On Intersection Problems for Polynomially Generated Sets

Wong Karianto[1], Aloys Krieg[2], and Wolfgang Thomas[1]

[1] Lehrstuhl für Informatik 7, RWTH Aachen, Germany
{karianto,thomas}@informatik.rwth-aachen.de
[2] Lehrstuhl A für Mathematik, RWTH Aachen, Germany
krieg@mathA.rwth-aachen.de

Abstract. Some classes of sets of vectors of natural numbers are introduced as generalizations of the semi-linear sets, among them the 'simple semi-polynomial sets.' Motivated by verification problems that involve arithmetical constraints, we show results on the intersection of such generalized sets with semi-linear sets, singling out cases where the non-emptiness of intersection is decidable. Starting from these initial results, we list some problems on solvability of arithmetical constraints beyond the semi-linear ones.

1 Introduction

The study of arithmetical constraints, in particular regarding their effective solvability, is of central interest in several branches of theoretical computer science. One of these fields, which serves as motivation for the present work, is the verification of infinite-state systems where the aspect of infinity arises by including the domain of the natural numbers in the model under consideration.

In the context of infinite-state verification, conditions on vectors of natural numbers usually occur in two roles. First, the considered transition systems $\mathcal{A}$ are assumed to have some mechanism of 'counting' and thus generate, by each run, some vector of $\mathbb{N}^n$; the set of all such vectors is the set $A_{\mathcal{A}} \subseteq \mathbb{N}^n$ generated by $\mathcal{A}$. An example is the computation of the Parikh mapping by an automaton on words over an alphabet with letters $a_1, \ldots, a_n$: the occurrences of the letters a_i are counted by updating a vector from $\mathbb{N}^n$ in each step, incrementing the i-th component by one for an a_i-labeled transition. Taking finite automata or pushdown automata $\mathcal{A}$, the corresponding sets $A_{\mathcal{A}}$ are known to coincide with the semi-linear sets (Parikh's Theorem [12]).

The second role of arithmetical conditions enters when the vectors arising from the runs of the transition systems under consideration are also subject to an 'acceptance condition' φ. In the context of automata, acceptance of an input word w then means that a corresponding run reaches a 'final state' and generates a vector that satisfies φ or, in other words, belongs to the set A_φ defined by φ. As a recent model of this kind, Klaedtke and Rueß [9] proposed 'Parikh automata,' which use more general transitions than those mentioned above: in the update

operation an arbitrary vector of $\mathbb{N}^n$ is added (rather than just 1 in a single component), and for the constraints φ formulas of Presburger arithmetic are used (which precisely define the semi-linear sets).

A fundamental property of Parikh automata is the decidability of the nonemptiness problem. This is established easily by observing that the nonemptiness of the language recognized by a Parikh automaton $\mathcal{A}$ with acceptance condition φ is equivalent to the nonemptiness of the intersection $A_{\mathcal{A}} \cap A_{\varphi}$. Since $A_{\mathcal{A}}$ is semi-linear, and since the semi-linear sets are effectively closed under intersection (and their nonemptiness is trivially decidable), one obtains an algorithm for solving the nonemptiness problem.

Many other papers on model-checking infinite-state systems follow similar ideas; see, for example, [1, 3, 7]. Another application area is the study of XML-document specifications. As observed by several authors [2, 10, 13, 14], the automata on unranked trees which capture document type definitions can be extended by counting conditions (on the occurrences of certain data as sons of an XML-tree node). If these arithmetical conditions are restricted to semi-linear sets, then the desired decidability results on type checking can be shown.

The purpose of the present paper is to explore possibilities of extending the framework of semi-linear sets (or, equivalently, Presburger arithmetic or systems of linear equations), while still keeping the fundamental property that nonemptiness of intersection is decidable. As noted above, the two sets of such an intersection may arise differently (e.g., as generated by a system and as specified by an acceptance condition), so it is reasonable to consider intersections $A \cap B$ where A and B are possibly from different classes.

We basically consider two classes extending the semi-linear sets. Firstly, we introduce 'simple semi-polynomial sets' and show initial results on closure properties with respect to intersection (with implications for deciding nonemptiness). Secondly, some variants of 'quadratic' sets are introduced, where a recent result of Grunewald and Segal [5] helps to show the decidability of certain nonemptiness problems. As a conclusion, we suggest some questions motivated by our observations.

In the present paper we do not address applications in detail, for example in concrete verification problems. Instead, we focus on the arithmetical aspects and only remark here that in the scenario above (regarding the sets $A_{\mathcal{A}}$ and A_{φ}) we obtain cases which are substantially more general (or, at least, different) than the existing framework of semi-linear sets and still allow an algorithmic solution.

2 Preliminaries

Recall that a subset A of $\mathbb{N}^n$, $n \geq 1$, is called *linear* if there are vectors $\bar{u}_0, \bar{u}_1, \ldots, \bar{u}_m \in \mathbb{N}^n$, $m \geq 0$, such that

$$A = \{\bar{u}_0 + k_1\bar{u}_1 + \cdots + k_m\bar{u}_m \mid k_1, \ldots, k_m \in \mathbb{N}\} \ . \tag{1}$$

The vector $\bar{u}_0$ is called the *constant vector*, the vectors $\bar{u}_1, \ldots, \bar{u}_m$ the *periods*, and all of them the *generators* of A. Alternatively, we may replace (1) with

$$A = \{(L_1(k_1, \ldots, k_m), \ldots, L_n(k_1, \ldots, k_m)) \mid k_1, \ldots, k_m \in \mathbb{N}\} \ , \qquad (2)$$

where $L_i(k_1, \ldots, k_m) := (\bar{u}_0)_i + k_1(\bar{u}_1)_i + \cdots + k_m(\bar{u}_m)_i$ for $i = 1, \ldots, n$.[3] In other words, $L_1, \ldots, L_n \in \mathbb{N}[X_1, \ldots, X_m]$ are linear forms with nonnegative integer coefficients. A finite union of linear sets is called *semi-linear*.

In [4] Ginsburg and Spanier showed that the solutions of a linear equation $c_0 + \sum_{i=1}^{n} c_i x_i = c'_0 + \sum_{i=1}^{n} c'_i x_i$, where $c_i, c'_i \in \mathbb{N}$, for $i = 0, \ldots, n$, form a semi-linear set. Further, if we close the sets defined by linear equations under Boolean operations and projection, the *Presburger-definable sets* (i.e., the first-order-definable sets over $(\mathbb{N}, +)$) are generated. Ginsburg and Spanier [4] also showed that the semi-linear sets coincide with the Presburger-definable ones. Moreover, all the logical closure operations are effective. For instance, given the generators of A and B, generators of $A \cap B$ can be computed. This implies that the nonemptiness of this intersection is decidable.

For a finite, nonempty alphabet $\Sigma = \{a_1, \ldots, a_n\}$, the *Parikh mapping* $\Phi\colon \Sigma^* \to \mathbb{N}^n$ is defined by $\Phi(w) := (|w|_{a_1}, \ldots, |w|_{a_n})$, for each $w \in \Sigma^*$. Parikh's Theorem [12] asserts that the *Parikh image* $\Phi(L) := \{\Phi(w) \mid w \in L\}$ of a context-free language L over Σ is semi-linear. Conversely, every semi-linear set is the Parikh image of a context-free language (even of a regular language).

3 Simple Semi-Polynomial Sets

A natural generalization of semi-linear sets involves general polynomials rather than just linear ones in (2): A subset A of $\mathbb{N}^n$, $n \geq 1$, is a *polynomial set* if there are polynomials $P_1, \ldots, P_n \in \mathbb{N}[X_1, \ldots, X_m]$ such that

$$A = \{(P_1(k_1, \ldots, k_m), \ldots, P_n(k_1, \ldots, k_m)) \mid k_1, \ldots, k_m \in \mathbb{N}\} \ . \qquad (3)$$

A finite union of polynomial sets is called *semi-polynomial*.

Since the polynomials in (3) may have mixed terms, i.e., terms in which more than one variable occur, we get a class which is not manageable. In fact, the nonemptiness of intersection is undecidable even for the case of a two-dimensional polynomial set and a semi-linear one. This is clear by a simple reformulation of Hilbert's Tenth Problem (note that the identity relation $\mathrm{id}_{\mathbb{N}} := \{(k, k) \mid k \in \mathbb{N}\}$ is a linear set):

$$\begin{aligned}
& \exists k_1 \ldots k_m \ P(k_1, \ldots, k_m) = 0 \ , \ \text{where } P \in \mathbb{Z}[X_1, \ldots, X_m] \\
\text{iff} \quad & \exists k_1 \ldots k_m \ Q(k_1, \ldots, k_m) = R(k_1, \ldots, k_m) \ , \ \text{where } Q, R \in \mathbb{N}[X_1, \ldots, X_m] \\
\text{iff} \quad & \left\{ \begin{pmatrix} Q(k_1, \ldots, k_m) \\ R(k_1, \ldots, k_m) \end{pmatrix} \mid k_1, \ldots, k_m \in \mathbb{N} \right\} \cap \mathrm{id}_{\mathbb{N}} \neq \emptyset \ .
\end{aligned}$$

[3] For a vector $\bar{x} \in \mathbb{N}^n$, we write $(\bar{x})_i$ for the i-th component of $\bar{x}$.

Therefore, we restrict the polynomials in (3) by disallowing mixed terms and obtain sets of the form

$$\left\{ \begin{pmatrix} c_1 + P_{11}(k_1) + \cdots + P_{1m}(k_m) \\ \vdots \\ c_n + P_{n1}(k_1) + \cdots + P_{nm}(k_m) \end{pmatrix} \mid k_1, \ldots, k_m \in \mathbb{N} \right\} \ , \tag{4}$$

where $c_1, \ldots, c_n \in \mathbb{N}$, and $P_{ij} \in \mathbb{N}[X]$ is a (univariate) polynomial without constants, for each $i = 1, \ldots, n$ and $j = 1, \ldots, m$. A set defined in this way is called a *simple polynomial set*, and *simple semi-polynomial sets* are finite unions of simple polynomial sets.

In analogy to (1) for linear sets, a simple polynomial set as in (4) can be represented in terms of its *generators* as follows:

$$\begin{aligned} \{ &\bar{u}_0 + k_1 \bar{u}_{1,1} + k_1^2 \bar{u}_{1,2} + \cdots + k_1^{d-1} \bar{u}_{1,d-1} + k_1^d \bar{u}_{1,d} \\ &+ \cdots + k_m \bar{u}_{m,1} + k_m^2 \bar{u}_{m,2} + \cdots + k_m^{d-1} \bar{u}_{m,d-1} + k_m^d \bar{u}_{m,d} \\ &\mid k_1, \ldots, k_m \in \mathbb{N} \} \ , \end{aligned} \tag{5}$$

where $\bar{u}_0$ and $\bar{u}_{i,j}$ ($1 \leq i \leq m$, $1 \leq j \leq d$) are vectors from $\mathbb{N}^n$. In this case, the simple polynomial set is said to be of *degree* d. Note that from a representation (4) one easily obtains (5), and vice versa.

Clearly, each (semi-)linear set is a simple (semi-)polynomial set. An interesting special case is given by the *simple quadratic sets*

$$\{ \bar{u}_0 + k_1 \bar{u}_{1,1} + k_1^2 \bar{u}_{1,2} + \cdots + k_m \bar{u}_{m,1} + k_m^2 \bar{u}_{m,2} \mid k_1, \ldots, k_m \in \mathbb{N} \}$$

and finite unions of such sets, the *simple semi-quadratic sets*.

Given the generators of a (simple) polynomial set as in (3) or (5), one can decide whether a given vector $\bar{v} = (v_1, \ldots, v_n)$ belongs to this set; it suffices to check the k_i-values up to $\max\{v_1, \ldots, v_n\}$. Hence, a (simple) semi-polynomial set is decidable.

Example 1. The set $A_1 := \{(u_1, u_2) \in \mathbb{N}^2 \mid u_2 = u_1^2\}$ is a simple quadratic set since $A_1 = \{(0,0) + k(1,0) + k^2(0,1) \mid k \in \mathbb{N}\}$.

Let us verify that A_1 is not semi-linear. Towards a contradiction, suppose that A_1 is a finite union of linear sets, say $A_1 = \bigcup_{i=1}^{r} B_i$, for some $r \geq 1$. Since A_1 is infinite, there is some linear set B_i that contains at least two elements. Let $\bar{u}_0$ be the constant vector and $\bar{u}_1, \ldots, \bar{u}_m$ be the periods of B_i. If $m = 0$, or if all periods of B_i are $\bar{0}$,[4] then B_i has only one element, namely $\bar{u}_0$, a contradiction. So we can assume that $\bar{u}_1$ is not $\bar{0}$. By definition of linear sets, $\bar{u}_0 + k\bar{u}_1 \in B_i \subseteq A_1$, for all $k \in \mathbb{N}$. Let $\bar{u}_0 = (u_{01}, u_{02})$ and $\bar{u}_1 = (u_{11}, u_{12})$. Then, by definition of A_1, we have for all $k \in \mathbb{N}$

$$(u_{01} + k u_{11})^2 = u_{02} + k u_{12} \ . \tag{6}$$

Since $\bar{u}_1 \neq \bar{0}$, at least one of u_{11} and u_{12} is not zero. Hence, (6) is a polynomial equation of degree one or two in k, which has at most two solutions. Contradiction.

[4] $\bar{0}$ denotes a vector consisting only of zeroes.

A copy of this argument shows that $\{(u_1, u_2) \in \mathbb{N}^2 \mid u_2 = u_1^{d+1}\}$ is not a simple semi-polynomial set of degree d, for any $d \geq 1$, and that $\{(u_1, u_2) \in \mathbb{N}^2 \mid u_2 = 2^{u_1}\}$ is not a simple semi-polynomial set.

Example 2. The product relation $A_{\text{prod}} := \{(u, v, uv) \mid u, v \in \mathbb{N}\} \subseteq \mathbb{N}^3$, which is clearly polynomial, is not a simple semi-polynomial set. To verify this, the simple comparison of growth rates does not suffice, and some structural analysis is needed.

Towards a contradiction, assume that A_{prod} is a finite union of simple polynomial sets, each of them of the form

$$A' = \left\{ \begin{pmatrix} a + P_1(k_1) + \cdots + P_m(k_m) \\ b + Q_1(k_1) + \cdots + Q_m(k_m) \\ c + R_1(k_1) + \cdots + R_m(k_m) \end{pmatrix} \mid k_1, \ldots, k_m \in \mathbb{N} \right\} ,$$

where $P_i, Q_i, R_i \in \mathbb{N}[X]$ are polynomials without constants, and where not all of P_i, Q_i, R_i are zero polynomials, for each $i = 1, \ldots, m$. Since $P_i(0) = Q_i(0) = R_i(0) = 0$ for $i = 1, \ldots, m$, we have, for each $j \geq 2$,

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix}, \begin{pmatrix} a + P_1(1) \\ b + Q_1(1) \\ c + R_1(1) \end{pmatrix}, \begin{pmatrix} a + P_j(1) \\ b + Q_j(1) \\ c + R_j(1) \end{pmatrix}, \begin{pmatrix} a + P_1(1) + P_j(1) \\ b + Q_1(1) + Q_j(1) \\ c + R_1(1) + R_j(1) \end{pmatrix} \in A_{\text{prod}} .$$

Since A_{prod} is the product relation, we have

$$\begin{aligned} c &= ab \\ c + R_1(1) &= (a + P_1(1))(b + Q_1(1)) \\ c + R_j(1) &= (a + P_j(1))(b + Q_j(1)) \\ c + R_1(1) + R_j(1) &= (a + P_1(1) + P_j(1))(b + Q_1(1) + Q_j(1)) \end{aligned}$$

It follows that $P_1(1)Q_j(1) + P_j(1)Q_1(1) = 0$. Since $(P_i(1), Q_i(1)) \neq (0, 0)$, for all $i = 1, \ldots, m$, we have

$$\begin{aligned} &P_1(1) = P_j(1) = 0 \quad \text{and hence} \quad P_1 = P_j \equiv 0 , \quad \text{or} \\ &Q_1(1) = Q_j(1) = 0 \quad \text{and hence} \quad Q_1 = Q_j \equiv 0 . \end{aligned}$$

Since $j \geq 2$ was arbitrarily chosen, all P_i or all Q_i are zero polynomials, for $i = 1, \ldots, m$, and thus, we have

$$A' \subseteq \{(a, y, ay) \mid y \in \mathbb{N}\} \subseteq A_{\text{prod}} , \quad \text{or} \quad A' \subseteq \{(x, b, bx) \mid x \in \mathbb{N}\} \subseteq A_{\text{prod}} .$$

Hence, there are s, t and $a_1, \ldots, a_s, b_1, \ldots, b_t$ such that

$$A_{\text{prod}} = \bigcup_{i=1}^{s} \{(a_i, y_i, a_i y_i) \mid y_i \in \mathbb{N}\} \cup \bigcup_{j=1}^{t} \{(x_j, b_j, x_j b_j) \mid x_j \in \mathbb{N}\} .$$

Projection to the first two components should yield $\mathbb{N}^2$. However, we obtain the union of the sets $\{(a_i, y_i) \mid y_i \in \mathbb{N}\}$ and $\{(x_j, b_j) \mid x_j \in \mathbb{N}\}$, which is a proper subset of $\mathbb{N}^2$, a contradiction.

As the semi-linear sets can be characterized as the Parikh images of the regular and the context-free languages, one may ask for such a characterization of the simple semi-polynomial sets. In [8] it is shown that all simple semi-polynomial sets (and more sets, e.g., A_{prod} of Example 2) can be obtained as the Parikh images of indexed languages, i.e., those languages which are recognized by level-two pushdown automata (pushdown automata with a stack of stacks).

4 Intersection Problems

We show two results: Simple semi-polynomial sets are not closed under intersection whereas the intersection of a simple semi-polynomial set with a semi-linear set of a 'special kind' is again a simple semi-polynomial set.

Theorem 3. *There exist two simple quadratic sets the intersection of which is not simple semi-polynomial.*

Proof. Consider the simple quadratic sets

$$A = \left\{ \binom{(k_1+1)^2 + (k_2+1)^2}{k_3} \mid k_1, k_2, k_3 \in \mathbb{N} \right\} \text{ and } B = \left\{ \binom{k^2}{k} \mid k \in \mathbb{N} \right\} .$$

The intersection $A \cap B$ consists of the pairs (k^2, k) where $k^2 = (k_1+1)^2+(k_2+1)^2$, for certain k_1, k_2, is a solution of the Pythagoras equation in positive integers. It is known from elementary number theory (see, e.g., [6]) that these pairs coincide with the pairs $(w^2(u^2+v^2)^2, w(u^2+v^2))$ where u, v, w are positive integers. By the Two-Square Theorem (see, e.g., [6]), the latter pairs coincide with the pairs (n^2, n) of natural numbers where $n \geq 2$ is even or divisible by some prime $p \equiv 1 \pmod 4$.

Suppose that $A \cap B$ is simple semi-polynomial, i.e. a union of sets

$$A_i = \left\{ \binom{\alpha + P_1(k_1) + \cdots + P_m(k_m)}{\beta + Q_1(k_1) + \cdots + Q_m(k_m)} \mid k_1, \ldots k_m \in \mathbb{N} \right\} \quad (i = 1, \ldots, s)$$

where $\alpha, \beta \in \mathbb{N}$ and $P_1, \ldots, P_m, Q_1, \ldots, Q_m \in \mathbb{N}[X]$ are nonzero polynomials without constants. Setting $k_1 = \cdots = k_m = 0$, we obtain $\alpha = \beta^2$. Fixing some $j \in \{1, \ldots, m\}$ and setting $k_r = 0$, for all $1 \leq r \leq s$ with $r \neq j$, we obtain $P_j(k_j) + \beta^2 = (Q_j(k_j) + \beta)^2$ and thus $P_j(k_j) = (Q_j(k_j))^2 + 2\beta Q_j(k_j)$, for each $k_j \in \mathbb{N}$. If $m \geq 2$, we would have for $1 < j \leq m$

$$P_1(k_1) + P_j(k_j) + \beta^2 = (Q_1(k_1) + Q_j(k_j) + \beta)^2 \ ,$$

and hence, $Q_1(k_1)Q_j(k_j) = 0$, for all $k_1, k_j \in \mathbb{N}$, which would imply that one of Q_1 and Q_j is zero, a contradiction. Hence, we have $m = 1$ and can assume

$$A_i = \left\{ \binom{(R_i(k_i))^2}{R_i(k_i)} \mid k_i \in \mathbb{N} \right\}$$

for some polynomial $R_i \in \mathbb{N}[X]$.

Let $N := 4K$, where K is the least common multiple of the coefficients of $R_1, \ldots, R_s$. Among these polynomials let $R_1, \ldots, R_t$ be the ones of degree 1, say, $R_i = a_i + b_i(X)$, which yields, for $i = 1, \ldots, t$,

$$R_i(\mathbb{N}) = a_i + b_i\mathbb{N} = \bigcup_{j=0}^{m} a_{ij} + N\mathbb{N} \tag{7}$$

as a disjoint union, for some $0 \leq m < N$. By Dirichlet's Prime-Number Theorem, each arithmetic progression $c+N\mathbb{N}$, where $c \equiv 3 \pmod 4$ and where c and N are relatively prime, contains infinitely many primes $q \equiv 3 \pmod 4$. Thus, $c + N\mathbb{N}$ does not occur in the union (7). Now, let p be a prime with $p \equiv 1 \pmod N$. Then, for any $n \in pc + pN\mathbb{N}$, the pair (n^2, n) belongs to $A \cap B$, which means that

$$pc + pN\mathbb{N} \subseteq \bigcup_{i=t+1}^{s} R_i(\mathbb{N}) \ , \tag{8}$$

where, for each $i = t+1, \ldots, s$, R_i is either a constant or of degree ≥ 2. In the latter case we have, $R_i(k_i + 1) - R_i(k_i) \geq 2k_i$, for each $k_i \in \mathbb{N}$. In other words, these differences tend to infinity, which contradicts (8). □

We now exhibit a case of an intersection operation which does not lead out of the simple semi-polynomial sets, respectively the semi-polynomial sets. We consider the intersection with a special form of semi-linear set: A set $A \subseteq \mathbb{N}^n$ is called *componentwise linear* if there are linear sets $A_1, \ldots, A_n \subseteq \mathbb{N}$ such that $A = A_1 \times \cdots \times A_n$. The set A is called *componentwise semi-linear* if it is a finite union of componentwise linear sets.

To simplify notation, in the sequel we do not distinguish between an ordinary natural number and a one-dimensional vector of natural numbers.

Theorem 4. *Let $n \geq 1$. If $A \subseteq \mathbb{N}^n$ is componentwise semi-linear and $B \subseteq \mathbb{N}^n$ is simple semi-polynomial (respectively semi-polynomial) of degree $d \geq 1$, then $A \cap B$ is simple semi-polynomial (respectively semi-polynomial) of degree d. Moreover, if A and B are given by their generators, generators of $A \cap B$ can be computed and hence nonemptiness of $A \cap B$ be checked effectively.*

Proof. We only consider simple semi-polynomial sets; the proof works in the same way for semi-polynomial sets. Furthermore, it suffices to consider the case that A is componentwise linear and B is a simple polynomial set. We construct a simple semi-polynomial representation of $A \cap B$ by a refinement process which successively covers more and more of the n components. For the intersection of the projections of A and B to the first component we obtain a simple semi-polynomial representation, which is then made thinner by taking into account the other components, one by one. To simplify matters, let us first treat the case that B is a simple quadratic set.

Case 1. Let $n = 1$, i.e. $A, B \subseteq \mathbb{N}$. Suppose $A, B \subseteq \mathbb{N}$ are given by

$$A = \{u_0 + k_1 u_1 + \ldots + k_m u_m \mid k_1, \ldots, k_m \in \mathbb{N}\} \ ,$$
$$B = \{v_0 + k_1 v_1 + k_1^2 w_1 + \cdots + k_r v_r + k_r^2 w_r \mid k_1, \ldots, k_r \in \mathbb{N}\} \ ,$$

where the u_i, v_i, w_i are natural numbers and $v_i + w_i \geq 1$ for all $i = 1, \ldots, r$. In order to avoid trivial cases, assume $u_i \geq 1$ for all $i = 1, \ldots, m$.

Let g be the greatest common divisor of $u_1, \ldots, u_m$. Clearly, $A \subseteq \{u_0 + kg \mid k \in \mathbb{N}\}$, and for sufficiently large c_0 (we may take $c_0 := u_0 + u_1 \cdots u_m$) the set

$$C := \{c_0 + kg \mid k \in \mathbb{N}\}$$

contains precisely the A-elements from c_0 onwards.

The set $A \setminus C$ is finite; so by decidability of B one computes the set $F := (A \setminus C) \cap B$.

The intersection $A \cap B$ is the union of F with $C \cap B$. Elements in $C \cap B$ have to be solutions of the congruence

$$v_0 + k_1 v_1 + k_1^2 w_1 + \ldots + k_r v_r + k_r^2 w_r \equiv c_0 \pmod{g} \ . \tag{9}$$

It suffices to check the congruence for values $k_i < g$. If no solution exists, we have $C \cap B = \emptyset$ and $A \cap B = F$. If a solution exists, say $\bar{s} = (s_1, \ldots, s_r) \in \{0, \ldots, g-1\}^r$, it produces the B-elements

$$x = v_0 + m_1 v_1 + m_1^2 w_1 + \ldots + m_r v_r + m_r^2 w_r \ , \tag{10}$$

where $m_i = s_i + n_i g$, $n_i \in \mathbb{N}$.

In order to ensure $x \geq c_0$ (i.e. to obtain $C \cap B$) it suffices to require $\sum_{i=1}^r n_i > \lfloor c_0/g \rfloor$. Only finitely many C-elements are missed by this requirement; we collect them in the finite set $E_{\bar{s}}$. The case $\sum_{i=1}^r n_i > \lfloor c_0/g \rfloor$ is split into finitely many subcases $n_1 \geq l_{1j}, \ldots, n_r \geq l_{rj}$ (where j ranges over a finite set J). If we write $l_{ij} + n_i$ ($n_i \geq 0$) instead of $n_i \geq l_{ij}$ and substitute $m_i = s_i + n_i g$ in (10) by $s_i + (l_{ij} + n_i)g$, we obtain the following simple quadratic set in the n_i:

$$C_{\bar{s},j} = \{v_0' + n_1 v_1' + n_1^2 w_1' + \ldots + n_r v_r' + n_r^2 w_r' \mid n_1, \ldots, n_r \in \mathbb{N}\} \ . \tag{11}$$

The intersection $C \cap B$ is the union of the finite sets $E_{\bar{s}}$ and the finitely many simple quadratic sets $C_{\bar{s},j}$. Hence, $A \cap B$ is a simple semi-quadratic set. Furthermore, the set is empty iff the finite set F mentioned above is empty and the congruence (9) has no solution.

Case 2. Let $n > 1$. Consider a componentwise linear set $A \subseteq \mathbb{N}^n$ and a simple quadratic set $B \subseteq \mathbb{N}^n$:

$$A = A_1 \times \cdots \times A_n \ ,$$
$$B = \{\bar{v}_0 + k_1 \bar{v}_1 + k_1^2 \bar{w}_1 + \cdots + k_r \bar{v}_r + k_r^2 \bar{w}_r \mid k_1, \ldots, k_r \in \mathbb{N}\} \ ,$$

where $\bar{v}_i, \bar{w}_i \in \mathbb{N}^n$.

We analyze the intersection $A \cap B$ for the first component as above. If this intersection is empty, this is also true for $A \cap B$ and we are done. Otherwise we invoke Case 1 for the first components of A and B, which shows that $(A)_1 \cap (B)_1$ is a simple semi-quadratic set.[5] If this intersection is finite (which means that (11) above is empty), it suffices to decide for each of the corresponding n-tuples $(k_1, \ldots, k_r)$ whether the second component of the A-element generated by $k_1, \ldots, k_r$ belongs to the simple quadratic set given by the second components of the B-elements.

If $(A)_1 \cap (B)_1$ is infinite, consider a set $C_{\bar{s},j}$ as constructed above. We have to find the $(B)_2$-elements of the form

$$(\bar{v}'_0)_2 + n_1(\bar{v}'_1)_2 + n_1^2(\bar{w}'_1)_2 + \cdots + n_r(\bar{v}'_r)_2 + n_r^2(\bar{w}'_r)_2 \ .$$

This is a simple quadratic set in the n_i, and the procedure of Case 1 can be invoked to find those vectors $(n_1, \ldots, n_r)$ which describe the second component of an A-element. We obtain a simple semi-quadratic representation of $(A)_{1,2} \cap (B)_{1,2}$ (the intersection of A and B restricted to the first two components), which moreover is testable for nonemptiness. After $n-1$ steps of this kind the procedure terminates with a simple semi-quadratic representation of $A \cap B$, giving also the information whether $A \cap B = \emptyset$.

The same argument is applicable to (simple) polynomial sets B instead of simple quadratic ones. The simple quadratic expressions in (9), (10), (11) change to (simple) polynomial ones, but the form of the solutions $(m_1, \ldots, m_r)$ still is of the form $m_i = s_i + n_i g$ since the component sets $(A)_j$ are (componentwise) linear. So the proof carries over in the obvious way. □

We have shown that for a (simple) semi-polynomial set B the intersection with a componentwise semi-linear set A yields again a (simple) semi-polynomial set whereas this fails in general for a simple semi-polynomial set A. The intermediate case of a semi-linear set A remains open, even for the weaker statement that nonemptiness of $A \cap B$ is decidable. Let us note that this decision problem is as hard as for the intersection of semi-polynomial sets in general. In fact, a decidability proof for semi-linear A and (simple) semi-polynomial B would immediately yield decidability of nonemptiness for intersections of two arbitrary (simple) semi-polynomial sets. The argument resembles the remark at the beginning of Sect. 3. Consider $C = \{(P_1(k_1, \ldots, k_r), \ldots, P_n(k_1, \ldots, k_r)) \mid k_1, \ldots, k_r \in \mathbb{N}\}$ and $D = \{(Q_1(l_1, \ldots, l_s), \ldots, Q_n(l_1, \ldots, l_s)) \mid l_1, \ldots, l_s \in \mathbb{N}\}$. We have $C \cap D \neq \emptyset$ iff there are $i_1, \ldots, i_n$ with $P_1(k_1, \ldots, k_r) = i_1 = Q_1(l_1, \ldots, l_s)$, $\ldots$, $P_n(k_1, \ldots, k_r) = i_n = Q_n(l_1, \ldots, l_s)$. This means that the polynomial set (of dimension $2n$)

$$B = \{(P_1(\bar{k}), Q_1(\bar{l}), \ldots, P_n(\bar{k}), Q_n(\bar{l})) \mid k_1, \ldots, k_r, l_1, \ldots, l_s \in \mathbb{N}\}$$

has a nonempty intersection with the linear set

$$A = \{(i_1(1,1,0,\ldots 0) + \cdots + i_n(0,\ldots,0,1,1) \mid i_1, \ldots, i_n \in \mathbb{N}\} \ .$$

[5] For a set $X \subseteq \mathbb{N}^n$, the set $(X)_i$ denotes $\{(\bar{x})_i \mid \bar{x} \in X\}$. Further, note that $(A)_i = A_i$ since A is componentwise linear.

5 Quadratic Forms

It is known that the undecidability of Hilbert's Tenth Problem holds for polynomial equations of degree four and for *systems* of polynomial equations of degree two (see [11]).

In this context, Xie, Dang, and Ibarra [16] solved a restricted case regarding pairs of quadratic equations which are generated by products of linear forms.

If only a *single* quadratic form

$$Q(x_1, \ldots, x_n) := \sum_{1 \le i,j \le n} a_{ij} x_i x_j + \sum_{1 \le i \le n} b_i x_i + c$$

is considered, where $a_{ij}, b_i, c \in \mathbb{Z}$, for $1 \le i, j \le n$, then the solvability of the equation $Q(x_1, \ldots, x_n) = 0$ has also been shown decidable, both in integers and in natural numbers. The solvability in integers follows from Siegel's work [15]. Regarding the solvability in natural numbers, a standard approach is to apply Lagrange's Theorem which characterizes the natural numbers as the sums of four squares (of integers). However, adding this requirement for each variable to a quadratic equation results in a *system* of quadratic equations, where Siegel's analysis does not apply. In a recent paper, Grunewald and Segal [5] show that the solvability of quadratic equations in integers stays decidable even under constraints given by linear inequalities:

Theorem 5 ([5]). *Given a quadratic form $Q \in \mathbb{Z}[X_1, \ldots, X_n]$ and linear forms $L_1, \ldots, L_k \in \mathbb{Z}[X_1, \ldots, X_n]$, it is decidable whether a system*

$$Q(x_1, \ldots, x_n) = 0 \ , \tag{12a}$$

$$L_j(x_1, \ldots, x_n) \ \# \ c_j, \text{ where } c_j \in \mathbb{Z} \text{ and } \# \in \{<, \le\}, \text{ for } j = 1, \ldots, k \ , \tag{12b}$$

$$(x_1, \ldots, x_n) \equiv (h_1, \ldots, h_n) \pmod{m}, \text{ where } h_1, \ldots, h_n \in \mathbb{Z},\ m \in \mathbb{N} \ , \tag{12c}$$

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

A decision procedure for solvability of quadratic equations in natural numbers can be obtained from Thm. 5 by imposing linear constraints of the form $-x_i \le 0$ for (12b).

The proof of the theorem requires deep number-theoretic constructions and does not come (as yet) with a complexity analysis. Rather than studying the general case it seems more tractable trying to isolate cases where reasonable complexity bounds can be provided.

In the sequel, we demonstrate how the decidability of the solvability of quadratic equations, in particular Thm. 5, can be applied to obtain two kinds of generalizations of semi-linear sets which are yet so modest that decidability results on the intersection problem are retained. The first result is concerned with sets defined via solutions of quadratic equations, and the second one refers to sets which are enumerated by quadratic and linear forms.

As a corollary of Thm. 5, the nonemptiness problem for the intersection of a semi-linear set with the solution set of a quadratic equation is decidable. For this, it suffices to recall that a semi-linear set is the solution set of a linear (in)equation system [4].

Corollary 6. *Nonemptiness of the intersection of a semi-linear set $A \subseteq \mathbb{N}^n$ with the solution set S of a quadratic equation $Q(x_1, \ldots, x_n) = 0$ is decidable.*

This can be applied, for example, to the following scenario indicated in Sect. 1: Given a system that produces a semi-linear set $A \subseteq \mathbb{N}^n$ (for instance, a finite automaton or a pushdown system) and an acceptance constraint given by a quadratic equation $Q(\bar{x}) = 0$ for $Q \in \mathbb{Z}[X_1, \ldots, X_n]$ then it can be decided whether some run of the automaton exists that satisfies the acceptance condition.

Next we introduce sets which refer to the value sets of quadratic forms $Q(\bar{x})$ rather than solutions of the equation $Q(\bar{x}) = 0$. We call a set $A \subseteq \mathbb{N}^n$ *one-quadratic* if A is a polynomial set such that the first component is given by a quadratic form $Q \in \mathbb{N}[X_1, \ldots, X_m]$ and the other components by linear forms $L_2, \ldots, L_n \in \mathbb{N}[X_1, \ldots, X_m]$:

$$A = \{(Q(k_1, \ldots, k_m), L_2(k_1, \ldots, k_m), \ldots, L_n(k_1, \ldots, k_m)) \mid k_1, \ldots, k_m \in \mathbb{N}\} \ .$$

A *semi-one-quadratic set* is a finite union of one-quadratic sets. The semi-one-quadratic sets encompass the semi-linear ones.

Deciding the nonemptiness of the intersection of one-quadratic sets leads to solving an equation system of the form (12): Given one-quadratic subsets A and B that are defined by $Q, L_2, \ldots, L_n \in \mathbb{N}[X_1, \ldots, X_m]$ and $Q', L'_2, \ldots, L'_n \in \mathbb{N}[X_1, \ldots, X_r]$, respectively, we have that $A \cap B \neq \emptyset$ iff there are $k_1, \ldots, k_m$ and $k'_1, \ldots, k'_r \in \mathbb{N}$ such that $Q(k_1, \ldots, k_m) = Q'(k'_1, \ldots, k'_r)$ and $L_j(k_1, \ldots, k_m) = L'_j(k'_1, \ldots, k'_r)$, for $j = 2, \ldots, n$. Now, we write the equations as $Q - Q' = 0$ and $L_j - L'_j = 0$, and then replace $L_j - L'_j = 0$ by $L_j - L'_j \leq 0$ and $L'_j - L_j \leq 0$. Hence, Thm. 5 can be applied. For the step from one-quadratic sets to semi-one-quadratic sets, we just use the distributivity of union over intersection.

Corollary 7. *Nonemptiness of the intersection of two semi-one-quadratic sets (and hence of a semi-one-quadratic with a semi-linear set) is decidable.*

6 Conclusion

The results of this paper are a small step into a field which is not well explored so far. We have suggested some classes of arithmetical constraints beyond the framework of semi-linear sets where effective solutions are possible. The main purpose of this note is to indicate some perspectives. Let us list some open problems:

1. Study the closure properties of simple semi-polynomial and simple semi-quadratic sets. In particular, does the intersection of a simple semi-polynomial set with a semi-linear set yield again a simple semi-polynomial set? What about the case of a semi-quadratic set?
2. The product relation of Example 2 shows a weakness of the simple semi-polynomial sets. One observes, however, that $2mn = (m+n)^2 - m^2 - n^2$, for any $m, n \in \mathbb{N}$, and thus the product function is (up to a factor) the difference of functions the graphs of which are simple quadratic. This suggests the study of the closure of simple (semi-)quadratic sets under additive operations.

3. Better upper bounds for deciding the membership in a simple semi-polynomial set should be found.
4. A way of extending the simple semi-polynomial sets is to consider the Parikh images of indexed languages. This would cover not only the product relation but also exponential relations like $\{(n, 2^n) \mid n \in \mathbb{N}\}$ (see [8]).
5. Start an algorithmic analysis of [5], and find forms of quadratic equations where reasonable upper bounds for deciding solvability can be established.
6. Study the case of quadratic inequations rather than equations.

References

1. Bruyére, V., Dall'Olio, E., Raskin, J.F.: Durations, parametric model-checking in timed automata with Presburger arithmetic. In Proc. STACS 2003. LNCS 2607. Springer (2003) 687–698
2. Dal Zilio, S., Lugiez, D.: XML schema, tree logic and sheaves automata. In Proc. RTA 2003. LNCS 2706. Springer (2003) 246–263
3. Dang, Z., Ibarra, O.H., Bultan, T., Kemmerer, R.A., Su, J.: Binary reachability analysis of discrete pushdown timed automata. In Proc. CAV 2000. LNCS 1855. Springer (2000) 69–84
4. Ginsburg, S., Spanier, E.H.: Semigroups, Presburger formulas, and languages. Pacific J. Math. **16** (1966) 285–296
5. Grunewald, F., Segal, D.: On the integer solutions of quadratic equations. J. Reine Angew. Math. **569** (2004) 13–45
6. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. 5th edn. Oxford University Press (1979)
7. Ibarra, O.H., Bultan, T., Su, J.: Reachability analysis for some models of infinite-state transition systems. In Proc. CONCUR 2000. LNCS 1877. Springer (2000) 183–198
8. Karianto, W.: Parikh automata with pushdown stack. Diploma thesis, RWTH Aachen (2004) Available at http://www-i7.informatik.rwth-aachen.de.
9. Klaedtke, F., Rueß, H.: Monadic second-order logics with cardinalities. In Proc. ICALP 2003. LNCS 2719. Springer (2003) 681–696
10. Lugiez, D.: Counting and equality constraints for multitree automata. In Proc. FOSSACS 2003. LNCS 2620. Springer (2003) 328–342
11. Matiyasevich, Y.V.: Hilbert's Tenth Problem. MIT Press (1993)
12. Parikh, R.J.: On context-free languages. J. ACM **13** (1966) 570–581
13. Seidl, H., Schwentick, T., Muscholl, A.: Numerical document queries. In Proc. PODS 2003. ACM Press (2003) 155–166
14. Seidl, H., Schwentick, T., Muscholl, A., Habermehl, P.: Counting in trees for free. In Proc. ICALP 2004. LNCS 3142. Springer (2004) 1136–1149
15. Siegel, C.L.: Zur Theorie der quadratischen Formen. Nachrichten der Akademie der Wissenschaften in Göttingen, II, Mathematisch-Physikalische Klasse **3** (1972) 21–46
16. Xie, G., Dang, Z., Ibarra, O.H.: A solvable class of quadratic Diophantine equations with applications to verification of infinite-state systems. In Proc. ICALP 2003. LNCS 2719. Springer (2003) 668–680