HAL
open science

Structural Presburger-definable Digit Vector Automata

Jérôme Leroux

To cite this version:

Jérôme Leroux. Structural Presburger-definable Digit Vector Automata. [Research Report] PI 1718, 2005. inria-00000039

HAL Id: inria-00000039
https://inria.hal.science/inria-00000039

Submitted on 20 May 2005

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

I R I S A
INSTITUT DE RECHERCHE EN INFORMATIQUE ET SYSTÈMES ALÉATOIRES

PUBLICATION
INTERNE
N° 1718

STRUCTURAL PRESBURGER-DEFINABLE DIGIT VECTOR AUTOMATA

JÉRÔME LEROUX

ISSN 1166-8687

IRISA
CAMPUS UNIVERSITAIRE DE BEAULIEU - 35042 RENNES CEDEX - FRANCE

IRISA
Tél. : (33) 02 99 84 71 00 – Fax : (33) 02 99 84 71 71
http://www.irisa.fr

Structural Presburger-definable Digit Vector Automata

Jérôme Leroux

Systèmes communicants
Projet VerTeCs

Publication interne n1718 — May 2005 — 13 pages

Abstract: Digit Vector Automata (DVA) provide a natural symbolic representation for regular sets of integer vectors encoded as strings of digit vectors (least significant digit first). We prove that the minimal DVA that represents a Presburger-definable set is structurally Presburger-definable: that means, the DVA obtained by modifying the initial state and the set of final states represents a Presburger-definable set.

Key-words: Automata, Presburger arithmetic, Semi-linear set, Symbolic representation

(Résumé : tsvp)

Centre National de la Recherche Scientifique
(UMR 6074) Université de Rennes 1 – Insa de Rennes

Institut National de Recherche en Informatique
et en Automatique – unité de recherche de Rennes

Structure des automates Presburger-définissables

Résumé : Les automates finis permettent de représenter symboliquement des ensembles infinis de vecteurs d'entiers, décomposés comme des mots de vecteurs de chiffres. On montre que l'automate minimal représentant un ensemble Presburger-définissable, est structurellement Presburger-définissable: c'est à dire, que les automates obtenus en changeant l'état initial et les états finaux représentent des ensembles Presburger-définissables.

Mots clés : Automate, Arithmétique de Presburger, Ensemble semilinéaire, Représentation symbolique

Presburger arithmetic [21] is a decidable logic used in a large range of applications. Different techniques [11] and tools have been developed for manipulating *the Presburger-definable sets* (the sets of integer vectors satisfying a Presburger formula): by working directly on the Presburger-formulas (implemented in OMEGA [20]), by using semi-linear sets [12] (implemented in BRAIN [22]), or by using Digit Vector Automata (DVA) that represent regular sets of integer vectors encoded as strings of digit vectors, least or most significant digit first [23, 7] (implemented in FAST [1], LASH [15] and CSL-ALV [2]). 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. Moreover, deciding if a given vector of integers is in a given set, is at least *NP-hard* [4, 12]. On the other hand, a minimization procedure for automata provides a canonical representation for *DVA-definable sets* (a set represented by a DVA). That means, the DVA that represents a given set only depends on the set and not on the way we have computed it. For this reason, DVA are well adapted for applications that require a lot of Boolean manipulations like model-checking.

Recently, the DVA obtained by modifying the set of final states, has provided some applications. First, we have proved that modifying the set of final states of a DVA, provides some simple sets that can be used for deciding in polynomial time if a DVA is Presburger-definable (that means, the DVA represents a Presburger-definable set) [17]. Recall that the previous algorithm for deciding this property, was given by Muchnik in 1991 [18, 19, 8], and works in *quadruply-exponential time*. Second, Bartzis and Bultan [3] provided a *widening operator* for DVA in order to enforce the convergence of the incrementally computed DVA, during the reachability state space exploration of an *infinite state system*. This operator is obtained by modifying the set of final states of Presburger-definable DVA, but they do not prove that the obtained DVA remain Presburger-definable.

However, from practical and theoretical point of view, working only with Presburger-definable DVA has some advantages. First the manipulation complexity (boolean operations and variable elimination) is at most 3-exponential time for Presburger-definable DVA (see [13, 17]) and non-elementary for general DVA (see [5]). Second, we can compute in polynomial time, a Presburger-formula that defines the set represented by a Presburger-definable DVA. Then this formula can be used in other tools like OMEGA.

In this paper, we introduce a new automata-based representation for regular subsets of $\mathbb{Z}^m$, called the *digit Vector automata (DVA)*. Even if DVA are very similar to other automata-based representations [6, 7, 8], it is the *first* automata-based representation for any regular subsets of $\mathbb{Z}^m$, that is both *canonical* (there exists a unique minimal DVA that represents a given set X) and *stable by modifying the initial state* (this stability provides a natural way for associating a subset of $\mathbb{Z}^m$ to any state of the DVA). Moreover, we prove that the minimal DVA that represents a Presburger-definable set is structurally Presburger-definable: that means, any DVA obtained by modifying the initial state and the set of final states, is Presburger-definable.

1 Notations

We denote by $\mathbb{Z}$ and $\mathbb{N}\backslash\{0\}$ respectively the set of integers and non-negative integers. The set X^m is called the set of vectors with $m \in \mathbb{N}$ components in a set X. Given an integer $i \in \{1, \dots, m\}$ and a vector $x \in X^m$, the i-th component of x is written $x[i] \in X$. We denote by $\mathbf{e}_0$ the vector $\mathbf{e}_0 = (0, \dots, 0)$. Vectors $x + y$ and $t.x$ are defined by $(x + y)[i] = (x[i]) + (y[i])$ and $(t.x)[i] = t.(x[i])$ for any $i \in \{1, \dots, m\}$, $x, y \in \mathbb{Q}^m$, $t \in \mathbb{Q}$. We denote by $\langle x, y\rangle = \sum_{i=1}^{m} x[i].y[i]$, the *dot product* of two vectors $x, y \in \mathbb{Q}^m$. Given a *functions* $f : X \to Y$, $A \subseteq X$ and $B \subseteq Y$, we define $f(A) = \{f(a);\ a \in A\}$ and $f^{-1}(B) = \{x \in X;\ f(x) \in B\}$.

Given a non-empty finite *alphabet* Σ, we denote by Σ^+ the set of non-empty *words* over Σ and we denote by ϵ the empty word. As usual Σ^* denotes the set of words $\Sigma^+ \cup \{\epsilon\}$. A subset $\mathcal{L} \subseteq \Sigma^*$ is called a *language*. The concatenation of two words σ_1 and σ_2 (resp. two languages $\mathcal{L}_1$ and $\mathcal{L}_2$) is denoted by $\sigma_1.\sigma_2$ (resp. $\mathcal{L}_1.\mathcal{L}_2 = \{\sigma_1.\sigma_2;\ (\sigma_1, \sigma_2) \in \mathcal{L}_1 \times \mathcal{L}_2\}$). Given a word $\sigma \in \Sigma^*$, we denote by $(\sigma^i)_{i\in\mathbb{N}}$ the

sequence of words defined by the induction $\sigma^0 = \epsilon$ and $\sigma^{i+1} = \sigma^i.\sigma$. We denote by σ^* the language $\sigma^* = \{\sigma^i;\ i \in \mathbb{N}\}$. The *length* of a word σ is denoted by $|\sigma| \in \mathbb{N}$. For any non-empty word $\sigma \in \Sigma^+$, we denote by $\sigma[1]$, ..., $\sigma[|\sigma|]$ the elements in Σ such that $\sigma = \sigma[1] \dots \sigma[|\sigma|]$.

2 Digit Vector Automata

In this section, the *Digit Vector Automata (DVA)* representation, a state-based representation of set of integer vectors, is presented. The sets obtained by *moving the initial state* and *modifying the set of final states* of a DVA are respectively characterized in sections 2.2 and 2.3.

2.1 Digit vector decomposition

Let us consider an integer $r \geq 2$ called the *basis of decomposition* and the *set of digits* $\Sigma_r = \{0, \dots, r-1\}$. In this section, we study the *least significant digit first decomposition* of an integer vector in $\mathbb{Z}^m$ into a word of *digit vectors* in $(\Sigma_r^m)^*$. This decomposition can be easily obtained by considering the sequence $(\gamma_{r,\sigma})_{\sigma \in (\Sigma_r^m)^*}$ of functions $\gamma_{r,\sigma} : \mathbb{Z}^m \to \mathbb{Z}^m$ uniquely defined by the following equalities [16]:

$$\begin{cases} \gamma_{r,b}(x) = r.x + b & (b, x) \in \Sigma_r^m \times \mathbb{Z}^m \\ \gamma_{r,\sigma_1.\sigma_2} = \gamma_{r,\sigma_1} \circ \gamma_{r,\sigma_2} & (\sigma_1, \sigma_2) \in (\Sigma_r^m)^* \times (\Sigma_r^m)^* \end{cases}$$

Assume that the dimension m is equal to 1 and consider a couple $(\sigma, s) \in \Sigma_r^* \times S_r$ where S_r is the set of *sign digits* $S_r = \{0, r-1\}$. The following equality is called the *least significant digit first decomposition with* 2*-complement*:

$$\gamma_{r,\sigma}\left(\frac{s}{1-r}\right) = \begin{cases} \sum_{i=1}^{|\sigma|} r^{i-1}\sigma[i] \in \mathbb{N} & \text{if } s = 0 \\ \sum_{i=1}^{|\sigma|} r^{i-1}\sigma[i] - r^{|\sigma|} \in \mathbb{Z}\backslash\mathbb{N} & \text{if } s = r-1 \end{cases}$$

The previous decomposition shows intuitively that $s = 0$ correspond to the *non-negative sign digit* whereas $s = r-1$ corresponds to the *negative one*.

For a general dimension $m \geq 1$, let us consider the function $\rho_r : (\Sigma_r^m)^* \times S_r^m \to \mathbb{Z}^m$ defined by the following equality:

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

A couple $(\sigma, s) \in (\Sigma_r^m)^* \times S_r^m$ such that $x = \rho_r(\sigma, s)$ is called a *r-decomposition* of $x \in \mathbb{Z}^m$. Remark that any $x \in \mathbb{Z}^m$ owns at least one r-decomposition.

Function ρ_r naturally associate to any language $\mathcal{L} \subseteq (\Sigma_r^m)^* \times S_r^m$ a subset $X = \rho_r(\mathcal{L})$ of $\mathbb{Z}^m$. Remark however that there exists some languages $\mathcal{L}_1$, $\mathcal{L}_2$ and $\mathcal{L}$ such that $\mathcal{L}_1 \cap \mathcal{L}_2 = \mathcal{L}$ and such that $\rho_r(\mathcal{L}_1) \cap \rho_r(\mathcal{L}_2) \neq \rho_r(\mathcal{L})$. For instance, consider $\mathcal{L}_1 = \{(\epsilon, 0)\}$, $\mathcal{L}_2 = \{(0, 0)\}$ and $\mathcal{L} = \emptyset$. Such a side effect is due to the fact that an integer vector $x \in \mathbb{Z}^m$ does not have a unique r-decomposition. The following lemma characterizes r-decompositions associated to the same vector.

Lemma 1 *Two r-decompositions (σ_1, s_1) and (σ_2, s_2) are associated to the same vector if and only if $s_1 = s_2$ and $\sigma_1.s_1^* \cap \sigma_2.s_2^* \neq \emptyset$.*

Proof : Let us first remark that for any sign digit vector $s \in S_r^m$, we have $\gamma_{r,s}(\frac{s}{1-r}) = \frac{s}{1-r}$. In particular, we have $\rho_r(\sigma.s^k, s) = \rho_r(\sigma, s)$ for any word $\sigma \in (\Sigma_r^m)^*$ and for any $k \in \mathbb{N}$. This equality is well known when $s = 0$ and it just means that *adding extra zero digits* to the least significant digit first decomposition of a non-negative integer does not change its value.

Assume first that (σ_1, s_1) and (σ_2, s_2) are such that $s_1 = s_2$ and $\sigma_1.s_1^* \cap \sigma_2.s_2^* \neq \emptyset$, and let us prove that $\rho_r(\sigma_1, s_1) = \rho_r(\sigma_2, s_2)$. There exist $k_1, k_2 \in \mathbb{N}$ such that $\sigma_1.s_1^{k_1} = \sigma_2.s_2^{k_2}$. In particular, from the previous paragraph we deduce $\rho_r(\sigma_1, s_1) = \rho_r(\sigma_1.s_1^{k_1}, s_1) = \rho_r(\sigma_2.s_2^{k_2}, s_2) = \rho_r(\sigma_2, s_2)$.

Next, assume that $\rho_r(\sigma_1, s_1) = \rho_r(\sigma_2, s_2)$ and let us prove that $s_1 = s_2$ and $\sigma_1.s_1^* \cap \sigma_2.s_2^* \neq \emptyset$. As the manipulated structures are defined component wise, we can assume without loss of generality that the dimension m is equal to 1. Remark that the sign digits s_1 and s_2 must be equal. In fact, otherwise, there exists $i_1, i_2 \in \{1, 2\}$ such that $s_{i_1} = 0$ and $s_{i_2} = r - 1$ and in this case we have shown that $\rho_r(\sigma_{i_1}, s_{i_1}) \in \mathbb{N}$ and $\rho_r(\sigma_{i_2}, s_{i_2}) \in \mathbb{Z}\backslash\mathbb{N}$ which is in contradiction with $\rho_r(\sigma_1, s_1) = \rho_r(\sigma_2, s_2)$. Let us consider $k_1, k_2 \in \mathbb{N}$ such that the words $w_1 = \sigma_1.s_1^{k_1}$ and $w_2 = \sigma_2.s_2^{k_2}$ have the same length denoted by $k \in \mathbb{N}$. The first paragraph shows that $\rho_r(w_1, s_1) = \rho_r(w_2, s_2)$. As $s_1 = s_2$, we deduce the following equality:

$$\sum_{i=1}^{k} r^{i-1}.(w_1[i] - w_2[i]) = 0$$

Assume by contradiction that $w_1 \neq w_2$. In this case $k \in \mathbb{N}\backslash\{0\}$ and there exists a maximal (for $\leq$) $j \in \{1, \ldots, k\}$ such that $w_1[j] \neq w_2[j]$. We have:

$$|w_1[i] - w_2[i]| \begin{cases} = 0 & \text{if } i > j \\ \geq 1 & \text{if } i = j \\ \leq r - 1 & \text{if } i < j \end{cases}$$

We deduce the following bound::

$$\begin{aligned} |\sum_{i=1}^{k} r^{i-1}.(w_1[i] - w_2[i])| &= |r^j.(w_1[j] - w_2[j]) + \sum_{i=1}^{j-1} r^{i-1}.(w_1[i] - w_2[i])| \\ &\geq |r^j.(w_1[j] - w_2[j])| - \sum_{i=1}^{j-1} |r^{i-1}.(w_1[i] - w_2[i])| \\ &\geq r^j - \sum_{i=1}^{j-1} r^{i-1}.(r-1) \\ &= 1 \end{aligned}$$

We obtain a contradiction. We deduce that $w_1 = w_2$ and in particular the word $w = w_1 = w_2$ is in $\sigma_1.s_1^* \cap \sigma_2.s_2^*$. Q.E.D

A *language* $\mathcal{L} \subseteq (\Sigma_r^m)^* \times S_r^m$ is said *saturated* [14] if for any $(\sigma, s) \in (\Sigma_r^m)^* \times S_r^m$, we have $(\sigma, s) \in \mathcal{L}$ if and only if $(\sigma.s, s) \in \mathcal{L}$. Previous lemma 1 shows that a language $\mathcal{L}$ is saturated if and only if there exists $X \subseteq \mathbb{Z}^m$ such that $\mathcal{L} = \rho_r^{-1}(X)$. In particular, we deduce that the *side effect* $\mathcal{L}_1 \cap \mathcal{L}_2 = \mathcal{L}$ and $\rho_r(\mathcal{L}_1) \cap \rho_2(\mathcal{L}_2) \neq \rho_r(\mathcal{L})$ is no longer true for saturated language. In fact, for any saturated languages $\mathcal{L}_1, \mathcal{L}_2$ and for any $\# \in \{\cup, \cap, \backslash, \Delta\}$, the language $\mathcal{L}_1 \# \mathcal{L}_2$ is saturated and $\rho_r(\mathcal{L}_1) \# \rho_r(\mathcal{L}_2) = \rho_r(\mathcal{L}_1 \# \mathcal{L}_2)$.

We are interested in associating to a saturated language a *state-based symbolic representation*, called *Digit Vector Automata*.

Definition 1 (Digit Vector Automata) *A* Digit Vector Automaton (DVA) $\mathcal{A}$ *is a tuple* $\mathcal{A} = (Q, \Sigma_r^m, \delta, q_0, F_0)$ *where:*

- Q *is a non-empty finite set of* states.
- $\delta : Q \times \Sigma_r^m \to Q$ *is the* transition function.
- $q_0 \in Q$ *is the* initial state.
- $F_0 \subseteq Q \times S_r^m$ *is the set of* final states *such that* $(q, s) \in F_0$ *if and only if* $(q', s) \in F_0$ *for every* $q' = \delta(q, s)$.

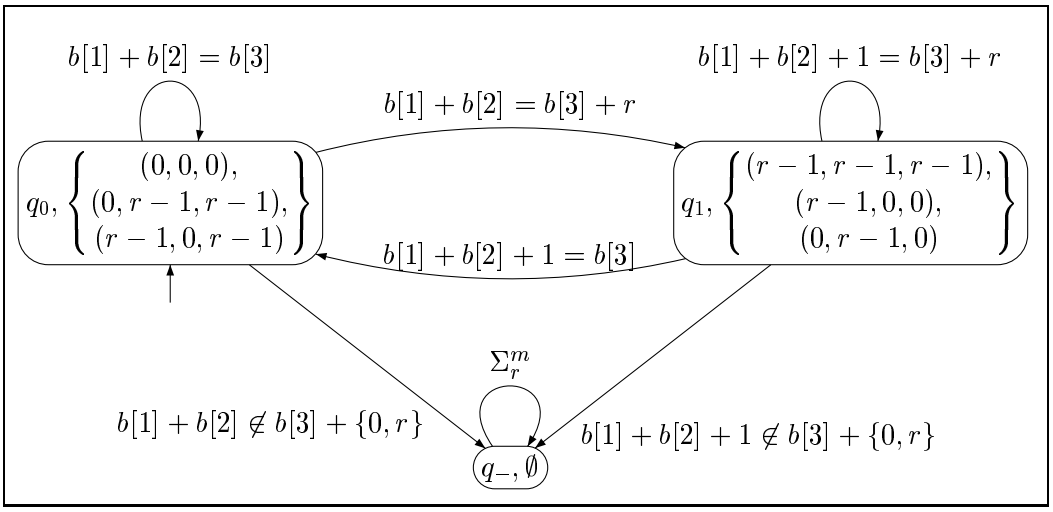

Figure 1: DVA $\mathcal{A}_X$ representing $X = \{x \in \mathbb{Z}^3;\ x[1] + x[2] = x[3]\}$

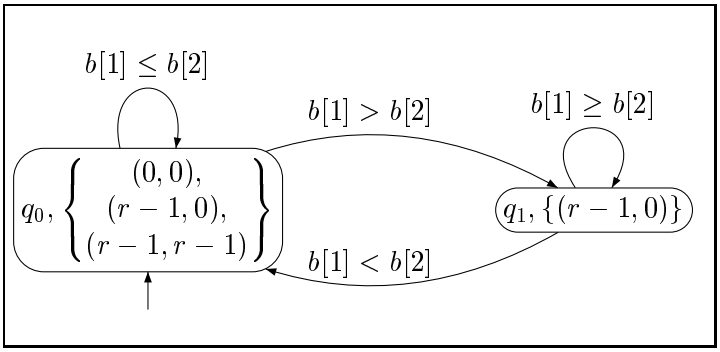

Figure 2: DVA $\mathcal{A}_X$ representing $X = \{x \in \mathbb{Z}^2;\ x[1] \leq x[2]\}$

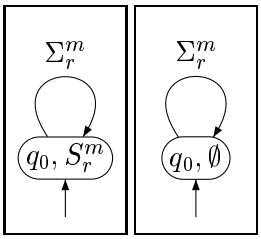

Figure 3: On the left, DVA $\mathcal{A}_{\mathbb{Z}^m}$. On the right, DVA $\mathcal{A}_\emptyset$

As usual, function δ is uniquely *extended* over $Q \times (\Sigma_r^m)^*$ by $\delta(q, \sigma_1.\sigma_2) = \delta(\delta(q, \sigma_1), \sigma_2)$. Moreover, a tuple (q, σ, q') such that $q' = \delta(q, \sigma)$ is denoted by $q \xrightarrow{\sigma} q'$ or just $q \to q'$, and called a *path* from q to q' *labeled* by σ. Such a state q' is said *reachable* from q (when $q = q_0$, we just say that q' is *reachable*).

The *language* $\mathcal{L}(\mathcal{A})$ *recognized* by a DVA $\mathcal{A}$ is defined by $\mathcal{L}(\mathcal{A}) = \{(\sigma, s) \in (\Sigma_r^m)^* \times S_r^m;\ (\delta(q_0, \sigma), s) \in F_0\}$. Thanks to the condition $(q, s) \in F_0$ if and only if $(q', s) \in F_0$ for every $q \xrightarrow{s} q'$, the language $\mathcal{L}(\mathcal{A})$ is saturated. The set $X = \rho_r(\mathcal{L}(\mathcal{A})) \subseteq \mathbb{Z}^m$ is called the set *represented* by the DVA $\mathcal{A}$.

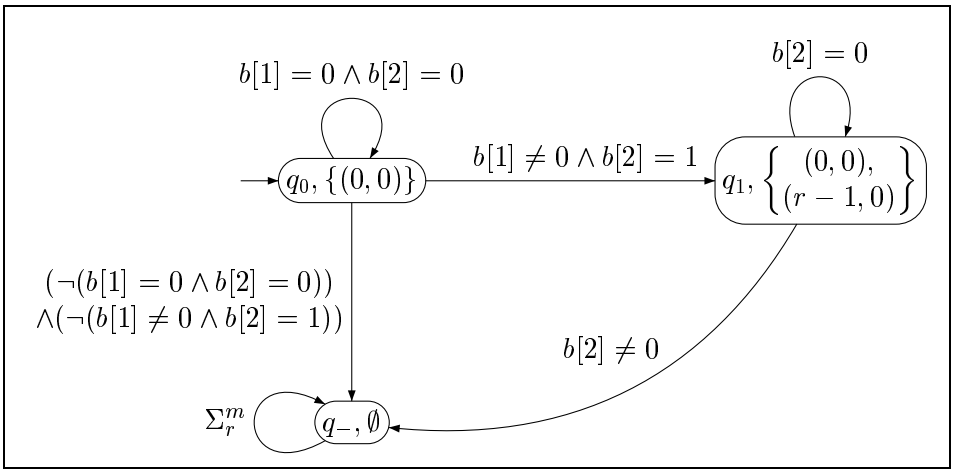

Figure 4: DVA $\mathcal{A}_X$ representing $X = \{x \in \mathbb{Z}^2;\ V_r(x[1]) = x[2]\}$

Sets represented by DVA correspond to the *r-definable sets*. Recall ([8]) that a set $X \subseteq \mathbb{Z}^m$ is said *r-definable* if it can be defined in the first order theory FO $(\mathbb{Z}, +, \leq, V_r)$ where $V_r : \mathbb{Z} \to \mathbb{Z}$ is the r-valuation function defined by $V_r(0) = 0$ and $V_r(x)$ is the greatest power of r that divides $x \in \mathbb{Z}\backslash\{0\}$ (figure 4). Recall also that a *Number Decision Diagram (NDD)* [6, 24] that represents a set $X \subseteq \mathbb{Z}^m$, is an automaton over Σ_r^m that recognizes the language $\{\sigma.s;\ (\sigma, s) \in \rho_r^{-1}(X)\}$. We do not consider NDD in this paper because the automaton obtained from a NDD by *replacing the initial state* by an other state is not a NDD in general (it does not recognizes a language of the form $\{\sigma.s;\ (\sigma, s) \in \rho_r^{-1}(X')\}$ where $X' \subseteq \mathbb{Z}^m$). However, DVA and NDD have slightly the same structure and we can easily compute a NDD from a DVA and conversely, that represents the same set X. In particular, we directly deduce from [8] and this remark, the following corollary 1

Corollary 1 *A set $X \subseteq \mathbb{Z}^m$ can be represented by a DVA if and only if it is r-definable.*

Remark 1 *As in the NDD case, DVA can be* efficiently manipulated *by reprensenting the set $\{b \in \Sigma_r^m;\ q \xrightarrow{b} q'\}$ and $\{s \in S_r^m;\ (q, s) \in F_0\}$ by some Binary Decision Diagrams (BDD) [9] over the alphabet Σ_r (and not the exponential one Σ_r^m).*

2.2 Moving the initial state

The DVA obtained from a DVA $\mathcal{A}$ by replacing the initial state q_0 by a state $q \in Q$ is denoted by $\mathcal{A}_q$. To simplify notations, when a set $X \subseteq \mathbb{Z}^m$ is implicitly represented by a DVA $\mathcal{A}$, we denote by $X_q \subseteq \mathbb{Z}^m$ the set represented by the DVA $\mathcal{A}_q$. We are going to characterize the set X_q in function of X. As an application, we show that any r-definable set $X \subseteq \mathbb{Z}^m$ is represented by a *unique minimal DVA*.

Proposition 1 *For any path $q \xrightarrow{\sigma} q'$ in a DVA $\mathcal{A}$ that represents a set X, we have $X_{q'} = \gamma_{r,\sigma}^{-1}(X_q)$.*

Proof : Without loss of generality, we can restrict our proof to a path $q_0 \xrightarrow{\sigma} q$ in a DVA $\mathcal{A}$ that represents a set X. Let us consider an integer vector $x \in X_q$. There exists a path $q \xrightarrow{w} q'$ and $s \in S_r^m$ such that $x = \rho_r(w, s)$ and $(q', s) \in F_0$. We deduce that we have a path $q_0 \xrightarrow{\sigma.w} q'$ with $(q', s) \in F_0$. Therefore $\rho_r(\sigma.w, s) \in X$. From $\rho_r(\sigma.w, s) = \gamma_{r,\sigma}(\rho_r(w, s)) = \gamma_{r,\sigma}(x)$, we deduce that $x \in \gamma_{r,\sigma}^{-1}(X)$ and we have proved the inclusion $X_q \subseteq \gamma_{r,\sigma}^{-1}(X)$. For the converse inclusion, consider an integer vector $x \in \gamma_{r,\sigma}^{-1}(X)$. As $\gamma_{r,\sigma}(x) \in X$, there exists a path $q_0 \xrightarrow{w} q'$ and $s \in S_r^m$ such that $\gamma_{r,\sigma}(x) = \rho_r(w, s)$ and $(q, s) \in F_0$. Moreover, as $x \in \mathbb{Z}^m$, there exists $(w', s') \in (\Sigma_r^m)^* \times S_r^m$ such that $x = \rho_r(w', s')$. From the equality $\gamma_{r,\sigma}(x) = \rho_r(w, s)$, we deduce that $\rho_r(\sigma.w', s') = \rho_r(w, s)$. Lemma 1 shows that $s' = s$ and there exists $k_1, k_2 \in \mathbb{N}$ such that $\sigma.w'.s^{k_1} = w.s^{k_2}$. As we have a path $q_0 \xrightarrow{w} q'$ with $(q', s) \in F_0$ and $\mathcal{A}$ is a DVA, we deduce that $q'' = \delta(q', s^{k_2})$ is such that $(q'', s) \in F_0$. From $\sigma.w'.s^{k_1} = w.s^{k_2}$, we get that $q_0 \xrightarrow{\sigma.w'.s^{k_1}} q''$. In particular we have a path $q \xrightarrow{w'.s^{k_1}} q''$ with $(q'', s) \in F_0$. We deduce that $x = \rho_r(w'.s^{k_1}, s) \in X_q$ and we have proved $\gamma_{r,\sigma}^{-1}(X) \subseteq X_q$. Q.E.D

The previous proposition 1 proves in particular that the set $Q_X = \{\gamma_{r,\sigma}^{-1}(X);\ \sigma \in (\Sigma_r^m)^*\}$ is finite when X is r-definable. The *minimal (for the number of states) DVA* that represents a r-definable set $X \subseteq \mathbb{Z}^m$ can be easily characterized by introducing the DVA $\mathcal{A}_X$ defined by the set of states Q_X, the transition function δ_X defined by a $\delta_X(X', b) = \gamma_{r,b}^{-1}(X')$ for any $X' \in Q_X$, the initial state $q_{0,X} = X$, the set of final states $F_{0,X} = \{(X', s) \in Q_X \times S_r^m;\ \frac{s}{1-r} \in X'\}$.

A DVA $\mathcal{A}$ is said *minimal* if for any DVA $\mathcal{A}'$ that represents the same set than $\mathcal{A}$, the number of states $|Q|$ of $\mathcal{A}$ is less than or equal to the number of states $|Q'|$ of $\mathcal{A}'$. Two DVA $\mathcal{A}_1 = (Q_1, \Sigma_r^m, \delta_1, q_{0,1}, F_{0,1})$ and $\mathcal{A}_2 = (Q_2, \Sigma_r^m, \delta_2, q_{0,2}, F_{0,2})$ are said *isomorph* if there exists a *one-to-one relation* $\sim \subseteq Q_1 \times Q_2$ such that $\delta_1(q_1, b) \sim \delta_2(q_2, b)$ and $\{s \in S_r^m;\ (q_1, s) \in F_{0,1}\} = \{s \in S_r^m;\ (q_2, s) \in F_{0,2}\}$ for any $q_1 \sim q_2$, and such that $q_{0,1} \sim q_{0,2}$.

Theorem 1 *For any r-definable set $X \subseteq \mathbb{Z}^m$, the DVA $\mathcal{A}_X$ is the unique (up to isomorphism) minimal DVA that represents X.*

Proof : First remark that $\mathcal{A}_X$ is a DVA that represents X. Next, let us consider a minimal DVA $\mathcal{A} = (Q, \Sigma_r^m, \delta, q_0, F_0)$ that represents X. Proposition 1 proves that there exists a function $f : Q_X \to Q$ such that $X_{f(X')} = X'$ for any $X' \in Q_X$. In particular $|Q_X| \leq |Q|$ and as $\mathcal{A}$ is minimal, we have $|Q_X| = |Q|$ and in particular $\mathcal{A}_X$ is also minimal. Moreover, we deduce that f is a one-to-one function. Just remark that $\mathcal{A}$ and $\mathcal{A}_X$ are isomorph for the one-to-one relation $\sim = \{(X', f(X'));\ X' \in Q_X\}$. Q.E.D

From the previous theorem 1 and corollary 1, we deduce that a set $X \subseteq \mathbb{Z}^m$ is r-definable if and only if $Q_X = \{\gamma_{r,\sigma}^{-1}(X);\ \sigma \in (\Sigma_r^m)^*\}$ is finite.

2.3 Replacing the set of final states

Given a DVA $\mathcal{A}$, the class of subsets $F \subseteq Q \times S_r^m$ such that $(q, s) \in F$ if and only if $(q', s) \in F$ for any transition $q \xrightarrow{s} q'$, is denoted by $\mathcal{F}_{\mathcal{A}}$. The DVA obtained from a DVA $\mathcal{A}$ be replacing the set of final states F_0 by a set $F \in \mathcal{F}_{\mathcal{A}}$ is denoted by $\mathcal{A}^F$. To simplify notions, when a set $X \subseteq \mathbb{Z}^m$ is implicitly represented by a DVA $\mathcal{A}$, we denote by X^F the set represented by the DVA $\mathcal{A}^F$. In this section, the set $\mathcal{F}_{\mathcal{A}}$ is geometrically characterized by introducing the notion of *eyes*, *semi-eyes* and *kernel*.

Let us consider the *equivalence relation* $\sim_{\mathcal{A}}$ over $Q \times S_{r^m}$ defined by $(q_1, s_1) \sim_{\mathcal{A}} (q_2, s_2)$ if and only if $s_1 = s_2$ and $\delta(q_1, s_1^*) \cap \delta(q_2, s_2^*) \neq \emptyset$.

An *eye* Y is an *equivalence class* for the relation $\sim_{\mathcal{A}}$ (see figure 5). A *semi-eye* is a finite union of eyes. Remark that the class of semi-eyes is exactly $\mathcal{F}_{\mathcal{A}}$.

Let us consider the function $\delta_e : Q \times S_r^m \to Q \times S_r^m$ defined by $\delta_e(q, s) = (\delta(q, s), s)$.

The *kernel* $\ker(Y)$ of a subset $Y \subseteq Q \times S_r^m$ is defined as $\ker(Y) = \bigcap_{n \in \mathbb{N}} \delta_e^n(Y)$ and corresponds to the greatest (for $\subseteq$) fix-point for δ_e included in Y. Remark that the kernel of any eye Y is a non

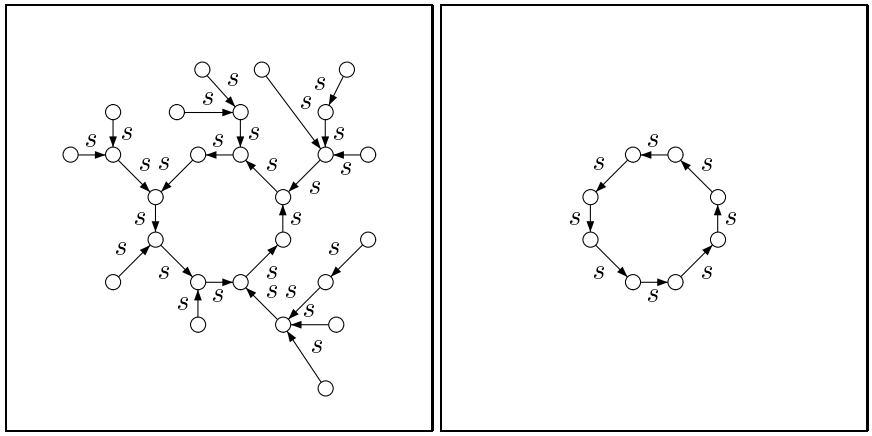

Figure 5: On the left an eye. On the right its kernel.

empty set of the form $\ker(Y) = \{(q_0, s), \dots, (q_{n-1}, s), (q_n, s) = (q_0, s)\}$ such that $\delta(q_i, s) = q_{i+1}$ for any $i \in \{0, \dots, n-1\}$ (see figure 5).

Example 1 *Let $\mathcal{A}_X$ be the minimal DVA representing $X = \{x \in \mathbb{Z}^3;\ x[1] + x[2] = x[3]\}$ given in figure 1. The eyes of $\mathcal{A}$ are $\{(q_0, (0,0))\}$, $\{(q_0, (r-1, r-1))\}$, $\{(q_1, (0,0))\}$, $\{(q_1, (r-1, r-1))\}$, $\{(q_0, (0, r-1)), (q_1, (0, r-1))\}$, and $\{(q_0, (r-1, 0)), (q_1, (r-1, 0))\}$.*

3 Presburger-definable DVA

A subset $X \subseteq \mathbb{Z}^m$ is said *Presburger-definable* if it can be defined by a formula in the first order theory $\mathrm{FO}(\mathbb{Z}, +, \leq)$ (see figure 6). A DVA $\mathcal{A}$ is said *Presburger-definable* if the set represented by $\mathcal{A}$ is Presburger-definable. A set X is said *structurally Presburger-definable* if the minimal DVA $\mathcal{A}$ that represents X, is such that $\mathcal{A}_q^F$ is Presburger-definable for any state $q \in Q$ and for any semi-eyes $F \in \mathcal{F}_{\mathcal{A}}$. Naturally, as $\mathcal{A}_{q_0}^{F_0}$ represents X, a structurally Presburger-definable set is Presburger-definable. In this section, we prove the converse.

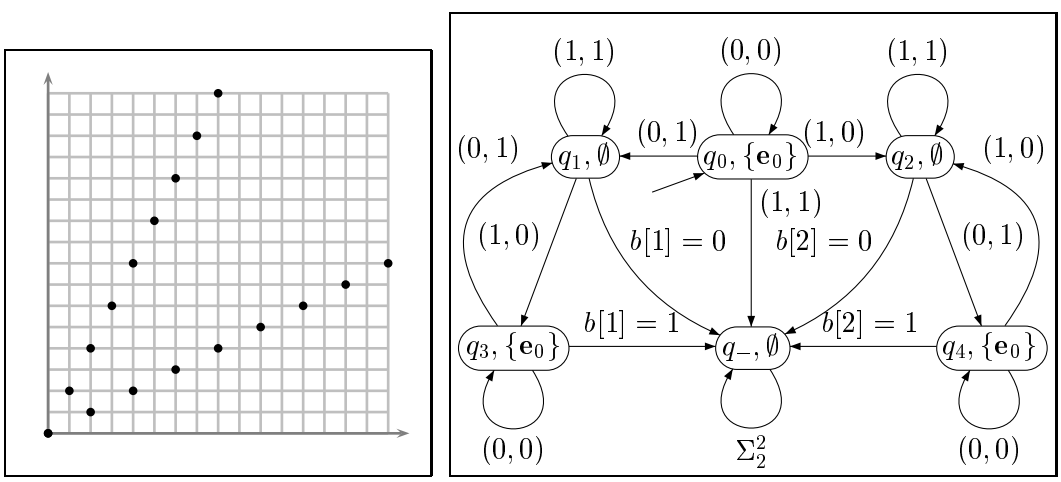

Figure 6: A Presburger-definable set $\{x \in \mathbb{N}^2;\ (x[1] = 2.x[2]) \vee (2.x[1] = x[2])\}$ and its minimal DVA $\mathcal{A}_X$ in basis $r = 2$.

Remark 2 *A* linear set *X of $\mathbb{Z}^m$ is a set of the form $X = b + \sum_{p \in P} \mathbb{N}.p$ where $b \in \mathbb{Z}^m$ is called the* basis *and $P \subseteq \mathbb{Z}^m$ is a finite subset of $\mathbb{Z}^m$ called the set of* periods. *A* semi-linear set *of $\mathbb{Z}^m$ is a finite union of linear sets of $\mathbb{Z}^m$. Recall that a set X is Presburger-definable if and only if it is* semi-linear *[12].*

Example 2 *The Presburger-definable set $X = \{x \in \mathbb{N}^2;\ (x[1] = 2.x[2]) \vee (2.x[1] = x[2])\}$ and its minimal DVA $\mathcal{A}_X$ in basis $r = 2$ are given in figure 6. Remark that the set of final states F_0 can be decomposed into 3 eyes $Y_0 = \{(q_0, \boldsymbol{e}_0)\}$, $Y_3 = \{(q_3, \boldsymbol{e}_0)\}$ and $Y_4 = \{(q_4, \boldsymbol{e}_0)\}$. The DVA $\mathcal{A}_X^{Y_0}$, $\mathcal{A}_X^{Y_3}$ and $\mathcal{A}_X^{Y_4}$ respectively represent $X^{Y_0} = \{\boldsymbol{e}_0\}$, $X^{Y_3} = \{x \in \mathbb{N}^2 \backslash \{\boldsymbol{e}_0\};\ x[1] = 2.x[2]\}$ and $X^{Y_4} = \{x \in \mathbb{N}^2 \backslash \{\boldsymbol{e}_0\};\ 2.x[1] = x[2]\}$.*

From proposition 1, we get the following corollary.

Corollary 2 *For any reachable state q of a Presburger-definable DVA $\mathcal{A}$, the DVA $\mathcal{A}_q$ is Presburger-definable.*

Proof : Let $\mathcal{A}$ be a DVA that represents a Presburger-definable set X and consider a reachable state q of $\mathcal{A}$. There exists a path $q_0 \xrightarrow{\sigma} q$. Proposition 1 proves that $X_q = \gamma_{r,\sigma}^{-1}(X)$. As X is Presburger-definable, there exists a Presburger-formula ϕ that defines X. Now, just remark that X_q is defined by the Presburger formula $\phi_\sigma(x) := \exists x'\ (x' = r^{|\sigma|}.x + \gamma_{r,\sigma}(\mathbf{e}_0) \wedge \phi(x'))$. Hence $\mathcal{A}_q$ is Presburger-definable. Q.E.D

A quantification elimination shows that a Presburger-definable set X is a boolean combination in $\mathbb{Z}^m$ of sets of the form $X = \{x \in \mathbb{Z}^m;\ x[i] \in c + n.\mathbb{Z}\}$ where $(i, c, n) \in \{1, \ldots, m\} \times \mathbb{Z} \times (\mathbb{N} \backslash \{0\})$, and sets of the form $X = \{x \in \mathbb{Z}^m;\ \langle \alpha, x \rangle \leq c\}$ where $(\alpha, c) \in (\mathbb{Z}^m \backslash \{0\}) \times \mathbb{Z}$. The following technical lemmas 2 and 3 prove that these sets are structurally Presburger-definable.

Lemma 2 *The set $X = \{x \in \mathbb{Z}^m;\ x[i] \in c + n.\mathbb{Z}\}$ where $(i, c, n) \in \{1, \ldots, m\} \times \mathbb{Z} \times (\mathbb{N} \backslash \{0\})$ is structurally Presburger-definable.*

Proof : Let $\mathcal{A}$ be the minimal DVA that represents $X = \{x \in \mathbb{Z}^m;\ x[i] \in c + n.\mathbb{Z}\}$. There exists a unique integer $k \in \mathbb{N}$ such that $n_0 = \frac{n}{r^k}$ is a r-prime integer (an integer relatively prime with r). Let us consider the set $\mathcal{L}$ of words $\sigma \in (\Sigma_r^m)^k$ such that $\gamma_{r,\sigma}^{-1}(X) \neq \emptyset$. Remark that for any word $\sigma \in \mathcal{L}$, we have $\gamma_{r,\sigma}^{-1}(X) = \{x \in \mathbb{Z}^m;\ r^k.x[i] \in c - \gamma_{r,\sigma}(\mathbf{e}_0)[i] + n.\mathbb{Z}\}$. As $\gamma_{r,\sigma}^{-1}(X) \neq \emptyset$, we deduce that $c_\sigma = \frac{c - \gamma_{r,\sigma}(\mathbf{e}_0)[i]}{r^k}$ is an integer, and in particular we get $\gamma_{r,\sigma}^{-1}(X) = \{x \in \mathbb{Z}^m;\ x[i] \in c_\sigma + n_0.\mathbb{Z}\}$. As n_0 is r-prime, there exists an integer $k_0 \in \mathbb{N}$ such that $r^{k_0} \in 1 + n_0.\mathbb{Z}$. For any $\sigma \in \mathcal{L}$ and for any $(w, s) \in ((\Sigma_r^m)^{k_0})^* \times S_r^m$, we have:

$$\begin{aligned}
\gamma_{r,\sigma.w}^{-1}(X) &= \gamma_{r,w}^{-1}(\{x \in \mathbb{Z}^m;\ x[i] \in c_\sigma + n_0.\mathbb{Z}^m\}) \\
&= \{x \in \mathbb{Z}^m;\ r^{|w|}.x[i] + \gamma_{r,w}(\mathbf{e}_0)[i] \in c_\sigma + n_0.\mathbb{Z}\} \\
&= \{x \in \mathbb{Z}^m;\ x[i] \in c_\sigma + \frac{s}{1-r} - \rho_r(w, s)[i] + n_0.\mathbb{Z}\}
\end{aligned}$$

Let us consider an eye Y of $\mathcal{A}$, let $s \in S_r^m$ be the unique sign vector such that $Y \subseteq Q \times \{s\}$. Let us consider the Presburger-definable set $Z_s = \{\rho_r(\sigma, s);\ \sigma \in (\Sigma_r^m)^*\}$ of vectors with the same sign s.

We first assume that $X_q \neq \emptyset$ for any $(q, s) \in \ker(Y)$. We denote by P the set of $p \in \mathbb{Z}$ such that $\{x \in \mathbb{Z}^m;\ x[i] \in -p + n_0.\mathbb{Z}\} \in \{X_q;\ (q, s) \in \ker(Y)\}$. Remark that P is Presburger-definable because

$P = (P \cap \{0, \dots, n_0 - 1\}) + n_0.\mathbb{Z}$. Moreover, we have:

$$\begin{aligned} x \in X^Y &\iff \exists \sigma \in (\Sigma_r^m)^* \; x = \rho_r(\sigma, s) \wedge (\delta(q_0, \sigma), s) \in Y \\ &\iff \exists \sigma \in \mathcal{L} \; \exists w \in ((\Sigma_r^m)^{k_0})^* \; x = \rho_r(\sigma.w, s) \wedge (\delta(q_0, \sigma.w), s) \in \ker(Y) \\ &\iff \exists \sigma \in \mathcal{L} \; \exists w \in ((\Sigma_r^m)^{k_0})^* \; \begin{cases} x = \gamma_{r,\sigma}(\rho_r(w, s)) \\ \wedge \rho_r(w, s)[i] \in c_\sigma + \frac{s}{1-r} + P \end{cases} \\ &\iff \exists \sigma \in \mathcal{L} \; \exists z \in Z_s \; x = \gamma_{r,\sigma}(z) \wedge z[i] \in c_\sigma + \frac{s}{1-r} + P \end{aligned}$$

We have proved that X^Y is Presburger-definable.

Finally, assume that $X_q = \emptyset$ for at least one $(q, s) \in \ker(Y)$. We have $X^Y = Z_s \backslash \bigcup_{Y' \in \mathcal{C} \backslash \{Y\}} X^{Y'}$ where $\mathcal{C}$ is the set of eyes $Y' \subseteq Q \times \{s\}$. Remark that if there exists an eye $Y' \in \mathcal{C} \backslash \{Y\}$ and $(q', s) \in \ker(Y')$ such that $X_{q'} = \emptyset$, as $\mathcal{A}$ is minimal, we get $q = q'$ and in particular $Y = Y'$ which is impossible. From the previous paragraph, we deduce that $X^{Y'}$ is Presburger-definable for any $Y' \in \mathcal{C} \backslash \{Y\}$. Therefore X^Y is Presburger-definable. Q.E.D

Lemma 3 *The set $X = \{x \in \mathbb{Z}^m;\ \langle \alpha, x \rangle \leq c\}$ where $(\alpha, c) \in (\mathbb{Z}^m \backslash \{0\}) \times \mathbb{Z}$ is structurally Presburger-definable.*

Proof : Let $\mathcal{A}$ be the minimal DVA that represents $X = \{x \in \mathbb{Z}^m;\ \langle \alpha, x \rangle \leq c\}$. For any $(\sigma, s) \in (\Sigma_r^m)^* \times S_r^m$, and for any $k \in \mathbb{N}$, we have:

$$\gamma_{r,\sigma.s^k}^{-1}(X) = \left\{ x \in \mathbb{Z}^m;\ \left\langle \alpha, x - \frac{s}{1-r} \right\rangle \leq \frac{c - \langle \alpha, \rho_r(\sigma, s) \rangle}{r^{|\sigma|+k}} \right\}$$

In particular, for any $(\sigma, s) \in (\Sigma_r^m)^* \times S_r^m$, there exists $k_0 \in \mathbb{N}$ such that for any integer $k \geq k_0$, we have:

$$\gamma_{r,\sigma.s^k}^{-1}(X) = \begin{cases} \{x \in \mathbb{Z}^m;\ \left\langle \alpha, x - \frac{s}{1-r} \right\rangle \leq 0\} & \text{if } \langle \alpha, \rho_r(\sigma, s) \rangle \leq c \\ \{x \in \mathbb{Z}^m;\ \left\langle \alpha, x - \frac{s}{1-r} \right\rangle < 0\} & \text{if } \langle \alpha, \rho_r(\sigma, s) \rangle > c \end{cases}$$

Let us consider an eye Y and the unique sign digit vector $s \in S_r^m$ such that $Y \subseteq Q \times \{s\}$. Let us consider the Presburger-definable set $Z_s = \{\rho_r(\sigma, s);\ \sigma \in (\Sigma_r^m)^*\}$ of vectors with the same sign s.

From the previous equality, we deduce that there exists $\# \in \{<, \leq\}$ such that for any $(q, s) \in \ker(Y)$ we have $X_q = \{x \in \mathbb{Z}^m;\ \left\langle \alpha, x - \frac{s}{1-r} \right\rangle \# 0\}$. In particular $\ker(Y)$ is reduced to $\ker(Y) = \{(q, s)\}$. Let us consider $\#' \in \{\leq, >\}$ such that $(\#, \#') \in \{(\leq, \leq), (<, >)\}$. We have:

$$\begin{aligned} x \in X^Y &\iff \exists \sigma \in (\Sigma_r^m)^* \; (\delta(q, \sigma.s^*), s) \cap \ker(Y) \neq \emptyset \\ &\iff x \in Z_s \wedge \langle \alpha, x \rangle \#' c \end{aligned}$$

Therefore X^Y is Presburger-definable. Q.E.D

Theorem 2 *A set X is structurally Presburger-definable if and only if it is Presburger-definable.*

Proof : Recall that a quantification elimination shows that a Presburger-definable set is a boolean combination in $\mathbb{Z}^m$ of sets of the form $X = \{x \in \mathbb{Z}^m;\ x[i] \in c + n.\mathbb{Z}\}$ and sets of the form $X = \{x \in \mathbb{Z}^m;\ \langle \alpha, x \rangle \leq c\}$. Lemmas 2 and 3 prove that these sets are structurally Presburger-definable. Moreover, as the complement of a structurally Presburger-definable set remains structurally Presburger-definable, it is sufficient to prove that the intersection $X = X_1 \cap X_2$ of two structurally Presburger-definable sets X_1 and X_2 remains structurally Presburger definable. Let $\mathcal{A}_1$, $\mathcal{A}_2$

and $\mathcal{A}'$ be the minimal DVA that represent respectively X_1, X_2 and X. Remark that X is represented by the *Cartesian product* $\mathcal{A} = (Q_1 \times Q_2, \Sigma_r^m, \delta, q_0, F_0)$ where $\delta((q_1, q_2), b) = (\delta_1(q_1, b), \delta_2(q_2, b))$, $q_0 = (q_{1,0}, q_{2,0})$, and $F_0 = F_{1,0} \times F_{2,0}$. Remark that for any eye Y of the DVA $\mathcal{A}'$, there exists a finite sequence $(Y_{1,i}, Y_{2,i})_{i \in I}$ where $Y_{1,i}$ and $Y_{2,i}$ are some eyes of respectivelly $\mathcal{A}_1$ and $\mathcal{A}_2$, such that X^Y is represented by the DVA $\mathcal{A}^{\bigcup_{i \in I} Y_{1,i} \times Y_{2,i}}$. Therefore $X^Y = \bigcup_{i \in I} X_1^{Y_1} \cap X_2^{Y_2}$ is Presburger-definable. In particular X is structurally Presburger-definable. We are done. Q.E.D

4 Future work

We have proved that any Presburger-definable set is structurally Presburger-definable. In particular, the widening operator for DVA introduced by Bartzis and Bultan provides Presburger-definable DVA from the widening of two Presburger-definable DVA. We are interested in extending the geometrical widening operators known for the *closed convex polyhedrons* [10], to the Presburger-definable DVA.

References

[1] Sébastien Bardin, Alain Finkel, Jérôme Leroux, and Laure Petrucci. FAST: Fast Acceleration of Symbolic Transition systems. In *Proc. 15th Int. Conf. Computer Aided Verification (CAV'2003), Boulder, CO, USA, July 2003*, volume 2725 of *Lecture Notes in Computer Science*, pages 118–121. Springer, 2003.

[2] Constantinos Bartzis and Tevfik Bultan. Efficient symbolic representations for arithmetic constraints in verification. *International Journal of Foundations of Computer Science (IJFCS)*, 14(4):605–624, August 2003.

[3] Constantinos Bartzis and Tevfik Bultan. Widening arithmetic automata. In *Proc. 16th Int. Conf. Computer Aided Verification (CAV'2004), Omni Parker House Hotel, Boston, USA, July 2004*, volume 3114 of *Lecture Notes in Computer Science*, pages 321–333. Springer, 2004.

[4] Leonard Berman. Precise bounds for Presburger arithmetic and the reals with addition: Preliminary report. In *Proc. 18th IEEE Symp. Foundations of Computer Science (FOCS'77), Providence, RI, USA, Oct.-Nov. 1977*, pages 95–99, Providence, Rhode Island, 31 October–2 November 1977. IEEE.

[5] Achim Blumensath and Erich Grädel. Finite presentations of infinite structures. In *Proc. 2nd Int. Workshop on Complexity in Automated Deduction (CiAD'2002)*, 2002.

[6] Bernard Boigelot. *Symbolic Methods for Exploring Infinite State Spaces*. PhD thesis, Université de Liège, 1998.

[7] Alexandre Boudet and 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*, volume 1059 of *Lecture Notes in Computer Science*, pages 30–43. Springer, 1996.

[8] Véronique Bruyère, Georges Hansel, Christian Michaux, and Roger Villemaire. Logic and p-recognizable sets of integers. *Bull. Belg. Math. Soc.*, 1(2):191–238, March 1994.

[9] Randal E. Bryant. Symbolic boolean manipulation with ordered binary-decision diagrams. *ACM Computing Surveys*, 24(3):293–318, 1992.

[10] Patrick Cousot and Nicholas Halbwachs. Automatic discovery of linear restraints among variables of a program. In *Conference Record of the Fifth annual ACM Symposium on Priniples of Programming Languages*, pages 84–96. ACM, ACM, January 1978.

[11] Vijay Ganesh, Sergey Berezin, and David 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*, volume 2517 of *Lecture Notes in Computer Science*, pages 171–186. Springer, 2002.

[12] Seymour Ginsburg and Edwin H. Spanier. Semigroups, Presburger formulas and languages. *Pacific J. Math.*, 16(2):285–296, 1966.

[13] 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*, pages 110–119. IEEE Comp. Soc. Press, 2004.

[14] Nils Klarlund, A. Møller, and M. I. Schwartzbach. MONA implementation secrets. *Int. J. of Foundations Computer Science*, 13(4):571–586, 2002.

[15] LASH homepage. `http://www.montefiore.ulg.ac.be/~boigelot/research/lash/`.

[16] 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*, volume 98 of *Electronic Notes in Theor. Comp. Sci.*, pages 89–104. Elsevier Science, 2004.

[17] Jérôme Leroux. A polynomial-time presburger criterion and synthesis for number decision diagrams. In *Proc. 20th Annual IEEE Symposium on Logic in Computer Science (LICS'05), Chicago, USA June 2005*. IEEE Comp. Soc. Press, 2005. to appear.

[18] A. Muchnik. Definable criterion for definability in presburger arithmetic and its applications. (in russian), preprint, Institute of new technologies, 1991.

[19] A. Muchnik. The definable criterion for definability in presburger arithmetic and its applications. *Theoretical Computer Science*, 290:1433–1444, 2003.

[20] OMEGA homepage. `http://www.cs.umd.edu/projects/omega/`.

[21] 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*, pages 92–101, 1929.

[22] Tatiana Rybina and 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*, volume 2422 of *Lecture Notes in Computer Science*, pages 489–494. Springer, 2002.

[23] Pierre Wolper and Bernard Boigelot. An automata-theoretic approach to Presburger arithmetic constraints. In *Proc. 2nd Int. Symp. Static Analysis (SAS'95), Glasgow, UK, Sep. 1995*, volume 983 of *Lecture Notes in Computer Science*, pages 21–32. Springer, 1995.

[24] Pierre Wolper and 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*, volume 1785 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2000.