On the Solvability of a Class of Diophantine Equations and Applications

Oscar H. Ibarra

Department of Computer Science, University of California
Santa Barbara, CA 93106, USA
ibarra@cs.ucsb.edu

Zhe Dang

School of Electrical Engineering & Computer Science
Washington State University
Pullman, WA 99164, USA
zdang@eecs.wsu.edu

Abstract

For $1 \leq i \leq k$, let R_i denote $p_i(y)F_i + G_i$, where $p_i(y)$ is a polynomial in y with integer coefficients, and F_i, G_i are linear polynomials in $x_1, ..., x_n$ with integer coefficients. Let $P(z_1, ..., z_k)$ be a Presburger relation over the nonnegative integers. We show that the following problem is decidable:

> **Given:** $R_1, ..., R_k$ and a Presburger relation P.
>
> **Question:** Are there nonnegative integer values for $y, x_1, ..., x_n$ such that for these values, $(R_1, ..., R_k)$ satisfies P?

We also give some applications to decision problems concerning counter machines.

Key words: Diophantine equation, counter machine.

1 Introduction

It is well-known that it is undecidable to determine, given an arbitrary multi-variable polynomial with integers coefficients, whether it has a solution over the nonnegative integers [7]. Some interesting nontrivial special cases have been shown to be decidable (e.g., [6]).

In this note, we look at a new class of systems of Diophantine equations for which the existence of solutions is decidable. These equations, given in the Abstract, arose when were investigating certain verification problems concerning counter machines [3] (see also [4]). Actually, the class we consider here is more general in that in [3], the $p_i(y)$'s are linear in y, and the Presburger relation P is of a special form – an "equality" relation. This is the class defined in Problem DE of Section 3. We recently learned that M. Bozga and R. Iosif have also been studying a similar class in relation to their work on flat counter automata [1].

In Section 2, we define formally the class of Diophantine equations and present a proof of its solvability. Then in Sections 3 and 4, we apply this decidability result to some problems left open in [3]. Finally, for completeness, in Section 5 we mention two variations of the diophantine equations which have been shown to be undecidable (decidable) in [3].

2 The Solvable Class

For $1 \leq i \leq k$, let R_i denote $p_i(y)F_i + G_i$, where $p_i(y)$ is a polynomial in y with integer coefficients (e.g., $8y^5 - 3y^2 + 7y - 6$), and F_i, G_i are linear polynomials in $x_1, ..., x_n$ with integer coefficients (e.g., $-10x_1+5x_2+7x_4-3x_7+9$). Let $P(z_1, ..., z_k)$ be a Presburger relation over the nonnegative integers, i.e., definable by a Presburger formula.

Theorem 2.1 *The following problem is decidable:*

> **Given:** *$R_1, ..., R_k$ and a Presburger relation P.*
> **Question:** *Are there nonnegative integer values for $y, x_1, ..., x_n$ such that for these values, $(R_1, ..., R_k)$ satisfies P?*

Note that p_i, F_i, G_i can be a constant (in particular, 0 or 1). Hence, R_i can be just p_i, F_i, or G_i. In particular, R_i can be y or one of the x-variables.

The proof of the above theorem uses the following known results concerning reversal-bounded multicounter machines:

(1) Let M be nondeterministic two-way finite automaton over a *unary* input (with left and right end markers) augmented with reversal-bounded counters. Thus the inputs to such a machine is of the form $\$o^y\$$, where y is a nonnegative integer, and \$ is the end marker. (A counter is reversal-bounded if at each step, it can be incremented/decremented by 1 or left unchanged and tested for zero, but can only reverse its mode from nondecreasing to nonincreasing and vice-versa at most a fixed number of times,

independent of the input.) Call this machine 2NCM.

It is known that the emptiness problem for 2NCMs (does the machine accept some unary input?) is decidable [5]. Note that, in contrast, it follows from Minsky's result [8], that the emptiness problem problem is undecidable for deterministic two-way finite automata over unary input (with end markers) augmented with one unrestricted counter.

(2) Let G be a nondeterministic finite automaton with r nondecreasing counters (thus at each step, each counter can only be incremented by 0 or 1). G starts with all counters zero. If G halts and accepts, then we say that the values $(n_1, ..., n_r)$ of the counters when it halts are generated by G. G is called a monotonic counter generator.

Let $P \subseteq N^r$. Then P is a Presburger relation or, equivalently, a semilinear set if and only if we can (effectively) construct a monotonic counter generator G such that the set of tuples generated by G is $\{(n_1, ..., n_r) \mid P(n_1, ..., n_r)$ is satisfied $\}$ [2].

We now give the proof of Theorem 2.1.

Proof. Let G be the monotonic counter generator for the Presburger relation $P(z_1, ..., z_k)$. We show how to construct a 2NCM M to accept the unary language $\{o^y \mid y$ is a nonnegative integer, and there exist $x_1, ..., x_n$ such that for these values, $(R_1, ..., R_k)$ satisfies $P\}$. M operates as follows:

(1) Given o^y, M first nondeterministically guesses $x_1, ..., x_n$ and stores them in k counters.
(2) With o^y on the input and $(x_1, ..., x_n)$ on the counters, and using (many) auxiliary reversal-bounded counters, M computes $R_i = p_i(y)F_i + G_i$ for $i = 1, ..., k$.
(3) Then M checks that $(R_1, ..., R_k)$ satisfies P, by simulating the generator G. (Note that in the simulation of the counters of G, an increment is simulated by a decrement.)

Items 1 and 3 above are obvious. That item 2 can be implemented by M using reversal-bounded counters follows from the the following observations:

1. Clearly, each $F_i(x_1, ..., x_n)$ and each $G_i(x_1, ..., x_n)$ can be computed using reversal-bounded counters.

2. $y^s x$ for any s and x can be computed using reversal-bounded counters as follows:

Suppose x is in counter 1 and o^y is on the input tape, M makes left-to-right (right-to-left) sweeps on the input while incrementing counter 2 on every move of the input head. At the end of every sweep, M decrements counter 1 by 1. When counter 1 becomes zero, counter 2 has value yx. Now that we have yx in counter 2, we can use the same idea to produce y^2x in counter 1, etc. Note that for a given s, $y^s x$ can be computed with counters 1 and 2 being reversal-bounded (each making no more than $s/2$ reversals).

Hence, the system has a solution if and only if the unary language accepted by M is not empty, which is decidable (since M is reversal-bounded). $\square$

3 Applications

As we have noted earlier, the question of the decidability of the class of Diophantine equations studied in Section 1 arose when we were studying some verification problems concerning counter machines in [3]. The decidability of one such property turned out to be equivalent to the decidability of the class in Section 1, where the $p_i(y)$'s are linear polynomials in y.

Consider a class of machines M as follows. M is a *deterministic* two-way finite automaton augmented with k monotonic counters $C_1, \cdots, C_k$. The two-way input, w (which is provided with left and right end markers), comes from a bounded language, i.e., $w = a_1^{i_1} \cdots a_n^{i_n}$ for some fixed n and distinct symbols $a_1, \cdots, a_n$, and $i_1, \cdots, i_n$ are nonnegative integers. The counters are initially zero and can be incremented by 0 or 1 at each step, but cannot be decremented. They do not participate in the dynamic of the machine. We shall simply call M a 2FAMC. We do not assume that the machine halts on all inputs.

Note that the set of tuples of nonnegative integers "generated" by a 2FACM (at a specified state) need not be semilinear (Presburger) in general. For example, consider a 2FACM with two monotonic counters C_1 and C_2. On unary input x of length n, M initially stores n in C_1. Then M makes left-to-right and right-to-left sweeps of the input, adding n to C_2 after every left-to-right sweep. M iterates this process without halting. Let s be the state of M just after a left-to-right sweep. Then the set of tuples of values of the counters when it is in state s is $Q_s = \{(n, kn) \mid n \geq 0, k > 0\}$, which is not semilinear.

We are interested in the problem of deciding, given a 2FAMC M and a Presburger relation E, whether the set of tuples generated by M satisfies E. The decidability of this question was left unresolved in [3], even for simple Presburger relations.

An atomic equality relation on the counters is a relation of the form $C_i = C_j$, $i \neq j$. An equality relation E is a conjunction of atomic equality relations.

An example of E is $(C_1 = C_3 \ \wedge \ C_1 = C_4 \ \wedge \ C_2 = C_3)$. We say that M satisfies E at state q if there is some input $w = a_1^{i_1} \cdots a_n^{i_n}$ such that M on input w, enters some configuration where the state is q and the counter values satisfy the relation E. For convenience, when q is understood, we simply say M satisfies E.

Since M does not necessarily halt, a configuration that satisfies E can be an intermediate configuration of a possibly infinite computation. Note also that M can satisfy E many times during the computation. We are interested in the following:

Reachability Problem Under Equality Relation:

> **Given:** A 2FAMC M and an equality relation E.
> **Question:** Does M satisfy E?

An obvious generalization of the above problem is when E is an arbitrary Presburger relation (note that an equality relation is a special form of a Presburger relation).

It turns out that the above problem (where E is an equality relation) is equivalent to the solvability of the following problem:

Problem DE:

> **Given:** A system S consisting of the following $(k+m)$ equations:
> $A_i = B_i, \ \ i = 1, \cdots, k$
> $yF_i = G_i, \ \ i = 1, \cdots, m$
>
> where A_i, B_i, F_i, G_i are linear polynomials in nonnegative integer variables $x_1, \cdots, x_n$ with integer coefficients. Hence these polynomials are of the form $a_0 + a_1 x_1 + \cdots + a_n x_n$, where each a_i is an integer (positive, negative, or zero).
>
> **Question:** Does S have a solution, i.e., there are nonnegative integers $y, x_1, \cdots, x_n$ satisfying S?

Note that the system S above is a special case of the system we considered in Section 1. Hence Problem DE is decidable. The following was shown in [3]:

Theorem 3.1 *The Reachability Problem under equality relation is equivalent to Problem DE in the following sense:*

(1) Given a system S, we can effectively construct a 2FAMC M and an equality relation E such that S has a solution if and only if M satisfies E.

(2) *Given a 2FAMC and an equality relation E, we can effectively construct a finite number of systems S of equations of the form $A_i = B_i$ or of the form $yF_i = G_i$ (where A_i, B_i, F_i, G_i are linear polynomials in nonnegative integer variables $x_1, \cdots, x_n$ with integer coefficients) such that M satisfies E if and only if one of the S's has a solution in the nonnegative integers $y, x_1, \cdots, x_n$.*

The following corollary follows from Theorems 2.1 and 3.1:

Corollary 3.1 *The Reachability Problem for 2FMACs under equality relation is decidable.*

4 Reachability Problem Under Arbitrary Presburger Relation

Corollary 3.1 only proved the Reachability Problem when E is an equality relation. In this section, we look at the general case when the relation E is an arbitrary Presburger relation $E(c_1, ..., c_k)$ over the counter values $c_1, ..., c_k$, and show that the reachability problem is still decidable, resolving a more general open problem that was also posed in [3].

The idea is as follows. In [3], it was shown that the value of counter c_i ($1 \leq i \leq k$) at any time can effectively be represented by equations of the form:

$$c_i = A_i + yB_i + C_i$$

where y is a nonnegative integer variable, and A_i, B_i, C_i are nonnegative linear polynomials in some nonnegative integer variables $x_1, ..., x_n$. (We can combine A_i and C_i into a single linear polynomial, but we wanted to first show the representation above to be consistent with the formulation in [3].) Then, the value of counter $c_i = yB_i + (A_i + C_i)$. It then follows from Theorem 2.1 that we can decide whether for this system of equations there exist nonnegative integers $y, x_1, ..., x_n$ such that $(c_1, ..., c_k)$ satisfies the Presburger relation E. Thus, we have:

Theorem 4.1 *The Reachability Problem for 2FAMCs under arbitrary Presburger relation is decidable.*

5 Variations

For completeness, we mention below two variations of systems of diophantine equations which have been shown to be undecidable (decidable) in [3]. They are related to certain verification problems concerning counter machines [3].

Consider the following system of equations, S, which we call a width-2 system:

$$\begin{aligned}&A_i = B_i, \quad i = 1, \cdots, k\\ &y_i F_i = G_i \ \wedge \ y_i H_i = I_i, \quad i = 1, \cdots, m\end{aligned}$$

where $A_i, B_i, F_i, G_i, H_i, I_i$ are linear polynomials in nonnegative variables $x_1, \cdots, x_n$. Note that each y_i is involved in exactly two equations. We say that S has a solution if there are nonnegative integers $y_1, \cdots, y_m, x_1, \cdots, x_n$ satisfying S. It was shown in [3] that is undecidable to determine, given a width-2 system S, whether it has a (nonnegative integer) solution in $y_1, ..., y_m, x_1, ..., x_n$.

However, consider the following simpler case, called width-1 system, S:

$$\begin{aligned}&A_i = B_i, \quad i = 1, \cdots, k\\ &y_i F_i = G_i, \quad i = 1, \cdots, m\end{aligned}$$

where, again, A_i, B_i, F_i, G_i are linear polynomials in $x_1, \cdots, x_n$. Thus, each y_i is involved in only one equation. It was also shown in [3] that it is decidable to determine, given a width-1 system, whether it has a solution.

Acknowledgements. The work of Oscar H. Ibarra was supported in part by NSF Grants CCR-0208595, CCF-0430945, IIS-0451097, and CCF-0524136. The work of Zhe Dang was supported in part by NSF Grant CCF-0430531.

References

[1] M. Bozga and R. Iosif. Flat Parametric Counter Automata, in preparation. *Personal Communication.*

[2] T. Harju, O. H. Ibarra J. Karhumaki, and A. Salomaa. Some Decision Problems Concerning Semilinearity and Commutation. *Journal of Computer and System Sciences*, vol. 65, pp. 278-294, 2002.

[3] O. H. Ibarra and Z. Dang. On Two-Way FA with Monotonic Counters and Quadratic Diophantine Equations. *Theoretical Computer Science*, vol. 312, pp. 359-378, 2004.

[4] O. H. Ibarra, Z. Dang, and Z.-W. Sun. Safety Verification for Two-Way Finite Automata with Monotonic Counters. *Proc. Sixth International Conference: Developments in Language Theory 2002*, Lecture Notes in Computer Science (LNCS), vol. 2450, pp. 326-338, 2003.

[5] O. H. Ibarra, T. Jiang, N. Tran, and H. Wang. New Decidability Results Concerning Two-way Counter Machines. *SIAM Journal on Computing*, vol. 24, no. 1, pp. 123-137, 1995.

[6] L. Lipshitz. The Diophantine Problem for Addition and Divisibility. *Transactions of AMS*, vol. 235, pp. 271-283, 1978.

[7] Y. V. Matiyasevich. *Hilbert's Tenth Problem.* MIT Press, 1993.

[8] M. Minsky. Recursive Unsolvability of Post's Problem of Tag and Other Topics in the Theory of Turing machines. *Ann. of Math*, vol. 74, pp. 437-455, 1961.