MATHEMATICS OF COMPUTATION
Volume 89, Number 325, September 2020, Pages 2507–2519
https://doi.org/10.1090/mcom/3533
Article electronically published on April 16, 2020

THE DIOPHANTINE PROBLEM IN SOME METABELIAN GROUPS

OLGA KHARLAMPOVICH, LAURA LÓPEZ, AND ALEXEI MYASNIKOV

Abstract. In this paper we show that the Diophantine problem in solvable Baumslag–Solitar groups $BS(1,k)$ and in wreath products $A \wr \mathbb{Z}$, where A is a finitely generated abelian group and $\mathbb{Z}$ is an infinite cyclic group, is decidable, i.e., there is an algorithm that, given a finite system of equations with constants in such a group, decides whether or not the system has a solution in the group.

1. Introduction

The problem of solving equations in various classes of groups and monoids has been an active research field for many years now. The first general results on equations in groups appeared in the 1960s in the works of Lyndon [10] and Mal′cev [11]. In the 1970s Makanin [12, 13] proved the solvability of (systems of) equations for free monoids and free groups. Makanin's decidability results have been extended to hyperbolic groups and right-angled Artin groups [3], and it was shown that certain group operations (graph products [2], HNN-extensions, and amalgamated products over finite groups) preserve decidability [9]. Moreover, significant progress concerning the computational complexity and the structure of solution sets have been obtained in recent years. On the negative side, by the Ershov–Romanovskiĭ–Noskov result the first-order theory of a finitely generated solvable group is decidable if and only if the group is virtually abelian. The corresponding problem has been posed in [8]. Eršhov proved this statement [5] in the nilpotent case, Romanovskiĭ [18] generalized it to the polycyclic case, and, finally, Noskov [14] established the most general statement for the case of a finitely generated solvable group. Denote by $\mathcal{EP}_1$ the problem of solvability of one equation. Roman'kov showed that $\mathcal{EP}_1$ is undecidable even for the subclass of all split equations of the form $w(x_1, \dots, x_n) = g$, where $w(x_1, \dots, x_n)$ is a coefficient-free word and g is an element of the underlying group G that is a free nilpotent of class ≥ 9 [16] (this bound was later reduced to ≥ 4 in [17]) or G is a free metabelian nonabelian group [17]. In [4] the authors proved that $\mathcal{EP}_1$ is decidable in the Heisenberg group that is free nilpotent of rank 2 and class 2. But the Diophantine problem (denoted by $\mathcal{EP}$ in [4]) is undecidable in any nonabelian free nilpotent group.

In this paper we show that the Diophantine problem in solvable Baumslag–Solitar groups $BS(1,k)$ and in wreath products $A \wr \mathbb{Z}$, where A is a finitely generated abelian group and $\mathbb{Z}$ is an infinite cyclic group, is decidable, i.e., there is an algorithm that,

Received by the editor July 28, 2019, and, in revised form, October 31, 2019, and January 11, 2020.

2010 *Mathematics Subject Classification.* Primary 20F16, 20F70.

The first author gratefully acknowledges support over the years by grant 422503 from the Simons Foundation.

given a finite system of equations with constants in such a group, decides whether or not the system has a solution in the group.

The metabelian Baumslag–Solitar groups are defined by one-relator presentations $BS(1,k) = \langle a, b \mid b^{-1}ab = a^k \rangle$, where $k \in \mathbb{N}$. If $k = 1$, then $BS(1,1)$ is free abelian of rank 2, so the Diophantine problem in this group is decidable (it reduces to solving finite systems of linear equations over the ring of integers $\mathbb{Z}$). Furthermore, the first-order theory of $BS(1,1)$ is also decidable [20]. However, if $k \geq 2$, then $BS(1,k)$ is metabelain which is not virtually abelian, so the first-order theory of $BS(1,k)$ is undecidable by [14]. As we mentioned above, in free metabelian nonabelian groups equations are undecidable [17]. In fact, in a finitely generated metabelian group G given by a finite presentation in the variety $\mathcal{M}_2$ of metabelian groups, the Diophantine problem is undecidable asymptotically almost surely if the deficiency of the presentation is at least 2 [6].

In general, if the quotient $G/\gamma_3(G)$ of a finitely generated metabelian group G by its third term of the lower central series is a nonvirtually abelian nilpotent group, then the decidability of the Diophantine problem in G would imply the decidability of the Diophantine problem for some finitely generated ring of algebraic integers O_G associated with $G/\gamma_3(G)$. The latter seems unlikely, since there is a well-known conjecture in number theory (see, for example, [1, 15]) that states that the Diophantine problem in rings of algebraic integers is undecidable. The discussion above shows that finitely generated metabelian groups G with virtually abelian quotients $G/\gamma_3(G)$ present an especially interesting case in the study of equations in metabelian groups. The groups $BS(1,k)$ and wreath products $A \wr \mathbb{Z}$, where A is a finitely generated abelian group and $\mathbb{Z}$ is an infinite cyclic group, are the typical examples of such groups. They provide first examples of nonvirtually abelian finitely generated metabelian groups with decidable Diophantine problem. This also gives a new look at one-relator groups. The groups $BS(1,k)$, $k \geq 2$, were until recently the only known examples of one-relator groups with undecidable first-order theory. Recently, we were able to show (still unpublished) that any one-relator group containing nonabelian group $BS(1,k)$ has undecidable first-order theory. However, it is quite possible that equations in such groups are still decidable.

2. Equations in $BS(1,k)$

Our first main result is the following theorem.

Theorem 1. *Equations in $BS(1,k)$ are decidable.*

To prove the theorem we have to construct an algorithm that decides whether the set of formulas of the form $\exists \bar{x} \bigwedge_{i=1}^{s} t_i(\bar{x}, a, b) = 1$ is decidable, where $t_i(\bar{x}, a, b)$ is a group word in the alphabet $\bar{x}, a, b$. Recall that the group $BS(1,k)$ is isomorphic to the group $\mathbb{Z}[1/k] \rtimes \mathbb{Z}$, where $\mathbb{Z}[1/k] \cong ncl(a)$ and $\mathbb{Z} \cong \langle b \rangle$, where

$$\mathbb{Z}[1/k] = \{zk^{-i}, z \in \mathbb{Z}, i \in \mathbb{N}\}$$

and the action of $\langle b \rangle$ is given by $b^{-1}ub = u^k$. Thus, we can think of elements in $BS(1,k)$ as pairs (zk^{-i}, r) where $z, r, i \in \mathbb{Z}$. The product is defined as

$$(z_1k^{-i_1}, r_1)(z_2k^{-i_2}, r_2) = (z_1k^{-i_1} + z_2k^{-(i_2+r_1)}, r_1 + r_2).$$

The inverse of an element (zk^{-y}, r) is $(-zk^{-(y-r)}, -r)$.

The following lemma reduces systems of equations in $BS(1,k)$ to systems of equations in $\mathbb{Z}$.

Lemma 1. *Any finite system of equations in $BS(1,k)$ is equivalent to a finite system of equations of the form*

$$\sum_i z_i k^{-y_i}\Big(\sum_j \pm k^{\tau_{ij}(\bar{r})}\Big) - \sum_t \gamma_t k^{\tau_t(\bar{r})} = 0 \tag{1}$$

and

$$\sum \beta_j r_j = \delta, \tag{2}$$

where $\tau_t(\bar{r}), \tau_{ij}(\bar{r}) = \sum_q \alpha_q r_q + c_q$ and where $\alpha_q, c_q, \delta, \gamma_t, \beta_j \in \mathbb{Z}$, and y_i, z_i, r_i, are variables.

The product $z_i k^{-y_i}$ can also be considered as a one variable in $\mathbb{Z}[1/k]$.

Proof. Note that

$$\begin{aligned}&(z_1 k^{-y_1}, r_1)\cdot(z_2 k^{-y_2}, r_2)\cdots(z_n k^{-y_n}, r_n)\\ &= (z_1 k^{-y_1} + z_2 k^{-(y_2+r_1)} + \cdots + z_n k^{-(y_n+r_1+\cdots+r_{n-1})}, r_1+\cdots+r_n).\end{aligned}$$

The system of equations in the first and second component corresponds to a system of equations of the form (1) and (2), respectively. □

To solve a system of equations in $BS(1,k)$, we begin by solving system (2). This system is just a linear system of equations $AX = B$ with integer coefficients, where $X = (r_1, \ldots, r_n)^T$ and A is the matrix of the system. Using integral elementary column operations on A and row operations on $(A|B)$ we can obtain an equivalent system $\bar{A}\bar{X} = \bar{B}$ such that $\bar{A}$ has a diagonal form. This is Smith normal form. Column operations on A correspond to a change of variables. Row operations on $(A|B)$ correspond to transformations of the system of equations into an equivalent system. If the system $\bar{A}\bar{X} = \bar{B}$ does not have a solution, then the corresponding system of equations in the group does not have a solution. If the system $\bar{A}\bar{X} = \bar{B}$ is solvable, then we change variables X to $\bar{X}$. Some of the new variables $\bar{X}$ will have fixed integer values and some will be arbitrary integers. Substitute those $\bar{X}$'s into system (1). We only have to check that there exist integer solutions $Z = \{z_1, \ldots, z_n\}$, $Y = \{y_1, \ldots, y_n\}$ and remaining $\bar{X}$ that we denote $\hat{X} = \{r_{i_1}, \ldots, r_{i_m}\}$.

We say that a system of equations $S(X) = 0$ with variables X is equivalent to a disjunction of systems $S_1(X) = 0, \ldots, S_m(X) = 0$ if every solution of $S(X) = 1$ is a solution of one of $S_i(X) = 0, i = 1, \ldots, m$, and every solution of $S_i(X) = 0$ is a solution of $S(X) = 0$. One can consider system (1) as a linear system with variables $z_i k^{-y_i}$, and linear combinations of exponential functions as coefficients (which contain variables $\hat{X}$). It can be transformed using row operations to an equivalent disjunction of triangular-like systems (with respect to variables $z_s k^{-y_s}$, $s = 1, \ldots, q$) of the following form:

$$z_s k^{-y_s}\Big(\sum_j \delta_{sj} k^{\tau_{sj}(\bar{r})}\Big) = \sum_{i>q} z_i k^{-y_i}\Big(\sum_j \delta_{ij} k^{\sigma_{ij}(\bar{r})}\Big) + \sum_t \gamma_t k^{\tau_t(\bar{r})}, s = 1, \ldots, q, \tag{3}$$

$$\sum_j a_j k^{\phi_j(\bar{r})} = 0 \text{ (system of such equations)}, \tag{4}$$

where $\delta_{sj}, \delta_{ij}, \gamma_t, a_j \in \mathbb{Z}$ and $\tau_{sj}, \sigma_{ij}, \tau_t, \phi_j$ are linear combinations of elements in $\hat{X}$ and constants. We will get a disjunction of systems because when multiplying equations by some coefficient we have to separately consider the case when this coefficient is zero.

Now we have to solve systems (3) and (4). We will first find all solutions of system (4). Semenov's ideas in [19] (where he proved that the theory of $\langle \mathbb{Z}, +, k^x \rangle$ is decidable) can be used to prove the following lemma.

Lemma 2. *Any system of equations over $\mathbb{Z}$ of the form*

$$F(\bar{y}) = \sum_j \beta_j k^{y_j} + C = 0, \tag{5}$$

where $\beta_j \in \mathbb{Z}$, $k \in \mathbb{N}, k > 1$, with variables $\bar{y} = (y_1, \dots, y_n)$, is equivalent to a disjunction of linear systems of equations over $\mathbb{Z}$.

Proof. Let $\bar{y} = (y_1, \dots, y_n)$, and let $\lambda : \{y_1, \dots, y_n\} \to \{+, -\}$ be a map that assigns to each variable a positive or negative sign (the agreement will be that zero has a positive sign). System (5) over $\mathbb{Z}$ is equivalent to a disjunction of 2^n systems each with an assignment λ. Now we fix one of these systems and we show how to describe all solutions.

We begin by rewriting each equation so that all variables are positive. We may do this by substituting in each equation $-y_i$ for y_i, for each y_i that has a negative assignment. Then we multiply each equation by $k^{y_{i_1}+\dots+y_{i_s}}$, where $y_{i_1}, \dots, y_{i_s}$ are all the variables whose signs were changed. For instance, suppose we have an equation $k^{y_1} - k^{y_2} + k^{y_3} + c = 0$ with assignment $y_1 < 0, y_2 \geq 0, y_3 \geq 0$. Then we rewrite it as $k^{-y_1} - k^{y_2} + k^{y_3} + c = 0$ with assignment $y_1 \geq 0, y_2 \geq 0, y_3 \geq 0$ and multiply the equation by k^{y_1}. We then obtain the equation

$$1 - k^{y_1+y_2} + k^{y_1+y_3} + ck^{y_1} = 0$$

with assignment $y_1 \geq 0, y_2 \geq 0, y_3 \geq 0$. We now obtain a system over $\mathbb{N}$ of the form

$$\sum_i \beta_i k^{\sum_j y_{ij}} + C = 0.$$

Next, we substitute all sums in exponents of k by new variables to obtain a system of equations over $\mathbb{N}$ of the form

$$F'(\bar{y}) = \sum_i \beta_i k^{\hat{y}_i} + C = 0. \tag{6}$$

Claim. A finite system of equations in the form (6) is equivalent to a disjunction of systems of linear equations of the form $\{\hat{y}_1 = \hat{y}_2 + c_1, \hat{y}_2 = \hat{y}_3 + c_2, \dots, \hat{y}_{s-1} = \hat{y}_s + c_s\}$.

Proof. Denote the new variables as $\bar{y}' = (\hat{y}_1, \dots, \hat{y}_m)$. We begin by showing that for each i, there is a $\Delta_i \in \mathbb{N}$ such that system (6) does not have a solution if $\hat{y}_i > \hat{y}_j + \Delta_i$ for all $j \neq i$.

Fix i. We can rewrite each equation in the system in the form $k^{\hat{y}} + \sum_i \gamma_i k^{\hat{x}_i} = \sum_j \delta_j k^{\hat{z}_j} + C$, where all γ_i, δ_j are positive integers, $\hat{y} = \hat{y}_i$, and $\hat{x}_i, \hat{z}_j$ are all variables in $\bar{y}' - \hat{y}_i$. For each equation, let $\Delta > \log_k(\sum_j \delta_j + C)$ if $C \geq 0$ and $\Delta > \log_k(\sum_j \delta_j)$ if $C < 0$, and $\hat{y} > \hat{x}_i + \Delta$ and $\hat{y} > \hat{z}_j + \Delta$ for all i, j. Then $k^{\hat{y}} > k^{\Delta} k^{\hat{z}_j} > (\sum_j \delta_j + C) k^{\hat{z}_j}$ for all j. Thus, the right side of the equation will always be smaller than the left side, and the equation has no solution. Thus, we can take Δ_i to be the smallest such Δ.

So we have shown that for all variables $\hat{y}_i$, if F' (or a finite system of equations where each equation has form F') has a solution, then there is a $j \neq i$ such that $\hat{y}_i \leq \hat{y}_j + \Delta_i$. Now consider a finite graph $\mathcal{G}$ with n vertices labeled $\hat{y}_1, \dots, \hat{y}_m$ and

directed edges from $\hat{y}_i$ to $\hat{y}_j$ whenever $\hat{y}_i \leq \hat{y}_j + \Delta_i$. Note that each vertex must be the initial vertex of some edge and thus the graph must contain a cycle in every connected component. Suppose there is a cycle $\hat{y}_{i_1}, \ldots, \hat{y}_{i_s} = \hat{y}_{i_1}$, $s \leq m+1$. Then

$$\hat{y}_{i_1} \leq \hat{y}_{i_2} + \Delta_{i_1} \leq \hat{y}_{i_3} + \Delta_{i_2} + \Delta_{i_1} \leq \cdots \leq \hat{y}_{i_s} + \Delta_{i_{(s-1)}} + \cdots + \Delta_{i_1}$$
$$= \hat{y}_{i_1} + \Delta_{i_{(s-1)}} + \cdots + \Delta_{i_1}.$$

Therefore for any $2 \leq j \leq s-1$, we have that

$$\hat{y}_{i_1} - \sum_{t=1}^{j-1} \Delta_{i_t} \leq \hat{y}_{i_j} \leq \hat{y}_{i_1} + \sum_{t=j}^{s-1} \Delta_{i_t}.$$

Therefore, the value of any $\hat{y}_{i_j}$ with $2 \leq j \leq s-1$ is bounded by the value of $\hat{y}_{i_1}$.

Fix a y_{i_j}, and let $\Delta_{j_1} = \sum_{t=1}^{j-1} \Delta_{i_t}$ and $\Delta_{j_2} = \sum_{t=j}^{m-1} \Delta_{i_t}$. Then we may replace the equation $F'(\bar{y})$ by a disjunction of equations $G(\bar{y} \backslash \hat{y}_{i_j})$ where G is the same as the formula F', but $\hat{y}_{i_j}$ is replaced by $\hat{y}_{i_1} - \Delta_{j_1}$ in one equation, $y_{i_1} - \Delta_{j_1} + 1$ in the next, and so on until $y_{i_1} + \Delta_{j_2}$.

Now we may eliminate variables from each equation in m variables inductively, obtaining at each step a new disjunction consisting of a system of equations in less variables and a set of linear equations of the form $\hat{y}_i = \hat{y}_j + c_i$ which we use to eliminate one variable. At the last level of each branch of this procedure, we will have one of three possible outcomes:

(1) All exponential terms have canceled out and we have a false equation with constant terms. In this case there is no solution to (6) or (5) in this branch.
(2) There is an equation $0 = 0$ (i.e., all terms cancel out after a substitution). In this case all variables (after renumbering) $\hat{y}_{i+1}, \ldots, \hat{y}_m$ that remained in the previous step of the branch are taken as free variables, and we obtain a general solution $\hat{y}_1 = \hat{y}_2 + c_1, \hat{y}_2 = \hat{y}_3 + c_2, \ldots, \hat{y}_i = \hat{y}_{i+1} + c_i$ to system (6) along this branch.
(3) There is one equation left of the form $\beta_s k^{y_s} + C = 0$. In this case, this equation has a unique solution $y_s = b$ or has no solution.

In the second case, any solution in $\mathbb{Z}$ of the linear system $\hat{y}_1 = \hat{y}_2 + c_1, \hat{y}_2 = \hat{y}_3 + c_2, \ldots, \hat{y}_i = \hat{y}_{i+1} + c_i$ will be a solution to system (6) since when we substitute the variables into this equation, the same cancellations will occur and we will remain with the equation $0 = 0$. This proves the claim. □

System (5) can also be reduced to a disjunction of linear systems by substituting each $\hat{y}_i$ back to the corresponding linear combination of $y_1, \ldots, y_n$. This completes the proof of the lemma. □

System (4) is also equivalent to a disjunction of linear systems—we first replace sums appearing in the exponent of k by new variables and then apply Lemma 2. We now solve this disjunction of linear systems—if it is solvable, the general solution will correspond to the disjunction of systems of linear equations on $\hat{X}$. We fix one of these systems and substitute those r_i's that are fixed numbers into system (3) that has triangular form. Denote the new tuple of r_i's by $\tilde{X}$. We now describe two procedures: the first will stop if it finds a solution to (3), the second will stop if there is no solution.

Procedure 1. If an integer solution to the system (3) exists, we can find it by enumerating all integer values of $\tilde{X}, Y, Z$.

Now we will justify the second procedure. We can assume all $y \in Y$ are nonnegative. Splitting into several cases as before, we can also assume that all $r \in \tilde{X}$ are nonnegative. Then system (3) is equivalent to a disjunction of systems

$$z_s k^{-y_s}\Big(\sum_j \delta_{sj} k^{\tau_{sj}(\bar{r})}\Big) = \sum_{i>q} z_i k^{-y_i}\Big(\sum_j \delta_{ij} k^{\sigma_{ij}(\bar{r})}\Big) + \sum_t \gamma_t k^{\tau_t(\bar{r})}, \tag{7}$$

where $s = 1, \dots, q$; $y_j, r_j \in \mathbb{N}$, τ_{sj}, σ_{ij} are linear combinations of elements in $\tilde{X}$ and constants, and $\delta_{is}, \delta_{ij}, \gamma_t \in \mathbb{Z}$.

Lemma 3. *Equation $zk^{-y}A = B$, where $A, B \in \mathbb{Z}$ has a solution in $\mathbb{Z}$ if and only if for any prime power p^m with p not dividing k, equation $zA = k^y B$ has a solution modulo p^m.*

Proof. If equation $zA = k^y B$ has a solution in $\mathbb{Z}$, then it has a solution modulo p^m for any p not dividing k.

Suppose that equation $zA = k^y B$ has a solution modulo p^m for any p not dividing k. Then every prime power p^m not dividing k, that divides A, also divides B. We can represent $A = A_1 A_2$, where A_1 is the maximal factor relatively prime with k, and let A_3 be such that $A_2 A_3 = k^a$ for some $a \in \mathbb{N}$. Then $zk^{-y} = B/(A_1 A_2) = k^{-a} B A_3 / A_1$ and A_1 divides B. Therefore the equation has a solution in $\mathbb{Z}$. □

Notice that we can multiply each equation of (7) by $k^{y_s + \sum_{i>q} y_i}$ and not have negative powers of k. Denote this equivalent system by (7′).

Lemma 4. *There is an integer solution to system (7) if and only if there are values for the variables $\tilde{X} \cup \{z_i, y_i | i > q\}$, for which the system obtained from system (7′) after substituting these values for variables in $\tilde{X} \cup \{z_i, y_i | i > q\}$ has a solution modulo any prime power p^m for any prime number p not dividing k, and any natural m.*

Proof. If there is an integer solution to system (7), then there is a solution modulo p^m for any prime number p not dividing k and any natural m.

Suppose there are values for the variables $\tilde{X} \cup \{z_i, y_i | i > q\}$, for which the system obtained from (7) after substituting these values for variables in $\tilde{X} \cup \{z_i, y_i | i > q\}$ has a solution modulo any prime power p^m for any prime number p not dividing k. After we substitute these values, each equation of the system will have the form as in Lemma 3. Also by Lemma 3 system (7) has an integer solution. □

Lemma 5. *If a prime p does not divide a positive natural number k, then the function k^y, $y \in \mathbb{N}$, is periodic modulo p^m with some period P, namely $k^P \equiv 1 \pmod{p^m}$.*

Proof. One can compute all possible values of k^y modulo p^m. Suppose these are $V = \{1, \dots, q\}$. Therefore there are different numbers $P_1 < P_2$ such that $k^{P_1} \equiv k^{P_2} \pmod{p^m}$. Hence $k^{P_1}(k^{P_2 - P_1} - 1) \equiv 0 \pmod{p^m}$. Since p does not divide k, $k^{P_2 - P_1} \equiv 1 \pmod{p^m}$. This implies that the function k^y, $y \in \mathbb{N}$, is periodic modulo p^m with some period P. □

We can now describe the second procedure.

Procedure 2. The procedure first enumerates all prime powers p^m not dividing k.

Each step of the procedure corresponds to a fixed prime power p^m. Let all values of k^y modulo p^m be $V = \{1, \dots, q\}$. We go through each equation in system (7′),

substituting each term k^y, k^r by a value in V and each variable z_i by a value in $\{0, \dots, p^m - 1\}$. Note that this is a finite process since there are finitely many possible solutions and a finite number of systems. If none of the systems has a solution, then system (7) does not have a solution. If some of the assignments for $\tilde{X}, Y, Z$ give a solution, then for each such assignment we rewrite the variables $\tilde{X}$ in the form $r_i = \hat{r}_i + P\bar{r}_i$, where $\hat{r}_i \in V$, variables $y_i, i > q$, in the form $y_i = a_i + P\bar{y}_i$, $0 \le a_i < P$, and $z_i, i > q$, in the form $z_i = b_i + p^m \bar{z}_i, 0 \le b_i < p^m$. This restricts their domains when considering prime powers on the following steps of the procedure. Variables $\tilde{X} = \{r_i\}$ we can substitute into linear combinations $\tau_{sj}, \sigma_{ij}, \tau_t$ and get new linear combinations in variables $\{\bar{r}_i\}$. Variables $\{z_i, y_i | i > q\}$ we take in the form $y_i = a_i + P\bar{y}_i$, $z_i = b_i + p^m \bar{z}_i$, plug them into system, and continue to test the next prime power $\bar{p}^{\bar{m}}$ obtaining similar restrictions on $\bar{y}_i, \bar{z}_i$. The restrictions on the domains of $\tilde{X} \cup \{z_i, y_i | i > q\}$ guarantee that when considering the prime powers on the subsequent steps of the procedure, we only consider those values of $\tilde{X} \cup \{z_i, y_i | i > q\}$ for which system (7′) has a solution modulo p^m for all previously considered prime powers p^m.

On each step of the second procedure we obtain a disjunction of possible domains for variables $\tilde{X} \cup \{z_i, y_i | i > q\}$, therefore we have a branching process. If system (7) does not have a solution the second procedure stops along all the branches.

3. Restricted wreath products with $\mathbb{Z}$

The restricted wreath product $G \wr \mathbb{Z}$ is isomorphic to the semidirect product $\bigoplus_{i\in\mathbb{Z}} G \rtimes \mathbb{Z}$, where the action of $\mathbb{Z}$ on $\bigoplus_{i\in\mathbb{Z}} G$ is by translation of indices, that is, $k \cdot \{g_n\}_{n\in\mathbb{Z}} = \{g_{n+k}\}_{n\in\mathbb{Z}}$. The product of two elements $(\{g_n\}_{n\in\mathbb{Z}}, k) \cdot (\{h_n\}_{n\in\mathbb{Z}}, l)$ is $(\{g_n + h_{n+k}\}_{n\in\mathbb{Z}}, k+l)$. When $G = \mathbb{Z}_2$ the group is called the lamplighter group.

If A is finitely generated abelian, then $A = \mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ as an additive group. Denote by R the ring $\mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$. In this case $A \wr \mathbb{Z}$ is isomorphic to the group of matrices of the form

$$M = \begin{pmatrix} t^x & P \\ 0 & 1 \end{pmatrix},$$

where P is a Laurent polynomial in $R[t, t^{-1}]$. Note that $P = f(t)t^{-k}$ where $f(t) \in R[t]$ and $k \in \mathbb{N}$.

We will first show that equations in $A \wr \mathbb{Z}$ are decidable for $A = \mathbb{Z}_n$ and $A = \mathbb{Z}$. We will denote $\mathbb{Z}_n \wr \mathbb{Z}$ by L_n and $\mathbb{Z} \wr \mathbb{Z}$ by L.

Theorem 2. *Equations in L_n are decidable.*

Proof. The product of n elements in L_n is

$$\begin{pmatrix} t^{x_1} & P_1 \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} t^{x_n} & P_n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} t^{x_1+\cdots+x_n} & Q \\ 0 & 1 \end{pmatrix},$$

where $P_j = f_j(t)t^{-y_j}$ and

$$Q = f_n(t)t^{-y_n}t^{x_1+\cdots+x_{n-1}} + f_{n-1}(t)t^{-y_{n-1}}t^{x_1+\cdots+x_{n-2}} + \cdots + f_1(t)t^{-y_1}.$$

In a system of equations in L_n, some of the $x_i, f_j(t)$, and y_j may be constants and some may be variables.

Thus, any system of equations in L_n is equivalent to a system of equations of the form

$$F_1(\bar{x}, t, t^{-1})f_1(t)t^{-y_1} + \cdots + F_m(\bar{x}, t, t^{-1})f_m(t)t^{-y_m} = P(\bar{x}, t, t^{-1}) \tag{8}$$

and

$$\sum_i c_i x_i + C = 0, \tag{9}$$

where $F_j(\bar{x}, t, t^{-1}) = \sum_i \alpha_i t^{\sigma_i(\bar{x})}$ where $\alpha_i = \pm 1$, and $\sigma_i(\bar{x})$ is a linear combination of elements in x and a constant, and $f_j(t)$ is a variable that runs over $\mathbb{Z}_n[t]$, y_j is a variable that runs over $\mathbb{N}$, $P(\bar{x}, t, t^{-1})$ is a polynomial in $\mathbb{Z}_n[t, t^{-1}]$ with linear combinations of $\bar{x}$ in the exponents of t and c_i, and $C \in \mathbb{Z}$.

We begin by solving the linear system (9) as in Section 2. If the system does not have a solution, then system (8) will not have a solution either. If the system has a solution, then we substitute those values of x_i into system (8). Some x_i will be replaced by integers, others by linear combinations of elements in $\bar{x}$ and constants.

Now we solve system (8). This system can be put in Smith normal form by regarding the terms $f_j(t)t^{-y_j}$ as variables, the terms $F_j(\bar{x}, t, t^{-1})$ as coefficients, and $P(\bar{x}, t, t^{-1})$ as a constant coefficient.

Thus, the system is equivalent to a disjunction of systems of the form

$$F'_s(\bar{x}, t, t^{-1}) f_s(t) t^{-y_s} = \sum_{i>q} F'_{s_i}(\bar{x}, t, t^{-1}) f_i(t) t^{-y_i} + P'_s(\bar{x}, t, t^{-1}) \tag{10}$$

for $s = 1, \ldots, q$, and

$$\sum_i a_i t^{\sigma_i(\bar{x}, d_i)} = 0, \tag{11}$$

where $a_i, \in \mathbb{Z}_n$ and $\sigma_i(\bar{x}, d_i)$ is a linear combination of elements in $\bar{x}$ with constants.

To solve system (11), we begin by grouping terms in each equation such that the sum of the coefficients of each group is zero modulo n. If there is no way to group each equation in the system in this way, then this system does not have a solution. For, suppose there is a solution to system (11). Then after substituting the solution in each equation and simplifying, the coefficients of each t^i should be zero in each equation, and thus the sum of the coefficients of t^i before simplifying must be zero modulo n.

There may be many ways to group the terms of each equation. We fix one system after grouping and for each equation, we set the powers of t in the terms that were grouped together equal to each other, consequently obtaining a system of linear equations.

For example, in L_5 the equation

$$3t^{3-x_1+x_2} + 4t^{-2+x_1} + 2t^{x_3-2} + 1 = 0$$

can be grouped as follows:

$$(3t^{3-x_1+x_2} + 2t^{x_3-2}) + (4t^{-2+x_1} + 1) = 0.$$

We then obtain the linear system

$$3 - x_1 + x_2 = x_3 - 2,$$

$$-2 + x_1 = 0.$$

We now solve this system of linear equations. If there is no solution, system (10) has no solution in this branch. If there is a solution, then we substitute the general solution back into (10).

To solve system (10), we will describe two procedures. The first will halt when a solution to the system is found, the second will halt if there is no solution to the system.

We can rewrite system (10) so that all the variables x_i have solutions in $\mathbb{N}$ and so that it is a system of equations over $\mathbb{Z}_n[t]$. We do this by rewriting the system as a disjunction of systems together with a sign assignment on the x_i (as in Section 2 in the proof of Lemma 2). We then fix one system and multiply both sides of each equation of the system by $t^{\sum x_i + \sum y_i + c}$, where the first sum is over all x_i with a negative assignment and c is the sum of all negative constant exponents. We then obtain a system with equations of the form

$$F'_s(\bar{x},t)f_s(t)t^{\sum_{i>q} y_i} = \sum_{i>q} F'_{i_s}(\bar{x},t)f_i(t)t^{y_s+\sum_{i\neq j, i>q} y_i} + P'_s(\bar{x},t)t^{y_s+\sum_{i>q} y_i} \tag{12}$$

for $s = 1, \ldots, q$.

Procedure 1. If a solution to the system exists, we can find it by enumerating and testing all possible solutions. We assign values in $\mathbb{N}$ to the x_i and the y_i, and values in $\mathbb{Z}_n[t]$ to the $f_i(t)$. In L, we follow the same procedure, but instead assign values in $\mathbb{Z}[t]$ to the $f_i(t)$.

Now we justify the second procedure for L_n.

Lemma 6. *Any element $g \in \mathbb{Z}_{p^n}[t]$, where p is a prime number, can be written as $g(t) = p^k \cdot u \cdot m(t)$, where u is a unit, $m(t)$ is a monic polynomial, and $k \in \mathbb{N}$.*

Proof. Note first that $g(t)$ can be written as $p^m f(t)$, where $f(t)$ is a regular polynomial (that is, it is not a zero divisor). This can be done by factoring out the maximum power of p so that at least one coefficient is not divisible by p.

Now we show that any regular polynomial $f(t)$ can be written as $f(t) = u \cdot m(t)$, where $m(t)$ is a monic polynomial and u is a unit. We will use the same proof as in [7] to show that for any regular polynomial $f(t)$, there is a sequence $\{f_i\}$ of monic polynomials such that

$$f_j = f_{j+1} \mod (p^j)$$

and that there is a $g_j \in (p)$ and a unit $b \in \mathbb{Z}_{p^n}$ such that

$$bf = f_j + g_j f_j \mod (p^j).$$

We will define this sequence inductively.

Let $f(t) = \sum_{i=0}^{n} d_i t^i$ be a regular polynomial, and let d_u be the coefficient with the highest degree that is a unit. Define $f_1(t) = d_u^{-1}(d_u t^u + \cdots + d_0)$, $g_1 = 0$ and $b = d_u^{-1}$. Now suppose $\{f_i\}_{i=1}^{j}$ satisfies the conditions so that $bf = f_j + g_j f_j + h$ where $h \in (p^j)$. Since f_j is monic, we can find a $q, r \in \mathbb{Z}_{p^n}[t]$ such that $h = f_j q + r$, where the $\deg(r) < \deg(f_j)$ or $r = 0$. Now we set $f_{j+1} = f_j + r$ and $g_{j+1} = g_j + q$, and we check that the conditions above are satisfied.

If $r = 0$, then we have the result. Suppose $r \neq 0$. Let $f_j = t^u + a_{u-1}t^{u-1} + \cdots + a_0$ and $q = c_s t^s + \cdots + c_1 t + c_0$. The coefficient of x^{s+u} in $f_j q$ is c_s, the coefficient of x^{s+u-1} is $c_{s-1} + a_{u-1}c_s$, and so on. Since $h = 0 \mod (p^j)$ and the $\deg(r) < \deg(f_j)$, we have that the coefficients $c_s \in (p^j)$ and $c_{s-1} \in (p^j)$, and so on, so $q \in (p^j)$. Then $g_{i+1} = g_i + q$ is in (p) and $r = h - q f_j \in (p^j)$.

Therefore, we have that

$$\begin{aligned} bf &= f_j + g_j f_j + h \\ &= (f_j + r) + (g_j + q)(f_j + r) - rg_j - rq \\ &= f_{j+1} + g_{j+1} f_{j+1} - r(g_j + q) \\ &= f_{j+1} + g_{j+1} f_{j+1} \mod (p^{j+1}). \end{aligned}$$

Finally, note that $f = b^{-1}(1 + g_n)f_n$, where f_n is monic, b^{-1} is a unit, and $g_n \in (p)$. Note that $(1+g_n)$ is a unit since its constant term is not a zero divisor. □

Lemma 7. *Any element $f \in \mathbb{Z}_n[t]$ can be written as $f(t) = \gamma \cdot z \cdot g$, where γ is a zero divisor, z is a unit, and g is a monic polynomial.*

Proof. Note that there is an isomorphism $\sigma : \mathbb{Z}_n[t] \to \mathbb{Z}_{p_1^{k_1}}[t] \times \cdots \times \mathbb{Z}_{p_m^{k_m}}[t]$, where $p_1, \ldots, p_m$ are distinct prime numbers and such that $n = p_1^{k_1} \cdots p_m^{k_m}$, and $k_1, \ldots, k_m \in \mathbb{N}$. Let $f \in \mathbb{Z}_n[t]$, and let $(f_1, \ldots, f_m)$ be its image under σ. Denote $\mathbb{Z}_{p_i^{k_i}}$ by S_i. By Lemma (6), for $i = 1, \ldots, m$ we have that $f_i = p_i^{s_i} \cdot u_i \cdot \bar{f}_i$, where u_i is a unit and $\bar{f}_i$ is a monic polynomial. Set $\gamma_i = (1_{S_1}, \ldots, p_i^{s_i}, \ldots, 1_{S_m})$, $z_i = (1_{S_1}, \ldots, u_i, \ldots 1_{S_m})$, and $g_i = (1_{S_1}, \ldots, \bar{f}_i, \ldots, 1_{S_m})$. Thus we have that $(f_1, \ldots, f_m) = \prod_{i=1}^m \gamma_i \cdot z_i \cdot \bar{f}_i$.

Note that the preimages of z and γ will be a unit and a zero divisor, respectively, since σ is an isomorphism. We need only check that the preimages of the g_i are monic polynomials. But this is easy to see, since σ maps a coefficient $1 \mapsto 1 \mod p_i^{k_i}$ which is 1. □

Lemma 8. *There is an integer solution to system* (12) *if and only if there are values for the variables $\bar{x} \cup \{f_i(t), y_i | i > q\}$ such that the system obtained from* (12) *by substituting the variables in $\bar{x} \cup \{f_i(t), y_i | i > q\}$ by these values has a solution modulo $h(t)$ for any monic polynomial $h(t)$ and in any $\mathbb{Z}_k[t]$, where $k|n$.*

Proof. An integer solution to system (12) may fail to exist only if there is a polynomial $h(t)$ in $\mathbb{Z}_n[t]$ that divides some $F'_s(\bar{x}, t)$ in the left side of some of the equations and does not divide the right side. For n prime, $\mathbb{Z}_n$ is a field, and it is enough to consider monic polynomials. For n composite, by [7, Lemma 4.6], every polynomial is a product of monic polynomials, a unit, and a zero divisor in $\mathbb{Z}_n$. Therefore it is enough to consider monic polynomials and zero divisors in $\mathbb{Z}_n$. Factoring by m that divides n is equivalent to considering (12) in $\mathbb{Z}_k[t]$, where $k = m/n$. □

Procedure 2 for L_n. By Lemma 8, system (12) does not have a solution if one of the following happens:

> **Case 1:** For any valuation of $\bar{x}, \bar{y}$, and $f_i(t)$, there is a monic polynomial $h(t) \in \mathbb{Z}_n[t]$ and an $s = 1, \ldots, q$ such that $h(t)$ divides $F'_s(\bar{x}, t)$ but $h(t)$ does not divide the right side of this equation.
>
> **Case 2:** For any values of $x_i, y_i, f_i(t)$, there is a $k|n$ and an $s = 1, \ldots, q$ such that $F'_s(\bar{x}, t)$ is zero in $\mathbb{Z}_k[t]$ but the right side of this equation is nonzero in $\mathbb{Z}_k[t]$.

We will describe two procedures that should alternate.

Case 1. We fix a monic polynomial $h(t)$ in $\mathbb{Z}_n[t]$. Note that each term $f_i(t)$, $i > q$, in system (12) can take finitely many values modulo $h(t)$, namely all polynomials in $\mathbb{Z}_k[t]$ with degree less than $h(t)$. Similarly, because the function t^n is periodic modulo any $h(t)$, then for any term t^{x_i} and t^{y_i} we only have to consider values

$\{0, \dots, P-1\}$ for the x_i and y_i, where P is the period of t^n modulo $h(t)$. We then test each possible solution set to see if there is a solution of the system modulo $h(t)$. If some of the possibilities for the $f_i(t), t^{x_i}, t^{y_i}$ work, then we rewrite our variables as follows: the terms $f_i(t)$ can be rewritten as $f_i(t) = r(t) + h(t)\bar{f}_i(t)$, where $r(t)$ is a polynomial in $\mathbb{Z}_k[t]$ with degree less than $h(t)$, and the terms x_i, y_i can be rewritten as $x_i = P\bar{x}_i + c_i$ and $y_i = P\bar{y}_i + d_i$, where P is the period of t^n modulo $h(t)$ and $c_i, d_i < P$. We may get more than one possible solution modulo $h(t)$ so that we have a new disjunction of systems. We continue this process for each monic polynomial in $\mathbb{Z}_n[t]$. If there is no solution, we will find an $h(t)$ for which (12) has no solution and the procedure will halt.

Case 2. Every time the coefficient $F'_s(\bar{x}, t)$ in the left side of some equation of system (12) is zero modulo k, where $k|n$, we have to exclude the corresponding $\bar{x}$ in the system corresponding to the right side:

$$\sum_{i>q} F'_{i_s}(\bar{x}, t) f_i(t) t^{y_s + \sum_{i \neq j, i>q} y_i} + P'_s(\bar{x}, t) t^{y_s + \sum_{i>q} y_i} = 0.$$

It has the same form as systems (10), (11). We will run Procedure 2 for this system in $\mathbb{Z}_k[t]$. This will include subprocedures for $\mathbb{Z}_s[t]$ for divisors s of k and eventually for $\mathbb{Z}_p[t]$ for prime divisors of n.

For $\mathbb{Z}_p[t]$ we will only have Case 1. □

Theorem 3. *Equations in L are decidable.*

A system of equations in L reduces to equations of the form (8) and (9), but the $f_j(t)$ are variables in $\mathbb{Z}[t]$ and $P(\bar{x}, t, t^{-1})$ is a polynomial with coefficients in $\mathbb{Z}$. To solve system (11) we group terms whose coefficients add up to 0. Then we reduce this system to system (12).

Lemma 9. *There is an integer solution to system* (12) *in $\mathbb{Z}[t]$ if and only if there is a value of $\bar{x}$, $f_i(t)$, and y_i for $i > q$, for which there is a solution to this system in any $\mathbb{Z}_n[t]$, where n is prime.*

Proof. In one direction the statement is obvious. Suppose now that there is no integer solution to system (12) in $\mathbb{Z}[t]$. Then for any value of $\bar{x}$, $f_i(t) \in \mathbb{Z}[t]$, and y_i for $i > q$, there is a polynomial $h(t)$ in $\mathbb{Z}[t]$ that divides the left side of one of the equations in system (12) and does not divide the right side of this equation. Then the right side of the equation has the form $h(t)g(y) + r(t)$ and there is n such that the images of $h(t)$ and $r(t)$ are not zeros in $\mathbb{Z}_n[t]$. □

The first procedure will be looking for a solution. The second procedure will be looking for a number n and a monic polynomial $h(t) \in \mathbb{Z}_n[t]$ such that for any value of $\bar{x}$, $f_i(t) \in \mathbb{Z}[t]$, and y_i for $i > q$ there is no solution to the system in $\mathbb{Z}_n[t]$ modulo $h(t)$.

Theorem 3 implies the following corollary.

Corollary 1. *The Diophantine problem is decidable in $\mathbb{Z}^n \wr \mathbb{Z}$.*

Proof. Equations in $\mathbb{Z}^n \wr \mathbb{Z}$ have the same form as equations (8) and (9) in the proof of Theorem 3, with the exception that the terms $f_i(t)$ are in the ring $\mathbb{Z}^n[t]$. Each equation of the form (8) is equivalent to n equations, each corresponding to a component of $\mathbb{Z}^n$. Thus, any system of equations in $\mathbb{Z}^n \wr \mathbb{Z}$ is equivalent to a system in $\mathbb{Z} \wr \mathbb{Z}$, so the decidability follows from the decidability of $\mathbb{Z} \wr \mathbb{Z}$. □

Combining Theorems 2 and 3 we obtain the second main result.

Theorem 4. *The Diophantine problem is decidable in $A \wr \mathbb{Z}$, where A is a finitely generated abelian group.*

Proof. Let $A = \mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$. Equations in $A \wr \mathbb{Z}$ have the same form as equations (8) and (9) in the proof of Theorems 2, 3 with the exception that the terms $f_i(t)$ are in the ring $R[t]$ (recall that R is the same as A but viewed as a ring). Each system of the form (8) is equivalent to several systems, some of them over $\mathbb{Z}$ and some over $\mathbb{Z}_{n_i}$, each corresponding to a component of $\mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$. Solving these systems simultaneously we will solve the original system. □

We conclude with some open problems.

Problem 1. What is the complexity of solving equations in $BS(1,k)$ and in wreath products $A \wr \mathbb{Z}$, where A is a finitely generated abelian group?

Problem 2. Prove that the existential theory of $BS(1,k)$ and wreath products $A \wr \mathbb{Z}$, where A is a finitely generated abelian group, is decidable.

Problem 3. Describe finitely generated metabelian groups with a decidable Diophantine problem.

Acknowledgments

We are very grateful to the referees for their important comments and suggestions.

References

[1] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2) **18** (1978), no. 3, 385–391, DOI 10.1112/jlms/s2-18.3.385. MR518221

[2] V. Diekert and M. Lohrey, *Existential and positive theories of equations in graph products*, Symposium on Theoretical Aspects of Computer Science (Antibes-Juan les Pins, 2002). Theory Comput. Syst. **37** (2004), no. 1, 133–156, DOI 10.1007/s00224-003-1110-x. MR2038406

[3] V. Diekert and A. Muscholl, *Solvability of equations in graph groups is decidable*, Internat. J. Algebra Comput. **16** (2006), no. 6, 1047–1069, DOI 10.1142/S0218196706003372. MR2286422

[4] M. Duchin, H. Liang, and M. Shapiro, *Equations in nilpotent groups*, Proc. Amer. Math. Soc. **143** (2015), no. 11, 4723–4731, DOI 10.1090/proc/12630. MR3391031

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

[6] A. Garreta, A. Miasnikov, and D. Ovchinnikov, *Random nilpotent groups, polycyclic presentations, and Diophantine problems*, Groups Complex. Cryptol. **9** (2017), no. 2, 99–115, DOI 10.1515/gcc-2017-0007. MR3717096

[7] O. Greco, *Unique non-unique factorization*, Master's thesis, 2010, University of Stockholm.

[8] M. I. Kargapolov, V. N. Remeslennikov, N. S. Romanovskiĭ, V. A. Roman′kov, and V. A. Čurkin, *Algorithmic questions for σ-powered groups*, Algebra i Logika **8** (1969), 643–659. MR0283060

[9] M. Lohrey and G. Sénizergues, *Theories of HNN-extensions and Amalgamated Products*, Automata, languages and programming. Part II, Lecture Notes in Comput. Sci., vol. 4052, Springer, Berlin, 2006, pp. 504–515, DOI 10.1007/11787006_43. MR2307261

[10] R. C. Lyndon, *Equations in free groups*, Trans. Amer. Math. Soc. **96** (1960), 445–457, DOI 10.2307/1993533. MR151503

[11] A. I. Mal′cev, *On the equation $zxyx^{-1}y^{-1}z^{-1} = aba^{-1}b^{-1}$ in a free group* (Russian), Algebra i Logika Sem. **1** (1962), no. 5, 45–50. MR0153726

[12] G. S. Makanin, *The problem of the solvability of equations in a free semigroup* (Russian), Mat. Sb. (N.S.) **103(145)** (1977), no. 2, 147–236, 319. MR0470107

[13] G. S. Makanin, *Equations in a free group* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), no. 6, 1199–1273, 1344. MR682490
[14] G. A. Noskov, *The elementary theory of a finitely generated almost solvable group* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **47** (1983), no. 3, 498–517. MR703594
[15] T. Pheidas and K. Zahidi, *Undecidability of Existential Theories of Rings and Fields: A Survey*, Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry (Ghent, 1999), Contemp. Math., vol. 270, Amer. Math. Soc., Providence, RI, 2000, pp. 49–105, DOI 10.1090/conm/270/04369. MR1802009
[16] V. A. Roman′kov, *Unsolvability of the problem of endomorphic reducibility in free nilpotent groups and in free rings*, Algebra and Logic **16** (1977), no. 4, 310–320.
[17] V. A. Roman′kov. *Equations in free metabelian groups*, Siberian Mathematical Journal, **20** (1979), no.3, 469–471.
[18] N. S. Romanovskiĭ, *On the elementary theory of an almost polycyclic group*, Mathematics of the USSR-Sbornik, **39** (1981), no. 1, 125–132.
[19] A. L. Semënov, 1984 Math. Logical theories of one-place functions on the set of natural numbers. USSR Izv. 22, 587–618.
[20] W. Szmielew, *Elementary properties of Abelian groups*, Fund. Math. **41** (1955), 203–271, DOI 10.4064/fm-41-2-203-271. MR72131

Department of Mathematics and Statistics, Hunter College and Graduate Center of City University of New York, Room 919/944 East, 695 Park Avenue, New York, New York 10065

The Graduate Center, City University of New York, 365 Fifth Avenue, New York, New York 10016

Department of Mathematical Sciences, Stevens Institute of Technology, One Castle Point Terrace, Hoboken, New Jersey 07030