problem; likewise for the class of finite groups with a co-NP-complete equivalence problem.

It is not yet clear whether or not these two complexity classes exhaust all finite groups.

PROBLEM 2. Is there a polynomial time/co-NP-complete dichotomy for the equivalence problem for finite groups?

At present we do not even have a good conjecture. For finite algebraic structures in general it is conjectured that there is no dichotomy of the computational complexity of the equivalence problem. We do not know how to classify even the smallest group that is neither nilpotent nor meta-abelian:

PROBLEM 3. Find the complexity of the equivalence problem for S_4.

References

1. S. Burris and J. Lawrence, 'Results on the equivalence problem for finite groups', *Algebra Universalis* 52 (2004) no. 4, 495–500 (2005).

2. S. Burris and J. Lawrence, 'The equivalence problem for finite rings', *Journal of Symbolic Computation* 15 (1993) 67–71.

3. M. R. Garey and D. S. Johnson, *Computers and intractability*, (W. H. Freeman & Co., San Francisco, 1979).

4. H. Hunt and R. Stearns, 'The complexity for equivalence for commutative rings', *Journal of Symbolic Computation* 10 (1990) 411–436.

5. G. Horváth and Cs. Szabó, 'The complexity of checking identities in groups', *International Journal of Algebra and Computation*, accepted (2005).

6. A. Kisielewicz, 'Complexity of semigroup identity checking' *Internat. J. Algebra Comput.* 14 (2004) no. 4, 455–464.

7. O. Klíma, 'Unification Modulo Associativity and Idempotency', PhD thesis, Masarik University, Brno, 2004.

8. H. Neumann, *Varieties of groups*, (Springer-Verlag, Berlin, 1967).

9. V. Yu. Popov and M. V. Volkov, 'Complexity of checking identities and quasi-identities in finite semigroups', *Journal of Symblic logic*.

10. D. J. S. Robinson, *A course in the theory of groups*, Springer-Verlag, New York, Berlin, Heidelberg, 1995.

11. S. Seif and Cs. Szabó 'The complexity of the identity checking problem for finite semigroups', *Semigroup Forum*, to appear (2006).

12. P. Tesson, 'Computational Complexity Questions Related to Finite Monoids and Semigroups', PhD thesis, McGill University, Montreal, 2004.

13. P. Tesson and D. Therien, 'Monoids and Computations', *Internat. J. Algebra Comput.* 14 (2004) no. 5-6, 801–816.

Gábor Horváth, László Mérai and Csaba Szabó
Eötvös Loránd University,
Department of Algebra and Number Theory,
1117 Budapest, Pázmány Péter sétány 1/c,
Hungary

ghorvath@cs.elte.hu
merai@cs.elte.hu
csaba@cs.elte.hu

John Lawrence
Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1

jwlawrence@math.uwaterloo.ca