

# On Intersection Problems for Polynomially Generated Sets

Wong Karianto<sup>1</sup>   Aloys Krieg<sup>2</sup>   Wolfgang Thomas<sup>1</sup>

<sup>1</sup>Lehrstuhl für Informatik 7  
RWTH Aachen

<sup>2</sup>Lehrstuhl A für Mathematik  
RWTH Aachen

33rd International Colloquium on  
Automata, Languages, and Programming  
Venice, 10–14 July 2006

**Presburger arithmetic** and **semi-linear sets**: well-known framework for algorithmic applications and verification where aspect of infinity arises from the domain of **natural numbers**.

**Presburger arithmetic** and **semi-linear sets**: well-known framework for algorithmic applications and verification where aspect of infinity arises from the domain of **natural numbers**.

**System** runs induce a **semi-linear set** of vectors of natural numbers.

**Specification** is a **semi-linear set** or, equivalently, a formula of **Presburger arithmetic** (i.e. FO-formula over the structure  $(\mathbb{N}, +)$ ).

**Presburger arithmetic** and **semi-linear sets**: well-known framework for algorithmic applications and verification where aspect of infinity arises from the domain of **natural numbers**.

**System** runs induce a **semi-linear set** of vectors of natural numbers.

**Specification** is a **semi-linear set** or, equivalently, a formula of **Presburger arithmetic** (i.e. FO-formula over the structure  $(\mathbb{N}, +)$ ).

Verification amounts to checking the **intersection** of both sets for **nonemptiness**.

**Presburger arithmetic** and **semi-linear sets**: well-known framework for algorithmic applications and verification where aspect of infinity arises from the domain of **natural numbers**.

**System** runs induce a **semi-linear set** of vectors of natural numbers.

**Specification** is a **semi-linear set** or, equivalently, a formula of **Presburger arithmetic** (i.e. FO-formula over the structure  $(\mathbb{N}, +)$ ).

Verification amounts to checking the **intersection** of both sets for **nonemptiness**.

## Aim

A framework **beyond** the semi-linear sets or Presburger arithmetic

- 1 Preliminaries
- 2 Polynomially Generated Sets
- 3 On the Intersection Problems
- 4 Quadratic Forms

1 Preliminaries

2 Polynomially Generated Sets

3 On the Intersection Problems

4 Quadratic Forms

**Linear set:**  $\{\bar{u}_0 + k_1\bar{u}_1 + \dots + k_m\bar{u}_m \mid k_1, \dots, k_m \in \mathbb{N}\}$  for some  $\bar{u}_0, \bar{u}_1, \dots, \bar{u}_m \in \mathbb{N}^n$

**Semi-linear set:** finite union of linear sets



**Linear set:**  $\{\bar{u}_0 + k_1\bar{u}_1 + \dots + k_m\bar{u}_m \mid k_1, \dots, k_m \in \mathbb{N}\}$  for some  $\bar{u}_0, \bar{u}_1, \dots, \bar{u}_m \in \mathbb{N}^n$

**Semi-linear set:** finite union of linear sets

**Presburger arithmetic:** first-order theory of  $(\mathbb{N}, +)$

A Presburger formula  $\varphi(x_1, \dots, x_n)$  defines the set

$$\{(u_1, \dots, u_n) \in \mathbb{N}^n \mid (\mathbb{N}, +) \models \varphi[u_1, \dots, u_n]\}$$

of vector of natural numbers.

**Linear set:**  $\{\bar{u}_0 + k_1\bar{u}_1 + \dots + k_m\bar{u}_m \mid k_1, \dots, k_m \in \mathbb{N}\}$  for some  $\bar{u}_0, \bar{u}_1, \dots, \bar{u}_m \in \mathbb{N}^n$

**Semi-linear set:** finite union of linear sets

**Presburger arithmetic:** first-order theory of  $(\mathbb{N}, +)$

A Presburger formula  $\varphi(x_1, \dots, x_n)$  defines the set

$$\{(u_1, \dots, u_n) \in \mathbb{N}^n \mid (\mathbb{N}, +) \models \varphi[u_1, \dots, u_n]\}$$

of vector of natural numbers.

Ginsburg and Spanier's theorems:

- equivalence between semi-linear and Presburger-definable sets
- effective closure under Boolean operations and projections

**Linear set:**  $\{\bar{u}_0 + k_1\bar{u}_1 + \dots + k_m\bar{u}_m \mid k_1, \dots, k_m \in \mathbb{N}\}$  for some  $\bar{u}_0, \bar{u}_1, \dots, \bar{u}_m \in \mathbb{N}^n$

**Semi-linear set:** finite union of linear sets

**Presburger arithmetic:** first-order theory of  $(\mathbb{N}, +)$

A Presburger formula  $\varphi(x_1, \dots, x_n)$  defines the set

$$\{(u_1, \dots, u_n) \in \mathbb{N}^n \mid (\mathbb{N}, +) \models \varphi[u_1, \dots, u_n]\}$$

of vector of natural numbers.

Ginsburg and Spanier's theorems:

- equivalence between semi-linear and Presburger-definable sets
- effective closure under Boolean operations and projections

Parikh's theorem:

- The image of any context-free language under the **Parikh mapping** is **effectively semi-linear**.

$$\begin{aligned}\Phi(w) &= (|w|_{a_1}, \dots, |w|_{a_n}) \\ \Phi(L) &= \{\Phi(w) \mid w \in L\}\end{aligned}$$

Parikh automaton [Klaedtke & Ruess, ICALP 2003] :

- finite automaton  $\mathcal{A}$  over extended alphabet  $\Sigma \times D$  ( $D \subseteq \mathbb{N}^n$ )
- Presburger formula  $\varphi(x_1, \dots, x_n)$  (or semi-linear set  $C \subseteq \mathbb{N}^n$ )

Parikh automaton [Klaedtke & Ruesch, ICALP 2003] :

- finite automaton  $\mathcal{A}$  over extended alphabet  $\Sigma \times D$  ( $D \subseteq \mathbb{N}^n$ )
- Presburger formula  $\varphi(x_1, \dots, x_n)$  (or semi-linear set  $C \subseteq \mathbb{N}^n$ )

## Example

- $\mathcal{A}$ :  

```
graph LR; S(( )) -- "(a, (1,0,0))" --> S1(( )); S1 -- "(a, (1,0,0))" --> S1; S1 -- "(b, (0,1,0))" --> S2(( )); S2 -- "(b, (0,1,0))" --> S2; S2 -- "(c, (0,0,1))" --> S3((( ))) ; S3 -- "(c, (0,0,1))" --> S3
```
- $\varphi$  :  $x_1 \geq 2(x_2 + x_3) \wedge x_2 = x_3$

Acceptance of a word requires **two conditions**:

- acceptance by automaton  $\mathcal{A}$  (via a run)
- sum of vectors accumulated along the run must satisfy  $\varphi$

Parikh automaton [Klaedtke & Ruesch, ICALP 2003] :

- finite automaton  $\mathcal{A}$  over extended alphabet  $\Sigma \times D$  ( $D \subseteq \mathbb{N}^n$ )
- Presburger formula  $\varphi(x_1, \dots, x_n)$  (or semi-linear set  $C \subseteq \mathbb{N}^n$ )

## Example

- $\mathcal{A}$ :  

```
graph LR; S(( )) -- "(a, (1,0,0))" --> S2(( )); S2 -- "(a, (1,0,0))" --> S2; S2 -- "(b, (0,1,0))" --> S3(( )); S3 -- "(b, (0,1,0))" --> S3; S3 -- "(c, (0,0,1))" --> S4((( ))) ; S4 -- "(c, (0,0,1))" --> S4
```
- $\varphi$  :  $x_1 \geq 2(x_2 + x_3) \wedge x_2 = x_3$

Acceptance of a word requires **two conditions**:

- acceptance by automaton  $\mathcal{A}$  (via a run)
- sum of vectors accumulated along the run must satisfy  $\varphi$

$L(\mathcal{A}, \varphi)$  : words of the form  $a^+b^+c^+$  satisfying “the first half of  $w$  consists only of  $a$ , and in the second half the number of  $b$ 's and  $c$ 's coincide”

1 Preliminaries

**2 Polynomially Generated Sets**

3 On the Intersection Problems

4 Quadratic Forms

Aim:

- generalize (semi-)linear sets to sets **generated by polynomials**
- solve the **intersection problem**, i.e. the **nonemptiness** problem for the **intersection** of two subsets of  $\mathbb{N}^n$



Aim:

- generalize (semi-)linear sets to sets **generated by polynomials**
- solve the **intersection problem**, i.e. the **nonemptiness** problem for the **intersection** of two subsets of  $\mathbb{N}^n$

$A \subseteq \mathbb{N}^n$  is **linear** if it is of the form

$$\{\bar{u}_0 + k_1\bar{u}_1 + \cdots + k_m\bar{u}_m \mid k_1, \dots, k_m \in \mathbb{N}\}.$$

Aim:

- generalize (semi-)linear sets to sets **generated by polynomials**
- solve the **intersection problem**, i.e. the **nonemptiness** problem for the **intersection** of two subsets of  $\mathbb{N}^n$

$A \subseteq \mathbb{N}^n$  is **linear** if it is of the form

$$\left\{ \begin{pmatrix} u_{01} + k_1 u_{11} + \cdots + k_m u_{m1} \\ \vdots \\ u_{0n} + k_1 u_{1n} + \cdots + k_m u_{mn} \end{pmatrix} \mid k_1, \dots, k_m \in \mathbb{N} \right\}$$

Aim:

- generalize (semi-)linear sets to sets **generated by polynomials**
- solve the **intersection problem**, i.e. the **nonemptiness** problem for the **intersection** of two subsets of  $\mathbb{N}^n$

$A \subseteq \mathbb{N}^n$  is **linear** if it is of the form

$$\left\{ \begin{pmatrix} u_{01} + k_1 u_{11} + \cdots + k_m u_{m1} \\ \vdots \\ u_{0n} + k_1 u_{1n} + \cdots + k_m u_{mn} \end{pmatrix} \mid k_1, \dots, k_m \in \mathbb{N} \right\}$$

linear functions in  $k_1, \dots, k_m$

Aim:

- generalize (semi-)linear sets to sets **generated by polynomials**
- solve the **intersection problem**, i.e. the **nonemptiness** problem for the **intersection** of two subsets of  $\mathbb{N}^n$

$A \subseteq \mathbb{N}^n$  is **linear** if it is of the form

$$\left\{ \begin{pmatrix} u_{01} + k_1 u_{11} + \cdots + k_m u_{m1} \\ \vdots \\ u_{0n} + k_1 u_{1n} + \cdots + k_m u_{mn} \end{pmatrix} \mid k_1, \dots, k_m \in \mathbb{N} \right\}$$

**linear functions in  $k_1, \dots, k_m$**

## Definition

$A \subseteq \mathbb{N}^n$  is called **polynomial** if it is of the form

$$\left\{ \begin{pmatrix} P_1(k_1, \dots, k_m) \\ \vdots \\ P_n(k_1, \dots, k_m) \end{pmatrix} \mid k_1, \dots, k_m \in \mathbb{N} \right\}$$

for some polynomials  $P_1, \dots, P_n \in \mathbb{N}[X_1, \dots, X_m]$ .

**Semi-polynomial set:** finite union of polynomial sets.

## Example

- square relation:  $\{(x, y) \in \mathbb{N}^2 \mid y = x^2\}$
- product relation:  $\{(x, y, z) \in \mathbb{N}^3 \mid z = x \cdot y\}$

## Example

- square relation:  $\{(x, y) \in \mathbb{N}^2 \mid y = x^2\}$
- product relation:  $\{(x, y, z) \in \mathbb{N}^3 \mid z = x \cdot y\}$

Some (trivial) properties of semi-polynomial sets:

- closure under finite union and projection
- decidability of membership problem
- strict hierarchy w.r.t. degree of polynomials
- do not capture sets like  $\{(x, y) \in \mathbb{N}^2 \mid y = 2^x\}$

## Hilbert's Tenth Problem

Given a polynomial  $P \in \mathbb{Z}[X_1, \dots, X_m]$ , does the polynomial equation

$$P(k_1, \dots, k_m) = 0$$

have a solution in natural numbers?  $\rightsquigarrow$  **undecidable**

## Hilbert's Tenth Problem

Given polynomials  $Q, R \in \mathbb{N}[X_1, \dots, X_m]$ , does the polynomial equation

$$Q(k_1, \dots, k_m) = R(k_1, \dots, k_m)$$

have a solution in natural numbers?  $\rightsquigarrow$  **undecidable**



## Hilbert's Tenth Problem

Given polynomials  $Q, R \in \mathbb{N}[X_1, \dots, X_m]$ , does the polynomial equation

$$Q(k_1, \dots, k_m) = R(k_1, \dots, k_m)$$

have a solution in natural numbers?  $\rightsquigarrow$  **undecidable**

Reformulation in terms of intersection problem:

- Let  $\text{id}_{\mathbb{N}} := \{(k, k) \mid k \in \mathbb{N}\}$  (identity relation).
- Is the intersection

$$\left\{ \left( \begin{array}{l} Q(k_1, \dots, k_m) \\ R(k_1, \dots, k_m) \end{array} \right) \mid k_1, \dots, k_m \in \mathbb{N} \right\} \cap \text{id}_{\mathbb{N}}$$

nonempty?

## Hilbert's Tenth Problem

Given polynomials  $Q, R \in \mathbb{N}[X_1, \dots, X_m]$ , does the polynomial equation

$$Q(k_1, \dots, k_m) = R(k_1, \dots, k_m)$$

have a solution in natural numbers?  $\rightsquigarrow$  **undecidable**

Reformulation in terms of intersection problem:

- Let  $\text{id}_{\mathbb{N}} := \{(k, k) \mid k \in \mathbb{N}\}$  (identity relation).
- Is the intersection

$$\left\{ \left( \begin{array}{l} Q(k_1, \dots, k_m) \\ R(k_1, \dots, k_m) \end{array} \right) \mid k_1, \dots, k_m \in \mathbb{N} \right\} \cap \text{id}_{\mathbb{N}}$$

nonempty?

## Corollary

Nonemptiness of intersection of polynomial sets and linear sets is **undecidable**.

## Definition

$A \subseteq \mathbb{N}^n$  is a **simple polynomial set** if it is of the form

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

where  $P_{ij} \in \mathbb{N}[X]$  are (univariate) polynomials.

**Simple semi-polynomial set:** finite union of simple polynomial sets.

## Definition

$A \subseteq \mathbb{N}^n$  is a **simple polynomial set** if it is of the form

$$\left\{ \left( \begin{array}{c} P_{11}(k_1) + \cdots + P_{1m}(k_m) \\ \vdots \\ P_{n1}(k_1) + \cdots + P_{nm}(k_m) \end{array} \right) \mid k_1, \dots, k_m \in \mathbb{N} \right\},$$

where  $P_{ij} \in \mathbb{N}[X]$  are (univariate) polynomials.

**Simple semi-polynomial set:** finite union of simple polynomial sets.

## Remark

- Properties of semi-polynomial sets carry over into simple semi-polynomial sets: closure under finite unions, decidability of membership problem, strict hierarchy w.r.t. degree, ....
- Simple semi-polynomial sets form a **proper subclass** of semi-polynomial sets. For example, the **product relation** is not simple semi-polynomial (see paper for proof).

- 1 Preliminaries
- 2 Polynomially Generated Sets
- 3 On the Intersection Problems**
- 4 Quadratic Forms

## Proposition

There are two simple quadratic sets whose intersection is **not simple semi-polynomial**.

## Proposition

There are two simple quadratic sets whose intersection is **not simple semi-polynomial**.

## Example (see paper for proof)

Intersection of the quadratic sets

$$\left\{ \begin{pmatrix} (k_1 + 1)^2 + (k_2 + 1)^2 \\ k_3 \end{pmatrix} \mid k_1, k_2, k_3 \in \mathbb{N} \right\} \quad \text{and} \quad \left\{ \begin{pmatrix} k^2 \\ k \end{pmatrix} \mid k \in \mathbb{N} \right\}$$

is **not simple semi-polynomial**.

## Proposition

There are two simple quadratic sets whose intersection is **not simple semi-polynomial**.

## Example (see paper for proof)

Intersection of the quadratic sets

$$\left\{ \begin{pmatrix} (k_1 + 1)^2 + (k_2 + 1)^2 \\ k_3 \end{pmatrix} \mid k_1, k_2, k_3 \in \mathbb{N} \right\} \quad \text{and} \quad \left\{ \begin{pmatrix} k^2 \\ k \end{pmatrix} \mid k \in \mathbb{N} \right\}$$

is **not simple semi-polynomial**.

Hence, consider intersection of a **simple semi-polynomial** set and a **semi-linear** set.



## Proposition

There are two simple quadratic sets whose intersection is **not simple semi-polynomial**.

## Example (see paper for proof)

Intersection of the quadratic sets

$$\left\{ \left( \begin{array}{c} (k_1 + 1)^2 + (k_2 + 1)^2 \\ k_3 \end{array} \right) \mid k_1, k_2, k_3 \in \mathbb{N} \right\} \quad \text{and} \quad \left\{ \left( \begin{array}{c} k^2 \\ k \end{array} \right) \mid k \in \mathbb{N} \right\}$$

is **not simple semi-polynomial**.

Hence, consider intersection of a **simple semi-polynomial** set and a **semi-linear** set.

Partial result: decidability for the case of **componentwise semi-linear sets**

Decidability of the general case remains an open question.

## Definition

$A \subseteq \mathbb{N}^n$  is called **componentwise linear** if there are **linear** sets  $A_1, \dots, A_n \subseteq \mathbb{N}$  such that

$$A = A_1 \times \dots \times A_n.$$

**Componentwise semi-linear set:** finite union of componentwise linear sets

## Definition

$A \subseteq \mathbb{N}^n$  is called **componentwise linear** if there are **linear** sets  $A_1, \dots, A_n \subseteq \mathbb{N}$  such that

$$A = A_1 \times \dots \times A_n.$$

**Componentwise semi-linear set:** finite union of componentwise linear sets

## Theorem

If  $A \subseteq \mathbb{N}^n$  is componentwise semi-linear and  $B \subseteq \mathbb{N}^n$  is a simple semi-polynomial set of degree  $d$ , then  $A \cap B$  is a **simple semi-polynomial set 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**.

## Definition

$A \subseteq \mathbb{N}^n$  is called **componentwise linear** if there are **linear** sets  $A_1, \dots, A_n \subseteq \mathbb{N}$  such that

$$A = A_1 \times \dots \times A_n.$$

**Componentwise semi-linear set:** finite union of componentwise linear sets

## Theorem

If  $A \subseteq \mathbb{N}^n$  is componentwise semi-linear and  $B \subseteq \mathbb{N}^n$  is a simple semi-polynomial set of degree  $d$ , then  $A \cap B$  is a **simple semi-polynomial set 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**.

## Remark

The result also holds for the intersection of a componentwise semi-linear sets with a **semi-polynomial** set.

### Theorem

If  $A \subseteq \mathbb{N}^n$  is componentwise semi-linear and  $B \subseteq \mathbb{N}^n$  is a (simple) semi-polynomial set of degree  $d$ , then  $A \cap B$  is a **(simple) semi-polynomial set 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 (sketch)

W.l.o.g.  $A$  componentwise linear,  $B$  simple polynomial.

First, **solve the case  $n = 1$**  (this is the core of the proof).

For  $n > 1$ , let  $A = A_1 \times \cdots \times A_n$ , and proceed as follows:

- Analyze  $A \cap B$  w.r.t. the **first** component, i.e.  $(A_1 \times \mathbb{N}^{n-1}) \cap B$ .
- If this set is nonempty, establish its **semi-polynomial representation**, say  $B'$ .
- Analyze the **second** component, i.e.  $(\mathbb{N} \times A_2 \times \mathbb{N}^{n-2}) \cap B'$ .
- ...

After  $n$  steps, we obtain a **semi-polynomial representation** of  $A \cap B$ .

Suppose

$$A = \{x_0 + k_1x_1 + \cdots + k_mx_m \mid k_1, \dots, k_m \in \mathbb{N}\}$$

$$B = \{P(\ell_1, \dots, \ell_r) \mid \ell_1, \dots, \ell_r \in \mathbb{N}\}$$

Suppose

$$A = \{x_0 + k_1x_1 + \cdots + k_mx_m \mid k_1, \dots, k_m \in \mathbb{N}\}$$

$$B = \{P(\ell_1, \dots, \ell_r) \mid \ell_1, \dots, \ell_r \in \mathbb{N}\}$$

Let  $g := \gcd(x_1, \dots, x_m)$ . Then, there is some  $z_0 \in \mathbb{N}$  such that

- $C := \{z_0 + kg \mid k \in \mathbb{N}\} \subseteq A$  and
- $A \setminus C$  is **finite**.

Hence, it suffices to consider only  $C \cap B$ .

Suppose

$$A = \{x_0 + k_1x_1 + \dots + k_mx_m \mid k_1, \dots, k_m \in \mathbb{N}\}$$

$$B = \{P(\ell_1, \dots, \ell_r) \mid \ell_1, \dots, \ell_r \in \mathbb{N}\}$$

Let  $g := \gcd(x_1, \dots, x_m)$ . Then, there is some  $z_0 \in \mathbb{N}$  such that

- $C := \{z_0 + kg \mid k \in \mathbb{N}\} \subseteq A$  and
- $A \setminus C$  is **finite**.

Hence, it suffices to consider only  $C \cap B$ .

$x \in C \cap B$  iff  $x = P(\ell_1, \dots, \ell_r)$  for some solution  $\ell_1, \dots, \ell_r$  of the congruence equation

$$z_0 \equiv P(\ell_1, \dots, \ell_r) \pmod{g}$$

If a solution exists, then also such with  $\ell_1, \dots, \ell_r < g$ .



Suppose

$$A = \{x_0 + k_1x_1 + \dots + k_mx_m \mid k_1, \dots, k_m \in \mathbb{N}\}$$

$$B = \{P(\ell_1, \dots, \ell_r) \mid \ell_1, \dots, \ell_r \in \mathbb{N}\}$$

Let  $g := \text{gcd}(x_1, \dots, x_m)$ . Then, there is some  $z_0 \in \mathbb{N}$  such that

- $C := \{z_0 + kg \mid k \in \mathbb{N}\} \subseteq A$  and
- $A \setminus C$  is **finite**.

Hence, it suffices to consider only  $C \cap B$ .

$x \in C \cap B$  iff  $x = P(\ell_1, \dots, \ell_r)$  for some solution  $\ell_1, \dots, \ell_r$  of the congruence equation

$$z_0 \equiv P(\ell_1, \dots, \ell_r) \pmod{g}$$

If a solution exists, then also such with  $\ell_1, \dots, \ell_r < g$ .

Such a solution  $s_1, \dots, s_r < g$  then generates elements of  $C \cap B$  of the form

$$x = P(s_1 + \ell'_1g, \dots, s_r + \ell'_rg)$$

where  $\ell'_i \in \mathbb{N}$  (up to finitely many exceptions). □

- 1 Preliminaries
- 2 Polynomially Generated Sets
- 3 On the Intersection Problems
- 4 Quadratic Forms**

Hilbert's Tenth Problem revisited:

- Undecidability holds already for solving polynomial equations of degree four and systems of quadratic equations in integers.
- Solvability of quadratic equations in integers is decidable (Siegel, 1972).

Hilbert's Tenth Problem revisited:

- Undecidability holds already for solving polynomial equations of degree four and systems of quadratic equations in integers.
- Solvability of quadratic equations in integers is decidable (Siegel, 1972).

Solvability of quadratic equations in natural numbers:

Hilbert's Tenth Problem revisited:

- Undecidability holds already for solving polynomial equations of degree four and systems of quadratic equations in integers.
- Solvability of quadratic equations in integers is decidable (Siegel, 1972).

Solvability of quadratic equations in natural numbers:

## Theorem (Grunewald & Segal, 2004)

Consider quadratic form  $Q \in \mathbb{Z}[X_1, \dots, X_n]$ , linear forms  $L_1, \dots, L_k \in \mathbb{Z}[X_1, \dots, X_n]$ , and the system

$$Q(x_1, \dots, x_n) = 0,$$

$$L_j(x_1, \dots, x_n) \# c_j, \text{ where } c_j \in \mathbb{Z} \text{ and } \# \in \{<, \leq\}, \text{ for } j = 1, \dots, k,$$

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

It is decidable whether a solution in  $\mathbb{Z}^n$  exists.

Remark: Linear constraints  $-x_i \leq 0$  restrict to solutions in natural numbers.

## Scenario 1

- system: semi-linear set
- specification: quadratic equation  $Q(x_1, \dots, x_n) = 0$

## Scenario 1

- system: semi-linear set
- specification: quadratic equation  $Q(x_1, \dots, x_n) = 0$

↪ **decidable**, as a semi-linear set is the solution set of a linear (in)equation systems

## Scenario 1

- system: semi-linear set
- specification: quadratic equation  $Q(x_1, \dots, x_n) = 0$

↪ **decidable**, as a semi-linear set is the solution set of a linear (in)equation systems

## Scenario 2

- system: semi-linear set
- specification: (semi-)one-quadratic set



## Scenario 1

- system: semi-linear set
- specification: quadratic equation  $Q(x_1, \dots, x_n) = 0$

↪ **decidable**, as a semi-linear set is the solution set of a linear (in)equation systems

## Scenario 2

- system: semi-linear set
- specification: (semi-)one-quadratic set

quadratic ————

linear ————

$$\left\{ \begin{array}{l} Q(k_1, \dots, k_m) \\ L_2(k_1, \dots, k_m) \\ \vdots \\ L_n(k_1, \dots, k_m) \end{array} \mid k_1, \dots, k_m \in \mathbb{N} \right\}$$

## Scenario 1

- system: semi-linear set
- specification: quadratic equation  $Q(x_1, \dots, x_n) = 0$

↪ **decidable**, as a semi-linear set is the solution set of a linear (in)equation systems

## Scenario 2

- system: semi-linear set (semi-one-quadratic set)
- specification: (semi-)one-quadratic set

$$\begin{array}{l}
 \text{quadratic} \\
 \text{linear}
 \end{array}
 \left. \begin{array}{l}
 \text{---} \\
 \text{---} \\
 \text{---}
 \end{array} \right\} \left( \begin{array}{c}
 Q(k_1, \dots, k_m) \\
 L_2(k_1, \dots, k_m) \\
 \vdots \\
 L_n(k_1, \dots, k_m)
 \end{array} \right) \left| \begin{array}{l} \\ \\ \\ \\
 \end{array} \right\} k_1, \dots, k_m \in \mathbb{N}$$

↪ **decidable**; transform nonemptiness question to (in)equation system described previously.

- Some possibilities of extending the framework of semi-linear sets with polynomials
- Some restrictions needed in order to retain decidability results w.r.t. intersection problem, e.g. simple semi-polynomial sets, componentwise semi-linear sets, one-quadratic sets
- Number-theoretical results and methods are required.

Overview of present results:

system	specification	intersection problem
semi-linear	semi-polynomial	undecidable
semi-linear	simple semi-polynomial	?
componentwise semi-linear	(simple) semi-polynomial	decidable
semi-linear	semi-one-quadratic	decidable (Grunewald & Segal, 2004)

- algorithmic and complexity analysis of Grunewald & Segal's results
- closure properties of (simple) semi-polynomial sets, e.g. under additive operations

### Open question

- intersection problem for simple semi-polynomial sets and semi-linear sets