Theoretical Computer Science 409 (2008) 549–556

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

Structural Presburger digit vector automata

Jérôme Leroux *

IRISA (INRIA), VERTECS project, Rennes, France
LaBRI (CNRS), Formal Method Team, Bordeaux, France

A R T I C L E   I N F O

Article history:
Received 17 May 2005
Received in revised form 12 February 2008
Accepted 12 September 2008
Communicated by B. Durand

Keywords:
Automaton
Presburger arithmetic

A B S T R A C T

The least significant digit first decomposition of integer vectors into words of digit vectors provides a natural way for representing sets of integer vectors by automata. In this paper, the minimal automata representing Presburger sets are proved structurally Presburger: automata obtained by moving the initial state and replacing the accepting condition represent Presburger sets.

Presburger arithmetic [17] is a decidable logic used in a large range of applications. Different techniques [8] and tools have been developed for manipulating *the Presburger sets* (the sets of integer vectors satisfying a Presburger formula): by working directly on the Presburger formulas [16], by using semi-linear sets [9,18], or by using automata that recognize sets of integer vectors encoded by strings of digit vectors [19,3]. Presburger formulas and semi-linear sets lack canonicity: there does not exist a natural way to canonically represent a set. As a direct consequence, a set that possesses a simple representation could unfortunately be represented in an unduly complicated way. On the other hand, a minimization procedure for automata provides a canonical representation. That means, a minimization procedure on Presburger automata (automata representing Presburger sets) performs like a simplification algorithm for the Presburger arithmetic.

In this paper we consider the usual least significant digit first decomposition of integer values extended component wise to integer vectors. This decomposition is implemented in tools Fast [4], Lash [11] and CSL-ALV [1]. Note that Lash also implements the most significant digit first decomposition.

Recently, automata transformations that move the initial state or replace the accepting condition have provided interesting applications. First, we have provided a polynomial time algorithm for deciding if an automaton is Presburger by extracting "simple sets" thanks to these automata transformations [13]. Recall that the previous algorithm for deciding this property was given by Muchnik in 1991 [14,15,6], and it works in *quadruple-exponential time*. Second, Bartzis and Bultan [2] provided a *widening operator* for automata in order to enforce the convergence of sequences of increasing sets of integer vectors represented by automata (such a sequence naturally appears during the state space exploration of *infinite state systems*). This operator is obtained by modifying the accepting condition of Presburger automata, but the obtained automata are not proved Presburger. However, from a practical and theoretical point of view, working only with Presburger automata has some advantages. First the manipulation complexity (boolean operations and variable elimination) is at most 3-exponential time for Presburger automata (see [10,13]) and non-elementary for general automata (see [5]). Second, we can compute, in polynomial time, a Presburger formula that defines the set represented by a Presburger automaton, and the computed formula can be exploited in other tools like Omega.

Contribution: In this paper, we introduce a new automata-based representation for sets of integer vectors encoded by the least significant digit first decomposition, called *digit vector automata*. Even if the digit vector automaton representation is

* Corresponding address: IRISA (INRIA), VERTECS project, Rennes, France. Tel.: +33 540003509.
E-mail address: leroux@labri.fr.

0304-3975/$ – see front matter
doi:10.1016/j.tcs.2008.09.037

very similar to other automata-based representations [7,3,6], it is the *first* one that is *canonical* (there exists a unique minimal for the number of states digit vector automaton that represents a given set X), *stable by moving the initial state* (this stability provides a natural way for associating a set of integer vectors to any state), and *stable by modifying the accepting condition*. We prove that minimal digit vector automata representing Presburger sets are structurally Presburger: that means, digit vector automata obtained by modifying the initial state and replacing the accepting condition represent Presburger sets.

Outline: In Section 1 the usual least significant digit first decomposition of integer values is extended to integer vectors. In Section 2 we introduce digit vector automata, a new automata-based representation using the least significant digit first decomposition. In Section 3 the expressiveness of this representation is logically defined. In Section 4 we characterize the sets obtained from (r, m)-digit vector automata by moving the initial state. This characterization is used in Section 5 to prove that sets representable by digit vector automata are represented by a unique (up to isomorphism) minimal for the number of states digit vector automaton. In Section 6 we characterize the sets obtained from (r, m)-digit vector automata by replacing the accepting condition by another one. Finally, in Section 7 we prove that the minimal digit vector automata that represent Presburger sets are structurally Presburger.

1. Least significant digit first decomposition

The usual *least significant digit first decomposition* provides a natural way to associate words of digits to integer values. In this section, we extend this decomposition to integer vectors. Intuitively this extension is obtained component wise. More formally, we denote by $\mathbb{Z}$ and $\mathbb{N}\backslash\{0\}$ respectively the set of integers and the set of non-negative integers. The least significant digit first decomposition is parameterized by an integer $r \geq 2$ called the *basis of decomposition* and an integer $m \geq 1$ called the *dimension*. The set $\Sigma_{r,m} = \Sigma_r^m$ with $\Sigma_r = \{0, \dots, r-1\}$ is called the set of (r, m)-*digit vectors* and the set $S_{r,m} = S_r^m$ with $S_r = \{0, r-1\}$ is called the set of (r, m)-*sign vectors*. An (r, m)-*decomposition* of an integer vector $x \in \mathbb{Z}^m$ is a couple $(\sigma, s) \in \Sigma_{r,m}^* \times S_{r,m}$ such that $x = \rho_{r,m}(\sigma, s)$, where $\rho_{r,m} : \Sigma_{r,m}^* \times S_{r,m} \to \mathbb{Z}^m$ is defined by the following equality for any $b_1, \dots, b_k \in \Sigma_{r,m}$ and for any $s \in S_{r,m}$:

$$\rho_{r,m}(b_1 \dots b_k, s) = r^k \frac{s}{1-r} + \sum_{i=1}^{k} r^{i-1} b_i.$$

Example 1. $(011, 0)$ is a $(2, 1)$-decomposition of $6 = 2^1 + 2^2$.

Example 2. $(\epsilon, 1), (1, 1), (11, 1), \dots, (1 \dots 1, 1)$ are the $(2, 1)$-decompositions of -1 and $(\epsilon, 0), (0, 0), \dots, (0 \dots 0, 0)$ are the $(2, 1)$-decompositions of 0.

Following notations introduced in [12], the function $\rho_{r,m}$ can be expressed thanks to the unique sequence $(\gamma_{r,m,\sigma})_{\sigma \in \Sigma_{r,m}^*}$ of functions $\gamma_{r,m,\sigma} : \mathbb{Z}^m \to \mathbb{Z}^m$ such that $\gamma_{r,m,\sigma_1.\sigma_2} = \gamma_{r,m,\sigma_1} \circ \gamma_{r,m,\sigma_2}$ for $\sigma_1, \sigma_2 \in \Sigma_{r,m}^*$, where $\gamma_{r,m,\epsilon}$ is the identity function, and such that $\gamma_{r,m,b}(x) = rx + b$ for any $(b, x) \in \Sigma_{r,m} \times \mathbb{Z}^m$. In fact, an immediate induction over the length of σ provides the following equality for any (r, m)-decomposition (σ, s):

$$\rho_{r,m}(\sigma, s) = \gamma_{r,m,\sigma}\left(\frac{s}{1-r}\right).$$

Observe that any integer vector in $\mathbb{Z}^m$ has at least one (r, m)-decomposition. Such a decomposition is not unique and the following lemma characterizes the (r, m)-decompositions of the same vector.

Lemma 3. *For any $(\sigma_1, s_1), (\sigma_2, s_2) \in \Sigma_{r,m}^* \times S_{r,m}$ we have $\rho_{r,m}(\sigma_1, s_1) = \rho_{r,m}(\sigma_2, s_2)$ if and only if $s_1 = s_2$ and $\sigma_1 s_1^* \cap \sigma_2 s_2^* \neq \emptyset$.*

Proof. First of all, observe that $\gamma_{r,m,s}(\frac{s}{1-r}) = \frac{s}{1-r}$ and thus $\rho_{r,m}(\sigma s^k, s) = \rho_{r,m}(\sigma, s)$ for any $(\sigma, s) \in \Sigma_{r,m}^* \times S_{r,m}$. Moreover, an immediate induction over $n \in \mathbb{N}$ shows that, for any $n \in \mathbb{N}$, for any $w_1, w_2 \in \Sigma_{r,m}^*$ such that $|w_1| = n = |w_2|$, and for any $s_1, s_2 \in S_{r,m}$ such that $\rho_{r,m}(w_1, s_1) = \rho_{r,m}(w_2, s_2)$, we have $(w_1, s_1) = (w_2, s_2)$. Now, let us consider $(\sigma_1, s_1), (\sigma_2, s_2) \in \Sigma_{r,m}^* \times S_{r,m}$. Assume first that $s_1 = s_2$ and $\sigma_1 s_1^* \cap \sigma_2 s_2^* \neq \emptyset$ and let us prove that $\rho_{r,m}(\sigma_1, s_1) = \rho_{r,m}(\sigma_2, s_2)$. As $\sigma_1 s_1^* \cap \sigma_2 s_2^* \neq \emptyset$, there exists $k_1, k_2 \in \mathbb{N}$ such that $\sigma_1 s_1^{k_1} = \sigma_2 s_2^{k_2}$. With $s_1 = s_2$ we deduce that $(\sigma_1 s_1^{k_1}, s_1) = (\sigma_2 s_2^{k_2}, s_2)$. Thus $\rho_{r,m}(\sigma_1, s_1) = \rho_{r,m}(\sigma_2, s_2)$. Conversely, let us assume that $\rho_{r,m}(\sigma_1, s_1) = \rho_{r,m}(\sigma_2, s_2)$ and let us prove that $s_1 = s_2$ and $\sigma_1 s_1^* \cap \sigma_2 s_2^* \neq \emptyset$. Let us consider $k_1, k_2 \in \mathbb{N}$ such that $|\sigma_1 s_1^{k_1}| = |\sigma_2 s_2^{k_2}|$ and let $w_1 = \sigma_1 s_1^{k_1}$ and $w_2 = \sigma_2 s_2^{k_2}$. From $\rho_{r,m}(\sigma_1, s_1) = \rho_{r,m}(\sigma_2, s_2)$ we get $\rho_{r,m}(w_1, s_1) = \rho_{r,m}(w_2, s_2)$. As $|w_1| = |w_2|$, we deduce that $(w_1, s_1) = (w_2, s_2)$. In particular $s_1 = s_2$ and $\sigma_1 s_1^* \cap \sigma_2 s_2^* \neq \emptyset$. □

2. Digit vector automata

Function $\rho_{r,m}$ provides a natural way to associate the language $\mathcal{L} = \rho_{r,m}^{-1}(X)$ to any set $X \subseteq \mathbb{Z}^m$. Intuitively $\rho_{r,m}^{-1}(X)$ is the language of (r, m)-decompositions of vectors in X. Such a language $\mathcal{L}$ is said to be (r, m)-*saturated*. In this section we introduce a new automata-based representation for recognizing (r, m)-saturated languages stable by moving the initial state.

We first introduce graphs labelled by (r, m)-digit vectors.

Definition 4. An (r, m)-*digit vector graph* is a tuple $G = (Q, \Sigma_{r,m}, \delta)$, where Q is a non-empty finite set of *states* and $\delta : Q \times \Sigma_{r,m} \to Q$ is a *transition function*.

In what follows, with slightly abuse of notation, we denote by $\delta : Q \times \Sigma_{r,m}^* \to Q$ the unique extension of δ satisfying $\delta(q, \epsilon) = q$ and $\delta(q, \sigma_1\sigma_2) = \delta(\delta(q, \sigma_1), \sigma_2)$ for any $q \in Q$ and for any $\sigma_1, \sigma_2 \in \Sigma_{r,m}^*$. A tuple (q, σ, q') such that $q' = \delta(q, \sigma)$ is called a *path*.

Naturally, by equipping an (r, m)-digit vector graph $G = (Q, \Sigma_{r,m}, \delta)$ with an initial state $q \in Q$ and a function $F : Q \to \mathcal{P}(S_{r,m})$ we obtain an automata-based representation for recognizing languages $\mathcal{L} \subseteq \Sigma_{r,m}^* \times S_{r,m}$. Since we are interested in an automata-based representation recognizing (r, m)-saturated languages and stable by moving the initial state, we introduce the following definition that provides a natural restriction on the functions F considered in what follows.

Definition 5. A function $F : Q \to \mathcal{P}(S_{r,m})$ is called an *accepting condition* for an (r, m)-digit vector graph $G = (Q, \Sigma_{r,m}, \delta)$ if the following language is (r, m)-saturated for any state $q \in Q$:

$$\{(\sigma, s) \in \Sigma_{r,m}^* \times S_{r,m} \mid s \in F(\delta(q, \sigma))\}. \tag{1}$$

The following proposition characterizes functions that are accepting conditions for a digit vector graph.

Proposition 6. *A function $F : Q \to \mathcal{P}(S_{r,m})$ is an accepting condition for an (r, m)-digit vector graph $G = (Q, \Sigma_{r,m}, \delta)$ if and only if $F(q_1) \cap \{s\} = F(q_2) \cap \{s\}$ for any path $(q_1, s, q_2) \in Q \times S_{r,m} \times Q$.*

Proof. For any state $q \in Q$ let us consider the language $\mathcal{L}_q = \{(\sigma, s) \in \Sigma_{r,m}^* \times S_{r,m} \mid s \in F(\delta(q, \sigma))\}$.

Assume first that F is an accepting condition for G and let us prove that $F(q_1) \cap \{s\} = F(q_2) \cap \{s\}$ for any path $(q_1, s, q_2) \in Q \times S_{r,m} \times Q$. As F is an accepting condition for G, the language $\mathcal{L}_q$ is (r, m)-saturated for any state $q \in Q$. Therefore, there exists a set $X_q \subseteq \mathbb{Z}^m$ such that $\mathcal{L}_q = \rho_{r,m}^{-1}(X_q)$. Assume first that $s \in F(q_1)$ and let us prove that $s \in F(q_2)$. In this case $(\epsilon, s) \in \rho_{r,m}^{-1}(X_{q_1})$. Since $\rho_{r,m}(s, s) = \rho_{r,m}(\epsilon, s)$ we deduce that $(s, s) \in \rho_{r,m}^{-1}(X_{q_1})$. The path (q_1, s, q_2) shows that $s \in F(q_2)$. Conversely, assume that $s \in F(q_2)$ and let us prove that $s \in F(q_1)$. The path (q_1, s, q_2) proves that $(s, s) \in \rho_{r,m}^{-1}(X_{q_1})$. From $\rho_{r,m}(s, s) = \rho_{r,m}(\epsilon, s)$ we deduce that $(\epsilon, s) \in \rho_{r,m}^{-1}(X_{q_1})$. Thus $s \in F(q_1)$. We have proved that $F(q_1) \cap \{s\} = F(q_2) \cap \{s\}$.

Now, assume that $F(q_1) \cap \{s\} = F(q_2) \cap \{s\}$ for any path $(q_1, s, q_2) \in Q \times S_{r,m} \times Q$ and let us prove that F is an accepting condition for G. An immediate induction shows that $F(q_1) \cap \{s\} = F(q_2) \cap \{s\}$ for any $(q_1, q_2) \in Q \times Q$ such that there exists $k_1, k_2 \in \mathbb{N}$ satisfying $\delta(q_1, s^{k_1}) = \delta(q_2, s^{k_2})$. Given a state $q \in Q$ we denote $X_q = \rho_{r,m}(\mathcal{L}_q)$. As expected, we are going to prove that $\mathcal{L}_q = \rho_{r,m}^{-1}(X_q)$. As $X_q = \rho_{r,m}(\mathcal{L}_q)$ we get the inclusion $\mathcal{L}_q \subseteq \rho_{r,m}^{-1}(X_q)$. For the other inclusion let us consider $(\sigma_1, s_1) \in \rho_{r,m}^{-1}(X_q)$. We deduce that $\rho_{r,m}(\sigma_1, s_1) \in X_q$. Thus there exists $(\sigma_2, s_2) \in \mathcal{L}_q$ such that $\rho_{r,m}(\sigma_1, s_2) = \rho_{r,m}(\sigma_2, s_2)$. This equality implies $s_1 = s_2$ and there exists $k_1, k_2 \in \mathbb{N}$ such that $\sigma_1 s_1^{k_1} = \sigma_2 s_2^{k_2}$. In particular the states $q_1 = \delta(q, \sigma_1)$ and $q_2 = \delta(q, \sigma_2)$ satisfy $\delta(q_1, s_1^{k_1}) = \delta(q_2, s_2^{k_2})$. From $(\sigma_2, s_2) \in \mathcal{L}_q$ we deduce that $s_2 \in F(q_2)$. Thus $s_1 \in F(q_1)$ from the beginning of this paragraph and $s_1 = s_2$. We have proved that $(\sigma_1, s_1) \in \mathcal{L}_q$. Therefore $\mathcal{L}_q = \rho_{r,m}^{-1}(X_q)$. We deduce that $\mathcal{L}_q$ is (r, m)-saturated. $\square$

Definition 7. An (r, m)-*digit vector automaton* is a tuple $\mathcal{A} = (q_0, G, F_0)$ where $G = (Q, \Sigma_{r,m}, \delta)$ is a (r, m)-digit vector graph, $q_0 \in Q$ is the *initial state*, and F_0 is an accepting condition for G.

The set $X = \rho_{r,m}(\{(\sigma, s) \in \Sigma_{r,m}^* \times S_{r,m} \mid s \in F_0(\delta(q_0, \sigma))\})$ is called the set *represented* by the (r, m)-digit vector automaton $\mathcal{A}$.

3. Expressiveness

Recall [6] that a set $X \subseteq \mathbb{Z}^m$ is said to be r-*definable* if it can be denoted by a formula in the first-order theory $\mathrm{FO}(\mathbb{Z}, \mathbb{N}, +, V_r)$, where $V_r : \mathbb{N} \to \mathbb{N}$ is the r-*valuation function* defined by $V_r(0) = 0$ and $V_r(x)$ is the greatest power of r that divides $x \in \mathbb{N}\backslash\{0\}$ (a $(r, 2)$-digit vector automaton that represents V_r is provided in Fig. 1). As expected, in this section we prove that a set $X \subseteq \mathbb{Z}^m$ is representable by an (r, m)-digit vector automaton if and only if it is r-definable.

Note [20] that a *Number Decision Diagram (NDD)* $\mathcal{A}$ in basis r and in dimension m representing a set $X \subseteq \mathbb{Z}^m$ is an automaton over the alphabet $\Sigma_{r,m}$ that recognizes the regular language $\{\sigma s \mid (\sigma, s) \in \rho_{r,m}^{-1}(X)\}$. Recall that a set $X \subseteq \mathbb{Z}^m$ can be represented by an NDD in basis r if and only if it is r-definable [20]. From this result, we deduce the following Corollary 8.

Corollary 8. *A set $X \subseteq \mathbb{Z}^m$ can be represented by an (r, m)-digit vector automaton if and only if X is r-definable.*

Proof. Observe that an NDD in basis r that represents an r-definable set X is computable from an (r, m)-digit vector automaton that represents X, and conversely an (r, m)-digit vector automaton that represents an r-definable set X is computable from an NDD in basis r that represents X. $\square$

We do not consider NDDs in this paper because (1) the class of regular languages included in $\Sigma_{r,m}^* S_{r,m}$ is not stable by residue, which means the automaton obtained by moving the initial state of an NDD is not an NDD any more, and (2) whereas replacing the accepting conditions of digit vector automata by other accepting conditions is structurally obvious, the corresponding operation over NDDs is not immediate.

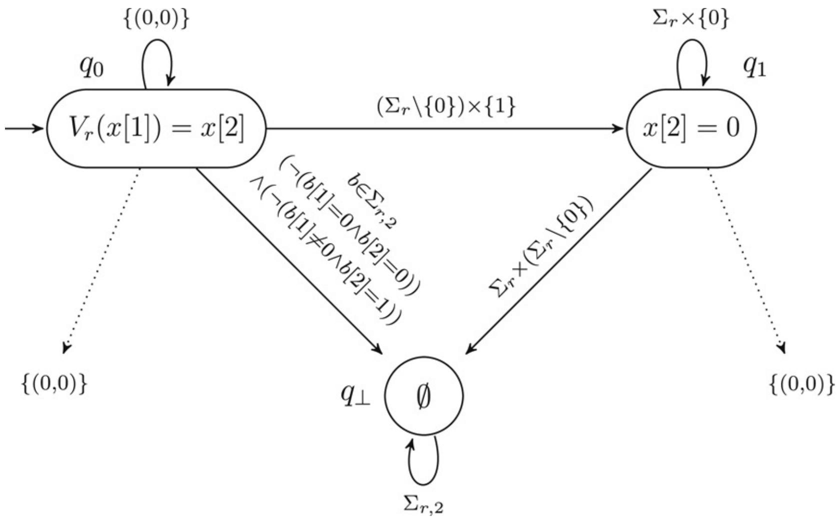

Fig. 1. $\mathcal{A}_{r,2}(\{x \in \mathbb{Z}^2 \mid V_r(x[1]) = x[2]\})$.

4. Moving the initial state

The digit vector automaton obtained from a digit vector automaton $\mathcal{A} = (q_0, G, F_0)$ by replacing the initial state q_0 by another state q is denoted by $\mathcal{A}_q = (q, G, F_0)$. Given a set X implicitly represented by a digit vector automaton $\mathcal{A}$, we denote by X_q the set represented by $\mathcal{A}_q$. Naturally the set X_q is r-definable for any state q. In this section we show that if X is Presburger then X_q is Presburger for any reachable state q from the initial state q_0.

We first geometrically characterize the set X_{q_2} as a function of X_{q_1} for any path $(q_1, w, q_2) \in Q \times \Sigma_{r,m}^* \times Q$.

Proposition 9. *$X_{q_2} = \gamma_{r,m,w}^{-1}(X_{q_1})$ for any path $(q_1, w, q_2) \in Q \times \Sigma_{r,m}^* \times Q$.*

Proof. Consider $x \in \gamma_{r,m,w}^{-1}(X_{q_1})$ and let us prove that $x \in X_{q_2}$. We denote by (σ, s) an (r, m)-decomposition of x. Note that $x_1 = \gamma_{r,m,w}(x)$ is in X_{q_1}. Thus there exists an (r, m)-decomposition (σ_1, s_1) of x_1 such that $s_1 \in F_0(\delta(q_1, \sigma_1))$. As F_0 is an accepting condition, by replacing σ_1 by a word in $\sigma_1 s_1^*$ we can also assume that $|\sigma_1| \geq |w| + |\sigma|$. Now observe that $\gamma_{r,m,w}(x) = \rho_{r,m}(\sigma_1, s_1)$ and $x = \rho_{r,m}(\sigma, s)$ implies $\rho_{r,m}(w\sigma, s) = \rho_{r,m}(\sigma_1, s_1)$. Thus $s = s_1$ and $w\sigma s^* \cap \sigma_1 s_1^* \neq \emptyset$. From $|\sigma_1| \geq |w| + |\sigma|$ and the previous non-empty intersection, there exists $k \in \mathbb{N}$ such that $\sigma_1 = w\sigma s^k$. From $s = s_1$, $s_1 \in F_0(\delta(q_1, \sigma_1))$ and $\delta(q_1, \sigma_1) = \delta(q_1, w\sigma s^k) = \delta(q_2, \sigma s^k)$ we deduce that $s \in F_0(\delta(q_2, \sigma s^k))$. Therefore $\rho_{r,m}(\sigma s^k, s) \in X_{q_2}$. As $\rho_{r,m}(\sigma s^k, s) = \rho_{r,m}(\sigma, s) = x$, we have proved that $x \in X_{q_2}$.

Conversely, let us consider $x \in X_{q_2}$ and let us prove that $x \in \gamma_{r,m,w}^{-1}(X_{q_1})$. From $x \in X_{q_2}$ we deduce that there exists an (r, m)-decomposition (σ, s) of x such that $s \in F_0(\delta(q_2, \sigma))$. As $\delta(q_2, \sigma) = \delta(q_1, w\sigma)$ we deduce that $\rho_{r,m}(w\sigma, s) \in X_{q_1}$. As $\rho_{r,m}(w\sigma, s) = \gamma_{r,m,w}(\rho_{r,m}(\sigma, s))$, we have proved that $\gamma_{r,m,w}(x) \in X_{q_1}$. Therefore $x \in \gamma_{r,m,w}^{-1}(X_{q_1})$. □

We deduce the following Theorem 10.

Theorem 10. *Let X be a Presburger set represented by an (r, m)-digit vector automaton $\mathcal{A} = (q_0, G, q)$. The set X_q is Presburger for any state q reachable from the initial state q_0.*

Proof. Let $\phi(x)$ be a Presburger formula denoting X and consider a path (q_0, σ, F_0). From Proposition 9, we deduce that X_q is denoted by the Presburger formula $\phi(\gamma_{r,m,\sigma}(x))$. Therefore X_q is Presburger. □

5. Minimal digit vector automata

In this section, we prove that any r-definable set $X \subseteq \mathbb{Z}^m$ is represented by a unique (up to isomorphism) minimal for the number of states (r, m)-digit vector automaton denoted by $\mathcal{A}_{r,m}(X)$.

We first associate an (r, m)-digit vector graph $G_{r,m}(X)$ to any r-definable set $X \subseteq \mathbb{Z}^m$. Proposition 9 shows that $Q_{r,m}(X) = \{\gamma_{r,m,\sigma}^{-1}(X) \mid \sigma \in \Sigma_{r,m}^*\}$ is finite. We deduce that $G_{r,m}(X) = (Q_{r,m}(X), \Sigma_{r,m}, \delta_{r,m})$ is an (r, m)-digit vector graph, where $\delta_{r,m}$ is defined by $\delta_{r,m}(Y, b) = \gamma_{r,m,b}^{-1}(Y)$ for any $Y \in Q_{r,m}(X)$ and $b \in \Sigma_{r,m}$.

Definition 11. $G_{r,m}(X)$ is called the *canonical* (r, m)-digit vector graph of X.

As expected, we are going to prove that $\mathcal{A}_{r,m}(X) = (X, G_{r,m}(X), F_{r,m})$ is an (r, m)-digit vector graph that represents X, where $F_{r,m}$ is the function defined by $F_{r,m}(Y) = S_{r,m} \cap ((1 - r)Y)$ for any $Y \in Q_{r,m}(X)$.

Proposition 12. *The tuple $\mathcal{A}_{r,m}(X)$ is an (r, m)-digit vector automaton that represents X.*

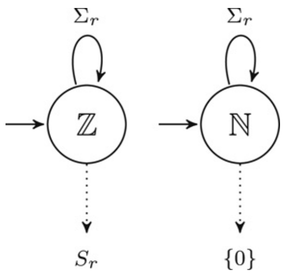

Fig. 2. On the left, $\mathcal{A}_{r,1}(\mathbb{Z})$. On the right, $\mathcal{A}_{r,1}(\mathbb{N})$.

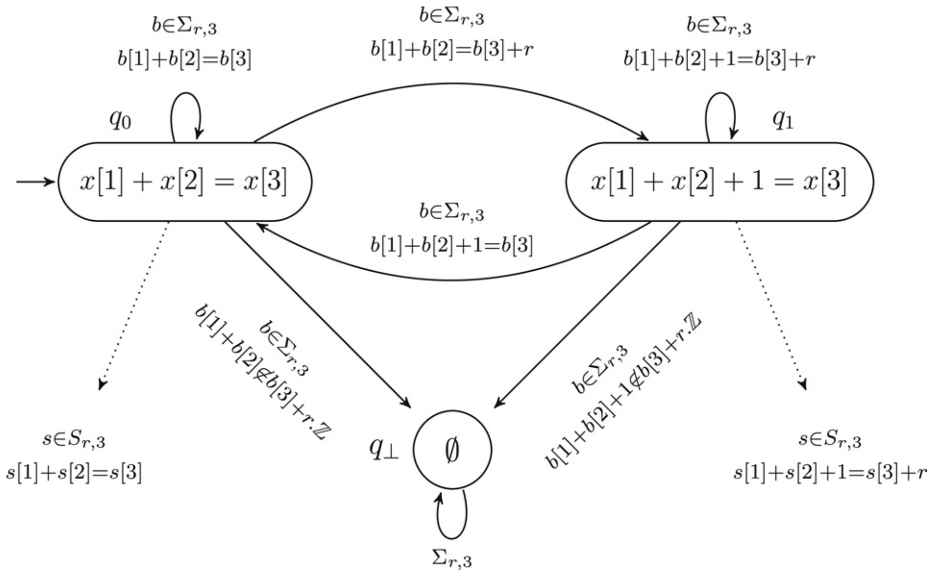

Fig. 3. $\mathcal{A}_{r,3}(\{x \in \mathbb{Z}^3 \mid x[1] + x[2] = x[3]\})$.

Proof. Let us first prove that $F_{r,m}$ is an accepting condition for $G_{r,m}(X)$. It is sufficient to show that $F_{r,m}(Y_1) \cap \{s\} = F_{r,m}(Y_2) \cap \{s\}$ for any path $(Y_1, s, Y_2) \in Q_{r,m}(X) \times S_{r,m} \times Q_{r,m}(X)$. Note that by definition of $G_{r,m}(X)$ we have $Y_2 = \gamma^{-1}_{r,m,s}(Y_1)$. Moreover, by definition of $F_{r,m}$ we get $F_{r,m}(Y_1) = S_{r,m} \cap ((1-r)Y_1)$ and $F_{r,m}(Y_2) = S_{r,m} \cap ((1-r)Y_2)$. As $\gamma_{r,m,s}(\frac{s}{1-r}) = \frac{s}{1-r}$ we deduce that $F_{r,m}(Y_1) \cap \{s\} = F_{r,m}(Y_2) \cap \{s\}$. Thus $F_{r,m}$ is an accepting condition for $G_{r,m}(X)$. We deduce that $\mathcal{A}_{r,m}(X)$ is an (r, m)-digit vector automaton. We denote by X' the set represented by $\mathcal{A}_{r,m}(X)$. As expected, we are going to prove that $X' = X$. Let $x \in X'$ and let us prove that $x \in X$. There exists an (r, m)-decomposition (σ, s) of x such that $s \in F_{r,m}(\delta_{r,m}(X, \sigma))$. Thus $s \in S_{r,m} \cap ((1-r)\gamma^{-1}_{r,m,\sigma}(X))$. We deduce that $\gamma_{r,m,\sigma}(\frac{s}{1-r}) \in X$. As $\gamma_{r,m,\sigma}(\frac{s}{1-r}) = \rho_{r,m}(\sigma, s)$ we have proved that $x \in X$. Conversely, let $x \in X$ and let us prove that $x \in X'$. Let us consider an (r, m)-decomposition (σ, s) of x. As $x = \rho_{r,m}(\sigma, s)$ and $\rho_{r,m}(\sigma, s) = \gamma_{r,m,\sigma}(\frac{s}{1-r})$, we get $s \in S_{r,m} \cap ((1-r)\gamma^{-1}_{r,m,\sigma}(X))$. Therefore $s \in F_{r,m}(\delta_{r,m}(X, \sigma))$ and we deduce $x \in X'$. We have proved that $X = X'$. $\square$

Definition 13. $\mathcal{A}_{r,m}(X)$ is called the *canonical* (r, m)*-digit vector automaton* that represents an r-definable set $X \subseteq \mathbb{Z}^m$.

Example 14. The canonical (r, m)-digit vector automata $\mathcal{A}_{r,2}(V_r)$, $\mathcal{A}_{r,1}(\mathbb{Z})$, $\mathcal{A}_{r,1}(\mathbb{N})$ and $\mathcal{A}_{r,3}(X_+)$ where $X_+ = \{x \in \mathbb{Z}^3 \mid x[1] + x[2] = x[3]\}$ are represented in Figs. 1–3. Observe that states $Y \in Q_{r,m}(X)$ are labelled by formulas denoting Y and we draw dot-edges from Y to a formula denoting $F_{r,m}(Y)$ when this last set is not empty.

The following proposition shows that $\mathcal{A}_{r,m}(X)$ is the unique (up to isomorphism) minimal for the number of states (r, m)-digit vector automaton that represents X.

Proposition 15. *For any r-definable set $X \subseteq \mathbb{Z}^m$, the canonical (r, m)-digit vector automaton $\mathcal{A}_{r,m}(X)$ is the unique (up to isomorphism) minimal for the number of states (r, m)-digit vector automaton that represents X.*

Proof. First of all, observe that Proposition 9 proves that for any (r, m)-digit vector automaton $\mathcal{A} = (q_0, G, F_0)$ that represents X the set of states Q satisfies $|Q| \geq |Q_{r,m}(X)|$. Thus, if $|Q|$ is minimal we have $|Q| = |Q_{r,m}(X)|$. Note that in this case Proposition 9 shows that $\mathcal{A}$ and $\mathcal{A}_{r,m}(X)$ are isomorphic by the bijective function $q \to X_q$. $\square$

6. Replacing the final function

The digit vector automaton obtained from a digit vector automaton $\mathcal{A} = (q_0, G, F_0)$ by replacing the accepting condition F_0 by another accepting condition F for G is denoted by $\mathcal{A}^F = (q_0, G, F)$. Given an r-definable set X implicitly represented by a digit vector automaton $\mathcal{A}$, we denote by X^F the set represented by the digit vector automaton $\mathcal{A}^F$.

Definition 16. A set $X' \subseteq \mathbb{Z}^m$ is said to be (r, m)-*detectable* in an r-definable set $X \subseteq \mathbb{Z}^m$ if for any (r, m)-digit vector automaton $\mathcal{A} = (q_0, G, F_0)$ that represents X there exists an accepting function F for G such that X' is represented by $\mathcal{A}^F$.

In Section 6.1 we characterize the (r, m)-detectability property. Observe that a set $X' \subseteq \mathbb{Z}^m$ that is (r, m)-detectable in an r-definable set $X \subseteq \mathbb{Z}^m$ is r-definable. In Section 6.2 we prove that if X is Presburger then X' is also Presburger.

6.1. Detectable sets

In order to characterize the (r, m)-detectability property, we first prove the following technical lemma.

Lemma 17. *For any r-definable set $X \subseteq \mathbb{Z}^m$ and for any accepting condition F for $G_{r,m}(X)$, the set X' represented by the (r, m)-digit vector automaton $(X, G_{r,m}(X), F)$ satisfies $\gamma^{-1}_{r,m,\sigma_1}(X') = \gamma^{-1}_{r,m,\sigma_2}(X')$ for any words $\sigma_1, \sigma_2 \in \Sigma^*_{r,m}$ such that $\gamma^{-1}_{r,m,\sigma_1}(X) = \gamma^{-1}_{r,m,\sigma_2}(X)$.*

Proof. Let us consider $\sigma_1, \sigma_2 \in \Sigma^*_{r,m}$ such that $\gamma^{-1}_{r,m,\sigma_1}(X) = \gamma^{-1}_{r,m,\sigma_2}(X)$. By construction of $\mathcal{A}_{r,m}(X)$, we deduce that $\delta_{r,m}(X, \sigma_1) = \delta_{r,m}(X, \sigma_2)$. From Proposition 9, as X' is represented by $\mathcal{A}_{r,m}(X)^F$, we deduce that $\gamma^{-1}_{r,m,\sigma_1}(X') = \gamma^{-1}_{r,m,\sigma_2}(X')$. □

Proposition 18. *A set $X' \subseteq \mathbb{Z}^m$ is (r, m)-detectable in an r-definable set $X \subseteq \mathbb{Z}^m$ if and only if $\gamma^{-1}_{r,m,\sigma_1}(X') = \gamma^{-1}_{r,m,\sigma_2}(X')$ for any words $\sigma_1, \sigma_2 \in \Sigma^*_{r,m}$ such that $\gamma^{-1}_{r,m,\sigma_1}(X) = \gamma^{-1}_{r,m,\sigma_2}(X)$.*

Proof. Assume first that X' is (r, m)-detectable in X. Since $\mathcal{A}_{r,m}(X) = (X, G_{r,m}(X), F_{r,m})$ is an (r, m)-digit vector automaton that represents X and X' is (r, m)-detectable in X, there exists an accepting condition F for $G_{r,m}(X)$ such that X' is represented by $(X, G_{r,m}(X), F)$. From Lemma 17 we deduce that $\gamma^{-1}_{r,m,\sigma_1}(X') = \gamma^{-1}_{r,m,\sigma_2}(X')$ for any words $\sigma_1, \sigma_2 \in \Sigma^*_{r,m}$ such that $\gamma^{-1}_{r,m,\sigma_1}(X) = \gamma^{-1}_{r,m,\sigma_2}(X)$. Conversely, assume that X' satisfies $\gamma^{-1}_{r,m,\sigma_1}(X') = \gamma^{-1}_{r,m,\sigma_2}(X')$ for any words $\sigma_1, \sigma_2 \in \Sigma^*_{r,m}$ such that $\gamma^{-1}_{r,m,\sigma_1}(X) = \gamma^{-1}_{r,m,\sigma_2}(X)$. Let us consider an (r, m)-digit vector automaton $\mathcal{A} = (q_0, G, F_0)$ that represents X. Let F be the function defined by $F(q) = \{s \in S_{r,m} \mid \exists \sigma \in \Sigma^*_{r,m} \mid \delta(q_0, \sigma) \in \delta(q, s^*) \wedge \rho_{r,m}(\sigma, s) \in X'\}$.

We first prove that F is an accepting condition for G. Consider a path (q, s, q') with $s \in S_{r,m}$, and let us prove that $s \in F(q)$ if and only if $s \in F(q')$. Assume first that $s \in F(q)$ and let us prove that $s \in F(q')$. As $s \in F(q)$, we deduce that there exists $\sigma \in \Sigma^*_{r,m}$ such that $\delta(q_0, \sigma) \in \delta(q, s^*)$ and $\rho_{r,m}(\sigma, s) \in X'$. Observe that $\delta(q_0, \sigma s) \in \delta(q', s^*)$ and since $\rho_{r,m}(\sigma s, s) = \rho_{r,m}(\sigma, s)$ we deduce that $s \in F(q')$. Now, assume that $s \in F(q')$ and let us prove that $s \in F(q)$. Since $s \in F(q')$ there exists $\sigma \in \Sigma^*_{r,m}$ such that $\delta(q_0, \sigma) \in \delta(q', s^*)$ and $\rho_{r,m}(\sigma, s) \in X'$. We remark that $\delta(q, s) = q'$ and thus $\delta(q', s^*) \subseteq \delta(q, s^*)$. In particular $\delta(q_0, \sigma) \in \delta(q, s^*)$. We deduce that $s \in F(q)$. We have proved that F is an accepting condition for G.

Finally, let us prove that $X' = X^F$. Let $x' \in X'$ and let us prove that $x' \in X^F$. We denote by (σ, s) an (r, m)-decomposition of x'. We have $\rho_{r,m}(\sigma, s) \in X'$. The state $q = \delta(q_0, \sigma)$ satisfies $\delta(q_0, \sigma) \in \delta(q, s^*)$. Thus $s \in F(q)$ and we deduce that $\rho_{r,m}(\sigma, s) \in X^F$. We have proved that $x' \in X^F$. Conversely, let $x' \in X^F$ and let us prove that $x' \in X'$. There exists an (r, m)-decomposition (w, s) of x' such that $s \in F(\delta(q_0, w))$. Using $q = \delta(q_0, w)$, the definition of $F(q)$ shows that there exists $\sigma \in \Sigma^*_{r,m}$ satisfying $\delta(q_0, \sigma) \in \delta(q, s^*)$ and $\rho_{r,m}(\sigma, s) \in X'$. Thus there exists $k \in \mathbb{N}$ such that $\delta(q_0, \sigma) = \delta(q, s^k)$. From $\delta(q_0, \sigma) = \delta(q_0, ws^k)$ and Proposition 9 we deduce that $\gamma^{-1}_{r,m,\sigma}(X) = \gamma^{-1}_{r,m,ws^k}(X)$. We deduce that $\gamma^{-1}_{r,m,\sigma}(X') = \gamma^{-1}_{r,m,ws^k}(X')$. From $\rho_{r,m}(\sigma, s) \in X'$ we deduce that $\frac{s}{1-r} \in \gamma^{-1}_{r,m,\sigma}(X')$. Therefore $\frac{s}{1-r} \in \gamma^{-1}_{r,m,ws^k}(X')$. We deduce that $\rho_{r,m}(ws^k, s) \in X'$. As $\rho_{r,m}(ws^k, s) = x'$ we get $x' \in X'$. We have proved that $X' = X^F$. □

Let us now characterize the sets that are (r, m)-detectable in any r-definable set $X \subseteq \mathbb{Z}^m$. Let $Z_{r,m,s} = \rho_{r,m}(\Sigma^*_{r,m} \times \{s\})$ be the set of vectors $x \in \mathbb{Z}^m$ satisfying the following Presburger formula:

$$\left(\bigwedge_{i \mid s[i]=0} x[i] \geq 0\right) \wedge \left(\bigwedge_{i \mid s[i]=r-1} x[i] < 0\right).$$

Proposition 19. *A set $X' \subseteq \mathbb{Z}^m$ is (r, m)-detectable in any r-definable set $X \subseteq \mathbb{Z}^m$ if and only if there exists $S \subseteq S_{r,m}$ such that $X' = \bigcup_{s \in S} Z_{r,m,s}$.*

Proof. Let us consider $S \subseteq S_{r,m}$ and an (r, m)-digit vector automaton $\mathcal{A} = (q_0, G, F_0)$ that represents an r-definable set X and remark that $\bigcup_{s \in S} Z_{r,m,s}$ is represented by the (r, m)-digit vector automaton $\mathcal{A}^F$, where $F : Q \to \mathcal{P}(S_{r,m})$ is defined by $F(q) = S$ for any $q \in Q$. Therefore $\bigcup_{s \in S} Z_{r,m,s}$ is (r, m)-detectable in any r-definable set $X \subseteq \mathbb{Z}^m$. Conversely, let us consider a set $X' \subseteq \mathbb{Z}^m$ that is (r, m)-detectable in any r-definable set X. Note that $\emptyset$ is represented by the canonical (r, m)-digit vector automaton $\mathcal{A}_{r,m}(\emptyset)$ with the set of states $Q_{r,m}(\emptyset) = \{\emptyset\}$. As X' is (r, m)-detectable in $\emptyset$, we deduce that there exists an accepting condition F such that X' is represented by $\mathcal{A}_{r,m}(\emptyset)^F$. Let $S = F(\emptyset)$ and observe that $X' = \bigcup_{s \in S} Z_{r,m,s}$. □

Remark 20. The set $X_1\#X_2$ is (r, m)-detectable in an r-definable set X for any (r, m)-detectable sets X_1, X_2 in X, and for any $\# \in \{\cup, \cap, \backslash, \Delta\}$.

6.2. Presburger detectable sets

Naturally, if a set $X' \subseteq \mathbb{Z}^m$ is (r, m)-detectable in an r-definable set $X \subseteq \mathbb{Z}^m$, then X' is r-definable. In this section, we show that if X is Presburger then X' is also Presburger.

We first prove the following technical lemma.

Lemma 21. *For any integer $n \geq 1$ there exists an integer $k \geq 1$ such that $r^{k+k} \in r^k + n\mathbb{Z}^m$.*

Proof. Consider the function $h_r : \mathbb{N}\backslash\{0\} \to \mathbb{N}\backslash\{0\}$ defined by $h_r(i) = \frac{i}{\gcd(i,r)}$, where $\gcd(i, r)$ is the *greatest common divisor* of i and r. Since h_r satisfies $0 < h_r(i) \leq i$ for any $i \in \mathbb{N}$, there exists an integer $k \in \mathbb{N}$ such that $h_r^{k+1}(n) = h_r^k(n)$. Let $n' = h_r^k(n)$. Since $h_r(n') = n'$, the integer n' is relatively prime with r. In particular there exists $k' \in \mathbb{N}\backslash\{0\}$ such that $r^{k'} \in 1 + n'\mathbb{Z}$. An immediate induction over $j \in \mathbb{N}$ shows that n divides $r^j h_r^j(n)$ for any $j \in \mathbb{N}$. In particular, n divides $r^k h_r^k(n) = r^k n'$. From $r^{k'} \in 1 + n'\mathbb{Z}$, we get $r^{k'+k} \in r^k + n'r^k\mathbb{Z}$. We have proved that $r^{k'+k} \in r^k + n\mathbb{Z}$. Observe that $k = (1 + k')k + k'$ satisfies $r^{k+k} \in r^k + n\mathbb{Z}$. Thus $r^{k+k} \in r^k + n\mathbb{Z}$. □

Theorem 22. *A set detectable in a Presburger set is Presburger.*

Proof. Consider a set $X' \subseteq \mathbb{Z}^m$ that is (r, m)-detectable in a Presburger set $X \subseteq \mathbb{Z}^m$. A quantification elimination shows that there exists a propositional formula $\mathcal{R}(p_1, \ldots, p_j)$ and a sequence $(\phi_i(x))_{1\leq i\leq j}$ of Presburger formulas of the form $\phi_i(x) := \langle\alpha_i, x\rangle < c_i \wedge x \in a_i + n_i\mathbb{Z}^m$, where $\alpha_i, a_i \in \mathbb{Z}^m$, $c_i \in \mathbb{Z}$ and $n_i \in \mathbb{N}\backslash\{0\}$ such that X is denoted by the Presburger formula $\phi(x) := \mathcal{R}(\ldots, \phi_i(x), \ldots)$. The product $n = n_1 \ldots n_j$ and Lemma 21 proves that there exists an integer $k \geq 1$ such that $r^{k+k} \in r^k + n_i\mathbb{Z}$ for any i. By replacing k by an integer in $(\mathbb{N}\backslash\{0\})k$ that is large enough, we can also assume that $|c_i| + m\|\alpha_i\|_\infty < r^k$ for any i. Given an integer $z \in \mathbb{Z}$, we denote by $f_k(z)$ the unique integer in $\{0, \ldots, k-1\}$ such that $f_k(z) \in z + k\mathbb{Z}$.

Let us consider the following Presburger formula $\psi_{i,z}(y, x')$ parameterized by $1 \leq i \leq j$ and $0 \leq z < k$:

$$\psi_{i,z}(y, x') := \bigvee_{s\in S_{r,m}} \begin{pmatrix} x' \in Z_{r,m,s} \\ \wedge \left(\left\langle\alpha_i, y - \dfrac{s}{1-r}\right\rangle < 0 \vee \left(\left\langle\alpha_i, y - \dfrac{s}{1-r}\right\rangle = 0 \wedge \langle\alpha_i, x'\rangle < c_i\right)\right) \\ \wedge\, r^{k+z}\left(y - \dfrac{s}{1-r}\right) + x' \in a + n_i\mathbb{Z}^m \end{pmatrix}.$$

Let us prove that for any (r, m)-decomposition $(\sigma, s) \in \Sigma_{r,m}^* \times S_{r,m}$ the two formulas $\phi_i(\gamma_{r,m,\sigma s^k}(y))$ and $\psi_{i,f_k(|\sigma|)}(y, \rho_{r,m}(\sigma, s))$ are equivalent. We denote by z the integer $z = f_k(|\sigma|)$. As $\gamma_{r,m,\sigma s^k}(y) = r^{|\sigma|+k}(y - \frac{s}{1-r}) + \rho_{r,m}(\sigma, s)$ we deduce that $\langle\alpha_i, \gamma_{r,m,\sigma s^k}(y)\rangle < c_i$ if and only if $\langle\alpha_i, y - \frac{s}{1-r}\rangle < \frac{c_i - \langle\alpha_i, \rho_{r,m}(\sigma,s)\rangle}{r^{|\sigma|+k}}$. Since $\|\rho_{r,m}(\sigma, s)\|_\infty \leq r^{|\sigma|}$ and $|c_i| + m\|\alpha_i\|_\infty < r^k$, we get $|\frac{c_i - \langle\alpha_i, \rho_{r,m}(\sigma,s)\rangle}{r^{|\sigma|+k}}| < 1$. As $\langle\alpha_i, y - \frac{s}{1-r}\rangle \in \mathbb{Z}$ for any $y \in \mathbb{Z}^m$, we deduce that $\langle\alpha_i, \gamma_{r,m,\sigma s^k}(y)\rangle < c_i$ if and only if $\langle\alpha_i, y - \frac{s}{1-r}\rangle < 0 \vee (\langle\alpha_i, y - \frac{s}{1-r}\rangle = 0 \wedge \langle\alpha_i, \rho_{r,m}(\sigma, s)\rangle < c_i)$. Moreover, as $\gamma_{r,m,\sigma s^k}(y) = r^{k+|\sigma|}(y - \frac{s}{1-r}) + \rho_{r,m}(\sigma, s)$ and $r^{k+k} \in r^k + n_i\mathbb{Z}$ we deduce that $\gamma_{r,m,\sigma s^k}(y) \in a_i + n_i\mathbb{Z}$ if and only if $r^{k+z}(y - \frac{s}{1-r}) + \rho_{r,m}(\sigma, s) \in a_i + n_i\mathbb{Z}$. We have proved that the two formulas $\phi_i(\gamma_{r,m,\sigma s^k}(y))$ and $\psi_{i,f_k(|\sigma|)}(y, \rho_{r,m}(\sigma, s))$ are equivalent.

Let us consider the Presburger formula $\psi_z(y, x') := \mathcal{R}(\ldots, \psi_{i,z}(y, x'), \ldots)$ parameterized by $0 \leq z < k$. Let us prove that for any (r, m)-decomposition $(\sigma, s) \in \Sigma_{r,m}^* \times S_{r,m}$ we have $\psi_{f_k(|\sigma|)}(y, \rho_{r,m}(\sigma, s))$ if and only if $y \in \gamma_{r,m,\sigma s^k}^{-1}(X)$. From the previous paragraph we deduce that $\psi_{f_k(|\sigma|)}(y, \rho_{r,m}(\sigma, s))$ is equivalent to $\mathcal{R}(\ldots, \phi_i(\gamma_{r,m,\sigma s^k}(y)), \ldots)$. Thus $\psi_{f_k(|\sigma|)}(y, \rho_{r,m}(\sigma, s))$ if and only if $\gamma_{r,m,\sigma s^k}(y) \in X$ if and only if $y \in \gamma_{r,m,\sigma s^k}^{-1}(X)$.

As X' is (r, m)-detectable in X, there exists a function $f : \mathcal{Q}_{r,m}(X) \to \mathcal{Q}_{r,m}(X')$ such that $f(\gamma_{r,m,\sigma}^{-1}(X)) = \gamma_{r,m,\sigma}^{-1}(X')$ for any $\sigma \in \Sigma_{r,m}^*$. Moreover, as X is Presburger observe that any set $Y \in \mathcal{Q}_{r,m}(X)$ is Presburger. Thus, there exists a Presburger formula $\phi_Y(y)$ that denotes Y. Let us consider the following Presburger formula $\psi(x')$.

$$\psi(x') := \bigvee_{\substack{Y\in\mathcal{Q}_{r,m}(X) \\ s\in S_{r,m}\cap((1-r)f(Y)) \\ z\in\{0,\ldots,k-1\}}} \left(x' \in Z_{r,m,s} \wedge (\forall y\ \psi_z(y, x') \Longleftrightarrow \phi_Y(y))\right).$$

Let us prove that $\psi(x')$ denotes the set X'. Consider a vector $x' \in X'$ and let us prove that $\psi(x')$ is satisfied. Consider an (r, m)-decomposition (σ, s) of x'. By definition of s we have $x' \in Z_{r,m,s}$. Let $Y = \gamma_{r,m,\sigma s^k}^{-1}(X)$ and let $z = f_k(|\sigma|)$. From $\rho_{r,m}(\sigma, s) \in X'$ and $\rho_{r,m}(\sigma, s) = \rho_{r,m}(\sigma s^k, s)$ we deduce that $s \in (1-r)\gamma_{r,m,\sigma s^k}^{-1}(X')$. By definition of the function f we deduce that $f(\gamma_{r,m,\sigma s^k}^{-1}(X)) = \gamma_{r,m,\sigma s^k}^{-1}(X')$. We have proved that $s \in S_{r,m} \cap ((1-r)f(Y))$. Recall that $\psi_z(y)$ is equivalent to

$y \in \gamma^{-1}_{r,m,\sigma s^k}(X)$. Thus the formula $\forall y\ \psi_z(y, x') \iff \phi_Y(y)$ is satisfied. We have proved that $\psi(x')$ is true. Conversely, let us consider a vector $x' \in \mathbb{Z}^m$ that satisfies $\psi(x')$. There exists $Y \in Q_{r,m}(X)$, $s \in S_{r,m} \cap ((1-r)f(Y))$ and $0 \leq z < k$ such that $x' \in Z_{r,m,s}$ and such that $\forall y\ \psi_z(y, x') \iff \phi_Y(y)$. As $x' \in Z_{r,m,s}$, there exists a word $\sigma \in \Sigma^*_{r,m}$ such that (σ, s) is an (r, m)-decomposition of x'. By replacing σ by a word in σs^*, we can also assume that $z = f_k(|\sigma|)$. Observe that in this case $\psi_z(y, \rho_{r,m}(\sigma, s))$ is equivalent to $y \in \gamma^{-1}_{r,m,\sigma s^k}(X)$. As $\psi_z(y, \rho_{r,m}(\sigma, s))$ is equivalent to $y \in Y$ we deduce that $Y = \gamma^{-1}_{r,m,\sigma s^k}(X)$. Therefore $f(Y) = \gamma^{-1}_{r,m,\sigma s^k}(X')$. From $\frac{s}{1-r} \in f(Y)$ we get $\rho_{r,m}(\sigma s^k, s) \in X'$. As $\rho_{r,m}(\sigma, s) = \rho_{r,m}(\sigma s^k, s)$ we get $x' \in X'$. We have proved that $\psi(x')$ denotes X'. □

7. Structural Presburger digit vector automata

An (r, m)-digit vector graph $G = (Q, \Sigma_{r,m}, \delta)$ is said to be Presburger if the (r, m)-digit vector automaton (q, G, F) represents a Presburger set for any initial state $q \in Q$ and for any accepting condition F for G. An (r, m)-digit vector automaton $\mathcal{A} = (q_0, G, F_0)$ is said to be *structurally Presburger* if G is Presburger. Observe that we have proved the following result.

Theorem 23. *The canonical (r, m)-digit vector automaton $\mathcal{A}_{r,m}(X)$ of a Presburger set $X \subseteq \mathbb{Z}^m$ is structurally Presburger.*

Proof. Let $X \subseteq \mathbb{Z}^m$ be a Presburger set and let $G_{r,m}(X)$ be the canonical (r, m)-digit vector graph of X. Let us consider an accepting condition F for $G_{r,m}(X)$. Lemma 17 shows that the set X' represented by the (r, m)-digit vector automaton $(X, G_{r,m}(X), F)$ is (r, m)-detectable in X. As X Presburger, Theorem 22 proves that X' is Presburger. Now, let us consider a state $q \in Q_{r,m}(X)$. As q is reachable from X and X' is Presburger, Theorem 10 proves that the set represented by the (r, m)-digit vector automaton $(q, G_{r,m}(X), F)$ is Presburger. We have proved that $G_{r,m}(X)$ is Presburger. □

The previous theorem shows that the digit vector automata obtained from minimal digit vector automata representing Presburger sets by moving the initial states and replacing the accepting conditions also represent Presburger sets. That means, a criterion for deciding if a digit vector automaton represents a Presburger set should be invariant by these two transformations.

References

[1] Constantinos Bartzis, Tevfik Bultan, Efficient symbolic representations for arithmetic constraints in verification, International Journal of Foundations of Computer Science 14 (4) (2003) 605–624.
[2] Constantinos Bartzis, Tevfik Bultan, Widening arithmetic automata, in: Proc. 16th Int. Conf. Computer Aided Verification, CAV'2004, Omni Parker House Hotel, Boston, USA, July 2004, in: Lecture Notes in Computer Science, vol. 3114, Springer, 2004, pp. 321–333.
[3] Alexandre Boudet, Hubert Comon, Diophantine equations, Presburger arithmetic and finite automata, in: Proc. 21st Int. Coll. on Trees in Algebra and Programming, CAAP'96, Linköping, Sweden, Apr. 1996, in: Lecture Notes in Computer Science, vol. 1059, Springer, 1996, pp. 30–43.
[4] Sébastien Bardin, Alain Finkel, Jérôme Leroux, Laure Petrucci, FAST: Fast acceleration of symbolic transition systems, in: Proc. 15th Int. Conf. Computer Aided Verification, CAV'2003, Boulder, CO, USA, July 2003, in: Lecture Notes in Computer Science, vol. 2725, Springer, 2003, pp. 118–121.
[5] Achim Blumensath, Erich Grädel, Finite presentations of infinite structures, in: Proc. 2nd Int. Workshop on Complexity in Automated Deduction, CiAD'2002, 2002.
[6] Véronique Bruyère, Georges Hansel, Christian Michaux, Roger Villemaire, Logic and p-recognizable sets of integers, Bull. Belg. Math. Soc. 1 (2) (1994) 191–238.
[7] Bernard Boigelot, Symbolic Methods for Exploring Infinite State Spaces, Ph.D. Thesis, Université de Liège, 1998.
[8] Vijay Ganesh, Sergey Berezin, D.L. Dill, Deciding Presburger arithmetic by model checking and comparisons with other methods, in: Proc. 4th Int. Conf. Formal Methods in Computer Aided Design, FMCAD'02, Portland, OR, USA, Nov. 2002, in: Lecture Notes in Computer Science, vol. 2517, Springer, 2002, pp. 171–186.
[9] Seymour Ginsburg, Edwin H. Spanier, Semigroups, Presburger formulas and languages, Pacific J. Math. 16 (2) (1966) 285–296.
[10] Felix Klaedtke, On the automata size for Presburger arithmetic, in: Proc. 19th Annual IEEE Symposium on Logic in Computer Science, LICS'04, Turku, Finland, July 2004, IEEE Comp. Soc. Press, 2004, pp. 110–119.
[11] Lash homepage. http://www.montefiore.ulg.ac.be/~boigelot/research/lash/.
[12] Jérôme Leroux, The affine hull of a binary automaton is computable in polynomial time, in: Proc. 5th Int. Workshop on Verification of Infinite State Systems, INFINITY 2003, Marseille, France, Sep. 2003, in: Electronic Notes in Theor. Comp. Sci., vol. 98, Elsevier Science, 2004, pp. 89–104.
[13] Jérôme Leroux, A polynomial-time Presburger criterion and synthesis for number decision diagrams, in: 20th IEEE Symposium on Logic in Computer Science (LICS 2005), 26–29 June 2005, Chicago, IL, USA, Proceedings, IEEE Computer Society, 2005, pp. 147–156.
[14] A. Muchnik, Definable criterion for definability in Presburger arithmetic and its applications (in Russian), preprint, Institute of new technologies, 1991.
[15] A. Muchnik, The definable criterion for definability in Presburger arithmetic and its applications, Theoret. Comput. Sci. 290 (2003) 1433–1444.
[16] Omega homepage. http://www.cs.umd.edu/projects/omega/.
[17] M. Presburger, Uber die volstandigkeit eines gewissen systems der arithmetik ganzer zahlen, in welchem die addition als einzige operation hervortritt, in: C. R. 1er congres des Mathematiciens des pays slaves, Varsovie, 1929, pp. 92–101.
[18] Tatiana Rybina, Andrei Voronkov, Brain: Backward reachability analysis with integers, in: Proc. 9th Int. Conf. Algebraic Methodology and Software Technology, AMAST'2002, Saint-Gilles-les-Bains, Reunion Island, France, Sep. 2002, in: Lecture Notes in Computer Science, vol. 2422, Springer, 2002, pp. 489–494.
[19] Pierre Wolper, Bernard Boigelot, An automata-theoretic approach to Presburger arithmetic constraints, in: Proc. 2nd Int. Symp. Static Analysis, SAS'95, Glasgow, UK, Sep. 1995, in: Lecture Notes in Computer Science, vol. 983, Springer, 1995, pp. 21–32.
[20] Pierre Wolper, Bernard Boigelot, On the construction of automata from linear arithmetic constraints, in: Proc. 6th Int. Conf. Tools and Algorithms for the Construction and Analysis of Systems, TACAS'2000, Berlin, Germany, Mar.–Apr. 2000, in: Lecture Notes in Computer Science, vol. 1785, Springer, 2000, pp. 1–19.