On Iterating Linear Transformations over Recognizable Sets of Integers ⋆

Bernard Boigelot

Université de Liège, Institut Montefiore, B28, B-4000 Liège Sart-Tilman, Belgium

Abstract

It has been known for a long time that the sets of integer vectors that are recognizable by finite-state automata are those that can be defined in an extension of Presburger arithmetic. In this paper, we address the problem of deciding whether the closure of a linear transformation preserves the recognizable nature of sets of integer vectors. We solve this problem by introducing an original extension of the concept of recognizability to sets of vectors with complex components. This generalization allows to obtain a simple necessary and sufficient condition over linear transformations, in terms of the eigenvalues of the transformation matrix. We then show that these eigenvalues do not need to be computed explicitly in order to evaluate the condition, and we give a full decision procedure based on simple integer arithmetic. The proof of this result is constructive, and can be turned into an algorithm for applying the closure of a linear transformation that satisfies the condition to a finite-state representation of a set. Finally, we show that the necessary and sufficient condition that we have obtained can straightforwardly be turned into a sufficient condition for linear transformations with linear guards.

Key words: automata, iterations, Presburger arithmetic, recognizable sets of integers

⋆ This work was partially funded by a grant of the "Communauté française de Belgique — Direction de la recherche scientifique — Actions de recherche concertées", and by the European Commission (FET project ADVANCE, contract No IST-1999-29082).

Email address: boigelot@montefiore.ulg.ac.be (Bernard Boigelot).
URL: http://www.montefiore.ulg.ac.be/~boigelot (Bernard Boigelot).

1 Introduction

In order to be able to compute exactly the set of reachable configurations of an infinite-state system, even for restricted classes of programs, one needs to solve the two following problems: Representing infinite sets by a finite amount of information, and generating in finite time infinite sets of reachable configurations.

A simple solution to the former problem consists in using *finite-state representations*, which amounts to representing a set by a finite-state automaton recognizing its elements with respect to a suitable encoding scheme. There are several motivations to following this approach. First, one knows efficient algorithms for manipulating finite-state automata [1]. In particular, finite-state representations can easily be reduced to a canonical form by means of a minimization operation [18]. Second, these representations have a high expressive power. Consider for instance programs relying on integer variables. Using the classical encoding of numbers as words of digits in a base $r > 1$, it is well known that all the sets that are definable in Presburger arithmetic, i.e., the first order theory $\langle \mathbb{Z}, +, \leq \rangle$, are recognizable by finite-state machines [10]. Finite-state representation methods have also been developed for other data domains, namely for real vectors [4] and unbounded FIFO channels [5–7].

In order to compute infinite sets of reachable configurations in finite time, the underlying idea to many central results in the field of infinite-state systems verification consists in studying the effect of *loops* executed by the programs being analyzed. Indeed, a loop that can be followed unboundedly many times from a location reached during a system run might lead to a infinite number of reachable configurations, thus generating an infinite set from a finite one. We can now restate our second problem in the more specific framework of studying the effect of loops: Given a representation of a set U of values and a transformation θ over these values, the goal is to compute a representation of the set $\theta^*(U)$ containing the images of the elements of U by arbitrary repetitions of θ. This computation is not always feasible though, since the set $\theta^*(U)$ may not always be representable by finite-state automata with respect to the encoding scheme that is used. We get around this limitation by decomposing our main goal into two separate problems :

- Given θ, deciding whether $\theta^*(U)$ is effectively representable for every representable U, and
- Given θ satisfying the previous criterion and a representation of U, computing a representation of $\theta^*(U)$.

The purpose of this paper is to solve the two previous problems in the following context :

- The data domain is $\mathbb{Z}^n$ ($n > 0$), i.e., the values are vectors of integers with a fixed dimension;
- The sets are expressed in a finite-state representation system based on the classical encoding of numbers in a given base $r > 1$;
- The operations θ are of the form $\theta(\vec{x}) = A\vec{x} + \vec{b}$, with $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$, i.e., they are linear transformations with arbitrary integer coefficients.

In addition, we will also show that the solutions obtained in this context are also applicable (with some restrictions) to more general operations, namely those combining a linear guard and a linear transformation.

This paper is structured as follows. First, we describe a finite-state representation system suited for unbounded integer vectors and present some of its properties. We also define some basic notions of algebra and combinatorics that are extensively used in the paper, and recall some known results. Next, we extend in an original way the notion of sets that are recognizable by finite-state automata to the domain of vectors with complex components. This generalized notion of recognizability is then used as a powerful tool for establishing necessary and sufficient conditions[1] over the linear transformations whose closure preserves the recognizable nature of sets. Then, we give algorithms implementing with finite-state representations the decision procedures expressed by the necessary and sufficient conditions. Next, we address the case of linear operations with guards. Finally, we conclude with some proofs that are omitted from the main text for clarity sake.

2 Finite-state Representation of Integer Vectors

2.1 Number Decision Diagrams

The first step towards obtaining a finite-state representation system suited for subsets of $\mathbb{Z}^n$ is to define an encoding scheme for vectors. We base ours on the classical encoding of integers as finite sequences of digits belonging to a finite alphabet.

Let $r \in \mathbb{N}$, with $r > 1$, be a *numeration base* (or simply *base*). Any positive integer z can be encoded as a finite word $w = a_{p-1} \cdot a_{p-2} \cdots a_1 \cdot a_0$ ($p \geq 0$) of *digits* belonging to $\{0, 1, \ldots, r-1\}$, such that $z = \sum_{0 \leq i < p} a_i r^i$. The encoding of z is not unique. Indeed, its length can be increased at will by adding an arbitrary number of leading "0" digits. This encoding scheme is

[1] In the main text, these conditions are first expressed in the form of several distinct theorems, which are then summarized into one main result.

easily generalized to all the integers in $\mathbb{Z}$ by requiring that the encoding of an integer $z \in \mathbb{Z}$ such that $-r^{p-1} \leq z < r^{p-1}$, where $p > 0$ is the smallest integer satisfying these inequalities, has at least p digits. If $z < 0$, then the encoding of z consists of the last p digits of the encoding of $r^p + z$ (the number $r^p + z$ is called the *r's complement* of z). As a consequence, the first digit of the encoding of an integer will be equal to 0 if the number is greater or equal to zero, and to $r-1$ otherwise (this first digit is called the *sign digit*). The fact that the word $w \in \{0, 1, \ldots, r-1\}^*$ encodes the integer $z \in \mathbb{Z}$ in base r is denoted $w \in [z]_r$.

Let $n \geq 0$ be a dimension and $r > 1$ be a base. The *synchronous encoding scheme* E_r is the relation that associates to a vector of $\mathbb{Z}^n$ the tuples composed of the same-length encodings in base r of the components of this vector. Formally, we have

$$E_r \subseteq \mathbb{Z}^n \times V_{E_r} = \{((v_1, \ldots, v_n), (w_1, \ldots, w_n)) \mid |w_1| = |w_2| = \cdots = |w_n| \\ \wedge w_1 \in [v_1]_r \wedge w_2 \in [v_2]_r \wedge \cdots \wedge w_n \in [v_n]_r\},$$

where $V_{E_r} = \bigcup_{k \in \mathbb{N}} (\{0, r-1\} \cdot \{0, \ldots, r-1\}^k)^n$ is the set of valid encodings.

An encoding of an element of $\mathbb{Z}^n$ can indifferently be viewed either as a tuple of n words of identical length over the alphabet $\{0, 1, \ldots, r-1\}$, or as a single word over the alphabet $\{0, 1, \ldots, r-1\}^n$.

We are now ready to define the representation system for sets of vectors.

Definition 1 *Let $n \geq 0$ be a dimension and $r > 1$ be a base. A* Number Decision Diagram (NDD) *representing the set $U \subseteq \mathbb{Z}^n$ is a finite-state automaton accepting the language*

$$L(U) = \{w \in V_{E_r} \mid (\exists \vec{v} \in U)(w \in E_r(\vec{v}))\}.$$

In other words, an NDD representing a set U is simply a finite-state automaton accepting all the synchronous encodings of all the elements of U.

2.2 Representable Sets of Vectors

Finite-state representations of sets of integer vectors have been studied for a long time [10]. In [11], Büchi gave the first characterization of representable sets of vectors in terms of logic. A flaw was discovered in Büchi's proof by MacNaughton [21], and a correct characterization was proposed in [21] and [9].

Simplified proofs of this characterization can be found in [22] and [29]. Precisely, the characterization is expressed as the following necessary and sufficient condition.

Theorem 2 *Let $n \geq 0$ be a dimension, $r > 1$ be a base, and $U \subseteq \mathbb{Z}^n$ be a set of vectors. A set U is recognizable by a finite-state automaton with respect to the synchronous encoding scheme E_r if and only if U is definable in the first-order theory $\langle \mathbb{Z}, \leq, +, V_r \rangle$, where V_r is a function defined as*

$$V_r : \mathbb{Z} \to \mathbb{N} : z \mapsto \begin{cases} \text{the greatest power of } r \text{ dividing } z & \text{if } z \neq 0, \\ 1 & \text{if } z = 0. \end{cases}$$

It is worth mentioning that the proof of the sufficient condition is constructive [10], and can easily be turned into an algorithm for building the representation of any set specified by a formula of $\langle \mathbb{Z}, \leq, +, V_r \rangle$.

The previous result characterizes the sets that are representable with respect to a particular base r. The question of determining whether a set can be represented by a finite-state automaton in any base has been solved by Cobham [13] and Semenov [23,27], whose main result can be stated as follows.

Theorem 3 *Let $n > 0$ be a dimension, and $U \subseteq \mathbb{Z}^n$ be a set of vectors. The set U is recognizable in every base $r > 1$ with respect to the synchronous encoding scheme E_r if and only if U is definable in the first-order theory $\langle \mathbb{Z}, \leq, + \rangle$. Moreover, an NDD representing U can be computed from a formula of $\langle \mathbb{Z}, \leq, + \rangle$ defining U.*

The theory $\langle \mathbb{Z}, \leq, + \rangle$ has been studied by Presburger [25] and is usually referred to as *Presburger arithmetic*. It is known [15,24,14] that deciding Presburger arithmetic is ATIME-ALT$[2^{2^{O(n)}}, O(n)]$-complete.

An advantage of considering the sets of vectors that are definable in Presburger arithmetic rather than the sets definable in $\langle \mathbb{Z}, \leq, +, V_r \rangle$ for some base $r > 1$ is that lots of techniques have been developed for dealing with Presburger arithmetic, and that efficient implementations of these techniques have been made available. An example of such an implementation is the *Omega Test* [26] which allows to manipulate formulas of Presburger arithmetic with a surprising efficiency. Another result of interest, due to Boudet and Comon [8], shows that the minimal and deterministic NDD representing the set of vectors that satisfies a system of linear equations and inequations is very compact and can be computed efficiently.

On the other hand, there are applications for which using the theory $\langle \mathbb{Z}, \leq, +, V_r \rangle$ for some base $r > 1$ is nonetheless more advantageous than using Pres-

burger arithmetic. For instance, the model of a hardware circuit performing some arithmetic operation on unbounded binary numbers might very well have a control location at which the set of reachable values is the set of the powers of 2. It can be shown that this set cannot be defined in Presburger arithmetic. It can however be denoted in $\langle \mathbb{Z}, \leq, +, V_2 \rangle$ by the formula $\varphi(x) \equiv V_2(x) = x$.

Since both theories have advantages, the approach followed in this paper is to stay as general as possible. Each result dealing with the possibility of representing a set of vectors as an NDD will thus be expressed twice: once with respect to the theory $\langle \mathbb{Z}, \leq, +, V_r \rangle$ for any $r > 1$, and once with respect to Presburger arithmetic. Intuitively, the former case consists in choosing the numeration base used by the NDD, and the latter one consists in requiring that the result has to hold in any base. We will make use of the following definitions.

Definition 4 *Let $r > 1$ be a base, $n \in \mathbb{N}$ be a dimension, and $U \subseteq \mathbb{Z}^n$ be a set of vectors. The set U is* r-recognizable *if it is recognizable with respect to the synchronous encoding E_r.*

Definition 5 *Let $n \in \mathbb{N}$ be a dimension and $U \subseteq \mathbb{Z}^n$ be a set of vectors. The set U is* Presburger-definable *if for every base $r > 1$, it is recognizable with respect to the synchronous encoding E_r.*

In the rest of this paper, we will only consider bases $r > 1$ for which there does not exist $j \in \mathbb{N}$, with $j \geq 2$, such that $r^{(1/j)} \in \mathbb{N}$. This can be done without loss of generality thanks to the following result [2].

The following result is well known [10].

Theorem 6 *Let $n \in \mathbb{N}$ be a dimension, $r > 1$ be a base and $U \subseteq \mathbb{Z}^n$ be a set of vectors. For every $k \in \mathbb{N}_0$, U is r-recognizable if and only if U is r^k-recognizable.*

PROOF SKETCH. A finite-state automaton recognizing U with respect to the base r can easily be turned into one operating in the base r^k by means of a transducer outputting exactly one symbol for every sequence of k consecutive input digits. The reverse transformation is carried out in a similar way after exchanging the input and the output labels of the transducer. A detailed proof is given in [3]. □

[2] The notation $\mathbb{N}_0$ is introduced as a shorthand for $\mathbb{N} \setminus \{0\}$, i.e., the set of all the strictly positive integers.

The sets of rational numbers and of complex numbers are respectively denoted by $\mathbb{Q}$ and $\mathbb{C}$. For every $n \in \mathbb{N}_0$, I_n denotes the identity matrix $I_n = \text{diag}(1, 1, \ldots, 1)$ of dimension n. The successive columns of I_n are denoted $\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n$. Let $A \in \mathbb{C}^{n \times n}$ be a complex matrix. If $S \subseteq \mathbb{C}^n$ is a set of vectors, then AS is a shorthand for $\{A\vec{x} \mid \vec{x} \in S\}$. Similarly, if $\vec{v} \in \mathbb{C}^n$, then $S + \vec{v}$ denotes the set $\{\vec{x} + \vec{v} \mid \vec{x} \in S\}$. The sets of rows and of columns of A are respectively denoted $\text{row}(A)$ and $\text{col}(A)$. The maximum number of linearly independent rows or columns of A is the *rank* of A. Any $\lambda \in \mathbb{C}$ and $\vec{x} \in (\mathbb{C}^n \setminus \{\vec{0}\})$ such that $A\vec{x} = \lambda\vec{x}$ are respectively called an *eigenvalue* and an *eigenvector* of A. The eigenvalues of A are the roots of the *characteristic polynomial* of A, defined as $\Pi(\lambda) = \det(A - \lambda I_n)$. They are also the roots of the *minimal polynomial* of A, which is defined as the polynomial $\Pi'(\lambda)$ of lowest degree such that $\Pi'(A) = (0)$. If $\lambda_1, \lambda_2, \ldots, \lambda_m$ are the eigenvalues of A, then $\lambda_1^p, \lambda_2^p, \ldots, \lambda_m^p$ are the eigenvalues of A^p for any $p \in \mathbb{N}_0$. For every $n \in \mathbb{N}_0$ and $\lambda \in \mathbb{C}$, the *Jordan block* of dimension n associated to λ is the matrix

$$J_{n,\lambda} = \begin{bmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}.$$

A matrix $A \in \mathbb{C}^{n \times n}$ only composed of Jordan blocks on its main diagonal, in other words such that $A = \text{diag}(J_{n_1,\lambda_1}, J_{n_2,\lambda_2}, \ldots)$, is said to be in *Jordan form*. For every $A \in \mathbb{C}^{n \times n}$, there exists a nonsingular matrix $U \in \mathbb{C}^{n \times n}$ such that $A = UA_JU^{-1}$, with A_J being in Jordan form (U is said to *transform* A into its Jordan form A_J). The Jordan form A_J of A is unique up to reordering its diagonal blocks. For each diagonal block J_{n_i,λ_i} composing A_J, the corresponding λ_i is an eigenvalue of A. Reciprocally, for every eigenvalue λ_i of A, there exists a (possibly non unique) Jordan block J_{n_i,λ_i} that belongs to the set of diagonal blocks of A_J. If the components of A and its eigenvalues belong to $\mathbb{Q}$, then there exists $U \in \mathbb{Q}^{n \times n}$ transforming A into A_J. If the Jordan form of A is diagonal (in other words, if all its Jordan blocks are of size 1), then A is said to be *diagonalizable*.

Let $p, q \in \mathbb{N}$ with $p \leq q$. The *binomial coefficient* $C_q^p \in \mathbb{N}$ is defined as

$$C_q^p = \frac{q!}{(q-p)!\,p!}.$$

Binomial coefficients are related to Jordan blocks in the following way. If $\lambda \in \mathbb{C}$ and n, $m \in \mathbb{N}$ with $0 < n \leq m$, then the m-th power of the Jordan block $J_{n,\lambda}$ is such that

$$J_{n,\lambda}^m = \begin{bmatrix} \lambda^m C_m^0 & \lambda^{m-1} C_m^1 & \lambda^{m-2} C_m^2 & \dots & \lambda^{m-n+1} C_m^{n-1} \\ & \lambda^m C_m^0 & \lambda^{m-1} C_m^1 & \dots & \lambda^{m-n+2} C_m^{n-2} \\ & & \lambda^m C_m^0 & \dots & \lambda^{m-n+3} C_m^{n-3} \\ & & & \ddots & \vdots \\ & & & & \lambda^m C_m^0 \end{bmatrix}.$$

We now define some notions related to cyclotomic fields. It is known that every polynomial with integer coefficients can be factorized into a product of *irreducible* polynomials with integer coefficients. This factorization is unique up to multiplicative constants. For every $n \in \mathbb{N}_0$, the indivisible factors of the polynomial $x^n - 1$ are called *cyclotomic polynomials*. There is a cyclotomic polynomial Φ_m associated to every integer $m \in \mathbb{N}_0$, defined as

$$\Phi_m(x) = \prod_{[k,m]} (x - e^{\frac{2ik\pi}{m}}),$$

where $[k, m]$ stands for $1 \leq k < m \wedge \gcd(k, m) = 1$. Actually, we have

$$x^n - 1 = \prod_{k|n} \Phi_k(x),$$

where $k|n$ means "k divides n". For every $m \in \mathbb{N}_0$, the degree of $\Phi_m(x)$ is equal to $\phi(m)$, where ϕ is the *Euler function*. This function is defined as

$$\phi : \mathbb{N}_0 \to \mathbb{N}_0 : x \mapsto x \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_q}\right),$$

where $p_1, p_2, \dots, p_q$ are the (distinct) prime factors of x. Actually, $\phi(m)$ represents the number of integers in $\{1, 2, \dots, m\}$ that are relatively prime to m.

3 Recognizability of Sets of Complex Vectors

Let $n \in \mathbb{N}$ be a dimension. In this section, we generalize the notion of recognizable set of vectors to subsets of $\mathbb{C}^n$. The reason why we consider complex

vectors is that Jordan forms of matrices will be heavily used, and that transforming a matrix into its Jordan form is generally not possible within $\mathbb{R}$. Intuitively, the idea behind the generalization of recognizability is the following. Let $S \subseteq \mathbb{Z}^n$ be a set of vectors and let $\theta = (\vec{x} := A\vec{x} + \vec{b})$, where $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$, be a linear transformation. If the matrix A is nonsingular, then the set S is recognizable (either with respect to a given base $r > 1$ or to all of them) if and only if the set $\theta(S)$ is recognizable. This shows that the recognizable nature of a set of integer vectors is not influenced by nonsingular linear transformations. It is therefore natural to define a set of complex vectors as recognizable if it can be expressed as the image of a recognizable set of integer vectors by some linear transformation. Formally, we have the following definition.

Definition 7 *Let $n, r \in \mathbb{N}_0$ with $r > 1$. A set of complex vectors $S \subseteq \mathbb{C}^n$ is* r-definable *if and only if there exist $m \in N_0$, $S' \subseteq \mathbb{Z}^m$ and $U \in \mathbb{C}^{n \times m}$ such that S' is r-recognizable and $S = US'$.*

The following result shows that the notion of r-definability is indeed an generalization of r-recognizability, i.e., that the two notions coincide for sets of integer vectors.

Theorem 8 *Let $n, r \in \mathbb{N}_0$ with $r > 1$. A set $S \subseteq \mathbb{Z}^n$ is r-definable if and only if it is r-recognizable.*

PROOF. The proof is given in Section 8. □

The next step is to show how to obtain definable sets of complex vectors. The following theorem establishes the definability of some elementary sets, and presents operations that can be used for combining definable sets.

Theorem 9 *Let $r \in \mathbb{N}$ with $r > 1$, $n_1, n_2 \in \mathbb{N}_0$, $S_1 \subseteq \mathbb{C}^{n_1}$, $S_2 \subseteq \mathbb{C}^{n_2}$ such that S_1 and S_2 are r-definable, $\vec{v} \in \mathbb{C}^{n_1}$, $p, q \in \mathbb{N}_0$, $k \in \mathbb{N}$ such that $0 < k \leq n_1$, and $T \in \mathbb{C}^{p \times n_1}$. The following sets are r-definable*[3] *:*

- *Any finite subset of $\mathbb{C}^{n_1}$,*
- $S_1 + \vec{v}$,
- TS_1,
- $S_1 \cup S_2$, *provided that* $n_1 = n_2$,
- $S_1 \cap S_2$, *provided that* $n_1 = n_2$,
- $S_1 \times S_2$,
- $\{(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_{n_1}) \mid (x_1, \ldots, x_{n_1}) \in S_1\}$,

[3] $\Re(\vec{x})$ and $\Im(\vec{x})$ denote respectively the real and the imaginary part of the complex vector $\vec{x}$.

- $\left\{ \begin{bmatrix} \vec{x} \\ \Re(\vec{x}) \\ \Im(\vec{x}) \end{bmatrix} \mid \vec{x} \in S_1 \right\}$,
- $expand(S_1, r^q) = \{r^{qk}\vec{x} \mid \vec{x} \in S_1 \wedge k \in \mathbb{N}\}$.

PROOF. The proof is given in Section 8. □

It is surprising that the intersection and union of two definable sets are always definable themselves. Indeed, S_1 and S_2 are images of recognizable sets of integer vectors by two linear transformations which might be different. It is worth noticing that their intersection or union can always be expressed as the image of a single set of integer vectors by the same transformation. This observation strengthens our claim that definable sets of complex vectors are a "good" generalization of recognizable sets of integer vectors.

Of course, not all sets of complex vectors are definable. The following theorems characterize families of sets that are proved to be undefinable. In Sections 4 and 8, those theorems will be used as tools for establishing that the closure of some linear operations does not preserve the definable nature of sets.

Theorem 10 *Let $r \in \mathbb{N}$ with $r > 1$, and $a, b, c \in \mathbb{Z}$ with $a \neq 0$. The set*

$$S = \{ak^2 + bk + c \mid k \in \mathbb{N}\}$$

is not r-definable[4] *.*

PROOF. The proof is given in Section 8. □

Theorem 11 *Let $r, p \in \mathbb{N}_0$ with $r > 1$, $\lambda \in \mathbb{C}$ such that $\lambda^p = 1$, and $a, b, c, d \in \mathbb{C}$ with $a \notin \mathbb{R} \setminus \mathbb{Q}$. The set*

$$S = \left\{ \lambda^k \begin{bmatrix} (j+a)(k+b)+c \\ j+d \end{bmatrix} \mid j, k \in \mathbb{N} \right\}$$

is not r-definable.

PROOF. The proof is given in Section 8. □

[4] A similar result for natural numbers appears in [11].

Theorem 12 *Let $r \in \mathbb{N}$ with $r > 1$, $\lambda \in \mathbb{C}$ such that there do not exist $p \in \mathbb{N}_0$ and $m \in \mathbb{N}$ such that $\lambda^p = r^m$. The set*

$$S = \{\lambda^k \mid k \in \mathbb{N}\}$$

is not r-definable.

PROOF. The proof is given in Section 8. □

Theorem 13 *Let $r, p, m \in \mathbb{N}_0$ with $r > 1$, $\lambda \in \mathbb{C}$ such that $\lambda^p = r^m$, and $a \in \mathbb{C}$ such that $a \notin \mathbb{R} \setminus \mathbb{Q}$. The set*

$$S = \{\lambda^k(k + a) \mid k \in \mathbb{N}\}$$

is not r-definable.

PROOF. The proof is given in Section 8. □

Theorem 14 *Let $r, p, m \in \mathbb{N}_0$ with $r > 1$, and $\lambda \in \mathbb{C}$ such that $\lambda^p = r^m$. The set*

$$S = \left\{ \begin{bmatrix} k \\ \lambda^k \end{bmatrix} \mid k \in \mathbb{N} \right\}$$

is not r-definable.

PROOF. The proof is given in Section 8. □

Theorem 15 *Let $r, p, m \in \mathbb{N}_0$ with $r > 1$, $\lambda \in \mathbb{C}$ such that $\lambda^p = r^m$, and $a \in \mathbb{C}$. The set*

$$S = \left\{ \begin{bmatrix} \lambda^k(j + a) \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \right\}$$

is not r-definable.

PROOF. The proof is given in Section 8. □

Theorem 16 *Let $r, p_1, p_2, m_1, m_2 \in \mathbb{N}_0$ with $r > 1$, and $\lambda_1, \lambda_2 \in \mathbb{C}$ such that $\lambda_1^{p_1} = r^{m_1}$, $\lambda_2^{p_2} = r^{m_2}$ and $|\lambda_1| \neq |\lambda_2|$. The set*

$$S = \left\{ \begin{bmatrix} \lambda_1^k \\ \lambda_2^k \end{bmatrix} \mid k \in \mathbb{N} \right\}$$

is not r-definable.

PROOF. The proof is given in Section 8. □

4 Necessary Conditions

Here, we give conditions that must be verified by A if the linear transformation $\theta = (\vec{x} := A\vec{x} + \vec{b})$ is such that θ^* preserves the definable nature of sets. Those conditions consist of conditions on the eigenvalues of A, and on the size of the blocks of the Jordan form of A. For clarity sake, each group of conditions is presented separately. A summary of all the necessary conditions follows.

The idea behind the necessary conditions that will be developed is to show that the violation of any of them implies that there exists a set that is at the same time r-definable and not r-definable. The sets that are considered are related to the Jordan form of the transformation matrix. Precisely, we have the following result.

Theorem 17 *Let $n, r \in \mathbb{N}_0$ with $r > 1$, $\theta = (\vec{x} := A\vec{x} + \vec{b})$ with $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$, $U \in \mathbb{C}^{n \times n}$ transforming A into its Jordan form A_J, $J_{m,\lambda}$ be a Jordan block of A_J with $m \in N_0$, $\lambda \in \mathbb{C}$, π be the projection mapping A_J onto $J_{m,\lambda}$, and S be a r-definable subset of $\mathbb{Z}^n$. If $\theta^*(S)$ is r-definable, then the set*

$$S' = \{J_{m,\lambda}^k \vec{x} + \sum_{0 \leq i < k} J_{m,\lambda}^i \vec{b'} \mid k \in \mathbb{N} \wedge \vec{x} \in \pi(U^{-1}S)\},$$

with $\vec{b'} = \pi(U^{-1}\vec{b})$, is r-definable.

PROOF. We have

$$\begin{aligned} \theta^*(S) &= \{A^k\vec{x} + \sum_{0 \leq i < k} A^i\vec{b} \mid k \in \mathbb{N} \wedge \vec{x} \in S\} \\ &= \{UA_J^kU^{-1}\vec{x} + \sum_{0 \leq i < k} UA_J^iU^{-1}\vec{b} \mid k \in \mathbb{N} \wedge \vec{x} \in S\}. \end{aligned}$$

If this set is r-definable, then applying Theorem 9 shows that $\pi(U^{-1}\theta^*(S))$ is r-definable. Hence the result. $\square$

We are now ready to state the necessary conditions on the eigenvalues of the transformation matrix. The first condition expresses a relationship that must exist between those eigenvalues and the numeration base.

Theorem 18 *Let $n, r \in \mathbb{N}_0$ with $r > 1$ and $\theta = (\vec{x} := A\vec{x} + \vec{b})$ with $A \in \mathbb{Z}^{n\times n}$ and $\vec{b} \in \mathbb{Z}^n$ be such that for every $\vec{v} \in \mathbb{Z}^n$, the set $\theta^*(\{\vec{v}\})$ is r-definable. For every nonzero eigenvalue λ of A, there exist $p \in \mathbb{N}_0$ and $m \in \mathbb{N}$ such that $\lambda^p = r^m$.*

PROOF. Let λ be a nonzero eigenvalue of A, A_J be the Jordan form of A, $J_{m,\lambda}$ be a block of A_J associated with λ ($m \in \mathbb{N}_0$), and π be the projection mapping A_J onto $J_{m,\lambda}$. From Theorem 17, it follows that for every $\vec{v} \in \mathbb{Z}^n$, the set

$$S' = \{J^k_{m,\lambda}\vec{v}' + \sum_{0\le i<k} J^i_{m,\lambda}\vec{b}' \mid k \in \mathbb{N}\},$$

with $\vec{v}' = \pi(U^{-1}\vec{v})$ and $\vec{b}' = \pi(U^{-1}\vec{b})$, is r-definable. Let π' be the projection mapping each vector onto its component of highest index. There are two possible situations.

- *If $\pi'(\vec{b}') = 0$.* We choose $\vec{v} \in \mathbb{Z}^n$ such that $\pi'(\pi(U^{-1}\vec{v})) \neq 0$ (this is always possible, otherwise U^{-1} would be singular). According to Theorem 9, this implies that the set

  $$\frac{1}{\pi'(\pi(U^{-1}\vec{v}))}\pi'(S') = \{\lambda^k \mid k \in \mathbb{N}\}$$

  is r-definable.
- *If $\pi'(\vec{b}') \neq 0$.* We choose $\vec{v} = \vec{0}$. According to Theorem 9, this implies that the following sets are r-definable:

  $$\frac{1}{\pi'(\vec{b}')}\pi'(S') = \{\sum_{0\le i<k} \lambda^i \mid k \in \mathbb{N}\},$$

  $$\{\lambda^k - 1 \mid k \in \mathbb{N}\},$$

  $$\{\lambda^k \mid k \in \mathbb{N}\}.$$

We have thus established that the set

$$\{\lambda^k \mid k \in \mathbb{N}\}$$

is r-definable. The existence of $p \in \mathbb{N}_0$ and $m \in \mathbb{N}$ such that $\lambda^p = r^m$ is then a consequence of Theorem 12. $\square$

The property expressed by Theorem 18 is easily adapted to sets of vectors that are definable in any base.

Corollary 19 *Let $n \in \mathbb{N}_0$ and $\theta = (\vec{x} := A\vec{x} + \vec{b})$ with $A \in \mathbb{Z}^{n\times n}$ and $\vec{b} \in \mathbb{Z}^n$ be such that for every $\vec{v} \in \mathbb{Z}^n$, the set $\theta^*(\{\vec{v}\})$ is Presburger-definable. For every nonzero eigenvalue λ of A, there exists $p \in \mathbb{N}_0$ such that $\lambda^p = 1$.*

PROOF. Since every Presburger-definable set of integer vectors is r-definable in any base $r > 1$, the result follows from applying Theorem 18 to two relatively prime bases r_1 and r_2 (chosen arbitrarily). $\square$

Now, we go further and establish a correlation between the different eigenvalues of the transformation matrix.

Theorem 20 *Let $n, r \in \mathbb{N}_0$ with $r > 1$, and $\theta = (\vec{x} := A\vec{x}+\vec{b})$ with $A \in \mathbb{Z}^{n\times n}$ and $\vec{b} \in \mathbb{Z}^n$ be such that for every $\vec{v} \in \mathbb{Z}^n$, the sets $\theta^*(\{\vec{v}\})$ and $\theta^*(\{j\vec{v} \mid j \in \mathbb{N}\})$ are r-definable. Every pair of nonzero eigenvalues (λ_1, λ_2) of A is such that $|\lambda_1| = |\lambda_2|$.*

PROOF. The proof is by contradiction. Let $U \in \mathbb{C}^{n\times n}$ be a matrix transforming A into its Jordan form A_J. Let S be either equal to $\{\vec{v}\}$ or to $\{j\vec{v} \mid j \in \mathbb{N}\}$, with $\vec{v} \in \mathbb{Z}^n$. The set

$$\begin{aligned}\theta^*(S) &= \{A^k\vec{x} + \sum_{0\le i<k} A^i\vec{b} \mid k \in \mathbb{N} \wedge \vec{x} \in S\} \\ &= \{UA_J^kU^{-1}\vec{x} + \sum_{0\le i<k} UA_J^iU^{-1}\vec{b} \mid k \in \mathbb{N} \wedge \vec{x} \in S\}\end{aligned}$$

is r-definable. Suppose that A has two nonzero eigenvalues λ_1 and λ_2 such that $|\lambda_1| \neq |\lambda_2|$. Without loss of generality, we may assume that $|\lambda_1| < |\lambda_2|$. Let J_{m_1,λ_1} and J_{m_2,λ_2} $(m_1, m_2 \in \mathbb{N}_0)$ be two blocks of A_J respectively associated to λ_1 and to λ_2, and let π be the projection onto the two components matching the positions of the last row of J_{m_1,λ_1} and of the last row of J_{m_2,λ_2} in A_J. According to Theorem 9, the set $S' = \pi(U^{-1}\theta^*(S))$ is r-definable. We have

$$S' = \left\{ \begin{bmatrix} \lambda_1^k & 0 \\ 0 & \lambda_2^k \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \sum_{0\le i<k} \begin{bmatrix} \lambda_1^i & 0 \\ 0 & \lambda_2^i \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \mid \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in S'', k \in \mathbb{N} \right\},$$

with $S'' = \pi(U^{-1}S)$ and $\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \pi(U^{-1}\vec{b})$. We distinguish several situations.

- *If* $\lambda_1 = 1$ *and* $b_1 = 0$. We have

$$S' = \left\{ \begin{bmatrix} x_1 \\ \lambda_2^k x_2 + \frac{\lambda_2^k - 1}{\lambda_2 - 1} b_2 \end{bmatrix} \mid \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in S'', k \in \mathbb{N} \right\}.$$

  Let $\vec{v} \in \mathbb{Z}^n$ be such that the two components of $\pi(U^{-1}\vec{v})$ are different from zero (such a $\vec{v}$ always exists, otherwise U^{-1} would be singular). Choosing $S = \{j\vec{v} \mid j \in \mathbb{N}\}$, we obtain that the set

$$S' = \left\{ \begin{bmatrix} jv_1 \\ j\lambda_2^k v_2 + \frac{\lambda_2^k - 1}{\lambda_2 - 1} b_2 \end{bmatrix} \mid j, k \in \mathbb{N} \right\},$$

  with $\begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = \pi(U^{-1}\vec{v})$, is r-definable. From Theorem 9, it follows that the set

$$\begin{bmatrix} 0 & \frac{1}{v_2} \\ \frac{1}{v_1} & 0 \end{bmatrix} \left(S' + \begin{bmatrix} 0 \\ \frac{b_2}{\lambda_2 - 1} \end{bmatrix} \right) = \left\{ \begin{bmatrix} \lambda_2^k \left(j + \frac{b_2}{v_2(\lambda_2 - 1)} \right) \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \right\}$$

  is r-definable, which contradicts Theorem 15.
- *If* $\lambda_1 = 1$ *and* $b_1 \neq 0$. We have

$$S' = \left\{ \begin{bmatrix} x_1 + kb_1 \\ \lambda_2^k x_2 + \frac{\lambda_2^k - 1}{\lambda_2 - 1} b_2 \end{bmatrix} \mid \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in S'', k \in \mathbb{N} \right\}.$$

  Let $\vec{v} \in \mathbb{Z}^n$ be such that the second component of $\pi(U^{-1}\vec{v})$ is different from $\frac{b_2}{1 - \lambda_2}$ (such a $\vec{v}$ always exists, otherwise U^{-1} would be singular). Choosing $S = \{\vec{v}\}$, we obtain that the set

$$S' = \left\{ \begin{bmatrix} v_1 + kb_1 \\ \lambda_2^k v_2 + \frac{\lambda_2^k - 1}{\lambda_2 - 1} b_2 \end{bmatrix} \mid k \in \mathbb{N} \right\},$$

  with $\begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = \pi(U^{-1}\vec{v})$, is r-definable. From Theorem 9, it follows that the

set

$$\begin{bmatrix} \frac{1}{b_1} & 0 \\ 0 & \frac{1}{v_2+\frac{b_2}{\lambda_2-1}} \end{bmatrix} \left(S' + \begin{bmatrix} -v_1 \\ \frac{b_2}{\lambda_2-1} \end{bmatrix} \right) = \left\{ \begin{bmatrix} k \\ \lambda_2^k \end{bmatrix} \mid k \in \mathbb{N} \right\}$$

is r-definable, which contradicts Theorem 14.

- *If* $\lambda_1 \neq 1$. We have

$$S' = \left\{ \begin{bmatrix} \lambda_1^k x_1 + \frac{\lambda_1^k-1}{\lambda_1-1} b_1 \\ \lambda_2^k x_2 + \frac{\lambda_2^k-1}{\lambda_2-1} b_2 \end{bmatrix} \mid \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in S'', k \in \mathbb{N} \right\}.$$

Let $\vec{v} \in \mathbb{Z}^n$ be such that the two components of $\pi(U^{-1}\vec{v})$ are respectively different from $\frac{b_1}{1-\lambda_1}$ and from $\frac{b_2}{1-\lambda_2}$ (such a $\vec{v}$ always exists, otherwise U^{-1} would be singular). Choosing $S = \{\vec{v}\}$, we obtain that the set

$$S' = \left\{ \begin{bmatrix} \lambda_1^k v_1 + \frac{\lambda_1^k-1}{\lambda_1-1} b_1 \\ \lambda_2^k v_2 + \frac{\lambda_2^k-1}{\lambda_2-1} b_2 \end{bmatrix} \mid k \in \mathbb{N} \right\},$$

with $\begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = \pi(U^{-1}\vec{v})$, is r-definable. From Theorem 9, it follows that the set

$$\begin{bmatrix} \frac{1}{v_1+\frac{b_1}{\lambda_1-1}} & 0 \\ 0 & \frac{1}{v_2+\frac{b_2}{\lambda_2-1}} \end{bmatrix} \left(S' + \begin{bmatrix} \frac{b_1}{\lambda_1-1} \\ \frac{b_2}{\lambda_2-1} \end{bmatrix} \right) = \left\{ \begin{bmatrix} \lambda_1^k \\ \lambda_2^k \end{bmatrix} \mid k \in \mathbb{N} \right\}$$

is r-definable, which contradicts Theorem 16.

□

Before establishing the conditions that involve the Jordan blocks of the transformation matrix, we need to give a few lemmas.

Lemma 21 *Let $n, r \in \mathbb{N}_0$ with $n > 1, r > 1$, $\lambda \in \mathbb{C}$ such that $\lambda \neq 1$, $p \in \mathbb{N}_0$, $m \in \mathbb{N}$ such that $\lambda^p = r^m$, $q \in \mathbb{N}$ with $1 < q \leq n$, $V \in \mathbb{C}^{q \times n}$ of rank q, and $\vec{b} \in \mathbb{Z}^n$. There exists a r-definable set $S \subseteq \mathbb{Z}^n$ such that the set*

$$S' = \{J_{q,\lambda}^k \vec{x} + \sum_{0 \leq i < k} J_{q,\lambda}^i \vec{b'} \mid \vec{x} \in VS \wedge k \in \mathbb{N}\},$$

where $\vec{b'} = V\vec{b}$, is not r-definable.

PROOF. The proof is given in Section 8. □

The next lemma deals with Jordan blocks associated to the eigenvalue 1.

Lemma 22 *Let $n, r \in \mathbb{N}_0$ with $n > 1, r > 1$, $q \in \mathbb{N}$ with $1 < q \leq n$, $V \in \mathbb{Q}^{q \times n}$ of rank q, and $\vec{b} \in \mathbb{Z}^n$. There exists a r-definable set $S \subseteq \mathbb{Z}^n$ such that the set*

$$S' = \{J_{q,1}^k \vec{x} + \sum_{0 \leq i < k} J_{q,1}^i \vec{b'} \mid \vec{x} \in VS \wedge k \in \mathbb{N}\},$$

where $\vec{b'} = V\vec{b}$, is not r-definable.

PROOF. The proof is given in Section 8. □

Lemma 23 *Let $n \in \mathbb{N}_0$ and $A \in \mathbb{Z}^{n \times n}$. There exists a nonsingular matrix $U \in \mathbb{C}^{n \times n}$ transforming A into its Jordan form A_J, and such that every row of U^{-1} at the same position as a row of a Jordan block $J_{q,\lambda}$ in A_J contains only rational components provided that λ is rational.*

The proof is given in Section 8. □

We are now ready to state the necessary condition on the size of the Jordan blocks of the transformation matrix.

Theorem 24 *Let $n, r \in \mathbb{N}_0$ with $r > 1$ and $\theta = (\vec{x} := A\vec{x} + \vec{b})$ with $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$ be such that for every r-definable set $S \subseteq \mathbb{Z}^n$, the set $\theta^*(S)$ is r-definable. Let A_J be the Jordan form of A. Every Jordan block of A_J corresponding to a nonzero eigenvalue of A is of size* 1.

PROOF. The proof is by contradiction. Suppose that A_J has a Jordan block $J_{m,\lambda}$ such that $\lambda \neq 0$ and $m > 1$. Let $U \in \mathbb{C}^{n \times n}$ transforming A into A_J, and such that its rows at the same position as a row of $J_{m,\lambda}$ in A_J contain only rational components if $\lambda = 1$ (according to Lemma 23, such a U always exists). Let π be the projection mapping A_J onto $J_{m,\lambda}$. Applying Theorem 17, we have that for every r-definable set $S \subseteq \mathbb{Z}^n$, the set

$$S' = \{J_{m,\lambda}^k \vec{x} + \sum_{0 \leq i < k} J_{m,\lambda}^i \vec{b'} \mid k \in \mathbb{N} \wedge \vec{x} \in \pi(U^{-1}S)\},$$

with $\vec{b'} = \pi(U^{-1}\vec{b})$, is r-definable. Depending on the value of λ, this contradicts either Lemma 21 or Lemma 22. □

The necessary conditions are now complete. They can be summarized as follows.

Theorem 25 *Let $n, r \in \mathbb{N}_0$ with $r > 1$ and $\theta = (\vec{x} := A\vec{x} + \vec{b})$ with $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$. If θ is such that for every r-definable set $S \subseteq \mathbb{Z}^n$, the set $\theta^*(S)$ is r-definable, then*

(1) There exist $p \in \mathbb{N}_0$ and $m \in \mathbb{N}$ such that every nonzero eigenvalue λ of A satisfies $\lambda^p = r^m$, and
(2) The Jordan form of A is such that all the blocks corresponding to a nonzero eigenvalue are of size 1.

PROOF. This result is a direct consequence of Theorems 18, 20, and 24. □

Corollary 26 *Let $n, r \in \mathbb{N}_0$ with $r > 1$, and $\theta = (\vec{x} := A\vec{x} + \vec{b})$ with $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$. If θ is such that for every r-definable set $S \subseteq \mathbb{Z}^n$, the set $\theta^*(S)$ is r-definable, then there exists $p \in N_0$ such that*

(1) A^p has at most one nonzero eigenvalue λ, and
(2) λ (if any) is an integer power of r, and
(3) A^p is diagonalizable.

PROOF. If θ is as required, then Theorem 25 implies that there exist $p' \in \mathbb{N}_0$ and $m' \in \mathbb{N}$ such that every nonzero eigenvalue λ' of A satisfies $(\lambda')^{p'} = r^{m'}$. Moreover, the Jordan form of A is such that all the blocks corresponding to a nonzero eigenvalue are of size 1. Let $a \in \mathbb{N}_0$ be such that $a > n/p'$, and let $p = ap'$, $m = am'$. Since every eigenvalue λ of A^p is the p-th power of an eigenvalue of A, we have $\lambda = r^m$. Furthermore, every matrix transforming A into its Jordan form A_J transforms A^p into A_J^p. This last matrix is diagonal, for any power of a block of size one is of size one, and the n-th power of a block associated to the eigenvalue zero is only composed of zeroes. □

Theorem 27 *Let $n \in \mathbb{N}_0$ and $\theta = (\vec{x} := A\vec{x} + \vec{b})$ with $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$. If θ is such that for every Presburger-definable set $S \subseteq \mathbb{Z}^n$ the set $\theta^*(S)$ is Presburger-definable, then there exists $p \in N_0$ such that*

(1) The eigenvalues of A^p belong to $\{0, 1\}$, and
(2) A^p is diagonalizable.

PROOF. The result is obtained by applying the same reasoning as in the proofs of Theorems 18, 20, 24 and 25 with two relatively prime bases r_1 and r_2 (chosen arbitrarily). This can be done only because the sets $\{\vec{v}\}$ and $\{j\vec{v} \mid j \in \mathbb{N}\}$ used in the proof of Theorem 20 and in the ones of Lemmas 21 and of 22 are Presburger-definable. □

5 Sufficient Conditions

Here, we show that the necessary conditions given in Section 4 are also sufficient. In other words, if a linear transformation satisfies the conditions expressed by Corollary 26, then its closure preserves the definable nature of sets of vectors. This property is formalized as follows.

Theorem 28 *Let $n, r \in \mathbb{N}_0$ with $r > 1$ and $\theta = (\vec{x} := A\vec{x} + \vec{b})$ with $A \in \mathbb{Z}^{n\times n}$ and $\vec{b} \in \mathbb{Z}^n$. If there exists $p \in N_0$ such that A^p is diagonalizable, A^p has at most one nonzero eigenvalue λ, and λ (if any) is an integer power of r, then for any r-definable set $S \subseteq \mathbb{Z}^n$, the set $\theta^*(S)$ is r-definable.*

PROOF. Suppose that there exists such a p. For any r-definable set $S \subseteq \mathbb{Z}^n$, we have

$$\begin{aligned}\theta^*(S) &= \bigcup_{0\leq j<p,\, k\in\mathbb{N}} \theta^{pk+j}(S)\\ &= \bigcup_{0\leq j<p} \theta^j\left(\bigcup_{k\in\mathbb{N}} \theta^{pk}(S)\right)\\ &= \bigcup_{0\leq j<p} \theta^j\left((\theta^p)^*(S)\right).\end{aligned}$$

According to Theorem 9, every θ^j preserves the r-definable nature of sets, as does the finite union of sets. Therefore, it is sufficient to prove that $(\theta^p)^*$ preserves r-definability. Let $S' = (\theta^p)^*(S)$, J be the Jordan form of A^p (we know that it is diagonal), and $U \in \mathbb{Q}^{n\times n}$ be a matrix transforming A^p into J. We have

$$S' = \{A^{pk}\vec{x} + \sum_{0\leq i<k} A^{pi}\vec{b'} \mid \vec{x} \in S \wedge k \in \mathbb{N}\},$$

with $\vec{b'} = \sum_{0\leq i<p} A^i\vec{b}$. Hence,

$$S' = \{UJ^kU^{-1}\vec{x} + \sum_{0\leq i<k} UJ^iU^{-1}\vec{b'} \mid \vec{x} \in S \wedge k \in \mathbb{N}\}.$$

We distinguish two situations.

- *If all the eigenvalues of A^p belong to $\{0, 1\}$.* We have

$$\begin{aligned}S' &= S \cup \{UJU^{-1}\vec{x} + (k-1)UJU^{-1}\vec{b'} + \vec{b'} \mid \vec{x} \in S \wedge k \in \mathbb{N}_0\}\\ &= S \cup \{A^p\vec{x} + kA^p\vec{b'} + \vec{b'} \mid \vec{x} \in S \wedge k \in \mathbb{N}\}.\end{aligned}$$

Since the last member of this equation is expressed in Presburger arithmetic, the set denoted by this term is r-definable, and so is S'.

- *If all the eigenvalues of A^p belong to $\{0, r^m\}$, with $m \in \mathbb{N}_0$.* We have

$$\begin{aligned}
S' &= \{UJ^kU^{-1}\vec{x} + \sum_{0\le i<k} UJ^iU^{-1}\vec{b'} \mid \vec{x} \in S \wedge k \in \mathbb{N}\} \\
&= S \cup \{r^{m(k-1)}UJU^{-1}\vec{x} + \sum_{0<i<k} r^{m(i-1)}UJU^{-1}\vec{b'} + \vec{b'} \\
&\qquad\qquad \mid \vec{x} \in S \wedge k \in \mathbb{N}_0\} \\
&= S \cup \{r^{mk}A^p\vec{x} + \sum_{0\le i<k} r^{mi}A^p\vec{b'} + \vec{b'} \mid \vec{x} \in S \wedge k \in \mathbb{N}\} \\
&= S \cup \{r^{mk}A^p\vec{x} + \frac{r^{mk}-1}{r^m-1}A^p\vec{b'} + \vec{b'} \mid \vec{x} \in S \wedge k \in \mathbb{N}\} \\
&= S \cup \left\{\frac{1}{r^m-1}\left[r^{mk}\left((r^m-1)A^p\vec{x} + A^p\vec{b'}\right) - A^p\vec{b'}\right] + \vec{b'} \right. \\
&\qquad\qquad \left. \mid \vec{x} \in S \wedge k \in \mathbb{N}\right\} \\
&= S \cup \frac{1}{r^m-1}\left[\text{expand}\left((r^m-1)A^pS + A^p\vec{b'}, r^m\right) - A^p\vec{b'}\right] + \vec{b'}
\end{aligned}$$

According to Theorem 9, the last formula denotes a r-definable set.

□

A similar result holds for Presburger-definable sets.

Theorem 29 *Let $n, r \in \mathbb{N}_0$ with $r > 1$ and $\theta = (\vec{x} := A\vec{x} + \vec{b})$ with $A \in \mathbb{Z}^{n\times n}$ and $\vec{b} \in \mathbb{Z}^n$. If there exists $p \in N_0$ such that A^p is diagonalizable and has its eigenvalues in $\{0, 1\}$, then for any Presburger-definable set $S \subseteq \mathbb{Z}^n$, the set $\theta^*(S)$ is Presburger-definable.*

PROOF. The proof is identical to the first part of the proof of Theorem 28. □

6 Algorithms

The necessary and sufficient conditions given in Sections 4 and 5 are not directly usable in practical applications. Indeed, they are defined in terms of eigenvalues and of Jordan blocks, which can in general only be computed up to a limited accuracy. In this section, we give an algorithm for determining whether a given linear transformation with integer coefficients satisfies the necessary and sufficient conditions expressed by Theorem 25. This decision

procedure is only based on integer arithmetic. An algorithm is also given for computing a finite-state representation of the set $\theta^*(S)$ given a representation of the set of vectors $S \subseteq \mathbb{Z}^n$ and a linear transformation θ that satisfies the necessary and sufficient conditions for preserving definability.

Let $r, n \in \mathbb{N}_0$ with $r > 1$, and θ be the linear transformation $\vec{x} := A\vec{x} + \vec{b}$ with $A \in \mathbb{Z}^{n\times n}$ and $\vec{b} \in \mathbb{Z}^n$. The first problem consists in checking whether $\theta^*(S)$ is r-definable for every r-definable set $S \subseteq \mathbb{Z}^n$. In addition, if the answer is positive, we would like to compute $m \in \mathbb{N}$ and $p \in \mathbb{N}_0$ such that A^p is diagonalizable and has all its eigenvalues in $\{0, r^m\}$.

First, we check whether the eigenvalues of A satisfy the conditions required by Theorem 25. We know that those eigenvalues are the roots of the characteristic polynomial $\Pi_1(x)$ of A. Since this polynomial has integer coefficients, the product a (or $-a$) of all its nonzero roots can easily be computed as the ratio of its nonzero coefficients of lowest and of highest degree (this implies $a \in \mathbb{Q}$). According to Theorem 25, all the nonzero roots of $\Pi_1(x)$ must be of the same magnitude, and this magnitude must be equal to some rational power of r. Therefore, if $|a|$ is not a rational power of r, then θ does not preserve the r-definable nature of sets of vectors.

Let us now assume that $|a| = r^{(u/v)}$, with $u \in \mathbb{Z}$, $v \in \mathbb{N}_0$ and $\gcd(u, v) = 1$. The eigenvalues of A satisfy the conditions expressed by Theorem 25 if and only if every nonzero root of $\Pi_1(x)$ has the magnitude $|a|^{(1/n')}$, where n' is the difference between the highest and the lowest degrees of the nonzero coefficients of $\Pi_1(x)$. If $n' = 0$, then zero is the only root of $\Pi_1(x)$ and the condition is trivially satisfied. If $n' > 0$, then let $z = (n'v)/\gcd(n'v, u)$ and $y = (zu)/(n'v)$. Every eigenvalue of A^z that is different from zero must have the magnitude r^y. Therefore, each root of the characteristic polynomial $\Pi_2(x)$ of A^z must be either equal to zero or of magnitude r^y. Hence, if $k \in \mathbb{N}$ is the greatest integer such that $\Pi_2(x)$ is divisible by the polynomial x^k, then all the roots of the polynomial $\Pi_3(x) = \Pi'_2(r^y x)$, where $\Pi'_2(x) = \Pi_2(x)/x^k$, must be complex roots of 1.

The problem consisting in checking whether the eigenvalues of A satisfy the conditions expressed by Theorem 25 has thus been reduced to checking if all the roots of $\Pi_3(x)$ are complex roots of 1. This is the case if and only if there exists $l \in \mathbb{N}_0$ such that $\Pi_3(x)$ divides $x^l - 1$. Since the polynomial $\Pi_3(x)$ has integer coefficients, such an integer l exists if and only if $\Pi_3(x)$ is a product of cyclotomic polynomials. Checking this by trying successively to divide $\Pi_3(x)$ by $\Phi_1(x), \Phi_2(x), \Phi_3(x), \ldots$ introduces two difficulties. First, given an integer $i \in \mathbb{N}_0$, computing the coefficients of $\Phi_i(x)$ is tedious. One must therefore find a way of testing the divisibility of $\Pi_3(x)$ by $\Phi_i(x)$ without computing explicitly $\Phi_i(x)$. Second, one must find an upper bound on the indices i of the $\Phi_i(x)$ that have to be considered.

The first problem is solved thanks to the following theorem.

Theorem 30 *Let $i \in N_0$ and $\Pi(x)$ be a polynomial with integer coefficients such that for every $0 < j < i$, $\Pi(x)$ is not divisible by the cyclotomic polynomial $\Phi_j(x)$. The polynomial $\Pi(x)$ is divisible by $\Phi_i(x)$ if and only if the degree of the polynomial $\gcd(x^i - 1, \Pi(x))$ is at least equal to 1.*

PROOF. We have $x^i - 1 = \Phi_i(x)\Phi_{j_1}(x) \cdots \Phi_{j_q}(x)$, where each j_k is such that $0 < j_k < i$. Since the factorization of $x^i - 1$ into cyclotomic polynomials is unique, the result is immediate. □

As a consequence of this theorem, trying successively to divide $\Pi_3(x)$ by $\Phi_1(x)$, $\Phi_2(x), \Phi_3(x), \ldots$ can be done by dividing successively $\Pi_3(x)$ by its common factors with $x - 1, x^2 - 1, x^3 - 1, \ldots$. The conditions on the eigenvalues of A are satisfied if and only if one eventually obtains a polynomial of degree 0.

It remain to give an upper bound on the indices i of the cyclotomic polynomials $\Phi_i(x)$ that can potentially divide $\Pi_3(x)$. Intuitively, the idea is that it is useless to consider the $\Phi_i(x)$ whose degree is greater than the one of Π_3. We have the following theorem.

Theorem 31 *For every integer $k \in \mathbb{N}_0$ and for every degree $d \in \mathbb{N}$ such that $k > 210 \left(\frac{d}{48}\right)^{\log_{10} 11}$, we have $\text{degree}(\Phi_k(x)) > d$.*

PROOF. It is known [19] that $\text{degree}(\Phi_k(x)) = \phi(k)$, where ϕ is the Euler function, defined as

$$\phi(k) = k \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_q}\right),$$

where $p_1, p_2, \ldots, p_q$ are the (distinct) prime factors of k.

Assume first that $q \geq 5$, i.e., that k has at least five distinct prime factors. We have $p_1 \geq 2$, $p_2 \geq 3$, $p_3 \geq 5$, $p_4 \geq 7$, as well as $p_i \geq 11$ for all $i \geq 5$. These inequalities imply

$$\left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right) \left(1 - \frac{1}{p_4}\right) \geq$$

$$\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) \qquad (1)$$

and

$$\left(1-\frac{1}{p_5}\right)\left(1-\frac{1}{p_6}\right)\cdots\left(1-\frac{1}{p_q}\right) \geq \left(1-\frac{1}{11}\right)^{(q-4)}. \tag{2}$$

Moreover, since $k \geq p_1 \cdots p_q$, we have $k \geq 2.3.5.7.11^{(q-4)}$, and hence $q-4 \leq \log_{11}(k/210)$. Replacing into Equation (2), we obtain

$$\left(1-\frac{1}{p_5}\right)\left(1-\frac{1}{p_6}\right)\cdots\left(1-\frac{1}{p_q}\right) \geq \left(1-\frac{1}{11}\right)^{\log_{11}\left(\frac{k}{210}\right)}. \tag{3}$$

Introducing Equations (1) and (3) into the expression of $\phi(k)$, we obtain

$$\phi(k) \geq k\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)^{\log_{11}\left(\frac{k}{210}\right)}.$$

Now, let us show that the previous inequality also holds if $q < 5$, i.e., if k does not have more than four distinct prime factors. Let $p'_1 = 2$, $p'_2 = 3$, $p'_3 = 5$ and $p'_4 = 7$. We have

$$\begin{aligned}
\phi(k) &= k\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_q}\right) \\
&\geq k\left(1-\frac{1}{p'_1}\right)\cdots\left(1-\frac{1}{p'_q}\right) \\
&= k\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)^{\log_{11}\left(\frac{k}{210}\right)}\varphi(k),
\end{aligned}$$

with

$$\varphi(k) = \frac{1}{\left(1-\frac{1}{p'_{q+1}}\right)\cdots\left(1-\frac{1}{p'_4}\right)\left(1-\frac{1}{11}\right)^{\log_{11}\left(\frac{k}{210}\right)}}.$$

It is thus sufficient to show that $\varphi(k) \geq 1$, i.e., that

$$\left(1-\frac{1}{p'_{q+1}}\right)\cdots\left(1-\frac{1}{p'_4}\right) \leq \left(1-\frac{1}{11}\right)^{-\log_{11}\left(\frac{k}{210}\right)}.$$

For every $i \in \{q+1, \ldots, 4\}$, we have

$$\left(1-\frac{1}{p'_i}\right) \leq 1-\frac{1}{11} \leq \left(1-\frac{1}{11}\right)^{\log_{11} p'_i},$$

which yields

$$\left(1-\frac{1}{p'_{q+1}}\right)\cdots\left(1-\frac{1}{p'_4}\right) \leq \left(1-\frac{1}{11}\right)^{(\log_{11} p'_{q+1}+\cdots+\log_{11} p'_4)} = \left(1-\frac{1}{11}\right)^{\log_{11}(p'_{q+1}\cdots p'_4)}.$$

Since $k \geq p'_1 \cdots p'_q$ and $p'_1 \cdots p'_4 = 210$, we have

$$p'_{q+1}\cdots p'_4 = \frac{210}{p'_1\cdots p'_q} \geq \frac{210}{k}.$$

Therefore,

$$\left(1-\frac{1}{11}\right)^{\log_{11}(p'_{q+1}\cdots p'_4)} \leq \left(1-\frac{1}{11}\right)^{\log_{11}\left(\frac{210}{k}\right)} = \left(1-\frac{1}{11}\right)^{-\log_{11}\left(\frac{k}{210}\right)}$$

and hence $\varphi(k) \geq 1$.

In summary, we have for every $k \in \mathbb{N}_0$

$$\phi(k) \geq k\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)^{\log_{11}\left(\frac{k}{210}\right)}.$$

This yields

$$\begin{aligned}\phi(k) &\geq \frac{8k}{35} e^{(\log_{11}(10)-1)\log_e \frac{k}{210}} \\ &= \frac{8k}{35}\left(\frac{k}{210}\right)^{\log_{11}(10)-1} \\ &= 48\left(\frac{k}{210}\right)^{\log_{11} 10}.\end{aligned}$$

If k is such that $k > 210\left(\frac{d}{48}\right)^{\log_{10} 11}$, then this last expression implies $\phi(k) > d$. $\square$

Note that the same reasoning can be followed so as to obtain a better bound (up to an arbitrary amount of accuracy), by considering a greater number of prime factors in the expansion of $\phi(k)$. The choice of expanding only the

first five prime factors was motivated by an explicit computation of the first few hundred cyclotomic polynomials, which demonstrated that the bound expressed by Theorem 31 is nearly optimal for these polynomials.

It remains to check whether the sizes of the Jordan blocks of A satisfy the conditions required by Theorem 25. We assume that the conditions on the eigenvalues of A are satisfied. Let $i_1, i_2, \ldots, i_q$ ($q \in \mathbb{N}$) be all the integers i such that $\Pi_3(x)$ has common factors with $x^i - 1$. The least common multiple l of $i_1, i_2, \ldots, i_q$ is such that the l-th power of every root of $\Pi_3(x)$ is exactly equal to 1. This means that all the nonzero eigenvalues of A^{zl} are equal to r^{yl}. Let

$$l' = \begin{cases} l & \text{if } zl \geq n \text{ or } \Pi_2(x) = \Pi_2'(x), \\ l\lceil n/(zl) \rceil & \text{if } zl < n \text{ and } \Pi_2(x) \neq \Pi_2'(x), \end{cases}$$

and let $m = yl'$, $p = zl'$. All the eigenvalues of A^p belong to $\{0, r^m\}$. If A^p has the eigenvalue 0, then the definition of l' yields $p \geq n$, which implies that the Jordan blocks of A^p associated to the eigenvalue 0 are only composed of zeroes. The condition on the size of the Jordan blocks of A will thus be satisfied if and only if A^p is diagonalizable. This can be checked thanks to the following result.

Theorem 32 *A square matrix is diagonalizable if and only if its minimal polynomial has only simple roots.*

PROOF. A proof of this well-known result can be found in [2] or [16]. □

In the present case, we know that the minimal polynomial of A^p has to be either 0, x, $x - r^m$ or $x(x - r^m)$, depending on the eigenvalues of A. This can be checked explicitly.

An algorithm formalizing the decision procedure that has just been developed is given in Figures 1 and 2. (In this algorithm, the test performed at Line 11 can easily be carried out by comparing the prime factors of a_0, a_1 and r.)

Theorem 33 *Let $r, n \in \mathbb{N}_0$ and θ be the linear transformation $\vec{x} = A\vec{x} + \vec{b}$ with $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$. The set $\theta^*(S)$ is r-definable for every r-definable set $S \subseteq \mathbb{Z}^n$ if and only if DEFINABLE-CLOSURE?(r, n, A) returns a triple of the form $(\mathbf{T}, m, p)$, with $m \in \mathbb{N}$ and $p \in \mathbb{N}_0$. If this is the case, then m and p are such that A^p is diagonalizable and has all its eigenvalues in $\{0, r^m\}$.*

PROOF. The algorithm in Figures 1 and 2 is a direct implementation of the computation method discussed in this section. In Lines 41–42, the condition

function DEFINABLE-CLOSURE?(base r, dimension n, integer matrix A) : $\{\mathbf{T}, \mathbf{F}\} \times \mathbb{N} \times \mathbb{N}_0$

1: **var** Π_1, Π_2, Π : polynomials with integer coefficients;
2: $d_0, d_1, a_0, a_1, a, u, v, n', z, y, i, m, p, l$: integers;
3: M : integer matrix;
4: **begin**
5: $\Pi_1(x)$:= characteristic polynomial of A;
6: d_0 := lowest degree of the nonzero terms of $\Pi_1(x)$;
7: d_1 := highest degree of the nonzero terms of $\Pi_1(x)$;
8: a_0 := coefficient of $\Pi_1(x)$ with the degree d_0;
9: a_1 := coefficient of $\Pi_1(x)$ with the degree d_1;
10: $a := a_0/a_1$;
11: **if** $(r > 1 \wedge \log_r(|a|) \notin \mathbb{Q}) \vee (r = 1 \wedge |a| \neq 1)$ **then** **return** $(\mathbf{F}, 0, 0)$;
12: **if** $r = 1$ **then** $(u, v) := (1, 1)$
13: **else let** $u/v := \log_r(|a|)$ **such that** $u \in \mathbb{Z} \wedge v \in \mathbb{N}_0 \wedge \gcd(u, v) = 1$;
14: $n' := d_1 - d_0$;
15: **if** $n' = 0$ **then return** $(\mathbf{T}, 0, n)$;
16: $z := (n'v)/\gcd(n'v, u)$;
17: $y := (zu)/(n'v)$;
18: $\Pi_2(x)$:= characteristic polynomial of A^z;
19: $n' := n$;
20: **while** x divides $\Pi_2(x)$ **do**
21: **begin**
22: $\Pi_2(x) := \Pi_2(x)/x$;
23: $n' := n' - 1$
24: **end**;

(. . .)

Fig. 1. Decision procedure for the preservation of r-definability by the closure of a linear transformation.

```
(...)
25:        Π3(x) := Π2(r^y x);
26:        l := 1;
27:        for i := 1 to ⌊210(n'/48)^(log10 11)⌋ do
28:            begin
29:                Π(x) := gcd(x^i − 1, Π3(x));
30:                if degree(Π(x)) > 0 then
31:                    begin
32:                        l := lcm(l, i);
33:                        while Π(x) divides Π3(x) do
34:                            Π3(x) := Π3(x)/Π(x)
35:                    end
36:            end;
37:        if degree(Π3(x)) > 0 then return (F, 0, 0);
38:        if zl < n ∧ n' < n then l := l⌈n/(zl)⌉;
39:        (m, p) := (yl, zl);
40:        M := I_n;
41:        if n' > 0 then M := (A^p − r^m I_n)M;
42:        if n' < n then M := A^p M;
43:        if A^p = (0) ∨ M = (0) then return (T, m, p);
44:        return (F, 0, 0)
45:    end.
```

Fig. 2. Decision procedure for the preservation of r-definability by the closure of a linear transformation (continued).

on the minimal polynomial of A^p is checked by taking advantage of the facts that $n' > 0$ if and only if A^p has the eigenvalue r^m, and that $n' < n$ if and only if A^p has the eigenvalue 0. □

Theorem 34 *Let $n \in \mathbb{N}_0$ and θ be the linear transformation $\vec{x} := A\vec{x} + \vec{b}$ with $A \in \mathbb{Z}^{n\times n}$ and $\vec{b} \in \mathbb{Z}^n$. The set $\theta^*(S)$ is Presburger-definable for every Presburger-definable set $S \subseteq \mathbb{Z}^n$ if and only if DEFINABLE-CLOSURE?$(1, n, A)$ returns a triple of the form $(\mathbf{T}, m, p)$, with $m \in \mathbb{N}$ and $p \in \mathbb{N}_0$. If this is the case, then p is such that A^p is diagonalizable and has all its eigenvalues in $\{0, 1\}$.*

function APPLY-STAR-BASE(base r, dimension n, NDD $\mathcal{A}$,
linear operation $\vec{x} := A\vec{x} + \vec{b}$) : NDD

1: **var** m, p : integers;
2: $\vec{b'}$: integer vector;
3: $\mathcal{A}'$: NDD;
4: **begin**
5: $(\mathbf{T}, m, p) :=$ DEFINABLE-CLOSURE?(r, n, A);
6: $\vec{b'} := \sum_{0 \leq i < p} A^i \vec{b}$;
7: **if** $m = 0$ **then**
8: $\mathcal{A}' := \mathrm{NDD}\Big(\mathrm{SET}(\mathcal{A}) \cup \{\vec{y} \in \mathbb{Z}^n \mid (\exists k \in \mathbb{N}, \vec{x} \in \mathrm{SET}(\mathcal{A}))$
$(\vec{y} = A^p\vec{x} + kA^p\vec{b'} + \vec{b'})\}\Big)$
9: **else**
10: $\mathcal{A}' := \mathrm{NDD}\Big(\mathrm{SET}(\mathcal{A}) \cup (1/(r^m - 1))$
$\Big[\mathrm{expand}\Big((r^m - 1)A^p\,\mathrm{SET}(\mathcal{A}) + A^p\vec{b'}, r^m\Big) - A^p\vec{b'}\Big] + \vec{b'}\Big)$;
11: **return** NDD $\left(\bigcup_{0 \leq j < p} \left(A^j\,\mathrm{SET}(\mathcal{A}') + \sum_{0 \leq i < j} A^i\vec{b}\right)\right)$
12: **end**.

Fig. 3. Image of an NDD by the closure of a linear transformation in a given base.

PROOF. The result is a direct consequence of Theorems 27 and 33. □

It remains to give an algorithm for computing the image of a definable set of vectors $S \subseteq \mathbb{Z}^n$ ($n \in \mathbb{N}$) by the closure of a linear transformation $\vec{x} := A\vec{x} + \vec{b}$ that satisfies DEFINABLE-CLOSURE?. An expression of this image in terms of S and of operations preserving the definable nature of sets has already been obtained in the proof of Theorem 28. Algorithms based on that result are given in Figures 3 and 4. In these algorithms, NDD(ϕ) and SET($\mathcal{A}$) denote respectively an NDD representing the formula ϕ, which can be computed thanks to the constructive proof of Theorem 2, and the set represented by the NDD $\mathcal{A}$.

Theorem 35 *Let $r, n \in \mathbb{N}_0$ with $r > 1$ and θ be the linear transformation $\vec{x} := A\vec{x} + \vec{b}$, with $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$, such that DEFINABLE-CLOSURE?$(r, n, A) = (\mathbf{T}, q, p)$ for some q and p. If $\mathcal{A}$ is an NDD representing the set of vectors $S \subseteq \mathbb{Z}^n$ in base r, then APPLY-STAR-BASE$(r, n, \mathcal{A}, \theta)$ is an NDD representing the set $\theta^*(S)$ in base r.*

function APPLY-STAR-PRESBURGER(dimension n, NDD $\mathcal{A}$,
linear operation $\vec{x} := A\vec{x} + \vec{b}$) : NDD

1: **var** p : integer;
2: $\vec{b'}$: integer vector;
3: $\mathcal{A}'$: NDD;
4: **begin**
5: $(\mathbf{T}, 0, p) :=$ DEFINABLE-CLOSURE?$(1, n, A)$;
6: $\vec{b'} := \sum_{0 \le i < p} A^i \vec{b}$;
7: $\mathcal{A}' :=$ NDD$\Big($SET$(\mathcal{A}) \cup \{\vec{y} \in \mathbb{Z}^n \mid (\exists k \in \mathbb{N}, \vec{x} \in$ SET$(\mathcal{A}))$
$(\vec{y} = A^p\vec{x} + kA^p\vec{b} + \vec{b'})\}\Big)$;
8: **return** NDD $\left(\bigcup_{0 \le k < p} \left(A^k \text{ SET}(\mathcal{A}') + \sum_{0 \le i < k} A^i \vec{b} \right) \right)$
9: **end**.

Fig. 4. Image of an NDD by the closure of a linear transformation in any base.

PROOF. The algorithm in Figure 3 is a direct implementation of the computation performed in the proof of Theorem 28. □

Theorem 36 *Let $n \in \mathbb{N}_0$ and θ be the linear transformation $\vec{x} := A\vec{x} + \vec{b}$, with $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$, such that DEFINABLE-CLOSURE?$(1, n, A) = (\mathbf{T}, q, p)$ for some q and p. If $\mathcal{A}$ is an NDD representing the Presburger-definable set of vectors $S \subseteq \mathbb{Z}^n$ in some base $r > 1$, then APPLY-STAR-PRESBURGER$(n, \mathcal{A}, \theta)$ is an NDD representing the Presburger-definable set $\theta^*(S)$ in base r.*

PROOF. The algorithm in Figure 4 is a direct implementation of the computation performed in the proof of Theorem 28. □

7 Linear Transformations with Guards

We now move to the more general case of operations of the form $\theta = (P\vec{x} \le \vec{q} \to \vec{x} := A\vec{x} + \vec{b})$, where $n, m \in \mathbb{N}$, $P \in \mathbb{Z}^{m \times n}$, $\vec{q} \in \mathbb{Z}^m$, $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$. The semantics of such a guarded transformation is defined by the function

$$\theta : \{\vec{v} \in \mathbb{Z}^n \mid P\vec{v} \le \vec{q}\} \to \mathbb{Z}^n : \vec{v} \mapsto A\vec{v} + \vec{b}$$

(i.e., $\theta(\vec{v})$ is equal to $A\vec{v}+\vec{b}$ if $P\vec{v} \leq \vec{q}$, and is undefined otherwise.)

We do not provide a general solution to the problem of checking whether the closure of a guarded linear transformation preserves the recognizable nature of sets. Instead, we show that the results developed in Sections 4, 5 and 6 can be adapted with little difficulty to guarded transformations, in the form of a *sufficient* condition for the preservation of recognizability.

Precisely, the sufficient condition is a consequence of a remarkable property: if θ is such that its underlying guardless transformation $\vec{x} := A\vec{x}+\vec{b}$ satisfies the necessary and sufficient conditions expressed by Theorem 25, then for every definable set $S \subseteq \mathbb{Z}^n$, the set $\theta^*(S)$ is definable. Moreover, an NDD representing $\theta^*(S)$ can be computed from an NDD representing S. Formally, we have the following result.

Theorem 37 *Let $n \in \mathbb{N}$, $r \in \mathbb{N}$ with $r > 1$, $m \in \mathbb{N}$, and $\theta = (P\vec{x} \leq \vec{q} \rightarrow \vec{x} := A\vec{x}+\vec{b})$ with $P \in \mathbb{Z}^{m\times n}$, $q \in \mathbb{Z}^m$, $A \in \mathbb{Z}^{n\times n}$ and $\vec{b} \in \mathbb{Z}^n$. If there exists $p \in N_0$ such that A^p is diagonalizable, has at most one nonzero eigenvalue λ, and λ (if any) is an integer power of r, then for any r-definable set $S \subseteq \mathbb{Z}^n$, the set $\theta^*(S)$ is r-definable.*

PROOF. Suppose that there exists a suitable p. Let $S \subseteq \mathbb{Z}^n$ be a r-definable set, θ' be the guardless linear transformation $(\vec{x} := A\vec{x}+\vec{b})$, and $V = \{\vec{x} \in \mathbb{Z}^n \mid P\vec{x} \leq \vec{q}\}$. We have

$$\begin{aligned}\theta^*(S) &= \{(\theta')^k(\vec{x}) \mid \vec{x} \in S \wedge k \in \mathbb{N} \wedge \bigwedge_{0\leq i<k} (\theta')^i(\vec{x}) \in V\} \\ &= \{(\theta')^{pk+j}(\vec{x}) \mid \vec{x} \in S \wedge k \in \mathbb{N} \wedge 0 \leq j < p \\ &\qquad \wedge \bigwedge_{0\leq i<j} [(\theta')^i(\vec{x}) \in V] \wedge \bigwedge_{0\leq i<k} \bigwedge_{0\leq l<p} [(\theta')^l((\theta')^{pi+j}(\vec{x})) \in V]\}.\end{aligned}$$

Let

$$V' = \{\vec{x} \in \mathbb{Z}^n \mid \bigwedge_{0\leq l<p} [(\theta')^l(\vec{x}) \in V]\}.$$

The expression of $\theta^*(S)$ becomes

$$\begin{aligned}\theta^*(S) &= \{(\theta')^{pk+j}(\vec{x}) \mid \vec{x} \in S \wedge k \in \mathbb{N} \wedge 0 \leq j < p \\ &\qquad \wedge \bigwedge_{0\leq i<j} [(\theta')^i(\vec{x}) \in V] \wedge \bigwedge_{0\leq i<k} [(\theta')^{pi+j}(\vec{x}) \in V']\} \\ &= \bigcup_{0\leq j<p} S_j,\end{aligned}$$

with for every $j \in \{0, 1, \ldots, p-1\}$,

$$S_j = \{(\theta')^{pk+j}(\vec{x}) \mid \vec{x} \in S \wedge k \in \mathbb{N} \wedge \bigwedge_{0 \leq i < j} [(\theta')^i(\vec{x}) \in V] \wedge \bigwedge_{0 \leq i < k} [(\theta')^{pi+j}(\vec{x}) \in V']\}.$$

Let us define

$$U_j = \{\vec{x} \in \mathbb{Z}^n | (\exists \vec{x}\,' \in S)(\vec{x} = (\theta')^j(\vec{x}\,') \wedge \bigwedge_{0 \leq i < j} [(\theta')^i(\vec{x}\,') \in V])\}.$$

We obtain

$$S_j = \{(\theta')^{pk}(\vec{x}) \mid k \in \mathbb{N} \wedge \vec{x} \in U_j \wedge \bigwedge_{0 \leq i < k} [(\theta')^{pi}(\vec{x}) \in V']\}.$$

By construction, V' is a convex set. Moreover, it follows from the algorithm in Figure 3 that all the the vectors belonging to $\{(\theta')^{pi}(\vec{x}), (\theta')^{p(i+1)}(\vec{x}), \ldots\}$ are colinear. It follows that for any $k > 1$, the condition

$$\bigwedge_{0 \leq i < k} [(\theta')^{pi}(\vec{x}) \in V']$$

is equivalent to

$$\vec{x} \in V' \wedge (\theta')^p(\vec{x}) \in V' \wedge (\theta')^{(k-1)p}(\vec{x}) \in V'.$$

Therefore, we have

$$\begin{aligned} S_j = {} & U_j \cup \{(\theta')^p(\vec{x}) \mid \vec{x} \in U_j \cap V'\} \\ & \cup \{(\theta')^{pk}(\vec{x}) \mid k \in \mathbb{N} \wedge k \geq 2 \wedge \vec{x} \in U_j \cap V' \\ & \qquad \wedge (\theta')^p(\vec{x}) \in V' \wedge (\theta')^{p(k-1)}(\vec{x}) \in V'\} \\ = {} & (\theta')^p(U_j \cap V') \cup (\theta')^p((\theta')^p([(\theta')^p]^*(U_j \cap V' \cap V'')) \cap V'), \end{aligned}$$

with $V'' = \{\vec{x} \in \mathbb{Z}^n \mid (\theta')^p(\vec{x}) \in V'\}$. Since V', V'' and every U_j are Presburger-definable (and thus r-definable), every S_j is r-definable. It follows that $\theta^*(S)$ is r-definable as well. $\square$

Unfortunately, the reciprocal of Theorem 37 does not hold. Indeed, there are guarded linear transformations that preserve the r-definable nature of sets of vectors, but whose underlying guardless transformation does not. The conditions expressed by Theorem 37 are thus sufficient, but not necessary. Obtaining

necessary and sufficient conditions over guarded linear transformations that preserve the r-definable nature of sets of vectors seems to be a very difficult problem. (Intuitively, the difficulty originates from the fact that, if a linear operation θ does not satisfy the hypotheses of Theorem 37, then the orbit $\{\theta^k(\vec{v}) \mid k \in \mathbb{N}\}$ of an individual vector $\vec{v} \in \mathbb{Z}^n$ to which θ is repeatedly applied is in general non-linear. This makes a manageable description of $\theta^*(S)$, for a subset S of $\mathbb{Z}^n$, much more difficult to obtain.)

A result similar to Theorem 37 holds for Presburger-definable sets.

Theorem 38 *Let $n \in \mathbb{N}$, $m \in \mathbb{N}$, and $\theta = (\vec{x} := P\vec{x} \leq \vec{q} \rightarrow A\vec{x} + \vec{b})$, with $P \in \mathbb{Z}^{m \times n}$, $q \in \mathbb{Z}^m$, $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$. If there exists $p \in N_0$ such that A^p is diagonalizable, has at most one nonzero eigenvalue λ, and $\lambda = 1$, then for any Presburger-definable set $S \subseteq \mathbb{Z}^n$, the set $\theta^*(S)$ is Presburger-definable.*

Identical to the proof of Theorem 37. □

The previous theorems state that one can use the function computed by the algorithm DEFINABLE-CLOSURE? of Figures 1 and 2 as a sufficient criterion for guarded transformations. It remains to give an algorithm for computing the image of a definable set of vectors $S \subseteq \mathbb{Z}^n$ ($n \in \mathbb{N}$) by the closure of a guarded linear operation $(P\vec{x} \leq \vec{q} \rightarrow \vec{x} := A\vec{x} + \vec{b})$ that satisfies this criterion. An expression of this image in terms of S and of operations preserving the definable nature of sets is given in the proof of Theorem 37. Algorithms based on that result are given in Figures 5 and 6.

Theorem 39 *Let $r, n \in \mathbb{N}_0$ with $r > 1$, and θ be the guarded linear transformation $(P\vec{x} \leq \vec{q} \rightarrow \vec{x} := A\vec{x} + \vec{b})$, with $m \in \mathbb{N}$, $P \in \mathbb{Z}^{m \times n}$, $q \in \mathbb{Z}^m$, $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$ such that DEFINABLE-CLOSURE?$(r, n, A) = (\mathbf{T}, q, p)$ for some q and p. If $\mathcal{A}$ is an NDD representing the set of vectors $S \subseteq \mathbb{Z}^n$ in base r, then APPLY-STAR-GUARDED-BASE$(r, n, \mathcal{A}, \theta)$ is an NDD representing the set $\theta^*(S)$ in base r.*

PROOF. The algorithm in Figure 5 is a direct implementation of the computation performed in the proof of Theorem 37. □

Theorem 40 *Let $n \in \mathbb{N}_0$ and θ be the linear operation $(P\vec{x} \leq \vec{q} \rightarrow \vec{x} := A\vec{x} + \vec{b})$, with $m \in \mathbb{N}$, $P \in \mathbb{Z}^{m \times n}$, $q \in \mathbb{Z}^m$, $A \in \mathbb{Z}^{n \times n}$ and $\vec{b} \in \mathbb{Z}^n$ such that DEFINABLE-CLOSURE?$(1, n, A) = (\mathbf{T}, q, p)$ for some q and p. If $\mathcal{A}$ is an NDD representing the Presburger-definable set of vectors $S \subseteq \mathbb{Z}^n$ in some base $r > 1$, then APPLY-STAR-GUARDED-PRESBURGER$(n, \mathcal{A}, \theta)$ is an NDD representing the Presburger-definable set $\theta^*(S)$ in base r.*

function APPLY-STAR-GUARDED-BASE(base r, dimension n, NDD $\mathcal{A}$, linear operation $(P\vec{x} \leq \vec{q} \rightarrow \vec{x} := A\vec{x} + \vec{b})$) : NDD

1: **var** m, p, j : integers;
2: θ' : guardless linear transformation;
3: $\mathcal{A}', \mathcal{A}'', \mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4$: NDDs;
4: **begin**
5: $(\mathbf{T}, m, p) := \text{DEFINABLE-CLOSURE?}(r, n, A)$;
6: $\theta' := (\vec{x} := A\vec{x} + \vec{b})$;
7: $\mathcal{A}_1 := \text{NDD}(\{\vec{x} \in \mathbb{Z}^n \mid P\vec{x} \leq \vec{q}\})$;
8: $\mathcal{A}_2 := \text{NDD}(\{\vec{x} \in \mathbb{Z}^n \mid \bigwedge_{0 \leq l < p} P(\theta')^l(\vec{x}) \leq \vec{q}\})$;
9: $\mathcal{A}_3 := \text{NDD}(\{\vec{x} \in \mathbb{Z}^n \mid \bigwedge_{0 \leq l < p} P(\theta')^{l+p}(\vec{x}) \leq \vec{q}\})$;
10: $\mathcal{A}' := \text{NDD}(\emptyset)$;
11: **for** $j := 0$ **to** $p - 1$ **do**
12: **begin**
13: $\mathcal{A}_4 := \text{NDD}\Big(\{\vec{x} \in \mathbb{Z}^n \mid (\exists \vec{x}\,' \in \text{SET}(\mathcal{A}))$
$(\vec{x} = (\theta')^j(\vec{x}\,') \wedge \bigwedge_{0 \leq i < j} [(\theta')^i(\vec{x}\,') \in \text{SET}(\mathcal{A}_1)])\}\Big)$;
14: $\mathcal{A}' := \mathcal{A}' \cup \mathcal{A}_4 \cup \text{NDD}((\theta')^p(\text{SET}(\mathcal{A}_4) \cap \text{SET}(\mathcal{A}_2)))$;
15: $\mathcal{A}'' := \text{APPLY-STAR-BASE?}(r, n,$
$\mathcal{A}_2 \cap \mathcal{A}_3 \cap \mathcal{A}_4, A^p, \sum_{0 \leq k < p} A^k\vec{b})$;
16: $\mathcal{A}' := \mathcal{A}' \cup \text{NDD}((\theta')^p((\theta')^p(\text{SET}(\mathcal{A}'')) \cap \text{SET}(\mathcal{A}_2)))$
17: **end**;
18: **return** $\mathcal{A}'$
19: **end**.

Fig. 5. Image of an NDD by the closure of a guarded transformation in a given base.

PROOF. The algorithm in Figure 6 is a direct implementation of the computation performed in the proof of Theorem 37. □

function APPLY-STAR-GUARDED-PRESBURGER(dimension n, NDD $\mathcal{A}$, linear operation $(P\vec{x} \leq \vec{q} \rightarrow \vec{x} := A\vec{x} + \vec{b})$) : NDD

1: **var** p, j : integers;
2: θ' : guardless linear transformation;
3: $\mathcal{A}', \mathcal{A}'', \mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4$: NDD;
4: **begin**
5: $(\mathbf{T}, 0, p) := \text{DEFINABLE-CLOSURE?}(n, A)$;
6: $\theta' := (\vec{x} := A\vec{x} + \vec{b})$;
7: $\mathcal{A}_1 := \text{NDD}(\{\vec{x} \in \mathbb{Z}^n \mid P\vec{x} \leq \vec{q}\})$;
8: $\mathcal{A}_2 := \text{NDD}(\{\vec{x} \in \mathbb{Z}^n \mid \bigwedge_{0 \leq l < p} P(\theta')^l(\vec{x}) \leq \vec{q}\})$;
9: $\mathcal{A}_3 := \text{NDD}(\{\vec{x} \in \mathbb{Z}^n \mid \bigwedge_{0 \leq l < p} P(\theta')^{l+p}(\vec{x}) \leq \vec{q}\})$;
10: $\mathcal{A}' := \text{NDD}(\emptyset)$;
11: **for** $j := 0$ **to** $p - 1$ **do**
12: **begin**
13: $\mathcal{A}_4 := \text{NDD}\Big(\{\vec{x} \in \mathbb{Z}^n \mid (\exists \vec{x}\,' \in \text{SET}(\mathcal{A}))(\vec{x} = (\theta')^j(\vec{x}\,') \wedge \bigwedge_{0 \leq i < j} [(\theta')^i(\vec{x}\,') \in \text{SET}(\mathcal{A}_1)]])\}\Big)$;
14: $\mathcal{A}' := \mathcal{A}' \cup \mathcal{A}_4 \cup \text{NDD}((\theta')^p(\text{SET}(\mathcal{A}_4) \cap \text{SET}(\mathcal{A}_2)))$;
15: $\mathcal{A}'' := \text{APPLY-STAR-PRESBURGER}(n, \mathcal{A}_2 \cap \mathcal{A}_3 \cap \mathcal{A}_4, A^p, \sum_{0 \leq k < p} A^k\vec{b})$;
16: $\mathcal{A}' := \mathcal{A}' \cup \text{NDD}((\theta')^p((\theta')^p(\text{SET}(\mathcal{A}'')) \cap \text{SET}(\mathcal{A}_2)))$
17: **end**;
18: **return** $\mathcal{A}'$
19: **end**.

Fig. 6. Image of an NDD by the closure of a guarded transformation in any base.

8 Proofs of Auxiliary Results

This section contains the proofs that were omitted from Sections 3 and 4 for clarity sake. They are presented according to their order of occurrence in the

main text.

Theorem 8 *Let $n, r \in \mathbb{N}_0$ with $r > 1$. A set $S \subseteq \mathbb{Z}^n$ is r-definable if and only if it is r-recognizable.*

PROOF.

- *If S is r-definable, then S is r-recognizable.* If S is r-definable, then there exist $m \in \mathbb{N}_0$, $S' \subseteq \mathbb{Z}^m$ and $U \in \mathbb{C}^{n \times m}$ such that S' is r-recognizable and $S = US'$. Let $B \subset \mathbb{Z}^m$ be a maximal subset of linearly independent vectors from S', i.e., a finite subset of S' such that each vector in S' can be expressed as a linear combination of vectors in B. There exists $a \in \mathbb{N}_0$ such that every vector in S' is a linear combination with integer coefficients of vectors in $(1/a)B$. Let p be the number of vectors in B, and $T \in \mathbb{Q}^{m \times p}$ be a matrix such that $\mathrm{col}(T) = (1/a)B$. Since S' is r-recognizable, the set

$$S'' = \{\vec{x} \in \mathbb{Z}^p \mid T\vec{x} \in S'\}$$

  is r-recognizable as well. We have $S' = TS''$, hence $S = (UT)S''$. Every column $\vec{c}$ of T belongs to $(1/a)S'$, and thus is such that $U\vec{c}$ belongs to $(1/a)S$. It follows that $UT \in \mathbb{Q}^{n \times p}$, and therefore the equation $S = (UT)S''$ leads to a definition of S in the first-order theory $\langle \mathbb{Z}, \leq, +, V_r \rangle$ (recall that S'' is r-recognizable). It follows that S is r-recognizable.
- *If S is r-recognizable, then S is r-definable.* Let $U = I_n$ and $S' = S$. We have $S = US'$, where S' is a r-recognizable subset of $\mathbb{Z}^n$, hence S is r-definable.

□

Before proving Theorem 9, we introduce the following lemma.

Lemma 41 *Let $r \in \mathbb{N}$ with $r > 1$, $n, m_1, m_2 \in \mathbb{N}_0$, $U_1 \in \mathbb{C}^{n \times m_1}$, and $U_2 \in \mathbb{C}^{n \times m_2}$. The set*

$$\left\{ \begin{bmatrix} \vec{x}_1 \\ \vec{x}_2 \end{bmatrix} \in \mathbb{Z}^{m_1+m_2} \mid U_1\vec{x}_1 = U_2\vec{x}_2 \right\}$$

is r-definable.

PROOF. It is sufficient to prove that for any $m \in \mathbb{N}_0$ and $\vec{u} \in \mathbb{C}^m$, the set S of all the vectors $\vec{x} \in \mathbb{Z}^m$ satisfying $\vec{u} \cdot \vec{x} = 0$ is Presburger-definable. Indeed,

applying this result to $m = m_1 + m_2$ and

$$\vec{u} = \begin{bmatrix} \vec{u}_1 \\ -\vec{u}_2 \end{bmatrix},$$

where $\vec{u}_1$ and $\vec{u}_2$ are rows at the same position in U_1 and in U_2, shows that the set of all the vectors

$$\begin{bmatrix} \vec{x}_1 \\ \vec{x}_2 \end{bmatrix} \in \mathbb{Z}^{m_1+m_2}$$

such that $\vec{u_1} \cdot \vec{x}_1 = \vec{u_2} \cdot \vec{x}_2$ is Presburger-definable. The intersection of the sets obtained for each pair of matching rows in U_1 and U_2 is thus Presburger-definable, and therefore r-definable.

It remains to prove that the set S of all the solutions in $\mathbb{Z}^m$ of $\vec{u} \cdot \vec{x} = 0$ is Presburger-definable. This set is an additive subgroup of $\mathbb{R}^m$. An additive subgroup of $\mathbb{R}^m$ is finitely generated if and only if it is discrete (Theorem 6.1 in [28]). Since $S \subseteq \mathbb{Z}^m$, S is discrete and thus finitely generated. Let $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_p$ be the generators of S. We have

$$S = \{a_1\vec{v}_1 + \cdots + a_p\vec{v}_p \mid a_1, \ldots, a_p \in \mathbb{Z}\}.$$

This expression can be rewritten as

$$S = \{\vec{x} \in \mathbb{Z}^m \mid (\exists a_1, \ldots, a_p \in \mathbb{Z})(\vec{x} = a_1\vec{v}_1 + \cdots + a_p\vec{v}_p)\},$$

which is a formula of Presburger arithmetic defining S. □

Theorem 9 *Let $r \in \mathbb{N}$ with $r > 1$, $n_1, n_2 \in \mathbb{N}_0$, $S_1 \subseteq \mathbb{C}^{n_1}$, $S_2 \subseteq \mathbb{C}^{n_2}$ such that S_1 and S_2 are r-definable, $\vec{v} \in \mathbb{C}^{n_1}$, $p, q \in \mathbb{N}_0$, $k \in \mathbb{N}$ such that $0 < k \leq n_1$, and $T \in \mathbb{C}^{p \times n_1}$. The following sets are r-definable:*

- *Any finite subset of $\mathbb{C}^{n_1}$,*
- *$S_1 + \vec{v}$,*
- *TS_1,*
- *$S_1 \cup S_2$, provided that $n_1 = n_2$,*
- *$S_1 \cap S_2$, provided that $n_1 = n_2$,*
- *$S_1 \times S_2$,*
- *$\{(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_{n_1}) \mid (x_1, \ldots, x_{n_1}) \in S_1\}$,*

- $\left\{ \begin{bmatrix} \vec{x} \\ \Re(\vec{x}) \\ \Im(\vec{x}) \end{bmatrix} \mid \vec{x} \in S_1 \right\}$,
- $expand(S_1, r^q) = \{r^{qk}\vec{x} \mid \vec{x} \in S_1 \wedge k \in \mathbb{N}\}$.

PROOF.

- *Any finite subset of $\mathbb{C}^{n_1}$ is r-definable.* Let $S_1 = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_m\}$. Defining $U = [\vec{v}_1; \ldots; \vec{v}_m]$ and $S' = \{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_{n_1}\}$, we obtain $S_1 = US'$, where $S' \subseteq \mathbb{Z}^{n_1}$ is r-definable. It follows that S_1 is r-definable.
- *$S_1 + \vec{v}$ is r-definable.* There exist $m \in \mathbb{N}_0$, $U \in \mathbb{C}^{n_1 \times m}$ and $S' \subseteq \mathbb{Z}^m$ such that S' is r-definable and $S_1 = US'$. Since $S_1 + \vec{v} = [U; \vec{v}]\,(S' \times \{1\})$, the set $S_1 + \vec{v}$ is r-definable.
- *TS_1 is r-definable.* There exist $m \in \mathbb{N}_0$, $U \in \mathbb{C}^{n_1 \times m}$ and $S' \subseteq \mathbb{Z}^m$ such that S' is r-definable and $S_1 = US'$. Since $TS_1 = (TU)S'$, the set TS_1 is r-definable.
- *$S_1 \cup S_2$ is r-definable.* There exist $m_1, m_2 \in \mathbb{N}_0$, $U_1 \in \mathbb{C}^{n_1 \times m_1}$, $U_2 \in \mathbb{C}^{n_1 \times m_2}$, $S'_1 \subseteq \mathbb{Z}^{m_1}$ and $S'_2 \subseteq \mathbb{Z}^{m_2}$ such that S'_1 and S'_2 are r-definable, $S_1 = U_1 S'_1$, and $S_2 = U_2 S'_2$. Since $S_1 \cup S_2 = [U_1; U_2]\,((S'_1 \times (0)^{m_2}) \cup ((0)^{m_1} \times S'_2))$, the set $S_1 \cup S_2$ is r-definable.
- *$S_1 \cap S_2$ is r-definable.* There exist $m_1, m_2 \in \mathbb{N}_0$, $U_1 \in \mathbb{C}^{n_1 \times m_1}$, $U_2 \in \mathbb{C}^{n_1 \times m_2}$, $S'_1 \subseteq \mathbb{Z}^{m_1}$ and $S'_2 \subseteq \mathbb{Z}^{m_2}$ such that S'_1 and S'_2 are r-definable, $S_1 = U_1 S'_1$, and $S_2 = U_2 S'_2$. Let $V \in \mathbb{Z}^{m_1+m_2}$ be the set

$$V = \left\{ \begin{bmatrix} \vec{x}_1 \\ \vec{x}_2 \end{bmatrix} \in \mathbb{Z}^{m_1+m_2} \mid U_1\vec{x}_1 = U_2\vec{x}_2 \right\},$$

  and S' be the set

$$S' = \{\vec{x}_1 \in \mathbb{Z}^{n_1} \mid \vec{x}_1 \in S'_1 \wedge (\exists \vec{x}_2 \in S'_2)(\begin{bmatrix} \vec{x}_1 \\ \vec{x}_2 \end{bmatrix} \in V)\}.$$

  According to Lemma 41, V is r-definable. It follows that the set S' is also r-definable. Since $S_1 \cap S_2 = U_1 S'$, the set $S_1 \cap S_2$ is r-definable.
- *$S_1 \times S_2$ is r-definable.* There exist $m_1, m_2 \in \mathbb{N}_0$, $U_1 \in \mathbb{C}^{n_1 \times m_1}$, $U_2 \in \mathbb{C}^{n_1 \times m_2}$, $S'_1 \subseteq \mathbb{Z}^{m_1}$ and $S'_2 \subseteq \mathbb{Z}^{m_2}$ such that S'_1 and S'_2 are r-definable, $S_1 = U_1 S'_1$, and $S_2 = U_2 S'_2$. Since $S_1 \times S_2 = \mathrm{diag}(U_1, U_2)(S'_1 \times S'_2)$, the set $S_1 \times S_2$ is r-definable.
- *$V = \{(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_{n_1}) \mid (x_1, \ldots, x_{n_1}) \in S_1\}$ is r-definable.* There exist $m \in \mathbb{N}_0$, $U \in \mathbb{C}^{n_1 \times m}$ and $S' \subseteq \mathbb{Z}^m$ such that S' is r-definable and $S_1 = US'$. Let $U' \in \mathbb{C}^{(n_1-1) \times m}$ be the matrix obtained by removing the k-th row from U. We have $V = U'S'$, hence V is r-definable.

- $\left\{ \begin{bmatrix} \vec{x} \\ \Re(\vec{x}) \\ \Im(\vec{x}) \end{bmatrix} \mid \vec{x} \in S_1 \right\}$ *is r-definable.* There exist $m \in \mathbb{N}_0$, $U \in \mathbb{C}^{n_1 \times m}$ and $S' \subseteq \mathbb{Z}^m$ such that S' is r-definable and $S_1 = US'$. Since

$$\left\{ \begin{bmatrix} \vec{x} \\ \Re(\vec{x}) \\ \Im(\vec{x}) \end{bmatrix} \mid \vec{x} \in S_1 \right\} = \begin{bmatrix} U \\ \Re(U) \\ \Im(U) \end{bmatrix} S',$$

  this set is r-definable.
- *expand*(S_1, r^q) *is r-definable.* There exist $m \in \mathbb{N}_0$, $U \in \mathbb{C}^{n_1 \times m}$ and $S' \subseteq \mathbb{Z}^m$ such that S' is r-definable and $S_1 = US'$. Let L be the language $E_r(S')$ of the synchronous encodings in base r of the vectors in S', expressed over the alphabet $\{0, \ldots, r-1\}^m$. Since S' is r-definable, L is regular.

  The language $L' = L \cdot ((0^m)^q)^*$ is thus also regular. It follows that the set $S'' \subseteq Z^m$ encoded by L' is r-definable. Since this set obeys

$$S'' = \{r^{qk}\vec{x} \mid \vec{x} \in S' \wedge k \in \mathbb{N}\},$$

  we have $US'' = \text{expand}(S_1, r^q)$, from which it follows that expand(S_1, r^q) is r-definable.

□

Theorem 10 *Let $r \in \mathbb{N}$ with $r > 1$, and $a, b, c \in \mathbb{Z}$ with $a \neq 0$. The set*

$$S = \{ak^2 + bk + c \mid k \in \mathbb{N}\}$$

is not r-definable.

PROOF. The proof is by contradiction. Suppose that the set $S = \{ak^2+bk+c \mid k \in \mathbb{N}\}$ is r-definable. This implies that $-S = \{-x \mid x \in S\}$ is r-definable as well. Therefore, we may assume that $a \geq 1$. Let P be the characteristic predicate of S:

$$P(y) \equiv (\exists k \in \mathbb{N})(y = ak^2 + bk + c).$$

Since S is r-definable, P is definable in $\langle \mathbb{Z}, \leq, +, V_r \rangle$. Let $n \in \mathbb{N}$ be greater than $-b/2a$, and $F(x, y)$ be the predicate

$$F(x, y) \equiv y = ax^2 + bx + c \wedge x \geq n.$$

This predicate is definable in $\langle \mathbb{Z}, \leq, +, V_r \rangle$:

$$\begin{aligned} F(x,y) \equiv\, & P(y) \wedge P(y + 2ax + a + b) \wedge x \geq n \\ & \wedge (\forall z)(\neg P(z) \vee z \leq y \vee z \geq y + 2ax + a + b). \end{aligned}$$

Indeed, $f(x) = ax^2 + bx + c$ is strictly increasing for $x \geq n$, and the second line of the expression of $F(x,y)$ states that y and $y + 2ax + a + b$ are two consecutive values $f(z)$ and $f(z+1)$ of the function f. Resolving

$$\begin{cases} y & = az^2 + bz + c \\ y + 2ax + a + b & = a(z+1)^2 + b(z+1) + c \end{cases}$$

yields $x = z$, hence $y = f(x)$. Now, let $M(x,y,z)$ be the predicate

$$M(x,y,z) \equiv x \geq 0 \wedge y \geq 0 \wedge z = xy.$$

This predicate is definable in $\langle \mathbb{Z}, \leq, +, V_r \rangle$:

$$\begin{aligned} M(x,y,z) \equiv\, & (\exists z_1,\, z_2,\, z_3,\, z_4)(F(x + y + n,\, z_1) \\ & \wedge F(x + n,\, z_2) \wedge F(y + n,\, z_3) \wedge F(n,\, z_4) \\ & \wedge 2az = z_1 - z_2 - z_3 + z_4). \end{aligned} \tag{4}$$

Indeed,

$$\begin{aligned} z_1 &= a(x + y + n)^2 + b(x + y + n) + c \\ z_2 &= a(x + n)^2 + b(x + n) + c \\ z_3 &= a(y + n)^2 + b(y + n) + c \\ z_4 &= an^2 + bn + c \end{aligned}$$

implies $z_1 - z_2 - z_3 + z_4 = 2axy$. From Equation (4), it follows that the first-order theory $\langle \mathbb{N}, +, . \rangle$ is a subset of the theory $\langle \mathbb{Z}, \leq, +, V_r \rangle$. This is clearly a contradiction, since the latter is decidable [29] and the former is not [12]. □

In order to prove Theorem 11, we need to establish the following result.

Theorem 42 *Let $r \in \mathbb{N}$ with $r > 1$, and $p, q \in \mathbb{Z}$ with $p \neq 0$. The set*

$$S = \left\{ \begin{bmatrix} (pj + q)k \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \right\}$$

is not r-definable.

PROOF. The proof is by contradiction. Suppose that S is r-definable. Let P be the characteristic predicate of S:

$$P(y,x) \equiv (\exists k \in \mathbb{N})(y = k(px+q)).$$

Since S is r-definable, P is definable in $\langle \mathbb{Z}, \leq, +, V_r \rangle$. The predicate $D(y,x)$ over $\mathbb{Z}^2$ which is true if and only if y is different from 0 and is divisible by $px+q$ is straightforwardly defined in terms of P:

$$D(y,x) \equiv y \neq 0 \ \wedge \ (P(y,x) \ \vee \ P(-y,x))$$

For every $x \in \mathbb{Z}$, we have $\gcd(px+q, p(x+1)+q) = \gcd(p, px+q) = \gcd(p,q)$, from which we deduce

$$\mathrm{lcm}(px+q, p(x+1)+q) = \frac{1}{\gcd(p,q)}(px+q)(p(x+1)+q).$$

If a number can be divided by two others, then it can be divided by their least common multiple. Therefore, for every y verifying

$$D(y,x) \ \wedge \ D(y,x+1), \tag{5}$$

there exists $k \in \mathbb{Z}$ such that

$$y = \frac{k}{\gcd(p,q)}(px+q)(p(x+1)+q).$$

Moreover, if we have $x > |q/p| + 1$, then the integer y verifying Equation (5) that has the smallest magnitude corresponds to $k = 1$. From this argument, it follows that the predicate

$$\begin{aligned} Q(y,x) \equiv x > \left|\frac{q}{p}\right| + 1 \ \wedge \ D(y,x) \ \wedge \ D(y,x+1) \ \wedge \\ (\forall z)(|z| \geq |y| \ \vee \ \neg D(z,x) \ \vee \ \neg D(z,x+1)), \end{aligned}$$

which is definable in $\langle \mathbb{Z}, \leq, +, V_r \rangle$, is such that

$$Q(y,x) \ \equiv \ x > \left|\frac{q}{p}\right| + 1 \ \wedge \ y = \frac{1}{\gcd(p,q)}(px+q)(p(x+1)+q).$$

Let $l \in \mathbb{N}$ be such that $l > |q/p| + 1$, and $R(y)$ be the predicate

$$R(y) \equiv (\exists x, z)(y = \gcd(p, q).z \wedge x \geq 0 \wedge Q(z, x + l)).$$

This predicate is definable in $\langle \mathbb{Z}, \leq, +, V_r \rangle$, and satisfies

$$R(y) \equiv (\exists k)(k \geq 0 \wedge y = (p(k + l) + q)(p(k + l + 1) + q)).$$

It follows that the set

$$\{(p(k + l) + q)(p(k + l + 1) + q) \mid k \in \mathbb{N}\}$$

is r-definable, which contradicts Theorem 10. $\square$

Theorem 11 *Let $r, p \in \mathbb{N}_0$ with $r > 1$, $\lambda \in \mathbb{C}$ such that $\lambda^p = 1$, and $a, b, c, d \in \mathbb{C}$ with $a \notin \mathbb{R} \setminus \mathbb{Q}$. The set*

$$S = \left\{ \lambda^k \begin{bmatrix} (j + a)(k + b) + c \\ j + d \end{bmatrix} \mid j, k \in \mathbb{N} \right\}$$

is not r-definable.

PROOF. Without loss of generality, we may assume that p is such that $\lambda^i \neq 1$ for every $i \in \{1, 2, \ldots, p - 1\}$. The proof is by contradiction. We suppose that S is r-definable. Let us show that this assumption implies that the set

$$S_0 = \left\{ \begin{bmatrix} (j + a)(k + b) + c \\ j + d \end{bmatrix} \mid j, \frac{k}{p} \in \mathbb{N} \right\}$$

is also r-definable. We have

$$\begin{aligned}(\forall j, k \in \mathbb{N}, 0 \leq k < p)((\exists l \in \mathbb{N})(\lambda^k(j + d) = l + d \wedge l > \lfloor 2|d| \rfloor) \\ \Leftrightarrow k = 0 \wedge j > \lfloor 2|d| \rfloor).\end{aligned}$$

Indeed,

- If there exists $l \in \mathbb{N}$ such that $\lambda^k(j+d) = l + d \wedge l > \lfloor 2|d| \rfloor$, then we have

$$\begin{aligned} & |j+d| = |l+d| \wedge l > \lfloor 2|d| \rfloor \\ \Rightarrow\ & j = l \wedge l > \lfloor 2|d| \rfloor \\ \Rightarrow\ & \lambda^k(j+d) = j + d \wedge j > \lfloor 2|d| \rfloor \\ \Rightarrow\ & k = 0 \wedge j > \lfloor 2|d| \rfloor. \end{aligned}$$

- If $k = 0 \wedge j > \lfloor 2|d| \rfloor$, then, by choosing $l = j$, we get

$$\lambda^k(j+d) = l + d \wedge l > \lfloor 2|d| \rfloor.$$

It follows that $S_0 = S_{01} \cup S_{02}$, with

$$S_{01} = \left\{ \begin{bmatrix} (j+a)(k+b)+c \\ j+d \end{bmatrix} \mid j \in \mathbb{N} \wedge j \leq \lfloor 2|d| \rfloor \wedge \frac{k}{p} \in \mathbb{N} \right\}$$

and

$$S_{02} = \left\{ \begin{bmatrix} (j+a)(k+b)+c \\ j+d \end{bmatrix} \mid j \in \mathbb{N} \wedge \frac{k}{p} \in \mathbb{N} \right.$$
$$\left. \wedge\ (\exists l \in \mathbb{N})(\lambda^k(j+d) = l + d \wedge l > \lfloor 2|d| \rfloor) \right\}.$$

In order to prove that S_0 is r-definable, we show that S_{01} and S_{02} are both r-definable.

- *S_{01} is r-definable.* The set S_{01} is a finite union of sets of the form

$$S_{01j} = \left\{ \begin{bmatrix} (j+a)(k+b)+c \\ j+d \end{bmatrix} \mid \frac{k}{p} \in \mathbb{N} \right\},$$

  with $j \in \mathbb{N}$. Each of those sets is the image of the set $\{k \mid \frac{k}{p} \in \mathbb{N}\}$ by a linear transformation, and is thus r-definable (thanks to Theorem 9).
- *S_{02} is r-definable.* We have

$$\begin{aligned} S_{02} =& \left\{ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in S \mid (\exists l \in \mathbb{N})(x_2 = l + d \wedge l > \lfloor 2|d| \rfloor) \right\} \\ =& S \cap (\pi_1(S) \times \{l + d \mid l \in \mathbb{N} \wedge l > \lfloor 2|d| \rfloor\}), \end{aligned}$$

where $\pi_1(S)$ denotes the projection of S over the first vector component. By Theorem 9, S_{02} is r-definable.

We have thus proved that S_0 is r-definable. Applying Theorem 9, it follows that the following sets are also r-definable:

$$S_0^{(1)} = S_0 - \begin{bmatrix} 0 \\ d \end{bmatrix} = \left\{ \begin{bmatrix} (j+a)(k+b)+c \\ j \end{bmatrix} \mid j, \frac{k}{p} \in \mathbb{N} \right\},$$

$$S_0^{(2)} = \begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix} S_0^{(1)} - \begin{bmatrix} c+ab \\ 0 \end{bmatrix} = \left\{ \begin{bmatrix} (j+a)k \\ j \end{bmatrix} \mid j, \frac{k}{p} \in \mathbb{N} \right\},$$

$$\bigcup_{0 \le i < p} \left(\begin{bmatrix} 1 & i \\ 0 & 1 \end{bmatrix} S_0^{(2)} + \begin{bmatrix} ia \\ 0 \end{bmatrix} \right) = \left\{ \begin{bmatrix} (j+a)k \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \right\}.$$

Let us show that the fact that the last set is r-definable leads to a contradiction. There are two possible cases.

- *If* $a \in \mathbb{Q}$. Let $q \in \mathbb{N}_0$ be such that $qa \in \mathbb{Z}$. The set

$$\left\{ \begin{bmatrix} (qj+qa)k \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \right\}$$

  is r-definable, which contradicts Theorem 42.
- *If* $a \in \mathbb{C} \setminus \mathbb{R}$. Applying Theorem 9, the following sets are r-definable:

$$S_0^{(3)} = \left\{ \begin{bmatrix} (j+a)k \\ \Im((j+a)k) \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \right\} = \left\{ \begin{bmatrix} (j+a)k \\ \Im(a)k \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \right\},$$

$$S_0^{(4)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{\Im(a)} & 0 \\ 0 & 0 & 1 \end{bmatrix} S_0^{(3)} = \left\{ \begin{bmatrix} (j+a)k \\ k \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \right\},$$

$$\begin{bmatrix} 1 & -a & 0 \\ 0 & 0 & 1 \end{bmatrix} S_0^{(4)} = \left\{ \begin{bmatrix} jk \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \right\}.$$

The fact that the last set is r-definable contradicts Theorem 42. $\square$

In order to be able to prove Theorem 12, we need an additional lemma.

Lemma 43 *Let $n, r \in \mathbb{N}_0$ with $r > 1$, $S \subseteq \mathbb{Z}^n$ be r-definable, and $\vec{u} \in \mathbb{C}^n$. If $\{\vec{u} \cdot \vec{x} \mid \vec{x} \in S\}$ is infinite, then there exist $\vec{y}_1, \vec{y}_2 \in \mathbb{Q}^n$ and $m \in \mathbb{N}_0$ such that $\{\vec{y}_1 + r^{mk}\vec{y}_2 \mid k \in \mathbb{N}\} \subseteq S$ and $\vec{u} \cdot \vec{y}_2 \neq 0$.*

PROOF. First, S must be infinite. Since it is r-definable, the language L of the shortest synchronous encodings of its elements in base r is regular. Indeed, this language is denoted by the expression

$$L = E_r(S) \setminus \bigcup_{a \in \{0,r-1\}^n} (a \cdot a \cdot \Sigma^*),$$

where $\Sigma = \{0, 1, \ldots, r-1\}^n$. Hence, there exists a finite-state automaton $\mathcal{A}$ accepting L. Let $|\mathcal{A}|$ denote the number of states of $\mathcal{A}$. Every word $w \in L$ such that $|w| \geq |\mathcal{A}|$ must be accepted by a path of $\mathcal{A}$ that contains at least one cycle, which can be suppressed or further repeated. One can thus decompose w into $w_3 \cdot w_2 \cdot w_1$, with $|w_2| > 0$ and $w_3 \cdot w_2^k \cdot w_1 \in L$ for every $k \in \mathbb{N}$. The language $w_3 \cdot w_2^k \cdot w_1$ encodes a subset S' of S satisfying

$$S' = \{\vec{x}_1 + \sum_{0 \leq i < k} r^{mi}\vec{x}_2 + r^{mk}\vec{x}_3 \mid k \in \mathbb{N}\},$$

with $m = |w_2| \in \mathbb{N}_0$, and $\vec{x}_1, \vec{x}_2, \vec{x}_3 \in \mathbb{Z}^n$. Indeed, $\vec{x}_1$ is the vector encoded by $0^n \cdot w_1$, $\vec{x}_2$ is the vector encoded by $0^n \cdot w_2$ multiplied by $r^{|w_1|}$, and $\vec{x}_3$ is the vector encoded by w_3 multiplied by $r^{|w_1|}$. Note that $\mathcal{A}$ only accepts vector encodings in which the sign digits are not repeated, which implies $r^m\vec{x}_3 + \vec{x}_2 \neq \vec{x}_3$. By defining $\vec{y}_1 = \vec{x}_1 - (1/(r^m - 1))\vec{x}_2$ and $\vec{y}_2 = (1/(r^m - 1))\vec{x}_2 + \vec{x}_3$, we obtain

$$S' = \{\vec{y}_1 + r^{mk}\vec{y}_2 \mid k \in \mathbb{N}\},$$

with $\vec{y}_1, \vec{y}_2 \in \mathbb{Q}^n$ and $\vec{y}_2 \neq \vec{0}$.

It remains to prove that it is always possible to choose $w \in L$ such that the corresponding $\vec{y}_2$ verifies $\vec{u} \cdot \vec{y}_2 \neq 0$. The proof is by contradiction. Suppose that for every $w \in L$ such that $|w| \geq |\mathcal{A}|$, we obtain $\vec{u} \cdot \vec{y}_2 = 0$. By removing one occurrence of the cycle labeled by w_2 from a path of $\mathcal{A}$ accepting w, we obtain $w' = w_3 \cdot w_1 \in L$. Let $\vec{x}$ and $\vec{x}\,'$ be the elements of S respectively encoded by w and w'. We have $\vec{x} = \vec{y}_1 + r^m\vec{y}_2$ and $\vec{x}\,' = \vec{y}_1 + \vec{y}_2$, and therefore $\vec{u} \cdot \vec{x} = \vec{u} \cdot \vec{x}\,'$. One can thus repeat the same operation so as to remove successively all the occurrences of cycles in w, finally obtaining w'' such that $|w''| < |\mathcal{A}|$. The word w'' encodes $\vec{x}\,'' \in S$, with $\vec{u} \cdot \vec{x} = \vec{u} \cdot \vec{x}\,''$. Since there is only a finite set of

w'' such that $|w''| < |\mathcal{A}|$, the set $\{\vec{u} \cdot \vec{x} \mid \vec{x} \in S\}$ is finite, which contradicts an hypothesis of the lemma. $\square$

Theorem 12 *Let $r \in \mathbb{N}$ with $r > 1$, $\lambda \in \mathbb{C}$ such that there do not exist $p \in \mathbb{N}_0$ and $m \in \mathbb{N}$ such that $\lambda^p = r^m$. The set*

$$S = \{\lambda^k \mid k \in \mathbb{N}\}$$

is not r-definable.

PROOF. The proof is by contradiction. Suppose that S is r-definable. There are two possible cases.

- *If S is finite.* Then, there exist $k_1, k_2 \in \mathbb{N}$ such that $k_1 < k_2$ and $\lambda^{k_1} = \lambda^{k_2}$. Choosing $p = k_2 - k_1$ and $m = 0$ leads to a contradiction.
- *If S is infinite.* Since S is r-definable, there exist $n \in \mathbb{N}_0$, $\vec{u} \in \mathbb{C}^n$ and a r-definable set $S' \subseteq \mathbb{Z}^n$ such that $S = \{\vec{u} \cdot \vec{x} \mid \vec{x} \in S'\}$. By Lemma 43, there exist $\vec{y_1}$, $\vec{y_2} \in \mathbb{C}^n$ and $m \in \mathbb{N}_0$ such that

  $$\{\vec{y_1} + r^{mk}\vec{y_2} \mid k \in \mathbb{N}\} \subseteq S',$$

  and $\vec{u} \cdot \vec{y_2} \neq 0$. Let S'' denote the set $\{\vec{y_1} + r^{mk}\vec{y_2} \mid k \in \mathbb{N}\}$. Since $S'' \subseteq S'$, we have

  $$\{\vec{u} \cdot \vec{x} \mid \vec{x} \in S''\} \subseteq \{\lambda^k \mid k \in \mathbb{N}\}.$$

  Let $g = \vec{u} \cdot \vec{y_2}$ and $h = \vec{u} \cdot \vec{y_1}$. We have

  $$\{gr^{mk} + h \mid k \in \mathbb{N}\} \subseteq \{\lambda^k \mid k \in \mathbb{N}\},$$

  with $g \neq 0$. Since the left-hand side of this equation is an unbounded set, it follows that $|\lambda| > 1$. We have

  $$\lim_{k \to \infty} \frac{gr^{m(k+1)} + h}{gr^{mk} + h} = r^m,$$

  which gives

  $$(\forall \varepsilon \in \mathbb{R}_0^+)(\exists k \in \mathbb{N}) \left(\left| \frac{gr^{m(k+1)} + h}{gr^{mk} + h} - r^m \right| < \varepsilon \right),$$

  where $\mathbb{R}_0^+$ denotes the set of strictly positive real numbers. There must exist $p_1, p_2 \in \mathbb{N}$ with $p_1 < p_2$ such that $gr^{mk} + h = \lambda^{p_1}$ and $gr^{m(k+1)} + h = \lambda^{p_2}$. Therefore, by choosing $p = p_2 - p_1$,

  $$(\forall \varepsilon \in \mathbb{R}_0^+)(\exists p \in \mathbb{N})(|\lambda^p - r^m| < \varepsilon).$$

Since $|\lambda| > 1$, there can only be a finite number of integers $p \in \mathbb{N}$ such that $|\lambda^p - r^m| < 1$, and taking $\varepsilon = 1/2^k$, $k = 1, 2, \ldots$ eventually leads to

$$\lambda^p = r^m$$

for some $p \in \mathbb{N}$. This contradicts an hypothesis of the theorem.

□

Before proving Theorem 13, we need to establish two auxiliary results.

Lemma 44 *Let $u, v \in \mathbb{R}$ with $u > 1$, $p, q \in \mathbb{N}_0$ with $p \geq 1$, and $\Pi(x)$ be a polynomial of degree greater than zero with its coefficients in $\mathbb{R}$. We have*

$$\{(u^{pk} + v)^q \mid k \in \mathbb{N}\} \not\subseteq \{u^{k'}\Pi(k') \mid k' \in \mathbb{N}\}.$$

PROOF. The proof is by contradiction. Suppose that we have

$$\{(u^{pk} + v)^q \mid k \in \mathbb{N}\} \subseteq \{u^{k'}\Pi(k') \mid k' \in \mathbb{N}\}.$$

This is equivalent to

$$(\forall k \in \mathbb{N})(\exists k' \in \mathbb{N})((u^{pk} + v)^q = u^{k'}\Pi(k')). \tag{6}$$

For sufficiently large values of k, the left-hand side of this equation is strictly increasing with respect to k. Since Π is a polynomial, that implies that there exists $m > 0$ such that

$$(\forall l_2 > l_1 > m)(\Pi(l_2) > \Pi(l_1) > 0).$$

Let $z = \max_{0 \leq x \leq m} u^x\Pi(x)$, and $n > 0$ be such that $(\forall k \geq n)((u^{pk} + v)^q > z)$. Equation (6) associates a unique $k' \in \mathbb{N}$ to every $k \in \mathbb{N}$ such that $k \geq n$. This k' satisfies $k' = l(k)$, where l is a function $\mathbb{R} \to \mathbb{R}$ verifying

$$(\forall x \in \mathbb{R}, x \geq n)((u^{px} + v)^q = u^{l(x)}\Pi(l(x))). \tag{7}$$

From this equation, we obtain for $x \geq n$

$$\frac{\mathrm{d}}{\mathrm{d}x}\left((u^{px} + v)^q\right) = \frac{\mathrm{d}}{\mathrm{d}l}\left(u^l\Pi(l)\right) . \frac{\mathrm{d}}{\mathrm{d}x}l(x).$$

The left-hand side and the first factor of the right-hand side of this equation being strictly positive for $x \geq n$ (and thus $l \geq m$), the second factor of the

right-hand side is strictly positive as well, from which we deduce that $l(x)$ is strictly increasing for $x \geq n$. Let us compute the derivative $l'(x)$ of $l(x)$ with respect to x. For $x \geq n$, Equation (7) gives

$$(u^{px} + v)^q = u^{l(x)}\Pi(l(x)).$$

Taking the natural logarithm of both sides, we obtain

$$q \log(u^{px} + v) = l(x) \log u + \log \Pi(l(x)).$$

Deriving with respect to x, and defining $\Pi'(x) = \mathrm{d}\Pi(x)/\mathrm{d}x$, we get

$$\frac{pq(\log u)u^{px}}{u^{px} + v} = (\log u)l'(x) + \frac{\Pi'(l(x))l'(x)}{\Pi(l(x))},$$

from which we extract

$$l'(x) = \frac{pq}{1 + \frac{v}{u^{px}}} \cdot \frac{1}{1 + \frac{1}{\log u} \cdot \frac{\Pi'(l(x))}{\Pi(l(x))}}.$$

This result implies that $\lim_{x \to +\infty} l'(x) = pq$, and therefore

$$(\forall \varepsilon > 0)(\exists n' \geq n)(\forall x > n')(pq - \varepsilon < l'(x) < pq + \varepsilon).$$

Let us take $\varepsilon = 1$. There exists $n' \geq n$ such that

$$(\forall x > n')(pq - 1 < l'(x) < pq + 1). \tag{8}$$

For any $k \in \mathbb{N}$ such that $k > n'$, we have

$$l(k+1) = l(k) + \int_k^{k+1} l'(x)\mathrm{d}x,$$

and it follows from Equation (8) that

$$pq - 1 < l(k+1) - l(k) < pq + 1.$$

Note that pq, $l(k)$ and $l(k+1)$ are integer numbers. The only integer number between $pq - 1$ and $pq + 1$ is pq, hence

$$(\forall k > n')(l(k+1) - l(k) = pq),$$

which gives

$$(\forall k > n')(l(k) = l_0 + pqk),$$

with $l_0 \in \mathbb{Z}$. Replacing $l(k)$ by its value in (7), we obtain for any $k > n'$

$$(u^{pk} + v)^q = u^{l_0+pqk}\Pi(l_0 + pqk),$$

hence

$$\Pi(l_0 + pqk) = u^{-l_0}(1 + \frac{v}{u^{pk}})^q.$$

This is clearly impossible, since

$$\lim_{k\to+\infty} \Pi(l_0 + pqk) = +\infty,$$

and

$$\lim_{k\to+\infty} u^{-l_0}(1 + \frac{v}{u^{pk}})^q = u^{-l_0}.$$

□

Theorem 45 *Let $r, l, a, b \in \mathbb{N}$ with $r > 1, l > 1$ and $a \geq 1$, such that $r^a = l^b$. If $\Pi(x)$ is a polynomial of degree greater than zero with its coefficients in $\mathbb{Z}$, then the set*

$$S = \{l^k\Pi(k) \mid k \in \mathbb{N}\}$$

is not r-definable.

PROOF. The proof is by contradiction. Suppose that S is r-definable. After applying Lemma 43 with $\vec{u} = (1)$, we obtain that there exist $m \in \mathbb{N}_0$ and $y_1, y_2 \in \mathbb{Q}$ such that $y_2 \neq 0$ and

$$\{y_1 + r^{mk}y_2 \mid k \in \mathbb{N}\} \subseteq S,$$

which can be rewritten as

$$\{(r^m)^k + \frac{y_1}{y_2} \mid k \in \mathbb{N}\} \subseteq \{l^k\Pi'(k) \mid k \in \mathbb{N}\},$$

where $\Pi'(k) = \Pi(k)/y_2$. This result implies

$$\{(r^m)^{ak} + \frac{y_1}{y_2} \mid k \in \mathbb{N}\} \subseteq \{l^k \Pi'(k) \mid k \in \mathbb{N}\},$$

and thus, since $l^b = r^a$,

$$\left\{ \left((r^{am})^k + \frac{y_1}{y_2} \right)^{bm} \mid k \in \mathbb{N} \right\} \subseteq \{(r^{am})^k \Pi'(k) \mid k \in \mathbb{N}\}.$$

Applying Lemma 44 to this result directly leads to a contradiction. □

We are now ready to prove Theorem 13.

Theorem 13 *Let $r, p, m \in \mathbb{N}_0$ with $r > 1$, $\lambda \in \mathbb{C}$ such that $\lambda^p = r^m$, and $a \in \mathbb{C}$ such that $a \notin \mathbb{R} \setminus \mathbb{Q}$. The set*

$$S = \{\lambda^k (k + a) \mid k \in \mathbb{N}\}$$

is not r-definable.

PROOF. Without loss of generality, we assume that p and m are relatively prime, and that there does not exist $j \in \mathbb{N}_0$ such that $j \geq 2$ and $r^{(1/j)} \in \mathbb{N}$ (thanks to Theorem 6). The proof is by contradiction. Suppose that S is r-definable. There are two possible cases, depending on the value of a. For each of them, we will show that our assumption implies that the set

$$S' = \{\lambda^k (k + a) \mid \frac{k}{p} \in \mathbb{N}\}$$

is r-definable, and that this result leads to a contradiction. For each $k \in \mathbb{N}$, we define $y_k = \lambda^k (k + a)$.

- *If $a \in \mathbb{Q}$.* For each $k \in \mathbb{N}$ such that $k > 2|a|$ and p divides k, we have

  $$\Im(y_k) = 0 \wedge \Re(y_k) > |\lambda|^{\lfloor 2|a| \rfloor} (2|a| + a).$$

  Reciprocally, for each $k \in \mathbb{N}$ such that y_k satisfies the previous formula, we have $k > 2|a|$ and p divides k. It follows that we have $S' = S'_1 \cup S'_2$, with

  $$S'_1 = \{\lambda^k (k + a) \mid \frac{k}{p} \in \mathbb{N}, k \leq 2|a|\},$$

  $$S'_2 = \{y_k \in S \mid \Im(y_k) = 0 \wedge \Re(y_k) > l\},$$

and

$$l = |\lambda|^{\lfloor 2|a| \rfloor}(2|a| + a).$$

The set S'_1 is finite, hence it is r-definable (thanks to Theorem 9). In order to prove that S' is r-definable, it remains to show that S'_2 is r-definable. Let $q \in \mathbb{N}$ be such that $qa \in \mathbb{Z}$. We have

$$S'_2 = S \cap \frac{1}{q}\{x \in \mathbb{N} \mid x > ql\},$$

whose r-definability follows from Theorems 8 and 9. Let us now show that the fact that S' is r-definable leads to a contradiction. We have

$$\begin{aligned} S' &= \{\lambda^k(k+a) \mid \frac{k}{p} \in \mathbb{N}\} \\ &= \{r^{\left(\frac{mk}{p}\right)}(k+a) \mid \frac{k}{p} \in \mathbb{N}\}. \end{aligned}$$

Theorem 9 implies that the set

$$\{r^{\left(\frac{mk}{p}\right)}(qk+qa) \mid \frac{k}{p} \in \mathbb{N}\}$$

is also r-definable, which contradicts Theorem 45.

- *If* $a \in \mathbb{C} \setminus \mathbb{R}$. We can assume without loss of generality that $\Im(a) > 0$. Indeed, Theorem 9 implies that the set

$$\overline{S} = \{\overline{\lambda}^k(k + \overline{a}) \mid k \in \mathbb{N}\},$$

where for every $z \in \mathbb{C}$, $\overline{z}$ denotes the complex conjugate of z, is r-definable if and only if S is r-definable. Let $N \in \mathbb{N}$ be such that $N > 2|a|$ and $0 < \arg(N + a) < \frac{2\pi}{p}$.

· For every $k > N$ such that p divides k, we have

$$\lambda^k = r^{\left(\frac{mk}{p}\right)} \Rightarrow \arg(y_k) = \arg(k+a) \Rightarrow 0 < \arg(y_k) < \frac{2\pi}{p}.$$

· For every $k > N$ such that p does not divide k, we have

$$\arg(y_k) > \frac{2\pi}{p}. \tag{9}$$

Let $M \in \mathbb{N}$ be such that $M > N$ and $M > |\lambda|^N|N + a|$, and let $\alpha = \arg(M + a)$. Note that $0 < \alpha < \frac{\pi}{2}$ (since $M > 2|a|$).

· For every $k > M$ such that p divides k, we have $0 < \arg(y_k) < \alpha \wedge \Im(y_k) > \Im(a)$.

· For every $k > M$ such that p does not divide k, we have $\arg(y_k) > \alpha$ (according to Inequation (9)).

· For every $k \leq M$, we have $\arg(y_k) \geq \alpha \vee \Im(y_k) \leq \Im(a)$. (Indeed, $0 < \arg(y_k) < \alpha \wedge \Im(y_k) > \Im(a)$ implies $k > M$.)

In summary, we have for each $k \in \mathbb{N}$:

$$k > M \wedge p \text{ divides } k \Leftrightarrow 0 < \arg(y_k) < \alpha \wedge \Im(y_k) > \Im(a).$$

It follows that we have $S' = S'_1 \cup S'_2$, with

$$S'_1 = \{\lambda^k(k+a) \mid \frac{k}{p} \in \mathbb{N}, k \leq M\}$$

and

$$S'_2 = \{y_k \in S \mid 0 < \arg(y_k) < \alpha \wedge \Im(y_k) > \Im(a)\}.$$

The set S'_1 is finite, hence it is r-definable (thanks to Theorem 9). In order to prove that S' is r-definable, it remains to show that S'_2 is r-definable. Let us consider the transformation $y_k \to \vec{x}$ such that

$$\vec{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = T \begin{bmatrix} \Re(y_k) \\ \Im(y_k) \end{bmatrix},$$

with

$$T = \begin{bmatrix} 1 & -\frac{\Re(a)}{\Im(a)} \\ 0 & \frac{1}{\Im(a)} \end{bmatrix}.$$

This transformation can be inverted as follows:

$$\begin{bmatrix} \Re(y_k) \\ \Im(y_k) \end{bmatrix} = \begin{bmatrix} 1 & \Re(a) \\ 0 & \Im(a) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

By Theorem 9, the set

$$S''_2 = \left\{ T \begin{bmatrix} \Re(y_k) \\ \Im(y_k) \end{bmatrix} \mid y_k \in S'_2 \right\}$$

is r-definable if and only if S'_2 is r-definable. Note that every $y_k \in S'_2$ is such that

$$T \begin{bmatrix} \Re(y_k) \\ \Im(y_k) \end{bmatrix} = \begin{bmatrix} \lambda^k k \\ \lambda^k \end{bmatrix} \in \mathbb{N}^2.$$

Let S'' be the set

$$S'' = \left\{ T \begin{bmatrix} \Re(y_k) \\ \Im(y_k) \end{bmatrix} \mid y_k \in S \right\}.$$

We thus have $S''_2 \subseteq \mathbb{N}^2$. From the previous results, we deduce

$$\begin{aligned} S''_2 = & \left\{ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in \mathbb{N}^2 \mid 0 < \arg(x_1 + \Re(a)x_2 + i\Im(a)x_2) < \alpha \right. \\ & \qquad \left. \wedge\ \Im(a)x_2 > \Im(a) \right\} \cap S'' \\ = & \left\{ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in \mathbb{N}^2 \mid \frac{\Im(a)x_2}{\Re(a)x_2 + x_1} < \frac{\Im(M+a)}{\Re(M+a)} \wedge x_2 > 1 \right\} \cap S'' \\ = & \left\{ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in \mathbb{N}^2 \mid x_2(\Re(a) + M) < x_2\Re(a) + x_1 \wedge x_2 > 1 \right\} \cap S'' \\ = & \left\{ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in \mathbb{N}^2 \mid x_1 > Mx_2 \wedge x_2 > 1 \right\} \cap S''. \end{aligned}$$

This set is r-definable (thanks to Theorem 9), hence S'_2 and S' are r-definable. Let us now show that the fact that S' is r-definable leads to a contradiction. We have

$$\begin{aligned} S' &= \{\lambda^k(k+a) \mid \frac{k}{p} \in \mathbb{N}\} \\ &= \{r^{(\frac{mk}{p})}(k+a) \mid \frac{k}{p} \in \mathbb{N}\}. \end{aligned}$$

It follows from Theorem 9 that the set

$$\left\{ \Re(x) - \frac{\Re(a)}{\Im(a)}\Im(x) \mid x \in S' \right\} = \left\{ r^{(\frac{mk}{p})}k \mid \frac{k}{p} \in \mathbb{N} \right\}$$

is r-definable, which contradicts Theorem 45.

□

Theorem 14 *Let $r, p, m \in \mathbb{N}_0$ with $r > 1$, and $\lambda \in \mathbb{C}$ such that $\lambda^p = r^m$. The set*

$$S = \left\{ \begin{bmatrix} k \\ \lambda^k \end{bmatrix} \mid k \in \mathbb{N} \right\}$$

is not r-definable.

PROOF. The proof is by contradiction. Without loss of generality, we assume that there does not exist $j \in \mathbb{N}_0$ such that $j \geq 2$ and $r^{(1/j)} \in \mathbb{N}$ (thanks to Theorem 6). Suppose that S is r-definable. According to Theorem 9, the following sets are also r-definable:

$$S \cap \mathbb{N}^2 = \left\{ \begin{bmatrix} pk \\ r^{mk} \end{bmatrix} \mid k \in \mathbb{N} \right\},$$

$$S' = \begin{bmatrix} \frac{1}{p} & 0 \\ 0 & 1 \end{bmatrix} (S \cap \mathbb{N}^2) = \left\{ \begin{bmatrix} k \\ r^{mk} \end{bmatrix} \mid k \in \mathbb{N} \right\}.$$

Let L be the language of the shortest synchronous encodings in base r of the vectors in S', expressed over the alphabet $\{0, 1, \ldots, r-1\}^2$. Since S' is r-definable, L is regular. Let $\mathcal{A}$ be a finite-state automaton accepting L. Any $w \in L$ is of the form

$$w = (0,0) \cdot (0,1) \cdot w_1 \cdot w_2,$$

where w_1 is equal to the empty word if $k = 0$ or to $(0,0)^{mk - \lfloor \log_r k \rfloor - 1}$ if $k \in \mathbb{N}_0$, and w_2 is such that $(0,0) \cdot w_2$ is the shortest encoding of $k\vec{e}_1$ in base r. For any sufficiently long word w in L, the path of $\mathcal{A}$ that accepts w must encounter an occurrence of a cycle while reading w_1. This cycle can be further iterated, accepting words that do not belong to L. Hence the contradiction. □

The proof of Theorem 15 requires three additional results.

Lemma 46 *Let $r, m, p \in \mathbb{N}_0$ with $r > 1$, $\lambda \in \mathbb{C}$ such that $\lambda^p = r^m$, and $a \in \mathbb{C}$. The set*

$$\left\{ \begin{bmatrix} \lambda^k j \\ \lambda^k (j + a) \end{bmatrix} \mid j, k \in \mathbb{N} \right\}$$

is r-definable.

PROOF. We have

$$S = \bigcup_{0 \leq i < p} \left\{ \lambda^i \begin{bmatrix} \lambda^k j \\ \lambda^k (j + a) \end{bmatrix} \mid j, \frac{k}{p} \in \mathbb{N} \right\}.$$

It is thus sufficient to prove that the set

$$S' = \left\{ \begin{bmatrix} \lambda^k j \\ \lambda^k (j+a) \end{bmatrix} \mid j, \frac{k}{p} \in \mathbb{N} \right\}$$

is r-definable. We have

$$S' = \left\{ r^{mk} \begin{bmatrix} j \\ j+a \end{bmatrix} \mid j, k \in \mathbb{N} \right\}.$$

The set $\mathbb{N}$ is r-definable, thus by Theorem 9, the set

$$S'' = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \mathbb{N} + \begin{bmatrix} 0 \\ a \end{bmatrix} = \left\{ \begin{bmatrix} j \\ j+a \end{bmatrix} \mid j \in \mathbb{N} \right\}$$

is r-definable. Since $S' = \text{expand}(S'', r^m)$, it follows from the same theorem that S' is r-definable. $\square$

Theorem 47 *Let $r, m \in \mathbb{N}_0$ with $r > 1$, and $p, q \in \mathbb{Z}$ with $p \neq 0$. The set*

$$S = \left\{ \begin{bmatrix} r^{mk}(pj+q) \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \right\}$$

is not r-definable.

PROOF. The proof is by contradiction. Suppose that S is r-definable. From Theorem 9, it follows that the set

$$S' = \left\{ \begin{bmatrix} r^{mk}(pj+q) \\ pj+q \end{bmatrix} \mid j, k \in \mathbb{N} \right\}$$

is also r-definable. Let L be the language of the shortest synchronous encodings in base r of the vectors in S', expressed as a set of pairs (w_1, w_2) of words of same length over the alphabet $\{0, \ldots, r-1\}^*$. Let f be the function

$$f : \mathbb{Z} \to \mathbb{Z} : x \mapsto \frac{x}{V_r(x)}.$$

Intuitively, $f(x)$ is the number obtained by removing all the trailing "0" digits from the encoding of x in base r. The value of $f(x)$ stays unchanged when x is multiplied by r. It follows that we have

$$(\forall \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in S')(f(x_1) = f(x_2)). \tag{10}$$

For any $l \in \mathbb{N}$, let us define

$$y_l = \begin{cases} p(r^l + 1) \text{ if } q = 0, \\ p(r^l) + q \text{ if } q \neq 0. \end{cases}$$

Note that $V_r(y_l)$ stays bounded with respect to l (in other words, the number of trailing "0" digits of y_l encoded in base r stays bounded when l increases). Let $n \in \mathbb{N}_0$ be such that $r^n > V_r(y_l)$ for every $l \in \mathbb{N}$, and such that n is greater than the length of the shortest synchronous encodings of p and of q in base r. Let $\mathcal{A}$ be a finite-state automaton accepting L. There exists $l \in \mathbb{N}$ such that the shortest synchronous encoding of y_l in base r has more than $|\mathcal{A}| + n$ symbols, where $|\mathcal{A}|$ denotes the number of states of $\mathcal{A}$. Let us take $k \in \mathbb{N}$ such that mk is greater than the length of the shortest synchronous encoding of y_l in base r. We know that the vector

$$\begin{bmatrix} r^{mk} y_l \\ y_l \end{bmatrix}$$

belongs to S'. Therefore, its shortest synchronous encoding (w_1, w_2) in base r, expressed as a pair of same-length words, belongs to L, and is thus accepted by $\mathcal{A}$. This encoding can be decomposed into $(w_1 \cdot w_1' \cdot w_1'', w_2 \cdot w_2' \cdot w_2'')$, with $|w_1'| = |w_2'| = |\mathcal{A}|$ and $|w_1''| = |w_2''| = n$. It follows that w_1' and w_2' only contain the symbol 0. Any subpath of A accepting (w_1', w_2') must contain a cycle that can be iterated one more time. This allows to transform a path accepting (w_1, w_2) into one accepting a different word (u_1, u_2), from which it follows that $(u_1, u_2) \in L$. By construction, w_1 and u_1 differ only by their number of trailing "0" digits, whereas u_2 and w_2 have the same number of trailing "0" digits and encode different integers. Let x_1 and x_2 be the integers encoded by u_1 and u_2. From the previous results, it follows that $f(x_1) = f(y_l)$ and $f(x_2) \neq f(y_l)$, and therefore that $f(x_1) \neq f(x_2)$. This contradicts Equation (10). Hence, S is not r-definable. □

Lemma 48 *Let $r, p, m \in \mathbb{N}_0$ with $r > 1$, $\lambda \in \mathbb{C}$ such that $\lambda^p = r^m$, and $a \in \mathbb{C}$. There exists $N \in \mathbb{N}$ such that for all $k_1, k_2, j_1, j_2 \in \mathbb{N}$ with $j_1 > N$ and $j_2 > N$,*

we have

$$\lambda^{k_1}(j_1 + a) = \lambda^{k_2}(j_2 + a) \Leftrightarrow \lambda^{k_1} = \lambda^{k_2} \wedge j_1 = j_2.$$

PROOF. That the right-hand side of the equivalence implies the left-hand one is immediate. Besides, if $\lambda^{k_1} = \lambda^{k_2}$, then

$$\lambda^{k_1}(j_1 + a) = \lambda^{k_2}(j_2 + a)$$

reduces to $j_1 = j_2$ and the proposition hence holds for any value of N. Moreover, the proposition is symmetrical in (k_1, j_1) and (k_2, j_2). It is therefore sufficient to prove that there exists $N \in \mathbb{N}$ such that for all $k_1, k_2, j_1, j_2 \in \mathbb{N}$ satisfying $k_1 > k_2$ and $j_1 > N$, the equation

$$\lambda^{k_1}(j_1 + a) = \lambda^{k_2}(j_2 + a) \tag{11}$$

does not hold.

Let $\mu = \lambda^{k_1 - k_2}$ and $\alpha = \arg(\mu)$. From the hypotheses on λ, we have $|\mu| > 0$ and $\alpha \in \{j2\pi/p \mid -p/2 \leq j \leq p/2 \wedge j \neq 0\}$. We distinguish two cases.

- *If* $|\alpha| = \pi$. Then, $\mu = -|\mu|$ and Equation 11 reduces to

  $$-|\mu|(j_1 + a) = j_2 + a,$$

  which yields

  $$j_1 = -\frac{j_2}{|\mu|} - \frac{a}{|\mu|} - a \leq 2|a|.$$

  Choosing $N = \lceil 2|a| \rceil$ thus makes Equation 11 unsatisfiable.
- *If* $|\alpha| < \pi$. Taking the imaginary part of each side of 11, one gets

  $$|\mu| \sin\alpha(j_1 + \Re(a)) + |\mu| \cos\alpha \Im(a) = \Im(a),$$

  which gives

  $$j_1 = \frac{\Im(a)}{|\mu| \sin\alpha} - \Im(a) \cot\alpha - \Re(a).$$

  The largest possible values of $|\sin\alpha|$ and $|\cot\alpha|$ are obtained with a value of α equal to $\beta = \lfloor (p-1)/2 \rfloor 2\pi/p$. Therefore,

  $$j_1 \leq \left(\frac{1}{|\sin\beta|} + |\cot\beta| \right) |\Im(a)| + |\Re(a)|.$$

Equation 11 is thus unsatisfiable for values of N at least equal to the right-hand side of this inequality. $\square$

We are now ready to prove Theorem 15.

Theorem 15 *Let $r, p, m \in \mathbb{N}_0$ with $r > 1$, $\lambda \in \mathbb{C}$ such that $\lambda^p = r^m$, and $a \in \mathbb{C}$. The set*

$$S = \left\{ \begin{bmatrix} \lambda^k(j+a) \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \right\}$$

is not r-definable.

PROOF. Without loss of generality, we assume that p and m are relatively prime, and that there does not exist $j \in \mathbb{N}_0$ such that $j \geq 2$ and $r^{(1/j)} \in \mathbb{N}$ (thanks to Theorem 6). The proof is by contradiction. Suppose that S is r-definable. By Lemma 48, there exists $N \in \mathbb{N}$ such that for all $k_1, k_2, j_1, j_2 \in \mathbb{N}$ with $j_1 > N$ and $j_2 > N$, we have

$$\lambda^{k_1}(j_1 + a) = \lambda^{k_2}(j_2 + a) \Leftrightarrow \lambda^{k_1} = \lambda^{k_2} \wedge j_1 = j_2. \tag{12}$$

With respect to such an integer N, the following set is r-definable:

$$S = \left\{ \begin{bmatrix} \lambda^k(j+a) \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \wedge j > N \right\}.$$

Applying Theorem 9, Lemma 46 and Equation 12, we obtain that the following sets are r-definable :

$$\left\{ \begin{bmatrix} \lambda^k(j+a) \\ \lambda^k j \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \wedge j > N \right\},$$

$$\left\{ \begin{bmatrix} \lambda^k j \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \wedge j > N \right\},$$

$$S' = \left\{ \begin{bmatrix} \lambda^k j \\ j \end{bmatrix} \mid j,k \in \mathbb{N} \wedge j > N \right\} \cap \mathbb{N}^2$$
$$= \left\{ \begin{bmatrix} r^{mk} j \\ j \end{bmatrix} \mid j,k \in \mathbb{N} \wedge j > N \right\}.$$

For each $j \in \mathbb{N}$, the set

$$S_j = \left\{ \begin{bmatrix} r^{mk} j \\ j \end{bmatrix} \mid k \in \mathbb{N} \right\} = \text{expand}(\{j\}, r^m) \times \{j\}$$

is r-definable thanks to Theorem 9.

The set

$$S' \cup \bigcup_{0 \le j \le N} S_j = \left\{ \begin{bmatrix} r^{mk} j \\ j \end{bmatrix} \mid j,k \in \mathbb{N} \right\}$$

is therefore r-definable, which contradicts Theorem 47. It follows that S is not r-definable. $\square$

Theorem 16 *Let $r, p_1, p_2, m_1, m_2 \in \mathbb{N}_0$ with $r > 1$, $\lambda_1, \lambda_2 \in \mathbb{C}$ such that $\lambda_1^{p_1} = r^{m_1}$, $\lambda_2^{p_2} = r^{m_2}$ and $|\lambda_1| \neq |\lambda_2|$. The set*

$$S = \left\{ \begin{bmatrix} \lambda_1^k \\ \lambda_2^k \end{bmatrix} \mid k \in \mathbb{N} \right\}$$

is not r-definable.

PROOF. Without loss of generality, we can assume that m_i and p_i are relatively prime for $i \in \{1,2\}$, that $m_1 < m_2$, and that there does not exist $j \in \mathbb{N}_0$ such that $j \geq 2$ and $r^{(1/j)} \in \mathbb{N}$ (thanks to Theorem 6). The proof is by contradiction. Suppose that S is r-definable. Theorem 9 implies that the set

$$S' = S \cap \mathbb{N}^2 = \left\{ \begin{bmatrix} r^{m_1 k} \\ r^{m_2 k} \end{bmatrix} \mid k \in \mathbb{N} \right\}$$

is r-definable as well. Let L be the language of the shortest encodings in base r of the vectors in S, expressed over the alphabet $\{0, 1, \ldots, r-1\}^2$. This language is of the form

$$L = \{(0,0) \cdot (0,1) \cdot (0,0)^{k(m_2-m_1)-1} \cdot (1,0) \cdot (0,0)^{km_1} \mid k \in \mathbb{N}\}.$$

Since L is not regular, S' is not r-definable. It follows that S is not r-definable either. $\square$

Lemma 21 *Let $n, r \in \mathbb{N}_0$ with $n > 1, r > 1$, $\lambda \in \mathbb{C}$ such that $\lambda \neq 1$, $p \in \mathbb{N}_0$, $m \in \mathbb{N}$ such that $\lambda^p = r^m$, $q \in \mathbb{N}$ with $1 < q \leq n$, $V \in \mathbb{C}^{q \times n}$ of rank q, and $\vec{b} \in \mathbb{Z}^n$. There exists a r-definable set $S \subseteq \mathbb{Z}^n$ such that the set*

$$S' = \{J^k_{q,\lambda}\vec{x} + \sum_{0 \leq i < k} J^i_{q,\lambda}\vec{b'} \mid \vec{x} \in VS \wedge k \in \mathbb{N}\},$$

where $\vec{b'} = V\vec{b}$, is not r-definable.

PROOF. Let us project S' onto the two vector components that have the highest index. We obtain

$$S'' = \left\{ \begin{bmatrix} \lambda^k & k\lambda^{k-1} \\ 0 & \lambda^k \end{bmatrix} \vec{x} + \sum_{0 \leq i < k} \begin{bmatrix} \lambda^i & i\lambda^{i-1} \\ 0 & \lambda^i \end{bmatrix} \vec{b''} \mid \vec{x} \in V'S \wedge k \in \mathbb{N} \right\},$$

where $V' \in \mathbb{C}^{2 \times n}$ is composed of the two last rows of V (and is therefore of rank 2), and $\vec{b''} = V'\vec{b}$. It is sufficient to prove that there exists a r-definable set $S \subseteq \mathbb{Z}^n$ such that the corresponding S'' is not r-definable. Let $\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \vec{b''}$. We distinguish four different situations (remark that $\lambda^p = r^m$ implies $|\lambda| \geq 1$).

- *If $|\lambda| = 1$ and $b_2 = 0$.* We have

$$S'' = \left\{ \begin{bmatrix} \lambda^k x_1 + k\lambda^{k-1} x_2 + \frac{\lambda^k - 1}{\lambda - 1} b_1 \\ \lambda^k x_2 \end{bmatrix} \mid \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in V'S \wedge k \in \mathbb{N} \right\}.$$

  Let $\vec{v} \in \mathbb{Z}^n$ be such that the second component of $V'\vec{v}$ is different from zero (such a $\vec{v}$ always exists, otherwise the rank of V' would be less than 2). Choosing $S = \{j\vec{v} \mid j \in \mathbb{N}\}$ yields

$$S'' = \left\{ \begin{bmatrix} \lambda^k j v'_1 + kj\lambda^{k-1} v'_2 + \frac{\lambda^k - 1}{\lambda - 1} b_1 \\ \lambda^k j v'_2 \end{bmatrix} \mid j, k \in \mathbb{N} \right\},$$

with $\begin{bmatrix} v'_1 \\ v'_2 \end{bmatrix} = V'\vec{v}$. If S'' is r-definable, then by Theorem 9 the following sets are also r-definable:

$$S^{(1)} = \begin{bmatrix} 1 & -\frac{v'_1}{v'_2} \\ 0 & \frac{1}{v'_2} \end{bmatrix} \left(S'' + \begin{bmatrix} \frac{b_1}{\lambda-1} \\ 0 \end{bmatrix} \right) = \left\{ \begin{bmatrix} kj\lambda^{k-1}v'_2 + \frac{\lambda^k}{\lambda-1}b_1 \\ \lambda^k j \end{bmatrix} \mid j,k \in \mathbb{N} \right\},$$

$$S^{(2)} = \begin{bmatrix} \frac{\lambda}{v'_2} & 0 \\ 0 & 1 \end{bmatrix} S^{(1)} = \left\{ \lambda^k \begin{bmatrix} kj + \frac{\lambda}{\lambda-1}\frac{b_1}{v'_2} \\ j \end{bmatrix} \mid j,k \in \mathbb{N} \right\},$$

$$\begin{bmatrix} 1 & \frac{\lambda}{\lambda-1}\frac{b_1}{v'_2} \\ 0 & 1 \end{bmatrix} S^{(2)} = \left\{ \lambda^k \begin{bmatrix} j(k + \frac{\lambda}{\lambda-1}\frac{b_1}{v'_2}) + \frac{\lambda}{\lambda-1}\frac{b_1}{v'_2} \\ j \end{bmatrix} \mid j,k \in \mathbb{N} \right\}.$$

By Theorem 11, this last set is not r-definable. It follows that S'' and S' are not r-definable.

- *If* $|\lambda| = 1$ *and* $b_2 \neq 0$. Let us take $S = \{j\vec{b} \mid j \in \mathbb{N}\}$. We obtain

$$S'' = \left\{ \begin{bmatrix} \lambda^k jb_1 + kj\lambda^{k-1}b_2 + \frac{\lambda^k-1}{\lambda-1}b_1 + \frac{(k-1)\lambda^k - k\lambda^{k-1}+1}{(\lambda-1)^2}b_2 \\ \lambda^k jb_2 + \frac{\lambda^k-1}{\lambda-1}b_2 \end{bmatrix} \mid j,k \in \mathbb{N} \right\}$$

If S'' is r-definable, then by Theorem 9 the following sets are also r-definable:

$$S^{(1)} = S'' + \begin{bmatrix} \frac{b_1}{\lambda-1} - \frac{b_2}{(\lambda-1)^2} \\ \frac{b_2}{\lambda-1} \end{bmatrix}$$

$$= \left\{ \lambda^k \begin{bmatrix} jb_1 + \frac{b_2}{\lambda}jk + \frac{1}{\lambda-1}b_1 + \frac{k}{\lambda(\lambda-1)}b_2 - \frac{1}{(\lambda-1)^2}b_2 \\ jb_2 + \frac{1}{\lambda-1}b_2 \end{bmatrix} \mid j,k \in \mathbb{N} \right\},$$

$$S^{(2)} = \begin{bmatrix} \frac{\lambda}{b_2} & 0 \\ 0 & \frac{1}{b_2} \end{bmatrix} S^{(1)}$$

$$= \left\{ \lambda^k \begin{bmatrix} jk + \lambda\frac{b_1}{b_2}j + \frac{\lambda}{\lambda-1}\frac{b_1}{b_2} + \frac{k}{\lambda-1} - \frac{\lambda}{(\lambda-1)^2} \\ j + \frac{1}{\lambda-1} \end{bmatrix} \mid j,k \in \mathbb{N} \right\}$$

$$= \left\{ \lambda^k \begin{bmatrix} (j + \frac{1}{\lambda-1})(k + \lambda\frac{b_1}{b_2}) - \frac{\lambda}{(\lambda-1)^2} \\ j + \frac{1}{\lambda-1} \end{bmatrix} \mid j,k \in \mathbb{N} \right\}.$$

Since we have $\frac{1}{\lambda-1} \notin \mathbb{R} \setminus \mathbb{Q}$, it follows from Theorem 11 that the last set is not r-definable. Therefore, S'' and S' are not r-definable.

- *If* $|\lambda| > 1$ *and* $b_2 = 0$. We have

$$S'' = \left\{ \begin{bmatrix} \lambda^k x_1 + k\lambda^{k-1} x_2 + \frac{\lambda^k - 1}{\lambda - 1} b_1 \\ \lambda^k x_2 \end{bmatrix} \mid \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in V'S \wedge k \in \mathbb{N} \right\}.$$

Let $\vec{v} \in \mathbb{Z}^n$ be such that the second component of $V'\vec{v}$ is different from zero (such a $\vec{v}$ always exists, otherwise the rank of V' would be less than 2). Choosing $S = \{\vec{v}\}$ yields

$$S'' = \left\{ \begin{bmatrix} \lambda^k v_1' + k\lambda^{k-1} v_2' + \frac{\lambda^k - 1}{\lambda - 1} b_1 \\ \lambda^k v_2' \end{bmatrix} \mid k \in \mathbb{N} \right\},$$

with $\begin{bmatrix} v_1' \\ v_2' \end{bmatrix} = V'\vec{v}$. If S'' is r-definable, then by Theorem 9 the following sets are also r-definable:

$$S^{(1)} = \begin{bmatrix} \lambda & \frac{-b_1}{v_2'} \\ 0 & 1 \end{bmatrix} \left(S'' + \begin{bmatrix} \frac{b_1}{\lambda - 1} \\ 0 \end{bmatrix} \right) = \left\{ \lambda^k \begin{bmatrix} k v_2' + \lambda v_1' + \frac{1}{\lambda - 1} b_1 \\ v_2' \end{bmatrix} \mid k \in \mathbb{N} \right\},$$

$$\begin{bmatrix} \frac{1}{v_2'} & -\frac{b_1}{(v_2')^2(\lambda-1)} - \frac{\lambda v_1'}{(v_2')^2} \end{bmatrix} S^{(1)} = \{\lambda^k k \mid k \in \mathbb{N}\}.$$

According to Theorem 13, the last set is not r-definable. It follows that S'' and S' are not r-definable.

- *If* $|\lambda| > 1$ *and* $b_2 \neq 0$. Let us take $S = \{\vec{b}\}$. We obtain

$$S'' = \left\{ \begin{bmatrix} \lambda^k b_1 + \lambda^{k-1} k b_2 + \frac{\lambda^k - 1}{\lambda - 1} b_1 + \frac{(k-1)\lambda^k - k\lambda^{k-1} + 1}{(\lambda - 1)^2} b_2 \\ \lambda^k b_2 + \frac{\lambda^k - 1}{\lambda - 1} b_2 \end{bmatrix} \mid k \in \mathbb{N} \right\}.$$

If S'' is r-definable, then by Theorem 9 the following sets are also r-definable:

$$S^{(1)} = S'' + \begin{bmatrix} \frac{b_1}{\lambda - 1} - \frac{b_2}{(\lambda - 1)^2} \\ \frac{b_2}{\lambda - 1} \end{bmatrix}$$

$$= \left\{ \lambda^k \begin{bmatrix} b_1 + \frac{k}{\lambda} b_2 + \frac{1}{\lambda - 1} b_1 + \frac{k}{\lambda(\lambda - 1)} b_2 - \frac{1}{(\lambda - 1)^2} b_2 \\ b_2 + \frac{1}{\lambda - 1} b_2 \end{bmatrix} \mid k \in \mathbb{N} \right\},$$

$$\begin{bmatrix} \frac{\lambda - 1}{b_2} & \frac{1}{\lambda b_2} - \frac{(\lambda - 1) b_1}{(b_2)^2} \end{bmatrix} S^{(1)} = \{\lambda^k k \mid k \in \mathbb{N}\}.$$

(Note that $|\lambda| > 1$ implies $1 + \frac{1}{\lambda - 1} \neq 0$.) According to Theorem 13, the last set is not r-definable. It follows that S'' and S' are not r-definable.

□

Lemma 22 *Let $n, r \in \mathbb{N}_0$ with $n > 1, r > 1$, $q \in \mathbb{N}$ with $1 < q \leq n$, $V \in \mathbb{Q}^{q \times n}$ of rank q, and $\vec{b} \in \mathbb{Z}^n$. There exists a r-definable set $S \subseteq \mathbb{Z}^n$ such that the set*

$$S' = \{J_{q,1}^k \vec{x} + \sum_{0 \leq i < k} J_{q,1}^i \vec{b'} \mid \vec{x} \in VS \wedge k \in \mathbb{N}\},$$

where $\vec{b'} = V\vec{b}$, is not r-definable.

PROOF. Let us project S' onto the two vector components that have the highest index. We obtain

$$S'' = \left\{ \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \vec{x} + \sum_{0 \leq i < k} \begin{bmatrix} 1 & i \\ 0 & 1 \end{bmatrix} \vec{b''} \mid \vec{x} \in V'S \wedge k \in \mathbb{N} \right\},$$

where $V' \in \mathbb{Q}^{2 \times n}$ is composed of the two last rows of V (and is therefore of rank 2), and $\vec{b''} = V'\vec{b}$. It is sufficient to prove that there exists a r-definable $S \subseteq \mathbb{Z}^n$ such that the corresponding S'' is not r-definable. Let $\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \vec{b''}$. We distinguish two different situations.

- *If $b_2 = 0$.* We have

$$S'' = \left\{ \begin{bmatrix} x_1 + kx_2 + kb_1 \\ x_2 \end{bmatrix} \mid \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in V'S \wedge k \in \mathbb{N} \right\}.$$

  Let $\vec{v} \in \mathbb{Z}^n$ be such that the second component of $V'\vec{v}$ is different from zero (such a $\vec{v}$ always exists, otherwise the rank of V' would be less than 2). Choosing $S = \{j\vec{v} \mid j \in \mathbb{N}\}$ yields

$$S'' = \left\{ \begin{bmatrix} jv'_1 + jkv'_2 + kb_1 \\ jv'_2 \end{bmatrix} \mid j, k \in \mathbb{N} \right\},$$

with $\begin{bmatrix} v'_1 \\ v'_2 \end{bmatrix} = V'\vec{v}$. If S'' is r-definable, then by Theorem 9 the following set is also r-definable:

$$\begin{bmatrix} \frac{1}{v'_2} & -\frac{v'_1}{(v'_2)^2} \\ 0 & \frac{1}{v'_2} \end{bmatrix} S'' = \left\{ \begin{bmatrix} jk + \frac{b_1}{v'_2}k \\ j \end{bmatrix} \mid j, k \in \mathbb{N} \right\}.$$

Since $\frac{b_1}{v'_2} \in \mathbb{Q}$ (because $\vec{v} \in \mathbb{Z}^n$ and $V' \in \mathbb{Q}^{2\times n}$), Theorem 11 implies that this set is not r-definable. It follows that S'' and S' are not r-definable.

- *If $b_2 \neq 0$.* We have

$$S'' = \left\{ \begin{bmatrix} x_1 + kx_2 + kb_1 + \frac{1}{2}k(k-1)b_2 \\ x_2 + kb_2 \end{bmatrix} \mid \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in VS' \wedge k \in \mathbb{N} \right\}.$$

Let $S = \{\vec{0}\}$. We obtain

$$S'' = \left\{ \begin{bmatrix} kb_1 + \frac{1}{2}k(k-1)b_2 \\ kb_2 \end{bmatrix} \mid k \in \mathbb{N} \right\}.$$

If S'' is r-definable, then by Theorem 9 the following sets are also r-definable:

$$S^{(1)} = \begin{bmatrix} 1 & -\frac{b_1}{b_2} \\ 0 & \frac{1}{b_2} \end{bmatrix} S'' = \left\{ \begin{bmatrix} \frac{1}{2}k(k-1)b_2 \\ k \end{bmatrix} \mid k \in \mathbb{N} \right\},$$

$$\begin{bmatrix} \frac{2}{b_2} & 0 \end{bmatrix} S^{(1)} = \{k(k-1) \mid k \in \mathbb{N}\}.$$

By Theorem 10, this last set is not r-definable. It follows that S'' and S' are not r-definable. □

Lemma 23 *Let $n \in \mathbb{N}_0$ and $A \in \mathbb{Z}^{n\times n}$. There exists a nonsingular matrix $U \in \mathbb{C}^{n\times n}$ transforming A into its Jordan form A_J, and such that every row of U^{-1} at the same position as a row of a Jordan block $J_{q,\lambda}$ in A_J contains only rational components provided that λ is rational.*

PROOF. In order for U to transform A into A_J, we must have $A_J = U^{-1}AU$. Let J be a Jordan block in A_J associated to a rational eigenvalue. Without loss of generality, we may assume that J is the first block of A_J. We have

$A_J U^{-1} = U^{-1} A$, which can be decomposed into

$$\begin{bmatrix} J & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} U_1 & U_2 \\ U_3 & U_4 \end{bmatrix} = \begin{bmatrix} U_1 & U_2 \\ U_3 & U_4 \end{bmatrix} A,$$

where $U_1, \ldots, U_4$ are parts of U^{-1} of appropriate sizes. This linear system can be split into the two equations

$$J\,[U_1; U_2] = [U_1; U_2]\,A \tag{13}$$

and

$$X\,[U_3; U_4] = [U_3; U_4]\,A.$$

If U exists, replacing $[U_1; U_2]$ by any solution of (13) whose rows are linearly independent from each other and from the rows of $[U_3; U_4]$ yields a matrix transforming A into A_J. Since all the coefficients of Equation (13) belong to $\mathbb{Q}$, it is always possible to find a suitable rational solution. $\square$

9 Conclusion

In this paper, we have developed general algorithms for deciding whether the closure of a linear transformation preserves the recognizable nature of sets of integer vectors, both with respect to a given single base or to all of them, as well as for computing the effect of iterating such transformations over finite-state representations of sets. It should be noted that these algorithms are expressed in terms of simple integer arithmetic operations and of elementary set transformations, and hence that their applicability is not restricted to finite-state representations of sets. In particular, the decision algorithm and the image computation procedure developed for Presburger-definable sets can easily be applied to the formula-based representations of sets used by symbolic packages such as the Omega library [26]. Besides, as far as finite-state representations are concerned, the results presented here can straightforwardly and naturally be extended to other encoding functions for integer vectors, such as least significant digit first encodings, interleaved schemes, ... [3,17].

We have not studied the worst-case complexity of our algorithms. This is mainly because we expect most of the problems that have been tackled to be computationally as hard as deciding Presburger arithmetic, which is a problem known to be almost intractable from the complexity theoricist's point

of view [24], but for which very satisfactory solutions are available in the real world [26,30]. The algorithms have indeed been implemented in an actual tool [20], and have been shown to be very effective in the context of symbolic state-space exploration of infinite state spaces.

10 Acknowledgments

The author wishes to thank Bernard Willems, Véronique Bruyère, Pierre Wolper, Pierre-Yves Schobbens and Alain Finkel, as well as the anonymous reviewers, for their insightful comments on a preliminary version of this paper. Special thanks go to Sébastien Jodogne for its careful review of the technical sections.

References

[1] A. Aho, J. E. Hopcroft, and J. D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley, 1974.

[2] E. Bodewig. *Matrix Calculus*. Elsevier North-Holland, Amsterdam, second edition edition, 1959.

[3] B. Boigelot. *Symbolic Methods for Exploring Infinite State Spaces*. Collection des publications de la Faculté des Sciences Appliquées de l'Université de Liège, Liège, Belgium, 1999.

[4] B. Boigelot, L. Bronne, and S. Rassart. An improved reachability analysis method for strongly linear hybrid systems. In *Proceedings of the 9th International Conference on Computer-Aided Verification*, number 1254 in Lecture Notes in Computer Science, pages 167–177, Haifa, Israel, June 1997. Springer-Verlag.

[5] B. Boigelot and P. Godefroid. Symbolic verification of communication protocols with infinite state spaces using QDDs. In *Proc. Computer Aided Verification*, volume 1102 of *Lecture Notes in Computer Science*, pages 1–12, New-Brunswick, New-Jersey, July 1996. Springer-Verlag.

[6] B. Boigelot, P. Godefroid, B. Willems, and P. Wolper. The power of QDDs. Submitted for publication, 1997.

[7] A. Bouajjani and P. Habermehl. Symbolic reachability analysis of FIFO channel systems with nonregular sets of configurations. In *Proceedings of ICALP'97*, number 1256 in Lecture Notes in Computer Science, pages 560–570, Bologna, Italy, July 1997. Springer-Verlag.

[8] A. Boudet and H. Comon. Diophantine equations, Presburger arithmetic and finite automata. In *Proceedings of CAAP'96*, number 1059 in Lecture Notes in Computer Science, pages 30–43. Springer-Verlag, 1996.

[9] V. Bruyère. Entiers et automates finis. Mémoire de fin d'études, Université de Mons, 1985.

[10] V. Bruyère, G. Hansel, C. Michaux, and R. Villemaire. Logic and p-recognizable sets of integers. *Bulletin of the Belgian Mathematical Society*, 1(2):191–238, March 1994.

[11] J. R. Büchi. Weak second-order arithmetic and finite automata. *Zeitschrift Math. Logik und Grundlagen der Mathematik*, 6:66–92, 1960.

[12] A. Church. A note on the entscheidungsproblem. *Journal of Symbolic Logic*, 1:40–41, 101–102, 1936.

[13] A. Cobham. On the base-dependence of sets of numbers recognizable by finite automata. *Mathematical Systems Theory*, 3:186–192, 1969.

[14] K.J. Compton and C.W. Henson. A uniform method for proving lower bounds on the computational complexity of logical theories. *Annals of Pure and Applied Logic*, 48:1–79, 1990.

[15] J. Ferrante and C. W. Rackoff. *The Computational Complexity of Logical Theories*, volume 718 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-Heidelberg-New York, 1979.

[16] J. N. Franklin. *Matrix Theory*. Prentice-Hall Series in Applied Mathematics. Prentice-Hall, 1968.

[17] Jesper G. Henriksen, Jakob L. Jensen, Michael E. Jørgensen, Nils Klarlund, Robert Paige, Theis Rauhe, and Anders Sandholm. Mona: Monadic second-order logic in practice. In Ed Brinksma, Rance Cleaveland, Kim Guldstrand Larsen, Tiziana Margaria, and Bernhard Steffen, editors, *Tools and Algorithms for the Construction and Analysis of Systems*, volume 1019 of *Lecture Notes in Computer Science*, pages 89–110. Springer-Verlag, 1995.

[18] J. E. Hopcroft. An $n \log n$ algorithm for minimizing states in a finite automaton. *Theory of Machines and Computation*, pages 189–196, 1971.

[19] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, second edition, 1990.

[20] The Liège Automata-based Symbolic Handler (LASH). Available at `http://www.montefiore.ulg.ac.be/~boigelot/research/lash/`.

[21] R. MacNaughton. Review of [11]. *Journal of Symbolic Logic*, 28:100–102, 1963.

[22] C. Michaux and F. Point. Les ensembles k-reconnaissables sont définissables dans $\langle \mathbb{N}, +, V_k \rangle$. *Comptes Rendus de l'Académie des Sciences de Paris*, 303:939–942, 1986.

[23] C. Michaux and R. Villemaire. Presburger arithmetic and recognizability of sets of natural numbers by automata: New proofs of Cobham's and Semenov's theorems. *Annals of Pure and Applied Logic*, 77(3):251–277, February 1996.

[24] D. C. Oppen. A $2^{2^{2^{pn}}}$ upper bound on the complexity of Presburger arithmetic. *Journal of Computer and System Sciences*, 16:323–332, 1978.

[25] M. Presburger. Über die Volständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. In *Comptes Rendus du Premier Congrès des Mathématiciens des Pays Slaves*, pages 92–101, Warsaw, Poland, 1929.

[26] W. Pugh. The Omega Test: A fast and practical integer programming algorithm for dependence analysis. *Communications of the ACM*, pages 102–114, August 1992.

[27] A. L. Semenov. Presburgerness of predicates regular in two number systems. *Siberian Mathematical Journal*, 18:289–299, 1977.

[28] I. Stewart and D. Tall. *Algebraic Number Theory*. Chapman and Hall Mathematics Series. John Wiley & Sons, New-York, 1979.

[29] R. Villemaire. The theory of $\langle \mathbb{N}, +, V_k, V_l \rangle$ is undecidable. *Theoretical Computer Science*, 106:337–349, 1992.

[30] P. Wolper and B. Boigelot. On the construction of automata from linear arithmetic constraints. In *Proceedings of TACAS*, volume 1785 of *Lecture Notes in Computer Science*, pages 1–19, Berlin, March 2000. Springer-Verlag.