PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 143, Number 11, November 2015, Pages 4723–4731
http://dx.doi.org/10.1090/proc/12630
Article electronically published on April 10, 2015

EQUATIONS IN NILPOTENT GROUPS

MOON DUCHIN, HAO LIANG, AND MICHAEL SHAPIRO

(Communicated by Kevin Whyte)

Abstract. We show that there exists an algorithm to decide any single equation in the Heisenberg group in finite time. The method works for all two-step nilpotent groups with rank-one commutator, which includes the higher Heisenberg groups. We also prove that the decision problem for systems of equations is unsolvable in all non-abelian free nilpotent groups.

1. Introduction

1.1. **The equation problems.** There are several variants on the *equation problem* in groups, studying the solvability of equations of the form $w = 1$, where w is a word written as a product of constants (fixed group elements) and variables (with values ranging over group elements). For instance, consider the Heisenberg group $H(\mathbb{Z}) = \langle a, b : [a, b, a], [a, b, b] \rangle$. One could seek values of x, y satisfying the equation $xyxya = 1$, in which case there are none. The equation problem is decidable if there is an algorithm for taking any single equation and answering YES or NO to the question of whether solutions exist. Harder than solving a single equation is to solve a system of simultaneous equations, and harder than that is to solve a system of equations and inequations, where "inequations" are of the form $w \neq 1$. Let us denote those three problems by $\mathcal{EP}_1$, $\mathcal{EP}$, and $\mathcal{EIP}$. Note that systems of equations without constants always have the trivial solution, but if inequations are also allowed, then it becomes meaningful to consider such systems; we can call this decision problem $\mathcal{EIP}nc$. In logic terms, $\mathcal{EP}_1$ is the *decision problem for unification* and $\mathcal{EIP}/\mathcal{EIP}nc$ are *decidability of the existential theory* (or equivalently the universal theory) of the group, depending on whether the language one is working over is taken to have constants or not; authors vary in this convention. ($\mathcal{EP}$ would then correspond to the *positive existential theory*.)

In the 1960s and 1970s many papers focused on effective algorithms to produce solutions to particular equations in particular groups; see [5] for a survey. The work of Makanin changed the terms of study when he showed that $\mathcal{EIP}$ is decidable in free groups. This work has been much generalized, and now $\mathcal{EIP}$ is known to be decidable in virtually free groups, hyperbolic groups, and certain free products and graph products (including right-angled Artin groups), by combined work of Rips-Sela, Dahmani-Guirardel, and Diekert-Lohrey-Muscholl, in various combinations. See [2] for an overview.

Received by the editors March 6, 2014 and, in revised form, August 29, 2014.
2010 *Mathematics Subject Classification.* Primary 20F10, 20F18, 20F70.
The first author was partially supported by NSF grants DMS-1207106 and DMS-1255442.
The third author wishes to acknowledge support from NIH grant K25 AI079404-05.

Roman'kov was the first to show that it is not the case that $\mathcal{EP}$ is decidable in all nilpotent groups by exhibiting a four-step, rank-six nilpotent group in which it is undecidable [8]. In the same paper he also proves that decidability of $\mathcal{EIP}nc$ in the Heisenberg group (or in any free two-step nilpotent group) is equivalent to an affirmative answer to Hilbert's Tenth Problem over the rationals, a major open problem in number theory. This leaves open (and motivates!) the more granular questions of which equation problems are solvable in which nilpotent groups. Up to now, the sharpest results we have found in the literature are as follows, where $N(p, q)$ represents the free nilpotent group of step p and rank q (defined below in §1.3), and we adopt the standing convention that $p, q \geq 2$. All of the undecidability results below are accomplished by showing that equations in the group can be used to encode diophantine equations and vice versa, then appealing to the negative solution to Hilbert's Tenth Problem over the integers.

Note that there are no easy implications between any of these decision problems in $N(p, q)$ and $N(p', q')$ for $(p, q) \neq (p', q')$, because both the constants and the variables change from one group to another.

Single equations.

- There is an algorithm to decide any single equation in one variable in any $N(2, q)$ (Repin [7]).
- There is an algorithm to decide any equation $w = 1$ in any $N(2, q)$, provided w is not a product of commutators (Burke-Truss [1]).
- There is an algorithm to decide any single equation in up to two variables in $H(\mathbb{Z}) = N(2, 2)$ (Truss [12]).
- $\mathcal{EP}_1$ is undecidable in $N(3, \infty)$ (Truss [12]).

Systems of equations.

- $\mathcal{EP}$ is undecidable in $N(2, q)$ if q is sufficiently large (Durnev [3]).
- $\mathcal{EP}$ is undecidable in $N(3, 2)$ (Truss [12]).

(Many of these references can be found in Roman'kov's 2012 survey [9].)

Below, we show that $\mathcal{EP}_1$ is decidable in $N(2, 2)$, but that $\mathcal{EP}$ (and therefore also $\mathcal{EIP}$) is undecidable in all $N(p, q)$, i.e., all non-abelian free nilpotent groups. We also note that Truss's argument is easily modified to prove that $\mathcal{EP}_1$ is undecidable in all $N(p, q)$ for $p \geq 3$, q sufficiently large. This leaves open some intermediate cases ($p = 2$ and/or small q) in which decidability of $\mathcal{EP}_1$ is still open.

Our result that any single equation in $H(\mathbb{Z})$ is decidable is the first such result in any (non-virtually-abelian) nilpotent group, as far as we know. This is accomplished by reducing this decision problem to solving a single diophantine quadratic equation in many variables, which is already known to be decidable. In fact, since algorithms for quadratic equations produce general solutions, this amounts to solving (and not just deciding) the unification problem.

Our method works for a larger class of groups, allowing us to decide any single equation in any two-step nilpotent group with rank-one commutator. This class includes all $\mathbb{Z}$-central extensions of free abelian groups, including the higher Heisenberg groups, and also allows for the possibility of torsion, as will be explained below.

1.2. **Relationship to number theory and logic.** First, some well-known facts from the theory of equations over $\mathbb{Z}$. A system of polynomials $f_1 = \cdots = f_n = 0$

to be solved over $\mathbb{Z}$ (or $\mathbb{Q}$) is equivalent to the single equation ${f_1}^2 + \cdots + {f_n}^2 = 0$, so a system of polynomials may be solved whenever one can solve a single equation of twice the maximal degree occurring in the system. Skolem observed that any polynomial equation can be converted to a system of at-most-quadratic equations by introducing extra variables. (For example, $y^2 = x^5 + 3$ is equivalent to $u = x^2$, $v = u^2$, $y^2 = xv + 3$.) Putting these together, we see that an arbitrary system of polynomial equations can be converted into a single polynomial of degree at most four. Thus Hilbert's Tenth Problem, asking whether an algorithm exists to decide if an arbitrary system of diophantine polynomials has a solution, can be reduced to finding solutions to single fourth-degree polynomials.

Let us abbreviate $\mathcal{E}_{\mathbb{Z}}(d, n)$ for the problem of finding an integer solution to a single polynomial in $\mathbb{Z}[x]$ of degree d in n variables. Then $\mathcal{E}_{\mathbb{Z}}(1, n)$ and $\mathcal{E}_{\mathbb{Z}}(2, n)$ are decidable for all n; the $d = 1$ case is a linear algebra exercise, and the quadratic case was settled in 1972 by Siegel [10]. $\mathcal{E}_{\mathbb{Z}}(1, d)$ is decidable for all d by approximating roots numerically and checking nearby integers. One can try to play d and n off each other to find the boundary of decidability: it is known that $d = 4$ and $n = 11$ suffice for undecidability, each paired with an appropriately large value in the other parameter. $\mathcal{E}_{\mathbb{Z}}(3, 2)$ is decidable (see [11] and its references). However, $\mathcal{E}_{\mathbb{Z}}(3, n)$ is still an open problem for every $n \geq 3$, and it is an open possibility that it is decidable for all n. Most of this is covered in the survey [6], discussing the negative solution to Hilbert's Tenth.

The undecidability results mentioned above for nilpotent groups all proceed by drawing a connection from the group theory to the number theory: one shows that any system of quadratic diophantine equations can be encoded as a system of equations in $N(p, q)$ such that one system has solutions if and only if the other does. Therefore undecidability of those group-theoretic problems follows from the classical results in number theory and logic.

1.3. **Nilpotent groups.** We will take the commutator convention $[a, b] = aba^{-1}b^{-1}$. Define the nested commutator by

$$[a, b, c, d] = [[a, b, c], d] = [[[a, b], c], d],$$

and so on. Then a finitely generated group is called k-step *nilpotent* if all nested commutators with $k + 1$ arguments are trivial, but not all those with k arguments.

With this notation, the standard discrete *Heisenberg group* is the two-step nilpotent group given by the presentation

$$H(\mathbb{Z}) = \langle a, b : [a, b, a], [a, b, b] \rangle.$$

It sits in the short exact sequence

$$1 \to \mathbb{Z} \to H(\mathbb{Z}) \to \mathbb{Z}^2 \to 1,$$

where a generator c of $\mathbb{Z}$ is mapped to $[a, b]$ by the inclusion map i. The second map is the projection $\pi : H(\mathbb{Z}) \to H(\mathbb{Z})/i(\mathbb{Z})$ where the image is identified with $\mathbb{Z}^2$ by mapping a and b to the standard basis vectors.

Recall that p-step nilpotent groups have lower central series

$$1 = G_{p+1} \trianglelefteq G_p \trianglelefteq \cdots \trianglelefteq G_2 \trianglelefteq G_1 = G,$$

where $G_{i+1} = [G_i, G]$, so that in particular G_2 is the usual commutator subgroup of G, and G_p is central in G. Each quotient G_i/G_{i+1} is an abelian group which

is virtually $\mathbb{Z}^{d_i}$, and we call d_i the *rank* of that quotient group. Recall that the indexing is set up so that $[G_i, G_j] \subseteq G_{i+j}$.

We do not treat the step-one (abelian) case in this paper because all of these decision problems that we discuss are solvable in abelian groups.

The *free nilpotent group* $N(p, q)$ of step $p \geq 2$ and rank $q \geq 2$ is formed by taking $H = F_q$, the free group on q generators, letting H_{p+1} be the group in its lower central series, and defining $N(p, q) = H/H_{p+1}$. In other words, it has q generators and only the relations required to make it p-step nilpotent. These are universal in the sense that any finitely generated nilpotent group is a quotient of an appropriate $N(p, q)$.

2. Two-step groups

2.1. **Mal'cev coordinates.** Consider any two-step nilpotent group G with rank-one commutator. We will now construct Mal'cev coordinates for the group. This is entirely standard in the torsion-free case, but we take some care to handle torsion.

By the fact that the commutator of a two-step group is abelian, the classification of abelian groups, and the rank assumption, the short exact sequence

$$1 \to [G, G] \to G \to G/[G, G] \to 1$$

becomes

$$1 \to \mathbb{Z} \oplus (\mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_s}) \to G \to \mathbb{Z}^n \oplus (\mathbb{Z}_{l_1} \oplus \cdots \oplus \mathbb{Z}_{l_r}) \to 1,$$

for appropriate cyclic groups. Let $\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_r)$ be lifts to G of a basis for $\mathbb{Z}^n$ and generators for $\mathbb{Z}_{l_i}$, respectively. Also let c and $\mathbf{d} = (d_1, \ldots, d_s)$ be generators of $[G, G]$, so that any word in the commutator subgroup can be written uniquely as $g = c^{\alpha} d_1^{\alpha_1} \cdots d_s^{\alpha_s}$. Then these a_i, b_i, c, and d_i form a generating set for G that we will call a *Mal'cev generating set* (or Mal'cev basis), denoted by $\{\mathbf{a}, \mathbf{b}, c, \mathbf{d}\}$. Its relations are completely given by declaring that c and all d_i are central, that each $d_i^{k_i} = 1$, and by freely choosing the exponents in the expression $c^* d_1^* \cdots d_s^*$ for each of the $[a_i, a_j](i < j)$, $[b_i, b_j](i < j)$, and $[a_i, b_j]$. By construction, commuting a letters with b letters only creates more central c and d letters, so each element can be written in the form $g = a_1^* \cdots a_n^* b_1^* \cdots b_r^* c^* d_1^* \cdots d_s^*$, and this is unique if the b and d exponents are reduced with respect to their modularities. This gives a normal form, i.e., a bijective correspondence between group elements and tuples in $\mathbb{Z}^n \oplus \mathbb{Z}_{l_1} \oplus \cdots \oplus \mathbb{Z}_{l_r} \oplus \mathbb{Z} \oplus \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_s}$. (Here we identify $\mathbb{Z}_m$ with $\{0, \ldots, m-1\} \subset \mathbb{Z}$.) This tuple is called the *Mal'cev coordinates* with respect to the Mal'cev basis.

Suppose $g, g' \in G$, with Mal'cev coordinates $(\mathbf{A}, \mathbf{B}, C, \mathbf{D})$ and $(\mathbf{A}', \mathbf{B}', C', \mathbf{D}')$, respectively. Let gg' have coordinates $(\mathbf{A}'', \mathbf{B}'', C'', \mathbf{D}'')$. To put gg' in normal form, we need only commute the a_i and b_i letters into place and reduce the b_i in the appropriate moduli. Hence we have $A_i'' = A_i + A_i'$ and $B_i'' \equiv B_i + B_i' \pmod{l_i}$. Next,

$$C'' = C + C' - \sum_{i<j} \alpha_{ij} A_i' A_j - \sum_{i<j} \beta_{ij} B_i' B_j - \sum_{i,j} \gamma_{ij} A_i' B_j + \sum_{\{i : B_i + B_i' \geq l_i\}} \epsilon_i,$$

where the α, β, γ are the exponents of c in the appropriate commutator relations and ϵ_i is the exponent of c in $b_i^{l_i}$. Each D_i'' is a similar expression, reduced modulo k_i.

2.2. $\mathcal{EP}_1$ in step two.

Lemma 1. *There is an algorithm to decide whether there are simultaneous solutions to any system of diophantine equations consisting of linear equations and a single quadratic equation.*

Proof. Let Σ be a system of linear equations and Q be a quadratic equation in the unknowns $y_1, \ldots, y_m$. We can write these out as $\Sigma_i : \sum_{j=1}^{m} \alpha_{ij} y_j = C_i$ and $Q : f(\mathbf{y}) = 0$, where $\mathbf{y} = (y_1, \ldots, y_m)$ and f is a quadratic polynomial. We will consider the system $\overline{\Sigma}$ consisting of Σ and Q. A solution of Σ exists exactly if C_i is an integer combination of the α_{ij} for each i. One easily checks if $\gcd(\alpha_{i1}, \ldots, \alpha_{im})$ divides C_i. If Σ has no solution, then $\overline{\Sigma}$ has no solution. Now suppose Σ has a nonempty solution set $S \subset \mathbb{Z}^m$ and let $\mathbf{s} \in S$ be a solution. Consider the corresponding homogeneous system Σ_0 whose i^{th} equation is $\sum_{j=1}^{m} \alpha_{ij} y_j = 0$, and let T_0 and S_0 be its solution spaces in $\mathbb{R}^m$ and $\mathbb{Z}^m$, respectively, so that $S_0 = T_0 \cap \mathbb{Z}^m$. From the α_{ij}, one can compute an integral basis $\mathbf{v}_1, \ldots, \mathbf{v}_d \in \mathbb{Z}^m$ of S_0, so that $S = \{c_1\mathbf{v}_1 + \cdots + c_d\mathbf{v}_d + \mathbf{s} : c_i \in \mathbb{Z}\}$. Now Σ has a solution if and only if there exists $\mathbf{y} \in S$ such that $f(\mathbf{y}) = 1$, where f is the quadratic polynomial from Q. But $f(\mathbf{y})$ is just a quadratic equation in $c_1, \ldots, c_d$, the integer parameters from above, and a single diophantine quadratic equation is decidable. □

Lemma 2. *There is an algorithm to decide whether there are simultaneous solutions to any system of diophantine equations consisting of arbitrarily many linear equations, arbitrarily many congruences, and a single quadratic equation.*

Proof. We suppose again that the variables are $y_1, \ldots, y_m$ and in addition to Σ and Q from above we add the system Ω of congruences, with k^{th} equation $\Omega_k : f_k(\mathbf{y}) \equiv 0 \pmod{M_k}$. Since $\mathbb{Z}_{M_k}$ is finite, we can enumerate all solutions; denote the solution set by $U_k \subset (\mathbb{Z}_{M_k})^m$. Let us consider the set $U \subset \mathbb{Z}^m$ that simultaneously lifts the U_k. This set is easily constructed by the Chinese Remainder Theorem, and it has the form $U = \{r_1\mathbf{u}_1 + \cdots + r_s\mathbf{u}_s + \mathbf{t}\}$. Therefore the intersection of U and S still has finitely many integer parameters, and the full system is decidable as in the previous lemma. □

Theorem 3. *$\mathcal{EP}_1$ is decidable in any two-step nilpotent group with rank-one commutator, and in particular in $H(\mathbb{Z}) = N(2, 2)$.*

Proof. Let G be a two-step nilpotent group with rank-one commutator and let $\{\mathbf{a}, \mathbf{b}, c, \mathbf{d}\}$ be a Mal'cev generating set of G, as above. Let $w = 1$ be an equation in G. We know that $w = 1$ if and only if the corresponding Mal'cev coordinate vector is the zero vector. For the $\mathbf{a}$, $\mathbf{b}$, and $\mathbf{d}$ coordinates, this reduces to finitely many linear equations and finitely many congruences.

The c-coordinate equation is nearly a quadratic in the input data, except for the ϵ terms coming from cases in the $\mathbf{b}$ values. However, there are only finitely many possible $\mathbf{b}$ values, and hence only finitely many solutions $\mathbf{B}$ of the $\mathbf{b}$-coordinate equations. For each of these, the c-coordinate equation becomes quadratic. We can check each of these finitely many systems using the algorithm described in the previous lemma. □

Remark. What happens if we try to run this argument in a two-step group with a higher-rank commutator, say of rank $d > 1$? Most of the argument goes through, but instead of one quadratic equation, we get d quadratic equations. Although

general systems of quadratic equations are undecidable, this process might produce systems falling into a special subclass of quadratic systems, and *a priori* this subclass could be decidable.

2.3. $\mathcal{EP}$ **in step two.** Next we show that systems of equations are undecidable in two-step groups, saving the higher-step case for the next section. We discovered after finding this proof that Roman'kov has used the same encoding scheme for various applications, for instance in [8].

Theorem 4. *$\mathcal{EP}$ is undecidable in $N(2,q)$ for all q. In particular, it is undecidable in $H(\mathbb{Z})$.*

Proof. Begin with an arbitrary system of diophantine quadratic equations $\hat{\Sigma}$ in variables $x_1, \dots, x_n$, whose i^{th} equation is

$$\hat{\Sigma}_i : \alpha_i + \sum_j \beta_{ij} x_j + \sum_{j,k} \gamma_{ijk} x_j x_k = 0.$$

We will encode this in $G = N(2,q)$ with a system of equations in twice as many variables and $3q$ additional equations. For each variable x_j in the integer system, we will have variables y_j, y_j' in the group. We will take the generators of $N(2,q)$ to be $a_1, \dots, a_q$ and let $c_i = [a_j, a_k]$, $j < k$, $i = 1, \dots, \binom{q}{2} =: t$. The $\{c_i\}$ are a basis of the free abelian group $G_2 \cong \mathbb{Z}^t$. For notational convenience, we take $a = a_1$, $b = a_2$, $c = c_1 = [a,b]$.

Observe that the $\{\mathbf{a}, \mathbf{c}\}$ form a Mal'cev basis for G; i.e., an arbitrary element of $N(2,q)$ can be written uniquely in the form

$$g = a^A b^B a_3^{m_3} \dots a_q^{m_q} c^C c_2^{n_2} \dots c_t^{n_t}.$$

We build a system of equations Σ in the group G having i^{th} equation

$$\Sigma_i : [a,b]^{\alpha_i} \cdot \prod_j [a, y_j']^{\beta_{ij}} \cdot \prod_{j,k} [y_j, y_k']^{\gamma_{ijk}} = 1$$

and the additional $3q$ equations $[a, y_j] = 1$, $[b, y_j'] = 1$, $[b, y_j] = [y_j', a]$ for all $1 \le j \le q$.

Using the normal form, it is immediate that $[a, y_j] = 1 \implies y_j = a^{r_j} g$ and $[b, y_j'] = 1 \implies y_j' = b^{r_j'} g'$ for some $g, g' \in G_2$. Since $[b, y_j] = [y_j', a]$, we have $r_j = r_j'$. It now follows that $[a, y_j'] = c^{r_j}$ and $[y_j, y_k'] = c^{r_j r_k}$. That lets us simplify Σ_i to $c^{\alpha_i + \sum_j \beta_{ij} r_j + \sum_{j,k} \gamma_{ijk} r_j r_k} = 1$, which of course is satisfied exactly if the exponent is zero. Thus a solution to Σ can produce a solution to $\hat{\Sigma}$ by letting $x_j = r_j$, and on the other hand a solution to $\hat{\Sigma}$ yields a solution to Σ by taking $y_j = a^{x_j}$, $y_j' = b^{x_j}$. □

Remark. It is interesting to note that this same argument can be adapted to higher-step groups by choosing two basic commutators in G_{p-1} (the second-to-last nontrivial group in the lower central series) to play the role of a and b here and copying the defining equations verbatim. However, this will not work in the group $N(3,2)$, where G_2 has only one basic commutator! In the next section, we present an alternative approach that works for all $N(p,q)$ with $p \ge 3$.

3. Higher-step groups

3.1. $\mathcal{EP}$ **in step** ≥ 3**.** In this section we give a machine to convert back and forth between equation systems in $N(p,q)$ and equation systems over the integers. The ability to do this hinges on a simple linearity lemma whose proof we include to keep the exposition self-contained. This is directly inspired by Truss's approach to $N(3,2)$ in [12]. (We note that linearity statements hold in all arguments, but this lemma only includes what we need below.)

Lemma 5. *In a k-step nilpotent group G, we have linearity in the last and second-to-last arguments of a k-fold commutator:*

$$[r_1, r_2, \ldots, r_{k-1}, st] = [r_1, r_2, \ldots, r_{k-1}, s] \cdot [r_1, r_2, \ldots, r_{k-1}, t] \ ;$$

$$[r_1, r_2, \ldots, r_{k-2}, st, r_k] = [r_1, r_2, \ldots, r_{k-2}, s, r_k] \cdot [r_1, r_2, \ldots, r_{k-2}, t, r_k].$$

Proof. Here are some basic identities about commutators that hold in all groups:

$$[x, yz] = [x, y] \cdot [y, [x, z]] \cdot [x, z], \tag{1}$$

$$[xy, z] = [x, [y, z]] \cdot [y, z] \cdot [x, z]. \tag{2}$$

Now let $R = [r_1, \ldots, r_{k-1}] \in G_{k-1}$, and we must show that $[R, st] = [R, s] \cdot [R, t]$. We have $[R, st] = [R, s] \cdot [s, [R, t]] \cdot [R, t]$ by (1), and the middle term is trivial because $[G_1, [G_{k-1}, G_1]] \subset G_{k+1} = 1$. That proves the first identity asserted in the lemma.

Now, letting $R = [r_1, \ldots, r_{k-2}] \in G_{k-2}$, we must show that $[R, st, r] = [R, s, r] \cdot [R, t, r]$. By (1), $[R, st] = [R, s] \cdot [s, [R, t]] \cdot [R, t]$. Now let $x = [R, s]$ and $y = [s, [R, t]] \cdot [R, t]$. Then $[R, st, r] = [xy, r] = [x, [y, r]] \cdot [y, r] \cdot [x, r]$ by (2). But $[x, [y, r]] \in [G_{k-1}, G_2] = 1$, so we have shown that $[R, st, r] = [y, r] \cdot [x, r]$. But our y is itself a product, so we can expand $[y, r]$ with (2), obtaining three terms, the only surviving one being $[R, t, r]$. Since we already know $[x, r] = [R, s, r]$, and since G_k is abelian, we have shown that $[R, st, r] = [R, s, r] \cdot [R, t, r]$. □

Proposition 6. $\mathcal{EP}$ *is undecidable in each $N(p,q)$ with $p \geq 3$.*

Proof. Let y_j be variables in $G = N(p,q)$ with $p \geq 3$, and let a, b be two of the generators of G in the standard presentation. Let $R = [a, b, b, \ldots, b] \in G_{p-2}$, so that $R = a$ if $p = 3$. We will show that the system Σ whose i^{th} equation is

$$\Sigma_i : [R, b, b]^{\alpha_i} \cdot \prod_j [R, b, y_j]^{\beta_{ij}} \cdot \prod_{j,k} [R, y_j, y_k]^{\gamma_{ijk}} = 1$$

has a solution in G if and only if the system $\hat{\Sigma}$ whose i^{th} equation is

$$\hat{\Sigma}_i : \alpha_i + \sum_j \beta_{ij} x_j + \sum_{j,k} \gamma_{ijk} x_j x_k = 0$$

has a solution in $\mathbb{Z}$.

If the standard generators of G are $a, b, c_3, \ldots, c_q$, then we can write $y_j = a^{A_j} b^{B_j} (\prod_{l=3}^{q} {c_l}^{C_{lj}}) h$ for some $h \in G_2$. Let us also write $f = [R, b, a]$ and $g = [R, b, b]$, so that these are among the many basic generators of G_k, which is a free abelian group. We note that $[R, b, y_j] = f^{A_j} g^{B_j} \prod [a, b, c_l]^{C_{lj}}$, because $[R, b, q] \in [G_{k-1}, G_2] = 1$. Similarly

$$[R, y_j, y_k] = f^{B_j A_k} g^{B_j B_k} \cdot \prod_l [R, b, c_l]^{B_j C_{lk}} \cdot \prod_{l,m} [R, c_l, c_m]^{C_{lj} C_{mk}}.$$

Since G_k is free abelian, a word spelled in its basis elements is trivial if and only if all exponents are zero. The exponent of f in Σ_i is $\sum_j \beta_{ij} A_j + \sum_{j,k} \gamma_{ijk} B_j A_k$. The exponent of g in Σ_i is $\alpha_i + \sum_j \beta_{ij} B_j + \sum_{j,k} \gamma_{ijk} B_j B_k$. The exponents of all other generators of G_k are quadratic polynomials in which every term contains some C_{ls}. We note that the expression coming from the exponent of g is the quadratic polynomial $\hat{\Sigma}_i$.

A solution to Σ in G would produce a solution to $\hat{\Sigma}$ in $\mathbb{Z}$ by letting $x_j = B_j$; conversely, a solution to $\hat{\Sigma}$ could be converted to a solution to Σ by letting $B_j = x_j$ while all of the A and C values are set to zero. □

Combining Theorem 4 ($p = 2$) and Proposition 6 ($p \geq 3$), we have shown that

Theorem 7. *For each non-abelian free nilpotent group $N(p, q)$, $\mathcal{EP}$ is undecidable.*

3.2. $\mathcal{EP}_1$ **in step** ≥ 3**.** We will quickly remark on the closely related argument for undecidability of $\mathcal{EP}_1$ in high rank. Truss showed that in the countable-rank group $N(3, \infty)$, one could label all of the generators in pairs as $a_1, b_1, a_2, b_2, \ldots$, and then use a single equation

$$\prod_i \left([a_i, b_i, b_i]^{\alpha_i} \prod_j [a_i, b_i, y_j]^{\beta_{ij}} \prod_{j,k} [a_i, y_j, y_k]^{\gamma_{ijk}} \prod_{j \neq i} [a_i, b_j, y'_{ij}] \cdot [a_i, y''_{ij}, b_j] \right) = 1$$

to encode a system of diophantine equations indexed by i. Here, the relationship of the diophantine solutions to the group-theoretic solutions will be given by $y_j = \prod_\ell b_\ell^{x_j}$, where the y' and y'' take whatever values are needed to cancel the commutators of the form $[a_i, b_j, b_k]$ that do *not* have matching indices $i = j = k$. We note that the values of these variables are uniquely determined because all three-term commutators are central. The effect of this is that the exponent of $[a_i, b_i, b_i]$ encodes the i^{th} equation from the diophantine system.

We simply observe that high rank suffices rather than countable rank, just because there are undecidable systems of finite (definite) size, and the needed rank is simply twice the number of equations in the system. Furthermore, this readily extends to step greater than three by once again replacing $[a_i, b_i, b_i]$ with longer commutators $[a_i, b_i, b_i, \ldots, b_i]$ and similarly lengthening the other terms, as we did above.

Proposition 8. *$\mathcal{EP}_1$ is undecidable in each $N(p, q)$ where $p \geq 3$ and q is sufficiently large.*

Acknowledgments

The authors would like to thank Bjorn Poonen, Martin Davis, François Dorais, and especially Pete Clark for helpful explanations of the number theory and logic connections, and V. Roman'kov for explaining his earlier work. The authors are also grateful to the anonymous referee.

References

[1] E. K. Burke and J. K. Truss, *Unification for nilpotent groups of class* 2, Forum Math. **7** (1995), no. 4, 435–457, DOI 10.1515/form.1995.7.435. MR1337148 (96g:20046)

[2] François Dahmani and Vincent Guirardel, *Foliations for solving equations in groups: free, virtually free, and hyperbolic groups*, J. Topol. **3** (2010), no. 2, 343–404, DOI 10.1112/jtopol/jtq010. MR2651364 (2012a:20069)

[3] V. G. Durnev, *Unsolvability of the problem of endomorphic reducibility for sets of elements of a free nilpotent group of rank* 2 (Russian), Problems in group theory and homological algebra (Russian), Matematika, Yaroslav. Gos. Univ., Yaroslavl′, 1988, pp. 88–93. MR1174997

[4] Ju. L. Eršov, *Elementary group theories* (Russian), Dokl. Akad. Nauk SSSR **203** (1972), 1240–1243. MR0297840 (45 #6892)

[5] Roger C. Lyndon, *Equations in groups*, Bol. Soc. Brasil. Mat. **11** (1980), no. 1, 79–102, DOI 10.1007/BF02584882. MR607019 (82j:20070)

[6] Bjorn Poonen, *Undecidability in number theory*, Notices Amer. Math. Soc. **55** (2008), no. 3, 344–350. MR2382821 (2008m:11238)

[7] N. N. Repin, *Solvability of equations with one indeterminate in nilpotent groups* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984), no. 6, 1295–1313. MR772117 (86d:20040)

[8] V. A. Roman′kov, *Universal theory of nilpotent groups* (Russian), Mat. Zametki **25** (1979), no. 4, 487–495, 635. MR534291 (80j:03058)

[9] Vitaliĭ Roman'kov, *Equations over groups*, Groups Complex. Cryptol. **4** (2012), no. 2, 191–239, DOI 10.1515/gcc-2012-0015. MR3043434

[10] Carl Ludwig Siegel, *Zur Theorie der quadratischen Formen* (German), Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1972), 21–46. MR0311578 (47 #140)

[11] R. J. Stroeker and N. Tzanakis, *Computing all integer solutions of a genus 1 equation*, Math. Comp. **72** (2003), no. 244, 1917–1933, DOI 10.1090/S0025-5718-03-01497-2. MR1986812 (2004b:11037)

[12] J. K. Truss, *Equation-solving in free nilpotent groups of class* 2 *and* 3, Bull. London Math. Soc. **27** (1995), no. 1, 39–45, DOI 10.1112/blms/27.1.39. MR1331679 (96f:20052)

Department of Mathematics, Tufts University, Medford, Massachusetts 02155
E-mail address: Moon.Duchin@tufts.edu

Department of Mathematics, Tufts University, Medford, Massachusetts 02155
E-mail address: Hao.Liang@tufts.edu

Department of Mathematics, Tufts University, Medford, Massachusetts 02155
E-mail address: Michael.Shapiro@tufts.edu