Jérôme Leroux

Least Significant Digit First Presburger Automata

DRAFT. Please do not distribute, but contact the author for a version

November 2, 2006

Springer

Aux Québécois

Contents

Part II Geometry

Part III From Automata to Presburger Formulas

1

Introduction

Presburger arithmetic [Pre29] is a decidable logic used in a large range of applications. As described in [Lat04], this logic is central in many areas including integer programming problems [Sch87], compiler optimization techniques [Ome], program analysis tools [BGP99, FO97, Fri00] and model-checking [BFL04, Fas, Las]. Different techniques [GBD02] 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 [Kla04] (implemented in Omega [Ome]), by using semi-linear sets [GS66] (implemented in Brain [RV02]), or automata (integer vectors being encoded as strings of digits) [WB95, BC96] (implemented in Fast [BFLP03], Lash [Las] and Mona [KMS02]). Presburger-formulas and semi-linear sets lack canonicity. 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* [Ber77, GS66]. On the other hand, a minimization procedure for automata provides a canonical representation. That means, the automaton that represents a given set only depends on this set and not on the way we compute it. For these reasons, autmata are well adapted for applications that require a lot of boolean manipulations such as model-checking.

Whereas there exist efficient algorithms for computing an automaton that represents the set defined by a given Presburger formula [Kla04, WB00, BC96], the inverse problem of computing a Presburger-formula from a Presburger-definable set represented by an automaton, called the *Presburger synthesis problem*, was first studied in [Ler03] and only *partially solved in exponential time* (resp. *doubly exponential time*) for *convex integer polyhedrons* [Lat04] (resp. for *semi-linear sets with the same set of periods* [Lug04]). Presburger-synthesis has many applications. For example, in software verification, we are interested in computing the set of reachable states of an infinite state system by using automata and in analyzing the structure of these sets with a tool such as [Ome] which manipulates Presburger-formulas. The Presburger-synthesis problem is also central to a new generation of constraint solvers

for Presburger arithmetic that manipulate both automata and Presburger-formulas [Lat04, Kla04].

The Presburger-synthesis problem is naturally related to the problem of deciding whether an autamaton represents a Presburger-definable set, a well-known hard problem first solved by Muchnik in 1991 [Muc91] with a quadruple exponential time algorithm. To the best of our knowledge no better algorithm for the full class of Presburger-definable sets has been proposed since 1991.

In this paper, given an automaton that represents a set X of integer vectors encoded by the least significant digit first decomposition, we prove that we can decide in *polynomial time* whether X is Presburger-definable. Moreover, in this case, we provide an algorithm that computes in *polynomial time* a Presburger-formula that defines X.

2

Notations

We provide in this chapter notations used in the sequel.

2.1 Sets, Functions, and Relations

We denote by $\mathbb{Q}$, $\mathbb{Q}_+$, $\mathbb{Z}$ and $\mathbb{N}$ respectively the set of *rational numbers*, *non-negative rational numbers*, *integers*, and *non-negative integers*.

The *intersection*, *union*, *difference*, and *symmetric difference* of two sets A and B are written $A \cap B$, $A \cup B$, $A \backslash B$, and $A \Delta B = (A \backslash B) \cup (B \backslash A)$.

The *class of subsets* (resp. *the class of finite subsets*) of a set E is denoted by $\mathcal{P}(E)$ (resp. $\mathcal{P}_f(E)$). The *cardinal* of a finite set X is written $|X| \in \mathbb{N}$. A *partition* $\mathcal{C}$ of a set E is a class of non-empty subsets of E such that $X_1 \cap X_2 = \emptyset$ for any $X_1, X_2 \in \mathcal{C}$ and $E = \bigcup_{X \in \mathcal{C}} X$.

The *Cartesian product* of two sets A and B is written $A \times B$. The set X^m is called the *set of vectors* with $m \in \mathbb{N}$ *components* in a set X. Given an integer $i \in \{1, \ldots, m\}$ and a vector $x \in X^m$, the i-th component of x is written $x[i] \in X$.

The set of *functions* $f : X \to Y$, also called *sequences* of elements in Y indexed by X is written Y^X. A function $f \in X^Y$ is said *injective* if $f(x_1) \neq f(x_2)$ for any $x_1 \neq x_2 \in X$, *surjective* if for any $y \in Y$ there exists $x \in X$ such that $y = f(x)$, and *bijective* or *one-to-one* if it is both injective and surjective. A function $f \in Y^X$ is either denoted by $f : X \to Y$, or it is denoted by $f = (f_x)_{x \in X}$ and in this last case Y is implicitly known. Given a function $f : X \to Y$ and two sets A and B, we define $f(A)$ and $f^{-1}(B)$ respectively the *image* and the *inverse image* of A and B by f, given by $f(A) = \{f(x);\ x \in X \cap A\}$ and $f^{-1}(B) = \{x \in X;\ f(x) \in B\}$ (remark that A is not necessary a subset of X and B is not necessary a subset of Y).

An *enumeration* of a set E is an injective function $f : \mathbb{N} \to E$. A *countable set* E is a set E that has an enumeration. Recall that a finite set is countable and the class of finite subsets of a countable set is countable.

Let V be a countable set of *boolean variables*. A *boolean formula* ϕ over the boolean variables V is a formula in the grammar $\phi := v|\phi \cap \phi|\phi \cup \phi|\phi \backslash \phi|\phi \Delta \phi$ where $v \in V$. A *boolean valuation* ρ is a function that maps each boolean variable v to a set $\rho(v)$. Observe that a boolean valuation ρ can be naturally extended to any boolean formula ϕ. Given a boolean formula $\phi(v_1, \ldots, v_n)$ where v_1, ..., v_n are the boolean variables *occurring* in ϕ and some sets E_1, ..., E_n, we denote by $\phi(E_1, \ldots, E_n)$ the unique set $\rho(\phi)$ where ρ is any valuation such that $\rho(v_i) = E_i$. A set E is called a *boolean combination* of sets in a class $\mathcal{C}$ of sets if there exists a boolean formula $\phi(v_1, \ldots, v_n)$ and some sets E_1, ..., E_n in $\mathcal{C}$ such that $E = \phi(E_1, \ldots, E_n)$.

Lemma 2.1. *We can decide in polynomial time if a finite set E is a boolean combination of sets in a finite class $\mathcal{C}$ of finite sets. Moreover, in this case we can compute in polynomial time a boolean formula $\phi(v_1, \ldots, v_n)$ and a sequence E_1, ..., E_n of sets in $\mathcal{C}$ such that $E = \phi(E_1, \ldots, E_n)$.*

Proof. Let us consider an enumeration E_1, ..., E_n of the sets in $\mathcal{C}$ and let $X = \bigcup_{i=1}^{n} E_i$. Let us consider the function $f : X \times \{1, \ldots, n\} \to \mathcal{P}(E)$ such that $f(x, i)$ is the unique set in $\{E_i, X \Delta E_i\}$ that contains x. Let us also consider the set $K_x = \bigcap_{i=1}^{n} f(x, i)$ and observe that E is a boolean combination of sets in $\mathcal{C}$ if and only $E = \bigcup_{e \in E} K_e$. □

A *relation* $\mathcal{R}$ is a subset of $S_1 \times S_2$ where S_1 and S_2 are two sets. We denote by $s_1 \mathcal{R} s_2$ if $(s_1, s_2) \in \mathcal{R}$. Such a relation is said *one-to-one* if there exists a unique $s_2 \in S_2$ such that $s_1 \mathcal{R} s_2$ for any $s_1 \in S_1$, and if there exists a unique $s_1 \in S_1$ such that $s_1 \mathcal{R} s_2$ for any $s_2 \in S_2$. The *concatenation* $\mathcal{R}_1.\mathcal{R}_2$ of two relations $\mathcal{R}_1 \subseteq S_1 \times S_2$ and $\mathcal{R}_2 \subseteq S_2 \times S_3$ is the relation $\mathcal{R}_1.\mathcal{R}_2 \subseteq S_1 \times S_3$ defined by $s_1 \mathcal{R}_1.\mathcal{R}_2 s_3$ if and only if there exists $s_2 \in S_2$ such that $s_1 \mathcal{R}_1 s_2$ and $s_2 \mathcal{R}_2 s_3$. A *binary relation* $\mathcal{R}$ over a set S is a relation $\mathcal{R} \subseteq S_1 \times S_2$ such that $S_1 = S = S_2$. Recall that a binary relation $\mathcal{R}$ over S is an *equivalence* if $\mathcal{R}$ is *reflexive* ($s \mathcal{R} s$ for any s), *symmetric* ($s_1 \mathcal{R} s_2$ if and only if $s_2 \mathcal{R} s_1$ for any $s_1, s_2 \in S$), and *transitive* ($s_1 \mathcal{R} s_2$ and $s_2 \mathcal{R} s_3$ implies $s_1 \mathcal{R} s_3$ for any $s_1, s_2, s_3 \in S$). Given an equivalence binary relation $\mathcal{R}$ over S, the *equivalence class* of an element $s \in S$ is the set of $s' \in S$ such that $s \mathcal{R} s'$. Recall that equivalence classes provide a partition of S.

2.2 Linear Algebra

The *unit vector* $\mathbf{e}_{j,m} \in \mathbb{Q}^m$ where $j \in \{1, \ldots, m\}$ is defined by $\mathbf{e}_{j,m}[j] = 1$ and $\mathbf{e}_{j,m}[i] = 0$ for any $i \in \{1, \ldots, m\} \backslash \{j\}$. The *zero vector* $\mathbf{e}_{0,m} \in \mathbb{Q}^m$ is defined by $\mathbf{e}_{0,m} = (0, \ldots, 0)$.

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 $i \in \{1, \ldots, m\}$, $x, y \in \mathbb{Q}^m$, $t \in \mathbb{Q}$. We naturally define $A + B = \{a + b;\ (a, b) \in A \times B\}$ and $T.A = \{t.a;\ (t, a) \in T \times A\}$ for any $A, B \subseteq \mathbb{Q}^m$

and $T \subseteq \mathbb{Q}$. For any $a, b \in \mathbb{Q}^m$ and $t \in \mathbb{Q}$, let us define $a + B = \{a\} + B$, $A + b = A + \{b\}$, $t.A = \{t\}.A$ and $T.a = T.\{a\}$.

The *infinite norm* of a vector $x \in \mathbb{Q}^m$ is defined by $||x||_\infty = \max_i |x[i]|$ where $|x[i]|$ is the *absolute value* of $x[i]$.

The *dot product* of two vectors $x, y \in \mathbb{Q}^m$ is denoted by $\langle x, y \rangle = \sum_{i=1}^m x[i].y[i]$.

The *greatest common divisor (gcd)* of $m \in \mathbb{N}\backslash\{0\}$ integers x_1, ..., x_m is denoted by $\gcd(x_1, \ldots, x_m)$. Recall that the gcd of of some integers can be efficiently computed in polynomial time thanks to an Euclidean algorithm.

A rational number $q \in \mathbb{Q}$ can be *canonically represented* as a tuple $(n, d) \in \mathbb{Z} \times (\mathbb{N}\backslash\{0\})$ such that $q = \frac{n}{d}$ and $\gcd(n, d) = 1$. The integer $\text{size}(q) \in \mathbb{N}$ is defined as the least (for $\leq$) integer such that $n, d \leq 2^{\text{size}(q)}$. The integer $\text{size}(x) \in \mathbb{N}$ where $x \in \mathbb{Q}^m$ is defined by $\text{size}(x) = \sum_{i=1}^m \text{size}(x[i])$. The integer $\text{size}(X) \in \mathbb{N}$ where $X \in \mathcal{P}_f(\mathbb{Q}^m)$ is defined by $\text{size}(X) = \sum_{x \in X} \text{size}(x)$.

A function $f : \mathbb{Q}^m \to \mathbb{Q}^{m'}$ is said *affine* if for any $i \in \{1, \ldots, m\}$, there exists $v_i \in \mathbb{Q}^m$ and $c_i \in \mathbb{Q}$ such that $f(x)[i] = c_i + \langle v_i, x \rangle$ for any $x \in \mathbb{Q}^m$.

The set of *matrices* with $n \in \mathbb{N}$ *rows* and $m \in \mathbb{N}$ *columns* with *coefficients* in a set $X \subseteq \mathbb{Q}$ is denoted by $\mathcal{M}_{m,n}(X)$. Its elements are denoted by $M[i, j] \in X$ where $1 \leq i \leq n$ and $1 \leq j \leq m$.

2.3 Alphabets, Graphs, and Automata

An *alphabet* Σ is a non-empty finite set. Given an alphabet Σ, we denote by Σ^+ the set of non-empty *words* over Σ. Given a non-empty word $\sigma = b_1 \ldots b_k$ of $k \in \mathbb{N}\backslash\{0\}$ elements $b_i \in \Sigma$, and an integer $i \in \{1, \ldots, k\}$, we denote by $\sigma[i]$ the element $\sigma[i] = b_i$. We denote by ϵ the empty word. As usual Σ^* denotes the set of words $\Sigma^+ \cup \{\epsilon\}$ and a *language* $\mathcal{L}$ is a subset of Σ^*. The *concatenation* of $\sigma_1 \in \Sigma^*$ and $\sigma_2 \in \Sigma^*$ (resp. $\mathcal{L}_1 \subseteq \Sigma^*$ and $\mathcal{L}_2 \subseteq \Sigma^*$) 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 define as usual σ^i where $i \in \mathbb{N}$ and $\sigma^* = \{\sigma^i;\ i \in \mathbb{N}\}$. The *length* of a word $\sigma \in \Sigma^*$ is denoted by $|\sigma| \in \mathbb{N}$. The *residue* $\sigma^{-1}.\mathcal{L}$ of a language $\mathcal{L} \subseteq \Sigma^*$ by a word $\sigma \in \Sigma^*$ is the language $\sigma^{-1}.\mathcal{L} = \{w \in \Sigma^*;\ \sigma.w \in \mathcal{L}\}$.

A *graph G labelled by Σ* is a tuple $G = (Q, \Sigma, \delta)$ such that Q is the non empty *set of states*, Σ is an alphabet and $\delta : Q \times \Sigma \to Q$ is the *transition function*. Two graphs $G_1 = (Q_1, \Sigma, \delta_1)$ and $G_2 = (Q_2, \Sigma, \delta_2)$ labelled by Σ are said *isomorph* by a one-to-one relation $\mathcal{R} \subseteq Q_1 \times Q_2$, if we have $\delta_1(q_1, b)\mathcal{R}\delta_2(q_2, b)$ for any $q_1 \mathcal{R} q_2$ and for any $b \in \Sigma$. As usual, the transition function δ is uniquely extended into a function $\delta : Q \times \Sigma^* \to Q$ such that $\delta(q, \epsilon) = q$ for any $q \in Q$ and such that $\delta(q, \sigma_1.\sigma_2) = \delta(\delta(q, \sigma_1), \sigma_2)$. Given a word $\sigma \in \Sigma^*$, we denote by $\xrightarrow{\sigma}$ the binary relation over Q defined by $q \xrightarrow{\sigma} q'$ if and only if $q' = \delta(q, \sigma)$. In this case, we say that there exists a *path* from a state q to a state q' labelled by σ. Such a path is called a *cycle on q* if $q = q'$ and $\sigma \neq \epsilon$. Given a language $\mathcal{L} \subseteq \Sigma^*$, the binary relation $\xrightarrow{\mathcal{L}}$ is defined by

$\xrightarrow{\mathcal{L}} = \bigcup_{\sigma\in\mathcal{L}} \xrightarrow{\sigma}$. The binary relation $\rightarrow$ is defined by $\rightarrow = \xrightarrow{\Sigma^*}$. A state q' is said *reachable* from a state q_0 if $q_0 \rightarrow q'$. The notion of reachability is naturally extended to the subsets of Q: a subset $Q' \subseteq Q$ is said *reachable* from a subset $Q_0 \subseteq Q$ if the exists a state $q' \in Q'$ reachable from a state $q_0 \in Q_0$. In this case the set Q' is said *co-reachable* from Q. A *strongly connected component* Q' is an equivalence class for the equivalence binary relation $\rightleftarrows$ defined over Q by $q \rightleftarrows q'$ if and only if $q \rightarrow q'$ and $q' \rightarrow q$. A graph G is said *finite* if Q is finite. In this case $|G| = |Q|$ denotes the number of states of G, and the integer $\text{size}(G) \in \mathbb{N}$ is defined by $\text{size}(G) = |\Sigma|.|Q|$.

An *automaton* $\mathcal{A}$ *labelled by* Σ is a tuple $\mathcal{A} = (k_0, K, \Sigma, \delta, K_F)$ such that (K, Σ, δ) is a graph labelled by Σ, $k_0 \in K$ is the *initial state* and $K_F \subseteq K$ is the set of *final states*. Two automata $\mathcal{A}_1 = (k_{0,1}, K_1, \Sigma, \delta_1, K_{F,1})$ and $\mathcal{A}_2 = (k_{0,2}, K_2, \Sigma, \delta_2, K_2)$ labelled by Σ are said *isomorph* by a one-to-one relation $\mathcal{R} \subseteq K_1 \times K_2$ if (K_1, Σ, δ_1) and (K_2, Σ, δ_2) are isomorph by $\mathcal{R}$, $(k_{0,1}, k_{0,2}) \in \mathcal{R}$, and we have $k_1 \in K_{F,1}$ if and only if $k_2 \in K_{F,2}$ for any $(k_1, k_2) \in \mathcal{R}$. An automaton with a finite set of states K is said *finite*. In this case, we denote by $|\mathcal{A}|$ the number of states $|K|$ and the integer $\text{size}(\mathcal{A})$ is defined by $\text{size}(\mathcal{A}) = |\Sigma|.|K|$. The language $\mathcal{L}(\mathcal{A}) \subseteq \Sigma^*$ *recognized* by an automaton $\mathcal{A}$ labelled by Σ is defined by $\mathcal{L}(\mathcal{A}) = \{\sigma \in \Sigma^*;\ \delta(q_0, \sigma) \in K_F\}$. A language $\mathcal{L} \subseteq \Sigma^*$ is said *regular* if it can be recognized by a finite automaton. Recall that a language $\mathcal{L} \subseteq \Sigma^*$ is regular if and only if the set of residues $\{\sigma^{-1}.\mathcal{L};\ \sigma \in \Sigma^*\}$ is finite. In this case the automaton $(\mathcal{L}, K, \Sigma, \delta, K_F)$ defined by the set of states $K = \{\sigma^{-1}.\mathcal{L};\ \sigma \in \Sigma^*\}$, the transition function $\delta(k, b) = b^{-1}.k$ which is in K since $b^{-1}.\sigma^{-1}.\mathcal{L} = (\sigma.b)^{-1}.\mathcal{L}$ and the final set of states $K_F = \{k \in K;\ \epsilon \in k\}$ is the unique (up to isomorphism) *minimal* (for the number of states) automaton labelled by Σ that recognizes $\mathcal{L}$.

Part I

Logic and Automata

3

Finite Digit Vector Automata

In this chapter, the *Finite Digit Vector Automata (FDVA)* representation, a state-based representation of set of integer vectors is presented.

3.1 Digit Vector Decomposition

In this paper, r denotes an integer in $\mathbb{N}\backslash\{0,1\}$ called *basis of decomposition*. The set $\Sigma_r = \{0,\ldots,r-1\}$ is called the set of *r-digits* and the set $S_r = \{0, r-1\} \subseteq \Sigma_r$ is called the set of *r-signs*. Given an integer $m \in \mathbb{N}\backslash\{0\}$ called *dimension*, we intensively used the alphabets $\Sigma_{r,m} = \Sigma_r^m$ and $S_{r,m} = S_r^m$ whose the elements are respectively called the (r,m)-*digit vectors* and the (r,m)-*sign vectors*. Naturally, a word over the alphabet $\Sigma_{r,m}$ can also be seen as a word over the alphabet Σ_r with a length multiple of m. In order to simplify notations, these words are identified. Moreover, given a word $\sigma \in \Sigma_{r,m}^*$, we denote by $|\sigma|_m$ the length of σ seens as a word over the alphabet $\Sigma_{r,m}$ and defined by $|\sigma|_m = \frac{|\sigma|}{m}$, and given a word $\sigma = b_1 \ldots b_k$ of $k \in \mathbb{N}\backslash\{0\}$ (r,m)-digit vectors $b_i \in \Sigma_{r,m}$ and an integer $i \in \{1,\ldots,k\}$, we denote by $\sigma[i]_m$ the (r,m)-digit vector $\sigma[i]_m = b_i$.

A (r,m)-*decomposition* (σ, s) of an integer vector $x \in \mathbb{Z}^m$ is a couple $(\sigma, s) \in \Sigma_{r,m}^* \times S_{r,m}$ corresponding to *a least significant digit first decomposition* of x in basis r. More formally, we have $x = \rho_{r,m}(\sigma, s)$ where $\rho_{r,m} : \Sigma_{r,m}^* \times S_{r,m} \to \mathbb{Z}^m$ is defined by the following equality:

$$\rho_{r,m}(\sigma, s) = r^{|\sigma|_m}.\frac{s}{1-r} + \sum_{i=1}^{|\sigma|_m} r^{i-1}.\sigma[i]_m$$

Example 3.1. $(011, 0)$ is a $(2,1)$-decomposition of $6 = 2^1 + 2^2$.

Example 3.2. $(\epsilon, 1)$, $(1,1)$, $(11,1)$, ..., $(1\ldots1,1)$ are the $(2,1)$-decompositions of -1 and $(\epsilon, 0)$, $(0,0)$, ..., $(0\ldots0,0)$ are the $(2,1)$-decompositions of 0.

Following notations introduced in [Ler04], function $\rho_{r,m}$ can be defined thanks to the unique sequence $(\gamma_{r,m,\sigma})_{\sigma\in\Sigma_r^*}$ 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 any $\sigma_1, \sigma_2 \in \Sigma_r^*$, $\gamma_{r,m,\epsilon}$ is the identity function, and such that $\gamma_{r,m,b}(x)$ is defined for any $(b, x) \in \Sigma_r \times \mathbb{Z}^m$ by the following equality:

$$\gamma_{r,m,b}(x[1], \ldots, x[m]) = (r.x[m] + b, x[1], \ldots, x[m-1])$$

In fact, we deduce that for any (r, m)-decomposition (σ, s), we have the following equality since $\gamma_{r,m,w}(x) = r.x + w$ for any $(w, x) \in \Sigma_{r,m} \times \mathbb{Z}^m$:

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

Function $\rho_{r,m}$ can be used to associate to any language $\mathcal{L} \subseteq \Sigma_{r,m}^* \times S_{r,m}$, the set of integer vectors $X = \rho_{r,m}(\mathcal{L})$. Remark that $\rho_{r,m}$ is a surjective function (we have $\rho_{r,m}(\Sigma_{r,m}^* \times S_{r,m}) = \mathbb{Z}^m$) because any vector $x \in \mathbb{Z}^m$ owns at least one (r, m)-decomposition. Hence, for any subset $X \subseteq \mathbb{Z}^m$, there exists at least one language $\mathcal{L}$ such that $X = \rho_{r,m}(\mathcal{L})$. However, intersection of languages does not correspond to intersection of sets of integer vectors: for instance, consider $\mathcal{L}_1 = \{(0, 0)\}$ and $\mathcal{L}_2 = \{(0.0, 0)\}$ and remark that $\{0\} = \rho_{r,1}(\mathcal{L}_1) \cap \rho_{r,1}(\mathcal{L}_2) \neq \rho_{r,1}(\mathcal{L}_1 \cap \mathcal{L}_2) = \emptyset$. In order to avoid this problem, we introduce the notion of *saturated languages*.

A language $\mathcal{L} \subseteq \Sigma_{r,m}^* \times S_{r,m}$ is said (r, m)-*saturated* if for any (r, m)-decompositions (σ_1, s_1) and (σ_2, s_2) of the same vector, we have $(\sigma_1, s_1) \in \mathcal{L}$ if and only if $(\sigma_2, s_2) \in \mathcal{L}$. Remark that $\Sigma_{r,m}^* \times S_{r,m}$ is a (r, m)-saturated language such that $\rho_{r,m}(\Sigma_{r,m}^* \times S_{r,m}) = \mathbb{Z}^m$, and $\mathcal{L}_1 \# \mathcal{L}_2$ is a (r, m)-saturated language such that $\rho_{r,m}(\mathcal{L}_1 \# \mathcal{L}_2) = \rho_{r,m}(\mathcal{L}_1) \# \rho_{r,m}(\mathcal{L}_2)$ for any pair $(\mathcal{L}_1, \mathcal{L}_2)$ of (r, m)-saturated languages, and for any $\# \in \{\cup, \cap, \setminus, \Delta\}$.

The (r, m)-decompositions of the same integer vector are characterized by the following lemma 3.3.

Lemma 3.3. *Two (r, m)-decompositions (σ_1, s_1) and (σ_2, s_2) represent the same integer vector if and only if $s_1 = s_2$ and $\sigma_1.s_1^* \cap \sigma_2.s_2^* \neq \emptyset$.*

Proof. Consider two (r, m)-decompositions (σ_1, s_1) and (σ_2, s_2) such that there exists $s \in S_{r,m}$ and $k_1, k_2 \in \mathbb{N}$ satisfying $s_1 = s = s_2$ and $\sigma_1.s_1^{k_1} = \sigma_2.s_2^{k_2}$, and let us prove that (σ_1, s_1) and (σ_2, s_2) represent the same vector. Just remark that $\gamma_{r,m,s}(\frac{s}{1-r}) = \frac{s}{1-r}$ for any $s \in S_{r,m}$. Hence, an immediate induction (over k_1 and k_2) shows that (σ_1, s_1) and (σ_2, s_2) represent the same vector.

For the converse, consider two (r, m)-decompositions (σ_1, s_1) and (σ_2, s_2) that represent the same vector. Remark that for any (r, m)-decomposition (σ, s) of an integer vector $x \in \mathbb{Z}^m$, we have $s[i] = 0$ if $x[i] \in \mathbb{N}$ and $s[i] = r-1$ if $x[i] \in \mathbb{Z}\setminus\mathbb{N}$ for any $i \in \{1, \ldots, m\}$. Therefore, as (σ_1, s_1) and (σ_2, s_2) represents the same vector, we deduce that there exists $s \in S_{r,m}$ such that $s_1 = s = s_2$. Consider k_1 and k_2 such that $|\sigma_1| + k_1 = |\sigma_2| + k_2$. From the first paragraph, we deduce that (w_1, s) and (w_2, s) represent the same vector where $w_1 = \sigma_1.s_1^{k_1}$ and $w_2 = \sigma_2.s_2^{k_2}$. By uniqueness of the (r, m)-decompositions with a fixed length, we deduce that $w_1 = w_2$. □

3.2 State-based Decomposition

A language of (r, m)-decompositions can be naturally represented by a state-based representation. Our representation is obtain by considering the natural one-to-one function from the set of (r, m)-decompositions to the set of words in $\Sigma_{r,m}^*.\Diamond.S_{r,m}$ that associate to a (r, m)-decomposition (σ, s) the word $\sigma.\Diamond.s$ where $\Diamond$ is an additional letter not in Σ_r.

Observe that an automaton $\mathcal{A}$ recognizing a language included in $\Sigma_{r,m}^*.\Diamond.S_{r,m}$ can be decomposed into (1) a graph called *Digit Vector Graph* corresponding to the part of $\mathcal{A}$ before a $\Diamond$ letter, and the part of $\mathcal{A}$ after a $\Diamond$ letter called a *final function*.

Definition 3.4. *A* Digit Vector Graph (DVG) *is a tuple* $G = (Q, m, K, \Sigma_r, \delta)$ *where* Q *is the non empty set of* principal states*,* $r \in \mathbb{N}\backslash\{0, 1\}$ *is the* basis of decomposition*,* $m \in \mathbb{N}\backslash\{0\}$ *is the* dimension*, and* (K, Σ_r, δ) *is a graph such that* $Q \subseteq K$ *and* $\delta(Q, \Sigma_{r,m}) \subseteq Q$*.*

A *Finite Digit Vector Graph (FDVG)* G is a DVG with a finite set of states K. Given a FDVG G, the integer size$(G) \in \mathbb{N}$ is defined by size$(G) = r.|K|$. The *parallelization* $[G]$ of a DVG $G = (Q, m, K, \Sigma_r, \delta)$ is the graph $[G] = (Q, \Sigma_{r,m}, \delta)$. We introduce DVG rather than graph labelled by $\Sigma_{r,m}$ in order to establish fine polynomial time complexity results that should be useless with an exponential size in m of the alphabet $\Sigma_{r,m}$. Naturally any graph labelled by $\Sigma_{r,m}$ is equal to the parallelization of at least one DVG in basis r and in dimension m.

Definition 3.5. *A* final function *is a tuple* $F = (Q, f, m, K, S_r, \delta, K_F)$ *where* Q *is the non empty set of* principal states*,* $r \in \mathbb{N}\backslash\{0, 1\}$ *is the* basis of decomposition*,* $m \in \mathbb{N}\backslash\{0\}$ *is the* dimension*,* (K, S_r, δ) *is a* finite *graph,* $f : Q \to K$ *is a function mapping principal states to states in* K*, and* $K_F \subseteq K$ *is the set of* final states *such that the language recognized by the automaton* $(f(q), K, S_r, \delta, K_F)$ *is a subset of* $S_{r,m}$ *for any principal state* $q \in Q$*.*

A final function F is said *finite* if the set of principal states Q is *finite* (observe that K is finite by definition). Given a finite final function F, the integer size$(F) \in \mathbb{N}$ is defined by size$(F) = |Q| + |K|$. The *parallelization* $[F]$ of a final function $F = (Q, f, m, K, S_r, \delta, K_F)$ is the function $[F] : Q \to \mathcal{P}(S_{r,m})$ such that $[F](q)$ is the language recognized by the automaton $(f(q), K, S_r, \delta, K_F)$.

A DVG G and a final function F are said *compatible* if they are defined over the same set of principal states with the same basis r and the same dimension m. Given a tuple (q, G, F) where q is a principal state, G is a DVG and F is a final function compatible, we denote by $\mathfrak{L}((q, G, F))$ the following language of (r, m)-decompositions:

$$\mathfrak{L}((q, G, F)) = \{(w, s) \in \Sigma_{r,m}^* \times S_{r,m};\ s \in [F](\delta(q, w))\}$$

Recall that we are interested in recognizing (r, m)-saturated languages. A final function F is said *saturated* for a DVG G if it is compatible with G and if $\mathfrak{L}((q, G, F))$ is (r, m)-saturated for any principal states $q \in Q$.

Proposition 3.6. *A final function F is saturated for a DVG G if and only if F and G are compatible and $[F](q_1) \cap \{s\} = [F](q_2) \cap \{s\}$ for any $q_1 \xrightarrow{s} q_2$ with $(q_1, s, q_2) \in Q \times S_{r,m} \times Q$.*

Proof. Assume first that $\mathfrak{L}((q, G, F))$ is (r, m)-saturated for any state $q \in Q$, and let us prove that $s \in [F](q_1)$ if and only if $s \in [F](q_2)$ for any $q_1 \xrightarrow{s} q_2$ with $(q_1, s, q_2) \in Q \times S_{r,m} \times Q$. Assume first that $s \in [F](q_1)$. Lemma 3.3 proves that $\rho_{r,m}(\epsilon, s) = \rho_{r,m}(s, s)$. As $\mathfrak{L}((q_1, G, F))$ is (r, m)-saturated, we deduce that $(s, s) \in \mathfrak{L}((q_1, G, F))$. From $q_2 = \delta(q_1, s)$ we get $s \in [F](q_2)$. Next assume that $s \in [F](q_2)$. We get $(s, s) \in \mathfrak{L}((q_1, G, F))$. As this language is (r, m)-saturated and $\rho_{r,m}(s, s) = \rho_{r,m}(\epsilon, s)$, we deduce that $(\epsilon, s) \in \mathfrak{L}((q_1, G, F))$. Therefore $s \in [F](q_1)$.

Next, assume that $[F](q_1) \cap \{s\} = [F](q_2) \cap \{s\}$ for any $q_1 \xrightarrow{s} q_2$ with $(q_1, s, q_2) \in Q \times S_{r,m} \times Q$, and let us prove that $\mathfrak{L}((q, G, F))$ is (r, m)-saturated for any state $q \in Q$. Let us consider two (r, m)-decomposition (σ, s) and (σ', s') of the same integer vector such that $(\sigma', s') \in \mathfrak{L}((q, G, F))$ and let us prove that $(\sigma, s) \in \mathfrak{L}((q, G, F))$. From lemma 3.3, we deduce that $s = s'$ and there exists $k, k' \in \mathbb{N}$ such that $\sigma.s^k = \sigma'.s^{k'}$. As $s \in \mathfrak{L}((q_1, G, F))$ if and only if $s \in \mathfrak{L}(q_2, G, F)$ for any $q_1 \xrightarrow{s} q_2$ with $q_1, q_2 \in Q$, an immediate induction shows that $(\sigma', s') \in \mathfrak{L}((q, G, F))$ implies $(\sigma, s) \in \mathfrak{L}((q, G, F))$. Therefore $\mathfrak{L}((q, G, F))$ is (r, m)-saturated for any $q \in Q$. □

We can now introduce our definition of digit vector automata.

Definition 3.7. *A* Digit Vector Automaton (DVA) *is a tuple $\mathcal{A} = (q_0, G, F_0)$ where $q_0 \in Q$ is the* initial state*, G is a DVG and F_0 is a final function saturated for G.*

A *Finite Digit Vector Automaton (FDVA)* $\mathcal{A}$ is a DVA with a finite DVG G and a finite final function F. Given a FDVA $\mathcal{A}$, the integer size($\mathcal{A}$) is defined by size($\mathcal{A}$) = size(G) + size(F). Given a DVA $\mathcal{A} = (q_0, G, F_0)$, the (r, m)-saturated language $\mathfrak{L}(\mathcal{A}) = \mathfrak{L}((q_0, G, F_0))$ is called the *recognized language* of $\mathcal{A}$. The set $X = \rho_{r,m}(\mathfrak{L}(\mathcal{A}))$ is called the set of integer vectors *represented* by $\mathcal{A}$.

Let us show that any set $X \subseteq \mathbb{Z}^m$ can be represented by a DVA by introducing the DVG $G_{r,m}(X) = (Q_{r,m}(X), m, K_{r,m}(X), \Sigma_r, \delta_{r,m})$ where $K_{r,m}(X) = \{\gamma^{-1}_{r,m,w}(X);\ w \in \Sigma_r^*\}$, $Q_{r,m}(X) = \{\gamma^{-1}_{r,m,w}(X);\ w \in \Sigma_{r,m}^*\}$, and $\delta_{r,m}$ is defined by $\delta_{r,m}(Y, b) = \gamma^{-1}_{r,m,b}(Y)$ for any $Y \in K_{r,m}(X)$ and $b \in \Sigma_r$. Finally, let us consider the tuple $\mathcal{A}_{r,m}(X) = (X, G_{r,m}(X), F_{r,m})$ where $F_{r,m}$ is any final function such that $[F_{r,m}](Y) = S_{r,m} \cap (1-r).Y$ for any $Y \in Q_{r,m}(X)$.

Proposition 3.8. *The tuple $\mathcal{A}_{r,m}(X)$ is a DVA in basis r and in dimension m that represents X.*

Proof. Let us first prove that $\mathcal{A}_{r,m}(X)$ is a DVA in basis r and in dimension m. It is sufficient to show that $[F_{r,m}](q_1) \cap \{s\} = [F_{r,m}](q_2) \cap \{s\}$ for any $q_1 \xrightarrow{s} q_2$ where $(q_1, s, q_2) \in Q \times S_{r,m} \times Q$. As $q_1 \xrightarrow{s} q_2$, we get $q_2 = \gamma^{-1}_{r,m,s}(q_1)$.

Remark that $[F_{r,m}](q_1) = S_{r,m} \cap (1-r).q_1$ and $[F_{r,m}](q_2) = S_{r,m} \cap (1-r).q_2$. As $\gamma_{r,m,s}(\frac{s}{1-r}) = \frac{s}{1-r}$, we deduce that $[F_{r,m}](q_1) \cap \{s\} = [F_{r,m}(q_2)] \cap \{s\}$. We are done.

Now, let X' be the set represented by the DVA $\mathcal{A}_{r,m}(X)$, and let us prove that $X' = X$. Let $x \in X'$. There exists a (r,m)-decomposition (σ, s) of x such that $(\sigma, s) \in \mathcal{L}(\mathcal{A}_{r,m}(X))$. Let $q = \delta_{r,m}(q_0, \sigma)$. We get $q = \gamma^{-1}_{r,m,\sigma}(X)$. From $s \in [F_{r,m}](q)$, we deduce $s \in S_{r,m} \cap (1-r).q$. Hence $\frac{s}{1-r} \in q = \gamma^{-1}_{r,m,\sigma}(X)$ and we obtain $\gamma_{r,m,\sigma}(\frac{s}{1-r}) \in X$. As $\rho_{r,m}(\sigma, s) = x$, we get $x \in X$ and we have proved the inclusion $X' \subseteq X$. For the converse inclusion, let $x \in X$. Let us consider a (r,m)-decomposition (σ, s) of x. As $x = \rho_{r,m}(\sigma, s)$ and $\rho_{r,m}(\sigma, s) = \gamma^{-1}_{r,m,\sigma}(X)$, we get $s \in S_{r,m} \cap (1-r).q$ where $q = \gamma^{-1}_{r,m,\sigma}(X)$. Therefore $q_0 \xrightarrow{\sigma} q$ and $s \in [F_{r,m}](q)$. That means $\rho_{r,m}(\sigma, s) \in X'$ and we have proved the other inclusion $X \subseteq X'$. $\square$

4

Modifying a DVA

The sets obtained by *moving the initial state* of a DVA are geometrically characterized in section 4.1 and the set obtained by *modifying the final function* of a DVA are studied in section 4.2.

4.1 Moving the initial state

The DVA obtained from $\mathcal{A}$ by replacing the initial state q_0 by another principal state $q \in Q$ is denoted by $\mathcal{A}_q$. Given a set X implicitly represented by a DVA $\mathcal{A}$ with a set of principal states Q, we denote by X_q the set represented by the DVA $\mathcal{A}_q$. In this section the set X_{q_2} is geometrically characterized in function of X_{q_1} for any path $q_1 \xrightarrow{w} q_2$ where $(q_1, w, q_2) \in Q \times \Sigma_{r,m}^* \times Q$.

Proposition 4.1. *Let X be a set represented by a DVA in basis r and in dimension m with a set Q of principal states. We have $X_{q_2} = \gamma_{r,m,w}^{-1}(X_{q_1})$ for any path $q_1 \xrightarrow{w} q_2$ where $(q_1, w, q_2) \in Q \times \Sigma_{r,m}^* \times Q$.*

Proof. Consider $x \in X_{q_2}$. There exists $(\sigma, s) \in \mathfrak{L}(\mathcal{A}_{q_2})$ such that $x = \rho_{r,m}(\sigma, s)$. From $(w.\sigma, s) \in \mathfrak{L}(\mathcal{A}_{q_1})$, we deduce that $\rho_{r,m}(w.\sigma, s) \in X_{q_2}$. Just remark that $\rho_{r,m}(w.\sigma, s) = \gamma_{r,m,w}(\rho_{r,m}(\sigma, s)) = \gamma_{r,m,w}(x)$. We have proved that $X_{q_2} \subseteq \gamma_{r,m,w}^{-1}(X_{q_1})$. For the converse, consider $x \in \gamma_{r,m,w}^{-1}(X_{q_1})$. As any vector owns at least one (r,m)-decomposition, there exists a (r,m)-decomposition (σ, s) such that $x = \rho_{r,m}(\sigma, s)$. From $x \in \gamma_{r,m,w}^{-1}(X_{q_1})$, we get $\gamma_{r,m,w}(x) \in X_{q_1}$. Just remark that $\gamma_{r,m,w}(x) = \rho_{r,m}(w.\sigma, s)$. As $\mathfrak{L}(\mathcal{A}_{q_1})$ is (r,m)-saturated, we get $(w.\sigma, s) \in \mathfrak{L}(\mathcal{A}_{q_1})$. In particular $(\sigma, s) \in \mathfrak{L}(\mathcal{A}_{q_2})$. Hence $x = \rho_{r,m}(\sigma, s) \in X_{q_2}$. We have proved the other inclusion $\gamma_{r,m,w}^{-1}(X_{q_1}) \subseteq X_{q_2}$. □

Theorem 4.2. *Let X be a Presburger-definable set represented by a DVA $\mathcal{A} = (q_0, G, F_0)$. The set X_q is Presburger-definable for any reachable (for $[G]$) principal state $q \in Q$.*

Proof. The proof is immediate because if X is Presburger-definable, there exists a formula ϕ in $\mathrm{FO}(\mathbb{Z}, \mathbb{N}, +)$ that defines X. Consider a reachable (for $[G]$) principal state $q \in Q$. There exists a path $q_0 \xrightarrow{\sigma} q$ with $\sigma \in \Sigma_{r,m}^*$. From proposition 4.1, we deduce that X_q is defined by the Presburger formula $\phi_\sigma(x) := \exists y;\ (y = \gamma_{r,m,\sigma}(x) \wedge \phi(y))$. Therefore X_q is Presburger-definable. □

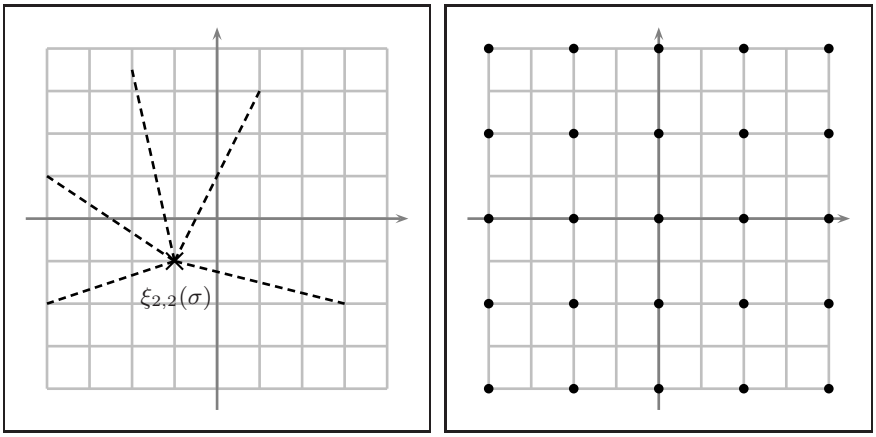

Fig. 4.1. On the left, $\Gamma_{2,2,\sigma}^{-1}$ with its fix-point $\xi_{2,2}(\sigma)$. On the right $\Gamma_{2,2,(0,0)}(\mathbb{Z}^2)$

Previous proposition 4.1 provides a characterization of the sets obtained by moving the initial state of a DVA to another principal state. This characterization can be translated into a geometrical one by considering the unique sequence $(\Gamma_{r,m,w})_{w\in\Sigma_r^*}$ of affine functions $\Gamma_{r,m,w} : \mathbb{Q}^m \to \mathbb{Q}^m$ such that $\Gamma_{r,m,w_1.w_2} = \Gamma_{r,m,w_1} \circ \Gamma_{r,m,w_2}$ for any $(w_1, w_2) \in \Sigma_r^*$, such that $\Gamma_{r,m,\epsilon}$ is the identity function and such that $\Gamma_{r,m,b}(x)$ is defined for any $(b, x) \in \Sigma_r \times \mathbb{Q}^m$ by the following equality:

$$\Gamma_{r,m,b}(x[1], \ldots, x[m]) = (r.x[m] + b, x[1], \ldots, x[m-1])$$

As $\gamma_{r,m,\sigma}(x) = \Gamma_{r,m,\sigma}(x)$ for any $x \in \mathbb{Z}^m$, we deduce that $\gamma_{r,m,\sigma}^{-1}(X) = \Gamma_{r,m,\sigma}^{-1}(X \cap \Gamma_{r,m,\sigma}(\mathbb{Z}^m))$. Now, just remark that given $\sigma \in \Sigma_{r,m}^*$, $\Gamma_{r,m,\sigma}(x) = r^{|\sigma|_m}.x + \gamma_{r,m,\sigma}(\mathbf{e}_{0,m})$ is simply a *scaling function* (an affine function of the form $x \to \mu.x + v$ where $\mu \in \mathbb{Q}\backslash\{0\}$ and $v \in \mathbb{Q}^m$) and $\Gamma_{r,m,\sigma}(\mathbb{Z}^m) = r^{|\sigma|}.\mathbb{Z}^m + \gamma_{r,m,\sigma}(\mathbf{e}_{0,m})$ is a *pattern* (see figure 4.1 and section 9.3).

Remark 4.3. Function $\Gamma_{r,m,w}$ is the unique affine function that *extends* $\gamma_{r,m,w}$: there exists a unique affine function $f : \mathbb{Q}^m \to \mathbb{Q}^m$ such that $f(x) = \gamma_{r,r,w}(x)$ for any $x \in \mathbb{Z}^m$.

The following lemma introduces the geometrically characterized vectors $\xi_{r,m}(\sigma)$ that will be useful in the sequel.

Lemma 4.4. *The function* $\xi_{r,m} : \Sigma_{r,m}^+ \to \mathbb{Q}^m$ *defined by* $\xi_{r,m}(\sigma) = \frac{\gamma_{r,m,\sigma}(\mathbf{e}_{0,m})}{1-r^{|\sigma|_m}}$ *is the unique function such that* $\xi_{r,m}(\sigma)$ *is a fix-point of* $\Gamma_{r,m,\sigma}$ *for any* $\sigma \in \Sigma_{r,m}^+$.

Proof. Remark that $\xi_{r,m}(\sigma)$ is a fix-point of $\Gamma_{r,m,\sigma}$, and if x is a fix-point of $\Gamma_{r,m,\sigma}$, then $r^{|\sigma|_m}.x + \gamma_{r,m,\sigma}(\mathbf{e}_{0,m}) = x$ and we deduce that $x = \xi_{r,m}(\sigma)$. □

In the sequel the sets $X \subseteq \mathbb{Z}^m$ such that there exists $\sigma \in \Sigma_{r,m}^+$ satisfying $\gamma_{r,m,\sigma}^{-1}(X) = X$ are useful since intuitively $\xi_{r,m}(\sigma)$ is a fix point of these sets. Such a set is said (r, m, σ)-*cyclic*.

4.2 Replacing the final function

Given a set X implicitly represented by a DVA $\mathcal{A} = (q_0, G, F_0)$ and given a final function F saturated for G, we denote by X^F the set represented by the DVA $\mathcal{A}^F$ obtained from $\mathcal{A}$ by replacing F_0 by F.

4.2.1 Detectable sets

A set $X' \subseteq \mathbb{Z}^m$ is said (r, m)-*detectable* in a set $X \subseteq \mathbb{Z}^m$ if $\gamma_{r,m,\sigma_1}^{-1}(X') = \gamma_{r,m,\sigma_2}^{-1}(X')$ for any words $\sigma_1, \sigma_2 \in \Sigma_{r,m}^*$ such that $\gamma_{r,m,\sigma_1}^{-1}(X) = \gamma_{r,m,\sigma_2}^{-1}(X)$. The following theorem 4.5 shows that these sets characterize the sets $X' \subseteq \mathbb{Z}^m$ such that for any DVA $\mathcal{A} = (q_0, G, F_0)$ that represents X, there exists a final function F saturated for G such that $X' = X^F$.

Theorem 4.5. *A set* $X' \subseteq \mathbb{Z}^m$ *is* (r, m)*-detectable in a set* $X \subseteq \mathbb{Z}^m$ *if and only if for any DVA* $\mathcal{A}$ *that represents* X*, there exists a final function* F *saturated for* G *such that* $X' = X^F$.

Proof. Assume first that for any DVA $\mathcal{A} = (q_0, G, F_0)$ that represents X, there exists a final function F saturated for G such that $X' = X^F$. Let us consider the DVA $\mathcal{A}_{r,m}(X) = (X, G_{r,m}(X), F_{r,m})$ where $G_{r,m}(X) = (Q_{r,m}(X), m, K_{r,m}(X), \Sigma_r, \delta_{r,m})$. There exists $F : Q_{r,m}(X) \to \mathcal{P}(S_{r,m})$ such that X' is represented by the DVA $(X, G_{r,m}(X), F)$. Consider $\sigma_1, \sigma_2 \in \Sigma_{r,m}^*$ such that $\gamma_{r,m,\sigma_1}^{-1}(X) = \gamma_{r,m,\sigma_2}^{-1}(X)$. By definition of $\mathcal{A}_{r,m}(X)$, there exists $Y \in Q_{r,m}(X)$ such that $\delta_{r,m}(X, \sigma_1) = Y = \delta_{r,m}(X, \sigma_2)$. Proposition 4.1 proves that $\gamma_{r,m,\sigma_1}^{-1}(X') = X_Y^F = \gamma_{r,m,\sigma_2}^{-1}(X')$. Therefore X' is (r, m)-detectable in X.

Next, assume that X' is (r, m)-detectable in X and let us consider a DVA $\mathcal{A} = (q_0, G, F_0)$ that represents X where $G = (Q, m, K, \Sigma_r, \delta)$. Let F be a final function over Q such that $[F](q) = \{s \in S_{r,m}; \exists \sigma \in \Sigma_{r,m}^*;\ \delta(q_0, \sigma) \in \delta(q, s^*) \wedge \rho_{r,m}(\sigma, s) \in X'\}$.

Let us first prove that F is saturated for G. Consider a transition $q \xrightarrow{s} q'$ 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 $s \in [F](q)$. We deduce that there exists $\sigma \in \Sigma_{r,m}^*$, and integer $k \in \mathbb{N}$ such that $\delta(q_0, \sigma) = \delta(q, s^k)$ and $\rho_{r,m}(\sigma, s) \in X'$. From $\delta(q_0, \sigma.s) = \delta(q', s^k)$ and $\rho_{r,m}(\sigma.s, s) = \rho_{r,m}(\sigma, s) \in X'$, we deduce that $s \in [F](q')$. Let us prove the converse and assume now that $s \in [F](q')$. There exists a word $\sigma \in \Sigma_r^*$, an integer $k \in \mathbb{N}$ such that $\delta(q_0, \sigma) = \delta(q', s^k)$ and such that $\rho_{r,m}(\sigma, s) \in X'$. Just remark that $\delta(q_0, \sigma.s) = \delta(q, s^{k+1})$ and $\rho_{r,m}(\sigma.s, s) = \rho_{r,m}(\sigma, s) \in X'$. Hence $s \in [F](q)$. We have proved that F is saturated for G.

By construction of F, we have $X' \subseteq X^F$. Let us prove the converse inclusion. Consider a vector $x \in X^F$. There exists a (r, m)-decomposition $(w, s) \in \mathfrak{L}_{q_0}^F$ such that $\rho_{r,m}(w, s) = x$. Let $q = \delta(q_0, w)$. We get $s \in [F](q)$. That means there exists $\sigma \in \Sigma_{r,m}^*$ such that $\delta(q_0, \sigma) \in \delta(q, s^*)$ and such that $\rho_{r,m}(\sigma, s) \in X'$. By replacing w by a word in $w.s^*$, we can assume that $\delta(q_0, \sigma) = q$. From $\delta(q_0, \sigma) = \delta(q_0, w)$, proposition 4.1 shows that $\gamma_{r,m,\sigma}^{-1}(X) = \gamma_{r,m,w}^{-1}(X)$. As X' is detectable in X, we get $\gamma_{r,m,\sigma}^{-1}(X') = \gamma_{r,m,w}^{-1}(X')$. Moreover, as $\rho_{r,m}(\sigma, s) \in X'$, we deduce from the previous equality that $x = \rho_{r,m}(w, s) \in X'$. We have proved the other inclusion $X^F \subseteq X'$. □

The following proposition will be useful for deciding if a set X' is (r, m)-detectable in a set X represented by a DVA $\mathcal{A}$ in basis r.

Proposition 4.6. *Let us consider a FDVA $\mathcal{A}$ in dimension m in basis r with n states. We can compute in polynomial time a set U of at most $r.m.n$ pairs (σ_1, σ_2) of words in $\Sigma_r^{\leq n}$ satisfying $|\sigma_1| + m.\mathbb{Z} = |\sigma_2| + m.\mathbb{Z}$ for any $(\sigma_1, \sigma_2) \in U$, and such that for any set $X' \subseteq \mathbb{Z}^m$, there exists a final function F such that X' is represented by $\mathcal{A}^F$ if and only if $\gamma_{r,m,\sigma_1}^{-1}(X') = \gamma_{r,m,\sigma_2}^{-1}(X')$ for any $(\sigma_1, \sigma_2) \in U$.*

Proof. We first show that for any $z \in \mathbb{N}$ and for any $X \subseteq \mathbb{Z}^m$ we have $\bigcup_{\sigma \in \Sigma_r^z} \gamma_{r,m,\sigma}(\gamma_{r,m,\sigma}^{-1}(X)) = X$. Naturally $\gamma_{r,m,\sigma}(\gamma_{r,m,\sigma}^{-1}(X)) \subseteq X$ for any word $\sigma \in \Sigma_r^*$ and in particular we get the inclusion $\bigcup_{\sigma \in \Sigma_r^z} \gamma_{r,m,\sigma}(\gamma_{r,m,\sigma}^{-1}(X)) \subseteq X$. For the converse inclusion, let $x \in X$. There exists a (r, m)-decomposition (w, s) of x and by replacing w by a word in $w.s^*$, we can assume that $|w| \geq z$. In particular there exists a decomposition of w into $w = \sigma.w'$ where $\sigma \in \Sigma_r^z$. Since $\rho_{r,m}(\sigma.w', s) = \gamma_{r,m,\sigma}(\rho_{r,m}(w', s))$ and $\rho_{r,m}(\sigma.w', s) = x \in X$, we deduce that $\rho_{r,m}(w', s) \in \gamma_{r,m,\sigma}^{-1}(X)$ and hence $x \in \gamma_{r,m,\sigma}(\gamma_{r,m,\sigma}^{-1}(X))$. We have proved the converse inclusion.

Let S be the set of couples $s = (k, Z) \in K \times \mathbb{Z}/m.\mathbb{Z}$ such that there exists a word $\sigma_s \in \Sigma_r^*$ satisfying $s = (\delta(q_0, \sigma_s), |\sigma_s| + m.\mathbb{Z})$, and let $(\sigma_s)_{s \in S}$ be a sequence of words satisfying the previous condition, $\sigma_{(q_0, m.\mathbb{Z})} = \epsilon$ and $|\sigma_s| < n$ for any $s \in S$. Observe that such a sequence $(\sigma_s)_{s \in S}$ is computable in polynomial time. Let us consider the set U of pairs $(\sigma_{s_1}.b, \sigma_{s_2})$ where $s_1 = (k_1, Z_1)$, $s_2 = (k_2, Z_2)$ are in S and $b \in \Sigma_r$ satisfies $s_2 = (\delta(k_1, b), Z_1 + 1)$.

Note that U is computable in polynomial time and it contains at most $r.m.n$ pairs (σ_1, σ_2) of words in $\Sigma_r^{\leq n}$ satisfying $|\sigma_1| + m.\mathbb{Z} = |\sigma_2| + m.\mathbb{Z}$ for any $(\sigma_1, \sigma_2) \in U$.

Assume first that there exists a final function F such that X' is represented by $\mathcal{A}^F$ and let us prove that $\gamma^{-1}_{r,m,\sigma_1}(X') = \gamma^{-1}_{r,m,\sigma_2}(X')$ for any $(\sigma_1, \sigma_2) \in U$. Remark that it sufficient to prove that $\gamma^{-1}_{r,m,\sigma_1}(X') = \gamma^{-1}_{r,m,\sigma_2}(X')$ for any pair (σ_1, σ_2) of words in Σ_r^* such that there exists $s = (k, Z) \in U$ satisfying $(\delta(q_0, \sigma_1), |\sigma_1| + m.\mathbb{Z}) = s = (\delta(q_0, \sigma_2), |\sigma_2| + m.\mathbb{Z})$. There exists $z \in \{0, \ldots, m-1\}$ such that $Z + z = m.\mathbb{Z}$. Since $\delta(q_0, \sigma_1) = \delta(q_0, \sigma_2)$ we deduce that $\delta(q_0, \sigma_1.\sigma) = \delta(q_0, \sigma_2.\sigma)$ for any word $\sigma \in \Sigma_r^z$. As $\sigma_1.\sigma$ and $\sigma_2.\sigma$ are both in $\Sigma_{r,m}^*$, proposition 4.1 shows that $\gamma^{-1}_{r,m,\sigma_1.\sigma}(X') = \gamma^{-1}_{r,m,\sigma_2.\sigma}(X')$. Thus $\gamma^{-1}_{r,m,\sigma}(X'_1) = \gamma^{-1}_{r,m,\sigma}(X'_2)$ for any $\sigma \in \Sigma_r^z$ where $X'_1 = \gamma^{-1}_{r,m,\sigma_1}(X')$ and $X'_2 = \gamma^{-1}_{r,m,\sigma_2}(X')$. We have proved that $\bigcup_{\sigma \in \Sigma^z_{r,m}} \gamma_{r,m,\sigma}(\gamma^{-1}_{r,m,\sigma}(X'_1)) = \bigcup_{\sigma \in \Sigma^z_r} \gamma_{r,m,\sigma}(\gamma^{-1}_{r,m,\sigma}(X'_2))$. From the first paragraph we get $X'_1 = X'_2$.

Next assume that $\gamma^{-1}_{r,m,\sigma_1}(X') = \gamma^{-1}_{r,m,\sigma_2}(X')$ for any $(\sigma_1, \sigma_2) \in U$ and let us prove that there exists a final function F such that X' is represented by $\mathcal{A}^F$. As previously, it is sufficient to prove that $\gamma^{-1}_{r,m,\sigma_1}(X') = \gamma^{-1}_{r,m,\sigma_2}(X')$ for any pair (σ_1, σ_2) of words in Σ_r^* such that there exists $s = (k, Z) \in S$ satisfying $(\delta(q_0, \sigma_1), |\sigma_1| + m.\mathbb{Z}) = s = (\delta(q_0, \sigma_2), |\sigma_2| + m.\mathbb{Z})$. Let us remark that it is sufficient to prove that $\gamma^{-1}_{r,m,\sigma}(X') = \gamma^{-1}_{r,m,\sigma_s}(X')$ for any $\sigma \in \Sigma_r^*$ where $s = (\delta(q_0, \sigma), |\sigma| + m.\mathbb{Z})$. Let us consider a sequence b_1, ..., b_i of r-digits $b_j \in \Sigma_r$ such that $\sigma = b_1 \ldots b_i$ and let $s_j = (\delta(q_0, b_1 \ldots b_j), j + m.\mathbb{Z}) \in S$ for any $j \in \{0, \ldots, i\}$. By hypothesis, we have $\gamma^{-1}_{r,m,\sigma_{s_{j-1}}.b_j}(X') = \gamma^{-1}_{r,m,\sigma_{s_j}}(X')$. In particular $\gamma^{-1}_{r,m,\sigma_{s_{j-1}}.b_j \ldots b_i}(X') = \gamma^{-1}_{r,m,\sigma_{s_j}.b_{j+1} \ldots b_i}(X')$ for any $j \in \{1, \ldots, i\}$. We deduce that $\gamma^{-1}_{r,m,\sigma_{s_0}.b_1 \ldots b_i}(X') = \gamma^{-1}_{r,m,\sigma_{s_i}}(X')$. Since $\sigma_{s_0} = \epsilon$, $\sigma = b_1 \ldots b_j$ and $s_i = s$, we have proved that $\gamma^{-1}_{r,m,\sigma}(X') = \gamma^{-1}_{r,m,\sigma_s}(X')$. □

Let $Z_{r,m,s}$ be the set of vectors $x \in \mathbb{Z}^m$ having a (r,m)-decomposition of the form (σ, s) where $\sigma \in \Sigma_{r,m}^*$. This set is defined by the follwoing Presburger-formula:

$$\Big(\bigwedge_{i;\ s[i]=0} x[i] \geq 0\Big) \wedge \Big(\bigwedge_{i;\ s[i]=r-1} x[i] < 0\Big)$$

The sets $Z_{r,m,s}$ naturally appear as (r,m)-detectable sets as shown by the following proposition 4.7 that characterize these sets.

Proposition 4.7. *A set is (r,m)-detectable in any set $X \subseteq \mathbb{Z}^m$ if and only if it is equal to a union of $Z_{r,m,s}$.*

Proof. Let us consider a finite set $\mathcal{L} \subseteq S_{r,m}$ and a DVA $\mathcal{A}$ that represents a set X and just remark that $\bigcup_{s \in \mathcal{L}} Z_{r,m,s}$ is represented by the DVA $\mathcal{A}^F$ where F is a final function such that $[F](q) = \mathcal{L}$ for any $q \in Q$. Therefore $\bigcup_{s \in \mathcal{L}} Z_{r,m,s}$ is (r,m)-detectable in any set $X \subseteq \mathbb{Z}^m$. Conversely, let us consider a set X' that is (r,m)-detectable in any set X. As $\emptyset$ is represented by a DVA with one unique principal state q_0, and X' is (r,m)-detectable in $\emptyset$, we deduce that

there exists a final function F such that X' is represented by $\mathcal{A}^F$. Therefore $X' = \bigcup_{s\in[F](q_0)} Z_{r,m,s}$. □

Example 4.8. The set $X_1 \# X_2$ is (r,m)-detectable in X for any (r,m)-detectable sets X_1, X_2 in X, and for any $\# \in \{\cup, \cap, \setminus, \Delta\}$. Thus, any boolean combination of sets (r,m)-detectable in X is (r,m)-detectable in X.

4.2.2 Eyes and kernel

Consider a FDVG $G = (Q, m, K, \Sigma_r, \delta)$. Given a (r,m)-sign vector $s \in S_{r,m}$, let us consider the equivalence relation $\sim_s$ over the principal states Q defined by $q_1 \sim_s q_2$ if and only if $\delta(q_1, s^*) \cap \delta(q_2, s^*) \neq \emptyset$. An equivalence class $Y \subseteq Q$ for $\sim_s$ is called an *s-eye* (or just an *eye*). Given an s-eye Y, we denote $F_{s,Y} : Q \to \mathcal{P}(S_{r,m})$ a final function defined by $[F_{s,Y}](q) = \{s\}$ if $q \in Y$ and defined by $[F_{s,Y}](q) = \emptyset$ otherwise. Notice that a final function $F : Q \to \mathcal{P}(S_{r,m})$ is saturated for G if and only if $[F]$ is a finite union of final functions $[F_{s,Y}]$.

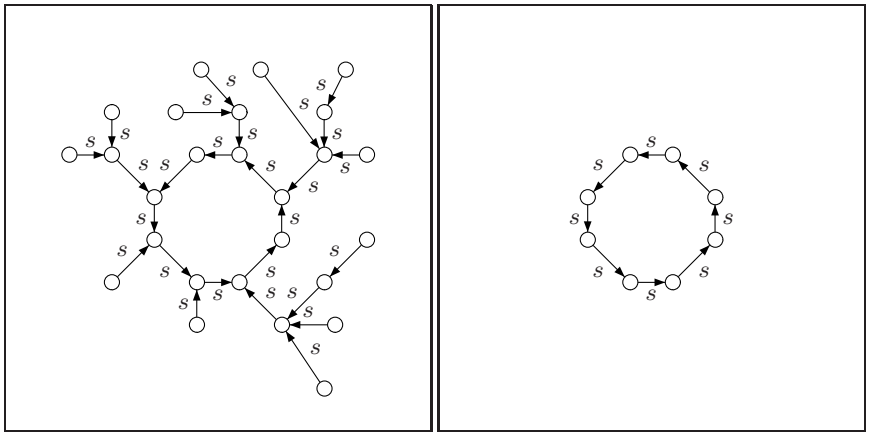

Fig. 4.2. On the left an s-eye. On the right its s-kernel.

The *s-kernel* $\ker_s(Y)$ of an s-eye $Y \subseteq Q$ is defined by $\ker_s(Y) = \bigcap_{i\in\mathbb{N}} \delta(Y, s^i)$. Remark that the s-kernel of an s-eye Y is a non empty set of the form $\ker_s(Y) = \{q_1, \ldots, q_k\}$ such that $q_1 \xrightarrow{s} q_2 \ldots q_k \xrightarrow{s} q_1$ (see figure 4.2).

5

Expressiveness

The expressiveness of the FDVA representation is studied in this section. We first prove in section 5.1 that a subset of $\mathbb{Z}^m$ can be represented by a FDVA if and only if it is r-definable [BHMV94]. Next in section section 5.2, we show that the *Number Decision Diagram (NDD)* [WB00] representation, an other state-based symbolic representation for subsets of $\mathbb{Z}^m$ is slightly equivalent (up to polynomial time translation) to the FDVA.

5.1 Sets r-definable

Recall [BHMV94] that a set $X \subseteq \mathbb{Z}^m$ is said *r-definable* if it can be defined in the first order theory $\mathrm{FO}(\mathbb{Z}, \mathbb{N}, +, V_r)$ 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 $x \in \mathbb{Z}\backslash\{0\}$. Note [BHMV94] that a subset $X \subseteq \mathbb{N}^m$ is definable in $\mathrm{FO}(\mathbb{N}, +, V_r)$ if and only if the language $\{\sigma \in \Sigma_{r,m}^*;\ \rho_{r,m}(\sigma, \mathbf{e}_{0,m})\}$ is regular. We are going to prove that a set $X \subseteq \mathbb{Z}^m$ can be represented by a FDVA in basis r if and only if it is r-definable by decomposing such a set into sets of the form $f_{r,m,s}(X_s)$ where $X_s \subseteq \mathbb{N}^m$, $s \in S_{r,m}$ is a (r,m)-sign vector, and $f_{r,m,s}$ is the function given in the following definition.

Definition 5.1. *Given a (r,m)-sign vector $s \in S_{r,m}$, we denote by $f_{r,m,s} : \mathbb{Z}^m \to \mathbb{Z}^m$ the function defined for any $x \in \mathbb{Z}^m$ and for any $i \in \{1, \ldots, m\}$ by:*

$$f_{r,m,s}(x)[i] = \begin{cases} x[i] & \text{if } s[i] = 0 \\ -1 - x[i] & \text{otherwise} \end{cases}$$

Remark that $X = \bigcup_{s \in S_{r,m}} f_{r,m,s}(X_s)$ where $X_s = \mathbb{N}^m \cap f_{r,m,s}(X)$. The following two propositions 5.2 and 5.3 shows that a FDVA that represents X_s is computable in linear time from a FDVA that represents X.

Proposition 5.2. *For any (r,m)-sign vectors $s \in S_{r,m}$, a FDVA that represents $f_{r,m,s}(X)$ in basis r is computable in time $O(m.size(\mathcal{A}))$ from a FDVA $\mathcal{A}$ that represents a set $X \subseteq \mathbb{Z}^m$ in basis r.*

Proof. Let us consider a FDVA $\mathcal{A} = (q_0, G, F_0)$ that represents X in basis r. Without loss of generality, we can assume that G and F_0 share the same set of states K and the same transition function δ. That means $G = (Q, m, K, S_r, \delta)$ and $F = (Q, f, m, K, S_r, \delta, K_F)$.

Let us first assume that there exists a function $l : K \to \mathbb{Z}/m.\mathbb{Z}$ such that $l(k') = l(k) + 1$ for any transition $k \xrightarrow{b} k'$ where $(k, b, k') \in K \times \Sigma_r \times K$, such that $l(q_0) = 1$ and $l(f(q)) = 1$ for any $q \in Q$. Let us consider the two bijective functions $t_{r,0}, t_{r,r-1} : \Sigma_r \to \Sigma_r$ where $t_{r,0}$ is the identity function and $t_{r,r-1}(b) = r-1-b$ for any $b \in \Sigma_r$. By replacing the function δ in G and F_0 by the function δ' given by $\delta'(k, b) = \delta(k, t_{r,s[l(k)]}(b))$ we deduce a DVG G' and a final function F' such that the DVA $\mathcal{A}' = (q_0, G', F')$ represents $f_{r,m,s}(X)$ in basis r. This result is well know and the proof is left to the reader.

In the general case, if the labeling function l does not exist, by multiplying the size of $\mathcal{A}$ by m, a DVA $\mathcal{A}''$ that represents X in basis r and owns a labelling function l can be easily obtained. Hence, we are done. □

Proposition 5.3. *A FDVA that represents $\mathbb{N}^m \cap X$ in basis r is computable in linear time from a FDVA that represents a set $X \subseteq \mathbb{Z}^m$ in basis r.*

Proof. Let us consider a FDVA $\mathcal{A} = (q_0, G, F_0)$ that represents X. Remark that in linear time we can compute a final function F with the set Q of principal states such that $[F](q) = \{\mathbf{e}_{0,m}\}$ if $\mathbf{e}_{0,m} \in [F_0](q)$ and $[F](q) = \emptyset$ otherwise. Now, just remark that $\mathbb{N}^m \cap X$ is represented by the FDVA (q_0, G, F). □

We can easily deduce the following theorem 5.4.

Theorem 5.4. *A set $X \subseteq \mathbb{Z}^m$ can be represented by a FDVA in basis r if and only if it is r-definable.*

Proof. Assume first that X is r-definable and let us prove that X can be represented by a FDVA in basis r. As X is r-definable, the set $X_s = \mathbb{N}^m \cap f_{r,m,s}(X)$ is r-definable for any $s \in S_{r,m}$. As $X_s \subseteq \mathbb{N}^m$, from [BHMV94] we deduce that $\{\sigma \in \Sigma_{r,m}^*;\ \rho_{r,m}(\sigma, \mathbf{e}_{0,m}) \in X_s\}$ is regular. Therefore X_s can be represented by a FDVA in basis r. From proposition 5.2 we deduce that $f_{r,m,s}(X_s)$ can be represented by a FDVA in basis r. Therefore $X = \bigcup_{s \in S_{r,m}} f_{r,m,s}(X_s)$ can be represented by a FDVA in basis r. For the converse, assume that X is represented by a FDVA in basis r and let us prove that X is r-definable. From propositions 5.2 and 5.3 we deduce that $X_s = \mathbb{N}^m \cap f_{r,m,s}(X)$ can be represented by a FDVA in basis r. As $X_s \subseteq \mathbb{N}^m$, from [BHMV94] we deduce that X_s is r-definable. As $X = \bigcup_{s \in S_{r,m}} f_{r,m,s}(X_s)$, we deduce that X is r-definable. □

Remark 5.5. We can easily prove that for any set $X \subseteq \mathbb{Z}^m$, the set X is r-definable if and only if the DVA $\mathcal{A}_{r,m}(X)$ is finite and moreover in this case it is the unique (up to isomorphism) minimal (for the total number of states) FDVA that represents X in basis r.

5.2 Number Decision Diagrams (NDD)

Recall [WB00] that a *Number Decision Diagram (NDD)* $\mathcal{A}$ in basis r and in dimension m that represents a r-definable set $X \subseteq \mathbb{Z}^m$ is a finite automaton over the alphabet Σ_r that recognizes the regular language $\{\sigma.s;\ (\sigma, s) \in \rho_{r,m}^{-1}(X)\}$. We do not consider NDD 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 a NDD is not a NDD anymore, and (2) rather than replacing the final function F_0 of a FDVA $\mathcal{A}$ by another final function F is structurally obvious, the corresponding operation over NDD is not immediate since the FDVG G and the finite final function F_0 are encoded into a single automaton. Nevertheless, polynomial time algorithms provided in this paper can be applied to NDD thanks to the following translation proposition 5.6.

Proposition 5.6. *A NDD that represents X in a basis r is computable in quadratic time from a FDVA that represents a set X in basis r. Conversely, a FDVA that represents X in basis r is computable in linear time from a NDD that represents a set X in basis r.*

Proof. Let us consider a letter $\Diamond$ not in Σ_r and let us consider the one-to-one function $f : \Sigma_{r,m}^*.\Diamond.S_{r,m} \to \Sigma_{r,m}^*.S_{r,m}$. It is sufficient to show that (1) a finite automaton that recognizes $\mathcal{L}' = f(\mathcal{L})$ is computable in quadratic time from a finite automaton that recognizes a language $\mathcal{L} \subseteq \Sigma_{r,m}^*.\Diamond.S_{r,m}$, and (2) a finite automaton that recognizes $\mathcal{L} = f^{-1}(\mathcal{L}')$ is computable in linear time from a finite automaton that recognizes a language $\mathcal{L}' \subseteq \Sigma_{r,m}^*.S_{r,m}$. These two computations are immediate. □

6

Some Examples of FDVA

The FDVA $\mathcal{A}_{r,1}(\mathbb{Z})$, $\mathcal{A}_{r,1}(\mathbb{N})$, $\mathcal{A}_{r,3}(+)$ and $\mathcal{A}_{r,2}(V_r)$, are given in figures 6.1, 6.2 and 6.3. Remark that a principal state $q \in Q$ is labelled by the set X_q (in fact a formula in FO $(\mathbb{Z}, \mathbb{N}, +, V_r)$ defining X_q), and a dot-edge from q to $[F_0](q)$ is drawn for each state $q \in Q$ such that $[F_0](q) \neq \emptyset$.

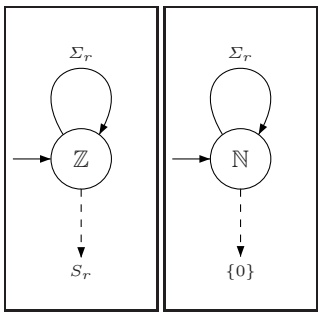

Fig. 6.1. On the left, FDVA $\mathcal{A}_{r,1}(\mathbb{Z})$. On the right, FDVA $\mathcal{A}_{r,1}(\mathbb{N})$

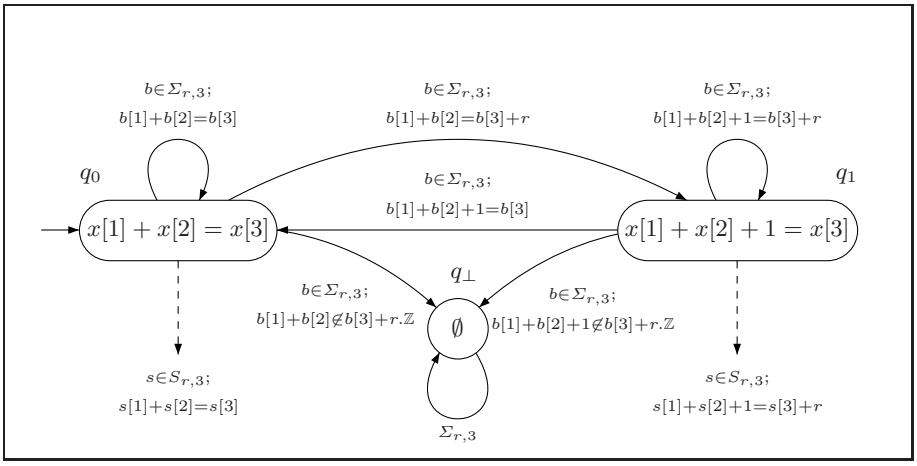

Fig. 6.2. The FDVA $\mathcal{A}_{r,3}(\{x \in \mathbb{Z}^3;\ x[1]+x[2]=x[3]\})$

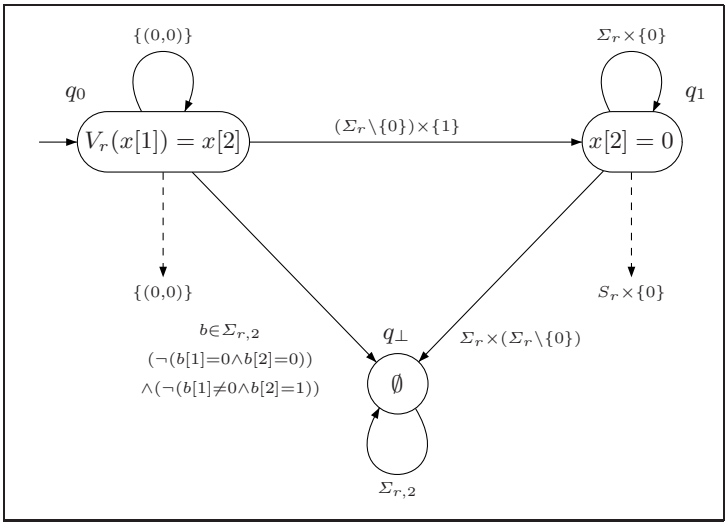

Fig. 6.3. FDVA $\mathcal{A}_{r,2}(\{x \in \mathbb{Z}^2;\ V_r(x[1])=x[2]\})$

7

Reductions

In this section, we prove that the problem of deciding if the set X represented by a FDVA $\mathcal{A}$ is Presburger-definable and in this case the problem of computing a Presburger formula that defines X can be reduced in polynomial time to:

- the cyclic case: there exists a loop on the initial state q_0. In particular the set X represented by $\mathcal{A}$ is cyclic from proposition 4.1.
- the positive case: the final function F_0 is such that $[F_0](q) \in \{\emptyset, \{\mathbf{e}_{0,m}\}\}$. In particular $X \subseteq \mathbb{N}^m$.

7.1 Cyclic reduction

Given a word $\sigma \in \Sigma_{r,m}^+$, a set $X \subseteq \mathbb{Z}^m$ is said (r, m, σ)-*cyclic* (or just *cyclic*) if $\gamma_{r,m,\sigma}^{-1}(X) = X$ and a DVA $\mathcal{A}$ is said (r, m, σ)-*cyclic* (or just *cyclic*) if $\delta(q_0, \sigma) = q_0$. From proposition 4.1, we deduce that the set represented by a (r, m, σ)-cyclic DVA $\mathcal{A}$ is (r, m, σ)-cyclic. Conversely, remark that if a set X is (r, m, σ)-cyclic then the DVA $\mathcal{A}_{r,m}(X)$ is (r, m, σ)-cyclic. The notion of cyclic sets is useful in the sequel for reducing some problems to the special cyclic case since a cyclic Presburger-definable set can be defined by a Presburger formula of a very particular form (see lemma 7.2).

Remark 7.1. The first application of the cyclic reduction is the positive reduction given in section 7.2.

Lemma 7.2. *For any (r, m, σ)-cyclic Presburger-definable set X, there exists an integer $n \in \mathbb{N}\backslash\{0\}$ relatively prime with r such that X can be defined by a formula equal to a boolean combination of formulas of the form $\langle \alpha, x - \xi_{r,m}(\sigma) \rangle < 0$ where $\alpha \in \mathbb{Z}^m$ and formulas of the form $x \in b + n.\mathbb{Z}^m$ where $b \in \mathbb{Z}^m$.*

Proof. A quantification elimination shows that there exists an integer $n_0 \in \mathbb{N}\backslash\{0\}$ and a finite set $D_0 \subseteq \mathbb{Z}^m \times \mathbb{Z}$ such that X can be defined by a formula equal to a boolean combination of formulas of the from $\langle \alpha, x\rangle < c$ where $(\alpha, c) \in D_0$ and $x \in b + n_0.\mathbb{Z}^m$ where $b \in \mathbb{Z}^m$. Remark that there exists an integer $k \in \mathbb{N}$ enough larger such that $n = \frac{n_0}{\gcd(n_0, r^{|\sigma^k|_m})}$ is relatively prime with r and such that the rational number $\beta_{\alpha,c} = r^{-|\sigma^k|_m}.((r-1).c - \langle \alpha, \rho_{r,m}(\sigma, \mathbf{e}_{0,m})\rangle)$ satisfies $|\beta_{\alpha,c}| < 1$ for any $(\alpha, c) \in D_0$. As $\gamma^{-1}_{r,m,\sigma^k}(X) = X$, we deduce that X can be defined by a formula equal to a boolean combination of formulas of the form $\left\langle \alpha, \gamma_{r,m,\sigma^k}(x)\right\rangle < c$ where $(\alpha, c) \in D_0$ and $\gamma_{r,m,\sigma^k}(x) \in b + n_0.\mathbb{Z}^m$ where $b \in \mathbb{Z}^m$. Now remark that $\left\langle \alpha, \gamma_{r,m,\sigma^k}(x)\right\rangle < c$ is equivalent to $\langle \alpha, (r-1).x + \rho_{r,m}(\sigma, \mathbf{e}_{0,m})\rangle < \beta_{\alpha,c}$. Since $\langle \alpha, (r-1).x + \rho_{r,m}(\sigma, \mathbf{e}_{0,m})\rangle \in \mathbb{Z}$ and $|\beta_{\alpha,c}| < 1$, we have proved that $\left\langle \alpha, \gamma_{r,m,\sigma^k}(x)\right\rangle < c$ is equivalent to $\langle \alpha, x - \xi_{r,m}(\sigma)\rangle < 0$ if $\beta_{\alpha,c} < 0$ and it is equivalent to $\neg \langle -\alpha, x - \xi_{r,m}(\sigma)\rangle < 0$ if $\beta_{\alpha,c} \geq 0$. Finally, remark that $\gamma_{r,m,\sigma}(x) \in b + n_s.\mathbb{Z}^m$ is either false if $b \notin n.\mathbb{Z}^m$ or equivalent to a formula of the form $x \in b' + n.\mathbb{Z}^m$ where $b' \in \mathbb{Z}^m$ otherwise. □

Lemma 7.3. *From an automaton $\mathcal{A}$ over Σ_r that represents a finite language $\mathcal{L} \subseteq \Sigma^*_{r,m}$, we can compute in polynomial time a Presburger formula ϕ that defines $\rho_{r,m}(\mathcal{L}, \boldsymbol{e}_{0,m})$.*

Proof. Let us consider a finite automaton $\mathcal{A} = (q_0, Q, \Sigma_r, \delta, Q_F)$ that recognizes $\mathcal{L}$. We denote by $\mathcal{A}_q$ the automaton obtained from $\mathcal{A}$ by replacing the initial state q_0 by an other state $q \in Q$. Let us remark that $\mathcal{L} \subseteq \Sigma_r^{\leq |Q|}$ since otherwise $\mathcal{L}$ is infinite thanks to the *pumping lemma*. For any $k \in \{0, \ldots, |Q|\}$, we can compute in polynomial time a finite automaton that recognizes $\mathcal{L} \cap \Sigma_r^k$. Hence, without loss of generality, we can assume that there exists $k \in \mathbb{N}$ such that $\mathcal{L} \subseteq \Sigma_r^k$. The cases $k = 0$ or $\mathcal{L} = \emptyset$ are left to the reader. Since $\mathcal{L} \subseteq \Sigma^*_{r,m}$ and $\mathcal{L}$ is not empty and included in $\Sigma^k_{r,m}$, we deduce that m divides k. Let $n = \frac{k}{m}$ and remark that $x \in \rho_{r,m}(\mathcal{L}, \mathbf{e}_{0,m})$ if and only if there exists a sequence b_1, ..., b_k of integers in Σ_r such that $\bigwedge_{j=1}^m x[j] = \sum_{i=0}^{n-1} b_{j+m.i}.r^i$ and such that $\delta(q_0, b_1 \ldots b_k) \in Q_F$. Now remark that this last property can be translated into a Presburger formula in polynomial time. □

Proposition 7.4. *Let $X \subseteq \mathbb{Z}^m$ be a set represented by a FDVA $\mathcal{A}$ in basis r and let Q_c be the set of principal states reachable for $[G]$ that have a loop. The set X is Presburger-definable if and only if X_{q_c} is Presburger-definable for any $q_c \in Q_c$. Moreover, from a sequence of Presburger formulas $(\phi_{q_c})_{q_c \in Q_c}$ such that ϕ_{q_c} defines X_{q_c}, we can compute in polynomial time a Presburger formula ϕ that defines X.*

Proof. Assume first that X is Presburger-definable. Recall that we have proved that X_q is Presburger-definable for any principal state q reachable for $[G]$. In particular X_{q_c} is Presburger-definable for any $q_c \in Q_c$. Next, assume that X_{q_c} is defined by a Presburger formula ϕ_{q_c} for any $q_c \in Q_c$

and let us prove that we can compute in polynomial time a Presburger formula ϕ that defines X. For any $k \in \{0, \dots, |Q|-1\}$ and for any $q \in Q$, we can compute in polynomial time an automaton $\mathcal{A}_{k,q}$ over Σ_r that recognizes $\mathcal{L}_{k,q} = \{\sigma \in \Sigma_{r,m}^k;\ \delta(q_0, \sigma) = q\}$. From lemma 7.3 we can compute in polynomial time a Presburger formula ϕ_{k,q_c} that defines the set $X_{k,q_c} = \rho_{r,m}(\mathcal{L}_{k,q_c}, \mathbf{e}_{0,m})$. Let us prove that X is defined by the Presburger formula $\phi(x) := \bigvee_{q_c \in Q_c} \bigvee_{k=0}^{|Q|-1} (\exists y\ \exists z\ ((x = r^k.y + z) \wedge \phi_{q_c}(y) \wedge \phi_{k,q_c}(z)))$. Let $x \in X$. There exists a (r,m)-decomposition (w,s) of x such that $|w|_m \geq m.|Q|$. In this case, w can be decomposed in $w = \sigma.w'$ where $\sigma \in \Sigma_{r,m}^{\leq |Q|}$ is such that there exists a loop on $q_c = \delta(q_0.\sigma)$ and $w' \in \Sigma_r^*$. From $x = \gamma_{r,m,\sigma}(x')$ where $x' = \rho_{r,m}(w', s)$ and $x \in X$, we deduce that $x' \in \gamma_{r,m,\sigma}^{-1}(X) = X_{q_c}$. Let $k = |\sigma|_m$. From $x = r^k.x' + \rho_{r,m}(\sigma, \mathbf{e}_{0,m}) \in r^k.X_{q_C} + X_{k,q_c}$ we deduce that $\phi(x)$ is true. For the converse, consider $x \in \mathbb{Z}^m$ such that $\phi(x)$ is true. There exists $(q_c, k) \in Q_C \times \{0, \dots, |Q|-1\}$, $x' \in X_{q_c}$ and a word $\sigma \in \mathcal{L}(\mathcal{A}_{k,q_c})$ such that $x = r^k.x' + \rho_{r,m}(\sigma, \mathbf{e}_{0,m})$. Let us consider a (r,m)-decomposition (w', s) of x'. As $|\sigma|_m = k$, we deduce that $x' = \gamma_{r,m,\sigma}(x)$. As $q_0 \xrightarrow{\sigma} q_c$, we have $X_{q_c} = \gamma_{r,m,\sigma}^{-1}(X)$. Hence $x \in \gamma_{r,m,\sigma}(\gamma_{r,m,\sigma}^{-1}(X)) \subseteq X$. We have proved that $x \in X$. $\square$

7.2 Positive reduction

The following proposition 7.5 and proposition 5.2 provide the positive reduction since a set S satisfying the following proposition 7.5 is computable in quadratic time.

Proposition 7.5. *Let $\mathcal{A}$ be a FDVA that represents a set $X \subseteq \mathbb{Z}^m$. Let us consider a set S of (r,m)-sign vectors such that $S \cap (F_0(q) \Delta F_0(q')) \neq \emptyset$ for any state $q, q' \in Q$ such that $F_0(q) \Delta F_0(q') \neq \emptyset$. The set X is Presburger-definable if and only if the set $\mathbb{N}^m \cap f_{r,m,s}(X)$ is Presburger-definable for any $s \in S$. Moreover from a sequence of Presburger formulas $(\phi_s)_{s \in S}$ such that ϕ_s defines $X_s = \mathbb{N}^m \cap f_{r,m,s}(X)$, we can compute in polynomial time a Presburger formula ϕ that defines X.*

Proof. Naturally, if X is Presburger-definable, then $X_s = \mathbb{N}^m \cap f_{r,m,s}(X)$ is Presburger-definable for any $s \in S$. Let us prove the converse. Form proposition 7.4, we can assume that there exists a loop on the initial state. Consider a sequence $(\phi_s)_{s \in S}$ of Presburger formulas ϕ_s that defines X_s. Let us consider the function sign : $\mathbb{Z}^m \to S_{r,m}$ that associate to any vector $x \in \mathbb{Z}^m$ the unique (r,m)-sign vector $s \in S_{r,m}$ such that there exists $x \in Z_{r,m,s}$.

Let us consider the following Presburger formula $\theta_s(x,k)$ and remark that $\theta_s(x,k)$ is true if and only if $x + k.\frac{s - \text{sign}(x)}{1-r} \in Z_{r,m,s} \cap X$. We denote by $K_{s,x}$ the Presburger-definable set $K_{s,x} = \{k \in \mathbb{Z};\ \theta_s(x,k)\}$. Since $K_{s,x}$ is a Presburger definable set included in $\mathbb{Z}$, there exists a unique minimal integer $n_{s,x} \in \mathbb{N} \backslash \{0\}$ such that there exists a finite set $B_{s,x} \subseteq \{0, \dots, n_{s,x} - 1\}$ and

an integer $k_{s,x} \in \mathbb{Z}$ such that $K_{s,x} \cap (k_{s,x} + \mathbb{N}) = k_{s,x} + B_{s,x} + n_{s,x}.\mathbb{N}$. Let us prove that $n_{s,x}$ is relatively prime with r. From lemma 7.2, we deduce that there exists an integer n_s relatively prime with r such that $Z_{r,m,s} \cap X$ can be defined by a formula equal to a boolean combination of formulas of the form $\langle \alpha, x \rangle < c$ and $x \in b + n_s.\mathbb{Z}^m$. Now, just remark that $n_{s,x}$ divides n_s. We deduce that $n_{s,x}$ is relatively prime with r.

$$\theta_s(x,k) := \exists y\ \phi_s \circ f_{r,m,s}(y) \wedge \bigwedge_{i=1}^{m} \begin{pmatrix} (x[i] \geq 0 \Longrightarrow y[i] = x[i] + k.\frac{s[i]}{1-r}) \\ \vee\ (x[i] < 0 \Longrightarrow y[i] = x[i] + k.\frac{s[i]-(r-1)}{1-r}) \end{pmatrix}$$

Let us consider the Presburger formula $W_s(x,n) := n \geq 1 \wedge \exists k_0\ \forall k \geq k_0;\ \theta_s(x,k) \iff \theta_s(x,k+n)$. Remark that $W_s(x,n)$ is true if and only if $n \in n_{s,x}.(\mathbb{N}\backslash\{0\})$.

Next, let us denote by Q_s the set of principal states $q \in Q$ such that $s \in [F_0](q)$. Observe that we can compute in polynomial time the partition $\mathcal{C}$ of Q corresponding to the equivalence relation $\sim$ defined by $q_1 \sim q_2$ if and only if $F_0[q_1] = F_0[q_2]$. Given $C \in \mathcal{C}$, remark that $[F_0](q)$ does not depend on $q \in C$ and we can denote by $[F_0](C)$ the unique subset of $S_{r,m}$ such that $[F_0](C) = [F_0](q)$ for any $q \in C$. From lemma 2.1, we deduce that for any $C \in \mathcal{C}$ there exists a boolean formula $\mathcal{R}_C$ computable in polynomial time such that C is defined by $\mathcal{R}_C([F_0](q)_{s \in S})$.

We are going to prove that X is defined by the following Presburger formula $\phi(x)$:

$$\phi(x) := \bigvee_{C \in \mathcal{C}} (\mathrm{sign}(x) \in [F_0](C) \wedge \forall N\ \exists n \geq N\ \mathcal{R}_C(\theta_s(x, 1+n) \wedge W_s(x,n))_{s \in S})$$

Let us consider $x \in \mathbb{Z}^m$ such that $\phi(x)$ is satisfied and let us prove that $x \in X$. There exists $C \in \mathcal{C}$ such that $\mathrm{sign}(x) \in [F_0](C)$ and for any N there exists $n \geq N$ such that $\mathcal{R}_C(\theta_s(x, 1+n))_{s \in S}$ and $W_s(x,n)$ are true. Let us consider $N = k_{s,x} - 1$ and let $n \geq N$ be such that $\mathcal{R}_C(\theta_s(x, 1+n))_{s \in S}$ and $W_s(x,n)$ are true. Since $W_s(x,n)$ is true, we deduce that $n \in n_{s,x}.(\mathbb{N}\backslash\{0\})$. Let us consider a (r,m)-decomposition (σ_0, s_0) of x_0 such that $r^{|\sigma_0|_m} \geq k_{s,x}$ for any $s \in S$. Since $n_{s,x}$ is relatively prime with r, by replacing σ_0 by a word in $\sigma_0.s_0^*$, we can assume that $r^{|\sigma_0|_m} \in 1 + n_{s,x}.\mathbb{Z}$. Since $1+n$ and $r^{|\sigma_0|_m}$ are both greater than $k_{s,x}$ and the difference of these two integers $(1+n) - (r^{|\sigma_0|_m})$ is in $n_{s,x}.\mathbb{Z}$, we deduce that $\theta_s(x, 1+n)$ is equivalent to $\theta_s(x, r^{|\sigma_0|_m})$. Therefore $\mathcal{R}_C(\theta_s(x, 1+n))_{s \in S}$ is true. Remark that $\theta_s(x, r^{|\sigma_0|_m})$ is true if and only if $x + r^{|\sigma_0|_m}.\frac{s - s_0}{1-r} \in Z_{r,m,s} \cap X$. Remark that $x + r^{|\sigma_0|_m}.\frac{s-s_0}{1-r} = \rho_{r,m}(\sigma_0, s)$. Therefore $\theta_s(x, r^{|\sigma_0|_m})$ is equivalent to $s \in [F_0](q)$ where $q = \delta(q_0, \sigma_0)$. We deduce that $\mathcal{R}_C(s \in [F_0](q))_{s \in S}$ is true. Hence $q \in C$ and from $s_0 \in [F_0](C)$ we get $s_0 \in [F_0](q)$. We have proved that $x \in X$.

Now, let us consider $x \in X$ and let us prove that $\phi(x)$ is true. Since Q is finite and $\prod_{s \in S} n_{s,x}$ is relatively prime with r, there exists a (r,m)-decomposition (σ_0, s_0) of x and an integer $d_0 \in \mathbb{N}\backslash\{0\}$ such that $q = \delta(q_0, \sigma_0)$

satisfies $\delta(q, s_0^{d_0}) = q$ and such that $r^{|\sigma_0|_m}$ and r^{d_0} are in $1 + n_{s,x}.\mathbb{Z}$. Since $\mathcal{C}$ is a partition of Q, there exists $C \in \mathcal{C}$ such that $q \in \mathcal{C}$. Let us consider $N \in \mathbb{Z}$. There exists $k \in \mathbb{N}$ such that the integer $n = r^{|\sigma_0|_m + k.d_0} - 1$ is greater than or equal to N and 1. Remark that $n \in n_{s,x}.(\mathbb{N}\backslash\{0\})$. Therefore $W_s(x, n)$ is true. Moreover, as $x \in X$ we deduce that $s_0 \in [F_0](q)$ and hence $\text{sign}(x) \in [F_0](C)$. Moreover, as $q \in C$ we get $\mathcal{R}_C(s \in [F_0](q))_{s \in S}$ is true. Remark that $s \in [F_0](q)$ if and only if $\rho_{r,m}(\sigma_0.s_0^{k.d_0}, s) \in Z_{r,m,s} \cap X$ if and only if $x + r^{|\sigma_0|_m + k.d_0}.\frac{s - s_0}{1-r} \in Z_{r,m,s} \cap X$ if and only if $\theta_s(x, 1 + n)$ is true. Therefore $\phi(x)$ is true. $\square$

Part II

Geometry

8

Linear Sets

8.1 Vector spaces

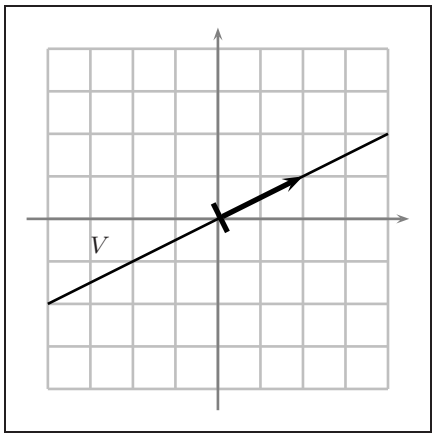

Fig. 8.1. The vector space $V = \mathbb{Q}.(2, 1)$

A *vector space* V of $\mathbb{Q}^m$ is a non empty subset of $\mathbb{Q}^m$ such that $\lambda.V \subseteq V$ for any $\lambda \in \mathbb{Q}$ and such that $V + V \subseteq V$. As any finite or infinite intersection of vector spaces of $\mathbb{Q}^m$ remains a vector space and we deduce that any set $X \subseteq \mathbb{Q}^m$ is included into a unique minimal (for $\subseteq$) vector space denoted by $\text{vec}(X)$ and called the *vector hull of* X or the *vector space generated* by X. A *basis* of a vector space V is a sequence v_1, .., v_d of vectors in V such that for any $x \in V$ there exists a unique sequence λ_1, ..., λ_d of rational numbers such that $x = \sum_{i=1}^{d} \lambda_i.v_i$. Recall that any vector space has a basis and the number of elements of a basis only depends on V and it is called the *dimension* of V, and it is denoted by $\dim(V) \in \{0, \ldots, m\}$.

There exists unduly complicated basis of vector spaces. For instance consider the vector space $V = \mathbb{Q}^2$ and for each $n \in \mathbb{N}$ let v_1^n, v_2^n be the basis of V given by $v_1^n = (2.n + 1, n)$ and $v_2^n = (2, 1)$. That means complex basis of simple vector spaces (for instance $\mathbb{Q}^2$) can be computed if vector spaces are symbolically manipulated by basis. In order to overcome this problem, we are going to associate to any vector space a canonical basis.

A *set of indices* $I \subseteq \{1, \ldots, m\}$ is said *full rank* for a vector space V if for any $x \in \mathbb{Q}^I$ there exists a *unique* $v \in V$ such that $v[i] = x[i]$ for any $i \in I$.

Proposition 8.1. *Any vector space has a full rank set of indices.*

Proof. Let us consider subset $I \subseteq \{1, \ldots, m\}$ maximal for the inclusion amongst the subset $J \subseteq \{1, \ldots, m\}$ satisfying for any $x \in \mathbb{Q}^J$, there exists a unique $v \in V$ such that $v[j] = x[j]$ for any $j \in J$. Remark that such a set I exists since $J = \emptyset$ satisfies the condition. Let us consider two vectors $v_1, v_2 \in V$ such that $v_1[i] = v_2[i]$ for any $i \in I$ and let $w = v_1 - v_2$. Assume by contradiction that $w \neq \mathbf{e}_{0,m}$. There exists $j_0 \in \{1, \ldots, m\} \backslash I$ such that $w[j_0] \neq 0$. Let $J = I \cup \{j_0\}$ and let us prove that for any $x \in \mathbb{Q}^J$ there exists $v \in V$ such that $v[j] = x[j]$ for any $j \in J$. By definition of I, there exists $v_0 \in V$ such that $v_0[i] = x[i]$ for any $i \in I$. Let $v = v_0 + \frac{x[j_0] - v_0[j_0]}{w[j_0]}.w$ and remark that $v[i] = x[i]$ for any $i \in I$ since $w[i] = 0$ and $v[j_0] = 0$. Therefore I is not maximal and we get a contradiction. Thus $w = \mathbf{e}_{0,m}$ and we have proved that for any $x \in \mathbb{Q}^I$, there exists a unique $v \in V$ such that $v[i] = x[i]$ for any $i \in I$. □

A *vector I-representation* of a vector space V where I is a full rank set of indices for V is a sequence $(v_i)_{i \in I}$ of vectors in V satisfying $v_i[i] = 1$ and $v_i[j] = 0$ for any $j \in I \backslash \{i\}$. Observe that such a sequence $(v_i)_{i \in I}$ is a basis of V and given a full rank set I, there exists a unique vector I-representation of V. The integer $\text{size}(V) \in \mathbb{N}$ of a vector space V is defined by $\text{size}(V) = \max_I(\sum_{i \in I} \text{size}(v_i))$ where $(v_i)_{i \in I}$ is the unique vector I-representation of V.

The following proposition provides a simple way for computing incrementally a vector I-representation of a vector space V.

Proposition 8.2. *Let I be a full rank set of indices for a vector space V, let $(v_i)_{i \in I}$ be the vector I-representation of V and let V' be the vector space $V' = V + \mathbb{Q}.x$ where x is any vector in $\mathbb{Q}^m$. The vector spaces V and V' are equal if and only if the vectors $y = x - \sum_{i \in I} x[i].v_i$ and $\mathbf{e}_{0,m}$ are equal. Moreover, if V' is not equal to V then given j_0 such that $y[j_0] \neq 0$, the set of indices $J = I \cup \{j_0\}$ is full rank for V' and the vector J-representation of V' is the following sequence $(v'_j)_{j \in J}$:*

$$v'_j = \begin{cases} v_j - v_j[j_0].\frac{y}{y[j_0]} & \text{if } j \in I \\ \frac{y}{y[j_0]} & \text{if } j = j_0 \end{cases}$$

Proof. Assume first that $y = \mathbf{e}_{0,m}$ and let us prove that $V = V'$. Since $y = \mathbf{e}_{0,m}$, we get $x = \sum_{i \in I} x[i].v_i \in V$ and we deduce $V = V'$. Otherwise, if $V = V'$ we deduce that $y \in V$. Since $(v_i)_{i \in I}$ is a basis of V, there exists a sequence $(\lambda_i)_{i \in I}$ of rational numbers such that $y = \sum_{i \in I} \lambda_i.v_i$. From this last equality, we get $y[i] = \lambda_i$ and from $y = x - \sum_{i \in I} x[i].v_i$, we get $y[i] = x[i] - x[i] = 0$. Thus λ_i for any i and we have proved that $y = \mathbf{e}_{0,m}$. We have proved that the vector spaces V and V' are equal if and only if the vectors $y = x - \sum_{i \in I} x[i].v_i$ and $\mathbf{e}_{0,m}$ are equal.

Now, assume that V' is not equal to V and observe that J is a set of indices full rank for V' and the sequence $(v'_j)_{j \in J}$ is a vector I-representation of V'. □

Our representation is motivated by the following corollary.

Corollary 8.3. *The size of a vector space V is at most polynomially larger than the size of any finite subset $V_0 \subseteq \mathbb{Q}^m$ that generates V.*

Proof. Assume fixed a full row set of indices I of V. Let us consider a finite set V_0 of vectors that generates V. It is sufficient to show that we can compute in polynomial time a sequence $(v_i)_{i \in I}$ from V_0. By applying the polynomial time algorithm given in proposition 8.2 and adding one by one the vector v_0 in V and by selecting j_0 in I, we deduce that the sequence $(v_i)_{i \in I}$ is computable in polynomial time. □

8.2 Affine spaces

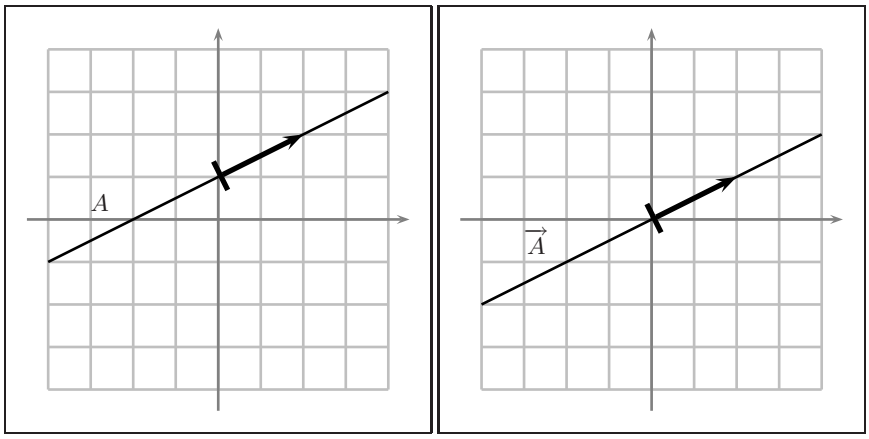

Fig. 8.2. On the left an affine space $A = (0,1) + \mathbb{Q}.(2,1)$. On the right its direction.

An *affine space* A of $\mathbb{Q}^m$ is either the empty-set, or a set of the form $A = a_0 + V$ where $a_0 \in \mathbb{Q}^m$ and V is a vector space of $\mathbb{Q}^m$. This vector space V is unique, denoted by $\overrightarrow{A}$ and called the *direction* of A (see figure 8.2). If $A = \emptyset$, we denote by $\overrightarrow{A} = \emptyset$ the *direction* of A. A non-empty affine space A is called a V-affine space if $\overrightarrow{A}$ is equal to a vector space V.

An *affine I-representation* of a V-affine space A where I is a full rank set of indices of V is a couple $(a, (v_i)_{i\in I})$ where a is a vector in A such that $a[i] = 0$ for any $i \in I$ and $(v_i)_{i\in I}$ is the I-vector representation of V. Observe that such a couple is unique. The integer $\text{size}(A) \in \mathbb{N}$ of a non-empty affine space A is defined by $\text{size}(A) = \max_I(\text{size}(a)) + \text{size}(V)$ where $(a, (v_i)_{i\in I})$ is the unique I-affine representation of A. The integer $\text{size}(\emptyset)$ is defined by $\text{size}(\emptyset) = 0$. Notice that $\text{size}(A) = \text{size}(V)$ if the affine space A is a vector space $A = V$ since in this case $a = \mathbf{e}_{0,m}$.

The direction of affine spaces, has an interesting application intensively used in the sequel and given by the following lemma.

Lemma 8.4 (Comparable affine lemma). *Two comparable (for $\subseteq$) affine spaces that have the same direction are equal.*

Proof. Consider two affine spaces A_1 and A_2 such that $A_1 \subseteq A_2$ and such that $\overrightarrow{A_1} = \overrightarrow{A_2}$. Naturally, if $A_1 = \emptyset$, as $\overrightarrow{A_1} = \overrightarrow{A_2}$ we deduce that $A_2 = \emptyset$ and we are done. Assume that $A_1 \neq \emptyset$. Consider $a_1 \in A_1$. As $a_1 \in A_1 \subseteq A_2$, we deduce that $A_2 = a_1 + \overrightarrow{A_2}$. From $\overrightarrow{A_1} = \overrightarrow{A_2}$, we get $A_2 = a_1 + \overrightarrow{A_1} = A_1$. □

Recall that any finite or infinite intersection of affine spaces of $\mathbb{Q}^m$ remains an affine space, and we deduce that any set $X \subseteq \mathbb{Q}^m$ is included into a unique minimal (for $\subseteq$) affine space denoted by $\text{aff}(X)$ and called the *affine hull of X* or the affine space generated by X. The direction of $\text{aff}(X)$ is denoted by $\overrightarrow{\text{aff}}(X) = \overrightarrow{\text{aff}(X)}$.

Finally, recall that the *orthogonal* $X^\perp$ of a subset $X \subseteq \mathbb{Q}^m$ is the vector space $X^\perp = \{y \in \mathbb{Q}^m;\ \forall x \in X\ \langle y, x\rangle = 0\}$. Recall that $(X^\perp)^\perp = \text{vec}(X)$. In particular, $X = V$ is a vector space if and only if $(V^\perp)^\perp = V$. The *orthogonal projection over a non-empty affine space A* is the unique function $\Pi_A : \mathbb{Q}^m \to A$ such that $\Pi_A(x) - x \in (\overrightarrow{A})^\perp$ for any $x \in \mathbb{Q}^m$ (see figure 8.3). Recall that Π_A is an affine function that satisfies $\Pi_A(x) = (1 - \sum_{i=1}^m x[i]).\Pi_A(\mathbf{e}_{0,m}) + \sum_{i=1}^m x[i].\Pi_A(\mathbf{e}_{i,m})$.

8.3 Vector lattices

An *additive group* M of $\mathbb{Q}^m$ is a non-empty finite subset of $\mathbb{Q}^m$ such that $-M \subseteq M$ and $M + M \subseteq M$. As any finite or infinite intersection of additive groups remains an additive group and $\mathbb{Q}^m$ is a group, any set $X \subseteq \mathbb{Q}^m$ is included into a minimal (for $\subseteq$) additive group, denoted by $\text{group}(X)$ and called the *group generated* by X. An additive group M such that there exists

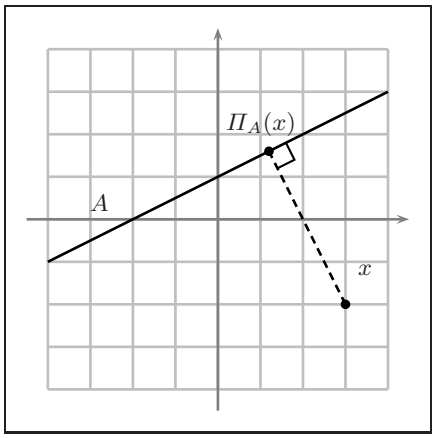

Fig. 8.3. Orthogonal projection $\Pi_A(x) = \frac{(6,3)}{5}$ of $x = (3,-2)$ over $A = (0,1) + \mathbb{Q}.(2,1)$.

a finite set X satisfying $M = \text{group}(X)$ is called a *vector lattice*. Lattices are characterized by introducing *discrete sets*. A set $Z \subseteq \mathbb{Q}^m$ is said *discrete* if for any $x \in M$, there exists a rational number $\epsilon > 0$ such that $||x - y||_\infty \geq \epsilon$ for any $y \in M \backslash \{x\}$.

Proposition 8.5 ([Tau92]). *A group is discrete if and only if it is a vector lattice.*

Proof. Assume first that M is a discrete group and let us prove that M is a vector lattice. Since $\mathbf{e}_{0,m} \in M$, there exists $\epsilon > 0$ such that $||x||_\infty > \epsilon$ for any $x \in M$. Let V be the vector space generated by M and let v_1, ..., v_d be a basis of V formed by vectors in M. Let us denote by $B = \{\sum_{i=1}^d \lambda[i].v_i;\ 0 \leq \lambda[i] \leq 1\}$. The rational $k = \sum_{i=1}^d ||v_i||_\infty$ satisfies $||b||_\infty \leq k$ for any $b \in B$. Assume by contradiction that $M \cap B$ contains more than $(\frac{2.k+1}{\epsilon})^n$ elements. Hence, there exists $x_1, x_2 \in M \cap B$ such that $x_1 \neq x_2$ and such that $||x_1 - x_2||_\infty \leq \epsilon$. By definition of ϵ we deduce that $x_1 - x_2 = \mathbf{e}_{0,m}$ and we get a contradiction. Thus $M \cap B$ is finite. For any $x \in M$, there exists $\lambda \in \mathbb{Q}^d$ such that $x = \sum_{i=1}^d \lambda[i].v_i$. Let us consider a vector $z \in \mathbb{Z}^d$ such that $0 \leq \lambda[i] - z[i] \leq 1$ and remark that $x - \sum_{i=1}^d z[i].v_i \in M \cap B$. Thus $M = \text{group}(\{v_1, \ldots, v_d\} \cup (M \cap B))$ and we have proved that there exists a finite set X of vectors such that $M = \text{group}(X)$. For the converse, assume that M is a vector lattice and let us prove that M is discrete. There exists a finite set X of vectors such that $M = \text{group}(X)$. Let us consider an integer $d \in \mathbb{N} \backslash \{0\}$ such that $d.X \subseteq \mathbb{Z}^m$ and let us remark that for any $x, y \in M$ such that $x \neq y$, we have $||x - y||_\infty \geq \frac{1}{d}$. Thus M is discrete. □

Thanks to this characterization, we deduce that any group included in a vector lattice is a vector lattice since any set included in a discrete set remains

discrete. Given a vector space V, a vector lattice M such that $V = \text{vec}(M)$ is called a V-vector lattice. The previous proposition also proves that $\mathbb{Z}^m \cap V$ is a V-vector lattice since it is a discrete group such that $\text{vec}(\mathbb{Z}^m \cap V) = V$.

8.3.1 Hermite representation

We are going to provide a canonical (up to a full rank set of indices I for V) representation of any V-vector lattice.

An *Hermite matrix* B of order d is a lower triangular (we have $B[i,j] = 0$ for any $j > i$), non-negative square matrix $B \in \mathcal{M}_{d,d}(\mathbb{Q}_+)$, in which each row has a unique maximal entry which is located on the main diagonal of B. Given a full row set of indices $I = \{i_1 < \cdots < i_d\}$ of a vector space V, an *Hermite I-representation* B of a V-vector lattice M is an Hermite matrix B of order d such that we have the following equality where $(v_i)_{i \in I}$ is the vector I-representation of V:

$$M = \text{group}\{\sum_{k=1}^{d} B[k,j].v_{i_k};\ j \in \{1, \ldots, d\}\}$$

The integer $\text{size}(M) \in \mathbb{N}$ of a V-vector lattice M is defined by $\text{size}(M) = \max_I(\text{size}(B)) + \text{size}(V)$.

The following theorem shows that the Hermite I-representation provides a canonical representation that is polynomially bounded by the size of any finite set X such that $M = \text{group}(X)$.

Theorem 8.6 (Theorem 4.1, 4.2 and 5.3 of [Sch87]). *Given a full rank set of indices I of a vector space V, any V-vector lattice M owns a unique Hermite I-representation. Moreover, this representation is computable in polynomial time from any finite set of vectors that generates M.*

This theorem also proves that for any V-vector lattice, there exists a basis v_1, ..., v_d of V such that $M = \sum_{j=1}^{d} \mathbb{Z}.v_j$ (for instance take $v_j = \sum_{k=1}^{d} B[k,j].v_{i_k}$). Such a sequence v_1, ..., v_d is called a $\mathbb{Z}$-*basis* of M.

The following proposition will be useful in the sequel.

Proposition 8.7 (Corollary 5.3b and 5.3c of [Sch87]). *From an I-representation of a vector space V, we can compute in polynomial time the Hermite I-representation of the V-vector lattice $\mathbb{Z}^m \cap V$.*

8.3.2 Stability by intersection

Naturally, any intersection of vector lattices remains a vector lattice. The following lemma 8.8 shows that the class of V-vector lattice is stable by finite intersection (remark 8.9 shows that this class is not stable by infinite intersection).

Lemma 8.8. *The class of V-vector lattices is stable by finite intersection. Moreover, given a finite sequence M_1, ..., M_n of V-vector lattices, we can compute in polynomial time the V-vector lattice $\bigcap_{j=1}^{n} M_j$.*

Proof. Let I be a full rank set of indices. Recall that from an Hermite I-representation of M_j, we get a $\mathbb{Z}$-basis $v_{1,j}$, ..., $v_{d,j}$ of M_j. Now, remark that $x \in M$ where $M = \bigcap_{j=1}^{n} M_j$ if and only if there exists z_1, ..., z_n in $\mathbb{Z}^d$ such that $x = \sum_{i=1}^{d} z_j.v_{i,j}$ for any $j \in \{1, \ldots, n\}$. Let us consider the vector space $W = \{(x, z_1, \ldots, z_n) \in \mathbb{Q}^n \times \mathbb{Q}^d \times \cdots \mathbb{Q}^d;\ \bigcap_{j=1}^{n} x = \sum_{i=1}^{d} z_j.v_{i,j}\}$. From proposition 8.7 we deduce in polynomial time a $\mathbb{Z}$-basis of $\mathbb{Z}^m \cap W$ of the form $(x_1, z_{1,1}, \ldots, z_{1,n})$, ..., $(x_d, z_{d,1}, \ldots, z_{d,n})$. Let us remark that $\bigcap_{j=1}^{d} M_j$ is the V-vector lattice generated by x_1, ..., x_d. We deduce the I-representation of M in polynomial time. □

Remark 8.9. The class of V-vector lattices is not stable by infinite intersection. In fact, let M_n be the V-vector lattice $M_n = (n+1).\mathbb{Z}^m$ where $V = \mathbb{Q}^m$, and just remark that $\bigcap_{n \in \mathbb{N}} M_n = \{\mathbf{e}_{0,m}\}$ is naturally a group as any intersection of groups, but it is not a V-vector lattice if $m \geq 1$.

8.3.3 Sub-lattice

The *quotient* M'/M of two V-vector lattices $M \subseteq M'$ is defined by $M/M' = \{m' + M;\ m' \in M\}$. The following theorem 8.10 proves that this set is finite.

Theorem 8.10 ([Tau92]). *Given two vector lattices $M \subseteq M'$, there exists a unique sequence n_1, ..., n_d of integers in $\mathbb{N}\backslash\{0\}$ such that n_i divides n_{i+1} for any i and such that there exists a $\mathbb{Z}$-basis v_1, ..., v_d of M' satisfying $n_1.v_1$, ..., $n_d.v_d$ is a $\mathbb{Z}$-basis of M. Moreover such a sequence (n_1, v_1), ..., (n_d, v_d) is computable in polynomial time.*

The unique sequence n_1, ..., n_d is called the *characteristic sequence* of M in M'.

The following lemma will be useful in the sequel.

Lemma 8.11 ([Tau92]). *Given three V-vector lattices $M \subseteq M' \subseteq M''$, we have the following equality:*

$$|M''/M'|.|M'/M| = |M''/M|$$

8.3.4 Vector lattices included in $\mathbb{Z}^m$

In the sequel we denote by $h_r : \mathbb{N}\backslash\{0\} \to \mathbb{N}\backslash\{0\}$ the function defined by $h_r(n) = \frac{n}{\gcd(n,r)}$, and we denote by θ_m is the function $\theta_m \in \{1, \ldots, m\} \to \{1, \ldots, m\}$ defined by $\theta_m(i) \in (i - 1 + m.\mathbb{Z}) \cap \{1, \ldots, m\}$.

Inverse image by $\gamma_{r,m,0}$

Theorem 8.10 proves that any V-vector lattice M included in $\mathbb{Z}^m$ is a set of the form $M = \sum_{i=1}^{d} n_i.\mathbb{Z}.v_i$ where v_1, ..., v_d is a $\mathbb{Z}$-basis of $\mathbb{Z}^m \cap V$ and n_1, ..., n_d are integers in $\mathbb{N}\backslash\{0\}$. Thus, the following lemma 8.12 shows that the class of V-vector lattices included in $\mathbb{Z}^m$ is stable by inverse image by $\gamma_{r,m,\mathbf{e}_{0,m}}$.

Lemma 8.12. *Given a $\mathbb{Z}$-basis v_1, ..., v_d of $\mathbb{Z}^m \cap V$ where V is a vector space and a sequence n_1, ..., n_d of integers in $\mathbb{N}\backslash\{0\}$, we have:*

$$\gamma^{-1}_{r,m,\mathbf{e}_{0,m}}(\sum_{i=1}^{d} n_i.\mathbb{Z}.v_i) = \sum_{i=1}^{d} h_r(n_i).\mathbb{Z}.v_i$$

Proof. Let $x \in \gamma^{-1}_{r,m,\mathbf{e}_{0,m}}(\sum_{i=1}^{d} n_i.\mathbb{Z}.v_i)$. There exists z_1, ..., z_d in $\mathbb{Z}$ such that $r.x = \sum_{i=1}^{d} n_i.z_i.v_i$. In particular $x \in \mathbb{Z}^m \cap V$ and there exists t_1, ..., t_d in $\mathbb{Z}$ such that $x = \sum_{i=1}^{d} t_i.v_i$. As v_1, ..., v_d is a $\mathbb{Z}$-basis, we get $r.t_i = n_i.z_i$ for any i. Therefore $r_i.t_i = h_r(n_i).z_i$ where $r_i = \frac{r}{\gcd(n_i,r)}$. As r_i and $h_r(n_i)$ are relatively prime, there exists u_i, u'_i in $\mathbb{Z}$ such that $u_i.r_i + u'_i.h_r(n_i) = 1$. From $u_i.r_i.t_i = h_r(n_i).u_i.z_i$, we get $t_i = h_r(n_i).(u_i.z_i + u'_i.t_i)$. Therefore, $x \in \sum_{i=1}^{d} h_r(n_i).\mathbb{Z}.v_i$ and we have proved the inclusion $\gamma^{-1}_{r,m,\mathbf{e}_{0,m}}(\sum_{i=1}^{d} n_i.\mathbb{Z}.v_i) \subseteq \sum_{i=1}^{d} h_r(n_i).\mathbb{Z}.v_i$. Let us prove the other inclusion. Consider $x \in \sum_{i=1}^{d} h_r(n_i).\mathbb{Z}.v_i$. There exists a sequence z_1, ..., z_d in $\mathbb{Z}$ such that $x = \sum_{i=1}^{d} h_r(n_i).z_i.v_i$. Hence $\gamma_{r,m,\mathbf{e}_{0,m}}(x) = \sum_{i=1}^{n} r.h_r(n_i).z_i.v_i$. As n_i divides $r.h_r(n_i)$, we deduce that $\gamma_{r,m,\mathbf{e}_{0,m}}(x) \in \sum_{i=1}^{d} n_i.\mathbb{Z}.v_i$. Therefore $x \in \gamma^{-1}_{r,m,\mathbf{e}_{0,m}}(\sum_{i=1}^{d} n_i.\mathbb{Z}.v_i)$ and we have proved the other inclusion. □

The stability of vector lattices by inverse image by $\gamma_{r,m,0}$ is provided by the following proposition 8.13.

Proposition 8.13. *The set $M_z = \gamma^{-z}_{r,m,0}(M)$ is a V_z-vector lattice included in $\mathbb{Z}^m$ for any V-vector lattice M included in $\mathbb{Z}^m$ where V_z is the vector space $V_z = \Gamma^{-z}_{r,m,0}(V)$ and for any $z \in \mathbb{N}$. Moreover, from an Hermite I-representation of M, we can compute in polynomial time the Hermite I_z-representation of M_z where $I_z = \theta^z_m(I)$.*

Proof. Recall that form the I-representation of M, we immediately deduce a $\mathbb{Z}$-basis v_1, ..., v_d of M. Let us remark that $\gamma^{-z}_{r,m,0}(M)$ is the set of vectors $x \in \mathbb{Z}^m$ such that there exists a vector $k \in \mathbb{Z}^d$ satisfying $\Gamma^{z}_{r,m,0}(x) = \sum_{i=1}^{d} k[i].v_i$. Let us consider the vector space $W = \{(k,x) \in \mathbb{Q}^d \times \mathbb{Q}^m;\ \Gamma^{z}_{r,m,0}(x) = \sum_{i=1}^{d} k[i].v_i\}$. Remark that W is a vector space and $J = \{1,\ldots,d\}$ is a full rank set of indices of W. From proposition 8.7 we deduce that we can compute in polynomial time the J-representation of W. That means we can compute in polynomial time a $\mathbb{Z}$-basis of $\mathbb{Z}^m \cap W$ denoted by (k_1,x_1), ..., $w_d = (k_d,x_d)$ where $k_i \in \mathbb{Z}^d$ and $x_i \in \mathbb{Z}^m$. Now, just remark that $\gamma^{-z}_{r,m,0}(M)$

is a the V_z-vector lattice generated by the vectors x_1, ..., x_d. Therefore, the I_z-representation of $\gamma_{r,m,0}^{-z}(M)$ is computable in polynomial time for any $z \in \{0, \ldots, m-1\}$. Observe that in general, an integer $z \in \mathbb{N}$ can be decomposed into $z = z' + m.k$ where $k \in \mathbb{N}$ and $z' \in \{0, \ldots, m-1\}$. Observe that $\gamma_{r,m,\mathbf{e}_{0,m}}^{-k}(M)$ can be computed in polynomial time thanks to lemma 8.12. □

Relatively prime properties

A V-vector lattice M included in $\mathbb{Z}^m$ is said *relatively prime with a basis of decomposition* r if the integer $|\mathbb{Z}^m \cap V/M|$ is relatively prime with r.

Thanks to lemma 8.11, we deduce that the class of V-vector lattices included in $\mathbb{Z}^m$ and relatively prime with r is stable by finite intersection. In fact given two relatively prime V-vector lattices M_1 and M_2 included in $\mathbb{Z}^m$, from $M_1 \cap M_2 \subseteq n.\mathbb{Z}^m \cap V \subseteq \mathbb{Z}^m \cap V$ where $n = |\mathbb{Z}^m \cap V/M_1|.|\mathbb{Z}^m \cap V/M_2|$, we deduce that $|\mathbb{Z}^m \cap V/M_1 \cap M_2|.|M_1 \cap M_2/n.\mathbb{Z}^m \cap V| = |\mathbb{Z}^m \cap V/n.\mathbb{Z}^m \cap V| = n^{\dim(V)}$. In particular $|\mathbb{Z}^m \cap V/M_1 \cap M_2|$ divides an integer relatively prime with r. That means it is relatively prime with r.

We are going to show that the V-vector lattices included in $\mathbb{Z}^m$ and relativelly prime with r naturally appear when computing inverse images of a V-vector lattice by $\gamma_{r,m,0}$.

As $h_r(n) \leq n$ for any integer $n \in \mathbb{N}\backslash\{0\}$ we deduce that $(h_r^k(n))_{k\in\mathbb{N}}$ is a non increasing sequence ultimely stationary: there exists $k_n \in \mathbb{N}$ such that $h_r^k(n) = h_r^{k_n}(n)$ for any $k \geq k_n$. We denote by $h_r^\infty(n)$ this limit. Remark that $h_r^\infty(n)$ is relatively prime with r and $h_r^\infty(n) = n$ if and only if n is relatively prime with r. The previous lemma 8.12 shows that $(\gamma_{r,m,\mathbf{e}_{0,m}}^{-k}(M))_{k\in\mathbb{N}}$ is a non decreasing sequence of V-vector lattices ultimately stationary. The limit is denoted by $\gamma_{r,m,\mathbf{e}_{0,m}}^{-\infty}(M)$ and naturally satisfies the following equality:

$$\gamma_{r,m,\mathbf{e}_{0,m}}^{-\infty}(M) = \bigcup_{k\in\mathbb{N}} \gamma_{r,m,\mathbf{e}_{0,m}}^{-k}(M)$$

From the previous lemma 8.12 we deduce that $\gamma_{r,m,\mathbf{e}_{0,m}}^{-\infty}(M)$ is relatively prime with r and if M is relatively prime with r then $\gamma_{r,m,\mathbf{e}_{0,m}}^{-\infty}(M) = M$. In particular the class of V-vector lattices relatively prime with r is stable by inverse image by $\gamma_{r,m,\mathbf{e}_{0,m}}$.

Let us remark that the elements in $\gamma_{r,m,\mathbf{e}_{0,m}}^{-\infty}(M)$ are geometrically characterized by the following lemma 8.14

Lemma 8.14. *Given a vector lattice M included in $\mathbb{Z}^m$ and a vector $x \in \mathbb{Z}^m$, we have $x \in \gamma_{r,m,\mathbf{e}_{0,m}}^{-\infty}(M)$ if and only if there exists $k \in \mathbb{N}$ such that $r^k.x \in M$.*

Proof. Let $V = \mathrm{vec}(M)$. There exists a $\mathbb{Z}$-basis of M of the form $n_1.v_1$, ..., $n_d.v_d$ where n_1, ..., n_d are integers in $\mathbb{N}\backslash\{0\}$ and v_1, ..., v_d is a $\mathbb{Z}$-basis of $\mathbb{Z}^m \cap V$. From lemma 8.12 we deduce that $h_r^\infty(n_1).v_1$, ..., $h_r^\infty(n_d).v_d$ is a $\mathbb{Z}$-basis of $\gamma_{r,m,\mathbf{e}_{0,m}}^{-\infty}(M)$. Remark that there exists an integer $k_0 \in \mathbb{N}$ such that $r^{k_0} h_r^\infty(n_i)$ divides n_i for any $i \in \{1, \ldots, d\}$.

First, let us first prove that there exists $k \in \mathbb{N}$ satisfying $r^k.x \in M$ for any $x \in \gamma^{-\infty}_{r,m,\mathbf{e}_{0,m}}(M)$. There exists $z \in \mathbb{Z}^d$ such that $x = \sum_{i=1}^{d} h^{\infty}_r(n_i).z[i].v_i$. In particular $r^{k_0}.x = \sum_{i=1}^{d} r^{k_0}.h^{\infty}_r(n_i).z[i].v_i \in M$ and we have proved that there exists an integer $k \in \mathbb{N}$ such that $r^k.x \in M$.

Next, let us show that $x \in \gamma^{-\infty}_{r,m,\mathbf{e}_{0,m}}(M)$ for any $x \in \mathbb{Z}^m$ such that there exists $k \in \mathbb{N}$ satisfying $r^k.x \in M$. As $r^k.x \in M$, we deduce that $x \in \mathbb{Z}^m \cap V$. Hence, there exists $z \in \mathbb{Z}^d$ such that $x = \sum_{i=1}^{d} z[i].v_i$. Hence $r^k.x = \sum_{i=1}^{d} z[i]r^k.z[i].v_i$. Moreover, as $r^k.x \in M$, there exists $t \in \mathbb{Z}^d$ such that $r^k.x = \sum_{i=1}^{d} n_i.t[i].v_i$. As v_1, ..., v_d is a $\mathbb{Z}$-base, we get $r^k.z[i] = n_i.t[i]$. As $h^{\infty}_r(n_i)$ divides n_i, we deduce that $n'_i = \frac{n_i}{h^{\infty}_r(n_i)}$ is $\mathbb{N}$. Hence $r^k.z[i] = h^{\infty}_r(n_i).n'_i.t[i]$. As $h^{\infty}_r(n_i)$ is relatively prime with r, then $h^{\infty}_r(n_i)$ is relatively prime with r^k, and we deduce that r^k divides $n'_i.t[i]$. Hence $z[i] \in h^{\infty}_r(n_i).\mathbb{Z}$. We deduce that $x \in \gamma^{-1}_{r,m,\mathbf{e}_{0,m}}(M)$. □

8.4 Affine lattices

An *affine lattice* P is a subset of $\mathbb{Q}^m$ of the form $P = a + M$ where $a \in \mathbb{Q}^m$ and M is a lattice. A *V-affine lattice* P is an *affine lattice* P of the form $P = a + M$ where M is a V-vector lattice.

Given a V-affine space A, observe that $\mathbb{Z}^m \cap A$ is either empty or a V-affine lattice of the form $a + (\mathbb{Z}^m \cap V)$ where a is any vector in $\mathbb{Z}^m \cap A$. The following proposition will be useful for computing a vector in $\mathbb{Z}^m \cap A$ when such a vector exists.

Proposition 8.15 (Corollary 5.3b and 5.3c of [Sch87]). *Given an affine space A, we can decide in polynomial time if $\mathbb{Z}^m \cap A$ is non empty and in this case, we can compute in polynomial time a vector a in this set.*

Corollary 8.16. *Given two affine lattices $P_1 = b_1 + M_1$ and $P_2 = b_2 + M_2$ where b_1, b_2 are two vectors in $\mathbb{Q}^d$ and M_1, M_2 are two vectors lattices, we can decide in polynomial time if $(b_1 + M_1) \cap (b_2 + M_2) \neq \emptyset$. Moreover, in this case we can compute in polynomial time a vector a in this set. Observe that we have $P_1 \cap P_2 = a + (M_1 \cap M_2)$.*

Proof. From the vector I_1-representation of M_1, we deduce in linear time a $\mathbb{Z}$-basis $v_{1,1}$, ..., v_{1,d_1} of M_1, and from the vector I_2-representation of M_2, we get in linear time a $\mathbb{Z}$-basis $v_{2,1}$, ..., v_{2,d_2} of M_2. Observe that $(b_1 + M_1) \cap (b_2 + M_2) \neq \emptyset$ if and only if $\mathbb{Z}^m \cap A$ is non empty where A is the affine space $A = \{(x_1, x_2) \in \mathbb{Q}^{d_1} \times \mathbb{Q}^{d_2};\ b_1 + \sum_{i=1}^{d_1} x_1[i].v_{1,i} = b_2 + \sum_{i=1}^{d_2} x_2[i].v_{2,i}\}$. Note that proposition 8.15 provides a polynomial time algorithm for deciding if $\mathbb{Z}^m \cap A$ is non-empty and in this case it provides in polynomial time a vector $(x_1, x_2) \in \mathbb{Z}^m \cap A$. Note that $a = b_1 + \sum_{i=1}^{d_1} x_1[i].v_{1,i}$ is a vector in $P_1 \cap P_2$. □

9

Semi-linear Sets

9.1 Semi-linear Spaces

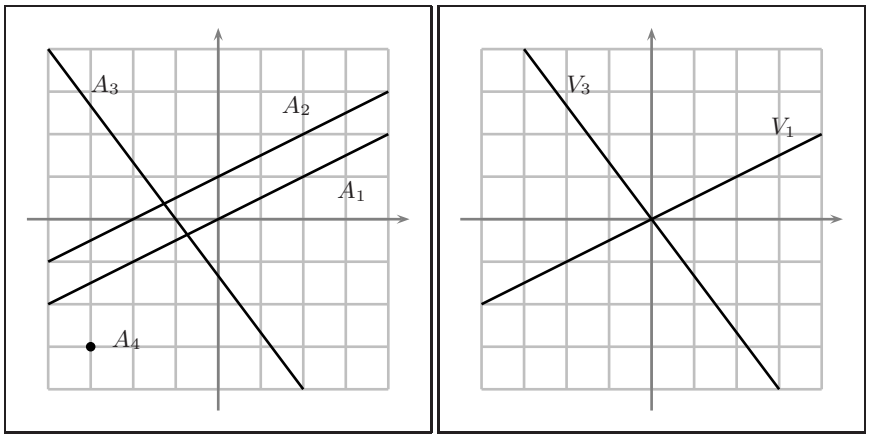

Fig. 9.1. On the left a semi-affine space S. On the right its direction.

A *semi-affine space* (resp. a *semi-vector space*) S of $\mathbb{Q}^m$ is a finite union of affine spaces (resp. vector spaces) of $\mathbb{Q}^m$ (see figure 9.1). Given a vector space V, a finite union of V-affine spaces is called a *semi-V-affine space*. In this section we show that a semi-affine space can be canonically decomposed into maximal affine spaces, called *affine components*. Moreover, by proving that any finite or infinite intersection of semi-affine spaces remains a semi-affine space, we define the notion of *semi-affine hull*.

9.1.1 Affine components

Definition 9.1. *An* affine component *A of a semi-affine space S is a maximal (for $\subseteq$) affine space included in S. The set of affine components is denoted by* $\mathrm{comp}(S)$.

We are going to prove that $\mathrm{comp}(S)$ provides a canonical representation of S. We first prove the following lemma, intensively used in the sequel.

Lemma 9.2 (Insecable lemma). *Let $\mathcal{C}$ be a non-empty finite class of affine spaces and A_0 be an affine space such that $A_0 \subseteq \bigcup_{A\in\mathcal{C}} A$. There exists $A \in \mathcal{C}$ such that $A_0 \subseteq A$.*

Proof. Let us consider an affine space A_0 and let us prove by induction over $n \in \mathbb{N}\backslash\{0\}$ that for any finite class $\mathcal{C}$ of affine spaces such that $|\mathcal{C}| = n$ and $A_0 \subseteq \bigcup_{A\in\mathcal{C}} A$, there exists $A \in \mathcal{C}$ such that $A_0 \subseteq A$. Naturally the case $n = 1$ is immediate. Assume that the induction hypothesis is true for an integer $n \in \mathbb{N}\backslash\{0\}$ and let us consider a finite class $\mathcal{C}$ of affine spaces such that $|\mathcal{C}| = n + 1$ and $A_0 \subseteq \bigcup_{A\in\mathcal{C}} A$. Let us consider $A' \in \mathcal{C}$. The case $A_0 \subseteq A'$ is also immediate so we can assume that $A_0 \not\subseteq A'$. Let us consider $\mathcal{C}' = \mathcal{C}\backslash\{A'\}$. As $A_0 \not\subseteq A'$, there exists $a_0 \in A_0\backslash A'$. Let $a_1 \in A_0$ and remark that $a_t = a_0 + t.(a_1 - a_0) \in A_0$ for any $t \in \mathbb{Q}$ because A_0 is an affine space. From $A_0 \subseteq \bigcup_{A\in\mathcal{C}} A$, we deduce that for any $t \in \mathbb{Q}$, there exists $A \in \mathcal{C}$ such that $a_t \in A$. As $\mathbb{Q}$ is infinite whereas $\mathcal{C}$ is finite, there exists $A \in \mathcal{C}$ and at least two different $t \in \mathbb{Q}$ satisfying $a_t \in A$. As A is an affine space, we deduce that $a_t \in A$ for every $t \in \mathbb{Q}$. From $a_0 \in A$ and $a_0 \notin A'$, we deduce that $A \in \mathcal{C}'$. We get $a_1 \in \bigcup_{A\in\mathcal{C}'} A$. We have proved that $A_0 \subseteq \bigcup_{A\in\mathcal{C}'} A$. From $|\mathcal{C}'| = n$, we deduce that there exists $A'' \in \mathcal{C}'$ such that $A_0 \subseteq A''$. We have proved the induction hypothesis for $\mathcal{C}$. □

Proposition 9.3. *The set* $\mathrm{comp}(S)$ *of a semi-affine space S is finite and S is equal to the finite union of its affine components $S = \bigcup_{A\in\mathrm{comp}(S)} A$. Moreover, from any finite class $\mathcal{C}$ of affine spaces such that $S = \bigcup_{A\in\mathcal{C}} A$, we can compute in polynomial time* $\mathrm{comp}(S)$.

Proof. Let us consider a semi-affine space $S = \bigcup_{A\in\mathcal{C}} A$ where $\mathcal{C}$ is a finite class of affine spaces.

Consider the class $\mathcal{C}'$ of non-empty affine spaces in $\mathcal{C}$ maximal for $\subseteq$. Let us first prove that $S = \bigcup_{A'\in\mathcal{C}'} A'$. Naturally, from $\mathcal{C}' \subseteq \mathcal{C}$, we deduce that $\bigcup_{A'\in\mathcal{C}'} A' \subseteq S$. For any $A \in \mathcal{C}$, either $A = \emptyset$ and in this case $A \subseteq \bigcup_{A'\in\mathcal{C}'} A'$, or $A \neq \emptyset$, and in this case there exists $A' \in \mathcal{C}'$ such that $A \subseteq A'$. Hence $A \subseteq \bigcup_{A'\in\mathcal{C}'} A'$. Therefore, $S = \bigcup_{A'\in\mathcal{C}'} A'$.

By replacing $\mathcal{C}$ by $\mathcal{C}'$, we can assume without loss of generality that $\mathcal{C}$ is a finite class of non-empty affine spaces such that $A_1 \subseteq A_2$ implies $A_1 = A_2$ for any A_1, A_2 in $\mathcal{C}$.

Let us now prove that $\mathrm{comp}(S) = \mathcal{C}$. Let $A_0 \in \mathcal{C}$ and consider an affine space A' such that $A_0 \subseteq A' \subseteq S$. Insecable lemma 9.2 proves that $A' \subseteq S =$

$\bigcup_{A\in\mathcal{C}} A$ implies that there exists $A \in \mathcal{C}$ such that $A' \subseteq A$. From $A_0 \subseteq A$ and A, A_0 in $\mathcal{C}$, we get $A_0 = A$. We deduce that $A_0 = A'$. Hence A_0 is a maximal (for $\subseteq$) non-empty affine space such that $A_0 \subseteq S$. That means $A_0 \in \text{comp}(S)$ and we have proved that $\mathcal{C} \subseteq \text{comp}(S)$. Let us prove the converse inclusion. Let $A_0 \in \text{comp}(S)$. As $A_0 \subseteq S = \bigcup_{A\in\mathcal{C}} A$, insecable lemma 9.2 shows that there exists $A \in \mathcal{C}$ such that $A_0 \subseteq A$. From $A_0 \subseteq A \subseteq S$, we deduce by maximality of A_0 that $A_0 = A$. Hence $A_0 \in \mathcal{C}$ and we have proved that $\text{comp}(S) \subseteq \mathcal{C}$. □

9.1.2 Size

The set of affine components provides a natural way for *canonically* representing semi-affine spaces as finite set of affine spaces. The integer $\text{size}(S) \in \mathbb{N}$ where S is a semi-affine space is naturally defined by $\text{size}(S) = \sum_{A\in\text{comp}(S)} \text{size}(A)$.

9.1.3 Direction

Definition 9.4. *The* direction $\overrightarrow{S}$ *of a semi-affine space* S *is defined by* $\overrightarrow{S} = \bigcup_{A\in\text{comp}(S)} \overrightarrow{A}$.

Remark that the semi-affine space direction definition extends the affine space direction definition because if $S = A$ is a non-empty affine space then $\text{comp}(S) = \{A\}$, and if $S = \emptyset$ then $\text{comp}(S) = \emptyset$. Remark also that insecable lemma 9.2 shows that for any class $\mathcal{C}$ of affine spaces such that $S = \bigcup_{A\in\mathcal{C}} A$, we have $\overrightarrow{S} = \bigcup_{A\in\mathcal{C}} \overrightarrow{A}$ even if $\mathcal{C}$ is not equal to $\text{comp}(S)$. That shows in particular that a semi-affine space S is a semi-vector space if and only if $\overrightarrow{S} = S$.

Example 9.5. Let us consider the semi-affine space $S = A_1 \cup A_2 \cup A_3 \cup A_4$ where $A_1 = \mathbb{Q}.(2,1)$, $A_2 = (0,1) + \mathbb{Q}.(2,1)$, $A_3 = (-1,0) + \mathbb{Q}.(3,-4)$ and $A_4 = \{(-3,-3)\}$ given in figure 9.1. We have $\overrightarrow{S} = V_1 \cup V_3$ where $V_1 = \mathbb{Q}.(2,1)$ and $V_3 = \mathbb{Q}.(3,-4)$. Remark that S owns 4 affine components $\text{comp}(S) = \{A_1, A_2, A_3, A_4\}$ and $\overrightarrow{S}$ owns only 2 affine components $\text{comp}(\overrightarrow{S}) = \{V_1, V_3\}$.

9.1.4 Semi-affine hull

Following proposition 9.6 proves that any finite or infinite intersection of semi-affine spaces remains a semi-affine space. In particular for any subset $X \subseteq \mathbb{Q}^m$, there exists a minimal (for $\subseteq$) semi-affine space written $\text{saff}(X)$ that contains X. This semi-affine space is called the *semi-affine hull* of X. The semi-vector space $\overrightarrow{\text{saff}(X)}$ is written $\overrightarrow{\text{saff}}(X)$.

Proposition 9.6. *Any finite or infinite intersection of semi-affine spaces remains a semi-affine space.*

Proof. Observe that a semi-affine space is a finite union of affine spaces that can be represented by a finite set of vectors in $\mathbb{Q}^m$. Hence the class of semi-affine spaces is *countable*. In order to prove the lemma, it is therefore sufficient to prove that $\bigcap_{n\in\mathbb{N}} S_n$ is a semi-affine space for any sequence $(S_n)_{n\in\mathbb{N}}$ of semi-affine spaces. As the class of semi-affine spaces is stable by finite intersection, we can also assume that $(S_n)_{n\in\mathbb{N}}$ is non-increasing. Let us prove by induction over the dimension $k \in \mathbb{N}\cup\{-1\}$ that any non-increasing sequence of semi-affine spaces $(S_n)_{n\in\mathbb{N}}$ such that $\dim(\overrightarrow{\mathrm{aff}}(S_0)) \leq k$, is ultimately stationary. Case $k=-1$ is immediate because in this case $S_n = \emptyset$ for any $n \in \mathbb{N}$. Now, assume the induction true for $k \geq -1$ and let us consider a non-increasing sequence of semi-affine spaces $(S_n)_{n\in\mathbb{N}}$ such that the dimension of $\overrightarrow{\mathrm{aff}}(S_0)$ is equal to $k+1$. Remark that if S_n is an affine space for any $n \geq 0$, then $(S_n)_{n\geq 0}$ is a non-increasing sequence of affine spaces. In particular, this sequence is ultimately constant. So, we can assume that there exists an integer $n_0 \geq 0$ such that S_{n_0} is not an affine space. There exists a finite class $\mathcal{C}$ of affine spaces such that $S_{n_0} = \bigcup_{A\in\mathcal{C}} A$. Let $A \in \mathcal{C}$. From $A \subseteq S_{n_0} \subseteq S_0 \subseteq \mathrm{aff}(S_0)$, we deduce that the dimension of $\overrightarrow{A}$ is less than or equal to $k+1$. Moreover, if it is equal to $k+1$, from $A \subseteq \mathrm{aff}(S_0)$, we deduce $A = \mathrm{aff}(S_0)$ and we get $S_{n_0} = A$ is an affine space which is a contradiction. As the sequence $(S_n \cap A)_{n\geq 0}$ is a non-increasing sequence of semi-affine spaces such that the dimension of $\overrightarrow{\mathrm{aff}}(S_n \cap A) \subseteq \overrightarrow{A}$ is less than or equal to k, the induction hypothesis proves that there exists $n_A \geq 0$ such that $S_n \cap A = S_{n_A} \cap A$ for any $n \geq n_A$. Let us consider $N = \max_{A\in\mathcal{C}}(n_0, n_A)$. For any $n \geq N$, we have $S_n \subseteq S_{n_0} = \bigcup_{A\in\mathcal{C}} A$ and $S_n \cap A = S_N \cap A$. Hence $S_n = S_n \cap (\bigcup_{A\in\mathcal{C}} A) = \bigcup_{A\in\mathcal{C}}(S_n \cap A) = \bigcup_{A\in\mathcal{C}}(S_N \cap A) = S_N \cap (\bigcup_{A\in\mathcal{C}} A) = S_N$ for any $n \geq N$ and we have proved the induction. □

Example 9.7. The semi-affine hull of a *finite* subset $X \subseteq \mathbb{Q}^m$ is equal to X because X is the finite union over $x \in X$ of the affine spaces $\{x\}$. The semi-affine hull of an *infinite* subset $X \subseteq \mathbb{Q}$ (remark that $m=1$) is equal to $\mathbb{Q}$. In fact, the class of affine spaces of $\mathbb{Q}$ is equal to $\{\mathbb{Q}, \emptyset\} \cup \{\{x\};\ x \in \mathbb{Q}\}$.

Remark 9.8. As $\mathrm{aff}(X)$ is an affine space and in particular a semi-affine space that contains X, we deduce that $\mathrm{saff}(X) \subseteq \mathrm{aff}(X)$. This last inclusion can be strict as shown by the example $X = \{\mathbf{e}_{0,m}, \ldots, \mathbf{e}_{m,m}\}$. In fact, in this case, we have $\mathrm{saff}(X) = X$ and $\mathrm{aff}(X) = \mathbb{Q}^m$.

The following lemma will be useful to compute the semi-affine hull of some subsets of $\mathbb{Q}^m$ (see example 9.10).

Lemma 9.9 (Covering lemma).

- *For any affine function $f : \mathbb{Q}^m \to \mathbb{Q}^{m'}$ and for any subset $X \subseteq \mathbb{Q}^m$, we have* $\mathrm{saff}(f(X)) = f(\mathrm{saff}(X))$.
- *For any subsets $X, X' \subseteq \mathbb{Q}^m$, we have*
  - $\mathrm{saff}(X \times X') = \mathrm{saff}(X) \times \mathrm{saff}(X')$,

- $\text{saff}(X \cup X') = \text{saff}(X) \cup \text{saff}(X')$, *and*
- $\text{saff}(X + X') = \text{saff}(X) + \text{saff}(X')$.

Proof. Let us consider an affine function f. From $X \subseteq \text{saff}(X)$, we deduce $f(X) \subseteq f(\text{saff}(X))$. As $f(\text{saff}(X))$ is a semi-affine space that contains $f(X)$ (observe that $f(A)$ is an affine space for any affine space A and for any affine function f), by minimality of the semi-affine hull, we deduce $\text{saff}(f(X)) \subseteq f(\text{saff}(X))$. Let us prove the converse inclusion. As $f(X) \subseteq \text{saff}(f(X))$, we have $X \subseteq f^{-1}(\text{saff}(f(X)))$. As $f^{-1}(\text{saff}(f(X)))$ is a semi-affine space (observe that $f^{-1}(A)$ is an affine space for any affine space A and for any affine function f), by minimality of the semi-affine hull, we get $\text{saff}(X) \subseteq f^{-1}(\text{saff}(f(X)))$. Hence $f(\text{saff}(X)) \subseteq f(f^{-1}(\text{saff}(f(X))))$. Recall that for any function $g : A \to B$, and for any subset $Y \subseteq B$, we have $g(g^{-1}(Y)) = g(A) \cap Y$. Hence $f(f^{-1}(\text{saff}(f(X)))) = f(\mathbb{Q}^m) \cap \text{saff}(f(X))$. From $f(X) \subseteq f(\mathbb{Q}^m)$, we also deduce $\text{saff}(f(X)) \subseteq f(\mathbb{Q}^m)$ and we get $f(\mathbb{Q}^m) \cap \text{saff}(f(X)) = \text{saff}(f(X))$. Therefore $f(\text{saff}(X)) \subseteq \text{saff}(f(X))$.

Let us consider $X, X' \subseteq \mathbb{Q}^m$ and let us prove that $\text{saff}(X \cup X') = \text{saff}(X) \cup \text{saff}(X')$. From $X \cup X' \subseteq \text{saff}(X) \cup \text{saff}(X')$, we deduce by minimality of the semi-affine hull $\text{saff}(X \cup X') \subseteq \text{saff}(X) \cup \text{saff}(X')$. Moreover, from $X \subseteq X \cup X' \subseteq \text{saff}(X \cup X')$, we get $\text{saff}(X) \subseteq \text{saff}(X \cup X')$ and symmetrically $\text{saff}(X') \subseteq \text{saff}(X \cup X')$. We have shown $\text{saff}(X) \cup \text{saff}(X') \subseteq \text{saff}(X \cup X')$.

Let us consider $X, X' \subseteq \mathbb{Q}^m$ and let us prove that $\text{saff}(X \times X') = \text{saff}(X) \times \text{saff}(X')$. From $X \times X' \subseteq \text{saff}(X) \times \text{saff}(X')$, we deduce that $\text{saff}(X \times X') \subseteq \text{saff}(X) \times \text{saff}(X')$. By considering the affine function $f_{1,x} : \mathbb{Q}^m \to \mathbb{Q}^{2m}$ defined by $f_{1,x}(x') = (x, x')$, we get $\text{saff}(\{x\} \times X') = \{x\} \times \text{saff}(X')$ for any $x \in X$. From $\{x\} \times X' \subseteq X \times X'$, we deduce $\text{saff}(\{x\} \times X') \subseteq \text{saff}(X \times X')$. So $X \times \text{saff}(X') \subseteq \text{saff}(X \times X')$. In particular, for any $x' \in \text{saff}(X')$, we have $X \times \{x'\} \subseteq \text{saff}(X \times X')$. Affine function $f_{2,x'} : \mathbb{Q}^m \to \mathbb{Q}^{2m}$ defined by $f_{2,x'}(x) = (x, x')$ proves that $\text{saff}(X) \times \{x'\} \subseteq \text{saff}(X \times X')$ for any $x' \in \text{saff}(X')$. So, we have proved $\text{saff}(X) \times \text{saff}(X') \subseteq \text{saff}(X \times X')$.

Let us consider $X, X' \subseteq \mathbb{Q}^m$ and let us prove that $\text{saff}(X + X') = \text{saff}(X) + \text{saff}(X')$. By considering the affine function $f : \mathbb{Q}^{2m} \to \mathbb{Q}^m$ defined by $f(x, x') = x + x'$, we deduce that $\text{saff}(X) \times \text{saff}(X') = f(\text{saff}(X) \times \text{saff}(X')) = f(\text{saff}(X \times X')) = \text{saff}(f(X \times X')) = \text{saff}(X + X')$. □

Example 9.10. The semi-affine hull of $\mathbb{N}^m$ is equal to $\mathbb{Q}^m$. In fact, from covering lemma 9.9, we deduce $\text{saff}(\mathbb{N}^m) = \sum_{i=1}^m \text{saff}(\mathbb{N}.\mathbf{e}_{i,m}) = \sum_{i=1}^m \text{saff}(\mathbb{N}).\mathbf{e}_{i,m} = \sum_{i=1}^m \mathbb{Q}.\mathbf{e}_{i,m} = \mathbb{Q}^m$.

9.1.5 Cyclic sets

Recall that a (r, m, σ)-cyclic set X where $\sigma \in \Sigma_{r,m}^*$ is a subset of $\mathbb{Z}^m$ such that $\gamma_{r,m,\sigma}^{-1}(X) = X$. The following proposition 9.11 shows that the semi-affine hull of a (r, m, σ)-cyclic set $X \subseteq \mathbb{Z}^m$ is a finite union of affine spaces of the form $\xi_{r,m}(\sigma) + V$ where V is a vector space.

Proposition 9.11. *We have* $\mathrm{saff}(X) = \xi_{r,m}(\sigma) + \overrightarrow{\mathrm{saff}}(X)$ *for any* (r, m, σ)*-cyclic set* $X \subseteq \mathbb{Z}^m$.

Proof. It is sufficient to prove that for any affine component A of $\mathrm{saff}(X)$, we have $\xi_{r,m}(s) \in A$. Consider $x \in X$. As $\gamma^{-1}_{r,m,\sigma}(X) = X$ then $\gamma^k_{r,m,\sigma}(x) = r^{k.|\sigma|}.(x - \xi(\sigma)) + \xi(\sigma) \in X$ for any $k \in \mathbb{N}$. Covering lemma 9.9 proves that $\mathbb{Q}.(x - \xi_{r,m}(\sigma)) + \xi_{r,m}(\sigma) \subseteq \mathrm{saff}(X)$. In particular, for any $\lambda \in \mathbb{Q}$, we have $\lambda.(X - \xi_{r,m}(\sigma)) + \xi_{r,m}(\sigma) \subseteq \mathrm{saff}(X)$. From covering lemma 9.9, we also prove that $\lambda.(\mathrm{saff}(X) - \xi_{r,m}(\sigma)) + \xi_{r,m}(\sigma) \subseteq \mathrm{saff}(X)$. Let A be an affine component of $\mathrm{saff}(X)$. We have proved that $\mathbb{Q}.(A - \xi_{r,m}(\sigma)) + \xi_{r,m}(\sigma) \subseteq \mathrm{saff}(X)$. From $A \subseteq \mathbb{Q}.(A - \xi_{r,m}(\sigma)) + \xi_{r,m}(\sigma) \subseteq \mathrm{saff}(X)$, we deduce by maximality of the affine component A, the equality $A = \mathbb{Q}.(A - \xi(\sigma)) + \xi_{r,m}(\sigma)$. In particular $\xi_{r,m}(\sigma) \in A$. □

9.2 Semi-affine lattices

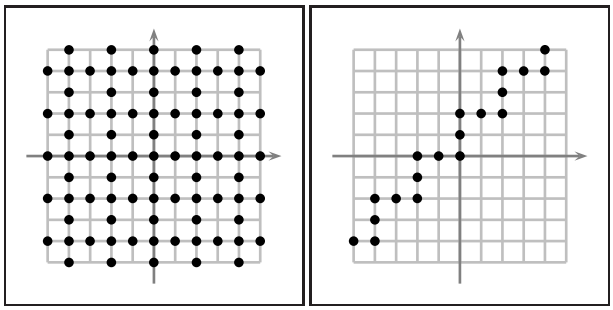

Fig. 9.2. On the left a semi-$\mathbb{Q}^2$-affine lattice P_1. On the right a semi-$\mathbb{Q}.(1, 1)$-affine lattice P_2.

A *semi-V-affine lattice* P is a finite union of V-affine lattices. Observe that the class of semi-V-affine lattice is stable by boolean combinations.

Lemma 9.12. *For any non-empty semi-V-affine lattice, there exists a non-empty finite set* $B \subseteq \mathbb{Q}^m$ *and a V-vector lattice M such that $P = B + M$.*

Proof. There exists a non-empty finite sequence $(a_j, M_j)_{j\in J}$ where $a_j \in \mathbb{Q}^m$ and M_j is a V-vector lattice such that $P = \bigcup_{j\in J}(a_j + M_j)$. From lemma 8.8, we deduce that $M = \bigcap_{j\in J} M_j$ is a V-vector lattice. Since $M \subseteq M_j$, theorem 8.10 shows that there exists a finite set $B_j \subseteq M_j$ such that $M_j = B_j + M$. We have proved that $P = B + M$ where B is the finite set $B = \bigcup_{j\in J}(a_j + B_j)$. □

The *group of invariants* $\mathrm{inv}(X)$ of a subset $X \subseteq \mathbb{Q}^m$ is the group of vectors $v \in \mathbb{Q}^m$ that let X invariant: we have $X - v = X$.

Lemma 9.13. *The group of invariants of a non empty semi-V-affine lattice is a V-vector lattice.*

Proof. Let P be a non-empty semi-V-affine lattice. Lemma 9.12 proves that there exists a non-empty finite set $B \subseteq \mathbb{Q}^m$ and a V-vector lattice M such that $P = B + M$. Let us show that $\mathrm{inv}(P) \subseteq (V \cap (B - B)) + M$. Consider a vector $v \in \mathrm{inv}(P)$. Let $b \in B$. Since $P - k.v = P$ for any $k \in \mathbb{N}$, there exists $b_k \in B$ and $m_k \in M$ such that $b - k.v = b_k + m_k$. Since B is finite, there exists $k_1 < k_2$ such that $b_{k_1} = b_{k_2}$. We deduce that $(k_1 - k_2).v = m_{k_2} - m_{k_1}$. In particular $v \in V$ since $M \subseteq V$. Moreover, from $v = b - b_1 + m_1$ and $m_1 \in M \subseteq V$, we get $b - b_1 \in V$. We have proved that $v \in (V \cap (B - B)) + M$. Thus $\mathrm{inv}(P)$ is included in the discrete set $(V \cap (B - B)) + M$ and we have proved that $\mathrm{inv}(P)$ is a vector lattice. Let us prove that $\mathrm{vec}(\mathrm{inv}(P)) = V$. From $\mathrm{inv}(P) \subseteq (V \cap (B - B)) + M$ we get $\mathrm{vec}(\mathrm{inv}(P)) \subseteq V$. Moreover, from $M \subseteq \mathrm{inv}(P)$ we get $V = \mathrm{vec}(M) \subseteq \mathrm{vec}(\mathrm{inv}(P))$. Therefore $\mathrm{inv}(P)$ is a V-vector lattice. □

The V-vector lattice of invariants of a non-empty semi-V-affine lattice is geometrically characterized by the following proposition 9.14.

Proposition 9.14. *Let P be a non-empty semi-V-affine lattice and let M be a V-vector lattice. There exists a finite subset $B \subseteq \mathbb{Z}^m$ such that $P = B + M$ if and only if $M \subseteq inv(P)$.*

Proof. Observe that if there exists a finite set $B \subseteq \mathbb{Z}^m$ such that $P = B + M$, we deduce that $M \subseteq \mathrm{inv}(P)$. Let us now prove the converse. Assume that M is a V-vector lattice such that $M \subseteq \mathrm{inv}_V(P)$ and let us prove that there exists a finite set $B \subseteq \mathbb{Z}^m$ such that $P = B + M$. Lemma 9.12 proves that there exists a non-empty finite set $B_0 \subseteq \mathbb{Q}^m$ and a V-vector lattice M_0 such that $P = B_0 + M_0$. As $M \subseteq \mathrm{inv}(P)$, we deduce that $P = B_0 + M_0 + M$. Since $M \subseteq M_0 + M$, theorem 8.10 proves that there exists a finite set $B_1 \subseteq M_0 + M$ such that $M_0 + M = B_1 + M$. Therefore $P = B + M$ where $B = B_0 + B_1$. □

Proposition 9.15. *Let M be a V-vector lattice and let B be a non-empty finite subset of $\mathbb{Q}^m$. We can compute in polynomial time the V-vector lattice of invariants of $P = B + M$.*

Proof. Let us fix a vector $b_0 \in B$ and let us prove that the V-vector lattice of invariant $\mathrm{inv}(P)$ is equal to the V-vector lattice M' generated by M and the vectors $v \in B - b_0$ such that $v + B + M = B + M$. Observe that $M' \subseteq \mathrm{inv}(P)$. Conversely, let $x \in \mathrm{inv}(P)$. We have $x + B + M = B + M$. In particular $x + b_0 \in B + M$ and we deduce that there exists $v \in B - b_0$ and $m \in M$ such that $x = v + m$. Observe that $x + B + M = B + M$ implies $v + B + M = B + M$. Thus $x \in M'$ and we have proved that $\mathrm{inv}(P) = M'$. Note that a vector

$v \in \mathbb{Q}^m$ satisfies $v + B + M = B + M$ if and only if for any $b \in B$ there exists $b' \in B$ such that $v + b - b' \in M$. Since we can decide in polynomial time if a vector is in M, we are done. □

Corollary 9.16. *Given two semi-affine lattice $P_1 = B_1 + M_1$ and $P_2 = B_2 + M_2$ where B_1, B_2 are two finite subsets of $\mathbb{Q}^m$, and M_1, M_2 are two vector lattices, we can decide in polynomial time if $B_1 + M_1 = B_2 + M_2$.*

Proof. Naturally if B_1 and B_2 are both empty then $P_1 = P_2$ and if only one of then is empty then $P_1 \neq P_2$. Thus, without loss of generality, we cam assume that B_1 and B_2 are non empty. From proposition 9.15, we deduce that $\text{inv}(P_1)$ and $\text{inv}(P_2)$ are computable in polynomial time. Observe that if $\text{inv}(P_1) \neq \text{inv}(P_2)$ then $P_1 \neq P_2$. Hence we can assume that there exists a vector lattice M such that $\text{inv}(P_1) = M = \text{inv}(P_2)$. We have reduced our problem to decide if $B_1 + M_1 = B_2 + M_2$ where M_1 and M_2 are equal to a V-vector lattice M. Let S_1 and S_2 be the semi-V-affine spaces $S_i = \bigcup_{b \in B_i} (b+V)$. If $S_1 \neq S_2$ then $P_1 \neq P_2$. So, we can assume that there exists a semi-V-vector space S such that $S_1 = S = S_2$. Remark that $P_1 = P_2$ if and only if $(B_1 \cap A) + M = (B_2 \cap A) + M$ for any affine component A of S. Thus we can assume that B_1 and B_2 are included into a V-affine space A. Let $a_0 \in A$ (for instance take $a_0 \in B_1$) and notice that $P_1 = P_2$ if and only if $(B_1 - a_0) + M = (B_2 - a_0) + M$. Hence, we can assume that B_1 and B_2 are included in V. From an Hermite I-representation of M, we get in linear time a $\mathbb{Z}$-basis v_1, ..., v_d of M. Let us consider the function $\lambda \in V \to \mathbb{Q}^d$ defined by $\lambda(v)$ is the unique $x \in \mathbb{Q}^d$ such that $0 \leq x[i] < 1$ and such that there exists $k \in \mathbb{Z}^d$ satisfying $v = \sum_{i=1}^{d} (x + k)[i].v_i$. Note that $\lambda(v)$ is computable in polynomial time and $B_1 + M = B_2 + M$ if and only if $\lambda(B_1) = \lambda(B_2)$. Thus, we can decide in polynomial time if $B_1 + M = B_2 + M$. □

Example 9.17. Let P_1 be the semi-$\mathbb{Q}^2$-affine lattice $P_1 = \{(0,0), (1,0), (0,1)\} + 2.\mathbb{Z}^2$ and let P_2 be the semi-$\mathbb{Q}.(1,1)$-affine lattice $P_2 = \{(0,0), (0,1), (0,2), (1,2)\} + \mathbb{Z}.(2,2)$ given in figure 9.2. We have $\text{inv}(P_1) = \mathbb{Z}.(2,0) + \mathbb{Z}.(0,2)$ and $\text{inv}(P_2) = \mathbb{Z}.(2,2)$.

9.3 Semi-patterns

A *V-pattern* is a V-affine lattice included in $\mathbb{Z}^m$ and a *semi-V-pattern* is a semi-V-affine lattice included in $\mathbb{Z}^m$.

Observe that the the V-lattice $\text{inv}(P)$ of a non-empty semi-V-pattern P is included in $\mathbb{Z}^m \cap V$ and if P is empty then $\text{inv}(P) = V$. We denote by $\text{inv}_V(P)$ the V-vector lattice $\text{inv}_V(P) = \mathbb{Z}^m \cap V \cap \text{inv}(X)$ for any (empty or non-empty) semi-V-pattern P.

9.3.1 Inverse image by $\gamma_{r,m,\sigma}$

Proposition 9.18 proves that the class of semi-patterns is stable by inverse image by $\gamma_{r,m,\sigma}$ where $\sigma \in \Sigma_r^*$.

Proposition 9.18. *Let B be a finite subset of $\mathbb{Z}^m$ and let M be a V-vector lattice included in $\mathbb{Z}^m$. For any word $\sigma \in \Sigma_r^*$, we can compute in polynomial time a finite set $B_\sigma \subseteq \mathbb{Z}^m$ such that $|B_\sigma| \leq |B|$ and $\gamma_{r,m,\sigma}^{-1}(B+M) = B_\sigma + \gamma_{r,m,0}^{-|\sigma|}(M)$.*

Proof. Let us consider for each $b \in B$ such that $\gamma_{r,m,\sigma}(\mathbb{Z}^m) \cap (b+M) \neq \emptyset$, a vector $b' \in \mathbb{Z}^m$ such that $\gamma_{r,m,\sigma}(b') \in b+M$. We denote by B' the set of $b' \in \mathbb{Z}^m$ obtained. Note that corollary 8.16 provides a polynomial time algorithm for computing B'. Let us prove that $\gamma_{r,m,\sigma}^{-1}(B+M) = B' + \gamma_{r,m,0}^{-|\sigma|}(M)$. Let $x \in B' + \gamma_{r,m,0}^{-|\sigma|}(M)$. That means, there exists $b' \in B'$ such that $\gamma_{r,m,0}^{|\sigma|}(x-b') \in M$. Moreover, by definition of b', there exists $b \in B$ such that $\gamma_{r,m,\sigma}(b') \in b+M$. From $\gamma_{r,m,0}^{|\sigma|}(x-b') = \gamma_{r,m,\sigma}(x) - \gamma_{r,m,0}^{-|\sigma|}(b')$, we get $\gamma_{r,m\sigma}(x) \in B+M$. Therefore $x \in \gamma_{r,m,\sigma}^{-1}(B+M)$, and we have proved the inclusion $B' + \gamma_{r,m,0}^{-|\sigma|}(M) \subseteq \gamma_{r,m,\sigma}^{-1}(B+M)$. For the converse inclusion, consider $x \in \gamma_{r,m,\sigma}^{-1}(B+M)$. There exists $b \in B$ such that $\gamma_{r,m,\sigma}(x) \in b+M$. By construction, there exists $b' \in \mathbb{Z}^m$ such that $\gamma_{r,m,\sigma}(b') \in b+M$. Hence $\gamma_{r,m,\sigma}(x) - \gamma_{r,m,\sigma}(b') \in M$. From $\gamma_{r,m,0}^{|\sigma|}(x-b') = \gamma_{r,m,\sigma}(x) - \gamma_{r,m,\sigma}(b')$, we get $\gamma_{r,m,0}^{|\sigma|}(x-b') \in M$. Therefore $x \in b' + \gamma_{r,m,0}^{-|\sigma|}(M)$ and we have proved the other inclusion. □

9.3.2 Relatively prime properties

A semi-V-pattern P is said *relatively prime* with r if the V-lattice $\mathrm{inv}_V(P)$ is relatively prime with r. From lemma 8.11 we deduce that the class of relatively prime semi-V-patterns is stable by boolean combinations. In fact, consider two semi-V-patterns P_1 and P_2 and $\# \in \{\cup, \cap, \setminus, \Delta\}$. Observe that $\mathrm{inv}_V(P_1) \cap \mathrm{inv}_V(P_2) \subseteq \mathrm{inv}_V(P_1 \# P_2) \subseteq \mathbb{Z}^m \cap V$. From these inclusions, lemma 8.11 proves $|\mathbb{Z}^m \cap V / \mathrm{inv}_V(P_1 \# P_2)| . |\mathrm{inv}_V(P_1 \# P_2) / \mathrm{inv}_V(P_1) \cap \mathrm{inv}_V(P_2)|$ is equal to the integer $|\mathbb{Z}^m \cap V / \mathrm{inv}_V(P_1) \cap \mathrm{inv}_V(P_2)|$. As $\mathrm{inv}_V(P_1)$ and $\mathrm{inv}_V(P_2)$ are two V-lattices relatively prime with r, we deduce that $\mathrm{inv}_V(P_1) \cap \mathrm{inv}_V(P_2)$ is relatively prime with r. In particular $|\mathbb{Z}^m \cap V / \mathrm{inv}_V(P_1 \# P_2)|$ divides an integer relatively prime with r and we deduce that this integer is relatively prime with r. Hence $P_1 \# P_2$ is relatively prime with r.

The following lemma provides a geometrical characterization of these semi-V-patterns. This characterization and proposition 9.18 prove that the class of semi-V-patterns relatively prime with r is stable by inverse image by $\gamma_{r,m\sigma}$ for any $\sigma \in \Sigma_{r,m}^*$.

Lemma 9.19. *A semi-V-pattern is relatively prime with r if and only if there exists a V-lattice M relatively prime with r and a finite set $B \subseteq \mathbb{Z}^m$ such that $P = B + M$.*

Proof. Remark that if P is relatively prime with r then there exists a finite subset $B \subseteq \mathbb{Z}^m$ such that $P = B + \mathrm{inv}_V(X)$. Conversely, assume that there exists a V-lattice M relatively prime with r and a finite set $B \subseteq \mathbb{Z}^m$ such that $P = B + M$ and let us prove that P is relatively prime with r. Since $M \subseteq \mathrm{inv}_V(X) \subseteq \mathbb{Z}^m \cap V$, lemma 8.11 shows that $|\mathbb{Z}^m \cap V/\mathrm{inv}_V(X)|.|\mathrm{inv}_V(X)/M| = |\mathbb{Z}^m \cap V/M|$. As $|\mathbb{Z}^m \cap V/M|$ is relatively prime with r, we deduce that $|\mathbb{Z}^m \cap V/\mathrm{inv}_V(X)|$ is relatively prime with r. Thus P is relatively prime with r. □

The class of semi-V-patterns relatively prime with r that are also included into a V-affine space naturally appear when computing the inverse image of a semi-V-pattern by $\gamma_{r,m,\sigma}$ when σ is a word enough longer in $\Sigma_{r,m}^*$ as proved by the following proposition 9.21.

Lemma 9.20. *Any (r, m, w)-cyclic semi-V-pattern P is relatively prime with r and included in the V-affine space $A = \xi_{r,m}(w) + V$.*

Proof. As P is (r, m, w)-cyclic, we deduce that $P = \gamma_{r,m,w^k}^{-1}(P)$ for any $k \in \mathbb{N}$. From proposition 9.18, we deduce that P is relatively prime with r. Moreover, from proposition 9.11, we get $\mathrm{saff}(P) = \xi_{r,m}(w) + \overrightarrow{\mathrm{saff}}(P)$. As P is a semi-V-pattern, we deduce that $\overrightarrow{\mathrm{saff}}(P)$ is either empty or equal to V. Hence $\mathrm{saff}(P) \subseteq \xi_{r,m}(w) + V$. From $P \subseteq \mathrm{saff}(P)$, we are done. □

Proposition 9.21. *The class of semi-V-pattern relatively prime with r and included into a V-affine space is stable by inverse image by $\gamma_{r,m,\sigma}$ for any $\sigma \in \Sigma_{r,m}^*$. Moreover, given a general semi-V-pattern P, there exists an integer $k \in \mathbb{N}$ such that $\gamma_{r,m,\sigma}^{-1}(P)$ is a semi-V-pattern relatively prime with r and included into a V-affine space for any word $\sigma \in \Sigma_{r,m}^{\geq k}$.*

Proof. Let us first consider a semi-V-pattern P relatively prime with r and included into a V-affine space A, let $\sigma \in \Sigma_{r,m}^*$ and let us prove that $\gamma_{r,m,\sigma}^{-1}(P)$ is a semi-V-pattern relatively prime with r and included into a V-affine space. Recall that we have previously proved that $\gamma_{r,m,\sigma}^{-1}(P)$ is a semi-V-pattern relatively prime with r. Since $P \subseteq A$, we deduce that $\gamma_{r,m,\sigma}^{-1}(P) \subseteq A'$ where A' is the V-affine space $A' = \Gamma_{r,m,\sigma}^{-1}(A)$. We are done.

Now, let us consider a general semi-V-pattern there exists an integer $k \in \mathbb{N}$ such that $\gamma_{r,m,\sigma}^{-1}(P)$ is a semi-V-pattern relatively prime with r and included into a V-affine space for any word $\sigma \in \Sigma_{r,m}^{\geq k}$. Since P is Presburger-definable, there exists a FDVA $\mathcal{A}$ that represents P in basis r. Let us consider the integer $k = |\mathcal{A}|$ the number of principal states of $\mathcal{A}$. Now consider $\sigma \in \Sigma_{r,m}^*$. Since $|\sigma| \geq |\mathcal{A}|$, the word σ can be decomposed in $\sigma = \sigma_1.\sigma_2$ such that there exists a loop $q \xrightarrow{w} q$ where $w \in \Sigma_{r,m}^+$ and $q = \delta(q_0, \sigma_1)$. As $P_q = \gamma_{r,m,\sigma_1}^{-1}(P)$ this set is a semi-V-pattern. Moreover, as $\gamma_{r,m,w}^{-1}(P_q) = P_q$, lemma 9.20 proves that P_q

is relatively prime r and included in a V-affine space. Finally, as $\gamma^{-1}_{r,m,\sigma}(P) = \gamma^{-1}_{r,m,\sigma_2}(P_q)$, the previous paragraph shows that $\gamma^{-1}_{r,m,\sigma}(P)$ is relatively prime with r and included into a V-affine space. □

Given a non-empty semi-V-pattern P included into a V-affine space A, we naturally deduce that $\gamma^{-1}_{r,m,\sigma}(A) = \emptyset$ implies $\gamma^{-1}_{r,m,\sigma}(P) = \emptyset$. The class of semi-$V$-pattern relatively prime r that are included into a V-affine space plays an important role since the following corollary 9.23 intensively used in the sequel proved that for this class, the converse is true: $\gamma^{-1}_{r,m,\sigma}(P) = \emptyset$ implies $\gamma^{-1}_{r,m,\sigma}(A) = \emptyset$.

Lemma 9.22. *Let P be a semi-V-pattern relatively prime with r and included into a V-affine space A. We have $\gamma^{-1}_{r,m,\sigma}(P) = \xi_{r,m}(s) + P - \rho_{r,m}(\sigma, s)$ for any semi-V-pattern P relatively prime with r and included into a V-affine space A and for any (r,m)-decomposition (σ, s) such that $\rho_{r,m}(\sigma, s) \in A$ and such that $r^{|\sigma|_m} \in 1 + |\mathbb{Z}^m \cap V/inv_V(P)|.\mathbb{Z}$.*

Proof. Let us consider $x \in \gamma^{-1}_{r,m,\sigma}(P)$. We have $\gamma_{r,m,\sigma}(x) = r^{|\sigma|_m}.x + \rho_{r,m}(\sigma, s)$. Hence $r^{|\sigma|_m}.(x - \xi_{r,m}(s)) \in P - \rho_{r,m}(\sigma, s)$. In particular, from $P \subseteq A$ and $\rho_{r,m}(\sigma, s) \in A$, we deduce that $r^{\sigma}.(x - \xi_{r,m}(s)) \in V$. Hence $x - \xi_{r,m}(s) \in \mathbb{Z}^m \cap V$. From $r^{|\sigma|_m} \in 1 + |\mathbb{Z}^m \cap V/\mathrm{inv}_V(P)|$, we deduce that $(r^{|\sigma|_m} - 1).(x - \xi_{r,m}(s)) \in \mathrm{inv}_V(P)$. As $x - \xi_{r,m}(s) \in P - (r^{|\sigma|_m} - 1).(x - \xi_{r,m}(s)) - \rho_{r,m}(\sigma, s)$, we get $x \in \xi_{r,m}(s) + P - \rho_{r,m}(\sigma, s)$ and we have proved the inclusion $\gamma^{-1}_{r,m,\sigma}(P) \subseteq \xi_{r,m}(s) + P - \rho_{r,m}(\sigma, s)$. For the converse inclusion, let $x \in \xi_{r,m}(s) + P - \rho_{r,m}(\sigma, s)$. From $\gamma_{r,m,\sigma}(x) = r^{|\sigma|_m}.(x - \xi_{r,m}(s)) + \rho_{r,m}(\sigma, s)$, we deduce that there exists $p \in P$ such that $\gamma_{r,m,\sigma}(x) = r^{|\sigma|_m}.(p - \rho_{r,m}(\sigma, s)) + \rho_{r,m}(\sigma, s)$. Hence $\gamma_{r,m,\sigma}(x) = p + (r^{|\sigma|_m} - 1).(p - \rho_{r,m}(\sigma, s))$. As $\rho_{r,m}(\sigma, s)$ and p are both in A, we deduce that $p - \rho_{r,m}(\sigma, s) \in \mathbb{Z}^m \cap V$. Moreover, as $r^{|\sigma|_m} - 1 \in |\mathbb{Z}^m \cap V/\mathrm{inv}_V(X)|.\mathbb{N}$, we deduce that $(r^{|\sigma|_m} - 1).(p - \rho_{r,m}(\sigma, s)) \in \mathrm{inv}_V(P)$. From $p \in P$, we get $\gamma_{r,m,\sigma}(x) \in P$ and we have proved the other inclusion $\xi_{r,m}(s) + P - \rho_{r,m}(\sigma, s) \subseteq \gamma^{-1}_{r,m,\sigma}(P)$. □

Corollary 9.23 (Dense pattern corollary). *Let P be a non-empty semi-V-pattern relatively prime with r and included into a V-affine space A. The set $\gamma^{-1}_{r,m,\sigma}(P)$ is a non-empty semi-$\Gamma^{-|\sigma|}_{r,m,0}(V)$-pattern relatively prime with r and included into the $\Gamma^{-|\sigma|}_{r,m,0}(V)$-affine space $\Gamma^{-1}_{r,m,\sigma}(A)$ for any word $\sigma \in \Sigma^*_r$ such that $\gamma^{-1}_{r,m,\sigma}(A) \neq \emptyset$.*

Proof. As $\gamma^{-1}_{r,m,\sigma}(A)$ is non empty, there exists a couple (w, s) such that $\rho_{r,m}(w, s) \in \gamma^{-1}_{r,m,\sigma}(A)$ and such that $|\sigma| + |w| \in m.\mathbb{Z}$. By replacing w by a word in $w.s^*$, we can assume without loss of generality that $r^{|\sigma.w|_m} \in 1 + |\mathbb{Z}^m \cap V/\mathrm{inv}_V(P)|.\mathbb{Z}$. From lemma 9.22, we deduce that $\gamma^{-1}_{r,m,\sigma.w}(P) = \xi_{r,m}(s) + P - \rho_{r,m}(\sigma.w, s)$. As $\gamma^{-1}_{r,m,\sigma.w}(P) = \gamma^{-1}_{r,m,w}(\gamma^{-1}_{r,m,\sigma}(P))$ and $\gamma^{-1}_{r,m,\sigma.w}(P) \neq \emptyset$, we deduce that $\gamma^{-1}_{r,m,\sigma}(P) \neq \emptyset$. From proposition 9.18 we deduce that $\gamma^{-1}_{r,m,\sigma}(P)$ is a semi-$\Gamma^{-|\sigma|}_{r,m,0}(V)$-pattern. Let us now show that $\gamma^{-1}_{r,m,\sigma}(P)$ is relatively

prime with r. Since $P \subseteq A$, we deduce that $\gamma_{r,m,\sigma}^{-1}(P)$ is included in the $\Gamma_{r,m,0}^{-|\sigma|}(V)$-affine space $\Gamma_{r,m,\sigma}^{-1}(A)$. Now, let us prove that $\gamma_{r,m,\sigma}^{-1}(P)$ is relatively prime with r. From proposition 9.18 we deduce that $\gamma_{r,m,0}^{-|\sigma|}(\mathrm{inv}_V(P)) \subseteq \mathrm{inv}_V(\gamma_{r,m,\sigma}^{-1}(P))$. As $\mathrm{inv}_V(P)$ is relatively prime with r we get $\gamma_{r,m,0}^{-\infty}(\mathrm{inv}_V(P)) = \mathrm{inv}_V(P)$. Hence $\gamma_{r,m,0}^{-\infty}(\gamma_{r,m,0}^{-|\sigma|}(\mathrm{inv}_V(P))) = \gamma_{r,m,0}^{-|\sigma|}(\gamma_{r,m,0}^{-\infty}(\mathrm{inv}_V(P))) = \gamma_{r,m,0}^{-|\sigma|}(\mathrm{inv}_V(P))$ and we have proved that $\gamma_{r,m,0}^{-|\sigma|}(\mathrm{inv}_V(P))$ is relatively prime with r. From the inclusion $\gamma_{r,m,0}^{-|\sigma|}(\mathrm{inv}_V(P)) \subseteq \mathrm{inv}_V(\gamma_{r,m,\sigma}^{-1}(P))$ and lemma 8.11, we deduce that $\mathrm{inv}_V(\gamma_{r,m,\sigma}^{-1}(P))$ is relatively prime with r. We are done. □

10

Degenerate Sets

Given a vector space V, a subset $X \subseteq \mathbb{Q}^m$ is said *V-degenerate* if V is not included in $\overrightarrow{\text{saff}}(\mathbb{Z}^m \cap X)$. The following lemma 10.1 shows that the binary relation $\sim^V$ defined over the subsets of $\mathbb{Q}^m$ by $X_1 \sim^V X_2$ if and only if $X_1 \Delta X_2$ is V-degenerate, is an equivalence relation. The equivalence class for $\sim^V$ of a subset $X \subseteq \mathbb{Q}^m$ is denote by $[X]^V$.

Lemma 10.1. *The binary relation $\sim^V$ is an equivalence.*

Proof. The binary relation $\sim^V$ is an equivalence relation. Naturally $\sim^V$ is reflexive and symmetric. So, it is sufficient to prove that $\sim^V$ is transitive. Consider $X_1, X_2, X_3 \subseteq \mathbb{Q}^m$ such that $X_1 \sim^V X_2$ and $X_2 \sim^V X_3$ and let us prove that $X_1 \sim^V X_3$. We have $\mathbb{Z}^m \cap (X_1 \Delta X_3) \subseteq (\mathbb{Z}^m \cap (X_1 \Delta X_2)) \cup (\mathbb{Z}^m \cap (X_2 \Delta X_3))$ and from insecable lemma 9.2, we deduce that V is not included in $\overrightarrow{\text{saff}}(\mathbb{Z}^m \cap (X_1 \Delta X_3))$. Hence $X_1 \sim^V X_3$. □

Given two equivalence classes $\mathcal{X}_1$ and $\mathcal{X}_2$ and a boolean operation $\# \in \{\cup, \cap, \setminus, \Delta\}$, the following lemma 10.2 shows that $[X_1 \# X_2]^V$ is independent of $X_1 \in \mathcal{X}_1$ and $X_2 \in \mathcal{X}_2$. This equivalence class is naturally denoted by $\mathcal{X}_1 \#^V \mathcal{X}_2$.

Lemma 10.2. *We have $[X_1 \# X_2]^V = [X_1' \# X_2']^V$ for any $X_1, X_1', X_2, X_2' \subseteq \mathbb{Q}^m$ such that $X_1 \sim^V X_1'$ and $X_2 \sim^V X_2'$ and for any $\# \in \{\cup, \cap, \setminus, \Delta\}$.*

Proof. Let us prove that $(X_1 \# X_2) \Delta (X_1' \# X_2') \subseteq (X_1 \Delta X_1') \# (X_2 \Delta X_2')$ for any $X_1, X_1', X_2, X_2' \subseteq \mathbb{Q}^m$ and for any $\# \in \{\cup, \cap, \setminus, \Delta\}$.

Case $\#$ equals to Δ: in this case, we have the equality $(X_1 \# X_2) \Delta (X_1' \# X_2') = (X_1 \Delta X_1') \# (X_2 \Delta X_2')$ and we are done.

Case $\#$ equals to $\cap$: we have $(X_1 \# X_2) \Delta (X_1' \# X_2') = ((X_1 \cap X_2) \setminus (X_1' \cap X_2')) \cup ((X_1' \cap X_2') \setminus (X_1 \cap X_2))$. Remark that $(X_1 \cap X_2) \setminus (X_1' \cap X_2') = ((X_1 \cap X_2) \setminus X_1') \cup ((X_1 \cap X_2) \setminus X_2')$. From $(X_1 \cap X_2) \setminus X_1' \subseteq X_1 \setminus X_1'$ and $(X_1 \cap X_2) \setminus X_2' \subseteq X_2 \setminus X_2'$, we deduce that $(X_1 \cap X_2) \setminus (X_1' \cap X_2') \subseteq (X_1 \setminus X_1') \cup (X_2 \setminus X_2') \subseteq (X_1 \Delta X_1') \cup (X_2 \Delta X_2')$. By symmetry, we also get $(X_1' \cap X_2') \setminus (X_1 \cap X_2) \subseteq (X_1 \Delta X_1') \cup (X_2 \Delta X_2')$. We are done.

Case # equals to \: this case can be reduced to the previous case ∩. In fact, if # is equal to \ then $(X_1\#X_2)\Delta(X_1'\#X_2') = (X_1 \cap (\mathbb{Q}^m\backslash X_2))\Delta(X_1' \cap (\mathbb{Q}^m\backslash X_2'))$. From the previous case ∩, we deduce that $(X_1\cap(\mathbb{Q}^m\backslash X_2))\Delta(X_1'\cap(\mathbb{Q}^m\backslash X_2')) \subseteq (X_1\Delta X_1') \cup ((\mathbb{Q}^m\backslash X_2)\Delta(\mathbb{Q}^m \cap X_2')$. As $(\mathbb{Q}^m\backslash X_2)\Delta(\mathbb{Q}^m \cap X_2') = X_2\Delta X_2'$, we are done.

Case # equals to ∪: we have $(X_1\#X_2)\Delta(X_1'\#X_2') = ((X_1 \cup X_2)\backslash(X_1' \cup X_2')) \cup ((X_1' \cup X_2')\backslash(X_1 \cup X_2))$. Remark that $(X_1 \cup X_2)\backslash(X_1' \cup X_2') = (X_1\backslash(X_1' \cup X_2')) \cup (X_2\backslash(X_1' \cup X_2'))$. From $X_1\backslash(X_1' \cup X_2') \subseteq X_1\backslash X_1'$ and $X_2\backslash(X_1' \cup X_2') \subseteq X_2\backslash X_2'$, we deduce that $(X_1 \cup X_2)\backslash(X_1' \cup X_2') \subseteq (X_1\backslash X_1') \cup (X_2\backslash X_2') \subseteq (X_1\Delta X_1') \cup (X_2\Delta X_2')$. By symmetry, we also get $(X_1' \cup X_2')\backslash(X_1 \cup X_2) \subseteq (X_1\Delta X_1') \cup (X_2\Delta X_2')$. We are done.

From insecable lemma 9.2, we deduce that if $X_1 \sim^V X_1'$ and $X_2 \sim^V X_2'$ then $X_1\#X_2 \sim^V X_1'\#X_2'$ for any $\# \in \{\cup, \cap, \backslash, \Delta\}$. □

For any equivalence class $\mathcal{X}$ and for any word $\sigma \in \Sigma_{r,m}^*$, following lemma 10.3 shows that the equivalence class $[\gamma_{r,m,\sigma}^{-1}(X)]^V$ does not depend on $X \in \mathcal{X}$. This equivalence class is denoted by $\gamma_{r,m,\sigma}^{-1}(\mathcal{X})$.

Lemma 10.3. *We have $\gamma_{r,m,\sigma}^{-1}(X) \sim^V \gamma_{r,m,\sigma}^{-1}(X')$ for any $X, X' \subseteq \mathbb{Q}^m$ such that $X \sim^V X'$, and for any $\sigma \in \Sigma_{r,m}^*$.*

Proof. Consider $X, X' \subseteq \mathbb{Q}^m$ such that $X \sim^V X'$. We denote by $Z = \mathbb{Z}^m \cap (X\Delta X')$. As $X \sim^V X'$, the vector space V is not included in $\overrightarrow{\text{saff}}(Z)$. We have $\mathbb{Z}^m \cap (\gamma_{r,m,\sigma}^{-1}(X_1)\Delta\gamma_{r,m,\sigma_2}^{-1}(X_2)) = \gamma_{r,m,\sigma}^{-1}(Z)$. From covering lemma we get $\text{saff}(\gamma_{r,m,\sigma}^{-1}(Z)) \subseteq \Gamma_{r,m,\sigma}^{-1}(\text{saff}(Z))$. By considering the direction of the previous inclusion, we get $\overrightarrow{\text{saff}}(\gamma_{r,m,\sigma}^{-1}(Z)) \subseteq \overrightarrow{\text{saff}}(Z)$ since $\Gamma_{r,m,\sigma}(x) = r^{|\sigma|}.x + \gamma_{r,m,\sigma}(\mathbf{e}_{0,m})$. As V is not included in $\overrightarrow{\text{saff}}(Z)$, we deduce that V is neither included in $\overrightarrow{\text{saff}}(\mathbb{Z}^m \cap (\gamma_{r,m,\sigma}^{-1}(X_1)\Delta\gamma_{r,m,\sigma_2}^{-1}(X_2)))$. Therefore $\gamma_{r,m,\sigma}^{-1}(X) \sim^V \gamma_{r,m,\sigma}^{-1}(X')$.

The following lemma 10.4 provides a commutativity result.

Lemma 10.4. *We have $\gamma_{r,m,\sigma}^{-1}(\mathcal{X}_1\#^V\mathcal{X}_2) = \gamma_{r,m,\sigma}^{-1}(\mathcal{X}_1)\#^V\gamma_{r,m,\sigma}^{-1}(\mathcal{X}_2)$ for any equivalence class $\mathcal{X}_1$ and $\mathcal{X}_2$, for any $\# \in \{\cup, \cap, \backslash, \Delta\}$, and for any $\sigma \in \Sigma_{r,m}^*$.*

Proof. Consider $X_1 \in \mathcal{X}_1$ and $X_2 \in \mathcal{X}_2$. We have $\gamma_{r,m,\sigma}^{-1}(\mathcal{X}_1\#^V\mathcal{X}_2) = [\gamma_{r,m,\sigma}^{-1}(X_1\#X_2)]^V = [\gamma_{r,m,\sigma}^{-1}(X_1)\#\gamma_{r,m,\sigma}^{-1}(X_2)]^V = [\gamma_{r,m,\sigma}^{-1}(X_1)]^V\#^V[\gamma_{r,m,\sigma}^{-1}(X_2)]^V = \gamma_{r,m,\sigma}^{-1}(\mathcal{X}_1)\#^V\gamma_{r,m,\sigma}^{-1}(\mathcal{X}_2)$. □

11

Polyhedrons

In this section, we recall the definition of a polyhedron and associate to a polyhedron C included into a vector space V, a boundary that only depends on the equivalence class $[C]^V$.

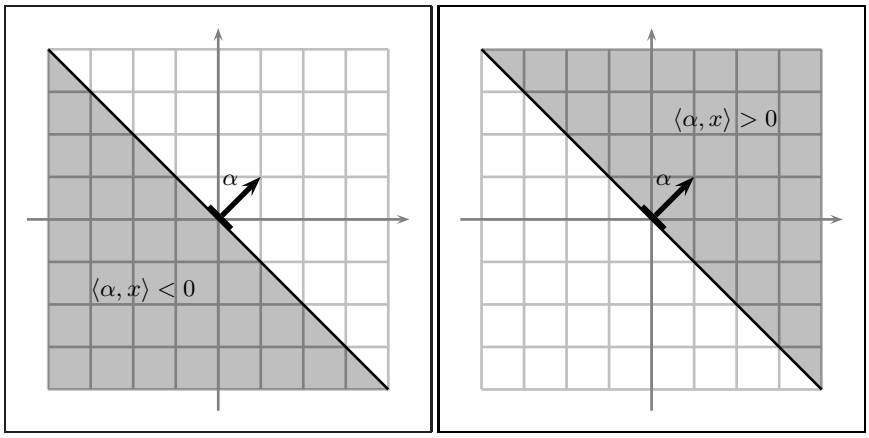

Fig. 11.1. Let $\alpha = (1, 1)$. On the left $\{x \in \mathbb{Q}^2;\ \langle \alpha, x \rangle < 0\}$. On the right $\{x \in \mathbb{Q}^2;\ \langle \alpha, x \rangle > 0\}$.

11.1 Orientation

A *V-hyperplane* H, where V is a vector space, is a set of the form $\{x \in V;\ \langle \alpha, x \rangle = c\}$ where $(\alpha, c) \in (V \backslash \{\mathbf{e}_{0,m}\}) \times \mathbb{Q}$. A V-hyperplane H provides a partition of $V \backslash H$ into two *open V-half spaces* $\{x \in V;\ \langle \alpha, x \rangle < c\}$ and

$\{x \in V;\ \langle \alpha, x\rangle > c\}$ that only depends on the V-hyperplane H (see figures 11.1).

An *orientation* o is a function that associate to any couple (V, H) where H is a V-hyperplane, one of these two open V-half spaces. Given an implicit orientation o, we denote by $(V, H)^>$ and $(V, H)^<$ the open V-half spaces $(V, H)^> = o(V, H)$ and $(V, H)^< = (V \backslash H) \backslash o(V, H)$. We denote by $(V, H)^=$ the hyperplane H and the *closed V-half spaces* $(V, H)^\geq$ and $(V, H)^\leq$ are naturally defined by $(V, H)^\geq = H \cup (V, H)^>$ and $(V, H)^\leq = H \cup (V, H)^<$.

Remark that a V-hyperplane H is an affine space and in particular $\overrightarrow{H}$ is well defined. Moreover, $\overrightarrow{H}$ is also a V-hyperplane. Remark that $H + (V, \overrightarrow{H})^>$ is an open half space of the form $(V, H)^\#$ where $\# \in \{<, >\}$ depends on H. A *uniform orientation* is an orientation that only depends on the direction of the V-hyperplane $\overrightarrow{H}$: we have $(V, H)^\# = H + (V, \overrightarrow{H})^\#$ for any $\# \in \{\leq, <, =, >, \geq\}$.

In the remaining of this paper, we assume fixed a uniform orientation (see remark 11.1 for the existence of such an *effective and efficient* orientation). Moreover when V is implicit, the set $(V, H)^\#$ is simply written $H^\#$.

Remark 11.1. Consider the function o that associate to any (V, H) where H is a V-hyperplane, the open V-half space $H + (\mathbb{Q}_+ \backslash \{0\}).\Pi_V(\mathbf{e}_i)$ where $i \in \{1, \ldots, m\}$ is the least (for $\leq$) integer such that $\Pi_V(\mathbf{e}_i) \notin \overrightarrow{H}$. Remark that such an integer i exists because if $\Pi_V(\mathbf{e}_i) \in \overrightarrow{H}$ for any $i \in \{1, \ldots, m\}$, then $V \subseteq \overrightarrow{H}$ which is impossible. Remark that o is an uniform orientation *computable in polynomial time.*

11.2 V-polyhedral equivalence class

Recall that a *polyhedron* C of $\mathbb{Q}^m$ is a boolean combination in $\mathbb{Q}^m$ of sets $H^\#$ where H is a $\mathbb{Q}^m$-hyperplane and $\# \in \{\leq, <, =, >, \geq\}$. A *$V$-polyhedron* C is a polyhedron included into a vector space V. A polyhedron C is said *$(V, \mathcal{H})$-definable*, where $\mathcal{H}$ is a finite set of V-hyperplanes if C is a boolean combination in V of sets in $\{H^\#;\ (H, \#) \in \mathcal{H} \times \{\leq, <, =, >, \geq\}\}$.

Lemma 11.2. *A polyhedron is a V-polyhedron if and only if it is $(V, \mathcal{H})$-definable for a finite set $\mathcal{H}$ of V-hyperplanes.*

Proof. Naturally, if C is $(V, \mathcal{H})$-definable then C is a V-polyhedron. For the converse, consider a V-polyhedron C. By definition $C \subseteq V$ and there exists $D_0 \in \mathcal{P}_f(\mathbb{Q}^m \backslash \{\mathbf{e}_{0,m}\})$ and $K \in \mathcal{P}_f(\mathbb{Q})$ such that C is a boolean combination in $\mathbb{Q}^m$ of sets $\{x \in \mathbb{Q}^m;\ \langle \alpha_0, x\rangle \# c\}$ where $(\alpha_0, c) \in D_0 \times K$ and $\# \in \{\leq, <, =, >, \geq\}$. From $C \subseteq V$ we deduce that $C = C \cap V$ and in particular C is a boolean combination in V of sets $\{x \in V;\ \langle \alpha_0, x\rangle \# c\} = \{x \in V;\ \langle \Pi_V(\alpha_0), x\rangle \# c\}$. Let $D = \Pi_V(D_0) \backslash \{\mathbf{e}_{0,m}\}$ and consider the set of V-hyperplanes $\mathcal{H} = \{\{x \in V;\ \langle \alpha, x\rangle = c\};\ (\alpha, c) \in D \times K\}$ and let us prove that C is $(V, \mathcal{H})$-definable.

Let $(\alpha_0, c) \in D_0 \times K$. Remark that $\{x \in V;\ \langle \Pi_V(\alpha_0), x\rangle \,\#c\}$ is either empty or equal to V in the case $\Pi_V(\alpha_0) = \mathbf{e}_{0,m}$, or it is in the class $\{H^{\#};\ (H,\#) \in \mathcal{H} \times \{\leq, <, =, >, \geq\}\}$ if $\Pi_V(\alpha_0) \neq \mathbf{e}_{0,m}$. □

Definition 11.3. *A V-*polyhedral equivalence class $\mathcal{C}$ *is the equivalence class for $\sim^V$ of a V-polyhedron.*

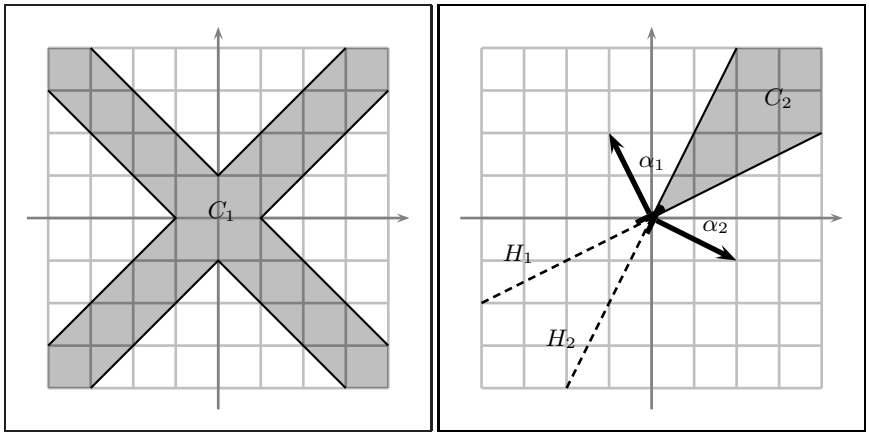

Fig. 11.2. Let $V = \mathbb{Q}^2$. On the left a V-degenerate V-polyhedron C_1. On the right a non V-degenerate V-polyhedron C_2.

11.3 Open convex polyhedrons

A V-polyhedron C is said *open convex* in V (or just open convex when V is implicitly known) if it is equal to a finite intersection of open V-half spaces (in particular V is an open convex).

Definition 11.4. *Given a finite set $\mathcal{H}$ of V-hyperplanes and a sequence $\# \in \{<,>\}^{\mathcal{H}}$, we denote by $C_{V,\#}$ the open convex V-polyhedron $C_{V,\#} = \bigcap_{H\in\mathcal{H}} H^{\#_H}$ (if $\mathcal{H} = \emptyset$, then $C_{V,\#} = V$).*

Given a $(V,\mathcal{H})$-definable polyhedron C, remark that $C\backslash(\bigcup_{H\in\mathcal{H}} H)$ is a finite union of open convex polyhedrons $C_{V,\#}$ where $\# \in \{<,>\}^{\mathcal{H}}$. As $[C]^V = [C\backslash(\bigcup_{H\in\mathcal{H}} H)]^V$, this property will be useful for decomposing V-polyhedrons.

11.4 Degenerate polyhedrons

We geometrically characterize the V-degenerate V-polyhedrons (see figure 11.2) thanks to the following proposition 11.7.

We first prove the following two lemmas 11.5 and 11.6.

Lemma 11.5. *For any V-hyperplanes H_1, H_2 such that $\overrightarrow{H_1} = \overrightarrow{H_2}$, the open convex V-polyhedron $H_1^> \cap H_2^<$ is V-degenerate.*

Proof. Let $\alpha \in \mathbb{Z}^m \cap V \backslash \{\mathbf{e}_{0,m}\}$ and $c_1, c_2 \in \mathbb{Q}$ such that $H_1^> = \{x \in V;\ \langle \alpha, x\rangle > c_1\}$ and such that $H_2^< = \{x \in V;\ \langle \alpha, x\rangle < c_2\}$. Let us prove that $C = H_1^> \cap H_2^<$ is V-degenerate. Let $K = \{k \in \mathbb{Z};\ c_1 < k < c_2\}$ and remark that for any $x \in \mathbb{Z}^m \cap C$ we have $c_1 < \langle \alpha, x\rangle < c_2$ and $\langle \alpha, x\rangle \in \mathbb{Z}$. Hence, there exists $k \in K$ such that $\langle \alpha, x\rangle \in K$. We deduce that $\mathbb{Z}^m \cap C \subseteq \bigcup_{k\in K} H_k$ where H_k is the V-hyperplane $H_k = \{x \in V;\ \langle \alpha, x\rangle = k\}$. Hence $\overrightarrow{\text{saff}}(\mathbb{Z}^m \cap C) \subseteq \{x \in V;\ \langle \alpha, x\rangle = 0\}$. As α is in V but not in this semi-vector space, we deduce that V is not included in $\overrightarrow{\text{saff}}(\mathbb{Z}^m \cap C)$. Hence C is V-degenerate. □

Lemma 11.6. *We have $[C_{V,\#}]^V \neq [\emptyset]^V$ if and only if $\bigcap_{H\in\mathcal{H}} \overrightarrow{H}^{\#_H} \neq \emptyset$, for any $\# \in \{<, >\}^{\mathcal{H}}$ where $\mathcal{H}$ is a finite set of V-hyperplanes.*

Proof. Let us consider a sequence $(\alpha_H, c_H)_{H\in\mathcal{H}}$ of elements in $(V\backslash\{\mathbf{e}_{0,m}\})\times\mathbb{Q}$ such that $H^{\#_H} = \{x \in V;\ \langle \alpha_H, x\rangle > c_H\}$, and let $C = \bigcap_{H\in\mathcal{H}} H^{\#_H}$.

Assume first that $\bigcap_{H\in\mathcal{H}} \overrightarrow{H}^{\#_H} \neq \emptyset$ and let us prove that C is non V-degenerate. Consider a vector v in this open convex V-polyhedron and remark that $\langle \alpha_H, v\rangle > 0$ for every $H \in \mathcal{H}$. By replacing v by a vector in $(\mathbb{N}\backslash\{0\}).v$, we can assume that $v \in \mathbb{Z}^m \cap V$. Let us first show that there exists $x_0 \in \mathbb{Z}^m \cap C$. In fact, there exists $k \in \mathbb{N}$ enough larger such that $\langle \alpha_H, k.v\rangle > c_H$ for any $H \in \mathcal{H}$. For such a k, just remark that $x_0 = k.v \in \mathbb{Z}^m \cap C$. Next, let us prove that there exists a finite set V_0 of vectors in $\mathbb{Z}^m$ that generates V and such that $\langle \alpha_H, v_0\rangle > 0$ for any $(v_0, H) \in V_0 \times \mathcal{H}$. We know that there exists a finite set V_0 of vectors in $\mathbb{Z}^m$ that generates V. By replacing V_0 by $V_0 + k.v$ where $k \in \mathbb{N}$ is enough larger, we can assume that $\langle \alpha_H, v_0\rangle > 0$ for any $(v_0, H) \in V_0 \times \mathcal{H}$. We have proved that $x_0 + \sum_{v_0\in V_0} \mathbb{N}.v_0 \subseteq \mathbb{Z}^m \cap C$. From covering lemma 9.9, we get $\text{saff}(x_0 + \sum_{v_0\in V_0} \mathbb{N}.v_0) = x_0 + V$. Hence $V \subseteq \overrightarrow{\text{saff}}(\mathbb{Z}^m \cap C)$. Therefore C is non V-degenerate.

Now, assume that $\bigcap_{H\in\mathcal{H}} \overrightarrow{H}^{\#_H} = \emptyset$. Hence, for any $v \in V$, there exists $H \in \mathcal{H}$ such that $\langle \alpha_H, v\rangle \leq 0$. In particular for any $v \in C$, there exists $H \in \mathcal{H}$ such that $c_H < \langle \alpha_H, v\rangle \leq 0$. Lemma 11.5 shows that C is V-degenerate. □

Proposition 11.7. *A V-polyhedron is V-degenerate if and only if it is included into a finite union of $H_1^> \cap H_2^<$ where H_1 and H_2 are two V-hyperplanes with the same direction.*

Proof. As a finite union of V-degenerate subsets of V remains V-degenerate, we deduce from lemma 11.5 that if a V-polyhedron is included into a finite union of $H_1^> \cap H_2^<$ where H_1 and H_2 are two V-hyperplanes with the same direction, then it is V-degenerate.

For the converse consider a V-polyhedron C such that for any finite set $D \subseteq V\backslash\{\mathbf{e}_{0,m}\}$, the V-polyhedron C is not included in $\bigcup_{\alpha\in D}\{x \in V;\ -1 <$

$\langle \alpha, x\rangle < 1\}$. Let $\mathcal{H}$ be a finite set of V-hyperplanes such that C is $(V,\mathcal{H})$-definable. Recall that $C' = C\backslash(\bigcup_{H\in\mathcal{H}} H)$ is a finite union of open convex definable polyhedron $C_{V,\#}$ where $\# \in \{<,>\}^{\mathcal{H}}$ and it satisfies $[C]^V = [C']^V$. So, we can assume without loss of generality that $C = C_{V,\#}$. Consider a sequence $(\alpha_H, c_H)_{H\in\mathcal{H}}$ of elements in $(V\backslash\{\mathbf{e}_{0,m}\})\times\mathbb{Q}$ such that $H^{\#_H} = \{x \in V;\ \langle \alpha_H, x\rangle > c_H\}$. Naturally, $C \neq \emptyset$ (otherwise we obtain a contradiction). Hence, there exists $x_0 \in C$. Let us consider $c \in \mathbb{Q}$ such that $c \geq 1$, $c \geq \langle \alpha_H, x_0\rangle$ and $c \geq -c_H$ for any $H \in \mathcal{H}$. As C is not included in $\bigcup_{H\in\mathcal{H}}\{x \in V;\ -1 < \langle \frac{\alpha_H}{c}, x\rangle < 1\}$, there exists $x_1 \in C$ and such that for any $H \in \mathcal{H}$ either $\langle \alpha_H, x_1\rangle > c$ or $\langle \alpha_H, x_1\rangle < -c$. As $x_1 \in C$, recall that $\langle \alpha_H, x_1\rangle > c_\alpha$. Hence $\langle \alpha_H, x_1\rangle < -c$ implies $c < -c_\alpha$ which is impossible. Therefore $\langle \alpha_H, x_1\rangle > c$ for any $H \in \mathcal{H}$. Consider $v = x_1 - x_0$ and remark that $\langle \alpha_H, v\rangle > 0$ for any $H \in \mathcal{H}$. Hence v is in $\bigcap_{H\in\mathcal{H}} \overrightarrow{H}^{\#_H}$. From lemma 11.10, we deduce that C is non V-degenerate. □

Example 11.8. The $\mathbb{Q}^2$-polyhedrons $C_1 = \{x \in \mathbb{Q}^2; (-1 \leq x[1] + x[2] \leq 1) \vee (-1 \leq x[1] - x[2] \leq 1)\}$ and $C_2 = \{x \in \mathbb{Q}^2;\ -x[1] + 2.x[2] \geq 0 \wedge 2.x[1] - x[2] \geq 0\}$ are given in figure 11.2. Remark that C_1 is $\mathbb{Q}^2$-degenerate because $\overrightarrow{\text{saff}}(\mathbb{Z}^m \cap C_1) = V_1 \cup V_2$ where $V_1 = \{x \in \mathbb{Q}^2;\ x[1] = x[2]\}$ and $V_2 = \{x \in \mathbb{Q}^2;\ x[1]+x[2] = 0\}$, and C_2 is non $\mathbb{Q}^2$-degenerate because $\overrightarrow{\text{saff}}(\mathbb{Z}^m \cap C_2) = \mathbb{Q}^2$.

11.5 Boundary

We are interested in associating to a V-polyhedral equivalence class $\mathcal{C}$, a set of V-hyperplanes that intuitively corresponds to the "constraints of $\mathcal{C}$".

A *possible V-boundary* $\mathcal{H}$ of a V-polyhedral equivalence class $\mathcal{C}$ is a finite set of V-hyperplanes such that there exists a $(V,\mathcal{H})$-definable polyhedron in $\mathcal{C}$. Following lemma shows that a possible V-boundary can be translated, and in particular the *direction of any possible V-boundary remains a possible V-boundary.*

Lemma 11.9. *For any possible V-boundary $\mathcal{H}$ of a V-polyhedral equivalence class $\mathcal{C}$ and for any sequence $(V_H)_{H\in\mathcal{H}}$ of non-empty finite subset of V, the set $\{v + H;\ H \in \mathcal{H}; v \in V_H\}$ is a possible V-boundary of $\mathcal{C}$.*

Proof. There exists a $(V,\mathcal{H})$-definable polyhedron $C \in \mathcal{C}$. That means C is a boolean combination in V of sets in $\{H^{\leq}, H^{<}, H^{=}, H^{>}, H^{\geq};\ H \in \mathcal{H}\}$. Lemma 11.5 proves that $[(v + H)^{\#}]^V = [H^{\#}]^V$ for any $(H,\#) \in \mathcal{H}\times\{\leq,<,=,>,\geq\}$ and for any $v \in V_H$. □

Lemma 11.10. *Let C be an open convex V-polyhedron and H_1 be a V-hyperplane such that $[C \cap H_1^{<}]^V \neq [\emptyset]^V$ and $[C \cap H_1^{>}]^V \neq [\emptyset]^V$. For any V-hyperplane H_0 such that $\overrightarrow{H_0} \neq \overrightarrow{H_1}$, there exist $\#_0 \in \{<,>\}$ such that $[C \cap H_0^{\#_0} \cap H_1^{<}]^V \neq [\emptyset]^V$ and $[C \cap H_0^{\#_0} \cap H_1^{>}]^V \neq [\emptyset]^V$.*

Proof. As C is an open convex set, there exists a finite set $\mathcal{H}$ of V-hyperplanes and $\# \in \{<,>\}^{\mathcal{H}}$ such that $C = C_{V,\#}$. Let us consider a sequence $(\alpha_H, c_H)_{H\in\mathcal{H}}$ of elements in $(V\backslash\{\mathbf{e}_{0,m}\})\times\mathbb{Q}$ such that $H^{\#_H} = \{x \in V;\ \langle\alpha_H, x\rangle \#_H c_H\}$. Let us also consider (α_0, c_0) and (α_1, c_1) in $(V\backslash\{0\}) \times \mathbb{Q}$ such that $H_0^{\#_0} = \{x \in V;\ \langle\alpha_0, x\rangle \#_0 c_0\}$ and $H_1^{\#_1} = \{x \in V;\ \langle\alpha_1, x\rangle \#_1 c_1\}$. As $[C \cap H_1^{\#_1}]^V \neq [\emptyset]^V$, lemma 11.6 shows that there exists $v_{\#_1} \in \mathbb{Q}^m$ such that $\langle\alpha_1, v_{\#_1}\rangle \#_1 0$ and such that $\langle\alpha_H, v_{\#_1}\rangle \#_H 0$ for any $H \in \mathcal{H}$.

Let us first prove that there exists a finite set V_1 of vectors in $\bigcap_{H\in\mathcal{H}} \overrightarrow{H}^{\#_H}$ that generates $\overrightarrow{H_1}$. There exist $\mu_<$ and $\mu_>$ in $\mathbb{Q}_+\backslash\{0\}$ such that the vector $v_= = \mu_<.v_< + \mu_>.v_>$ satisfies $\langle\alpha_1, v_=\rangle = 0$. Remark that $v_= \in \overrightarrow{H_1}$ and satisfies $\langle\alpha_H, v_=\rangle \#_H 0$ for any $H \in \mathcal{H}$. Let us consider a finite set of vectors V_1 that generate $\overrightarrow{H_1}$ and just remark that there exists $\mu \in \mathbb{Q}_+$ enough larger such that $\langle\alpha_H, v\rangle \#_H 0$ for any $(H, v) \in \mathcal{H} \times (V_1 + \mu.v_=)$. Finally, as V_1 generates $\overrightarrow{H_1}$ and $v_= \in \overrightarrow{H_1}$, the set $V_1 + \mu.v_=$ also generates $\overrightarrow{H_1}$. By replacing V_1 by $V_1 + \mu.v_=$, we are done.

Naturally, if $V_1 \subseteq \overrightarrow{H_0}$ then $\overrightarrow{H_1} = \overrightarrow{H_0}$ which is impossible. Hence, there exists $v_1 \in V_1$ such that $\langle\alpha_0, v_1\rangle \neq 0$. Let $\#_0 \in \{<,>\}$ such that $\langle\alpha_0, v_1\rangle \#_0 0$. Remark that there exists $\mu \in \mathbb{Q}_+$ enough larger such that $v_{\#_1} + \mu.v_1 \in \bigcap_{H\in\mathcal{H}} \overrightarrow{H}^{\#_H} \cap \overrightarrow{H_0}^{\#_0} \cap \overrightarrow{H_1}^{\#_1}$ for any $\#_1 \in \{<,>\}$. Lemma 11.6 shows that $[C \cap H_0^{\#_0} \cap H_1^{<}]^V \neq [\emptyset]^V$ and $[C \cap H_0^{\#_0} \cap H_1^{>}]^V \neq [\emptyset]^V$. □

Lemma 11.11. *Let C be an open convex V-polyhedron and H be a V-hyperplane such that $[C \cap H^{<}]^V \neq [\emptyset]^V$ and $[C \cap H^{>}]^V \neq [\emptyset]^V$. The set $\overrightarrow{C \cap H}$ is non $\overrightarrow{H}$-degenerate open convex $\overrightarrow{H}$-polyhedron.*

Proof. Without loss of generality, we can assume that $\overrightarrow{C} = X$ and $\overrightarrow{H} = H$. Since $C \cap H^{\#}$ is an open convex non V-degenerate V-polyhedron, there exists a vector $v_{\#}$ in this set. Let us remark that there exists two rational numbers $x_<, x_>$ in $\mathbb{Q}_+\backslash\{0\}$ such that $x = x_<.v_< + x_>.v_> \in H$. Since $x_<, x_>$ are both in C and $x_<, x_>$ are strictly positive rational numbers, we deduce that $x \in C$. Hence $x \in H \cap C$ and from lemma 11.6 we deduce that $H \cap C$ is non-H-degenerate. □

Proposition 11.12. *Let $\mathcal{C}$ be a V-polyhedral equivalence class and $\mathcal{H}_V(\mathcal{C})$ be the set of V-hyperplanes H such that there exists an open convex V-polyhedron C_H such that $[C_H \cap H^{<}]^V \neq [\emptyset]^V$ and $[C_H \cap H^{>}]^V \neq [\emptyset]^V$, and such that $[C_H]^V \cap^V \mathcal{C}$ is equal to one of these two equivalence classes. The set $\overrightarrow{\mathcal{H}_V(\mathcal{C})}$ is a possible V-boundary of $\mathcal{C}$ included into the direction of any possible V-boundary of $\mathcal{C}$.*

Proof. Let us first consider a possible V-boundary $\mathcal{H}$ of $\mathcal{C}$ and let us prove that for any $H_0 \in \mathcal{H}\backslash\mathcal{H}_V(\mathcal{C})$, the set $\mathcal{H}\backslash\{H_0\}$ is a possible V-boundary of $\mathcal{C}$. Let $\mathcal{H}' = \mathcal{H}\backslash\{H_0\}$. As $\mathcal{H}$ is a possible V-boundary of $\mathcal{C}$, there exists a $(V, \mathcal{H})$-definable polyhedron C in $\mathcal{C}$. We have the following equality:

$$\mathcal{C} = \left[C \setminus \left(\bigcup_{H\in\mathcal{H}} H\right)\right]^V$$
$$= \bigcup_{\#\in\{<,>\}^{\mathcal{H}'}}^{V} \left[C_{V,\#} \cap H_0^{<} \cap C\right]^V \cup^V \left[C_{V,\#} \cap H_0^{>} \cap C\right]^V$$

As C is $(V,\mathcal{H})$-definable, we deduce that $C_{V,\#} \cap H_0^{\#_0} \cap C$ is either empty or equal to $C_{V,\#} \cap H_0^{\#_0}$. Let us prove that $[C_{V,\#} \cap C]^V$ is either equal to $[\emptyset]^V$ or equal to $[C_{V,\#}]^V$. Naturally, if $C_{V,\#} \cap H_0^{<}$ or $C_{V,\#} \cap H_0^{>}$ is V-degenerate, we are done. Otherwise, $[C_{V,\#} \cap H_0^{<}]^V \neq [\emptyset]^V$ and $[C_{V,\#} \cap H_0^{>}]^V \neq [\emptyset]^V$. As $C_{V,\#}$ is an open convex V-polyhedron and $H_0 \notin \mathcal{H}_V(\mathcal{C})$, we deduce that $[C_{V,\#}]^V \cap^V \mathcal{C}$ is neither equal to $[C_{V,\#} \cap H_0^{<}]^V$ nor equal to $[C_{V,\#} \cap H_0^{>}]^V$. However, $(C_{V,\#} \cap C)\backslash H_0$ is either equal to $\emptyset$, $C_{V,\#}\backslash H_0$, $C_{V,\#} \cap H_0^{<}$ or $C_{V,\#} \cap H_0^{>}$. As the two last cases are impossible, we deduce that $[C_{V,\#}]^V \cap^V \mathcal{C}$ is either equal to $[\emptyset]^V$ in the first case, or equal to $[C_{V,\#}]^V$ in the second case. We have proved that the following $(V,\mathcal{H}')$-definable polyhedron C' is in $\mathcal{C}$. That means $\mathcal{H}'$ is a possible V-boundary.

$$C' = \bigcup_{\#\in\{<,>\}^{\mathcal{H}'};\, [C_{V,\#}]^V \cap^V \mathcal{C} \neq [\emptyset]^V} C_{V,\#}$$

Finally, let us now consider a possible V-boundary $\mathcal{H}$ of $\mathcal{C}$ and $H_0 \in \mathcal{H}_V(\mathcal{C})$, and let us prove that $\overrightarrow{H_0} \in \overrightarrow{\mathcal{H}}$. Lemma 11.9 shows that we can assume that $\overrightarrow{\mathcal{H}} = \mathcal{H}$. As $H_0 \in \mathcal{H}_V(\mathcal{C})$, there exists an open convex V-polyhedron C_{H_0} such that $[C_{H_0} \cap H_0^{<}]^V \neq [\emptyset]^V$ and $[C_{H_0} \cap H_0^{>}]^V \neq [\emptyset]^V$ and such that $[C_{H_0}]^V \cap^V \mathcal{C}$ is equal to one of these two equivalence classes. Assume by contradiction that $\overrightarrow{H_0} \notin \overrightarrow{\mathcal{H}}$. From lemma 11.10, an immediate induction proves there exists $\# \in \{<,>\}^{\mathcal{H}}$ such that $[C_{H_0} \cap C_{V,\#} \cap H_0^{<}]^V \neq [\emptyset]^V$ and $[C_{H_0} \cap C_{V,\#} \cap H_0^{>}]^V \neq [\emptyset]^V$. As $\mathcal{H}$ is a possible V-boundary of $\mathcal{C}$, we deduce that $[C_{V,\#}]^V \cap^V \mathcal{C}$ is either equal to $[\emptyset]^V$ or equal to $[C_{V,\#}]^V$. In particular $[C_{H_0} \cap C_{V,\#}]^V \cap^V \mathcal{C}$ is either equal to $[\emptyset]^V$ or equal to $[C_{H_0} \cap C_{V,\#}]^V$. Moreover, as $[C_{H_0}]^V \cap^V \mathcal{C}$ is equal to $[C_{H_0} \cap H_0^{<}]^V$ or $[C_{H_0} \cap H_0^{>}]^V$, we also deduce that $[C_{H_0} \cap C_{V,\#}]^V \cap^V \mathcal{C}$ is either equal to $[C_{H_0} \cap C_{V,\#} \cap H_0^{<}]^V$ or equal to $[C_{H_0} \cap C_{V,\#} \cap H_0^{>}]^V$. Hence there exists $\#_0 \in \{<,>\}$ such that $[C_{H_0} \cap C_{V,\#} \cap H_0^{\#_0}]^V$ is either equal to $[\emptyset]^V$ or equal to $[C_{H_0} \cap C_{V,\#}]^V$. The first case is impossible and the second case implies $[C_{H_0} \cap C_{V,\#} \cap H_0^{\#'_0}]^V = [\emptyset]^V$ where $\#'_0 \in \{<,>\}\backslash\{\#_0\}$. We obtain a contradiction. Therefore $\overrightarrow{H_0} \in \overrightarrow{\mathcal{H}}$. □

The previous proposition 11.12 shows in particular that the set of directions of possible V-boundaries of a V-polyhedron C, owns a minimal elements for $\subseteq$.

Definition 11.13. *The finite class* $\overrightarrow{\mathcal{H}_V(\mathcal{C})}$ *is denoted by* $bound_V(\mathcal{C})$ *and called the* V-boundary *of* $\mathcal{C}$.

Example 11.14. Let $C_2 = \{x \in \mathbb{Q}^2;\ \langle \alpha_1, x\rangle \geq 0 \wedge \langle \alpha_2, x\rangle \geq 0\}$ be the $\mathbb{Q}^2$-polyhedron given in figure 11.2 where $\alpha_1 = (-1, 2)$ and $\alpha_2 = (2, -1)$. Let H_1 and H_2 be the $\mathbb{Q}^2$-hyperplanes defined by $H_1 = \{x \in \mathbb{Q}^2;\ \langle \alpha_1, x\rangle = 0\}$ and $H_2 = \{x \in \mathbb{Q}^2;\ \langle \alpha_2, x\rangle = 0\}$. Naturally, as C_2 is $(\mathbb{Q}^2, \{H_1, H_2\})$-definable, we deduce that $\{H_1, H_2\} \subseteq \text{bound}_{\mathbb{Q}^2}([C_2]^{\mathbb{Q}^2})$. Let us show the converse inclusion. Consider the open convex $\mathbb{Q}^2$-polyhedron $C_{H_1} = \{x \in \mathbb{Q}^2;\ \langle \alpha_2, x\rangle > 0 \wedge x[2] > 0\}$. Remark that $[C_{H_1} \cap H_1^<]^{\mathbb{Q}^2}$ and $[C_{H_1} \cap H_1^>]^{\mathbb{Q}^2}$ are not equal to $[\emptyset]^{\mathbb{Q}^2}$ and $[C_{H_1} \cap C_2]^{\mathbb{Q}^2}$ is equal to one of this two classes. We deduce that $H_1 \in \text{bound}_{\mathbb{Q}^2}(C_2)$. Symmetrically, we get $H_2 \in \text{bound}_{\mathbb{Q}^2}([C_2]^{\mathbb{Q}^2})$. Therefore $\text{bound}_{\mathbb{Q}^2}([C_2]^{\mathbb{Q}^2}) = \{H_1, H_2\}$.

11.6 Polyhedrons of the form $C + V^\perp$

In the sequel, we often consider $\mathbb{Q}^m$-polyhedrons of the form $C + V^\perp$ where C is a V-polyhedron. In this section, we provide some properties satisfied by these sets.

Given a V-polyhedral equivalence class $\mathcal{C}$, following lemma 11.15 shows that the equivalence class $[C + V^\perp]^V$ does not depend on the V-polyhedron $C \in \mathcal{C}$. This equivalence class $[C + V^\perp]^V$ is naturally denoted by $\mathcal{C} + V^\perp$.

Lemma 11.15. *We have $C + V^\perp \sim^V C' + V^\perp$ for any V-polyhedrons C and C' such that $C \sim^V C'$*

Proof. We have $\mathbb{Z}^m \cap ((C + V^\perp) \Delta (C' + V^\perp)) = \mathbb{Z}^m \cap (C_0 + V^\perp)$ where $C_0 = C \Delta C'$. As $C \sim^V C'$, we deduce that C_0 is V-degenerate. In order to prove the lemma, we have to show that V is not included in $\overrightarrow{\text{saff}}(\mathbb{Z}^m \cap (C_0 + V^\perp))$. Proposition 11.7 proves that there exists a finite set $D \subseteq \mathbb{Z}^m \cap V \backslash \{\mathbf{e}_{0,m}\}$ and an integer $k \in \mathbb{N}$ such that $C_0 \subseteq \bigcup_{\alpha \in D} \{x \in V;\ |\langle \alpha, x\rangle| \leq k\}$. Let $K = \{-k, \ldots, k\}$ and remark that we get $\mathbb{Z}^m \cap (C_0 + V^\perp) \subseteq \bigcup_{(\alpha,k) \in D \times K} \{x \in \mathbb{Q}^m;\ \langle \alpha, x\rangle = k\}$. Hence $\overrightarrow{\text{saff}}(\mathbb{Z}^m \cap (C_0 + V^\perp)) \subseteq \bigcup_{\alpha \in D} \alpha^\perp$. As $\alpha \in V$ for any $\alpha \in D$, we deduce that V is not included in $\alpha^\perp$ for any $\alpha \in D$. From insecable lemma 9.2 we deduce that V is not included in $\bigcup_{\alpha \in D} \alpha^\perp$. In particular V is not included in $\overrightarrow{\text{saff}}(\mathbb{Z}^m \cap (C_0 + V^\perp))$. Therefore $C + V^\perp \sim^V C' + V^\perp$. □

Remark that even if $[C + V^\perp]^V$ does not depends on a V-polyhedron $C \in \mathcal{C}$, there exist subsets $X \subseteq V$ in $\mathcal{C}$ such that $[X + V^\perp]^V \neq [C + V^\perp]^V$ as shown by the following example 11.16. That explains why our definition of $\mathcal{C} + V^\perp$ is limited to V-polyhedral equivalence classes $\mathcal{C}$.

Example 11.16. Assume that $m = 2$, let $V = \{x \in \mathbb{Q}^2;\ x[1] = x[2]\}$. Let us consider the V-polyhedron $C = \emptyset$ and the set $X = (\frac{1}{2}, \frac{1}{2}) + (\mathbb{Z}^m \cap V)$. Remark that $[C]^V = [X]^V$. However $[C + V^\perp]^V = [\emptyset]^V$ whereas $[X + V^\perp]^\perp \neq [\emptyset]^V$ since $\mathbb{Z}^m \cap (X + V^\perp) = (0, 1) + 2.\mathbb{Z}^2$.

Let us finally proves that $\gamma^{-1}_{r,m,\sigma}(\mathcal{C} + V^\perp) = \mathcal{C} + V^\perp$ for any V-polyhedral equivalence class $\mathcal{C}$ and for any word $\sigma \in \Sigma^*_{r,m}$. In fact, given a V-polyhedron $C \in \mathcal{C}$, we have the following equalities:

$$\begin{aligned}\gamma^{-1}_{r,m,\sigma}(\mathcal{C} + V^\perp) &= \gamma^{-1}_{r,m,\sigma}([C + V^\perp]^V) \\ &= [\gamma^{-1}_{r,m,\sigma}(C + V^\perp)]^V \\ &= [\Gamma^{-1}_{r,m,\sigma}(C + V^\perp)]^V\end{aligned}$$

We can easily prove that $\Gamma^{-1}_{r,m,\sigma}(C + V^\perp)$ is a $\mathbb{Q}^m$-polyhedron of the form $C' + V^\perp$ by introducing the sequence $(\Gamma_{V,r,m,\sigma})_{\sigma \in \Sigma^*_{r,m}}$ of affine functions $\Gamma_{V,r,m,\sigma} : V \to V$ defined by the following equality for any $x \in V$:

$$\Gamma_{V,r,m,\sigma}(x) = r^{|\sigma|}.x + \Pi_V(\gamma_{r,m,\sigma}(\mathbf{e}_{0,m}))$$

Remark that $\Gamma_{V,r,m,\sigma_1.\sigma_2} = \Gamma_{V,r,m,\sigma_1} \circ \Gamma_{V,r,m,\sigma_2}$ for any word $\sigma_1, \sigma_2 \in \Sigma^*_{r,m}$, $\Gamma_{V,r,m,\epsilon}$ is the identity function, and $\Gamma^{-1}_{r,m,\sigma}(C + V^\perp) = \Gamma^{-1}_{V,r,m,\sigma}(C) + V^\perp$ for any subset $C \subseteq V$.

Thanks to the following proposition 11.17, we deduce the following corollary 11.18.

Proposition 11.17. *We have $[\Gamma^{-1}_{r,m,\sigma}(C)]^V = [C]^V$ for any V-polyhedron C and for any $\sigma \in \Sigma^*_{r,m}$.*

Proof. Let us consider a finite class $\mathcal{H}$ of V-polyhedrons such that C is $(V, \mathcal{H})$-definable. As C is a boolean combination in V of sets $H^\#$ where $H \in \mathcal{H}$ and $\# \in \{<, >\}$, we can assume that C is equal to such a set. As H and $\Gamma^{-1}_{V,r,m,\sigma}(H)$ have the same direction, from lemma 11.5, we are done. □

Corollary 11.18. *We have $\gamma^{-1}_{r,m,\sigma}(\mathcal{C} + V^\perp) = \mathcal{C} + V^\perp$ for any V-polyhedral equivalence class and for any $\sigma \in \Sigma^*_{r,m}$.*

12

Presburger Decomposition

A subset $X \subseteq \mathbb{Q}^m$ can be naturally decomposed into $X = \bigcup_{V \in \mathrm{comp}(\overrightarrow{\mathrm{saff}}(X))} X_V$ where X_V is defined by the following equality:

$$X_V = X \cap \left(\bigcup_{\substack{A \in \mathrm{comp}(\mathrm{saff}(X)) \\ \overrightarrow{A} \subseteq V}} A \right)$$

Obseve that X_V is non empty and as shown by the following dense component lemma 12.1, the semi-affine hull direction $\overrightarrow{\mathrm{saff}}(X_V)$ is equal to V.

Lemma 12.1 (Dense component lemma). *We have* $\mathrm{saff}(X \cap A) = A$ *for any subset* $X \subseteq \mathbb{Q}^m$ *and for any affine component* A *of* $\mathrm{saff}(X)$.

Proof. We have $\mathrm{saff}(X) = A \cup S$ where S is the semi-affine space equal to the finite union of affine spaces $A' \in \mathrm{comp}(\mathrm{saff}(X)) \backslash \{A\}$. From $X \subseteq \mathrm{saff}(X)$, we deduce that $X \subseteq (X \cap A) \cup S \subseteq \mathrm{saff}(X \cap A) \cup S$. By minimality of the semi-affine hull, we get $\mathrm{saff}(X) \subseteq \mathrm{saff}(X \cap A) \cup S$. As $A \subseteq \mathrm{saff}(X)$, insecable lemma 9.2 shows that either $A \subseteq \mathrm{saff}(X \cap A)$ or $A \subseteq S$. In this last case, by definition of S, insecable lemma 9.2 proves that there exists $A' \in \mathrm{comp}(\mathrm{saff}(X)) \backslash \{A\}$ such that $A \subseteq A'$. As A is an affine component of $\mathrm{saff}(X)$ and $A \subseteq A' \subseteq \mathrm{saff}(X)$, we get the equality $A = A'$ which is impossible. Therefore $A \subseteq \mathrm{saff}(X \cap A)$. Moreover, as $X \cap A \subseteq A$, we get the other inclusion $\mathrm{saff}(X \cap A) \subseteq A$. □

We are going to prove that this decomposition of X can be refined when X is Presburger-definable. In fact, in this case, we show that X_V can be decomposed (up to V-degenerate sets) into sets of the form $P \cap (C + V^\perp)$ where P is a semi-V-pattern and C is a V-polyhedron.

Naturally, a set $P \cap (C + V^\perp)$ is Presburger-definable. The semi-affine hull direction of such a set is characterized by the following lemma 12.2

Lemma 12.2. *Let P be a semi-V-pattern and $\mathcal{C}$ a V-polyhedral equivalence class. We have $[P]^V \cap^V (\mathcal{C} + V^\perp) \neq [\emptyset]^V$ if and only if $P \neq \emptyset$ and $\mathcal{C} \neq [\emptyset]^V$.*

Proof. Naturally if $P = \emptyset$ or $\mathcal{C} = [\emptyset]^V$ then $[P]^V = [\emptyset]^V$ or $\mathcal{C} + V^\perp = [\emptyset]^V$ and in this case $[P]^V \cap^V (\mathcal{C} + V^\perp) = [\emptyset]^V$. Assume that $P \neq \emptyset$ and $\mathcal{C}$ is non V-degenerate and let us prove that $[P]^V \cap^V (\mathcal{C} + V^\perp) \neq [\emptyset]^V$. As $\mathcal{C}$ is polyhedral, there exists a V-polyhedron $C \in \mathcal{C}$. Let us consider a finite class $\mathcal{H}$ of V-hyperplanes such that V is $(V, \mathcal{H})$-definable. As $C \backslash (\bigcup_{H \in \mathcal{H}} H)$ is a finite union of V-polyhedrons of the form $C_{V,\#}$ where $\# \in \{<, >\}^{\mathcal{H}}$ and $[H]^V = [\emptyset]^V$, we can assume without loss of generality that there exists $\#$ such that $\mathcal{C} = [C_{V,\#}]^V$. Moreover,as a semi-$V$-pattern is a finite union of V-pattern, we can also assume without loss of generality that there exists $a \in \mathbb{Z}^m$ and a V-group M such that $P = a + M$. We have to prove that $[P]^V \cap^V (\mathcal{C} + V^\perp) \neq [\emptyset]^V$. That means V is included in $\overrightarrow{\text{saff}}((a+M) \cap (V_{V,\#} + V^\perp))$. Let $(\alpha_H, c_H)_{H \in \mathcal{H}}$ be a sequence of elements in $(V \backslash \{\mathbf{e}_{0,m}\}) \times \mathbb{Q}$ such that $H^{\#_H} = \{x \in V;\ \langle \alpha_H, x \rangle > c_H\}$ for any $H \in \mathcal{H}$. Lemma 11.6 proves that there exists $v \in V$ such that $\langle \alpha_H, v \rangle > 0$ for any $H \in \mathcal{H}$. By replacing v by a vector in $(\mathbb{N} \backslash \{0\}).v$, we can assume that $v \in M$. Let $a' = \Pi_V(a)$ be the orthogonal projection of a over V. Vector $v' = a - a' \in V^\perp$. There exists an integer $k \in \mathbb{N}$ enough larger such that $\langle \alpha, a' + k.v \rangle > c_H$ for any $H \in \mathcal{H}$. In particular $a' + k.v \in C$. As $k.v \in M$, we deduce that $a + k.v \in P$. From $a + k.v = (a' + k.v) + v'$ we get $a + k.v \in C + V^\perp$. Hence $x_0 = a + k.v \in P \cap (C + V^\perp)$. Let us now consider a finite set V_0 of $\dim(V)$ vectors in $\mathbb{Q}^m$ that generates V. By replacing V_0 by $k.V_0$ where $k \in \mathbb{N} \backslash \{0\}$ is enough larger, we can assume that $V_0 \subseteq M$. Moreover, by replacing V_0 by $V_0 + k.v$ where $k \in \mathbb{N}$ is enough larger, we can assume that $\langle \alpha_H, v_0 \rangle > 0$ for every $(H, v_0) \in \mathcal{H} \times V_0$. We deduce that $x_0 + \sum_{v_0 \in V_0} \mathbb{N}.v_0 \subseteq P \cap (C + V^\perp)$. Covering lemma 9.9 proves that $\overrightarrow{\text{saff}}(x_0 + \sum_{v_0 \in V_0} \mathbb{N}.v_0) = V$. In particular from $x_0 + \sum_{v_0 \in V_0} \mathbb{N}.v_0 \subseteq P \cap (C + V^\perp)$ we get $V \subseteq \overrightarrow{\text{saff}}(P \cap (C + V^\perp))$. □

Definition 12.3. *A* V-polyhedral partition $(\mathcal{C}_i)_{i \in I}$ *is a non empty finite sequence of V-polyhedral equivalence classes such that $\mathcal{C}_{i_1} \cap^V \mathcal{C}_{i_2} = [\emptyset]^V$ if and only if $i_1 \neq i_2$ and such that $[V]^V = \bigcup^V_{i \in I} \mathcal{C}_i$.*

Theorem 12.4 (Decomposition theorem). *Let $X \subseteq \mathbb{Z}^m$ be a Presburger-definable set and V be an affine component of $\overrightarrow{\text{saff}}(X)$. There exists a unique V-polyhedral partition $(\mathcal{C}_{V,P}(X))_{P \in \mathcal{P}_V(X)}$ indexed by a non-empty finite class $\mathcal{P}_V(X)$ of semi-V-patterns such that:*

$$[X_V]^V = \bigcup_{P \in \mathcal{P}_V(X)}^V ([P]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp))$$

Proof. Let us first prove that two V-polyhedral partitions $(\mathcal{C}_{V,P})_{P \in \mathcal{P}_V}$ and $(\mathcal{C}'_{V,P'})_{P' \in \mathcal{P}'_V}$ that satisfies $[X_V]^V = \bigcup^V_{P \in \mathcal{P}_V} ([P]^V \cap^V (\mathcal{C}_{V,P} + V^\perp))$ and $[X_V]^V = \bigcup^V_{P' \in \mathcal{P}'_V} ([P']^V \cap^V (\mathcal{C}'_{V,P'} + V^\perp))$ are equal. Consider $P \in \mathcal{P}_V$. As

$[V]^V = \bigcup^V_{P'\in\mathcal{P}'_V} \mathcal{C}'_{V,P'}$, we deduce that $\mathcal{C}_{V,P} = \bigcup^V_{P'\in\mathcal{P}'_V}(\mathcal{C}_{V,P} \cap^V \mathcal{C}'_{V,P'})$. In particular, there exists $P' \in \mathcal{P}'_V$ such that $\mathcal{C}_{V,P} \cap^V \mathcal{C}'_{V,P'} \neq [\emptyset]_V$. Consider such a $P' \in \mathcal{P}'_V$. By intersecting the equality $\bigcup^V_{P\in\mathcal{P}_V}([P]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp)) = \bigcup^V_{P'\in\mathcal{P}'_V}([P']^V \cap^V (\mathcal{C}'_{V,P'}(X) + V^\perp))$ with $\mathcal{C}_{V,P} \cap^V \mathcal{C}'_{V,P'}$, we get $[P\Delta P']^V \cap^V ((\mathcal{C}_{V,P} \cap^V \mathcal{C}'_{V,P'}) + V^\perp) = [\emptyset]^V$. Lemma 12.2 proves that $P\Delta P' = \emptyset$. Hence $P = P'$ and we have proved the inclusion $\mathcal{P}_V \subseteq \mathcal{P}'_V$ and by symmetry the equality $P_V = \mathcal{P}'_V$. Remark that we have also proved that for any $P' \in \mathcal{P}'_V\backslash\{P\}$ we have $\mathcal{C}_{V,P} \cap^V \mathcal{C}'_{V,P'} = [\emptyset]^V$. Therefore $\mathcal{C}_{V,P} \cap^V (\bigcup^V_{P'\in\mathcal{P}'_V\backslash\{P\}} \mathcal{C}'_{V,P'}) = [\emptyset]^V$. As $(\mathcal{C}'_{V,P'})_{P'\in\mathcal{P}'_V}$ is a V-polyhedral partition, we deduce that $\mathcal{C}_{V,P} \subseteq^V \mathcal{C}'_{V,P}$ and by symmetry $\mathcal{C}_{V,P} = \mathcal{C}'_{V,P}$. We have proved that $(\mathcal{C}_{V,P})_{P\in\mathcal{P}_V}$ and $(\mathcal{C}'_{V,P'})_{P'\in\mathcal{P}'_V}$ are equal.

Next, let us prove that there exists a V-polyhedral partition $(\mathcal{C}_{V,P})_{P\in\mathcal{P}_V}$ satisfying $[X_V]^V = \bigcup^V_{P\in\mathcal{P}_V}([P]^V \cap^V (\mathcal{C}_{V,P} + V^\perp))$. Let us denote by $\mathcal{A}_V$ the set of $A \in \mathrm{comp}(\mathrm{saff}(X_V))$ such that $\overrightarrow{A} = V$ and let $X'_V = X_V \cap (\bigcup_{A\in\mathcal{A}_V} A)$. As X'_V is Presburger-definable, a quantification elimination shows that X'_V is a boolean combination in $\mathbb{Z}^m$ of sets of the form $\{x \in \mathbb{Z}^m;\ \langle\alpha, x\rangle \in c + n.\mathbb{Z}\}$ and of the form $\{x \in \mathbb{Z}^m;\ \langle\alpha, x\rangle \,\#c\}$ where $(\alpha, \#, c, n) \in (\mathbb{Z}^m\backslash\{0\}) \times \{<, >\} \times \mathbb{Z} \times (\mathbb{N}\backslash\{0\})$. Remark that any boolean combination of sets of the form $\{x \in \mathbb{Z}^m;\ \langle\alpha, x\rangle \in c+n.\mathbb{Z}\}$ is a semi-$\mathbb{Q}^m$-pattern and any boolean combination in $\mathbb{Q}^m$ of $\{x \in \mathbb{Q}^m;\ \langle\alpha, x\rangle \,\#c\}$ is a polyhedron. Hence, there exists a finite sequence $(P_i, C_i)_{i\in I}$ where P_i is a semi-$\mathbb{Q}^m$-pattern and C_i is a polyhedron such that $X'_V = \bigcup_{i\in I}(P_i \cap C_i)$. Let us consider a sequence $(v'_A)_{A\in\mathcal{A}_V}$ of vectors $v'_A \in A$. For any $i \in I$ and $A \in \mathcal{A}_V$, we have $A \cap C_i = A \cap (C_{i,A} + V^\perp)$ where $C_{i,A}$ is the V-polyhedron $C_{i,A} = (A \cap C_i) - v'_A$. As $I \times \mathcal{A}_V$ is finite, there exists a finite set $\mathcal{H}$ of V-hyperplanes such that $C_{i,A}$ is $(V, \mathcal{H})$-definable for any $(i, A) \in I \times \mathcal{A}_V$. We have:

$$\begin{aligned}
X'_V\backslash(\bigcup_{H\in\mathcal{H}}(H + V^\perp)) &= \bigcup_{\#\in\{<,>\}^{\mathcal{H}}} (X'_V \cap (C_{V,\#} + V^\perp)) \\
&= \bigcup_{\#\in\{<,>\}^{\mathcal{H}}} \bigcup_{(i,A)\in I\times\mathcal{A}_V} (P_i \cap A \cap (C_{i,A} + V^\perp) \cap (C_{V,\#} + V^\perp)) \\
&= \bigcup_{\#\in\{<,>\}^{\mathcal{H}}} \bigcup_{(i,A)\in I\times\mathcal{A}_V} (P_i \cap A \cap ((C_{i,A} \cap C_{V,\#}) + V^\perp)) \\
&= \bigcup_{\#\in\{<,>\}^{\mathcal{H}}} P_\# \cap (C_{V,\#} + V^\perp)
\end{aligned}$$

Where $P_\#$ is the semi-V-pattern $P_\# = \bigcup_{(i,A)\in I\times\mathcal{A}_V;\ C_{i,A}\cap C_{V,\#}\neq\emptyset}(P_i \cap A)$ (recall that $C_{i,A} \cap C_{V,\#}$ is either empty or equal to $C_{V,\#}$). Let us denote by $\mathcal{P}_V = \{P_\#;\ [C_{V,\#}]_V \neq [\emptyset]_V\}$ and consider the sequence $(C_{V,P})_{P\in\mathcal{P}_V}$ of V-polyhedrons defined by:

$$C_{V,P} = \bigcup_{\#\in\{<,>\}^{\mathcal{H}};\ P_\#=P} C_{V,\#}$$

Remark that $(\mathcal{C}_{V,P})_{P\in\mathcal{P}_V}$ where $\mathcal{C}_{V,P} = [C_{V,P}]^V$ is a V-polyhedral partition. Moreover, the set $Z_V = X_V \Delta(\bigcup_{P\in\mathcal{P}_V}(P \cap (C_{V,P} + V^\perp)))$ is included in the union of $\bigcup_{A\in \mathrm{comp}(\mathrm{saff}(X_V))\setminus\mathcal{A}_V} A$, $\bigcup_{\#\in\{<,>\}^{\mathcal{H}};\ [C_{V,\#}]_V=[\emptyset]_V}(P_\# \cap (C_{V,\#}+V^\perp))$, and $\bigcup_{H\in\mathcal{H}}(X_V \cap (H + V^\perp))$. Remark that for any $A \in \mathrm{comp}(\mathrm{saff}(X_V))\setminus\mathcal{A}_V$, we have $[A]^V = [\emptyset]^V$, for any $\# \in \{<,>\}^{\mathcal{H}}$ such that $[C_{V,\#}]_V = [\emptyset]_V$, lemma 12.2 shows that $[P_\# \cap (C_{V,\#} + V^\perp)]^V = [\emptyset]^V$, and for any $H \in \mathcal{H}$, we have $[X_V \cap (H+V^\perp)]^V = [X_V]^V \cap^V [H+V^\perp]^V = [X_V]^V \cap^V [\emptyset]^V = [\emptyset]^V$. We deduce that $[Z_V]^V = [\emptyset]^V$. Therefore $[X_V]^V = \bigcup^V_{P\in\mathcal{P}_V}([P]^V \cap^V (\mathcal{C}_{V,P} + V^\perp))$. □

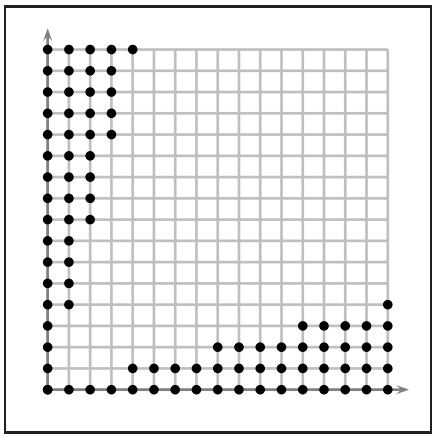

Fig. 12.1. The Presburger-definable set $X = \{x \in \mathbb{N}^2;\ (x[2] \geq 4.x[1]) \vee (x[1] \geq 4.x[2])\}$

Example 12.5. Let us consider the Presburger-definable set $X = \{x \in \mathbb{N}^2;\ (x[2] \geq 4.x[1]) \vee (x[1] \geq 4.x[2])\}$ given in figure 12.1. We have $\mathrm{saff}(X) = \mathbb{Q}^2$. Hence $V = \mathbb{Q}^2$ is the only affine component of $\overrightarrow{\mathrm{saff}}(X)$. The V-polyhedral partition $([C_{V,P}]^V)_{P\in\mathcal{P}_V}$ defined by $\mathcal{P}_V = \{\mathbb{Z}^2, \emptyset\}$, $C_{V,\mathbb{Z}^2} = \{x \in \mathbb{Q}^2;\ 0 \leq x[1] \leq 4.x[2] \vee 0 \leq x[2] \leq 4.x[1]\}$ and $C_{V,\emptyset} = V\setminus C_{V,\mathbb{Z}^2}$ satisfies decomposition theorem.

The following proposition shows that the decomposition theorem can be also applied to $[X]^V$ since $[X_V]^V = [X]^V$.

Proposition 12.6. *We have* $[X_V]^V = [X]^V$ *for any set* $X \subseteq \mathbb{Z}^m$ *and for any affine component* V *of* $\overrightarrow{\mathrm{saff}}(X)$.

Proof. Let us consider the semi-affine space S equal to the affine component A of $\mathrm{comp}(\mathrm{saff}(X))$ such that $\overrightarrow{A} \subseteq V$. Recall that $X_V = X \cap S$. In order to prove that $[X_V]^V = [X]^V$, it is sufficient to show that V is not included in

$\overrightarrow{\text{saff}}(\mathbb{Z}^m \cap (X \Delta X_V))$. Remark that $\mathbb{Z}^m \cap (X_V \Delta X) = X \backslash S$. Moreover as $X \subseteq \bigcup_{A \in \text{comp}(\text{saff}(X))} A$, we deduce that $X \backslash S \subseteq \bigcup_{A \in \text{comp}(\text{saff}(X))} (A \backslash S)$. Naturally, if $\overrightarrow{A} \subseteq V$ then $A \subseteq S$ and in particular $A \backslash S = \emptyset$. Hence $X \backslash S$ is included into the finite union of affine component A of $\text{saff}(X)$ such that $\overrightarrow{A} \not\subseteq V$. Assume by contradiction that V is included in $\overrightarrow{\text{saff}}(X \backslash S)$. From insecable lemma 9.2, we deduce that there exists such an affine component A such that $V \subseteq \overrightarrow{A}$. Hence $V \subseteq \overrightarrow{A} \subseteq \overrightarrow{\text{saff}}(X)$ and as V is an affine component of $\overrightarrow{\text{saff}}(X)$, we deduce that $V = \overrightarrow{A}$ which is in contradiction with $\overrightarrow{A} \not\subseteq V$. Hence V is not included in $\overrightarrow{\text{saff}}(X \backslash S)$ and we have proved that $[X_V]^V = [X]^V$. $\square$

Part III

From Automata to Presburger Formulas

13

Strongly Connected Components

A *component* T of a FDVG G is a strongly connected component of the parallelization $[G]$.

13.1 Untransient strongly connected components

A component T is said *untransient* if there exists a loop $q \xrightarrow{\sigma} q$ where $q \in T$ and $\sigma \in \Sigma_{r,m}^+$. Otherwise, the component T is said *transient*.

In this section, we prove that for any untransient component T of a FDVG G there exists a unique vector space $V_G(T)$ and a unique sequence $(a_G(q))_{q\in T}$ of vectors in $V_G(T)^\perp$ such that we have the following equality:

$$\mathrm{saff}(\{\xi_{r,m}(w);\ q \xrightarrow{w\in\Sigma_{r,m}^+} q\}) = a_G(q) + V_G(T)$$

Moreover, an algorithm for computing $V_G(T)$ and $(a_G(q))_{q\in T}$ in polynomial time is provided.

Remark 13.1. The vector space $V_G(T)$ does not depend on $q \in T$.

The polynomial time computation is based on a fix-point system provided by the following proposition 13.2

Proposition 13.2. *Let T be an untransient component of a FDVG G and let K_0 be the set of states $k_0 \in K$ reachable and co-reachable from T. There exists a unique minimal (for the point-wise inclusion) sequence of affine spaces $(A_{k_0})_{k_0\in K_0}$ not equal to $(\emptyset)_{k_0\in K_0}$ such that for any transition $k_0 \xrightarrow{b} k_0'$ where $(k_0, b, k_0') \in K_0 \times \Sigma_r \times K_0$, we have the following inclusion:*

$$\Gamma_{r,m,b}^{-1}(A_{k_0}) \subseteq A_{k_0'}$$

Moreover, this sequence satisfies $\mathrm{saff}(\{\xi_{r,m}(w);\ k_0 \xrightarrow{w\in\Sigma_{r,m}^+} k_0\}) = A_{k_0}$ *for any $k_0 \in K_0$.*

Proof. We denote by Z_{k_0} the set of $Z_{k_0} = \{\xi_{r,m}(w);\ k_0 \xrightarrow{w\in\Sigma_{r,m}^+} k_0\}$. By developing the expression $\xi_{r,m}(\sigma_1.w^k.\sigma_2)$ where σ_1, σ_2 are in Σ_r^* such that $\sigma_1.\sigma_2 \in \Sigma_{r,m}^+$, $w \in \Sigma_{r,m}^+$ and $n \in \mathbb{N}$, we obtain the following equality:

$$\xi_{r,m}(\sigma_1.w^n.\sigma_2) = \frac{\Gamma_{r,m,\sigma_1} \circ \xi_{r,m}(w)}{1 - r^{|\sigma_1.\sigma_2|_m + n.|w|_m}} + \Gamma^{-1}_{r,m,\sigma_2} \circ \xi_{r,m}(w)$$

Let us first prove that $(\mathrm{saff}(Z_{k_0}))_{k_0\in K_0}$ satisfies the fix-point system. Consider a transition $k_0 \xrightarrow{b} k_0'$ where $(k_0, b, k_0') \in K_0 \times \Sigma_r \times K_0$. As k_0 and k_0' and in the same strongly connected component, there exists a path $k_0' \xrightarrow{\sigma_1} k_0$. By replacing σ_1 by $\sigma_1.(b.\sigma_1)^{m-1}$, we can assume that $\sigma_1.b \in \Sigma_{r,m}^+$. Let us consider $x \in Z_{k_0}$. There exists a loop $k_0 \xrightarrow{w} k_0$ where $w \in \Sigma_{r,m}^+$ such that $x = \xi_{r,m}(w)$. Remark that for any $n \in \mathbb{N}$, we have the loop $k_0' \xrightarrow{\sigma_1.w^n.b} k_0'$. Therefore $\xi_{r,m}(\sigma_1.w^n.b) \in Z_{k_0'}$. Thanks the the equality given in the first paragraph and covering lemma 9.9, we deduce that $\mathbb{Q}.\Gamma_{r,m,\sigma_1}(x) + \Gamma^{-1}_{r,m,b}(x) \subseteq \mathrm{saff}(Z_{k_0'})$. In particular $\Gamma^{-1}_{r,m,b}(x) \in \mathrm{saff}(Z_{k_0'})$. We have proved the inclusion $\Gamma^{-1}_{r,m,b}(Z_{k_0}) \subseteq \mathrm{saff}(Z_{k_0'})$ and from covering lemma 9.9, we get $\Gamma^{-1}_{r,m,b}(\mathrm{saff}(Z_{k_0})) \subseteq \mathrm{saff}(Z_{k_0'})$. We have proved that $(\mathrm{saff}(Z_{k_0}))_{k_0\in K_0}$ satisfies the fix-point system.

Now, let us prove that $\mathrm{saff}(Z_{k_0})$ is an affine space. Remark that this semi-affine space is not empty and in particular there exists at least one affine component A of $\mathrm{saff}(Z_{k_0})$. Let $x \in Z_{k_0}$. Assume by contradiction that $Z_{k_0}\backslash A$ is not empty. Let us consider a vector $x \in Z_{k_0}\backslash A$. By definition of Z_{k_0}, there exists a loop $k_0 \xrightarrow{w} k_0$ where $w \in \Sigma_{r,m}^+$ such that $x = \xi_{r,m}(w)$. From the previous paragraph, we deduce that $\Gamma^{-1}_{r,m,w^n}(\mathrm{saff}(Z_{k_0})) \subseteq \mathrm{saff}(Z_{k_0})$ for any $n \in \mathbb{N}$. In particular $\Gamma^{-1}_{r,m,w^n}(A) \subseteq \mathrm{saff}(Z_{k_0})$ for any $n \in \mathbb{N}$. Remark that $\Gamma^{-1}_{r,m,w^n}(A) = r^{-n.|w|}.(A - x) + x$ thanks to $x = \xi_{r,m}(w)$. Covering lemma 9.9 shows that $\mathbb{Q}.(A-x)+x \subseteq \mathrm{saff}(Z_{k_0})$. As $A \subseteq \mathbb{Q}.(A-x)+x \subseteq \mathrm{saff}(Z_{k_0})$ and A is an affine component of $\mathrm{saff}(Z_{k_0})$, we deduce the equality $A = \mathbb{Q}.(A - x) + x$. In particular $x \in A$ and we obtain a contradiction. We have proved that $Z_{k_0}\backslash A = \emptyset$. Therefore $Z_{k_0} \subseteq A$. We get $\mathrm{saff}(Z_{k_0}) = A$. Therefore $\mathrm{saff}(Z_{k_0})$ is an affine space (remark that even if these proof is similar to the one provided by proposition 9.11, we cannot apply this proposition since Z_{k_0} is not necessary (r, m, w)-cyclic).

Finally, let us consider a sequence of affine spaces $(A_{k_0})_{k_0\in K_0}$ not equal to $(\emptyset)_{k_0\in K_0}$ such that $\Gamma^{-1}_{r,m,b}(A_{k_0}) \subseteq A_{k_0'}$ for any transition $(k_0 \xrightarrow{b} k_0'$ with $(k_0, b, k_0') \in K_0 \times \Sigma_r \times K_0$ and let us prove that $\mathrm{saff}(Z_{k_0}) \subseteq A_{k_0}$ for any $k_0 \in K_0$. An immediate induction shows that $\Gamma^{-1}_{r,m,\sigma}(A_{k_0}) \subseteq A_{k_0'}$ for any path $k_0 \xrightarrow{\sigma} k_0'$ where $(k_0, \sigma, k_0') \in K_0 \times \Sigma_r^* \times K_0$. Since $\mathrm{saff}(Z_{k_0})$ is an affine space, it is sufficient to show that $Z_{k_0} \subseteq A_{k_0}$. Since $(A_{k_0})_{k_0\in K_0}$ is not equal to the empty sequence $(\emptyset)_{k_0\in K_0}$, there exists at least a state $k_1 \in K_0$ such that $A_{k_1} \not\emptyset$. By definition of K_0, there exists a path $k_1 \xrightarrow{\sigma} k_0$. From $\Gamma^{-1}_{r,m,\sigma}(A_{k_1}) \subseteq A_{k_0}$ we deduce that $A_{k_0} \neq \emptyset$. Hence, there exists $a \in A_{k_0}$. Since $x \in Z_{k_0}$, there exists $w \in \Sigma_{r,m}^+$ such that $k_0 \xrightarrow{w} k_0$. From the path $k_0 \xrightarrow{w^n} k_0$, we get

$\Gamma^{-1}_{r,m,w^n}(A_{k_0}) \subseteq A_{k_0}$ for any $n \in \mathbb{N}$. Hence $\Gamma^{-1}_{r,m,w^n}(a) \in A_{k_0}$ for any $n \in \mathbb{N}$. Since $\Gamma^{-1}_{r,m,w^n}(a) = r^{-|w|_m}.(a - \xi_{r,m}(w)) + \xi_{r,m}(w)$, from covering lemma 9.9, we get $\mathbb{Q}.(a - \xi_{r,m}(w)) + \xi_{r,m}(w) \in A_{k_0}$. In particular $\xi_{r,m}(w) \in A_{k_0}$ and we have proved that $Z_{k_0} \subseteq A_{k_0}$. Thus $\mathrm{saff}(Z_{k_0}) \subseteq A_{k_0}$ for any $k_0 \in K_0$.

Since $(\mathrm{saff}(Z_{k_0}))_{k_0 \in K_0}$ is not equal to $(\emptyset)_{k_0 \in K_0}$, we are done. □

We deduce the following proposition 13.3 that shows that a characteristic vector space denoted by $V_G(T)$ is associated to any untransient component T of a finite DVG G. This vector space is extremely useful in the sequel for extracting geometrical properties from a FDVA.

Proposition 13.3. *Let T be an untransient component of a finite graph G labelled by $\Sigma_{r,m}$. There exists a unique vector space $V_G(T)$ and a unique sequence $(a_G(q))_{q \in T}$ of vectors in $V_G(T)^\perp$ such that for any $q \in Q$:*

$$\mathrm{saff}(\{\xi_{r,m}(w);\ q \xrightarrow{w \in \Sigma^+_{r,m}} q\}) = a_G(q) + V_G(T)$$

Proof. Let $A_q = \mathrm{saff}(\{\xi_{r,m}(w);\ q \xrightarrow{w \in \Sigma^+_{r,m}} q\})$. The previous proposition 13.2 proves that A_q is a non empty affine space. It is sufficient to show that the vector space $\overrightarrow{A_q}$ that does not depend on $q \in T$. By symmetry, it is sufficient to prove that $\overrightarrow{A_{q_1}} \subseteq \overrightarrow{A_{q_2}}$ for any $q_1, q_2 \in T$. Since T is strongly connected, there exists a path $q_1 \xrightarrow{\sigma} q_2$ with $\sigma \in \Sigma^*_{r,m}$. Proposition 13.2 proves by an immediate induction that $\Gamma^{-1}_{r,m,\sigma}(A_{q_1}) \subseteq A_{q_2}$. Since the affine space $\Gamma^{-1}_{r,m,w}(A_{q_1})$ is equal to $r^{-|w|_m}.(A_{q_1} - \rho_{r,m}(w, \mathbf{e}_{0,m}))$, its direction is equal to $\overrightarrow{A_{q_1}}$. We deduce that $\overrightarrow{A_{q_1}} \subseteq \overrightarrow{A_{q_2}}$. □

13.1.1 A polynomial time algorithm

Thanks to the fix-point system provided by proposition 13.2, we are going to show that $V_G(T)$ is computable in polynomial time from G.

Theorem 13.4. *Let T be an untransient component of a FDVG G. The vector space $V_G(T)$ is computed in polynomial by the algorithm given in figure 13.1.*

Proof. Naturally, the algorithm terminates in polynomial time. Let us prove that the vector space V returned by the algorithm is equal to $V_G(T)$. Let $(S_{k_0})_{k_0 \in K_0}$ be the sequence of affine spaces $S_{k_0} = \mathrm{saff}(\{\xi_{r,m}(w);\ k_0 \xrightarrow{w \in \Sigma^+_{r,m}} k_0\})$. For any state $k_0 \in K_0$ let us consider the set $J_{k_0} = \lambda(k_0) - \lambda(k_0)$ the set of difference of two elements in $\lambda(k_0)$.

Let us show that for any $k_0, k_0' \in K_0$, we have $J_{k_0} + m.\mathbb{Z} = J_{k_0'} + m.\mathbb{Z}$. It is sufficient to show the inclusion $J_{k_0} \subseteq J_{k_0'} + m.\mathbb{Z}$. Let $i_1, i_2 \in J_{k_0}$. There exists two paths $q_1 \xrightarrow{\sigma_1} k_0$ and $q_2 \xrightarrow{\sigma_2} k_0$ where $|\sigma_1| \in i_1 + m.\mathbb{Z}$, $|\sigma_2| \in i_2 + m.\mathbb{Z}$ and $q_1, q_2 \in T$. Since T is strongly connected (for $[G]$), there exists

a path $k_0 \xrightarrow{w} k'_0$. From the path $q_1 \xrightarrow{\sigma_1.w} k'_0$ and $q_2 \xrightarrow{\sigma_2.w} k'_0$ we deduce that $(|\sigma_1| + |w|) - (|\sigma_2| + |w|) \in J_{k'_0} + m.\mathbb{Z}$. Hence $i_1 - i_2 \in J_{k'_0} + m.\mathbb{Z}$. We have proved that for any $k_0, k'_0 \in K_0$, we have $J_{k_0} + m.\mathbb{Z} = J_{k'_0} + m.\mathbb{Z}$.

Thanks to the previous paragraph, we deduce that $\Gamma^{-i_1}_{r,m,0}(V) = \Gamma^{-i_2}_{r,m,0}(V)$ for any $i_1, i_2 \in \lambda(k_0)$ and for any $k_0 \in K_0$ is an invariant of the algorithm. Thus, for any $k_0 \in K_0$, there exists a vector space V_{k_0} such that $V_{k_0} = \Gamma^{-i}_{r,m,0}(V)$ for any $i \in \lambda(k_0)$. For any transition $k_0 \xrightarrow{b} k'_0$ such that $(k_0, b, k'_0) \in K_0 \times \Sigma_r \times K_0$, let $x_{k_0,b,k'_0} = \Gamma^{-1}_{r,m,b}(\xi_{r,m}(\sigma_{k_0})) - \xi_{r,m}(\sigma_{k'_0})$, and let $A_{k_0} = \xi_{r,m}(\sigma_{k_0}) + V_{k_0}$.

Let us show that $V_G(T) \subseteq V$. Since for any transition $k_0 \xrightarrow{b} k'_0$ where $(k_0, b, k'_0) \in K_0 \times \Sigma_r \times K_0$ and for any $i \in \lambda(k_0)$, we have $\Gamma^i_{r,m,0}(x_{k_0,b,k'_0}) \in V$, we deduce that $\Gamma^{-1}_{r,m,b}(A_{k_0}) = A_{k'_0}$ and in particular $(A_{k_0})_{k_0 \in K_0}$ is a sequence of affine spaces satisfying the fix-point system provided by proposition 13.2 and not equal to $(\emptyset)_{k_0 \in K_0}$. By minimality of the sequence $(S_{k_0})_{k_0 \in K_0}$, we deduce that $S_{k_0} \subseteq A_{k_0}$. Taking the direction of the previous inclusion, we get $V_G(T) \subseteq V$.

Let us prove the converse inclusion $V \subseteq V_G(T)$. Remark that V is generated by vectors $\Gamma^i_{r,m,0}(x_{k_0,b,k'_0})$ where $k_0 \xrightarrow{b} k'_0$ is a transition such that $(k_0, b, k'_0) \in K_0 \times \Sigma_r \times K_0$, and $i \in \lambda(k_0)$. Since $V_G(T)$ is a vector space, it is sufficient to prove that $\Gamma^{i+1}_{r,m,0}(x_{k_0,b,k'_0}) \in V_G(T)$. Remark that $\xi_{r,m}(\sigma_{k_0}) \in S_{k_0}$ and since $\Gamma^{-1}_{r,m,b}(S_{k_0}) \subseteq S_{k'_0}$, we get $\Gamma^{-1}_{r,m,b}(\xi_{r,m}(\sigma_{k_0})) \in S_{k'_0}$. Moreover, as $\xi_{r,m}(\sigma_{k'_0}) \in S_{k'_0}$ and $S_{k'_0}$ is an affine space, we get $x_{k_0,b,k'_0} \in \overrightarrow{S}_{k'_0}$. By definition of λ, there exists a path $q \xrightarrow{\sigma} k_0$ such that $|\sigma| \in i + m.\mathbb{Z}$. As T is strongly connected for $[G]$, there exists a path $k'_0 \xrightarrow{w} q$ where $q \in T$ and $\sigma.b.w \in \Sigma^*_{r,m}$. As $\Gamma^{-1}_{r,m,w}(S_{k'_0}) \subseteq S_q$, taking the direction of the previous inclusion provides $\Gamma^{-|w|}_{r,m,0}(\overrightarrow{S}_{k'_0}) \subseteq V_G(T)$. From $x_{k_0,b,k'_0} \in \overrightarrow{S}_{k'_0}$ we get $x_{k_0,b,k'_0} \in \Gamma^{|w|}_{r,m,0}(V_G(T))$. As $\Gamma^m_{r,m,0}(V_G(T)) = V_G(T)$ (in fact for any vector space W we have $\Gamma^m_{r,m,0}(W) = W$), we deduce that $Gamma^{|w|}_{r,m,0}(V_G(T)) = \Gamma^{-(i+1)}_{r,m,0}(V_G(T))$. Thus $\Gamma^{i+1}_{r,m,0}(x_{k_0,b,k'_0}) \in V_G(T)$ and we have proved the other inclusion $V \subseteq V_G(T)$. □

Example 13.5. Let $\mathcal{A}_{r,1}(\{1\})$ be the FDVA given in figure 13.2. The two components $T_1 = \{\{0\}\}$ and $T_\perp = \{\emptyset\}$ are untransient,and the component $T_0 = \{\{1\}\}$ is transient.

Example 13.6. Let $\mathcal{A}_{r,3}(+)$ be the FDVA representing $\{x \in \mathbb{Z}^3;\ x[1] + x[2] = x[3]\}$ and given in figure 6.2. We denote by q_0, q_1 and $q_\perp$, the principal states $q_0 = \{x \in \mathbb{Z}^3;\ x[1] + x[2] = x[3]\}$, $q_1 = \{x \in \mathbb{Z}^m;\ x[1] + x[2] + 1 = x[3]\}$ and $q_\perp = \emptyset$. The two strongly connected components $T_0 = \{q_0, q_1\}$ and $T_\perp = \{q_\perp\}$ are untransient. We have $V_G(T_\perp) = \mathbb{Q}^3$ and $V_G(T_0) = \{x \in \mathbb{Q}^3;\ x[1] + x[2] = x[3]\}$.

function $V_G(T)$.
input
A FDVG $G = (Q, m, K, \Sigma_r, \delta)$ and an untransient component of T of G.
output
$V_G(T)$.
begin
  let K_0 be the set of states $k_0 \in K$ reachable and co-reachable from T.
  for each state $k_0 \in K_0$.
    let $\sigma_{k_0} \in \Sigma_{r,m}^+$ such that $k_0 \xrightarrow{\sigma_{k_0}} k_0$.
    let $\lambda(k_0) \leftarrow \{i \in \{0, \ldots, m-1\};\ T \xrightarrow{\Sigma_{r,m}^* . \Sigma_r^i} k_0\}$.
  end for.
  let $V \leftarrow \{\mathbf{e}_{0,m}\}$.
  for each transition $k_0 \xrightarrow{b} k_0'$.
    let $x \leftarrow \Gamma_{r,m,b}^{-1}(\xi_{r,m}(\sigma_{k_0})) - \xi_{r,m}(\sigma_{k_0'})$.
    let $V \leftarrow V + \sum_{i \in \lambda(k_0)} \mathbb{Q}.\Gamma_{r,m,0}^{i+1}(x)$.
  end for.
  return V.
end

Fig. 13.1. An algorithm computing in polynomial time $V_G(T)$.

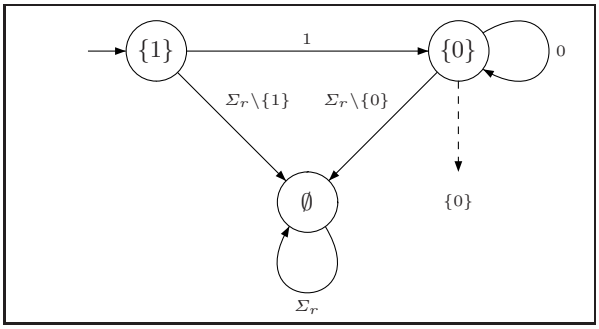

Fig. 13.2. The FDVA $\mathcal{A}_{r,1}(\{1\})$

Example 13.7. Let $\mathcal{A}_{r,2}(V_r)$ be the FDVA representing $\{x \in \mathbb{Z}^2;\ V_r(x[1]) = x[2]\}$ and given in figure 6.3. We denote by q_0, q_1 and $q_\perp$ the principal states $q_0 = \{x \in \mathbb{Z}^2;\ V_r(x[1]) = x[2]\}$, $q_1 = \mathbb{Z} \times \{0\}$ and $q_\perp = \emptyset$. The three strongly connected components $T_0 = \{q_0\}$, $T_1 = \{q_1\}$ and $T_\perp = \{q_\perp\}$ are untransient. Moreover, the vector spaces associated to T_0, T_1, $T_\perp$ are respectively equal to $\{\mathbf{e}_{0,m}\}$, $\mathbb{Q} \times \{0\}$ and $\mathbb{Q}^2$.

13.2 Detectable semi-V-patterns

In this section, we prove that any semi-V-pattern $P \in \mathcal{P}_V(X)$ introduced by decomposition theorem 12.4 is (r,m)-detectable in X for any affine component V of $\overrightarrow{\text{saff}}(X)$ and for any Presburger-definable set X. That means, given a DVA $\mathcal{A}$ that represents X, there exists a final function F such that P is represented by $\mathcal{A}^F$. Independently, being given a semi-V-pattern P and a FDVA $\mathcal{A}$ that represents a set X not necessary Presburger-definable, a polynomial time algorithm for deciding if there exists a final function F such that P is represented by $\mathcal{A}^F$ is provided.

Lemma 13.8. *Given a Presburger definable set X, an affine component V of $\overrightarrow{\text{saff}}(X)$ and a word $\sigma \in \Sigma^*_{r,m}$, we have:*

$$[\gamma^{-1}_{r,m,\sigma}(X)]^V = \bigcup_{P\in\mathcal{P}_V(X)}^{V} ([\gamma^{-1}_{r,m,\sigma}(P)]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp))$$

Proof. Recall that $[X]^V = \bigcup^V_{P\in\mathcal{P}_V(X)}([P]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp))$ from decomposition theorem 12.4 and proposition 12.6. We deduce that $[\gamma^{-1}_{r,m,\sigma}(X)]^V = \bigcup^V_{P\in\mathcal{P}_V(X)}([\gamma^{-1}_{r,m,\sigma}(P)]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp))$ from lemmas 10.3 and 10.4 and corollary 11.18. □

Corollary 13.9. *Let X be a Presburger-definable set and V be an affine component of $\overrightarrow{\text{saff}}(X)$. Any set $P \in \mathcal{P}_V(X)$ is detectable in X.*

Proof. Let us consider a pair (σ_1, σ_2) of words in $\Sigma^*_{r,m}$ such that $\gamma^{-1}_{r,m,\sigma_1}(X) = \gamma^{-1}_{r,m,\sigma_2}(X)$. From lemma 13.8 we deduce that $\bigcup^V_{P\in\mathcal{P}_V(X)}([\gamma^{-1}_{r,m,\sigma_1}(P)]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp)) = \bigcup^V_{P\in\mathcal{P}_V(X)}([\gamma^{-1}_{r,m,\sigma_2}(P)]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp))$. By intersecting the previous equality by $\mathcal{C}_{V,P}(X) + V^\perp$, we get $[\gamma^{-1}_{r,m,\sigma_1}(P)]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp) = [\gamma^{-1}_{r,m,\sigma_2}(P)]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp)$. From lemma 12.2 we deduce that $\gamma^{-1}_{r,m,\sigma_1}(P) = \gamma^{-1}_{r,m,\sigma_2}(P)$. □

Even if the following two corollaries are not used in this section, they become useful in the sequel.

Corollary 13.10. *Let X be a (r,m,w)-cyclic Presburger-definable set and let V be an affine component of $\overrightarrow{\text{saff}}(X)$. Any semi-$V$-pattern $P \in \mathcal{P}_V(X)$ is relatively prime with r and included in the V-affine space $A = \xi_{r,m}(w) + V$.*

Proof. Since any $P \in \mathcal{P}_V(X)$ is (r,m)-detectable in X, we deduce that any $P \in \mathcal{P}_V(X)$ is (r,m,w)-cyclic. From lemma 9.20, any $P \in \mathcal{P}_V(X)$ is relatively prime with r and included in A. □

Corollary 13.11. *The set $\mathbb{Z}^m \cap (\xi_{r,m}(w) + V)$ is (r,m)-detectable in X for any Presburger-definable set $X \subseteq \mathbb{Z}^m$ and any affine component $V \in$ comp(saff(X)).*

Proof. Let A be the V-affine space $A = \xi_{r,m}(w) + V$. Let us consider $P \in \mathcal{P}_V(X)\backslash\{\emptyset\}$. It is sufficient to prove that $\mathbb{Z}^m \cap A$ is (r,m)-detectable in P. Consider a pair (σ_1, σ_2) of words in $\Sigma_{r,m}^*$ such that there exists P' satisfying $\gamma_{r,m,\sigma_1}^{-1}(P) = P' = \gamma_{r,m,\sigma_2}^{-1}(P)$. Remark that if $P' = \emptyset$ then the dense pattern corollary 9.23 shows that $\gamma_{r,m,\sigma_1}^{-1}(\mathbb{Z}^m \cap A) = \emptyset = \gamma_{r,m,\sigma_2}^{-1}(\mathbb{Z}^m \cap A)$. If $P' = \emptyset$, we deduce that $\mathrm{saff}(\gamma_{r,m,\sigma_i}^{-1}(P)) = \Gamma_{r,m,\sigma_i}^{-1}(A)$. Therefore $\Gamma_{r,m,\sigma_1}^{-1}(A) = \Gamma_{r,m,\sigma_2}^{-1}(A)$. In particular, by intersecting the previous equality by $\mathbb{Z}^m$, we get $\gamma_{r,m,\sigma_1}^{-1}(\mathbb{Z}^m \cap A) = \gamma_{r,m,\sigma_2}^{-1}(\mathbb{Z}^m \cap A)$. □

Theorem 13.12. *Let $\mathcal{A}$ be a FDVA, let M be a V-vector lattice included in $\mathbb{Z}^m$, and let B be a non empty finite subset of $\mathbb{Z}^m$. We can compute in polynomial time a partition B_0, B_1, ..., B_n of B such that a semi-V-pattern P of the form $P = B' + M$ where $B' \subseteq B$ is represented by a FDVA of the form $\mathcal{A}^F$ if and only if there exists $J \subseteq \{1, \ldots, n\}$ such that $B = \bigcup_{j\in J} B_j$.*

Proof. Let us denote by $\mathcal{C}$ the class of subsets of $X' \subseteq \mathbb{Z}^m$ that can be represented by the FDVA $\mathcal{A}^F$ where F is any final function. Since $\mathcal{C}$ is stable by boolean operations in $\{\cup, \cap, \backslash, \Delta\}$, we deduce that exists a unique partition B_0, B_1, ..., B_n of a subset of B satisfying the theorem. From proposition 4.6, we deduce that there exists a finite set U of pairs (σ_1, σ_2) of words in Σ_r^* computable in polynomial time such that $|\sigma_1| + m.\mathbb{Z} = |\sigma_2| + m.\mathbb{Z}$ for any $(\sigma_1, \sigma_2) \in U$, and such that a subset $X' \subseteq \mathbb{Z}^m$ is in in $\mathcal{C}$ if and only if $\gamma_{r,m,\sigma_1}^{-1}(X') = \gamma_{r,m,\sigma_2}^{-1}(X')$ for any $(\sigma_1, \sigma_2) \in U$. Let us consider the binary relation $\mathcal{R}$ over B defined by $b_1 \mathcal{R} b_2$ if and only if there exists $(\sigma_1, \sigma_2) \in U$ such that $\gamma_{r,m,\sigma_1}^{-1}(b_1 + M) \cap \gamma_{r,m,\sigma_2}^{-1}(b_2 + M) \neq \emptyset$. The symmetrical and transitive closure of $\mathcal{R}$ denoted by $\mathcal{R}'$ provides an equivalence relation of B. Let us consider the equivalence classes B'_1, ..., B'_k of $\mathcal{R}'$ such that the last classes $B'_{n'+1}$, ..., B'_k are the equivalence classes such that $B'_i + M$ is not in $\mathcal{C}$.

Let us prove that $B_0 = \bigcup_{i=n+1}^k B'_i$ and B_1, ..., B_n are equal up to a permutation to B'_1, ..., $B'_{n'}$. Observe that $B_i + M$ is in $\mathcal{C}$ for any $i \geq 1$. Thus for any $(\sigma_1, \sigma_2) \in U$, we have $\gamma_{r,m,\sigma_1}^{-1}(B_i + M) = \gamma_{r,m,\sigma_2}^{-1}(B_i + M)$. In particular $b_1 \mathcal{R} b_2$ implies that there exists $i \geq 0$ such that $b_1, b_2 \in B_i$. We have proved that for any equivalence class B' of $\mathcal{R}'$, there exists i such that $B' \subseteq B_i$. Note that if $B' \subseteq B_0$ then $B' + M$ is not in $\mathcal{C}$ by definition of B_0. Next, assume that $B' \subseteq B_i$ with $i \geq 1$. Let us consider $(\sigma_1, \sigma_2) \in U$ and let $x \in \gamma_{r,m,\sigma_1}^{-1}(B' + M)$. There exists $b_1 \in B'$ such that $\gamma_{r,m,\sigma_1}(x) \in b_1 + M$. Since $B_i + M \in \mathcal{C}$, we get $\gamma_{r,m,\sigma_1}^{-1}(B_i + M) = \gamma_{r,m,\sigma_2}^{-1}(B_i + M)$. As $b_1 \in B' \subseteq B_i$, we deduce that there exists $b_2 \in B_i$ such that $\gamma_{r,m,\sigma_2}(x) \in b_2 + M$. Thus $\gamma_{r,m,\sigma_1}^{-1}(b_1 + M) \cap \gamma_{r,m,\sigma_2}^{-1}(b_2 + M) \neq \emptyset$ and we have proved that $b_1 \mathcal{R} b_2$. Since $b_1 \in B'$ we get $b_2 \in B'$ and we have proved that $\gamma_{r,m,sigma_1}^{-1}(B' + M) \subseteq \gamma_{r,m,\sigma_2}^{-1}(B' + M)$. By symmetry, we get the equality $\gamma_{r,m,\sigma_1}^{-1}(B' + M) = \gamma_{r,m,\sigma_2}^{-1}(B' + M)$. We have proved that $B' + M \in \mathcal{C}$. Since B' is non empty and included in B_i, we deduce that $B' = B_i$. We have proved that $B_0 = \bigcup_{i=n+1}^k B'_i$ and B_1, ..., B_n are equal up to a permutation to B'_1, ..., $B'_{n'}$.

Therefore, it is sufficient to prove that we can decide in polynomial time if $\gamma_{r,m,\sigma_1}^{-1}(b_1 + M) \cap \gamma_{r,m,\sigma_2}^{-1}(b_2 + M) \neq \emptyset$ for any $b_1, b_2 \in B$, and we can decide

in polynomial time if $B' + M \in \mathcal{C}$ for any $B' \subseteq B$. Proposition 9.18 prove that for any word σ and for any finite subset $B' \subseteq \mathbb{Z}^m$, we can compute in polynomial time a finite subset $B_\sigma \subseteq \mathbb{Z}^m$ and a vector lattice M_σ such that $|B_\sigma| \leq |B'|$ and $\gamma^{-1}_{r,m,\sigma}(B' + M) = B_\sigma + M_\sigma$. Therefore, it is sufficient to prove that given two vector lattices M_1 and M_2, two finite subsets B_1 and B_2 of $\mathbb{Z}^m$, and two vectors b_1 and B_2 in $\mathbb{Z}^m$, we can decide in polynomial time if $b_1 + M_1 \cap b_2 + M_2 \neq \emptyset$ and we can decide in polynomial time if $(B_1 + M_1) = (B_2 + M_2)$. From corollaries 8.16 and 9.16, we are done. □

13.3 Terminal components

A *terminal component* T of a FDVA $\mathcal{A} = (q_0, G, F_0)$ is a component of G satisfying:

- T is reachable (for $[G]$) from the initial state q_0,
- there exists a state $q \in T$ such that $[F_0](q) \neq \emptyset$, and
- any state q' reachable (for $[G]$) from T such that $[F_0](q') \neq \emptyset$ is in T.

The set of terminal components of a FDVA $\mathcal{A}$ is denoted by $\mathcal{T}_\mathcal{A}$.

Observe that $V_G(T)$ is defined for any terminal component T since the following proposition 13.13 show that such a T is untransient.

Proposition 13.13. *A terminal component is untransient.*

Proof. Let T be a terminal component of a FDVA $\mathcal{A}$. Consider a state $q \in T$ such that $[F_0](q) \neq \emptyset$, and let $s \in [F_0](q)$. Since F_0 is saturated for G and $s \in [F_0](q)$ we deduce that $s \in [F_0](\delta(q, s^n))$ for any $n \in \mathbb{N}$. As T is terminal, we have $\delta(q_0, s^n) \in T$. Moreover, as Q is finite, there exits $n \in \mathbb{N}$ and $d \in \mathbb{N}\backslash\{0\}$ such that $\delta(q_0, s^{n+d}) = \delta(q_0, s^n)$. We have proved that there exists a loop of the state $q' = \delta(q, s^n)$. From $q' \in T$ we deduce that T is untransient. □

The *terminal components* have a lot of applications in the sequel. In this section we show that $\mathrm{saff}(X_q) = a_G(q) + V_G(T)$ and we provide a geometrical characterization of the sets X_q.

Lemma 13.14 (Destruction lemma). *Let $\sigma \in \Sigma^+_{r,m}$ be a non-empty word and let A be an affine space. There exists $k_0 \in \mathbb{N}$ such that $\gamma^{-1}_{r,m,\sigma^{k_0}}(\mathbb{Z}^m \cap A) = \emptyset$ if and only if $\xi_{r,m}(\sigma) \notin A$ or $\mathbb{Z}^m \cap A = \emptyset$.*

Proof. We can assume without loss of generality that $\mathbb{Z}^m \cap A \neq \emptyset$. In particular $\overrightarrow{A}$ is a vector space (because A is non empty) and there exists a finite set $D \subseteq \mathbb{Z}^m\backslash\{\mathbf{e}_{0,m}\}$ such that $\overrightarrow{A} = \{x \in \mathbb{Q}^m;\ \bigwedge_{\alpha \in D} \langle \alpha, x\rangle = 0\}$.

Assume first that $\xi_{r,m}(\sigma) \in A$. The set $\mathbb{Z}^m \cap A$ is equal to $\{x \in \mathbb{Z}^m;\ \bigwedge_{\alpha \in D} \langle \alpha, x - \xi_{r,m}(\sigma)\rangle = 0\}$. Remark that $\gamma^{-1}_{r,m,\sigma}(\mathbb{Z}^m \cap A) = \{x \in \mathbb{Z}^m;\ \bigwedge_{\alpha \in D} \langle \alpha, \gamma_{r,m,\sigma}(x) - \xi_{r,m}(\sigma)\rangle = 0\} = \mathbb{Z}^m \cap A$. In particular $\gamma^{-1}_{r,m,\sigma^k}(\mathbb{Z}^m \cap A) \neq \emptyset$ for any $k \in \mathbb{N}$.

Next, assume that $\gamma_{r,m,\sigma^k}^{-1}(\mathbb{Z}^m \cap A) \neq \emptyset$ for any $k \in \mathbb{N}$. As $\mathbb{Z}^m \cap A \neq \emptyset$, there exists $a \in A$. For any $k \in \mathbb{N}$, we have:

$$\begin{aligned}
&\gamma_{r,m,\sigma^k}^{-1}(\mathbb{Z}^m \cap A)\\
&= \left\{ x \in \mathbb{Z}^m;\ \bigwedge_{\alpha \in D} \left\langle \alpha, \gamma_{r,m,\sigma^k}(x) - a \right\rangle = 0 \right\}\\
&= \left\{ x \in \mathbb{Z}^m;\ \bigwedge_{\alpha \in D} \left\langle \alpha, r^{k.|\sigma|_m}.(x - \xi_{r,m}(\sigma)) + \xi_{r,m}(\sigma) - a \right\rangle = 0 \right\}\\
&= \left\{ x \in \mathbb{Z}^m;\ \bigwedge_{\alpha \in D} \left\langle \alpha, (r^{|\sigma|_m} - 1).x + \gamma_{r,m,\sigma}(\mathbf{e}_{0,m}) \right\rangle = (r^{|\sigma|_m} - 1).\frac{\langle \alpha, a - \xi_{r,m}(\sigma) \rangle}{r^{k.|\sigma|_m}} \right\}
\end{aligned}$$

Let us consider $k \in \mathbb{N}$ enough larger such that $|(r^{|\sigma|_m} - 1).\frac{\langle \alpha, a - \xi_{r,m}(\sigma) \rangle}{r^{k.|\sigma|_m}}| < 1$ for any $\alpha \in D$. As $\gamma_{r,m,\sigma^k}^{-1}(\mathbb{Z}^m \cap A) \neq \emptyset$, there exists x in this set. From $\left\langle \alpha, (r^{|\sigma|_m} - 1).x + \gamma_{r,m,\sigma}(\mathbf{e}_{0,m}) \right\rangle \in \mathbb{Z}$, we deduce that $(r^{|\sigma|_m} - 1).\frac{\langle \alpha, a - \xi_{r,m}(\sigma) \rangle}{r^{k.|\sigma|_m}}$ is in the set $\{c \in \mathbb{Z};\ |c| < 1\} = \{0\}$. Therefore $\langle \alpha, a - \xi_{r,m}(\sigma) \rangle = 0$ for any $\alpha \in D$. That means $\xi_{r,m}(\sigma) \in A$. □

Proposition 13.15. *Let $\mathcal{A} = (q_0, G, F_0)$ by a FDVA that represents a set X, let Y be an s-eye of a FDVG G and let T be a terminal component that contains* $\ker_s(Y)$. *We have* $\mathrm{saff}(X_q^{F_{s,Y}}(G)) = a_G(q) + V_G(T)$ *for any principal state $q \in T$.*

Proof. Let us denote by Z_q the set $Z_q = \{\xi_{r,m}(w);\ q \xrightarrow{w} q\}$. Recall that $\mathrm{saff}(Z_q) = a_G(q) + V_G(T)$.

Let us first prove that $\mathrm{saff}(Z_q) \subseteq \mathrm{saff}(X_q^{F_{s,Y}})$. Consider a vector $x \in Z_q$. There exists a loop $q \xrightarrow{w} q$ with $w \in \Sigma_{r,m}^+$ such that $x = \xi_{r,m}(w)$. Let $q' \in \ker_s(Y)$. As q and q' are in the same component, there exists a path $q \xrightarrow{\sigma} q'$ with $\sigma \in \Sigma_{r,m}$. Remark that $\rho_{r,m}(w^k.\sigma, s) \in X_q^{F_{s,Y}}$ for any $k \in \mathbb{N}$. By developing $\rho_{r,m}(w^k.\sigma, s)$, we get $\rho_{r,m}(w^k.\sigma, s) = r^{k.|w|_m}.(\rho_{r,m}(\sigma, s) - x) + x$. From covering lemma 9.9, we get $\mathbb{Q}.(\rho_{r,m}(\sigma, s) - x) + x \subseteq \mathrm{saff}(X_q^{F_{s,Y}})$. In particular $x \in \mathrm{saff}(X_q^{F_{s,Y}})$ and we get $Z_q \subseteq \mathrm{saff}(X_q^{F_{s,Y}})$. By minimality of the semi-affine full, we deduce the inclusion $\mathrm{saff}(Z_q) \subseteq \mathrm{saff}(X_q^{F_{s,Y}})$.

For the converse inclusion, let us consider a vector $x \in X_q^{F_{s,Y}}$. There exists a (r,m)-decomposition (σ, s) of x such that $\delta(q, \sigma) \in Y$. By replacing σ by a word in $\sigma.s^*$, we can assume that $q' = \delta(q, \sigma)$ is in $\ker_s(Y)$. In particular, there exists $n_1 \in \mathbb{N}\backslash\{0\}$ such that $\delta(q', s^{n_1}) = q'$. Proposition 13.2 shows that $\Gamma_{r,m,w}(\xi_{r,m}(s^{n_1})) \in \mathrm{saff}(\xi_{r,m,q})$. Remark that $\xi_{r,m}(s^{n_1}) = \frac{s}{1-r}$, and we deduce that $x = \rho_{r,m}(w, s) \in \mathrm{saff}(Z_q)$. We have proved the inclusion $X_q^{F_{s,Y}} \subseteq \mathrm{saff}(Z_q)$. By minimality of the semi-affine hull, we deduce the other inclusion $\mathrm{saff}(X_q^{F_{s,Y}}) \subseteq \mathrm{saff}(Z_q)$. □

The following proposition shows that for any state q in a terminal component of a FDVA that represents a set X, the semi-affine space $\mathrm{saff}(X_q)$ can be easily computed thanks to $a_G(q)$ and $V_G(T)$.

Proposition 13.16. *Let X be a set represented by a FDVA $\mathcal{A}$ and let T be a terminal component. We have $\mathrm{saff}(X_q) = a_G(q) + V_G(T)$ for any state $q \in T$.*

Proof. Let us consider the class $\mathcal{C}_T$ of couple $(s, Y) \in S_{r,m} \times \mathcal{P}(Q)$ such that Y is an s-eye satisfying $\ker_s(Y) \subseteq T$ and $F_{s,Y} \subseteq F_0$. As T is terminal, this class is non-empty. Proposition 13.15 shows that $\mathrm{saff}(X_q^{F_{s,Y}}) = a_G(q) + V_G(T)$ for any $(s, Y) \in \mathcal{C}_T$. Let $F = \bigcup_{(s,Y)\in\mathcal{C}_T} F_{s,Y}$. As $q \in T$ and T is terminal, we deduce that $X_q = X_q^F = \bigcup_{(s,Y)\in\mathcal{C}_T} X_q^{F_{s,Y}}$. From covering lemma 9.9, we get $\mathrm{saff}(X_q) = a_G(q) + V_G(T)$. □

Remark that by definition of $\mathrm{bound}_V(X)$, there exists a unique semi-V-pattern $P \in \mathcal{P}_V(X)$ such that $[C_{V,\#}]^V \subseteq^V \mathcal{C}_{V,P}(X)$ for any sequence $\# \in \{<,>\}^{\mathrm{bound}_V(X)}$ such that $[C_{V,\#}]_V \neq [\emptyset]_V$. Let X be a Presburger-definable set, let V be an affine component of $\overrightarrow{\mathrm{saff}}(X)$, and let $P \in \mathcal{P}_V(X)$ be a semi-V-pattern. We denote by $\mathcal{S}_{V,P}(X)$ the set of sequences $\# \in \{<,>\}^{\mathrm{bound}_V(X)}$ such that $[C_{V,\#}]^V \subseteq^V \mathcal{C}_{V,P}(X)$.

The following theorem provides a geometrical form of the set X_q when q is a state in a terminal component of a FDVA that represents a Presburger-definable set X.

Theorem 13.17. *Let X be a Presburger-definable set represented by a FDVA $\mathcal{A}$ and let V be an affine component of $\overrightarrow{\mathrm{saff}}(X)$. For any state q in a terminal component T such that $V_G(T)$ is equal to V, there exists a vector $a_q \in \mathbb{Q}^m$ such that we have:*

$$X_q = \bigcup_{P\in\mathcal{P}_V(X)} \bigcup_{\#\in\mathcal{S}_{V,P}(X)} (P_q \cap (a_q + C_{V,\#} + V^\perp))$$

such that for any $j \in \{1, \ldots, m\}$, we have $-1 < a_q[j] \leq 0$ if $V \subseteq \boldsymbol{e}_{j,m}^\perp$ and we have $-1 < a_q[j] < 0$ otherwise.

Proof. Let us first prove that there exists a loop $q \xrightarrow{w_j} q$ such that $w_j \notin (\Sigma_{r,m} \cap \mathbf{e}_{j,m}^\perp)^*$ for any $j \in \{1, \ldots, m\}$ satisfying $V \not\subseteq \mathbf{e}_{j,m}^\perp$. As $\overrightarrow{\mathrm{saff}}(X_q) = V$, from proposition 14.11 we deduce that there exists $P \in \mathcal{P}_V(X)$ such that $P_q \neq \emptyset$. Let us consider a vector $x \in P_q$. As $V \not\subseteq \mathbf{e}_{j,m}^\perp$, there exists a vector $v \in V$ such that $v[j] \neq 0$ and by replacing v by a vector in $(\mathbb{Z}\backslash\{0\}).v$, we have proved that there exists a vector $v \in \mathrm{inv}_V(P_q)$ such that $v[j] > 0$. In particular $x + \mathbb{Z}.v \subseteq P_q$. As $v[j] > 0$, there exists $k \in \mathbb{N}$ enough larger such that $(x+k.v)[j] > 0$. Let us consider a (r, m)-decomposition (σ, s) of $x+k.n.v$. Naturally, as $(x + k.n.v)[j] > 0$, we have $\sigma \notin (\Sigma_{r,m} \cap \mathbf{e}_{j,m}^\perp)^*$. Moreover, as $\rho_{r,m}(\sigma, s) \in P_q$, we get $P_{q'} \neq \emptyset$ where $q' = \delta(q, \sigma)$. Proposition 14.11 shows that $X_{q'} \neq \emptyset$. As T is terminal, we have proved that $q' \in T$. Hence, there

exists a path $q' \xrightarrow{\sigma'} q$. Remark that the loop $q \xrightarrow{w_j} q$ where $w_j = \sigma.\sigma'$ satisfies $w_j \notin (\Sigma_{r,m} \cap \mathbf{e}_{j,m}^{\perp})^*$.

Let us consider the sequence $(C_{V,P})_{P \in \mathcal{P}_V(X)}$ of V-polyhedrons defined by $C_{V,P} = \bigcup_{\# \in \mathcal{S}_{V,P}(X)} C_{V,\#}$. Remark that $\mathcal{C}_{V,P}(X) = [C_{V,P}]^V$ for any $P \in \mathcal{P}_V(X)$. Hence, the set $Z = X \Delta (\bigcup_{P \in \mathcal{P}_V(X)} \bigcup_{\# \in \mathcal{S}_{V,P}(X)} (P_q \cap (a_q + C_{V,\#} + V^{\perp})))$ is such that $[Z]^V = [\emptyset]^V$. Let us consider a path $q_0 \xrightarrow{\sigma} q$ with q in a terminal component T such that $V_G(T) = V$. Thanks to the first paragraph, we can assume without loss of generality that $\sigma \notin (\Sigma_{r,m} \cap \mathbf{e}_{j,m}^{\perp})^*$ for any $j \in \{1, \ldots, m\}$ satisfying $V \not\subseteq \mathbf{e}_{j,m}^{\perp}$. As $\overrightarrow{\text{saff}}(X_q) = V$, and $[\gamma_{r,m,\sigma}^{-1}(Z)]^V = \gamma_{r,m,\sigma}^{-1}([\emptyset]^V) = [\emptyset]^V$, we deduce that X_q is not included in $\text{saff}(\gamma_{r,m,\sigma}^{-1}(Z))$. Hence, there exists a (r,m)-decomposition $(w_1, s) \in \rho_{r,m}^{-1}(X_q)$ such that $\rho_{r,m}(w_1, s) \notin \text{saff}(\gamma_{r,m,\sigma}^{-1}(Z))$. Destruction lemma 13.14 shows that by replacing w_1 by a word in $w_1.s^*$, we can assume that $\gamma_{r,m,\sigma.w_1}^{-1}(Z) = \emptyset$. Let $q' = \delta(q, w_1)$. As $s \in F_0(q')$ and T is terminal, we deduce that $q' \in T$. As q and q' are in the strongly connected component T, there exists a path $q' \xrightarrow{w_2} q$. Let $w = w_1.w_2$ and let $a_q = \Gamma_{r,m,\sigma.w}^{-1}(\mathbf{e}_{0,m})$. As $\sigma \notin (\Sigma_{r,m} \cap \mathbf{e}_{j,m}^{\perp})^*$ for any $j \in \{1, \ldots, m\}$ satisfying $V \not\subseteq \mathbf{e}_{j,m}^{\perp}$, we deduce that for any $j \in \{1, \ldots, m\}$, we have $-1 < a_q[j] \leq 0$ if $V \subseteq \mathbf{e}_{j,m}^{\perp}$ and we have $-1 < a_q[j] < 0$ otherwise. Remark that for any V-hyperplane H such that $\overrightarrow{H} = H$ and for any $\# \in \{<, \leq, =, \geq, >\}$, we have $\Gamma_{r,m,\sigma.w}^{-1}(H^{\#} + V^{\perp}) = a_q + H^{\#} + V^{\perp}$. As $\gamma_{r,m,\sigma.w}^{-1}(Z) = \emptyset$ then $X_q = \bigcup_{P \in \mathcal{P}_V(X)} \bigcup_{\# \in \mathcal{S}_{V,P}(X)} (P_q \cap (a_q + C_{V,\#} + V^{\perp}))$. □

14

Extracting Geometrical Properties

14.1 Semi-affine hull direction of a Presburger-definable FDVA

In this section we prove that the semi-affine hull direction $\overrightarrow{\text{saff}}(X)$ of a Presburger-definable set X represented by a FDVA is computable in polynomial time.

This computation cannot be extended to $\text{saff}(X)$. In fact, as shown by the following lemma 14.1, the size of $\text{saff}(X)$ can be exponentially larger than the size of a FDVA representing X.

Lemma 14.1. *There exist $\alpha, \beta \in \mathbb{Q}_+ \backslash \{0\}$, a sequence $(\mathcal{A}_n)_{n\in\mathbb{N}}$ of FDVA that represents a sequence $(X_n)_{n\in\mathbb{N}}$ of Presburger-definable sets in basis r, such that $\lim_{n\to+\infty} \text{size}(\mathcal{A}_n) = +\infty$ and $\text{size}(\text{saff}(X_n)) \geq \alpha.2^{\beta.\text{size}(\mathcal{A}_n)}$.*

Proof. Consider the finite set $X_n = \{0, \ldots, r^n - 1\}^m$. Remark that X_n is Presburger-definable and the FDVA $\mathcal{A}_{r,1}(X_n)$ that represents X_n has $n + 2$ principal states. Moreover, as $\text{comp}(\text{saff}(X_n)) = \{\{x\};\ x \in X_n\}$, we deduce that $\text{size}(\text{saff}(X_n)) = r^n$. □

Remark 14.2. The semi-affine hull of a set X represented by a FDVA (X is not necessarily Presburger-definable) can be computed in exponential time thanks to the algorithm provided in [Ler03]. This result is not used in this paper.

Our computation of $\overrightarrow{\text{saff}}(X)$ is based on the following lemma 14.3 that shows that an under-approximation of $\overrightarrow{\text{saff}}(X)$ can be easily computed from a FDVA that represents a set X. In this section, we prove that this under-approximation is exact if X is Presburger-definable.

Lemma 14.3. *Let X be a set represented by a FDVA. We have $\bigcup_{T\in\mathcal{T}_\mathcal{A}} V_G(T) \subseteq \overrightarrow{\text{saff}}(X)$.*

Proof. Let us consider a FDVA $\mathcal{A}$ that represents a set X. Let us consider a terminal component $T \in \mathcal{T}_{\mathcal{A}}$ and let us prove that $V_G(T) \subseteq \overrightarrow{\text{saff}}(X)$. Let us consider $q \in T$. As T is reachable (for $[G]$) from the initial state, there exists a path $q_0 \xrightarrow{\sigma \in \Sigma^*_{r,m}} q$. We have $X_q = \gamma^{-1}_{r,m,\sigma}(X) \subseteq \Gamma^{-1}_{r,m,\sigma}(X)$. Covering lemma 9.9 shows that $\overrightarrow{\text{saff}}(X_q) \subseteq \overrightarrow{\text{saff}}(X)$. Moreover, as $q \in T$, proposition 13.16 shows that $\overrightarrow{\text{saff}}(X_q) = V_G(T)$. Therefore $V_G(T) \subseteq \overrightarrow{\text{saff}}(X)$ and we have proved the inclusion $\bigcup_{T \in T_{\mathcal{A}}} V_G(T) \subseteq \overrightarrow{\text{saff}}(X)$. □

Proposition 14.4. *Let X be a Presburger-definable set represented by a FDVA $\mathcal{A}$ and let V be an affine component of $\overrightarrow{\text{saff}}(X)$. For any principal state q reachable for $[G]$, there exists $P \in \mathcal{P}_V(X)$ such that $P_q \neq \emptyset$ if and only if there exists a terminal component $T \in \mathcal{T}_{\mathcal{A}}$ reachable from q for $[G]$ such that $V_G(T) = V$.*

Proof. Assume first that there exists a terminal component $T \in \mathcal{T}_{\mathcal{A}}$ reachable from q for $[G]$ such that $V_G(T) = V$ and let us prove that there exists $P \in \mathcal{P}_V(X)$ such that $P_q \neq \emptyset$. There exists $q' \in T$ and a path $q \xrightarrow{\sigma \in \Sigma^*_{r,m}} q'$. From theorem 13.17, since $X_{q'} \neq \emptyset$, we deduce that there exists $P \in \mathcal{P}_V(X)$ such that $P_{q'} \neq \emptyset$. As $P_{q'} = \gamma^{-1}_{r,m,\sigma}(P_q)$ we get $P_q \neq \emptyset$ and we have proved that there exists $P \in \mathcal{P}_V(X)$ such that $P_q \neq \emptyset$. Let us prove the converse. Assume that there exists $P \in \mathcal{P}_V(X)$ such that $P_q \neq \emptyset$ and let us prove that there exists a terminal component $T \in \mathcal{T}_{\mathcal{A}}$ reachable from q for $[G]$ such that $V_G(T) = V$. Since q is reachable for $[G]$ from the initial state, there exists a path $q_0 \xrightarrow{\sigma_0} q$. Let us consider a sequence $(C_{V,P})_{P \in \mathcal{P}_V(X)}$ of V-polyhedrons such that $C_{V,P} \in \mathcal{C}_{V,P}(X)$. Let us consider $Z = X \Delta \bigcup_{P \in \mathcal{P}_V(X)} (P \cap (C_{V,P} + V^{\perp}))$. We have $[Z]^V = [\emptyset]^V$. That means V is not included in $\overrightarrow{\text{saff}}(Z)$. Let $Z' = \gamma^{-1}_{r,m,\sigma_0}(Z)$. From covering lemma 9.9, we deduce that V is not included in $\overrightarrow{\text{saff}}(Z')$. Observe that if there exists $P \in \mathcal{P}_V(X)$ such that $P_q \neq \textit{emptyset}$ then from $Z' = X_q \Delta \bigcup_{P \in \mathcal{P}_V(X)} (P_q \cap (C_{V,P} + V^{\perp}))$, we deduce that V is included in $\overrightarrow{\text{saff}}(X_q)$. Thus, there exists a (r,m)-decomposition (σ, s) such that $\rho_{r,m}(\sigma, s) \in X_q$ and $\rho_{r,m}(\sigma, s) \notin \text{saff}(Z')$. Destruction lemma 13.14 proves that by replacing σ by a word in $\sigma.s^*$, we can assume that $\gamma^{-1}_{r,m,\sigma}(Z') = \emptyset$. Let $q' = \delta(q, \sigma)$ and remark that $X_{q'} = \bigcup_{P \in \mathcal{P}_V(X)} (P_{q'} \cap (\Gamma^{-1}_{V,r,m,\sigma}(C_{V,P}) + V^{\perp}))$. As $\rho_{r,m}(\epsilon, s) \in X_q$ then $s \in F_0(q')$. So there exists a terminal component T reachable (for $[G]$) from q'. Let $q'' \in T$. There exists a path $q' \xrightarrow{w \in \Sigma^*_{r,m}} q''$ such that $q'' \in T$. We have $X_{q''} = \bigcup_{P \in \mathcal{P}_V(X)} (P_{q''} \cap (\Gamma^{-1}_{V,r,m,\sigma.w}(C_{V,P}) + V^{\perp}))$. As $X_{q''} \neq \emptyset$, there exists $P \in \mathcal{P}_V(X)$ such that $P_{q''} \neq \emptyset$. In particular $P_{q''}$ is a non-empty semi-V-pattern. As $C_{V,P}$ is non-V-degenerate and $[C_{V,P}]_V = [\Gamma^{-1}_{V,r,m,\sigma.w}(C_{V,P})]_V$, we deduce that $\Gamma^{-1}_{V,r,m,\sigma.w}(C_{V,P})$ is non-V-degenerate. Lemma 12.2 proves that V is included in $\overrightarrow{\text{saff}}(P_{q''} \cap (\Gamma^{-1}_{V,r,m,\sigma.w}(C_{V,P}) + V^{\perp}))$. Therefore $V \subseteq \overrightarrow{\text{saff}}(X_{q''})$.

Moreover, as $\overrightarrow{\text{saff}}(P_{q''}) \subseteq V$ for any $P \in \mathcal{P}_V(X)$, we deduce that $\overrightarrow{\text{saff}}(X_{q''}) = V$. As $q'' \in T$, recall that $V_G(T) = \overrightarrow{\text{saff}}(X_{q''})$. Therefore, we have proved that there exists a terminal component T such that $V_G(T) = V$. □

From the previous proposition 14.4, we deduce that $\overrightarrow{\text{saff}}(X)$ can be easily computed in polynomial time from the sequence of vector spaces associated to the terminal components.

Proposition 14.5. *For any Presburger-definable set X represented by a FDVA $\mathcal{A}$, we have:*

$$\overrightarrow{\text{saff}}(X) = \bigcup_{T \in \mathcal{T}_{\mathcal{A}}} V_G(T)$$

Proof. Lemma 14.3 shows that $\bigcup_{T \in \mathcal{T}_{\mathcal{A}}} V_G(T) \subseteq \overrightarrow{\text{saff}}(X)$. Now, let us prove the converse inclusion. Let V be an affine component of $\overrightarrow{\text{saff}}(X)$. Proposition 14.4 shows that there exists a terminal component T such that $V_G(T) = V$. Therefore $V \subseteq \bigcup_{T \in T_{\mathcal{A}}} V_G(T)$. We deduce the other inclusion $\overrightarrow{\text{saff}}(X) \subseteq \bigcup_{T \in T_{\mathcal{A}}} V_G(T)$. □

From theorem 13.4 and the previous proposition 14.5, we get one of the *main powerful theorem of this paper*.

Theorem 14.6. *The semi-affine hull direction of a Presburger-definable set represented by a FDVA is computable in polynomial time.*

14.1.1 An example

Let us consider the set $X = X_1 \cup X_2$ where $X_1 = \{x \in \mathbb{N}^2;\ x[1] = 2.x[2]\}$ and $X_2 = \{x \in \mathbb{N}^2;\ x[2] = 2.x[1]\}$. Naturally, the semi-vector space $\overrightarrow{\text{saff}}(X_1)$ is equal to the vector space $V_1 = \{x \in \mathbb{Q}^2;\ x[1] = 2.x[2]\}$ and symmetrically the semi-vector space $\overrightarrow{\text{saff}}(X_2)$ is equal to the vector space $V_2 = \{x \in \mathbb{Q}^2;\ x[2] = 2.x[1]\}$. As $\overrightarrow{\text{saff}}(X)$ has two affine components V_1 and V_2, from proposition 14.5, we deduce that whatever the FDVA $\mathcal{A}$ that represents X we consider, for any terminal terminal components T, we have $V_G(T) \subseteq V_1$ or $V_G(T) \subseteq V_2$ (remark that we have implicitly used the insecable lemma 9.2). Moreover, we also deduce that there exists at least one terminal component T_1 such that $V_G(T_1) = V_1$ and at least one terminal component T_2 such that $V_G(T_2) = V_2$.

This property can be verified in practice. Figure 14.1 represents the minimal FDVA $\mathcal{A}_{2,2}(X_1 \cup X_2)$ where $X_1' = \{x \in \mathbb{N};\ x[1] = 2.x[2] + 1\}$ and $X_2' = \{x \in \mathbb{N};\ x[2] = 2.x[1] + 1\}$. Remark that this FDVA has 2 terminal components T_1 and T_2 defined by $T_1 = \{X_1, X_1'\}$ and $T_2 = \{X_2, X_2'\}$. We have $V_G(T_1) = \overrightarrow{\text{aff}}(X_1) = \overrightarrow{\text{aff}}(X_1') = V_1$ and $V_G(T_2) = \overrightarrow{\text{aff}}(X_2) = \overrightarrow{\text{aff}}(X_2') = V_2$.

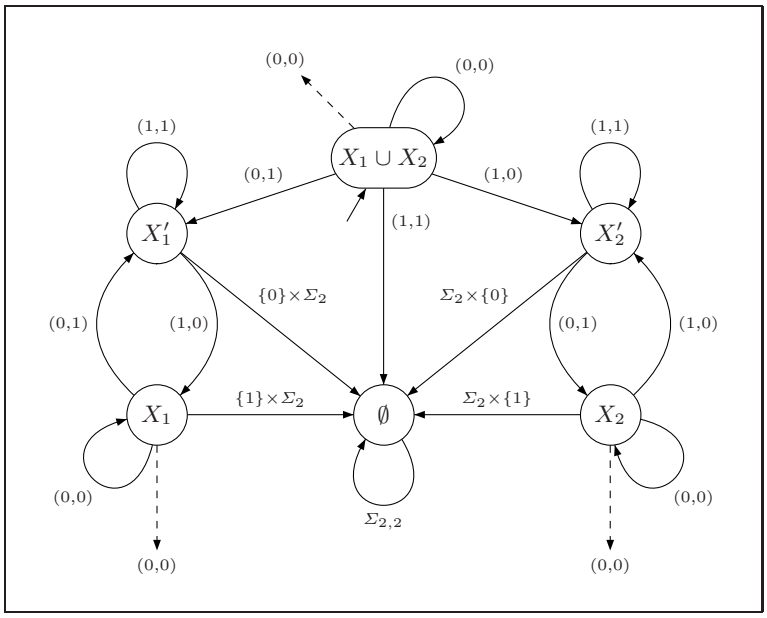

Fig. 14.1. The FDVA $\mathcal{A}_{2,2}(X_1 \cup X_2)$

14.2 Polynomial time invariant computation

Let X be a Presburger-definable set and V be an affine component of $\overrightarrow{\text{saff}}(X)$. The V-vector lattice $\text{inv}_V(X)$ of invariants of X is defined by the following equality:

$$\text{inv}_V(X) = \bigcap_{P \in \mathcal{P}_V(X)} \text{inv}_V(P)$$

In this section we prove that the V-vector lattice of invariants $\text{inv}_V(X)$ is computable in polynomial time from a *cyclic* FDVA $\mathcal{A}$ that represents X in basis r. We also prove that $|\mathbb{Z}^m \cap V/\text{inv}_V(X)|$ is bounded by the number of principal states of $\mathcal{A}$.

Recall that corollary 13.10 proves that any $P \in \mathcal{P}_V(X)$ is relatively prime with r and included in the V-affine space $\xi_{r,m}(s)+V$. This V-affine space will be useful in the sequel. Our algorithm is based on the following proposition 14.8 and the remaining of this section is devoted to prove that all structures needed for applying this proposition are small and they can be computed efficiently.

Lemma 14.7. *Let A be a V-affine space and $s \in S_{r,m}$ be a (r,m)-sign vector such that $[Z_{r,m,s} \cap A]^V \neq [\emptyset]^V$. There exists a vector $v \in V$ such that $v[i] < 0$ if $s[i] = r-1$ and $v[i] > 0$ if $s[i] = 0$ for any $i \in \{1,\ldots,m\}$ such that $\boldsymbol{e}_{i,m} \notin V^\perp$.*

Proof. Since A is a V-affine space, there exists $a \in A$. We denote by $\#_0$ the binary relation $\geq$ and by $\#_{r-1}$ the binary relation $<$, and we denote by I the set of $i \in \{1, \ldots, m\}$ such that $\mathbf{e}_{i,m} \notin V^\perp$. Remark that $Z_{r,m,s} \cap A = \mathbb{Z}^m \cap A \cap (C + \Pi_V(a) + V^\perp)$ where C is the V-polyhedron $C = \bigcap_{i=1}^m \{x \in V;\ x[i] + a[i]\#_{s[i]}0\}$. As $\{x \in V;\ x[i] + a[i]\#_{s[i]}0\} = \{x \in V;\ \langle \Pi_V(\mathbf{e}_{i,m}), x\rangle + a[i]\#_{s[i]}0\}$, we deduce that $\{x \in V;\ x[i] + a[i]\#_{s[i]}0\}$ is either empty or equal to V for any $i \in \{1, \ldots, m\}\backslash I$. Moreover, as $[Z_{r,m,s} \cap A]^V \neq [\emptyset]^V$, we get $\{x \in V;\ x[i] + a[i]\#_{s[i]}0\} = V$ for any $i \in \{1, \ldots, m\}\backslash I$. Hence $C = \bigcap_{i \in I} \{x \in V;\ \langle \Pi_V(\mathbf{e}_{i,m}), x\rangle + a[i]\#_{s[i]}0\}$. As $[\mathbb{Z}^m \cap A \cap (C + \Pi_V(a) + V^\perp)]^v \neq [\emptyset]^V$, lemma 12.2 shows that $[C]^V \neq [\emptyset]^V$. From lemma 11.6 we deduce that there exists a vector $v \in V$ such that $v[i] > 0$ if $s[i] = 0$ and $v[i] < 0$ if $s[i] = r - 1$ for any $i \in I$. □

Proposition 14.8. *Let X be a (r, m, w)-cyclic Presburger-definable set and let V be an affine component of $\overrightarrow{\text{saff}}(X)$. Assume that we have:*

- *A (r, m)-sign vector $s \in S_{r,m}$ such that $[Z_{r,m,s} \cap (\xi_{r,m}(s) + V)]^V \neq [\emptyset]^V$,*
- *A couple (q_0, G) such that q_0 is a principal state of a FDVG G such that $\delta(q_0, \sigma_1) = \delta(q_0, \sigma_2)$ if and only if $(\gamma^{-1}_{r,m,\sigma_1}(P))_{P \in \mathcal{P}_V(X)} = (\gamma^{-1}_{r,m,\sigma_2}(P))_{P \in \mathcal{P}_V(X)}$ for any $\sigma_1, \sigma_2 \in \Sigma^*_{r,m}$,*
- *The set Q' of principal states reachable for $[G]$ from q_0 such that $(\emptyset)_{P \in \mathcal{P}_V(X)} \neq (\gamma^{-1}_{r,m,\sigma}(P))_{P \in \mathcal{P}_V(X)}$ if and only if $q' \in Q'$ for any path $q_0 \xrightarrow{\sigma} q'$ with $\sigma \in \Sigma^*_{r,m}$,*
- *An integer $n_0 \in \mathbb{N}\backslash\{0\}$ relatively prime with r such that $|\mathbb{Z}^m \cap V/inv_V(X)|$ divides n_0,*
- *An integer $n \in \mathbb{N}\backslash\{0\}$ such that $r^n \in 1 + n_0.\mathbb{Z}$.*

We denote by U the set of pairs $u = (k, Z) \in K \times \mathbb{Z}/mn.\mathbb{Z}$ such that there exists a pair of words (σ_u, σ'_u) in Σ^*_r satisfying $|\sigma_u.\sigma'_u| \in m.n.\mathbb{Z}$, $(k, Z) = (\delta(q_0, \sigma_u), |\sigma_u| + m.n.\mathbb{Z})$ and there exists an s-eye Y' such that $\delta(k, \sigma'_u) \in \ker_s(Y') \subseteq Q'$. Given a sequence $(\sigma_u, \sigma'_u)_{u \in U}$ satisfying the previous conditions and such that $\sigma_{(q_0, m.n.\mathbb{Z})} = \epsilon$, the vector lattice of invariants $inv_V(X)$ is equal to the vector lattice generated by $n_0.\mathbb{Z}^m \cap V$ and the vectors $\rho_{r,m}(\sigma_{u_1}.b.\sigma'_{u_2}, s) - \rho_{r,m}(\sigma_{u_2}.\sigma'_{u_2}, s)$ where $u_1 = (k_1, Z_1) \in U$, $b \in \Sigma_r$ and $u_2 = (k_2, Z_2) \in U$ are such that $(k_2, Z_2) = (\delta(k_1, b), Z_1 + 1)$.

Proof. Let us denote by A the V-affine space $A = \xi_{r,m}(w) + V$.

Since $\delta(q_0, \sigma_1) = \delta(q_0, \sigma_2)$ if and only if $(\gamma^{-1}_{r,m,\sigma_1}(P))_{P \in \mathcal{P}_V(X)} = (\gamma^{-1}_{r,m,\sigma_2}(P))_{P \in \mathcal{P}_V(X)}$ for any $\sigma_1, \sigma_2 \in \Sigma^*_{r,m}$, for any principal state q reachable for $[G]$ from q_0, there exists a unique sequence denoted by $(P_q)_{P \in \mathcal{P}_V(X)}$ such that $P_q = \gamma^{-1}_{r,m,\sigma}(P)$ for any $P \in \mathcal{P}_V(X)$ and for any $\sigma \in \Sigma^*_{r,m}$ such that $q = \delta(q_0, \sigma)$.

We first prove that $\rho_{r,m}(\sigma', s) \in A$ for any word $\sigma' \in \Sigma^*_{r,m}$ such that there exists an s-eye Y' satisfying $\delta(q_0, \sigma') \in \ker_s(Y') \subseteq Q'$. As the principal state $q' = \delta(q_0, \sigma')$ is in Q', there exists $P \in \mathcal{P}_V(X)$ such that $P_{q'} \neq \emptyset$. As there exists a path $q' \xrightarrow{s^+} q'$ since $q' \in \ker_s(Y')$, we get $\text{saff}(P_{q'}) = \xi_{r,m}(s) + V$ from lemma 9.20. Remark that $P_{q'} = \gamma^{-1}_{r,m,\sigma'}(P)$. Thus, from covering lemma

9.9, we get $\xi_{r,m}(s)+V \subseteq \Gamma_{r,m,\sigma'}(\mathrm{saff}(P))$ in particular from $\mathrm{saff}(P)=A$ and $\rho_{r,m}(\sigma,s)=\Gamma_{r,m,\sigma}(\xi_{r,m}(s))$, we deduce that $\rho_{r,m}(\sigma',s)\in A$.

Next, let us show that for any pair of integers $z_1,z_2\in\mathbb{N}$ such that $z_1+m.n.\mathbb{Z}=z_2+m.n.\mathbb{Z}$ and for any $x\in\mathbb{Z}^m$, we have $x'=\gamma^{z_2}_{r,m,0}(x)-\gamma^{z_1}_{r,m,0}(x)\in n_0.\mathbb{Z}^m$. Naturally, by symmetry, we can assume that $z_1<z_2$ and by replacing x by $\gamma^{z_1}_{r,m,0}(x)$ and (z_1,z_2) by $(0,z_2-z_1)$ we can assume that $z_1=0$. In this case $z=\frac{z_2}{m.n}$ is in $\mathbb{N}$ and $x'=(r^{n.z}-1).x$. Since r^n-1 divides $r^{n.z}-1$ and n_0 divides r^n-1, we have prove that $x'\in n_0.\mathbb{Z}^m$.

Let us denote by M the vector lattice generated by $n_0.\mathbb{Z}^m\cap V$ and the vectors $\rho_{r,m}(\sigma_{u_1}.b.\sigma'_{u_2},s)-\rho_{r,m}(\sigma_{u_2}.\sigma'_{u_2},s)$ where $u_1=(k_1,Z_1)\in U$, $b\in\Sigma_r$ and $u_2=(k_2,Z_2)\in U$ are such that $(k_2,Z_2)=(\delta(k_1,b),Z_1+1)$.

We first prove the inclusion $M\subseteq \mathrm{inv}_V(X)$.

Let us show that $\rho_{r,m}(\sigma_2,s)-\rho_{r,m}(\sigma_1,s)\in\mathrm{inv}_V(X)$ for any pair of words (σ_1,σ_2) in $(\Sigma^n_{r,m})^*$ such that there exists a principal state q' satisfying $\delta(q_0,\sigma_1)=q'=\delta(q_0,\sigma_2)$ and there exists an s-eye Y' satisfying $q'\in\ker_s(Y')\subseteq Q'$. The previous paragraphs shows that $\rho_{r,m}(\sigma_1,s)$ and $\rho_{r,m}(\sigma_2,s)$ are both in A. Thus, from lemma 9.22 we get $\gamma^{-1}_{r,m,\sigma_i}(P)=\xi_{r,m}(s)+P-\rho_{r,m}(\sigma_i,s)$ for any $i\in\{1,2\}$ and for any $P\in\mathcal{P}_V(X)$. In particular $\rho_{r,m}(\sigma_2,s)-\rho_{r,m}(\sigma_1,s)\in\mathrm{inv}_V(X)$.

We can now easily prove that $M\subseteq\mathrm{inv}_V(X)$ since $n_0.\mathbb{Z}^m\cap V\subseteq\mathrm{inv}_V(X)$ (recall that $|\mathbb{Z}^m\cap V/\mathrm{inv}_V(X)|$ divides n_0) and from the previous paragraph we deduce that $\rho_{r,m}(\sigma_{u_1}.b.\sigma'_{u_2},s)-\rho_{r,m}(\sigma_{u_2}.\sigma'_{u_2},s)\in\mathrm{inv}_V(X)$ for any $u_1=(k_1,Z_1)\in U$, $b\in\Sigma_r$ and $u_2=(k_2,Z_2)\in U$ such that $(k_2,Z_2)=(\delta(k_1,b),Z_1+1)$.

Next, let us prove the converse inclusion $\mathrm{inv}_V(X)\subseteq M$.

Let us show that $\rho_{r,m}(\sigma_2.\sigma',s)-\rho_{r,m}(\sigma_1.\sigma',s)\in\rho_{r,m}(\sigma_2.\sigma'',s)-\rho_{r,m}(\sigma_1.\sigma'',s)+M$ for any pair of words (σ_1,σ_2) in Σ_r^* such that there exists $u=(k,Z)\in U$ satisfying $(\delta(q_0,\sigma_1),|\sigma_1|+m.n.\mathbb{Z})=u=(\delta(q_0,\sigma_2),|\sigma_2|+m.n.\mathbb{Z})$ and for any pair of words (σ',σ'') in Σ_r^* satisfying $Z+|\sigma'|=m.n.\mathbb{Z}=Z+|\sigma''|+m.n.\mathbb{Z}$ and there exists two s-eyes Y' and Y'' satisfying $\delta(k,\sigma')\in\ker_s(Y')\subseteq Q'$ and $\delta(k,\sigma'')\in\ker_s(Y'')\subseteq Q'$. Let $x'=(\rho_{r,m}(\sigma_2.\sigma',s)-\rho_{r,m}(\sigma_1.\sigma',s))-(\rho_{r,m}(\sigma_2.\sigma'',s)-\rho_{r,m}(\sigma_1.\sigma'',s))$. This vector is in V since the vectors $\rho_{r,m}(\sigma_1.\sigma',s)$, $\rho_{r,m}(\sigma_2.\sigma',s)$, $\rho_{r,m}(\sigma_1.\sigma'',s)$, and $\rho_{r,m}(\sigma_2.\sigma'',s)$ are in the V-affine space A from the previous paragraphs. Moreover, let us remark that $x'=\gamma^{z_2}_{r,m,0}(x)-\gamma^{z_1}_{r,m,0}(x)$ where $z_1=|\sigma_1|$, $z_2=|\sigma_2|$ and $x=\rho_{r,m}(\sigma',s)-\rho_{r,m}(\sigma'',s)$. Thus, from the previous paragraphs, we get $x\in n_0.\mathbb{Z}^m$ and we have proved that $x'\in n_0.\mathbb{Z}^m\cap V\subseteq M$.

Let us show that $\rho_{r,m}(\sigma_2,s)-\rho_{r,m}(\sigma_1,s)\in M$ for any pair of words (σ_1,σ_2) in $(\Sigma^n_{r,m})^*$ such that there a principal state q' satisfying $\delta(q_0,\sigma_1)=q'=\delta(q_0,\sigma_2)$ and there exists an s-eyes Y' satisfying $q'\in\ker_s(Y')\subseteq Q'$. Since M is a vector lattice, it is sufficient to prove that $\rho_{r,m}(\sigma,s)-\rho_{r,m}(\sigma_u,s)\in M$ for any word $\sigma\in(\Sigma^n_{r,m})^*$ such that $u=(\delta(q_0,\sigma),m.n.\mathbb{Z})$ is in U. Let us consider a sequence b_1, ..., b_i of r-digits $b_j\in\Sigma_r$ such that $\sigma=b_1\dots b_i$. We denote by u_i the couple $u_i=(\delta(q_0,b_1\dots b_j),j+m.n.\mathbb{Z})$. Since $u_i=u$ is in U, we deduce that $u_j\in U$ for any $k\in\{0,\dots,i\}$. By definition of M, we have

$\rho_{r,m}(\sigma_{u_{j-1}}.b_j.\sigma'_{u_j}, s) - \rho_{r,m}(\sigma_{u_j}.\sigma'_{u_{j+1}}, s) \in M$ for any $j \in \{1, \dots, i\}$. From the previous paragraph, we get $\rho_{r,m}(\sigma_{u_{j-1}}.b_j \dots b_i, s) - \rho_{r,m}(\sigma_{u_j}.b_{j+1} \dots b_i, s) \in M$ for any $j \in \{1, \dots, i\}$. By summing all the vectors, we deduce that $\rho_{r,m}(\sigma_{u_0}.b_1 \dots b_i) - \rho_{r,m}(\sigma_{u_i}) \in M$. Now, just remark that $\sigma_{u_0} = \epsilon$ and $u_i = u$.

Let us consider $v \in \mathrm{inv}_V(X)$ and let us prove that $v \in M$. Lemma 14.7 shows that there exists a vector $v_0 \in V$ such that $v_0[i] < 0$ if $s[i] = r-1$ and $v_0[i] > 0$ if $s[i] = 0$ for any $i \in \{1, \dots, m\}$ such that $\mathbf{e}_{i,m} \notin V^\perp$. By replacing v_0 by a vector in $(\mathbb{N}\backslash\{0\}).v_0$, we can assume that $v_0 \in \mathrm{inv}_V(X)$, $v_0[i] + v[i] < 0$ if $s[i] = r-1$ and $v_0[i] + v[i] > 0$ if $s[i] = 0$ for any $i \in \{1, \dots, m\}$ such that $\mathbf{e}_{i,m} \notin V^\perp$. Since $[Z_{r,m,s} \cap A]^V \neq [\emptyset]^V$, there exists a vector $a \in Z_{r,m,s} \cap A$. Let $a_1 = a + v_0$ and let $a_2 = a + v_0 + v$. Remark that $a_1, a_2 \in Z_{r,m,s}$ since for any $i \in \{1, \dots, m\}$, if $\mathbf{e}_i \notin V^\perp$ then $a_1[i] = a[i] + v_0[i]$, $a_2[i] = a[i] + v_0[i] + v[i]$ and if $\mathbf{e}_i \in V^\perp$ then $a_1[i] = a[i]$, $a_2[i] = a[i]$. As $a_1, a_2 \in Z_{r,m,s}$, there exist $\sigma_1, \sigma_2 \in \Sigma^*_{r,m}$ such that $a_1 = \rho_{r,m}(\sigma_1, s)$ and $a_2 = \rho_{r,m}(\sigma_2, s)$. By replacing σ_1 by a word in $\sigma_1.s^*$ and σ_2 by a word in $\sigma_2.s^*$ we can also assume that $|\sigma_1|$ and $|\sigma_2|$ are in $m.n.\mathbb{Z}$. Let $P \in \mathcal{P}_V(X)$. Since $\rho_{r,m}(\sigma_i, s) \in A$ and $r^{|\sigma_i|_m} \in 1 + |\mathbb{Z}^m \cap V/\mathrm{inv}_V(P)|.\mathbb{Z}$, lemma 9.22 proves that $\gamma^{-1}_{r,m,\sigma_i}(P) = \xi_{r,m}(s) + P - \rho_{r,m}(\sigma_i, s)$ for any $i \in \{1, 2\}$. As $\rho_{r,m}(\sigma_2, s) - \rho_{r,m}(\sigma_1, s) = v_0 \in \mathrm{inv}_V(X)$, we deduce that $\gamma^{-1}_{r,m,\sigma_1}(P) = \gamma^{-1}_{r,m,\sigma_2}(P)$ for any $P \in \mathcal{P}_V(X)$. Therefore there exists a state $q' \in Q'$ such that $\delta(q_0, \sigma_1) = q' = \delta(q_0, \sigma_2)$. Let us consider the s-eye Y' that contains q'. Since $\gamma^{-1}_{r,m,\sigma_1.s^n}(P) = \xi_{r,m}(s) + P - \rho_{r,m}(\sigma_i.s^n, s)$ from lemma 9.22, we deduce that $(\gamma^{-1}_{r,m,\sigma_1.s^n}(P))_{P \in \mathcal{P}_V(X)} = (\gamma^{-1}_{r,m,\sigma_1}(P))_{P \in \mathcal{P}_V(X)}$. We have proved that $\delta(q', s^n) = q'$ and in particular $q' \in \ker_s(Y')$. By considering $P \in \mathcal{P}_V(X)\backslash\{\emptyset\}$ let us remark that $\gamma^{-1}_{r,m,\sigma_1}(P) = \xi_{r,m}(s) + P - \rho_{r,m}(\sigma_i, s)$ is not empty. That means $q' \in Q'$. Moreover, as for any $q'' \in \ker_s(Y')$ there exists a path $q'' \xrightarrow{s^*} q'$ and $P_{q'} \neq \emptyset$ we get $P_{q''} \neq \emptyset$. Thus $\ker_s(Y') \subseteq Q'$. From the previous paragraph, we get $\rho_{r,m}(\sigma_2, s) - \rho_{r,m}(\sigma_1, s) \in M$. Now, just remark that $\rho_{r,m}(\sigma_2, s) - \rho_{r,m}(\sigma_1, s) = v$ and we have proved that $v \in M$. □

The following proposition 14.9 provides a simple algorithm for computing in polynomial time a (r, m)-sign vector $s \in S_{r,m}$ such that $[Z_{r,m,s} \cap (\xi_{r,m}(w) + V)]^V \neq [\emptyset]^V$ from a FDVA that represents a (r, m, w)-cyclic Presburger definable set X in basis r.

Proposition 14.9. *Let $X \subseteq \mathbb{Z}^m$ be a (r, m, w)-cyclic Presburger-definable set represented by a FDVA $\mathcal{A}$ in basis r, and let V be an affine component of $\overrightarrow{\mathrm{saff}}(X)$. We have $[Z_{r,m,s} \cap (\xi_{r,m}(w) + V)]^V \neq [\emptyset]^V$ for any (r, m)-sign vector $s \in S_{r,m}$ such that $s \in [F_0](q)$ where q is a principal state in a terminal component T such that $V_G(T) = V$.*

Proof. Let us consider a terminal component T of $\mathcal{A}$, a principal state $q \in T$ and a (r, m)-sign vector $s \in [F_0](q)$. Let Y be the s-eye that contains q. As T is terminal we deduce that $\ker_s(Y) \subseteq T$. From proposition 13.15, we deduce that $\mathrm{saff}(X_q^{F_{s,Y}}) = a_q(G) + V_G(T)$. From $X_q^{F_{s,Y}} \subseteq Z_{r,m,s} \cap X_q$, we deduce that $V \subseteq \overrightarrow{\mathrm{saff}}(Z_{r,m,s} \cap X_q)$. As q is reachable, there exists a path

$q_0 \xrightarrow{w} q$ and we get $X_q = \gamma^{-1}_{r,m,w}(X)$. As $\gamma^{-1}_{r,m,w}(Z_{r,m,s} \cap X) = Z_{r,m,s} \cap X_q$, we have proved that $V \subseteq \overrightarrow{\text{saff}}(Z_{r,m,s} \cap X)$ thanks to the covering lemma 9.9. Let A be an affine component of $\text{saff}(Z_{r,m,s} \cap X)$ such that $V \subseteq \overrightarrow{A}$. From $V \subseteq \overrightarrow{A} \subseteq \overrightarrow{\text{saff}}(X)$ and as V is an affine component of $\overrightarrow{\text{saff}}(X)$, we deduce that $V = \overrightarrow{A}$. Moreover, as $Z_{r,m,s} \cap X$ is (r, m, w)-cyclic we deduce that $\xi_{r,m}(w) \in A$. Hence $A = \xi_{r,m}(w) + V$. From the dense component lemma 12.1, we get $\text{saff}(Z_{r,m,s} \cap X \cap A) = A$. In particular $A \subseteq \text{saff}(Z_{r,m,s} \cap A)$ and we have proved that $[Z_{r,m,s} \cap (\xi_{r,m}(w) + V)]^V \neq [\emptyset]^V$. □

A couple (q_0, G) and a set Q' satisfying proposition 14.8 is obtained by a quotient of a FDVA $\mathcal{A}$ that represents X in basis r by the equivalence relation $\sim^V$ defined over the principal states of $\mathcal{A}$ by $q_1 \sim^V q_2$ if and only if $X_{q_1} \sim^V X_{q_2}]^V$. Remark that $\sim^V$ is a polynomial time equivalence relation since $q_1 \sim^V q_2$ if and only V is not included in $\overrightarrow{\text{saff}}(X_{q_1} \Delta X_{q_2})$, and this last condition can be decided in polynomial because a FDVA that represents the Presburger-definable set $X_{q_1} \Delta X_{q_2}$ is computable in quadratic time and the semi-affine hull direction of this set is computable in polynomial time thanks to theorem 14.6. The following propositions 14.10 and 14.11 provides immediately the following corollary 14.12.

Proposition 14.10. *Let X be a Presburger-definable set and let V be an affine component of $\overrightarrow{\text{saff}}(X)$. Given a pair (σ_1, σ_2) of words in $\Sigma^*_{r,m}$, we have the equality $(\gamma^{-1}_{r,m,\sigma_1}(P))_{P \in \mathcal{P}_V(X)} = (\gamma^{-1}_{r,m,\sigma_2}(P))_{P \in \mathcal{P}_V(X)}$ if and only if $\gamma^{-1}_{r,m,\sigma_1}(X) \sim^V \gamma^{-1}_{r,m,\sigma_2}(X)$.*

Proof. Consider a pair (σ_1, σ_2) of words in $\Sigma^*_{r,m}$. From lemma 13.8 we deduce that $[\gamma^{-1}_{r,m,\sigma_i}(X)]^V = \bigcup^V_{P \in \mathcal{P}_V(X)} ([\gamma^{-1}_{r,m,\sigma_i}(P)]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp))$ for any $i \in \{1, 2\}$. As $(\mathcal{C}_{V,P}(X))_{P \in \mathcal{P}_V(X)}$ is a polyhedral V-partition, we get $[\gamma^{-1}_{r,m,\sigma_1}(X) \Delta \gamma^{-1}_{r,m,\sigma_2}(X)]^V = \bigcup^V_{P \in \mathcal{P}_V(X)} ([\gamma^{-1}_{r,m,\sigma_1}(P) \Delta \gamma^{-1}_{r,m,\sigma_2}(P)]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp))$. Remark that if $(\gamma^{-1}_{r,m,\sigma_1}(P))_{P \in \mathcal{P}_V(X)} = (\gamma^{-1}_{r,m,\sigma_2}(P))_{P \in \mathcal{P}_V(X)}$ then we have $[\gamma^{-1}_{r,m,\sigma_1}(X) \Delta \gamma^{-1}_{r,m,\sigma_2}(P)]^V = [\emptyset]^V$ and conversely if $[\gamma^{-1}_{r,m,\sigma_1}(X) \Delta \gamma^{-1}_{r,m,\sigma_2}(X)]^V = [\emptyset]^V$, by intersecting the following equality by $\mathcal{C}_{V,P}(X) + V^\perp$, we get $[\emptyset]^V = [\gamma^{-1}_{r,m,\sigma_1}(P) \Delta \gamma^{-1}_{r,m,\sigma_2}(P)]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp)$:

$$[\gamma^{-1}_{r,m,\sigma_1}(X) \Delta \gamma^{-1}_{r,m,\sigma_2}(X)]^V = \bigcup_{P \in \mathcal{P}_V(X)}^V ([\gamma^{-1}_{r,m,\sigma_1}(P) \Delta \Gamma^{-1}_{r,m,\sigma_2}(P)]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp))$$

From lemma 12.2 we get $\gamma^{-1}_{r,m,\sigma_1}(P) \Delta \gamma^{-1}_{r,m,\sigma_2}(P) = \emptyset$. □

Proposition 14.11. *Let X be a Presburger-definable set and V be an affine component of $\overrightarrow{\text{saff}}(X)$. Given a word $\sigma \in \Sigma^*_{r,m}$, we have $(\gamma^{-1}_{r,m,\sigma}(P))_{P \in \mathcal{P}_V(X)} = (\emptyset)_{P \in \mathcal{P}_V(X)}$ if and only if $\gamma^{-1}_{r,m,\sigma}(X) \sim^V \emptyset$.*

Proof. From lemma 13.8 we deduce that $[\gamma^{-1}_{r,m,\sigma}(X)]^V = \bigcup^V_{P\in\mathcal{P}_V(X)}([\gamma^{-1}_{r,m,\sigma}(P)]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp))$. Remark that if $(\gamma^{-1}_{r,m,\sigma}(P))_{P\in\mathcal{P}_V(X)} = (\emptyset)_{P\in\mathcal{P}_V(X)}$ then $[\gamma^{-1}_{r,m,\sigma}(X)]^V = [\emptyset]^V$ and conversely if $[\gamma^{-1}_{r,m,\sigma}(X)]^V = [\emptyset]^V$, by intersecting the equality $[\gamma^{-1}_{r,m,\sigma}(X)]^V = \bigcup^V_{P\in\mathcal{P}_V(X)}([\gamma^{-1}_{r,m,\sigma}(P)]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp))$ by $\mathcal{C}_{V,P}(X) + V^\perp$, we get $[\emptyset]^V = [\gamma^{-1}_{r,m,\sigma}(P)]^V \cap^V (\mathcal{C}_{V,P}(X) + V^\perp)$. From lemma 12.2 we get $\gamma^{-1}_{r,m,\sigma}(P) = \emptyset$. □

Corollary 14.12. *Let X be a (r, m, w)-cyclic Presburger-definable set represented by a FDVA $\mathcal{A}$ in basis r, and let V be an affine component of $\overrightarrow{\text{saff}}(X)$. We can compute in polynomial time a couple (q_0, G) such that q_0 is a principal state of a FDVG G such that $\delta(q_0, \sigma_1) = \delta(q_0, \sigma_2)$ if and only if $(\gamma^{-1}_{r,m,\sigma_1}(P))_{P\in\mathcal{P}_V(X)} = (\gamma^{-1}_{r,m,\sigma_2}(P))_{P\in\mathcal{P}_V(X)}$ for any $\sigma_1, \sigma_2 \in \Sigma^*_{r,m}$, and we can compute in polynomial time the set Q' of principal states reachable for $[G]$ from q_0 such that $(\gamma^{-1}_{r,m,\sigma}(P))_{P\in\mathcal{P}_V(X)} \neq (\emptyset)_{P\in\mathcal{P}_V(X)}$ if and only if $q' \in Q'$ for any path $q_0 \xrightarrow{\sigma} q'$ with $\sigma \in \Sigma^*_{r,m}$.*

Let us consider a (r, m, w)-cyclic Presburger definable set X represented by a FDVA $\mathcal{A}$ in basis r. The following proposition 14.13 provides an algorithm for computing in polynomial time an integer $n_1 \in \{1, \ldots, |\mathcal{A}|\}$ such that there exists $z_0 \in \mathbb{N}\backslash\{0\}$ satisfying $n_1 = z_0.|\mathbb{Z}^m \cap V/\text{inv}_V(X)|$. Naturally the integer n_1 is not necessary relatively prime with r. However, let us remark that $n_0 = h^\infty_r(n_1)$ is also computable in polynomial time (by an Euclid's algorithm) and it is also in $\{1, \ldots, n_1\} \subseteq \{1, \ldots, |\mathcal{A}|\}$. Moreover, as $\text{inv}_V(X)$ is relatively prime with r (recall that X is cyclic), we deduce that $|\mathbb{Z}^m \cap V/\text{inv}_V(X)|$ divides n_0. That means we have provided a polynomial time algorithm for computing an integer $n_0 \in \{1, \ldots, |\mathcal{A}|\}$ that satisfies proposition 14.8. Now let us remark that an integer $n \in \{1, \ldots, n_0\}$ satisfying proposition 14.8 can be easily computed in polynomial time. In fact, since n_0 is relatively prime with r, there exists an integer $n \in \{1, \ldots, n_0\}$ such that $r^n \in 1 + n_0.\mathbb{Z}$. By enumerating the integers in $\{1, \ldots, n_0\}$ we compute in polynomial an integer n satisfying proposition 14.8.

Proposition 14.13. *Let X be a cyclic Presburger-definable set and let V be an affine component of $\overrightarrow{\text{saff}}(X)$. There exists an integer $z_0 \in \mathbb{N}\backslash\{0\}$ such that for any (q_0, G) and Q' satisfying the same conditions as the one provided in proposition 14.8, and for any (r, m)-sign vector $s \in S_{r,m}$ satisfying $[Z_{r,m,s} \cap (\xi_{r,m}(w) + V)]^V \neq [\emptyset]^V$, we have the following equality:*

$$|\mathbb{Z}^m \cap V/inv_V(X)| = \frac{1}{z_0}\Big(\sum_{\substack{Y \text{ s-eye of } [G] \\ \ker_s(Y)\subseteq Q'}} |\ker_s(Y)|\Big)$$

Proof. Let us recall that A is the V-affine space $A = \xi_{r,m}(w) + V$. As $\bigcup_{P\in\mathcal{P}_V(X)} P$ is a non empty set included in $\mathbb{Z}^m \cap A$, there exists a vector

a_0 in $\mathbb{Z}^m \cap A$. As r and $|\mathbb{Z}^m \cap V/\mathrm{inv}_V(X)|$ are relatively prime, there exists an integer $z_1 \in \mathbb{N}\backslash\{0\}$ such that $r^{z_1} \in 1+|\mathbb{Z}^m \cap V/\mathrm{inv}_V(X)|.\mathbb{N}$. As $P-a_0$ is a relatively prime semi-V-pattern included in V and $\rho_{r,m}(\mathbf{e}_{0,m}^{z_1}, \mathbf{e}_{0,m}) = \mathbf{e}_{0,m} \in V$, lemma 9.22 proves that $\gamma_{r,m,\mathbf{e}_{0,m}}^{-z_1}(P-a_0) = P-a_0$ for any $P \in \mathcal{P}_V(X)$. In particular, there exists a minimal integer z_0 in $\mathbb{N}\backslash\{0\}$ such that there exists a vector $v_0 \in \mathbb{Z}^m \cap V$ satisfying $\gamma_{r,m,\mathbf{e}_{0,m}}^{-z_0}(P-a_0) = P-a_0+v_0$ for any $P \in \mathcal{P}_V(X)$. Let us denote by I the set of indexes $i \in \{1,\ldots,m\}$ such that $\mathbf{e}_{i,m} \notin V^\perp$. Let us consider $s \in S_{r,m}$ such that $[A \cap (\xi_{r,m}(w)+V)]^V \neq [\emptyset]^V$. Let Q_s be the union of the s-kernel $\ker_s(Y)$ where Y is an s-eye of G such that $\ker_s(Y) \subseteq Q'$.

We are going to prove that there exists a one-to-one function from Q_s to $\{0,\ldots,z_0-1\} \times B_0$ by remarking that for any $z, z' \in \{0,\ldots,z_0-1\}$ and for any $v, v' \in B_0$ such that $(\xi_{r,m}(s)+\gamma_{r,m,\mathbf{e}_{0,m}}^{-z}(P-a_0+v))_{P\in\mathcal{P}_V(X)}$ and $(\xi_{r,m}(s)+\gamma_{r,m,\mathbf{e}_{0,m}}^{-z'}(P-a_0+v'))_{P\in\mathcal{P}_V(X)}$ are equal, we have $v=v'$ and $z=z'$. Thanks to this one-to-one function we will obtain $|Q_s| = z_0.|\mathbb{Z}^m \cap V/\mathrm{inv}_V(X)|$ and concluded the proof of the proposition.

Let us prove that for any state $q \in Q_s$, there exists $z \in \{0,\ldots,z_0-1\}$ and $v \in B_0$ such that $P_q = \xi_{r,m}(s) + \gamma_{r,m,\mathbf{e}_{0,m}}^{-z}(P-a_0+v)$ for any $P \in \mathcal{P}_V(X)$. Let Y be the s-eye such that $q \in \ker_s(Y) \subseteq Q'$. As q is reachable, there exists a path of the form $q_0 \xrightarrow{\sigma} q$. As $q \in \ker_s(Y)$, there exists $n \in \mathbb{N}\backslash\{0\}$ such that $q \xrightarrow{s^n} q$. By replacing n by an integer enough larger in $n.(\mathbb{N}\backslash\{0\})$, we can assume that there exists $\alpha, \beta \in \mathbb{N}$ and $z \in \{0,\ldots,z_0-1\}$ such that $n = \alpha+z+\beta.z_0$ and $|\sigma|_m + \alpha \in z_1.\mathbb{N}$. Let $q' = \delta(q, s^\alpha)$. As $(\emptyset)_{P\in\mathcal{P}_V(X)}$ is not in $\ker_s(Y)$, we deduce that there exists $P \in \mathcal{P}_V(X)$ such that $P_{q'} \neq \emptyset$. Moreover, as $P_{q'}$ is (r,m,s^n)-cyclic and non-empty, from destruction lemma 13.14, we get $\xi_{r,m}(s) \in \mathrm{saff}(P_{q'})$. From $P_{q'} = \gamma_{r,m,\sigma.s^\alpha}^{-1}(P)$, covering lemma 9.9 proves that $\mathrm{saff}(P_{q'}) \subseteq \Gamma_{r,m,\sigma.s^\alpha}^{-1}(\mathrm{saff}(P))$ and $P \subseteq A$, we deduce that $\xi_{r,m}(s) \in \Gamma_{r,m\sigma.s^\alpha}^{-1}(A)$. Therefore $\rho_{r,m}(\sigma.s^\alpha, s) \in A$. Moreover as $|\sigma.s^\alpha|_m \in 1+z_1.\mathbb{N}$, we deduce from lemma 9.22 that $P_{q'} = \xi_{r,m}(s)+P-\rho_{r,m}(\sigma,s)$. Let $v' = a_0 - \rho_{r,m}(\sigma,s)$. As a_0 and $\rho_{r,m}(\sigma,s)$ are both in A, we deduce that $v' \in \mathbb{Z}^m \cap V$. Remark that $P_q = \gamma_{r,m,s}^{-(z+\beta.z_0)}(\xi_{r,m}(s)+P-a_0+v')$ and we have proved that $P_q = \xi_{r,m}(s)+\gamma_{r,m,\mathbf{e}_{0,m}}^{-(z+\beta.z_0)}(P-a_0+v')$ for any $P \in \mathcal{P}_V(X)$. Let us consider an integer $u \in \mathbb{N}$ such that $u.r \in 1+|\mathbb{Z}^m \cap V/\mathrm{inv}_V(X)|.\mathbb{N}$. An immediate induction over $\beta \in \mathbb{N}$ provides $\gamma_{r,m,\mathbf{e}_{0,m}}^{-\beta.z_0}(P-a_0+v') = P-a_0+v$ where v is the vector in B_0 satisfying $v \in u^{\beta.z_0}.v' + (u^{(\beta-1).z_0} + \cdots u^{0.z_0}).v_0 + \mathrm{inv}_V(X)$. Hence $P_q = \xi_{r,m}(s) + \gamma_{r,m,\mathbf{e}_{0,m}}^{-z}(P-a+v)$ for any $P \in \mathcal{P}_V(X)$.

Now, let us prove that for any $z \in \{0,\ldots,z_0-1\}$ and any $v \in B_0$, there exists a state $q \in Q_s$ such that $P_q = \xi_{r,m}(s) + \gamma_{r,m,\mathbf{e}_{0,m}}^{-z}(P-a_0+v)$ for any $P \in \mathcal{P}_V(X)$. From lemma 14.7 we deduce that there exists a vector $v_0 \in V$ such that $v_0[i] < 0$ if $s[i] = r-1$ and $v_0[i] > 0$ if $s[i] = 0$ for any $i \in I$. By replacing v_0 by a vector in $(\mathbb{N}\backslash\{0\}).v_0$, we can assume that $v_0 \in \mathrm{inv}_V(X)$ and $(a-v+v_0)[i] > 0$ if $s[i] = 0$ and $(a-v+v_0)[i] < 0$ if $s[i] = r-1$ for any $i \in I$. As $[Z_{r,m,s} \cap A]^V \neq [\emptyset]^V$, there exists a vector a in $Z_{r,m,s} \cap A$.

Remark that for any $i \in \{1,\dots,m\}$, if $i \in I$ the sign of $(a_0 - v + v_0)[i]$ is $s[i]$ and if $i \notin I$, as $\mathbf{e}_{i,m} \in V^\perp$, we have $(a_0 - v + v_0)[i] = a_0[i] = a[i]$ and form $a \in Z_{r,m,s}$, we also deduce that the sign of $(a_0 - v + v_0)[i]$ is $s[i]$. Hence $a - v + v_0 \in Z_{r,m,s}$. That implies there exists a word $\sigma \in \Sigma^*_{r,m}$ such that $\rho_{r,m}(\sigma, s) = a - v + v_0$. By replacing σ by a word in $\sigma.s^*$, we can assume that $|\sigma|_m \in z_1.\mathbb{N}$. From $\rho_{r,m}(\sigma, s) \in A$ and $|\sigma|_m \in z_1.\mathbb{N}$, lemma 9.22 shows that $\gamma^{-1}_{r,m,\sigma}(P) = \xi_{r,m}(s) + P - \rho_{r,m}(\sigma, s) = \xi_{r,m}(s) + P - a_0 + v + v_0$. From $P + v_0 = P$, we deduce that $\gamma^{-1}_{r,m,\sigma}(P) = \xi_{r,m}(s) + P - a_0 + v$. Hence $\gamma^{-1}_{r,m,\sigma.s^z}(P) = \xi_{r,m}(s) + \gamma^{-1}_{r,m,\mathbf{e}_{0,m}}(P - a_0 + v)$. Let $q = \delta(q_0, \sigma.s^z)$ and let Y be the s-eye that contains q. As $\gamma^{-1}_{r,m,s^{z_1}}(P_q) = P_q$ for any $P \in \mathcal{P}_V(X)$, we deduce that $q \in \ker_s(Y)$. Moreover, as there exists $P \in \mathcal{P}_V(X)\backslash\{\emptyset\}$ we deduce that $P_q \neq \emptyset$. Remark that for any $q' \in \ker_s(Y)$ there exists a path $q' \xrightarrow{s^*} q$ and $P_q \neq \emptyset$, we deduce that $P_{q'} \neq \emptyset$. Hence $\ker_s(Y) \subseteq Q'$. Therefore $q \in Q_s$. □

Theorem 14.14. *Given a cyclic Presburger-definable set $X \subseteq \mathbb{Z}^m$ represented by a FDVA $\mathcal{A}$ in basis r, and given an affine component V of $\overrightarrow{\text{saff}}(X)$ and given a full rank set of indices I of V, the I-representation of $inv_V(X)$ is computable in polynomial time. Moreover $|\mathbb{Z}^m \cap V/inv_V(X)|$ is bounded by the number of principal states of $\mathcal{A}$.*

14.3 Boundary of a Presburger-definable FDVA

Let X be a Presburger-definable set and V be an affine component of $\overrightarrow{\text{saff}}(X)$. The *$V$-boundary* $\text{bound}_V(X)$ of X is defined by the following equality:

$$\text{bound}_V(X) = \bigcup_{P \in \mathcal{P}_V(X)} \text{bound}_V(\mathcal{C}_{V,P}(X))$$

In this section, we prove that $\text{bound}_V(X)\backslash(\bigcup_{j=1}^m \{V \cap \mathbf{e}^\perp_{j,m}\})$ is computable in polynomial time from a FDVA that represents X.

The set $\text{bound}_V(X)$ plays an important role as proved by the following proposition 14.15 (see also figure 14.2).

Proposition 14.15. *Let X be a Presburger-definable set and let V be an affine component of $\overrightarrow{\text{saff}}(X)$. For any $H \in bound_V(X)$, there exist two different semi-V-patterns $P^< \neq P^>$ in $\mathcal{P}_V(X)$, an open convex V-polyhedron C_H satisfying $[C_H \cap H^<]^V \neq [\emptyset]^V$, $[C_H \cap H^>]^V \neq [\emptyset]^V$ and such that:*

$$[X \cap (C_H + V^\perp)]^V = [P^< \cap ((C_H \cap H^<) + V^\perp)]^V \cup^V [P^> \cap ((C_H \cap H^>) + V^\perp)]^V$$

Moreover, if X is (r,m,w)-cyclic then one of these two sets is (r,m)-detectable in X:

$$(P^< \cap (\xi_{r,m}(w) + H^< + V^\perp)) \cup (P^> \cap (\xi_{r,m}(w) + H^\geq + V^\perp))$$

$$(P^< \cap (\xi_{r,m}(w) + H^\leq + V^\perp)) \cup (P^> \cap (\xi_{r,m}(w) + H^> + V^\perp))$$

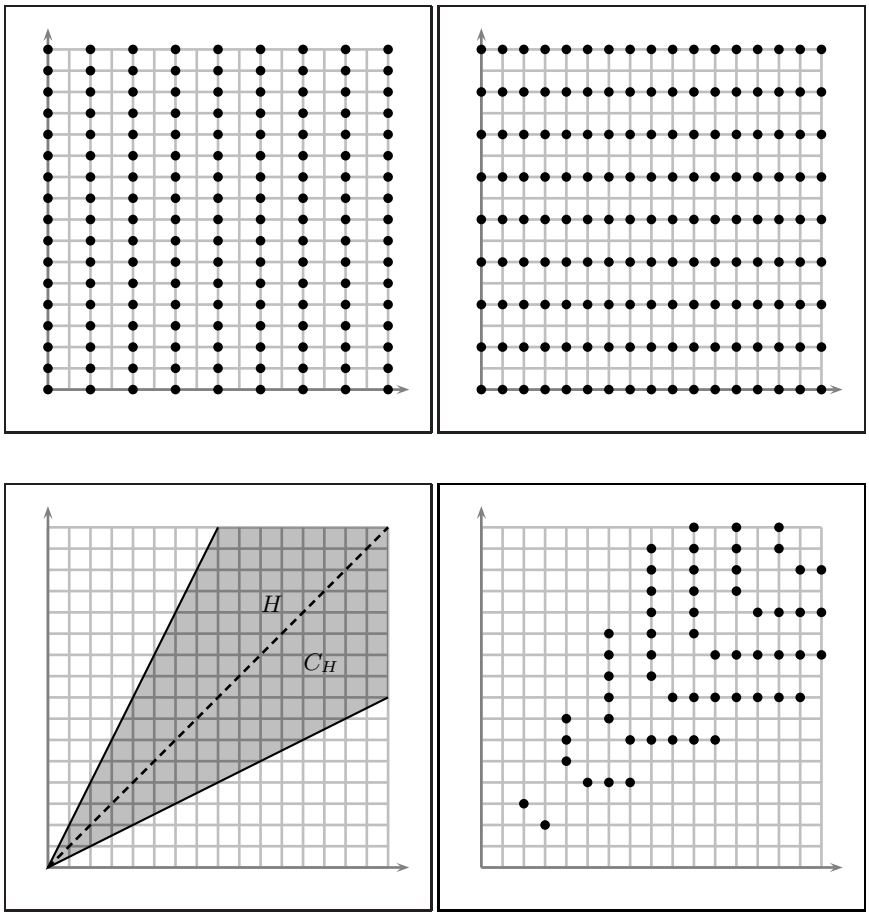

Fig. 14.2. On top left a semi-$\mathbb{Q}^2$-pattern $P^<$, on top right a semi-$\mathbb{Q}^2$-pattern $P^>$, on bottom left an open convex $\mathbb{Q}^2$-polyhedron C_H and a $\mathbb{Q}^2$-hyperplane H, on bottom right the set $(P^< \cap C_H \cap H^<) \cup (P^> \cap C_H \cap H^>)$.

Proof. Let $H \in \text{bound}_V(X)$ and let us prove that there exist two different semi-V-patterns $P^< \neq P^>$ in $\mathcal{P}_V(X)$, an open convex V-polyhedron C_H satisfying $[C_H \cap H^<]^V \neq [\emptyset]^V$, $[C_H \cap H^>]^V \neq [\emptyset]^V$ and such that $[X \cap (C_H + V^\perp)]^V = [P^< \cap ((C_H \cap H^<) + V^\perp)]^V \cup^V [P^> \cap ((C_H \cap H^>) + V^\perp)]^V$. From decomposition theorem 12.4, we have $[X]^V = \bigcup_{P \in \mathcal{P}_V(X)} ([P]^V \cap (\mathcal{C}_{V,P}(X) + V^\perp))$. Let $H \in \text{bound}_V(X)$ and let $\mathcal{H}' = \text{bound}_V(X) \backslash \{H\}$. By definition of $\text{bound}_V(X)$, there exists $P_0 \in \mathcal{P}_V(X)$ such that $H \in \text{bound}_V(\mathcal{C}_{V,P_0}(X))$. Hence, there exist an open convex V-polyhedron C and $\#_0 \in \{<, >\}$ such that $[C \cap H^<]^V \neq [\emptyset]^V$, $[C \cap H^>]^V \neq [\emptyset]^V$ and $\mathcal{C}_{V,P_0}(X) \cap^V [C]^V = [C \cap H^{\#_0}]^V$. From lemma 11.10, we deduce that there exists $\#' \in \{<, >\}^{\mathcal{H}'}$ such that

$[C \cap C_{V,\#'} \cap H^<]^V \neq [\emptyset]^V$, $[C \cap C_{V,\#'} \cap H^>]^V \neq [\emptyset]^V$. Let us denote by C_H the open convex V-polyhedron $C_H = C \cap C_{V,\#'}$. Since $\mathcal{H}' \cup \{H\} = \text{bound}_V(X)$ we deduce that $\mathcal{C}_{V,P}(X) \cap [C_{V,\#'} \cap H^\#]^V$ is either equal to $[\emptyset]^V$ or equal to $[C_{V,\#'} \cap H^\#]^V$ for any $P \in \mathcal{P}_V(X)$ and for any $\# \in \{<, >\}$. By definition of the sequence $(\mathcal{C}_{V,P}(X))_{P \in \mathcal{P}_V(X)}$ (a kind of partition of $[V]^V$) and since $[C_H \cap H^\#]^V \neq [\emptyset]^V$, there exists a unique $P^\# \in \mathcal{P}_V(X)$ such that $\mathcal{C}_{V,P^\#}(X) \cap^V [C_H \cap H^\#]^V = [C_H \cap H^\#]^V$. Since $\mathcal{C}_{V,P_0}(X) \cap^V [C_H]^V = [C_H \cap H^{\#_0}]^V$ we deduce that $\mathcal{C}_{V,P_0}(X) \cap^V [C_H \cap H^{\#_0}]^V = [C_H \cap H^{\#_0}]^V$ and $\mathcal{C}_{V,P_0}(X) \cap^V [C_H \cap H^{\#_1}]^V = [\emptyset]^V$ where $\#_1 \in \{<, >\} \backslash \{\#_0\}$. Hence $P^{\#_0} = P_0$ and $P^{\#_1} \neq P_0$. That means $P^< \neq P^>$ and we have proved that $[X \cap (C_H + V^\perp)]^V = [(P^< \cap ((C_H \cap H^<) + V^\perp)) \cup (P^> \cap ((C_H \cap H^>) + V^\perp))]^V$ with $P^< \neq P^>$ in $\mathcal{P}_V(X)$.

Now, assume that X is (r, m, w)-cyclic, let A be the V-affine space $A = \xi_{r,m}(w) + V$. Let $H \in \text{bound}_V(X)$, let $P^<$ and $P^>$ be two different semi-V-patterns in $\mathcal{P}_V(X)$, let C_H be an open convex V-polyhedron such that $[C_H \cap H^<]^V \neq [\emptyset]^V$, $[C_H \cap H^>]^V \neq [\emptyset]^V$ and such that $[X \cap (C_H + V^\perp)]^V = [P^< \cap ((C_H \cap H^<) + V^\perp)]^V \cup^V [P^> \cap ((C_H \cap H^>) + V^\perp)]^V$, and let us prove that one of these two sets is (r, m)-detectable in X:

$$(P^< \cap (\xi_{r,m}(w) + H^< + V^\perp)) \cup (P^> \cap (\xi_{r,m}(w) + H^\geq + V^\perp))$$

$$(P^< \cap (\xi_{r,m}(w) + H^\leq + V^\perp)) \cup (P^> \cap (\xi_{r,m}(w) + H^> + V^\perp))$$

Let $X' = X \cap A$. Corollary 13.11 shows that $\mathbb{Z}^m \cap A$ is (r, m)-detectable in X. By replacing C_H by $\overrightarrow{C_H}$, we can assume that $C_H = \overrightarrow{C_H}$. Let $X' = X \cap A$. Corollary 13.11 shows that $\mathbb{Z}^m \cap A$ is (r, m)-detectable in X and in particular X' is (r, m)-detectable in X. Since X is (r, m, w)-cyclic and P is (r, m)-detectable in X from corollary 13.9, we deduce that any $P \in \mathcal{P}_V(X)$ is (r, m, w)-cyclic. From lemma 9.20, we deduce that any $P \in \mathcal{P}_V(X)$ is relatively prime with r and included in A.

Let us prove that by modifying C_H, we can assume that $X' \backslash (\xi_{r,m}(w) + H) \cap (\xi_{r,m}(w) + C_H + V^\perp) = (P^< \cap (\xi_{r,m}(w) + C_H \cap H^< + V^\perp)) \cup (P^> \cap (\xi_{r,m}(w) + C_H \cap H^> + V^\perp))$. Let $Z = (X' \backslash (\xi_{r,m}(w) + V) \cap (\xi_{r,m}(w) + C_H + V^\perp)) \Delta ((P^< \cap (\xi_{r,m}(w) + C_H \cap H^< + V^\perp)) \cup (P^> \cap (\xi_{r,m}(w) + C_H \cap H^> + V^\perp)))$. From $[X \cap (C_H + V^\perp)]^V = [(P^< \cap ((C_H \cap H^<) + V^\perp)) \cup (P^> \cap ((C_H \cap H^>) + V^\perp))]^V$, we deduce that $[Z]^V = [\emptyset]^V$. Since X', $P^<$ and $P^>$ are included in A, we deduce that $\text{saff}(Z) \subseteq A$. In particular $\overrightarrow{\text{saff}}(Z) \subseteq V$. Since $[Z]^V = [\emptyset]^V$, we deduce that V is not included in $\overrightarrow{\text{saff}}(Z)$. Assume by contradiction that $H \subseteq \overrightarrow{\text{saff}}(Z)$. There exists an affine component W of $\overrightarrow{\text{saff}}(X)$ such that $H \subseteq W$. Since H is a V-hyperplane, either $W = H$ or $W = V$. The last case is not possible since V is not included in $\overrightarrow{\text{saff}}(Z)$. Hence $W = H$ is an affine component of $\overrightarrow{\text{saff}}(Z)$. Since $\text{saff}(Z) = \xi_{r,m}(w) + \overrightarrow{\text{saff}}(Z)$ we deduce that $\xi_{r,m}(w) + H$ is an affine component of $\text{saff}(Z)$. From the dense component lemma 12.1, we deduce that $\text{saff}(Z \cap (\xi_{r,m}(w) + H)) = \xi_{r,m}(w) + H$. As $Z \cap (\xi_{r,m}(w) + H) = \emptyset$, we deduce a contradiction. Hence, there exists a finite set $\mathcal{H}_0$ of V-hyperplane such that

$\overrightarrow{\mathcal{H}_0} = \mathcal{H}_0$, $H \notin \mathcal{H}_0$ and such that $\overrightarrow{\text{saff}}(Z) \subseteq \bigcup_{H_0 \in \mathcal{H}_0} H_0$. Thanks to lemma 11.10, we deduce that there exists $\# \in \{<, >\}^{\mathcal{H}_0}$ such that $[C_H \cap C_{V,\#} \cap H^>] \neq [\emptyset]^V$ and $[C_H \cap C_{V,\#} \cap H^<] \neq [\emptyset]^V$. Hence, by replacing C_H by $C_H \cap C_{V,\#}$, since $Z \cap C_{V,\#} = \emptyset$, we can assume without loss of generality that $Z = \emptyset$. Thus $X' \backslash (\xi_{r,m}(w) + V) \cap (\xi_{r,m}(w) + C_H + V^\perp) = (P^< \cap (\xi_{r,m}(w) + C_H \cap H^< + V^\perp)) \cup (P^> \cap (\xi_{r,m}(w) + C_H \cap H^> + V^\perp))$.

Assume first that $\mathbb{Z}^m \cap (\xi_{r,m}(w) + V)$ is (r,m)-detectable in X and let us show that $X'' = (P^< \cap (\xi_{r,m}(w) + H^< + V^\perp)) \cup (P^> \cap (\xi_{r,m}(w) + H^> + V^\perp))$ is (r,m)-detectable in X. Let us consider a pair (σ_1, σ_2) of words in $\Sigma_{r,m}^*$ such that $\gamma_{r,m,\sigma_1}^{-1}(X) = \gamma_{r,m,\sigma_2}^{-1}(X)$. Let us consider $x \in \gamma_{r,m,\sigma_1}^{-1}(X'')$. Then $\gamma_{r,m,\sigma_1}(x) \in (P^< \cap (\xi_{r,m}(w) + H^< + V^\perp)) \cup (P^> \cap (\xi_{r,m}(w) + H^> + V^\perp))$. By definition of v, there exists an integer $k \in \mathbb{N}$ enough larger such that $\gamma_{r,m,\sigma_1}(x + k.v)$ is in $X'' \cap (\xi_{r,m}(w) + C_H + V^\perp)$ and such that $\gamma_{r,m,\sigma_2}(x + k.v) \in \xi_{r,m}(w) + C_H + V^\perp$. Since $X'' \cap (\xi_{r,m}(w) + C_H + V^\perp) = X' \backslash (\xi_{r,m}(w) + H) \cap (\xi_{r,m}(w) + C_H + V^\perp)$, we deduce that $\gamma_{r,m,\sigma_1}(x + k.v) \in X' \backslash (\xi_{r,m}(w) + H)$. Since X' and $\mathbb{Z}^m \cap (\xi_{r,m}(w) + H)$ are both (r,m)-detectable in X, we deduce that $\gamma_{r,m,\sigma_2}(x + k.v) \in X' \backslash (\xi_{r,m}(w) + H)$. Moreover, as $\gamma_{r,m,\sigma_2}(x + k.v)(x) \in (\xi_{r,m}(w) + C_H + V^\perp)$, we have proved that $\gamma_{r,m,\sigma_2}(x + k.v) \in X' \backslash (\xi_{r,m}(w) + H) \cap (\xi_{r,m}(w) + C_H + V^\perp)$. Since this last set is equal to $X'' \cap (\xi_{r,m}(w) + C_H + V^\perp)$ we get $\gamma_{r,m,\sigma_2}(x + k.v) \in X''$. By definition of v, we get $\gamma_{r,m,\sigma_2}(x) \in X''$. Therefore X'' is (r,m)-detectable in X.

We deduce that if $\mathbb{Z}^m \cap (\xi_{r,m}(w) + H)$ is (r,m)-detectable in X, since $P^< \cap (\xi_{r,m}(w) + H)$ and $P^> \cap (\xi_{r,m}(w) + H)$ are both (r,m)-detectable in X as the intersection of (r,m)-detectable sets, the following two sets are (r,m)-detectable in X:

$$(P^< \cap (\xi_{r,m}(w) + H^< + V^\perp)) \cup (P^> \cap (\xi_{r,m}(w) + H^\geq + V^\perp))$$

$$(P^< \cap (\xi_{r,m}(w) + H^\leq + V^\perp)) \cup (P^> \cap (\xi_{r,m}(w) + H^> + V^\perp))$$

Now, assume that $\mathbb{Z}^m \cap (\xi_{r,m}(w) + H)$ is not (r,m)-detectable in X

Let us first show that there exists a pair (σ_1, σ_2) of words such that $\gamma_{r,m,\sigma_1}^{-1}(X) = \gamma_{r,m,\sigma_2}^{-1}(X)$, $\Gamma_{r,m,\sigma_1}^{-1}(\xi_{r,m}(w) + V)$ and $\Gamma_{r,m,\sigma_2}^{-1}(\xi_{r,m}(w) + V)$ are equal, $\mathbb{Z}^m \cap \Gamma_{r,m,\sigma_1}^{-1}(\xi_{r,m}(w) + H)$ is not empty, and such that $\Gamma_{r,m,\sigma_1}^{-1}(\xi_{r,m}(w) + H + V^\perp)$ and $\Gamma_{r,m,\sigma_2}^{-1}(\xi_{r,m}(w) + H + V^\perp)$ have an empty intersection. Since $\mathbb{Z}^m \cap (\xi_{r,m}(w) + H)$ is not (r,m)-detectable in X, there exists a pair (σ_1, σ_2) of words in $\Sigma_{r,m}^*$ such that $\gamma_{r,m,\sigma_1}^{-1}(X) = \gamma_{r,m,\sigma_2}^{-1}(X)$ and such that $\gamma_{r,m,\sigma_1}^{-1}(\mathbb{Z}^m \cap (\xi_{r,m}(w) + H))$ and $\gamma_{r,m,\sigma_2}^{-1}(\mathbb{Z}^m \cap (\xi_{r,m}(w) + H))$ are disjoint. Remark that $\gamma_{r,m,\sigma_i}^{-1}(\mathbb{Z}^m \cap (\xi_{r,m}(w) + H)) = \mathbb{Z}^m \cap \Gamma_{r,m,\sigma_i}^{-1}(\xi_{r,m}(w) + H)$ for any $i \in \{1, 2\}$. By replacing (σ_1, σ_2) by (σ_2, σ_1), we can assume that $\mathbb{Z}^m \cap \Gamma_{r,m,\sigma_1}^{-1}(\xi_{r,m}(w) + H)$ is not empty. Since $\mathbb{Z}^m \cap (\xi_{r,m}(w) + V)$ is (r,m)-detectable in X, we deduce that $\mathbb{Z}^m \cap \Gamma_{r,m,\sigma_1}^{-1}(\xi_{r,m}(w) + V)$ and $\mathbb{Z}^m \cap \Gamma_{r,m,\sigma_2}^{-1}(\xi_{r,m}(w) + V)$ are equal. Moreover, as $\mathbb{Z}^m \cap \Gamma_{r,m,\sigma_1}^{-1}(\xi_{r,m}(w) + H)$ is non empty and $H \subseteq V$, we deduce that the sets $\mathbb{Z}^m \cap \Gamma_{r,m,\sigma_1}^{-1}(\xi_{r,m}(w) + V)$ and $\mathbb{Z}^m \cap \Gamma_{r,m,\sigma_2}^{-1}(\xi_{r,m}(w) + V)$ are non empty. Taking the semi-affine hull of these sets, we get $\Gamma_{r,m,\sigma_1}^{-1}(\xi_{r,m}(w) + V) = \Gamma_{r,m,\sigma_2}^{-1}(\xi_{r,m}(w) + V)$. Assume by contradiction that $\Gamma_{r,m,\sigma_1}^{-1}(\xi_{r,m}(w) + H + V^\perp)$

and $\Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+H+V^\perp)$ have a non empty intersection and let x be a vector in this intersection. From $x \in \Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+H+V^\perp)$ we deduce that there exists $v_\perp \in V^\perp$ such that $x - v_\perp \in \Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+H) \subseteq \Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+V)$. From $\Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+V) = \Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+V)$, we deduce that $x - v \in \Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+V)$. Moreover, since $x \in \Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+H+V^\perp)$, we get $x - v \in \Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+H)$. Therefore $\Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+H)$ and $\Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+H)$ are equal and we get a contradiction.

Since $\Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+H+V^\perp)$ and $\Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+H+V^\perp)$ have an empty intersection, there exists $\# \in \{<,>\}$ such that $\Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+H+V^\perp) \subseteq \Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+H^\#+V^\perp)$.

Let us consider the (r,m,w)-cyclic Presburger definable set $X'_H = X' \cap (\xi_{r,m}(w)+H)$ and the semi-H-pattern $P^\#_H = P^\# \cap (\xi_{r,m}(w)+H)$, and let us prove the following equality:

$$\gamma^{-1}_{r,m,\sigma_1}(X'_H \cap (\xi_{r,m}(w)+C_H \cap H)) = \gamma^{-1}_{r,m,\sigma_1}(P^\#_H \cap (\xi_{r,m}(w)+C_H \cap H))$$

Remark that $\gamma^{-1}_{r,m,\sigma_2}(X'\backslash(\xi_{r,m}(w)+H)) \cap \Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+C_H \cap H+V^\perp)$ is equal to $\gamma^{-1}_{r,m,\sigma_2}(X')\backslash\Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+H+V^\perp) \cap \Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+C_H \cap H+V^\perp)$. Since $\Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+H+V^\perp)$ and $\Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+H+V^\perp)$ have an empty intersection, and $\gamma^{-1}_{r,m,\sigma_1}(X') = \gamma^{-1}_{r,m,\sigma_2}(X')$, we deduce that $\gamma^{-1}_{r,m,\sigma_2}(X'\backslash(\xi_{r,m}(w)+C_H \cap H+V^\perp)) \cap \Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+C_H \cap H+V^\perp)$ is equal to $\gamma^{-1}_{r,m,\sigma_1}(X'_H \cap (\xi_{r,m}(w)+C_H \cap H+V^\perp))$. On the other hand, since $X'\backslash(\xi_{r,m}(w)+H+V^\perp) \cap (\xi_{r,m}(w)+V_H+V^\perp) = \bigcup_{\#' \in \{<,>\}}(P^{\#'} \cap (\xi_{r,m}(w)+C_H \cap H^{\#'}+V^\perp)))$, we get $\gamma^{-1}_{r,m,\sigma_2}(X'\backslash(\xi_{r,m}(w)+H+V^\perp) \cap (\xi_{r,m}(w)+V_H+V^\perp)) \cap \Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+H+V^\perp) = \bigcup_{\#' \in \{<,>\}}(\gamma^{-1}_{r,m,\sigma_2}(P^{\#'}) \cap \Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+C_H \cap H^{\#'}+V^\perp) \cap \Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+H+V^\perp))$. Remark that $\Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+H^{\#'}+V^\perp)$ and $\Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+H+V^\perp)$ have an empty intersection if $\#'$ is not equal to $\#$ and $\Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+C_H \cap H^\#+V^\perp) \cap \Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+H+V^\perp) = \Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+C_H+V^\perp) \cap \Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+H+V^\perp)$. As $\Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+V) = \Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+V)$ and $\overrightarrow{C_H} = C_H$, we deduce that $\Gamma^{-1}_{r,m,\sigma_2}(\xi_{r,m}(w)+C_H+V^\perp) = \Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+C_H+V^\perp)$. Moreover, since $\gamma^{-1}_{r,m,\sigma_2}(P^\#) = \gamma^{-1}_{r,m,\sigma_1}(P^\#)$, we have proved that $\gamma^{-1}_{r,m,\sigma_2}(X'\backslash(\xi_{r,m}(w)+H+V^\perp)) \cap \Gamma^{-1}_{r,m,\sigma_1}(\xi_{r,m}(w)+C_H \cap H+V^\perp) = \gamma^{-1}_{r,m,\sigma_1}(P^\# \cap (\xi_{r,m}(w)+\mathcal{C}_H \cap H+V^\perp))$. Combining the two equalities proved in this paragraph, we are done.

Let us prove that $C_H \cap H$ is a non H-degenerate H-polyhedron. The proof is obtained thanks to lemma 11.6. Since $[C_H \cap H^\#]^V \neq [\emptyset]^V$, there exists a vector $v_\# \in H^\# \cap C_H$. Now just remark that there exists $k_<$, $k_>$ in $\mathbb{Q}_+\backslash\{0\}$ such that $v = k_<.v_< + k_>.v_>$ is in H. In particular $v \in H \cap C_H$. Thus $H \cap C_H$ is non-H-degenerate.

Next, let us prove that $[X'_H \cap (\xi_{r,m}(w)+C_H \cap H)]^H = [P^\#_H \cap (\xi_{r,m}(w)+C_H \cap H)]^H$. Since $\gamma^{-1}_{r,m,\sigma_1}(\mathbb{Z}^m \cap (\xi_{r,m}(w)+H))$ is non empty, there ex-

ists a (r,m)-decomposition (w,s) such that $\rho_{r,m}(w,s)$ is in this set. By replacing w by a word in $w.s^*$, since $\mathrm{inv}_V(P^\#)$ is relatively prime with r, we can assume that $r^{|\sigma_1.w|_m} \in 1+|\mathbb{Z}^m \cap V/\mathrm{inv}_V(P^\#)|.\mathbb{Z}$. From lemma 9.22 we get $\gamma^{-1}_{r,m,\sigma_1.w}(P^\#) = \xi_{r,m}(w) + P^\# - \rho_{r,m}(\sigma_1.w,s)$. In particular, if $[X'_H]^H = [\emptyset]^H$, then $[\gamma^{-1}_{r,m,\sigma_1.w}(X'_H)]^H = [\emptyset]^H$ and from the equality $\gamma^{-1}_{r,m,\sigma_1}(X'_H \cap (\xi_{r,m}(w) + C_H \cap H)) = \gamma^{-1}_{r,m,\sigma_1}(P^\#_H \cap (\xi_{r,m}(w) + C_H \cap H))$ we deduce that $[\gamma^{-1}_{r,m,\sigma_1.w}(P^\#_H \cap (\xi_{r,m}(w) + C_H \cap H))]^H = [\emptyset]^H$. Since $C_H \cap H$ is non H-degenerate, we get $[P^\#_H]^H = [\emptyset]^H$ and we have proved that $[X'_H \cap (\xi_{r,m}(w) + C_H \cap H)]^H = [P^\#_H \cap (\xi_{r,m}(w) + C_H \cap H)]^H$. So, we can assume that $[X'_H]^H \neq [\emptyset]^H$. In this case H is an affine component of the (r,m,w)-cyclic Presburger definable set X'_H. In particular $\mathrm{inv}_H(X'_H)$ is relatively prime with r and by replacing w by a word in $w.s^*$ we can assume that $r^{|\sigma_1.w|_m} \in 1+|\mathbb{Z}^m \cap H/\mathrm{inv}_H(X)|.\mathbb{Z}$. Since $\rho_{r,m}(\sigma.w,s) \in \mathbb{Z}^m \cap (\xi_{r,m}(w)+H)$, from lemma 9.22 we deduce that $\gamma^{-1}_{r,m,\sigma_1.w}(P) = \xi_{r,m}(s) + P - \rho_{r,m}(\sigma_1.w,s)$. From $[X'_H]^H = \bigcup^H_{P\in\mathcal{P}_H(X'_H)}([P]^H \cap^H \mathcal{C}_{H,P}(X'_H) + H^\perp)$, we deduce that $[\gamma^{-1}_{r,m,\sigma_1.w}(X'_H)]^H = \bigcup^H_{P\in\mathcal{P}_H(X'_H)}([\gamma^{-1}_{r,m,\sigma_1.w.s}(P)]^H \cap^H \mathcal{C}_{H,P}(X'_H)+H^\perp)$. From the equality $[X'_H \cap (\xi_{r,m}(w) + C_H \cap H)]^H = [P^\#_H \cap (\xi_{r,m}(w) + C_H \cap H)]^H$, decomposition theorem 12.4 shows that there exists $P \in \mathcal{P}_H(X'_H)$ such that $[C_H \cap H]^H \subseteq^H \mathcal{C}_{H,P}(X'_H)$ and such that $\gamma^{-1}_{r,m,\sigma_1.w}(P) = \gamma^{-1}_{r,m,\sigma_1.w}(P^\#_H)$. Since $\gamma^{-1}_{r,m,\sigma_1.w}(P) = \xi_{r,m}(s) + P - \rho_{r,m}(\sigma_1.w,s)$ and $\gamma^{-1}_{r,m,\sigma_1.w}(P^\#_H) = \xi_{r,m}(s) + P^\#_H - \rho_{r,m}(\sigma_1.w,s)$ we get $P = P^\#_H$. Thus $[X'_H \cap (\xi_{r,m}(w) + C_H \cap H)]^H = [P^\#_H \cap (\xi_{r,m}(w) + C_H \cap H)]^H$ and we are done.

Let us consider the set $E = (P^< \cap (\xi_{r,m}(w)+H^<+V^\perp)) \cup (P^\# \cap (\xi_{r,m}(w)+H+V^\perp)) \cup (P^> \cap (\xi_{r,m}(w)+H^\geq+V^\perp))$ and remark that these set is equal to one of the following two sets and it is such that $[Z]^H = [\emptyset]^H$ where $Z = (X' \Delta E) \cap (\xi_{r,m}(w) + C_H + V^\perp)$.

$$(P^< \cap (\xi_{r,m}(w) + H^< + V^\perp)) \cup (P^> \cap (\xi_{r,m}(w) + H^\geq + V^\perp))$$

$$(P^< \cap (\xi_{r,m}(w) + H^\leq + V^\perp)) \cup (P^> \cap (\xi_{r,m}(w) + H^> + V^\perp))$$

Let us prove that E is (r,m)-detectable in X. Consider a pair (w_1,w_2) of words in $\Sigma^+_{r,m}$ such that $\gamma^{-1}_{r,m,w_1}(X) = \gamma^{-1}_{r,m,w_2}(X)$. Since X' is (r,m)-detectable in X, we deduce that $t\gamma^{-1}_{r,m,w_1}(X') = \gamma^{-1}_{r,m,w_2}(X')$. From $Z = (X'\Delta E) \cap (\xi_{r,m}(w) + C_H + V^\perp)$, we deduce that $Z' = (\gamma^{-1}_{r,m,w_1}(E) \Delta \gamma^{-1}_{r,m,w_2}(E)) \cap (C' + V^\perp)$ where C' is the open convex V-polyhedron such that $C' + V^\perp = \Gamma^{-1}_{r,m,w_1}(\xi_{r,m}(w) + C_H + V^\perp) \cap \Gamma^{-1}_{r,m,w_2}(\xi_{r,m}(w) + C_H + V^\perp)$ and $Z' = (\gamma^{-1}_{r,m,w_1}(E) \Delta \gamma^{-1}_{r,m,w_2}(E)) \cap (C' + V^\perp)$. Since $[Z]^H = [\emptyset]^H$, from covering lemma 9.9, we get $[Z']^H = [\emptyset]^H$. Moreover, as $[C']^V = [C_H]^V$, we deduce that C' is non V-degenerate and such that $[C' \cap H^<]^V$ and $[C' \cap H^>]^V$ are both non equal to $[\emptyset]^V$. Let us remark that $\gamma^{-1}_{r,m,w_1}(E) \Delta \gamma^{-1}_{r,m,w_2}(E)$ is a semi-H-pattern and $C' \cap H$ is a non-H-degenerate H-polyhedron from lemma 11.11. Since $[Z']^H = [\emptyset]^H$, we deduce from lemma 12.2 that $\gamma^{-1}_{r,m,w_1}(E) = \gamma^{-1}_{r,m,w}(E)$. Thus E is (r,m)-detectable. We are done. □

Recall that a semi-V-pattern P detectable in a (r, m, w)-cyclic set X are relatively prime with r. The following proposition will become useful in the last section in order to check that some sets that must be detectable in X if X is Presburger-definable are effectively detectable in X.

Proposition 14.16. *Let $\mathcal{A}$ be a FDVA, let $P_1 = B_1 + M$, $P_2 = B_2 + M$ be two semi-V-patterns where B_1, B_2 are two finite subsets of $\mathbb{Z}^m$, and M is a V-vector lattices included in $\mathbb{Z}^m$ relatively prime with r, let H be a V-hyperplane, let $a_0 \in \mathbb{Q}^m$ and let $(\#_1, \#_2) \in \{(<, \geq), (\leq, >)\}$. Assume that there exists a final function F_i such that P_i is represented by $\mathcal{A}^{F_i}$. We can decide in polynomial time if there exists a final function F such that the following set is represented by $\mathcal{A}^F$:*

$$(P_1 \cap (a_0 + H^{\#_1} + V^{\perp})) \cup (P_2 \cap (a_0 + H^{\#_2} + V^{\perp}))$$

Proof. From proposition 4.6 we deduce in polynomial time a set U of pairs (σ_a, σ_b) of words in Σ_r^* such that $|\sigma_a| + m.\mathbb{Z} = |\sigma_b| + m.\mathbb{Z}$ for any $(\sigma_a, \sigma_b) \in U$ and such that a set $X' \subseteq \mathbb{Z}^m$ is represented by a FDVA of the form $\mathcal{A}^F$ if and only if $\gamma_{r,m,\sigma_a}^{-1}(X') = \gamma_{r,m,\sigma_b}^{-1}(X')$ for any $(\sigma_a, \sigma_b) \in U$. Let X' be the set $X' = (P_1 \cap (a_0 + H^{\#_1} + V^{\perp})) \cup (P_2 \cap (a_0 + H^{\#_2} + V^{\perp}))$. Since $\gamma_{r,m,\sigma_a}^{-1}(P_i) = \gamma_{r,m,\sigma_b}^{-1}(P_i)$ for any $i \in \{1, 2\}$, for proving the proposition, it is sufficient to show that given a pair (σ_a, σ_b) of words such that $|\sigma_a| + m.\mathbb{Z} = |\sigma_b| + m.\mathbb{Z}$ and $\gamma_{r,m,\sigma_a}^{-1}(P_i) = \gamma_{r,m,\sigma_b}^{-1}(P_i)$ for any i, we can decide in polynomial time if $\gamma_{r,m,\sigma_a}^{-1}(X') = \gamma_{r,m,\sigma_b}^{-1}(X')$. In polynomial time, we can compute a vector $\alpha \in \mathbb{Z}^m \cap V$ such that $H^{\#} = \{x \in V;\ \langle \alpha, x \rangle \, \#0\}$ for any $\# \in \{<, \leq, =, \geq, >\}$. Let $z \in \{0, \ldots, m-1\}$ such that $|\sigma_a| + m.\mathbb{Z} = z + m.\mathbb{Z} = |\sigma_b| + m.\mathbb{Z}$, let α_z be the vector in $\mathbb{Z}^m$ such that $\langle \alpha, \gamma_{r,m,0}^z(x) \rangle = \langle \alpha_z, x \rangle$ for any $x \in \mathbb{Q}^m$, and let V_z be the vector space $V_z = \Gamma_{r,m,0}^{-z}(V)$. Proposition 9.18 proves that we can compute in polynomial time two finite subsets B_1' and B_2' of $\mathbb{Z}^m$ such that $\gamma_{r,m,\sigma_a}^{-1}(P_i) = B_i' + \gamma_{r,m,0}^{-|\sigma|}(M)$. Since M is relatively prime with r, we deduce that $\gamma_{r,m,0}^{-|\sigma|}(M)$ is equal to $M_z = \gamma_{r,m,0}^{-z}(M)$. Note that $\gamma_{r,m,\sigma_b}^{-1}(P_i) = B_i' + M_z$. Let $c_a = r^{\frac{z-|\sigma_a|}{m}}.\langle \alpha, a_0 \rangle$ and $c_b = r^{\frac{z-|\sigma_b|}{m}}.\langle \alpha, a_0 \rangle$. Observe that $x \in \Gamma_{r,m,\sigma_a}^{-1}(a_0 + H^{\#} + V^{\perp})$ if and only if $\Gamma_{r,m,\sigma_a}(x) \in a_0 + H^{\#} + V$ if and only if $\langle \alpha, \Gamma_{r,m,\sigma_a}(x) \rangle \, \# \, \langle \alpha, a_0 \rangle$ if and only if $\langle \alpha_z, x \rangle \, \# c_a$. We deduce the following equalities (the equality with σ_b is obtained by symmetry):

$$\begin{cases} \gamma_{r,m,\sigma_a}^{-1}(X') = \{x \in B_1' + M_z;\ \langle \alpha_z, x \rangle \, \#_1 c_a\} \cup \{x \in B_2' + M_z;\ \langle \alpha_z, x \rangle \, \#_2 c_a\} \\ \gamma_{r,m,\sigma_b}^{-1}(X') = \{x \in B_1' + M_z;\ \langle \alpha_z, x \rangle \, \#_1 c_b\} \cup \{x \in B_2' + M_z;\ \langle \alpha_z, x \rangle \, \#_2 c_b\} \end{cases}$$

If $c_a = c_b$ then $\gamma_{r,m,\sigma_a}^{-1}(X') = \gamma_{r,m,\sigma_2}^{-1}(X')$. Otherwise, by symmetry, we can assume that $c_a < c_b$. In this case, the set $\gamma_{r,m,\sigma_a}^{-1}(X') \Delta \gamma_{r,m,\sigma_b}^{-1}(X')$ is equal to the following set:

$$\{x \in (B_1' + M_z) \Delta (B_2' + M_z);\ c_a(-\#_2) \, \langle \alpha_z, x \rangle \, \#_1 c_b\}$$

Let us consider the set B equal to the union of the set of vectors $b \in B_1$ such that there does not exist $b_2 \in B_2$ such that $b - b_2 \in M_z$ and the set of vectors $b \in B_2$ such that there does not exist $b_1 \in B_1$ satisfying $b - b_1 \in M_z$. Observe that B is computable in polynomial time and $(B'_1 + M_z)\Delta(B'_2 + M_z) = B + M_z$. Thus we have reduced our problem to decide if there exists $b \in B$ such that the following set is non empty where $c'_1 = c_a - \langle \alpha_z, b \rangle$, $c'_2 = c_b - \langle \alpha_z, b \rangle$, and $(\#'_1, \#'_2) = (-\#_2, \#_1)$:

$$\{x \in M_z;\ c'_1 \#'_1 \langle \alpha_z, x \rangle \#'_2 c'_2\}$$

From an Hermite representation of M_z, we deduce in linear time a $\mathbb{Z}$-basis v_1, ..., v_d of M_z. Note that the set $\{\langle \alpha_z, x \rangle\ ;\ x \in M_z\}$ is equal to $\sum_{i=1}^{d} \mathbb{Z}.\langle \alpha_z, v_i \rangle$. Thus, considering the lattice generated by $\{\langle \alpha_z, v_i \rangle\ ;\ 1 \leq i \leq d\}$, we compute in polynomial time a rational number $\mu > 0$ such that $\{\langle \alpha_z, x \rangle\ ;\ x \in M_z\}$ is equal to $\mathbb{Z}.\mu$. We deduce that $\{x \in M_z;\ c'_1 \#'_1 \langle \alpha_z, x \rangle \#'_2 c'_2\}$ is non empty if and only if there exists an integer $z \in \mathbb{Z}$ such that $\frac{c'_1}{\mu} \#'_1 z \#'_2 \frac{c'_2}{\mu}$. This property property is decidable in linear time. We are done. □

14.3.1 A polynomial time algorithm

As for any pair of serialized encoded FDVA $(\mathcal{A}_1, \mathcal{A}_2)$, we can compute in quadratic time a serialized encoded FDVA $\mathcal{A}$ that represents $X_1 \Delta X_2$ where X_i is the set represented by $\mathcal{A}_i$, the following proposition 14.17 shows that our computation problem can be effectively done in polynomial time thanks to the semi-affine hull direction computation.

Proposition 14.17. *Let X be a Presburger-definable set represented by a FDVA $\mathcal{A}$ and let V be an affine component of $\overrightarrow{\text{saff}}(X)$. Consider $I_{\mathcal{A}}(V)$, the set of pairs of states $(q_1, q_2) \in T \times T$ where T is a terminal component such that $V_G(T) = V$ and such that $q_1 \sim^V q_2$. We have the following equality:*

$$\mathit{bound}_V(X) \backslash (\bigcup_{j=1}^{m} \{V \cap \boldsymbol{e}_{j,m}^{\perp}\}) = \text{comp}(\bigcup_{(q_1,q_2) \in I_{\mathcal{A}}(V)} \overrightarrow{\text{saff}}(X_{q_1} \Delta X_{q_2}))$$

Proof. Let J be the set of indices in $\{1, \ldots, m\}$ such that $V \cap \mathbf{e}_{j,m}^{\perp}$ is a V-hyperplane. As $\text{bound}_V(X)$ contains only V-hyperplanes, we deduce that $\text{bound}_V(X) \backslash (\bigcup_{j=1}^{m} \{V \cap \mathbf{e}_{j,m}^{\perp}\})$ and $\text{bound}_V(X) \backslash (\bigcup_{j \in J} \{V \cap \mathbf{e}_{j,m}^{\perp}\})$ are equal. We denote by $\mathcal{H}_0$ this class. The semi-affine space $S = \bigcup_{H \in \mathcal{H}_0} H$ satisfies $\text{comp}(S) = \mathcal{H}_0$. Consider the semi-affine space $S' = \bigcup_{(q_1,q_2) \in I_{\mathcal{A}}(V)} \overrightarrow{\text{saff}}(X_{q_1} \Delta X_{q_2})$. We have to prove that $S = S'$.

Let us first prove the inclusion $S' \subseteq S$. Let $(q_1, q_2) \in I_A(V)$ and let $W = \overrightarrow{\text{saff}}(X_{q_1} \Delta X_{q_2})$. Naturally, if $W = \emptyset$, we immediately have $W \subseteq S$. So we can assume that $W \neq \emptyset$. Let us consider an affine component A_0 of W.

From theorem 13.17 there exists $a_1, a_2 \in \mathbb{Q}^m$ satisfying the following equality (where $i \in \{1, 2\}$) and such that $-1 < a_i[j] < 0$ for any $(i, j) \in \{1, 2\} \times J$:

$$X_{q_i} = \bigcup_{P\in\mathcal{P}_V(X)} \bigcup_{\#\in\mathcal{S}_{V,P}(X)} P_{q_i} \cap (a_i + C_{V,\#} + V^\perp)$$

We denote by v_i the vector $v_i = \Pi_V(a_i)$ for $i \in \{1,2\}$. Remark that $P_{q_1} = P_{q_2}$ for any $P \in \mathcal{P}_V$ since $q_1 \sim^V q_2$. We denote by P_{q_1,q_2} this semi-V-pattern.

Let us prove that there exists $H \in \text{bound}_V(X)$, $\# \in \{<,>\}$ and a V-affine space A such that $A_0 \subseteq \overrightarrow{\text{saff}}(\mathbb{Z}^m \cap A \cap (((v_1 + H^\#)\Delta(v_2 + H^\#)) + V^\perp))$. The set $X_{q_1}\Delta X_{q_2}$ is included into the finite union of sets $P_{q_1,q_2} \cap (((v_1 + C_{V,\#})\Delta(v_2 + C_{V,\#})) + V^\perp)$ over $P \in \mathcal{P}_V(X)$ and $\# \in \mathcal{S}_{V,P}(X)$. As $C_{V,\#} = \bigcap_{H\in\text{bound}_V(X)} H^{\#_H}$, we deduce that $X_{q_1}\Delta X_{q_2}$ is included into the finite union of sets $P_{q_1,q_2} \cap (((v_1 + H^\#)\Delta(v_2 + H^\#)) + V^\perp)$ over $P \in \mathcal{P}_V(X)$, $H \in \text{bound}_V(X)$ and $\# \in \{<,>\}$. From insecable lemma 9.2, we deduce that there exists $P \in \mathcal{P}_V(X)$, $H \in \text{bound}_V(X)$ and $\# \in \{<,>\}$ such that $A_0 \subseteq \overrightarrow{\text{saff}}(P_{q_1,q_2} \cap (((v_1 + H^\#)\Delta(v_2 + H^\#)) + V^\perp))$. As P_{q_1,q_2} is a semi-V-pattern, it is included into a finite union of sets of the form $\mathbb{Z}^m \cap A$ where A is a V-affine space. From insecable lemma 9.2 we deduce that there exists a V-affine space A such that $A_0 \subseteq \overrightarrow{\text{saff}}(\mathbb{Z}^m \cap A \cap (((v_1 + H^\#)\Delta(v_2 + H^\#)) + V^\perp))$.

Let us show that $H \notin \{V \cap \mathbf{e}_{j,m}^\perp;\ j \in J\}$. As $A_0 \neq \emptyset$, it is sufficient to show that otherwise, the set $\mathbb{Z}^m \cap A \cap (((v_1 + H^\#)\Delta(v_2 + H^\#)) + V^\perp)$ is empty. Remark that this set is included in $(\mathbb{Z}^m \cap (a_1 + H^\# + V^\perp))\Delta(\mathbb{Z}^m \cap (a_1 + H^\# + V^\perp))$. If $H = V \cap \mathbf{e}_{j,m}^\perp$ where $j \in J$, there exists $\epsilon \in \{-1,1\}$ such that $H^\# = \{x \in V;\ \epsilon.x[j]\#0\}$. Remark that $a_i + H^\# + V^\perp = \{x \in \mathbb{Q}^m;\ \epsilon.(x[j] - a_i[j])\#0\}$. As $a_1[j]$ and $a_2[j]$ are two rational numbers in $\{x \in \mathbb{Q};\ -1 < x < 0\}$. We deduce that $\mathbb{Z}^m \cap (a_1 + H^\# + V^\perp)$ and $\mathbb{Z}^m \cap (a_2 + H^\# + V^\perp)$ are equal. Therefore $(\mathbb{Z}^m \cap (a_1 + H^\# + V^\perp))\Delta(\mathbb{Z}^m \cap (a_1 + H^\# + V^\perp))$ is empty. We have proved that $H \notin \{V \cap \mathbf{e}_{j,m}^\perp;\ j \in J\}$.

Let us prove that $A_0 \subseteq H$. Consider $\alpha \in \mathbb{Z}^m \cap V \backslash \{\mathbf{e}_{0,m}\}$ such that $H^\# = \{x \in V;\ \langle \alpha, x\rangle \#0\}$. Let $K = \{k \in \mathbb{Z};\ k \leq \max\{|\langle \alpha, v_1\rangle|, |\langle \alpha, v_2\rangle|\}\}$ and remark that for any $x \in \mathbb{Z}^m \cap (((v_1 + H^\#)\Delta(v_2 + H^\#)) + V^\perp)$, we have $\langle \alpha, x\rangle \in K$. Hence $\mathbb{Z}^m \cap A \cap (((v_1 + H^\#)\Delta(v_2 + H^\#)) + V^\perp)$ is included into $\bigcup_{k\in K}\{x \in A;\ \langle \alpha, x\rangle = k\}$. From insecable lemma 9.2, we deduce that $A_0 \subseteq H$.

We have proved that $A_0 \subseteq S$ for any affine component A_0 of W. Therefore $W \subseteq S$. We deduce that $S' \subseteq S$.

Now, let us prove the converse inclusion $S \subseteq S'$. Consider a V-hyperplane $H_0 \in \mathcal{H}_0 = \text{bound}_V(X) \backslash (\bigcup_{j\in J}(V \cap \mathbf{e}_{j,m}^\perp))$. Let $\mathcal{H} = \text{bound}_V(X) \backslash \{H_0\}$. We denote by $\alpha_0 \in V \backslash \{\mathbf{e}_{0,m}\}$ a vector such that $H_0^{\#_0} = \{x \in V;\ \langle \alpha_0, x\rangle \#_0 0$ for any $\#_0 \in \{<,>\}$. Given $\# \in \{<,>\}^{\mathcal{H}}$ and $\#_0 \in \{<,>\}$, we denote by $(\#, \#_0)$ the sequence in $\{<,>\}^{\text{bound}_V(X)}$ naturally defined. Remark that for any sequence $\# \in \{<,>\}^{\mathcal{H}}$ and for any $\#_0 \in \{<,>\}$ such that $[C_{V,(\#,\#_0)}]_V \neq [\emptyset]_V$, there exists a unique $P_{\#,\#_0} \in \mathcal{P}_V(X)$ such that $(\#, \#_0) \in \mathcal{S}_{V,P_{\#,\#_0}}$.

Let us prove that there exists $\# \in \{<,>\}^{\mathcal{H}}$ such that $[C_{V,(\#,<)}]_V$ and $[C_{V,(\#,>)}]_V$ are both not equal to $[\emptyset]_V$, and such that $P_{\#,<} \neq P_{\#,>}$. By

contradiction, if for any $\# \in \{<,>\}^{\mathcal{H}}$ such that $[C_{V,(\#,<)}]_V$ and $[C_{V,(\#,>)}]_V$ are both not equal to $[\emptyset]_V$, we have $P_{\#,<} = P_{\#,>}$, decomposition theorem 12.4 shows that $\text{bound}_V(X) \subseteq \mathcal{H}$ which is impossible. Hence, there exists at least one sequence $\# \in \{<,>\}^{\mathcal{H}}$ such that $[C_{V,\#} \cap H_0^<]_V$ and $[C_{V,\#} \cap H_0^>]_V$ are both not equal to $[\emptyset]_V$ and such that $P_{\#,<} \neq P_{\#,>}$.

From the previous paragraph, we deduce that the semi-V-pattern $P_0 = P_{\#,<} \Delta P_{\#,>}$ is not empty. Moreover, as $P_{\#,<}$ and $P_{\#,>}$ are both (r,m)-detectable in X, we deduce that P_0 is also (r,m)-detectable in X and for any reachable state $q \in Q$, the set $(P_0)_q$ is well defined.

Let us prove that there exists a terminal component T such that $V_G(T) = V$ and such that $(P_{\#,<})_q \neq (P_{\#,>})_q$ for any state $q \in T$. As P_0 is not empty, there exists a (r,m)-decomposition $(\sigma_0, s) \in \rho_{r,m}^{-1}(P_0)$. By replacing σ_0 by a word in $\sigma_0.s^*$, we can assume that there exists a loop labelled by a word in s^+ on the state $q_0' = \delta(q_0, \sigma_0)$. In particular $\text{inv}_V((P_0)_{q_0'})$ is relatively prime with r and $\xi_{r,m}(s) \in (P_0)_{q_0'}$. From destruction lemma 13.14, we deduce that $P_{q_0'} \subseteq \xi_{r,m}(s) + \mathbb{Z}^m \cap V$ for any $P \in \mathcal{P}_V(X)$. As $(P_0)_{q_0'}$ is non empty, there exists $\#_0 \in \{<,>\}$ such that $(P_{\#,\#_0})_{q_0'} \neq \emptyset$. From proposition 14.11, we deduce that V is included in $\overrightarrow{\text{saff}}(X_{q_0'})$. As $X_{q_0'} \subseteq \Gamma_{r,m,\sigma_0}^{-1}(X)$, covering lemma 9.9 shows that V is an affine component of $\overrightarrow{\text{saff}}(X_{q_0'})$. Proposition 14.5 applied to $X_{q_0'}$ shows that there exists a terminal component T reachable from q_0' such that $V_G(T) = V$. Consider a state $q \in T$ and let us consider a path $q_0' \xrightarrow{\sigma_1} q$. From proposition 14.11, we deduce that there exists $P \in \mathcal{P}_V(X)$ such that $P_q \neq \emptyset$. Therefore $\gamma_{r,m,\sigma_1}^{-1}(P_{q_0'}) \not\emptyset$. From $P_{q_0'} \subseteq \xi_{r,m}(s) + \mathbb{Z}^m \cap V$, we deduce that $\gamma_{r,m,\sigma_1}^{-1}(\xi_{r,m}(s) + \mathbb{Z}^m \cap V)$. From the dense pattern corollary 9.23 we deduce that $\gamma_{r,m,\sigma_1}^{-1}((P_0)_{q_0'}) \neq \emptyset$. That means $(P_{\#,<})_q \neq (P_{\#,>})_q$ for any $q \in T$.

As there exists a loop on each state q of T, we deduce that P_q is relatively prime with r for any $P \in \mathcal{P}_V(X)$ and for any $q \in T$. Hence, there exists an integer n relatively prime with r such that $\text{inv}_V(P_q) \subseteq n.(\mathbb{Z}^m \cap V)$ for any $P \in \mathcal{P}_V(X)$ and for any $q \in T$.

From an immediate induction and lemma 11.10, we deduce that there exists a sharing of J into $J = J_< \cup J_>$ such that $[C_{V,\#} \cap C \cap H_0^{\#_0}]_V \neq [\emptyset]_V$ for any $\#_0 \in \{<,>\}$ where $C = \bigcap_{j \in J_<} \{x \in V;\ x[j] < 0\} \bigcap_{j \in J_>} \{x \in V;\ x[j] > 0\}$. In particular there exists a vector $v_{\#_0} \in C_{V,\#} \cap C \cap H_0^{\#_0}$ for each $\#_0 \in \{<,>\}$. By replacing $v_{\#_0}$ by a vector in $(\mathbb{N}\backslash\{0\}).v_{\#_0}$, we can also assume that $v_{\#_0} \in n.(\mathbb{Z}^m \cap V)$.

Let us show that there exists a (r,m)-sign vector $s \in S_{r,m}$ and a state $q \in T$ such that $\frac{s}{1-r} \in (P_0)_q$ and such that $s[j] = r-1$ for any $j \in J_<$ and such that $s[j] = 0$ for any $j \in J_>$. Consider a state $q' \in T$. As $(P_0)_{q'}$ is not empty, there exists a vector x is this set. As $v_{\#_0} \in \mathbb{Z}^m \cap V$ and $(P_0)_{q'}$ is a semi-V-pattern, we deduce that $x_k = x + k.n.v_{\#_0}$ is in $(P_0)_{q'}$ for any $k \in \mathbb{Z}$. As $v_{\#_0}[j] < 0$ for any $j \in J_<$ and $v_{\#_0}[j] > 0$ for any $j \in J$, we deduce that there exists $k \in \mathbb{N}$ enough larger such that $x_k[j] < 0$ for any $j \in J_<$ and such that $x_k[j] > 0$ for any $j \in J_>$. Let us consider a (r,m)-decomposition (σ, s) of x_k and remark that $s[j] = r-1$ for any $j \in J_<$ and $s[j] = 0$ for any $j \in J_>$.

Moreover, $\frac{s}{1-r} \in (P_0)_q$ where $q = \delta(q'_0, \sigma)$. As $(P_0)_q \neq \emptyset$, proposition 14.11 proves that $X_q \neq \emptyset$. As T is a terminal component and q is reachable from T, we deduce that $q \in T$.

Consider a (r,m)-decomposition $(\sigma_{\#_0}, s_{\#_0})$ of $\frac{s}{1-r} + v_{\#_0}$ for each $\#_0 \in \{<, >\}$. By replacing $\sigma_{\#_0}$ by a word in $\sigma_{\#_0}.s^*_{\#_0}$, as n is relatively prime with r, we can assume that $r^{|\sigma_{\#_0}|} \in 1 + n.\mathbb{N}$ for any $\#_0 \in \{<, >\}$. We denote by $w_{\#_0}$ the word $w_{\#_0} = \sigma^n_{\#_0}$.

Let us show that $s_< = s = s_>$. For any $j \in \{1, \ldots, m\} \backslash J$, as $V \cap \mathbf{e}^{\perp}_{j,m}$ is not a V-hyperplane, we deduce that $\mathbf{e}_{j,m} \in V^{\perp}$. That means $v[j] = 0$ for any $v \in V$. In particular $(\frac{s}{1-r} + v_{\#_0})[j] = \frac{s}{1-r}[j]$ and we deduce that $s_<[j] = s[j] = s_>[j]$. For any $j \in J_<$, as $s[j] = r - 1$ and $v_{\#_0}[j] < 0$, we get $s_{\#_0}[j] = r - 1 = s[j]$. Symmetrically, for any $j \in J_>$, we get $s_{\#_0}[j] = 0 = s[j]$. Therefore $s_< = s = s_>$.

Let us prove that $\gamma^{-1}_{r,m,w_{\#_0}}(P_q) = P_q$ for any $P \in \mathcal{P}_V(X)$ and for any $\#_0 \in \{<, >\}$. Let $P \in \mathcal{P}_V(X)$. Remark that $\gamma_{r,m,\sigma_{\#_0}}(x) \in x + \gamma_{r,m,\sigma_{\#_0}}(\mathbf{e}_{0,m}) + n.\mathbb{Z}^m$ for any $x \in \mathbb{Z}^m$. Hence $\gamma_{r,m,w_{\#_0}}(x) \in x + n.\mathbb{Z}^m$ for any $x \in \mathbb{Z}^m$. As $M_{q,P}$ is a n-mask, we deduce that $\gamma^{-1}_{r,m,w_{\#_0}}(M_{q,P}) = M_{q,P}$. Moreover, from $\frac{s}{1-r} \in (P_0)_q$ we deduce that $\frac{s}{1-r} \in A_q$. Hence $A_q = \frac{s}{1-r} + V$. So $\Gamma^{-1}_{r,m,\sigma_{\#_0}}(A_q) = r^{-|\sigma_{\#_0}|}.(\frac{s}{1-r} - \gamma_{r,m,\sigma_{\#_0}}(\mathbf{e}_{0,m})) + V$. Recall that $\rho_{r,m}(\sigma_{\#_0}, s) = \frac{s}{1-r} + v_{\#_0}$ and remark that $\rho_{r,m}(\sigma_{\#_0}, s) = \gamma_{r,m,\sigma_{\#_0}}(\mathbf{e}_{0,m}) + r^{|\sigma_{\#_0}|}.\frac{s}{1-r}$. We get $\Gamma^{-1}_{r,m,\sigma_{\#_0}}(A_q) = \frac{s}{1-r} - r^{-|\sigma_{\#_0}|}.v_{\#_0} + V = A_q$. An immediate induction show that $\Gamma^{-1}_{r,m,w_{\#_0}}(A_q) = A_q$. As $P_q = M_{q,P} \cap A_q$, we get $\gamma^{-1}_{r,m,w_{\#_0}}(P_q) = \gamma^{-1}_{r,m,w_{\#_0}}(M_{q,P}) \cap \Gamma^{-1}_{r,m,w_{\#_0}}(A_q) = M_{q,P} \cap A_q = P_q$. We have proved that $\gamma^{-1}_{r,m,w_{\#_0}}(P_q) = P_q$ for any $P \in \mathcal{P}_V(X)$ and for any $\#_0 \in \{<, >\}$.

Let us prove that $\delta(q, w^*_{\#_0}) \subseteq T$ for any $\#_0 \in \{<, >\}$. From the previous paragraph, we deduce that for any $k \in \mathbb{N}$, the set $\gamma^{-k}_{r,m,w_{\#_0}}((P_0)_q) = (P_0)_q$ is not empty. From proposition 14.11, we deduce that $\gamma^{-k}_{r,m,w_{\#_0}}(X_q)$ is also non empty. As T is a terminal component, we deduce that $\delta(q, w^k_{\#_0}) \in T$.

As T is a finite set, there exists a state $q_{\#_0} \in T$ such that there exists a path $q \xrightarrow{w^{r_{\#_0}}_{\#_0}} q_{\#_0}$ and a loop $q_{\#_0} \xrightarrow{w^{k_{\#_0}}_{\#_0}} q_{\#_0}$ where $r_{\#_0} \in \mathbb{N}$ and $k_{\#_0} \in \mathbb{N} \backslash \{0\}$.

From theorem 13.17, we deduce that there exists a vector $a \in \mathbb{Q}^m$ such that:

$$X_q = \bigcup_{\substack{P \in \mathcal{P}_V(X) \\ \#' \in \mathcal{S}_{V,P}(X)}} (P_q \cap (a + C_{V,\#'} + V^{\perp}))$$

As $\gamma^{-1}_{r,m,w_{\#_0}}(P_q) = P_q$ for any $P \in \mathcal{P}_V(X)$ and for any $\#_0 \in \{<, >\}$ we deduce the following equality for any $\#_0 \in \{<, >\}$ and for any $k \in r_{\#_0} + \mathbb{N}.k_{\#_0}$:

$$X_{q_{\#_0}} = \bigcup_{\substack{P \in \mathcal{P}_V(X) \\ \#' \in \mathcal{S}_{V,P}(X)}} (P_q \cap (\Gamma^{-1}_{r,m,w^k_{\#_0}}(a) + C_{V,\#'} + V^{\perp}))$$

As $P_{q_<} = P_{q_>}$ for any $P \in \mathcal{P}_V(X)$, we deduce that $q_< \sim^V q_>$. Hence $(q_<, q_>) \in I_{\mathcal{A}}(V)$.

Let us prove that $X_{q_{\#_0}} \cap (\frac{s}{1-r} + C_{V,\#} \cap C \cap H_0) = P_{q_{\#_0}} \cap (\frac{s}{1-r} + C_{V,\#} \cap C \cap H_0)$. Let us consider a vector $x \in (\frac{s}{1-r} + C_{V,\#} \cap C \cap H_0)$. By developing the expression $\Gamma^{-1}_{r,m,w^k_{\#_0}}(a)$, we deduce that $\lim_{k\to\infty} \Gamma^{-1}_{r,m,w^k_{\#_0}}(a) = \frac{s}{1-r} - \frac{v_{\#_0}}{r^{|\sigma_{\#_0}|}-1}$. As $v_{\#_0} \in C_{V,\#} \cap C \cap H_0^{\#_0}$ and $\frac{1}{r^{|\sigma_{\#_0}|}-1} \in \mathbb{Q}_+ \backslash \{0\}$, we deduce that there exists $k \in r_{\#_0} + \mathbb{N}.k_{\#_0}$ enough larger such that $x \in \Gamma^{-1}_{r,m,w^k_{\#_0}}(a) + C_{V,(\#,\#_0)} \cap C \cap H_0 + V^\perp$. Therefore $X_q \cap \{x\} = P_{\#_0} \cap \{x\}$ and we have proved that $X_{q_{\#_0}} \cap (\frac{s}{1-r} + C_{V,\#} \cap C \cap H_0) = P_{\#_0} \cap (\frac{s}{1-r} + C_{V,\#} \cap C \cap H_0)$.

We deduce that $(P_0)_q \cap (\frac{s}{1-r} + H_0) \cap (\frac{s}{1-r} + C_{V,\#} \cap C \cap H_0) \subseteq X_{q<} \Delta X_{q_>}$. Since $[C_{V,\#} \cap C \cap H_0^<]_V$ and $[C_{V,\#} \cap C \cap H_0^>]_V$ are both not equal to $[\emptyset]_V$, lemma 11.11 shows that $C_{V,\#} \cap C \cap H_0$ is a non H_0-degenerate H_0-polyhedron. Moreover, since $(P_0)_q \cap (\frac{s}{1-r} + H_0)$ is a non-empty semi-H_0-pattern, from lemma 12.2, we deduce that $\overrightarrow{\text{saff}}((P_0)_q \cap (\frac{s}{1-r} + H_0) \cap (\frac{s}{1-r} + C_{V,\#} \cap C \cap H_0)) = H_0$. Hence $H_0 \subseteq \overrightarrow{\text{saff}}(X_{q_<} \Delta X_{q_>})$. As $(q_<, q_>) \in I_{\mathcal{A}}(V)$, we also get $\overrightarrow{\text{saff}}(X_{q_<} \Delta X_{q_>}) \subseteq S'$. We deduce that $H_0 \subseteq S'$. We have proved that $S \subseteq S'$. □

From the previous proposition 14.17, theorem 14.6 and theorem 13.4, we deduce the following main theorem of this paper.

Theorem 14.18. *Let X be a Presburger-definable set represented by a serialized encoded FDVA, and let V be an affine component of $\overrightarrow{\text{saff}}(X)$. The boundary $\text{bound}_V(X) \backslash (\bigcup_{j=1}^m \{V \cap \boldsymbol{e}^\perp_{j,m}\})$ is computable in polynomial time.*

14.3.2 An example

Let us consider the set $X = \{x \in \mathbb{N}^2;\ x[1] \leq 2.x[2]\}$ given in figure 14.3.

The minimal FDVA $\mathcal{A}_{2,2}(X)$ that represents X is given in figure 14.4. We denote by $q_{-1} = \{x \in \mathbb{N}^2;\ x[1] \leq 2.x[2] - 1\}$, $q_0 = \{x \in \mathbb{N}^2;\ x[1] \leq 2.x[2]\}$ and $q_1 = \{x \in \mathbb{N}^2;\ x[1] \leq 2.x[2] + 1\}$ the states of this FDVA.

Remark that $T = \{q_{-1}, q_0, q_1\}$ is the unique terminal component. Moreover, the algorithm that computes the vector space associated to an untransient component provides $V_G(T) = \mathbb{Q}^2$. Remark that from proposition 14.5, we get $\overrightarrow{\text{saff}}(X) = V_T(T) = \mathbb{Q}^2$. That means $V = \mathbb{Q}^2$ is the only affine component of $\overrightarrow{\text{saff}}(X)$.

Let us prove that $\overrightarrow{\text{saff}}(X_{q_i} \Delta X_{q_j}) = H$ for any $i \neq j$. In figure 14.5, we have represented the FDVA Cartesian products of the FDVA $\mathcal{A}_{q_i}$ and the FDVA $\mathcal{A}_{q_j}$ that recognize the sets $X_{q_i} \Delta X_{q_j}$ where $i, j \in \{-1, 0, 1\}$. These FDVA (when $i \neq j$) have only one terminal component $T' = \{(X_{q_0} \Delta X_{q_1}), (X_{q_{-1}} \Delta X_{q_0})\}$ and we have $V_{G'}(T') = H$. Therefore $\overrightarrow{\text{saff}}(X_{q_i} \Delta X_{q_j}) = H$ for any $i \neq j$.

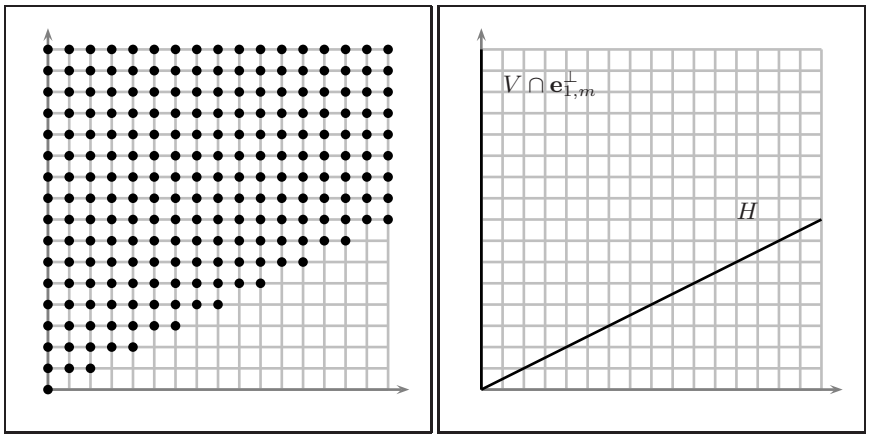

Fig. 14.3. On the left the Presburger-definable set $X = \{x \in \mathbb{N}^2;\ (x[1] \leq 2.x[2])$. On the right $\text{bound}_V(X)$ where $V = \mathbb{Q}^2$ and $H = \{x \in V;\ x[1] = 2.x[2]\}$.

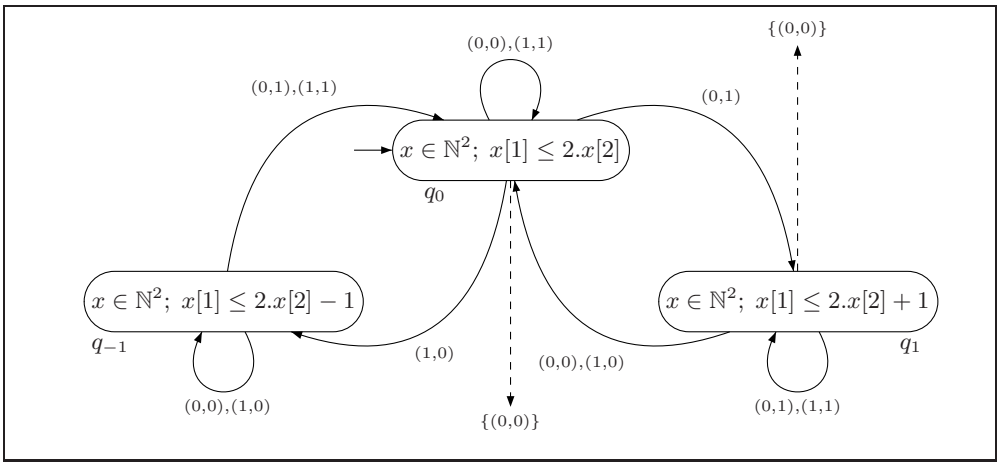

Fig. 14.4. The minimal FDVA $\mathcal{A}_{2,2}(\{x \in \mathbb{N}^2;\ x[1] \leq 2.x[2]\})$

Symmetrically, we get $\overrightarrow{\text{saff}}(X_{q_i} \Delta X_{q_j}) = H$ for any $i \neq j$. We deduce that $I_{\mathcal{A}}(V) = \{(q_i, q_j);\ i \neq j\}$ and $\bigcup_{(q_i,q_j) \in I_{\mathcal{A}}(V)} \overrightarrow{\text{saff}}(X_{q_i} \Delta X_{q_j}) = H$. From proposition 14.17, we get $\text{bound}_V(X) \backslash \{V \cap \mathbf{e}_{1,m}^{\perp}, V \cap \mathbf{e}_{2,m}^{\perp}\} = \{H\}$.

Now, just remark that the previous computation can be done in polynomial time from serialized encoded FDVA. Remark also that on this example $\text{bound}_V(X) = \{H, V \cap \mathbf{e}_{1,m}^{\perp}\}$.

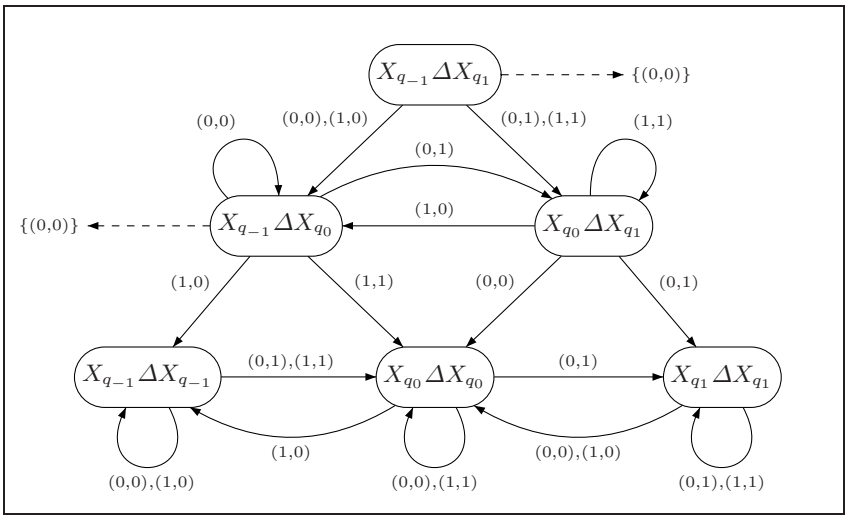

Fig. 14.5. The Cartesian product $\mathcal{A}'$ of $\mathcal{A}_{q_0}$ and $\mathcal{A}_{q_1}$ that represents the symmetrical difference $X_{q_0}\Delta X_{q_1}$ where X is represented by the FDVA $\mathcal{A}$ given in figure 14.4.

15

The polynomial time algorithm

In this section we provide a polynomial time algorithm for deciding if the set represented by a FDVA is Presburger-definable and in this case we provide in polynomial time a Presburger formula that defines the same set.

The algorithm is based on the fact that even if the set X represented by a FDVA $\mathcal{A}$ is not Presburger-definable, the algorithms developed in the previous sections can be applied in order to extract from $\mathcal{A}$ sets of the form $P \cap H^{\#}$ where P is a semi-V-pattern relatively prime with r included in a V-affine space and H is a V-hyperplane, and if X is Presburger definable then these sets are (r, m)-detectable in X and X is equal to a boolean combination of these sets.

In the remaining of this section we assume that $\mathcal{A}$ is a positive (r, m, w)-cyclic FDVA that represents a set $X_0 \subseteq \mathbb{N}^m$ in basis r and dimension m. Naturally these conditions are not restrictive thanks to the cyclic reduction provided by proposition 7.4 and thanks to the positive reduction given by proposition 7.5.

Since a positive final function F is such that $[F](q) \in \{\{\mathbf{e}_{0,m}\}, \emptyset\}$, without ambiguity such a function can be denoted as the set of principal states $q \in Q$ such that $[F](q) = \{\mathbf{e}_{0,m}\}$. In the sequel, a positive final function F is always denoted as a subset of Q.

The following proposition shows that given a set $X' \subseteq \mathbb{N}^m$ that can be represented by a FDVA of the form $\mathcal{A}^F$ where F is an unknown final function, the computation of a positive final function F' such that X' is represented by $\mathcal{A}^{F'}$ can be reduced the membership problem for X'.

Proposition 15.1. *Let $\mathcal{A}$ be a FDVA. We denote by $\mathcal{Y}$ the set of $\boldsymbol{e}_{0,m}$-eye Y such that Y is reachable for $[G]$ from the initial state. For any eye $Y \in \mathcal{Y}$, let us consider a word $\sigma_Y \in \Sigma_{r,m}^*$ such that $\delta(q_0, \sigma_Y) \in \ker_{\boldsymbol{e}_{0,m}}(Y)$. Any set $X' \subseteq \mathbb{N}^m$ such that there exists a final function F satisfying X' is represented by $\mathcal{A}^F$ is represented by $\mathcal{A}^{F'}$ where F' is the union of eyes $Y \in \mathcal{Y}$ such that $\rho_{r,m}(\sigma_Y, \boldsymbol{e}_{0,m}) \in X'$.*

Proof. Let X be the set represented by $\mathcal{A}^{F'}$ and let us prove that $X = X'$. Consider $x \in X$. Let $(\sigma, \mathbf{e}_{0,m})$ be a (r,m)-decomposition of x. There exists an eye $Y \in \mathcal{Y}$ such that $\delta(q_0, \sigma) \in Y$. Since $\delta(q_0, \sigma_Y) \in \ker_{\mathbf{e}_{0,m}}(Y)$, by replacing σ by a word in $\sigma.\mathbf{e}_{0,m}^*$, we can assume without loss of generality that $\delta(q_0, \sigma) = \delta(q_0, \sigma_Y)$. Since there exists a final function F such that X' is represented by $\mathcal{A}^F$, we deduce that $\gamma_{r,m,\sigma}^{-1}(X') = \gamma_{r,m,\sigma_Y}^{-1}(X')$. From $\rho_{r,m}(\sigma_Y, \mathbf{e}_{0,m}) \in X'$ and the previous equality, we get $\rho_{r,m}(\sigma, \mathbf{e}_{0,m}) \in X'$. Therefore $x \in X'$ and we have proved the inclusion $X \subseteq X'$. For the converse inclusion, let $x \in X'$. Consider a (r,m)-decomposition $(\sigma, \mathbf{e}_{0,m})$ of x and let $Y \in \mathcal{Y}$ such that $\delta(q_0, \sigma) \in Y$. By replacing σ by a word in $\sigma.\mathbf{e}_{0,m}^*$ since $\delta(q_0, \sigma_Y) \in \ker_s(Y)$, we can assume that $\delta(q_0, \sigma) = \delta(q_0, \sigma_Y)$. As $\gamma_{r,m,\sigma}^{-1}(X') = \gamma_{r,m,\sigma_Y}^{-1}(X')$ and $\rho_{r,m}(\sigma, \mathbf{e}_{0,m}) \in X'$, we get $\rho_{r,m}(\sigma_Y, \mathbf{e}_{0,m}) \in X'$. We have proved that $\delta(q_0, \sigma_Y) \in F'$. Thus $\delta(q_0, \sigma) \in F'$ and we have proved that $x \in X$. We have proved the other inclusion $X' \subseteq X$. □

Observe that we can decide in linear time if X_0 is empty. Thus, we can assume that X_0 is non-empty (otherwise we decide that X_0 is Presburger-definable and defined by the formula false). Theorem 14.6 proves that a non-empty semi-vector space S such that $\mathrm{saff}(X_0) = \xi_{r,m}(w) + S$ if X_0 is Presburger-definable is computable in polynomial time.

Let us fix an affine component V of S and let T_V be the finite union of terminal components $T \in \mathcal{T}_\mathcal{A}$ such that $V_G(T) = V$. By construction of the semi-affine space S, for any affine component V of S, there exists at least one terminal component T such that $V_G(T) = V$.

Observe that if X_0 is Presburger-definable then $\mathbb{Z}^m \cap (\xi_{r,m}(w) + V)$ is non empty from the dense component lemma 12.1. Since this property can be decided in polynomial time by proposition 8.15, we can assume that this set is non-empty (otherwise we decide that X_0 is not Presburger-definable) and from this same proposition we compute in polynomial time a vector $a_0 \in \mathbb{Z}^m \cap (\xi_{r,m}(w) + V)$.

Theorem 14.14 proves that we can compute in polynomial time a V-vector lattice M included in $\mathbb{Z}^m$ such that if X_0 is Presburger-definable then $M = \mathrm{inv}_V(X_0)$ is relatively prime with r and $|\mathbb{Z}^m \cap V / \mathrm{inv}_V(X_0)|$ is bounded by the number of principal states of $\mathcal{A}$. Theorem 8.10 proves that we can compute in polynomial time the characteristic sequence n_1, ..., n_d of M in $\mathbb{Z}^m \cap V$ and a $\mathbb{Z}$-basis v_1, .., v_d of $\mathbb{Z}^m \cap V$ such that $n_1.v_1$, ..., $n_d.v_d$ is a $\mathbb{Z}$-basis of M. Observe that $|\mathbb{Z}^m \cap V/M| = n_1 \dots n_d$. We can assume that $n_1 \dots n_d$ is relatively prime with r and it is bounded by the number of principal states of $\mathcal{A}$ (otherwise we decide that X_0 is not Presburger-definable). Let B be the finite set $B = \{a_0 + \sum_{i=1}^d k_i.v_i;\ 0 \leq k_1 < n_1 \wedge \dots \wedge 0 \leq k_d < n_d\}$. Observe that the cardinal of B is equal to $n_1 \dots n_d$. Thus B is computable in polynomial time. Moreover, by definition of $\mathrm{inv}_V(X_0) = M$, we deduce that if X_0 is Presburger-definable, for any semi-V-pattern $P \in \mathcal{P}_V(X_0)$, there exists a subset $B' \subseteq B$ such that $P = B' + M$.

Theorem 13.12 shows that we can compute in polynomial time a partition B_0, B_1, ..., B_n of B such that a semi-V-pattern P of the form $P = B' + M$ where $B' \subseteq B$ is represented by a FDVA of the form $\mathcal{A}^F$ if and only if there exists $J \subseteq \{1, \ldots, n\}$ such that $B' = \bigcup_{j \in J} B_j$. Let $i \geq 1$. Observe that there exists a final function F such that $\mathbb{N}^m \cap (B_i + M)$ is represented by $\mathcal{A}^F$. Since we can decide in polynomial time if a vector x is in $\mathbb{N}^m \cap (B_i + M)$, proposition 15.1 proves that we can compute in polynomial time a positive final function Q_i such that $\mathbb{N}^m \cap (B_i + M)$ is represented by $\mathcal{A}^{Q_i}$.

Note that $Z_i = X_0 \cap (B_i + M) = X_0 \cap (\mathbb{N}^m \cap (B_i + M))$ is represented by the FDVA $\mathcal{A}^{F_0 \cap Q_i}$. Theorem 14.6 proves that a semi-vector space S_i such that $\mathrm{saff}(Z_0) = \xi_{r,m}(w) + S_i$ if X_0 is Presburger-definable is computable in polynomial time. Let us consider the set I of $i \in \{1, \ldots, n\}$ such that $V \subseteq S_i$.

Let us show that if X_0 is Presburger-definable, then any state $q \in Q_i$ is co-reachable from T_V. Consider a state $q \in Q_i$, there exists a word $\sigma \in \Sigma_{r,m}^*$ such that $\delta(q_0, \sigma) = q$ and $\rho_{r,m}(\sigma, \mathbf{e}_{0,m}) \in B_i + M$. In particular $\rho_{r,m}(\sigma, \mathbf{e}_{0,m}) \in a_0 + V$. Considering a semi-$V$-pattern $P \in \mathcal{P}_V(X) \backslash \{\emptyset\}$ and recall that since P is (r, m)-detectable in X (from corollary 13.9), the semi-V-pattern P is relatively prime with r and included into the V-affine space $a_0 + V$ (from lemma 9.20). The dense pattern corollary 9.23 proves that $\gamma_{r,m,\sigma}^{-1}(P) \neq \emptyset$. Proposition 14.4 proves that if X_0 is Presburger-definable, then T_V is co-reachable from q. Therefore, we have proved that any state $q \in Q_i$ is co-reachable from T_V if X_0 is Presburger-definable. Since this property is decidable in polynomial time, we can assume that it is verified (otherwise we decide that X_0 is not Presburger-definable).

Now, let us prove that if X_0 is Presburger-definable then $F_0 \cap T_V \subseteq \bigcup_{i \in I} Q_i$. Consider $q \in F_0 \cap T_V$. There exists a path $q_0 \xrightarrow{\sigma} q$ with $\sigma \in \Sigma_{r,m}^*$. Since $q \in F_0$, we get $\rho_{r,m}(\sigma, \mathbf{e}_{0,m}) \in X_0$. Theorem 13.17 proves that there exists $P \in \mathcal{P}_V(X_0) \backslash \{\emptyset\}$ such that $\rho_{r,m}(\sigma, \mathbf{e}_{0,m}) \in P$. Since there exists a $J \subseteq \{1, \ldots, n\}$ such that $P = \bigcup_{j \in J} B_j + M$, we deduce that there exists $j \in \{1, \ldots, n\}$ such that $\rho_{r,m}(\sigma, \mathbf{e}_{0,m}) \in B_j + M$. Theorem 13.17 proves that in this case $\overrightarrow{\mathrm{saff}}(Z_j) = V$. Thus $j \in J$ and $q \in \bigcup_{i \in I} Q_i$ and we have proved that $F_0 \cap T_V \subseteq \bigcup_{i=1}^n Q_i$. Since this property is decidable in polynomial time, we can assume that it is true (otherwise we decide that X_0 is not Presburger-definable).

If X_0 is Presburger-definable then Z_i is Presburger-definable and if $i \in I$ then $[Z_i]^V = V$ and in this case $\mathcal{P}_V(X_0) \backslash \{\emptyset\} = \{B_i + M\}$ since for any semi-V-pattern $P \in \mathcal{P}_V(X_0)$, there exists $J \subseteq \{1, \ldots, n\}$ such that $P = \bigcup_{j \in J} B_j + M$ (recall that corollary 13.9 proves that any semi-V-pattern $P \in \mathcal{P}_V(X_0)$ is (r, m)-detectable in X_0). Theorem 14.18 provides a polynomial time algorithm for computing a finite set $\mathcal{H}_i$ of vector spaces such that if X_0 is Presburger-definable then $\mathrm{bound}_V(Z_i) \backslash \bigcup_{i=1}^m \{V \cap \mathbf{e}_{i,m}^{\perp}\} = \mathcal{H}_i$. We can assume that $\mathcal{H}_i$ is a set of V-hyperplanes (otherwise we decide that X_0 is not Presburger-definable). Proposition 14.15 shows that if X_0 is Presburger-definable then for any $H \in \mathcal{H}_i$, there exists $\#_{i,H} \in \{\geq, >\}$ such that $(B_i + M) \cap (\xi_{r,m}(w) +$

$H^{\#_{i,H}} + V^{\perp}$) is represented by a FDVA of the form $\mathcal{A}^F$. Since we can decide this property in polynomial time thanks to proposition 14.16, we can assume that such a relation $\#_{i,H}$ exists. As we can decide in polynomial time if a vector x is in $\mathbb{N}^m \cap (B_i + M) \cap (\xi_{r,m}(w) + H^{\#_{i,H}} + V^{\perp})$, proposition 15.1 proves that we can compute in polynomial time a positive final function $Q_{i,H}$ such that $\mathbb{N}^m \cap (B_i + M) \cap (\xi_{r,m}(w) + H^{\#_{i,H}} + V^{\perp})$ is represented by $\mathcal{A}^{Q_{i,H}}$.

Now observe that if X_0 is Presburger-definable, lemma 13.8 proves that there exists a boolean combination Z_i' of the set $\mathbb{N}^m \cap (B_i + M)$ and the sets $\mathbb{N}^m \cap (B_i + M) \cap (\xi_{r,m}(w) + H^{\#_{i,H}} + V^{\perp})$ such that $[X_0 \Delta Z_i']^V = [\emptyset]^V$. Since any state in Q_i is co-reachable from T_V, if such a boolean combination exists, there exists a boolean combination Q_i' of the set Q_i and the sets $Q_{i,H}$ where $H \in \mathcal{H}_i$ such that $Q_i' \cap T_V = F_0 \cap T_V$. In particular $F_0 \cap T_V$ is a boolean combination of the set $Q_i \cap T_V$ and the sets $Q_{i,H} \cap T_V$. Since this last property is decidable in polynomial time by the lemma 2.1 we can assume that such a boolean combination exists (otherwise we decide that X_0 is not Presburger-definable). This same lemma 2.1 also proves that we can compute in polynomial time a boolean formula ψ_i such that $q \in F_0 \cap T_V$ is defined by $\psi_i(q \in Q_i \cap T_V, (q \in Q_{i,H} \cap T_V)_{H \in \mathcal{H}_i})$. Observe that the set Q_i' defined by $q \in Q_i'$ if $\psi_i(q \in Q_i, (q \in Q_{i,H})_{H \in \mathcal{H}_i})$ is computable in polynomial time. Moreover, the set Z_i' represented by $\mathcal{A}^{Q_i'}$ is defined by the Presburger-formula ϕ_i:

$$\phi_i(x) := (x \in \mathbb{N}^m \cap (B_i + M)) \wedge \psi_i(\text{true}, (x \in a_0 + H^{\#_{i,H}} + V^{\perp})_{H \in \mathcal{H}_i})$$

Now, let us consider the Presburger formula $\phi' := \bigvee_{i \in I} \phi_i$ and the positive final function $Q' = \bigcup_{i \in I} Q_i'$. Remark that the set $Z' = \bigcup_{i \in I} Z_i'$ is represented by the FDVA $\mathcal{A}^{Q'}$ and it is defined by the Presburger formula ϕ'.

Note that $X_1 = X \Delta Z'$ is the set represented by the FDVA $\mathcal{A}^{F_1}$ where $F_1 = F_0 \Delta F'$ and X_0 is Presburger-definable if and only if X_1 is Presburger-definable. Moreover, by construction of F', any state $q \in F'$ is co-reachable from T_V and $F' \cap T_V = F_0 \cap T_V$. That means the set of strongly-connected components of $\mathcal{A}^{F_1}$ reachable from the initial state and co-reachable from a final state is strictly included in the strongly connected components of $\mathcal{A}^{F_0}$ satisfying this same property.

Thus, by repeating the previous constructions we obtain a finite sequence X_0, X_1,..., X_k where k is bounded by the number of strongly connected components of $\mathcal{A}$, and a sequence ϕ_1, ..., ϕ_k of Presburger-formulas ϕ_i defining $X_{i-1} \Delta X_i$ such that $X_k = \emptyset$. Note that X_0 is therefore Presburger-definable since we have the following equality:

$$X_0 = (X_0 \Delta X_1) \Delta \cdots \Delta (X_{n-1} \Delta X_k)$$

Moreover, from ϕ_1, ..., ϕ_k we get a Presburger-formula ϕ that defines X.

We have proved the following theorem.

Theorem 15.2. *Let $X \subseteq \mathbb{Z}^m$ be the set represented by a FDVA $\mathcal{A}$ in basis r and in dimension m. We can decide in polynomial time if X is Presburger-*

definable. Moreover, in this case, we can compute in polynomial time a Presburger-formula ϕ that defines X.

References

[BC96] 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.

[Ber77] 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.

[BFL04] Sébastien Bardin, Alain Finkel, and Jérôme Leroux. Faster acceleration of counter automata. In *Proc. 10th Int. Conf. Tools and Algorithms for the Construction and Analysis of Systems (TACAS'2004) Barcelona, Spain, Mar. 2004*, volume 2988 of *Lecture Notes in Computer Science*, pages 576–590. Springer, 2004.

[BFLP03] 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.

[BGP99] Tevfik Bultan, Richard Gerber, and William Pugh. Model-checking concurrent systems with unbounded integer variables: symbolic representations, approximations, and experimental results. *ACM Transactions on Programming Languages and Systems*, 21(4):747–789, 1999.

[BHMV94] 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.

[Fas] FAST homepage. `http://www.lsv.ens-cachan.fr/fast/`.

[FO97] Laurent Fribourg and Hans Olsén. Proving safety properties of infinite state systems by compilation into Presburger arithmetic.

In *Proc. 8th Int. Conf. Concurrency Theory (CONCUR'97), Warsaw, Poland, Jul. 1997*, volume 1243 of *Lecture Notes in Computer Science*, pages 213–227. Springer, 1997.

[Fri00] Laurent Fribourg. Petri nets, flat languages and linear arithmetic. Invited lecture. In M. Alpuente, editor, *Proc. 9th Int. Workshop. on Functional and Logic Programming (WFLP'2000), Benicassim, Spain, Sept. 2000*, pages 344–365, 2000. Proceedings published as Ref. 2000.2039, Universidad Politécnica de Valencia, Spain.

[GBD02] 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.

[GS66] Seymour Ginsburg and Edwin H. Spanier. Semigroups, Presburger formulas and languages. *Pacific J. Math.*, 16(2):285–296, 1966.

[Kla04] 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.

[KMS02] Nils Klarlund, A. Møller, and M. I. Schwartzbach. MONA implementation secrets. *Int. J. of Foundations Computer Science*, 13(4):571–586, 2002.

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

[Lat04] Louis Latour. From automata to formulas: Convex integer polyhedra. In *Proc. 19th Annual IEEE Symposium on Logic in Computer Science (LICS'04), Turku, Finland July 2004*, pages 120–129. IEEE Comp. Soc. Press, 2004.

[Ler03] Jérôme Leroux. *Algorithmique de la vérification des systèmes à compteurs. Approximation et accélération. Implémentation de l'outil Fast.* PhD thesis, Ecole Normale Supérieure de Cachan, Laboratoire Spécification et Vérification. CNRS UMR 8643, décembre 2003.

[Ler04] 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.

[Lug04] Denis Lugiez. From automata to semilinear sets: a solution for polyhedra and even more general sets. In *Proc. 9th. Int. Conf. on Implementation and Application of Automata (CIAA'04), Queen's University, Kingston, Ontario, Canada, Jul. 2004*, volume 3317

of *Lecture Notes in Computer Science*, pages 321–322. Springer, 2004.

[Muc91] A. Muchnik. Definable criterion for definability in presburger arithmetic and its applications. (in russian), preprint, Institute of new technologies, 1991.

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

[Pre29] 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.

[RV02] 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.

[Sch87] Alexander Schrijver. *Theory of Linear and Integer Programming*. John Wiley and Sons, New York, 1987.

[Tau92] Patrice Tauvel. *Mathématiques générales pour l'agrégation*. MASSON, Paris Milan Barcelone Bonn, 1992.

[WB95] 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.

[WB00] 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.

Index

Notations