Theoretical Computer Science 416 (2012) 1–16

Contents lists available at SciVerse ScienceDirect

Theoretical Computer Science

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

Quasi-polynomials, linear Diophantine equations and semi-linear sets[☆]

Flavio D'Alessandro[a,b,*], Benedetto Intrigila[c], Stefano Varricchio[c,1]

[a] Dipartimento di Matematica, Università di Roma "La Sapienza", Piazzale Aldo Moro 2, 00185 Roma, Italy
[b] Department of Mathematics, Boğaziçi University, 34342 Bebek, Istanbul, Turkey
[c] Dipartimento di Matematica, Università di Roma "Tor Vergata", via della Ricerca Scientifica, 00133 Roma, Italy

ARTICLE INFO

Article history:
Received 27 May 2010
Received in revised form 15 October 2011
Accepted 20 October 2011
Communicated by D. Perrin

Keywords:
Semi-linear set
Linear Diophantine equation
Vector partition function

ABSTRACT

We investigate the family of semi-linear sets of $\mathbb{N}^t$ and $\mathbb{Z}^t$. We study the growth function of semi-linear sets and we prove that such a function is a piecewise quasi-polynomial on a polyhedral partition of $\mathbb{N}^t$. Moreover, we give a new proof of combinatorial character of a famous theorem by Dahmen and Micchelli on the partition function of a system of Diophantine linear equations.

1. Introduction

Semi-linear sets play a role in the study of several problems of Mathematics and Computer Science and they have been widely investigated in the last three decades. Two fundamental results describe the structure of such sets: a theorem by Ginsburg and Spanier [18] that characterizes semi-linear sets of $\mathbb{N}^t$ and of $\mathbb{Z}^t$ as the sets that are first order definable in the Presburger Arithmetic over $\mathbb{N}$ and over $\mathbb{Z}$ respectively; a theorem [16] by Eilenberg and Schützenberger that characterizes such sets as finite and disjoint unions of *simple sets*, that is unambiguous linear sets of $\mathbb{N}^t$ and of $\mathbb{Z}^t$ respectively. It is worth mentioning that the set of non-negative solutions of a system of Diophantine linear equations is a semi-linear set, a first remarkable bridge, obtained by Ginsburg, between the concepts we consider in this paper (see [17]). Now we want to introduce some mathematical notions that will be used in the paper. The concepts of *quasi-polynomial* and that of *piecewise quasi-polynomial* are among the most relevant in this work. A quasi-polynomial is a map $F : \mathbb{N}^t \to \mathbb{N}$ (resp. $F : \mathbb{Z}^t \to \mathbb{N}$) defined by a finite family of polynomials in t variables $x_1, \ldots, x_t$, with rational coefficients:

$$\{p_{(d_1,d_2,\ldots,d_t)} \mid d_1, \ldots, d_t \in \mathbb{N},\ 0 \le d_i < d\},$$

such that every polynomial of the family is indexed by a vector $(d_1, d_2, \ldots, d_t)$ whose components are remainders with respect to a fixed positive integer d. Then, for every $(n_1, \ldots, n_t) \in \mathbb{N}^t$ (resp. $(n_1, \ldots, n_t) \in \mathbb{Z}^t$), the value of F computed at $(n_1, \ldots, n_t)$ is given by:

$$F(n_1, \ldots, n_t) = p_{(d_1,d_2,\ldots,d_t)}(n_1, \ldots, n_t),$$

where, for every $i = 1, \ldots, t,\ d_i$ is the remainder of the division of n_i by d.

☆ This work was partially supported by MIUR project "Aspetti matematici e applicazioni emergenti degli automi e dei linguaggi formali". The first author also acknowledges the partial support of fundings "Facoltà di Scienze MM. FF. NN. 2008" of the University of Rome "La Sapienza".

* Correspondence to: Dipartimento di Matematica, Università di Roma "La Sapienza", Piazzale Aldo Moro 2, 00185 Roma, Italy. Tel.: +39 06 49 91 37 67.
E-mail addresses: dalessan@mat.uniroma1.it (F. D'Alessandro), intrigil@mat.uniroma2.it (B. Intrigila).

1 Stefano Varricchio suddenly passed away on August 20th 2008. At that moment, many topics of the present paper had been discussed at length with him. So we want to include his name as an author of this work. Stefano Varricchio was a best friend of both of us. For a scientific and personal memory, see D'Alessandro and A. de Luca (2008) [8].

0304-3975/$ – see front matter
doi:10.1016/j.tcs.2011.10.014

The second concept mentioned above is that of piecewise quasi-polynomial. A map $F : \mathbb{N}^t \to \mathbb{N}$ (resp., $F : \mathbb{Z}^t \to \mathbb{N}$) is said to be a *piecewise quasi-polynomial on polyhedral regions in* $\mathbb{N}^t$ (resp., $\mathbb{Z}^t$) if there exist a partition of $\mathbb{N}^t$ (resp., $\mathbb{Z}^t$) into a finite number of polyhedral regions $P_1, \ldots, P_s$, determined by hyperplanes with rational equations, and a finite number of quasi-polynomials $q_1, \ldots, q_s$, where, for any $(n_1, \ldots, n_t)$ one has:

$$F(n_1, \ldots, n_t) = q_j(n_1, \ldots, n_t),$$

where j is the index of the polyhedron P_j such that $(n_1, \ldots, n_t) \in P_j$.

An interesting application of quasi-polynomials has been given in the theory of Diophantine linear equations. In [5], Bell proved that the number of non-negative solutions of a Diophantine linear equation with non-negative coefficients is a quasi-polynomial. Bell's result has been subsequently extended to systems of Diophantine linear equations in [12] by Dahmen and Micchelli. It is appropriate to describe such result in more details.

Let $A \in \mathbb{Z}^{t\times n}$ be a matrix of integers and let $\mathbf{b} \in \mathbb{Z}^t$ be a vector of integers, with $n \geq t$. Let $A\mathbf{x} = \mathbf{b}$ be the system of Diophantine linear equations defined by A and $\mathbf{b}$, where $\mathbf{x} = (x_1, \ldots, x_n)$ stands for the vectors of the unknowns of the system. Under suitable conditions on A (see Section 4), one can prove that, for every vector $\mathbf{b} \in \mathbb{Z}^t$, the system $A\mathbf{x} = \mathbf{b}$ has a finite number of non-negative solutions. Therefore, one can associate with the system a function $\mathcal{S}_A : \mathbb{Z}^t \longrightarrow \mathbb{N}$ that maps every vector $\mathbf{b} \in \mathbb{Z}^t$, into the number $\mathcal{S}_A(\mathbf{b})$ of all non-negative solutions of $A\mathbf{x} = \mathbf{b}$. This function is called the *partition function* of the vector $\mathbf{b}$ (see [13–15]). In the paper mentioned above, Dahmen and Micchelli proved that $\mathcal{S}_A$ is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{Z}^t$, where the polyhedra of such partition are polyhedral cones with apex in $\mathbf{0}^t$ (*conic regions*, for short). The result above is obtained by making use of notions and techniques of the theory of *box splines*. Further investigations are in [13,14,28], where important theorems on the algebraic and combinatorial structure of the partition function have been obtained.

Moreover, such results have also important constructive aspects which make possible to have efficient algorithms to compute in several cases the partition functions as well as related functions. As a relevant example, it is worth mentioning that in 1993, Barvinok [3] found an algorithm to count integer points inside polyhedra. When the dimension is fixed the algorithm can count the number of lattice points in a polytope in polynomial time on the size of the input. Other interesting results can be found in [1,2].

In this theoretical setting, it is worth mentioning that, in a previous paper [10], we have focused our attention on Diophantine systems $A\mathbf{x} = \mathbf{b}$, where the entries of A and of $\mathbf{b}$ respectively are non-negative numbers. In this case, for every vector $\mathbf{b}$, the number of non-negative solutions of the system $A\mathbf{x} = \mathbf{b}$ is obviously finite so that the function $\mathcal{S}_A$ is well defined. For this case, a description of the partition function in terms of piecewise quasi-polynomials on conic regions in $\mathbb{N}^t$ has been given in [10] with a purely combinatorial proof. Another and different proof of this result has been also obtained in [27].

The concepts of quasi-polynomial and piecewise quasi-polynomial have been also used in Formal Language Theory, where an exact description of the counting and of the growth function of bounded regular languages [24] and of bounded context-free languages [9,10] is given in terms of quasi-polynomials. In this context, another result proven in [10], perhaps of some interest, is that the Parikh counting function of a bounded context-free language is a piecewise quasi-polynomial on polyhedral regions. Moreover, the latter result is effective: indeed, starting from the grammar that generates such a language, one can effectively construct a piecewise quasi-polynomial on polyhedral regions that describes the Parikh counting function of the language.

Now we would like to describe the results obtained in the present paper. They can be synthesized as follows:

- We study the *growth function* of semi-linear sets and we prove that such function is a *piecewise quasi-polynomial on polyhedral regions in* $\mathbb{N}^t$.
- We give a new proof of *combinatorial character* of a version of the theorem of Dahmen and Micchelli.

Let us give a short description of our results. The first result concerns the growth function of semi-linear sets. If X is a subset of $\mathbb{N}^t$ or $\mathbb{Z}^t$, we define the growth function of X as the function $\mathcal{G}_X : \mathbb{N}^t \longrightarrow \mathbb{N}$ which associates with non-negative integers $n_1, \ldots, n_t$, the number $\mathcal{G}_X(n_1, \ldots, n_t)$ of all the elements $(x_1, \ldots, x_t) \in X$ such that:

$$\begin{cases} |x_1| & \leq n_1 \\ \quad . & \quad . \\ \quad . & \quad . \\ \quad . & \quad . \\ |x_t| & \leq n_t. \end{cases}$$

The function $\mathcal{G}_X$ seems to be a natural way to count the number of points of X. Indeed, in case X lies in $\mathbb{N}^t$ (resp. $\mathbb{Z}^t$), $\mathcal{G}_X$ counts the number of points of X lying in larger and larger hyper-parallelepipeds, starting from the origin of $\mathbb{N}^t$ (resp. centered at the origin of $\mathbb{Z}^t$). In this paper, we prove that, given a semi-linear set X of $\mathbb{N}^t$ (resp., $\mathbb{Z}^t$), its growth function $\mathcal{G}_X$ is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$. Moreover, this theorem can be reformulated in a *"language-theoretic"* way. More precisely, we prove that there exists a finite partition of $\mathbb{N}^t$ in simple sets such that the function $\mathcal{G}_X$ is a polynomial on each simple set of the partition. Finally, we show that the univariate version of $\mathcal{G}_X$ is ultimately a quasi-polynomial.

As the second main result of this paper, we provide a version of the theorem of Dahmen and Micchelli. By using the previous description of the growth function of semi-linear sets of $\mathbb{N}^t$ and of $\mathbb{Z}^t$ as well as some deep results from the theory of semi-linear sets, we prove that the partition function of a system $A\mathbf{x} = \mathbf{b}$, where $A \in \mathbb{Z}^{t\times n}$, $\mathbf{b} \in \mathbb{Z}^t$, is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{Z}^t$. Moreover, also in this case, we provide a formulation, of *"language-theoretic"* character, of this theorem, by proving that there exists a finite partition of $\mathbb{Z}^t$ in simple sets such that the function $\mathcal{S}_A$ is a polynomial on each simple set of the partition.

We would like to emphasize the fact that the study of the partition function of Diophantine systems of linear equations (*cf.* [12–14,27]) has required *highly non trivial* techniques of algebraic and geometrical nature. On the other hand, by taking advantage of the theory of semi-linear sets, we present proofs of these results which appears to be new and of elementary character.

Finally we remark that all the theorems of this paper are effective. In particular, if X is a semi-linear set of $\mathbb{N}^t$ or $\mathbb{Z}^t$, starting from a representation of X, we are able to effectively construct a polyhedral partition of $\mathbb{N}^t$ and a family of quasi-polynomials that describe the growth function of X as a piecewise quasi-polynomial. Similarly, starting from a matrix A, with integer entries, we are able to effectively construct a polyhedral partition of $\mathbb{Z}^t$ and a family of quasi-polynomials that describe the partition function $\mathcal{S}_A$ as a piecewise quasi-polynomial.

The paper is organized as follows. In Section 2, we recall some basic notions and results on the structures used in this investigation: semi-linear sets, convex polyhedra, quasi-polynomials and piecewise quasi-polynomials, as well as some theorems on the partition functions of systems of Diophantine linear equations. In Section 3, we will study the growth functions of semi-linear sets of $\mathbb{N}^t$ and of $\mathbb{Z}^t$ while, in Section 4, the version mentioned above of the theorem of Dahmen and Micchelli is presented.

Some of the results of this paper were presented at WORDS 2009 [11].

2. Preliminaries and basic definitions

2.1. Semi-linear sets

The aim of this section is to recall some results about semi-linear sets of the free commutative monoid and the free commutative group. The free abelian monoid and the free abelian group on k generators are respectively identified with $\mathbb{N}^k$ and $\mathbb{Z}^k$ with the usual additive structure. The operation of addition is extended from elements to subsets: if $X, Y \subseteq \mathbb{N}^k$ (resp. $X, Y \subseteq \mathbb{Z}^k$), $X + Y \subseteq \mathbb{N}^k$ (resp. $X + Y \subseteq \mathbb{Z}^k$) is the set of all sums $\mathbf{x} + \mathbf{y}$, where $\mathbf{x} \in X$, $\mathbf{y} \in Y$. Let $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ be a finite subset of $\mathbb{N}^k$ (resp., $\mathbb{Z}^k$). Then we denote by $B^\oplus$ the submonoid of $\mathbb{N}^k$ (resp., $\mathbb{Z}^k$) generated by B, that is

$$B^\oplus = \mathbf{b}_1^\oplus + \cdots + \mathbf{b}_n^\oplus = \{m_1\mathbf{b}_1 + \cdots + m_n\mathbf{b}_n \mid m_i \in \mathbb{N}\}.$$

The following definitions are useful.

Definition 1. Let X be a subset of $\mathbb{N}^k$ (resp. $\mathbb{Z}^k$). Then

1. X is *linear* in $\mathbb{N}^k$ (resp. $\mathbb{Z}^k$) if
$$X = \mathbf{a} + \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}^\oplus,$$
where $\mathbf{a}, \mathbf{b}_1, \ldots, \mathbf{b}_n$ are vectors of $\mathbb{N}^k$ (resp. $\mathbb{Z}^k$).
2. X is *simple* in $\mathbb{N}^k$ (resp. $\mathbb{Z}^k$) if the vectors $\mathbf{a}, \mathbf{b}_1, \ldots, \mathbf{b}_n$ are linearly independent in $\mathbb{Q}^k$;
3. X is *semi-linear* in $\mathbb{N}^k$ (resp. $\mathbb{Z}^k$) if X is a finite union of linear sets in $\mathbb{N}^k$ (resp. $\mathbb{Z}^k$);
4. X is *semi-simple* in $\mathbb{N}^k$ (resp. $\mathbb{Z}^k$) if X is a finite disjoint union of simple sets in $\mathbb{N}^k$ (resp. $\mathbb{Z}^k$).

In the definition of simple set, the vector $\mathbf{a}$ and those of the set $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ shall be called a *representation* of X.

There exists a classical and important connection between the concept of semi-linear set and the *Presburger arithmetic*. Denote by $\mathcal{Z} = \langle \mathbb{Z}; =; <; +; 0; 1\rangle$ and by $\mathcal{N} = \langle \mathbb{N}; =; +; 0; 1\rangle$ respectively the *standard* and the *positive Presburger arithmetic*. Given a subset X of $\mathbb{N}^k$ (resp. $\mathbb{Z}^k$), we say that X is *first-order definable* in $\mathcal{N}$ (resp. $\mathcal{Z}$), or a *Presburger set* of $\mathbb{N}^k$ (resp. $\mathbb{Z}^k$), if

$$X = \{(x_1, \ldots, x_k) \mid P(x_1, \ldots, x_k) \text{ is true}\},$$

where P is a Presburger formula (with at most k free variables) over $\mathbb{N}$ (resp. $\mathbb{Z}$).

The following characterization of semi-linear sets holds.

Theorem 1. *Given a subset X of $\mathbb{N}^k$ (resp. $\mathbb{Z}^k$), the following assertions are equivalent:*

1. *X is first-order definable in $\mathcal{N}$ (resp. $\mathcal{Z}$);*
2. *X is semi-linear in $\mathbb{N}^k$ (resp. $\mathbb{Z}^k$);*
3. *X is semi-simple in $\mathbb{N}^k$ (resp. $\mathbb{Z}^k$).*

The equivalence of Conditions 1 and 2 has been proved by Ginsburg and Spanier in [18]. The equivalence of Conditions 2 and 3 has been proven by Eilenberg and Schützenberger in [16] in the larger context of finitely generated commutative monoids. In [20], independently, Ito proved the equivalence mentioned above in $\mathbb{N}^t$. Given a monoid M, a subset of M is *rational* if it is obtained from finite subsets of M by applying finitely many times the rational operations, that is, the set union, the product, and the *Kleene closure* operator. Obviously, a semi-linear set of $\mathbb{N}^k$ or $\mathbb{Z}^k$ is rational but one can prove that the opposite is true.

For a recent treatment of the subject, see Choffrut and Frigeri [6,7].

Observe that Theorem 1 is effective. Indeed, one can effectively represent a semi-linear set X as a semi-simple set. More precisely, one can effectively construct a finite family $\{V_i\}$ of finite sets of vectors such that the vectors in V_i form a representation of a simple set X_i and X is the disjoint union of the sets X_i.

2.2. Polyhedra and semi-linear sets

We can consider elements of $\mathbb{N}^k$ and $\mathbb{Z}^k$ as vectors of integer coordinates in the vector space $\mathbb{R}^k$. In the following we briefly recall some geometric notions on $\mathbb{R}^k$ and we refer to [19,22] for more details. As usual a *hyperplane* π of $\mathbb{R}^k$ is given by a linear equation of the form:

$$a_0 + a_1x_1 + a_2x_2 + \cdots + a_kx_k = 0 \tag{1}$$

once an equation for π is specified, we denote it by $\pi(\mathbf{x}) = 0$. We shall always assume that our hyperplanes are *rational*, i.e. they are defined by a linear equation with rational coefficients and constant. Observe that, by eliminating denominators, we can require that coefficients and constant are *integers*. A hyperplane π determines two *open half-spaces* by the inequalities $\pi(\mathbf{x}) > 0$ and, respectively, $\pi(\mathbf{x}) < 0$; also π determines two *closed half-spaces* by the inequalities $\pi(\mathbf{x}) \geq 0$ and, respectively, $\pi(\mathbf{x}) \leq 0$. A *closed polyhedron* is the intersection of a finite number of closed half-spaces.

Let $X, Y \subseteq \mathbb{R}^k$. Then the set

$$X + Y = \{x + y \ : \ x \in X, \ y \in Y\},$$

is called the *Minkowski sum* of X and Y. We will denote by $X - Y$ the Minkowski sum of X and the set $-Y = \{-y \ : \ y \in Y\}$. We observe that the restriction of the Minkowski sum to $\mathbb{N}^k$ or to $\mathbb{Z}^k$ is equal to the sum of subsets of $\mathbb{N}^k$ or of $\mathbb{Z}^k$ defined in the previous subsection.

As usual, an *affine subspace* (or a *flat*) H is a set of the form $\mathbf{b} + V$, where V is a linear subspace of $\mathbb{R}^k$. An *open polyhedron* is the intersection of a finite number of flats and open half-spaces. Equivalently, an open polyhedron is *the relative interior* of some closed polyhedron (see [26]).

As usual, we denote by $\mathbf{0}$ the origin of $\mathbb{R}^k$; when the dimension k is not clear from the context, we use the notation $\mathbf{0}^k$. A set C is a *cone with apex* $\mathbf{0}$ if $\mathbf{x} \in C$ and $\lambda \geq 0$ implies $\lambda\mathbf{x} \in C$. A set C is a *cone with apex* $\mathbf{a}$, if $C - \mathbf{a}$ is a cone with apex $\mathbf{0}$.

We shall only consider *polyhedral cones*, that is cones that are also (closed or open) polyhedra. It is well known [4] that a polyhedral cone C with apex $\mathbf{a}$ can be finitely generated by vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k$ that is, $C = \{\mathbf{a} + \lambda_1\mathbf{v}_1 + \cdots + \lambda_k\mathbf{v}_k : \lambda_i \in \mathbb{R}_+\}$. C is said to be *simplicial* if its generators $\mathbf{v}_1, \ldots, \mathbf{v}_k$ are linearly independent.

The following remarkable result is known since long time (see [25] and the historical notes therein).

Lemma 1. *A polyhedral cone can be written as union of finitely many simplicial cones.*

Now we want to define some suitable regions of $\mathbb{R}^k$. More precisely, our regions will be (open) polyhedra determined by a family of hyperplanes. We proceed as follows. Let π be a hyperplane of $\mathbb{R}^k$, with equation $\pi(\mathbf{x}) = 0$. We associate with π a map

$$f_\pi : \mathbb{R}^k \longrightarrow \{+, 0, -\}$$

defined as: for any $\mathbf{x} \in \mathbb{R}^k$,

$$f_\pi(\mathbf{x}) = \begin{cases} + & \text{if } \pi(\mathbf{x}) > 0, \\ 0 & \text{if } \pi(\mathbf{x}) = 0, \\ - & \text{if } \pi(\mathbf{x}) < 0. \end{cases}$$

We remark that the map defined above depends upon the hyperplane π and its equation in the obvious geometrical way. We can now give the following important two definitions. Recall that we only consider hyperplanes with rational coefficients and constants.

Definition 2. Let $\Pi = \{\pi_1, \ldots, \pi_m\}$ be a family of hyperplanes of $\mathbb{R}^k$. Let $\sim_\Pi$ be the equivalence defined over the set $\mathbb{R}^k$ as: for any $\mathbf{x}, \ \mathbf{x}' \in \mathbb{R}^k$

$$\mathbf{x} \ \sim_\Pi \ \mathbf{x}' \quad \Longleftrightarrow \quad \forall\, i = 1, \ldots, m, \quad f_{\pi_i}(\mathbf{x}) = f_{\pi_i}(\mathbf{x}').$$

The set $\mathcal{P}$ of the cosets of $\sim_\Pi$ of $\mathbb{R}^k$ is called a *polyhedral partition of* $\mathbb{R}^k$ *with respect to* Π.

We define the equivalence relations $\sim_{\Pi,\mathbb{N}}$ and $\sim_{\Pi,\mathbb{Z}}$ over $\mathbb{N}^k$ and, respectively, over $\mathbb{Z}^k$ as the restriction of $\sim_\Pi$ to elements of $\mathbb{N}^k$ and, respectively, of $\mathbb{Z}^k$.

The set $\mathcal{P}$ of the cosets of $\sim_{\Pi,\mathbb{N}}$ of $\mathbb{N}^k$ (respectively, of the cosets of $\sim_{\Pi,\mathbb{Z}}$ of $\mathbb{Z}^k$) is called a *polyhedral partition of* $\mathbb{N}^k$ (respectively, *of* $\mathbb{Z}^k$) *with respect to* Π.

The following lemma is immediate.

Lemma 2. *Every coset of* $\sim_\Pi$ *is an open polyhedron.*

Assume that, in Definition 2, the family Π satisfies the additional property that every hyperplane of Π passes through the origin. In this case, by Lemma 2, the cosets of $\sim_\Pi$ are open polyhedral cones with apex $\mathbf{0}$ and, therefore, they will be called *conic regions*. It may be also useful to notice that the singleton composed by the origin is a region.

Moreover it is useful to observe that every coset of the equivalence $\sim_\Pi$ is uniquely determined by a sequence of m components in $\{+, 0, -\}$. On the other hand, a sequence of such kind defines a region only if the corresponding set of points of $\mathbb{R}^k$ is not empty. It is easily seen that, in general, the latter condition may be very well false, that is, the set of points defined by the sequence is empty.

Now we want to show that the integer points lying in every coset determine a semi-simple set, or equivalently that every coset of $\sim_{\Pi,\mathbb{N}}$ and $\sim_{\Pi,\mathbb{Z}}$ is a semi-simple set of $\mathbb{N}^k$ and, respectively, of $\mathbb{Z}^k$. The following results are immediate consequence of the characterization of semi-linear sets in terms of first order definability in Presburger arithmetic (see Theorem 1).

Lemma 3. *Let* π *be a rational hyperplane. Then the set of all points of* $\mathbb{N}^k$ *(of* $\mathbb{Z}^k$*) such that* $\pi(\mathbf{x}) \le 0$ *is a semi-simple set of* $\mathbb{N}^k$ *(resp. of* $\mathbb{Z}^k$*).*

Lemma 4. *Let P be a (closed or open) polyhedron defined by hyperplanes represented by equations with rational coefficients. Then the set of points of* $\mathbb{N}^k$ *(of* $\mathbb{Z}^k$*) contained in P is a semi-simple subset of* $\mathbb{N}^k$ *(of* $\mathbb{Z}^k$*).*

Proposition 1. *Every coset of* $\sim_{\Pi,\mathbb{N}}$ *and* $\sim_{\Pi,\mathbb{Z}}$ *is a semi-simple set of* $\mathbb{N}^k$ *and, respectively, of* $\mathbb{Z}^k$*.*

2.3. Quasi-polynomials

For a given positive integer d, denote by $\equiv$ the arithmetic congruence modulo d. Such congruence obviously extends to the set $\mathbb{Z}^t$, $t \ge 1$. Indeed, if $\mathbf{m} = (m_1, \ldots, m_t)$ and $\mathbf{m}' = (m'_1, \ldots, m'_t) \in \mathbb{Z}^t$, then $\mathbf{m}$ and $\mathbf{m}'$ will be *congruent modulo d* if, for $i = 1, \ldots, t$, $m_i \equiv m'_i \mod d$. With a minor abuse of notation, we still denote by $\equiv$ (mod) the relation defined above on $\mathbb{Z}^t$. For every $\mathbf{m} \in \mathbb{Z}^t$, $[\mathbf{m}]_d$ denotes the congruence class of $\mathbf{m}$ with respect to $\equiv$ (we drop the dependency on d when it is clear from the context). Moreover, the set $[\mathbf{m}]_d \cap \mathbb{N}^t$ will be denoted by $[\mathbf{m}]_{d,\mathbb{N}}$.

As it is well known, with every equivalence class $[\mathbf{m}]_d$, with $\mathbf{m} = (m_1, \ldots, m_t) \in \mathbb{Z}^t$, one can associate, as its *canonical representative* of the class, the vector $(d_1, \ldots, d_t) \in \mathbb{N}^t$, where, for every $i = 1, \ldots, t$, d_i is the remainder of the division of m_i by d. The same holds for the equivalence classes $[\mathbf{m}]_{d,\mathbb{N}}$ in $\mathbb{N}^t$. We write $[(d_1, \ldots, d_t)]_d$ and $[(d_1, \ldots, d_t)]_{d,\mathbb{N}}$ to denote the corresponding equivalence classes in $\mathbb{Z}^t$ and respectively in $\mathbb{N}^t$.

A set X of $\mathbb{N}^t$ (resp., $\mathbb{Z}^t$) is said to be *recognizable* if it is union of finitely many classes of the congruence $\equiv$.

Remark 1. We observe that the previous definition is the special case to $\mathbb{N}^t$ (resp., $\mathbb{Z}^t$) of the classical notion of *abstract recognizability* of a subset of a monoid (*see* [23]).

The set of classes $[\mathbf{m}]_d$, with $\mathbf{m} \in \mathbb{Z}^t$, or the set of classes $[\mathbf{m}]_{d,\mathbb{N}}$, $\mathbf{m} \in \mathbb{N}^t$ determines the well-known finite group $\mathbb{Z}_d^t = \mathbb{Z}_d \times \cdots \times \mathbb{Z}_d$.

The following lemma states an useful property of equivalence classes and it is easily proven.

Lemma 5. *Let* $\mathbf{m} \in \mathbb{Z}^t$*. Then* $[\mathbf{m}]_d$ *and* $[\mathbf{m}]_{d,\mathbb{N}}$ *are semi-simple subsets of* $\mathbb{Z}^t$ *and* $\mathbb{N}^t$ *respectively.*

Definition 3. A map $F : \mathbb{N}^t \longrightarrow \mathbb{N}$ (resp., $F : \mathbb{Z}^t \longrightarrow \mathbb{N}$) is said to be a *quasi-polynomial* if there exist $d \in \mathbb{N}$, $d \ge 1$, and a family of polynomials in t variables with rational coefficients:

$$\{p_{(d_1,d_2,\ldots,d_t)} \mid d_1, \ldots, d_t \in \mathbb{N},\ 0 \le d_i < d\},$$

where, for every $(n_1, \ldots, n_t) \in \mathbb{N}^t$ (resp., $(n_1, \ldots, n_t) \in \mathbb{Z}^t$), if $(n_1, \ldots, n_t) \equiv (d_1, \ldots, d_t)$, one has:

$$F(n_1, \ldots, n_t) = p_{(d_1,d_2,\ldots,d_t)}(n_1, \ldots, n_t).$$

The number d is called the *period* of F.

In the sequel, to simplify the notation, the polynomial $p_{(d_1,d_2,\ldots,d_t)}$ is denoted $p_{d_1 d_2 \cdots d_t}$.

Definition 4. Let $F : \mathbb{N}^t \longrightarrow \mathbb{N}$ be a map (resp., $F : \mathbb{Z}^t \longrightarrow \mathbb{N}$). Given a subset C of $\mathbb{N}^t$ (resp., $\mathbb{Z}^t$), F is said to be a *quasi-polynomial over C* if there exists a quasi-polynomial q, such that $F(\mathbf{x}) = q(\mathbf{x})$, for any $\mathbf{x} \in C$.

The following lemmata states some useful closure properties of quasi-polynomials.

Lemma 6. *Let* $F_1, F_2 : \mathbb{N}^t \longrightarrow \mathbb{N}$ *(resp.,* $F_1, F_2 : \mathbb{Z}^t \longrightarrow \mathbb{N}$*) be quasi-polynomials. Then* $F_1 + F_2$ *is a quasi-polynomial.*

Proof. First we treat the case where the domains of F_1 and F_2 is $\mathbb{N}^t$. Let $F_1, F_2 : \mathbb{N}^t \longrightarrow \mathbb{N}$ be quasi-polynomials of periods d_1, d_2 respectively and let

$$\{p_{a_1\cdots a_t} \mid \forall\, i = 0, \dots, t,\ 0 \le a_i \le d_1 - 1\}, \quad \text{and}$$
$$\{q_{b_1\cdots b_t} \mid \forall\, i = 0, \dots, t,\ 0 \le b_i \le d_2 - 1\}$$

be the families of polynomials that define F_1 and F_2 respectively. Define a new quasi-polynomial F as follows. Take $d = d_1 d_2$ as the period of F and, for every $(c_1, \dots, c_t) \in \{0, 1, \dots, d-1\}^t$, take

$$F_{c_1\cdots c_t} = p_{a_1\cdots a_t} + q_{b_1\cdots b_t},$$

where, for any $i = 1, \dots, t$, a_i and b_i are the remainders of the division of c_i by d_1 and d_2 respectively. It is easily checked that the quasi-polynomial F is the sum of F_1 and F_2. Indeed, if $\mathbf{x} = (x_1, \dots, x_t) \in \mathbb{N}^t$ and, for every $i = 1, \dots, t$, $x_i \equiv c_i \mod d$, then one has

$$c_i \equiv a_i \mod d_1 \iff x_i \equiv a_i \mod d_1$$
$$c_i \equiv b_i \mod d_2 \iff x_i \equiv b_i \mod d_2.$$

Therefore, if $\mathbf{x} = (x_1, \dots, x_t) \in \mathbb{N}^t$ and $x_i \equiv c_i \bmod d$, then we have:

$$F(\mathbf{x}) = F_{c_1\cdots c_t}(\mathbf{x}) = p_{a_1\cdots a_t}(\mathbf{x}) + q_{b_1\cdots b_t}(\mathbf{x}) = F_1(\mathbf{x}) + F_2(\mathbf{x}).$$

The claim is thus proved. The case where the domain of F is $\mathbb{Z}^t$ is treated similarly. □

Now we introduce the definitions of *piecewise quasi-polynomial* and *piecewise polynomial*.

Definition 5. Let $F : \mathbb{N}^t \longrightarrow \mathbb{N}$ (resp., $F : \mathbb{Z}^t \longrightarrow \mathbb{N}$) be a map. Then F is said to be:

- a *piecewise quasi-polynomial on polyhedral regions in* $\mathbb{N}^t$ *(resp.,* $\mathbb{Z}^t$*)* if there exists a polyhedral partition of $\mathbb{N}^t$ (resp., of $\mathbb{Z}^t$)

  $$\mathcal{P} = \{P_1, \dots, P_s\}$$

  and a family $\{q_1, \dots, q_s\}$ of quasi-polynomials with rational coefficients, such that:
  - every quasi-polynomial q_j is associated with the region P_j of $\mathcal{P}$;
  - for any $\mathbf{b} \in \mathbb{N}^t$ (resp., $\mathbf{b} \in \mathbb{Z}^t$), one has:

    $$F(\mathbf{b}) = q_j(\mathbf{b}),$$

    where j is the index of the region P_j that contains $\mathbf{b}$.
- a *piecewise quasi-polynomial on conic regions in* $\mathbb{N}^t$ *(resp.,* $\mathbb{Z}^t$*)* if, in the previous definition, all the polyhedra of $\mathcal{P}$ are cones;
- a *piecewise polynomial on simple subsets in* $\mathbb{N}^t$ *(resp.,* $\mathbb{Z}^t$*)* if there exists a partition in simple subsets of $\mathbb{N}^t$ (resp., of $\mathbb{Z}^t$)

  $$\mathcal{R} = \{R_1, \dots, R_s\}$$

  and a family $\{p_1, \dots, p_s\}$ of polynomials with rational coefficients such that:
  - every polynomial p_j is associated with the simple subset R_j of $\mathcal{R}$;
  - for any $\mathbf{b} \in \mathbb{N}^t$ (resp., $\mathbf{b} \in \mathbb{Z}^t$), one has:

    $$F(\mathbf{b}) = p_j(\mathbf{b}),$$

    where j is the index of the simple subset R_j that contains $\mathbf{b}$.

An important relationship between piecewise quasi-polynomials on polyhedral regions and piecewise polynomials on simple sets is given in the following proposition.

Proposition 2. *Let F be a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$ (resp., $\mathbb{Z}^t$). Then F is also a piecewise polynomial on simple subsets in $\mathbb{N}^t$ (resp., $\mathbb{Z}^t$).*

Proof. Suppose that F is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$. Let $\mathcal{P}$ be the polyhedral partition of $\mathbb{N}^t$ and $\{q_1, \dots, q_s\}$ be the family of quasi-polynomials that define F. Let P be a polyhedron of $\mathcal{P}$ and let q be its corresponding quasi-polynomial.

In order to achieve the claim, it is clearly enough to prove the existence of a partition $\{R_1, R_2, \dots, R_\ell\}$ of P into a finite family of simple subsets of $\mathbb{N}^t$ such that, for every $i = 1, \dots, \ell$, there exists a polynomial p_i with the property that:

$$\forall\, \mathbf{x} \in R_i, \quad q(\mathbf{x}) = p_i(\mathbf{x}).$$

Let d be the period of q and let $(d_1, \dots, d_t)$ be a vector of $\mathbb{N}^t$, with $d_i \le d - 1$. The polyhedron P admits a partition into a finite family of sets of the form

$$[(d_1, \dots, d_t)]_{\mathbb{N}} \cap P.$$

By Lemma 4, by Lemma 5 and the fact that the family of semi-simple subsets of $\mathbb{N}^t$ is a Boolean algebra, it follows that, for every vector $(d_1, \ldots, d_t)$, with $d_i \leq d-1$, the set $[(d_1, \ldots, d_t)]_{\mathbb{N}} \cap P$ is a semi-simple subset in $\mathbb{N}^t$. Therefore, P admits a partition into finitely many simple sets of $\mathbb{N}^t$.

On the other hand, for every $\mathbf{b} \in [(d_1, \ldots, d_t)]_{\mathbb{N}} \cap P$, one has $q(\mathbf{b}) = p_{(d_1,\ldots,d_t)}(\mathbf{b})$. This concludes the proof.

The case where the domain of F is $\mathbb{Z}^t$ is treated similarly. □

Also the converse of the statement above is true. For the sake of completeness, we give an outline of a proof. This proof is based upon the following result that can be considered *folklore*.

Proposition 3. *For every semi-linear set X of $\mathbb{N}^t$ (resp., $\mathbb{Z}^t$), there exist a partition of $\mathbb{N}^t$ (resp., $\mathbb{Z}^t$) into polyhedral regions $R_1, \ldots, R_s$ and recognizable sets $G_1, \ldots, G_s$, $s \geq 1$, such that $X = \bigcup_{i=1}^{s} R_i \cap G_i$.*

As an immediate consequence of the previous result, one can get the following.

Corollary 1. *Let F be a piecewise polynomial on simple sets in $\mathbb{N}^t$ (resp., $\mathbb{Z}^t$). Then F is also a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$ (resp., $\mathbb{Z}^t$).*

We close this section with the following closure property of piecewise quasi-polynomial on polyhedral regions.

Lemma 7. *Let $F_1, F_2 : \mathbb{N}^t \longrightarrow \mathbb{N}$ (resp., $F_1, F_2 : \mathbb{Z}^t \longrightarrow \mathbb{N}$) be piecewise quasi-polynomials on polyhedral regions. Then $F_1 + F_2$ is a piecewise quasi-polynomial on polyhedral regions.*

Proof. First we treat the case where the domains of F_1 and F_2 is $\mathbb{N}^t$. Let $\mathcal{P}_1 = \{P_1, \ldots, P_s\}$ and $\mathcal{P}_2 = \{P'_1, \ldots, P'_r\}$ be the polyhedra partitions of F_1 and F_2 respectively. Moreover, let $\{q_1, \ldots, q_s\}$ and $\{q'_1, \ldots, q'_r\}$ be the families of quasi-polynomials of F_1 and F_2 respectively.

Consider the piecewise quasi-polynomial defined as follows. Let $\mathcal{P}$ be the polyhedral partition of $\mathbb{N}^t$ given by the intersection of $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively. Then every region of $\mathcal{P}$ is defined as the intersection of a polyhedron of $\mathcal{P}_1$ and of a polyhedron of $\mathcal{P}_2$. Let $P \in \mathcal{P}$, with $P = P_\ell \cap P'_m$, where $P_\ell \in \mathcal{P}_1, P'_m \in \mathcal{P}_2$. Then we associate with P the function $r_{lm} = q_l + q'_m$. For every $\mathbf{x} \in P$ we have

$$F_1(\mathbf{x}) + F_2(\mathbf{x}) = q_l(\mathbf{x}) + q'_m(\mathbf{x}) = r_{lm}(\mathbf{x}).$$

By Lemma 6, r_{lm} is a quasi-polynomial. Therefore the polyhedral partition of $\mathbb{N}^t$

$$\mathcal{P} = \{P_{\ell m} = P_\ell \cap P'_m \neq \emptyset \;:\; P_\ell \in \mathcal{P}_1,\; P'_m \in \mathcal{P}_2\},$$

and the set of quasi-polynomials

$$\{r_{lm} = q_l + q'_m \;:\; \ell = 1, \ldots, s,\; m = 1, \ldots, r\},$$

allows one to define $F_1 + F_2$ as a piecewise quasi-polynomial on polyhedral regions.

The case where the domain of F_1 or F_2 is $\mathbb{Z}^t$ is treated similarly. □

Remark 2. In the proof of Lemma 6 and Lemma 7 respectively, the key points are the following:

- given two recognizable sets, their intersection is still a recognizable set;
- given two partitions of $\mathbb{N}^t$ (resp. of $\mathbb{Z}^t$) into polyhedral regions, there exists a partition of $\mathbb{N}^t$ (resp. of $\mathbb{Z}^t$) into polyhedral regions which is a common refinement of the two partitions.

Once such properties are established, the previous lemmata depend only on the closure property of polynomials w.r.t. sum. Therefore a similar result holds if we replace "polynomials" with any class of functions closed w.r.t. sum.

2.4. Counting solutions of systems of Diophantine equations

The aim of this section is to recall some results about the partition function of a system of Diophantine linear equations. We consider a system of Diophantine linear equations of the form $\mathbf{a_0} + A\mathbf{x} = \mathbf{b}$ where $A \in \mathbb{N}^{t\times k}$, $k \geq t$, denotes the matrix of the system, $\mathbf{b} \in \mathbb{N}^{t\times 1}$ denotes its vector of constant terms, $\mathbf{x} = (x_1, \ldots, x_k)$ denotes the vector of its unknowns, and $\mathbf{a_0} \in \mathbb{N}^{t\times 1}$ is a constant vector. We can associated with the system $\mathbf{a_0} + A\mathbf{x} = \mathbf{b}$ its counting function $\mathcal{S}_A : \mathbb{N}^t \longrightarrow \mathbb{N} \cup \{\infty\}$ which maps every vector $\mathbf{b}$ into the number of non-negative solutions of the Diophantine system. We remark that, under the assumption that all columns of A are non-null, since all coefficients of the system are non-negative, then, for every $\mathbf{b}$, $\mathcal{S}_A(\mathbf{b}) \in \mathbb{N}$. The following theorem holds (for a proof, see [10], Theorem 9).

Theorem 2. *The map $\mathcal{S}_A$ is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$. Moreover the regions and the quasi-polynomials that define $\mathcal{S}_A$ can be effectively constructed starting from the coefficients of the system.*

In the case that the vector $\mathbf{a_0}$ is null, one can prove that the polyhedral regions of the quasi-polynomial $\mathcal{S}_A$ are conic.

Remark 3. Theorem 2 can be reformulated in "*language-theoretic*" way. Indeed, as an immediate consequence of the previous theorem and of Proposition 2, one obtains that S_A is a piecewise polynomial on simple subsets in $\mathbb{N}^t$.

3. The growth function of semi-linear sets of $\mathbb{N}^t$ and of $\mathbb{Z}^t$

In the Theory of Formal Languages the growth function of a language L is defined, in a natural way, as the function $g_L : \mathbb{N} \longrightarrow \mathbb{N}$ that maps every $n \in \mathbb{N}$ into the number of words of L of length not larger than n. In the context of semi-linear sets of $\mathbb{N}^t$ or $\mathbb{Z}^t$, to define the corresponding notion of growth function of a semi-linear set X, we need to specify a size measure on the vectors of $\mathbb{N}^t$ or, respectively, of $\mathbb{Z}^t$. It appears that we have two natural choices:

- an *univariate* size measure, which given a n, with $n \in \mathbb{N}$, returns the cardinality of the set of vectors $\mathbf{x} = (x_1, \ldots, x_t)$ of X such that $x_i \leq n$, for every i with $1 \leq i \leq t$, if $X \subseteq \mathbb{N}^t$ (and using the absolute value if $X \subseteq \mathbb{Z}^t$);
- a *multivariate* size measure, which given $n_1, \ldots, n_t$, with $n_i \in \mathbb{N}$, for $i = 1, \ldots, t$, returns the cardinality of the set of vectors $\mathbf{x} = (x_1, \ldots, x_t)$ of X such that $x_i \leq n_i$, for every i with $1 \leq i \leq t$, if $X \subseteq \mathbb{N}^t$ (and again using the absolute value if $X \subseteq \mathbb{Z}^t$).

In the following we shall use the multivariate approach, which gives more information and is strictly related to the vector partition function. From the results obtained, we are also able to characterize the univariate growth function (see Section 3.3). We shall not discuss here what are the *abstract properties* of a *reasonable growth function*. We just mention that e.g. the use of the *Euclidean norm* gives rise to non-linear inequalities, difficult to treat [15]. We think that this interesting problem deserves a specific investigation. Now we turn to the formal definitions.

Definition 6. We define the *growth function* of a subset X of $\mathbb{N}^t$ or $\mathbb{Z}^t$, $t \geq 1$ as the function $\mathcal{g}_X : \mathbb{N}^t \longrightarrow \mathbb{N}$ which associates with non-negative integers $n_1, \ldots, n_t$, the number $\mathcal{g}_X(n_1, \ldots, n_t)$ of all the elements $(x_1, \ldots, x_t) \in X$ such that:

$$\begin{cases} |x_1| & \leq n_1 \\ \quad\cdot & \quad\cdot \\ \quad\cdot & \quad\cdot \\ \quad\cdot & \quad\cdot \\ |x_t| & \leq n_t. \end{cases} \tag{2}$$

In case X lies in $\mathbb{N}^t$ (resp. $\mathbb{Z}^t$), $\mathcal{g}_X$ counts the number of points of X lying in larger and larger hyper-parallelepipeds, starting from the origin of $\mathbb{N}^t$ (resp. centered at the origin of $\mathbb{Z}^t$). In the sequel of this section, we will prove the following remarkable results:
(Theorem 4, Theorem 6). *Let X be a semi-linear subset of $\mathbb{N}^t$ (resp., $\mathbb{Z}^t$). Then $\mathcal{g}_X$ is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$.*

Remark 4. As an immediate consequence of an argument used in the previous section, one obtains that $\mathcal{g}_X$ is a piecewise polynomial on simple sets in $\mathbb{N}^t$.

3.1. *The growth function of semi-linear sets of $\mathbb{N}^t$*

We start with some technical definitions.

Definition 7. Let X be a subset of $\mathbb{N}^t$ and let $t_1, t_2 \in \mathbb{N}$ such that $t = t_1 + t_2$. We associate with X a function

$$\mathcal{g}^+{}_{X,\, t_1,t_2} : \mathbb{N}^t \longrightarrow \mathbb{N}$$

that returns, for every $(n_1, \ldots, n_{t_1}, m_1, \ldots, m_{t_2}) \in \mathbb{N}^t$, the number of elements $(x_1, \ldots, x_t) \in X$ such that:

$$\begin{cases} \quad x_1 \;= & n_1 \\ \quad\;\cdot & \cdot \\ \quad\;\cdot & \cdot \\ \quad\;\cdot & \cdot \\ \quad x_{t_1} \;= & n_{t_1} \\ 0 \leq x_{t_1+1} \;\leq & m_1 \\ \quad\;\cdot & \cdot \\ \quad\;\cdot & \cdot \\ \quad\;\cdot & \cdot \\ 0 \leq x_t \;\leq & m_{t_2}. \end{cases} \tag{3}$$

Theorem 3. *Let X be a semi-linear set of $\mathbb{N}^t$ and let $t_1, t_2 \in \mathbb{N}$ such that $t = t_1 + t_2$. Then $\mathcal{g}^+{}_{X,t_1,t_2}$ is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$.*

Proof. Let $t_1, t_2 \in \mathbb{N}$ such that $t = t_1 + t_2$ and let X be a semi-linear set of $\mathbb{N}^t$. To avoid a heavy notation, in this proof, we suppress the dependency of $\mathcal{G}^+{}_{X,t_1,t_2}$ on t_1 and t_2 and we simply write $\mathcal{G}^+{}_X$. By Theorem 1, X is semi-simple so that

$$X = \bigcup_{i=1,\ldots,\ell} X_i$$

is a finite and disjoint union of simple sets of $\mathbb{N}^t$. As a straightforward consequence, one can easily check that, for every $(n_1, \ldots, n_t) \in \mathbb{N}^t$,

$$\mathcal{G}^+{}_X(n_1, \ldots, n_t) = \sum_{i=1}^{\ell} \mathcal{G}^+{}_{X_i}(n_1, \ldots, n_t).$$

In order to conclude the proof, by the equality above and by Lemma 7 it is enough to prove that, for every simple set X of $\mathbb{N}^t$, $\mathcal{G}^+{}_X$ is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$.
For this purpose, let

$$X = \mathbf{b_0} + \mathbf{b_1}^{\oplus} + \cdots + \mathbf{b_k}^{\oplus},$$

be a representation of X as a simple set where, for every $j = 0, \ldots, k$,

$$\mathbf{b_j} = (b_{j1}, \ldots, b_{jt}) \in \mathbb{N}^t.$$

Therefore we can write Eq. (3) for the set X as a system of t inequalities in k unknowns $y_1, \ldots, y_k$:

$$\begin{cases} b_{01} + b_{11}y_1 + b_{21}y_2 + \cdots + b_{k1}y_k & = n_1 \\ b_{02} + b_{12}y_1 + b_{22}y_2 + \cdots + b_{k2}y_k & = n_2 \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ b_{0t_1} + b_{1t_1}y_1 + b_{2t_1}y_2 + \cdots + b_{kt_1}y_k & = n_{t_1} \\ b_{0t_1+1} + b_{1t_1+1}y_1 + b_{2t_1+1}y_2 + \cdots + b_{kt_1+1}y_k & \le m_1 \\ b_{0t_1+2} + b_{1t_1+2}y_1 + b_{2t_1+2}y_2 + \cdots + b_{kt_1+2}y_k & \le m_2 \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ b_{0t} + b_{1t}y_1 + b_{2t}y_2 + \cdots + b_{kt}y_k & \le m_{t_2}. \end{cases} \tag{4}$$

Since X is a simple set of $\mathbb{N}^t$, there exists a bijection between the set of non-negative solutions of the system (4) and the set of elements of X that satisfy Eq. (3). Consider now the Diophantine system of equations obtained from (4) where $z_1, z_2, \ldots, z_{t_2}$ form a set of t_2 unknowns disjoint from the set of unknowns $y_1, \ldots, y_k$:

$$\begin{cases} b_{01} + b_{11}y_1 + b_{21}y_2 + \cdots + b_{k1}y_k & = n_1 \\ b_{02} + b_{12}y_1 + b_{22}y_2 + \cdots + b_{k2}y_k & = n_2 \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ b_{0t_1} + b_{1t_1}y_1 + b_{2t_1}y_2 + \cdots + b_{kt_1}y_k & = n_{t_1} \\ b_{0t_1+1} + b_{1t_1+1}y_1 + b_{2t_1+1}y_2 + \cdots + b_{kt_1+1}y_k + z_1 & = m_1 \\ b_{0t_1+2} + b_{1t_1+2}y_1 + b_{2t_1+2}y_2 + \cdots + b_{kt_1+2}y_k + z_2 & = m_2 \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ b_{0t} + b_{1t}y_1 + b_{2t}y_2 + \cdots + b_{kt}y_k + z_{t_2} & = m_{t_2}. \end{cases} \tag{5}$$

Let $\mathbf{n} = (n_1, \ldots, n_{t_1}, m_1, \ldots, m_{t_2})$ be an arbitrary vector in $\mathbb{N}^t$. Denote by $\mathcal{S}_A : \mathbb{N}^t \longrightarrow \mathbb{N}$ the function that maps $\mathbf{n}$ into the number of non-negative solutions of the Diophantine system (5). By Theorem 2 applied to $\mathcal{S}_A$, we have that $\mathcal{S}_A$ is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$.

On the other hand, one can easily check that the number of non-negative solutions of the Diophantine system of inequalities (4) is equal to the number of non-negative solutions of the Diophantine system (5). This implies that $\mathcal{G}^+{}_X(\mathbf{n}) = \mathcal{S}_A(\mathbf{n})$ and this concludes the proof. $\square$

As a consequence of the previous theorem, we have the first remarkable result of this section.

Theorem 4. *Let X be a semi-linear set of $\mathbb{N}^t$. Then the growth function $\mathcal{g}_X$ of X is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$.*

Proof. Let $t = t_1 + t_2$ with $t_1 = 0$. Then, for every $\mathbf{x} \in \mathbb{N}^t$, $\mathcal{g}_X(\mathbf{x}) = \mathcal{g}^+{}_{X,t_1,t_2}(\mathbf{x})$. Then the claim follows by applying Theorem 3 to $\mathcal{g}^+{}_{X,t_1,t_2}$. $\square$

3.2. The growth function of semi-linear sets of $\mathbb{Z}^t$

Now we deal with the description of the growth function of a semi-linear set of $\mathbb{Z}^t$. We start with some auxiliary results. The following lemma is useful (see [6]).

Lemma 8. *If X is linear in $\mathbb{Z}^t$ then $X \cap \mathbb{N}^t$ is a semi-linear set of $\mathbb{N}^t$.*

As an immediate consequence, we have:

Corollary 2. *If X is a semi-linear set of $\mathbb{Z}^t$ then $X \cap \mathbb{N}^t$ is a semi-linear set of $\mathbb{N}^t$.*

Corollary 3. *Let X be a semi-linear set of $\mathbb{Z}^t$ and let $t_1, t_2 \in \mathbb{N}$ such that $t = t_1 + t_2$. Set $X' = X \cap \mathbb{N}^t$. Then $\mathcal{g}_{X',\ t_1,t_2}$ is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$.*

Proof. Since, by hypothesis, X is a semi-linear set of $\mathbb{Z}^t$, by Corollary 2, X' is a semi-linear set of $\mathbb{N}^t$. The claim follows by applying Theorem 3 to X'. $\square$

We now introduce the following technical definition.

Definition 8. Let X be a subset of $\mathbb{Z}^t$ and let $t_1, t_2 \in \mathbb{N}$ such that $t = t_1 + t_2$. We associate with X a function

$$\mathcal{g}_{X,\ t_1,t_2} : \mathbb{N}^t \longrightarrow \mathbb{N}$$

that returns, for every $(n_1, \ldots, n_{t_1}, m_1 \ldots, m_{t_2}) \in \mathbb{N}^t$, the number of elements $(x_1, \ldots, x_t) \in X$ such that:

$$\begin{cases} |x_1| = n_1 \\ \quad\vdots \\ |x_{t_1}| = n_{t_1} \\ |x_{t_1+1}| \leq m_1 \\ \quad\vdots \\ |x_t| \leq m_{t_2}. \end{cases} \tag{6}$$

The function $\mathcal{g}_{X,\ t_1,t_2}$ is called the *generalized growth function* of X.

The following theorem holds.

Theorem 5. *Let X be a semi-linear set of $\mathbb{Z}^t$ and let $t_1, t_2 \in \mathbb{N}$ such that $t = t_1 + t_2$. Then $\mathcal{g}_{X,\ t_1,t_2}$ is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$.*

Proof. Let X be a semi-linear set of $\mathbb{Z}^t$ and let $t_1, t_2 \in \mathbb{N}$ such that $t = t_1 + t_2$.

Let Π be the family of planes π_i of equation $x_i = 0$, for every $i = 1, \ldots, t$ and let $\sim_{\Pi,\mathbb{Z}}$ be the equivalence relation over the set $\mathbb{Z}^t$ introduced in Definition 2. Let $\mathcal{C}$ be the set of cosets of $\sim_{\Pi,\mathbb{Z}}$. The set X can be written as a finite and disjoint union

$$X = \bigcup_{C \in \mathcal{C}} (X \cap C).$$

Therefore, for any $\mathbf{b} \in \mathbb{N}^t$, one has:

$$\mathcal{g}_{X,\ t_1,t_2}(\mathbf{b}) = \sum_{C \in \mathcal{C}} \mathcal{g}_{X \cap C,\ t_1,t_2}(\mathbf{b}). \tag{7}$$

Let C be a coset of $\mathcal{C}$. Let $(\epsilon_1, \ldots, \epsilon_t)$, with $\epsilon_i \in \{+, 0, -\}$, $i = 1, \ldots, t$, be the unique tuple that determines C and let $(e_1, \ldots, e_t)$ be the tuple of integers $\{\pm 1\}$ defined as: $e_i = -1$ if and only if $\epsilon_i = -$, $i = 1, \ldots, t$. Let $f : \mathbb{Z}^t \longrightarrow \mathbb{Z}^t$ be the map defined as: for every $(x_1, \ldots, x_t) \in \mathbb{Z}^t$, $f(x_1, \ldots, x_t) = (e_1 x_1, \ldots, e_t x_t)$. It is easily checked that $f(X \cap C)$ is a semi-linear set of $\mathbb{N}^t$ and, since f is an isometry, for every $\mathbf{x} \in \mathbb{N}^t$, one obtains

$$\mathcal{g}_{X \cap C, t_1,t_2}(\mathbf{x}) = \mathcal{g}^+_{f(X \cap C), t_1,t_2}(\mathbf{x}).$$

By applying Theorem 3 to $\mathcal{g}^+_{f(X \cap C), t_1,t_2}$, one has that $\mathcal{g}_{X \cap C, t_1,t_2}$ is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$. Finally the claim follows from Eq. (7), by applying Lemma 7. $\square$

As a consequence of the previous theorem, we have:

Theorem 6. *Let X be a semi-linear set of $\mathbb{Z}^t$. Then the growth function $\mathcal{G}_X$ of X is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$.*

Proof. Let $t = t_1 + t_2$ with $t_1 = 0$. Then, for every $\mathbf{x} \in \mathbb{Z}^t$, $\mathcal{G}_X(\mathbf{x}) = \mathcal{G}_{X,t_1,t_2}(\mathbf{x})$. Then the claim follows by applying Theorem 5 to $\mathcal{G}_{X,t_1,t_2}$. □

3.3. On the univariate growth function

In this paragraph, we use the previous results to characterize the *univariate* version of the growth function. In particular we show that such function is *ultimately* a quasi-polynomial.

Definition 9. We define the *univariate growth function* of a subset X of $\mathbb{N}^t$ or $\mathbb{Z}^t$, $t \geq 1$ as the function $\mathcal{G}^U_X : \mathbb{N} \longrightarrow \mathbb{N}$ which associates with a non-negative integer n, the number $\mathcal{G}^U_X(n)$ of all the elements $(x_1, \ldots, x_t) \in X$ such that:

$$\begin{cases} |x_1| & \leq n \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ |x_t| & \leq n. \end{cases}$$

As a corollary of Theorem 4 and of Theorem 6, we obtain the following result.

Theorem 7. *Let X be a semi-linear set of $\mathbb{N}^t$ or of $\mathbb{Z}^t$. Then the univariate growth function $\mathcal{G}^U_X$ of X is ultimately an univariate quasi-polynomial, that is there exists a natural number $n_0 \in \mathbb{N}$ such that $\mathcal{G}^U_X$ is an univariate quasi-polynomial on the values $n \geq n_0$.*

Proof. We give the proof for $\mathbb{N}^t$, the same argument holds for $\mathbb{Z}^t$. By Theorem 4, the (multivariate) growth function $\mathcal{G}_X$ of X is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$. Such polyhedral regions are determined by a finite set of hyperplanes of $\mathbb{R}^t$, say $\pi_1, \ldots, \pi_s$. Now consider the line $\mathcal{L}$ of $\mathbb{R}^t$ with parametric equation $\mathbf{x} = \mathbf{0}^t + r\mathbf{1}^t$, where $r \in \mathbb{R}$ is the parameter and $\mathbf{1}^t$ is the vector with each component equal to 1. The line $\mathcal{L}$ can cross each hyperplane π_j, with $j = 1, \ldots, s$, at most in one point, or otherwise is a line of the hyperplane π_j. It follows that there exists $n_0 \in \mathbb{N}$ such that for all values of the parameter r greater than n_0, all the corresponding points of the line $\mathcal{L}$ lie in the same polyhedral region P. Let q be the quasi-polynomial corresponding to $\mathcal{G}_X$ in the region P. It follows that for $n \geq n_0$, $\mathcal{G}^U_X(n)$ coincides with the (univariate) quasi-polynomial $q(n, \ldots, n)$. □

4. On a theorem of Dahmen and Micchelli

In this section, we present a combinatorial proof of a version of a famous theorem of Dahmen and Micchelli [12].

Let A be a matrix in $\mathbb{Z}^{t\times n}$. In the sequel, we will suppose that $n \geq t$. Assume that the following condition holds:

$$\forall\, \mathbf{x} \in \mathbb{R}^n,\ \mathbf{x} \geq \mathbf{0}^n,\ A\mathbf{x} = \mathbf{0}^t \implies \mathbf{x} = \mathbf{0}^n. \tag{8}$$

The following property holds.

Lemma 9. *Let A be a matrix in $\mathbb{Z}^{t\times n}$, satisfying (8). If $\mathbf{b}$ is a vector in $\mathbb{Z}^t$, then the number of non-negative integer solutions of the system $A\mathbf{x} = \mathbf{b}$ is always finite.*

Proof. By contradiction, assume that the number of non-negative integer solutions of the system $A\mathbf{x} = \mathbf{b}$ is infinite. Since $\mathbb{N}^n$ is well quasi-ordered, there exist two solutions $\mathbf{x}_1$ and $\mathbf{x}_2$ of the system $A\mathbf{x} = \mathbf{b}$ such that $\mathbf{x_1} > \mathbf{x_2}$. Thus the vector $\mathbf{x_1} - \mathbf{x_2}$ is a non null non-negative solution of the system $A\mathbf{x} = \mathbf{0}^t$. This contradicts the hypothesis that A satisfies (8). The claim is thus proved. □

Therefore, given a matrix A satisfying (8), we can define a function

$$\mathcal{S}_A : \mathbb{Z}^t \longrightarrow \mathbb{N},$$

which associates, with every vector $b \in \mathbb{Z}^t$, the number of non-negative integer solutions of the Diophantine system $A\mathbf{x} = \mathbf{b}$. The following result is a version of a more general theorem of Dahmen and Micchelli [12]:

Let A be a matrix in $\mathbb{Z}^{t\times n}$, that satisfies (8). Then the function $\mathcal{S}_A$ is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{Z}^t$.

In the following, we give a combinatorial proof of this theorem. Our proof is based on the results of the previous section and on some properties of semi-simple sets in $\mathbb{Z}^t$.

Let $\mathrm{Sol}_{A,\mathbf{b}}$ be the set of all non-negative real solutions of the system $A\mathbf{x} = \mathbf{b}$, with $\mathbf{b} \in \mathbb{Z}^t$. Now, we want to show that Condition (8) on the matrix A implies that $\mathrm{Sol}_{A,\mathbf{b}}$ is a bounded set in $\mathbb{R}^n_+$. First, as done in [12], we observe that (8) is equivalent to say that the convex hull H_A of the columns $\mathbf{a}_i$'s of the matrix A, that is

$$H_A = \left\{ \sum_{i=1}^{n} \alpha_i \mathbf{a}_i \ : \ \alpha_i \in \mathbb{R},\ \alpha_i \geq 0,\ \sum_{i=1}^{n} \alpha_i = 1 \right\},$$

does not contain the origin $\mathbf{0}^t$.

Denote by $\|\mathbf{x}\|$ the Euclidean norm of a point $\mathbf{x} \in \mathbb{R}^t$. Since H_A is a convex and closed set of $\mathbb{R}^t$, by standard facts from Convex geometry (see [22]) we have:

Proposition 4. *Let A be a matrix in $\mathbb{Z}^{t\times n}$, that satisfies (8). Then there exists a real number $\delta > 0$ such that, for every $\mathbf{x} \in H_A$, $\|\mathbf{x}\| > \delta$.*

Proposition 5. *Let A be a matrix in $\mathbb{Z}^{t\times n}$, that satisfies (8). If $\mathbf{b}$ is a vector in $\mathbb{Z}^t$, then the set $\mathrm{Sol}_{A,\mathbf{b}}$ is bounded in $\mathbb{R}^n_+$.*

Proof. We argue by contradiction. Assume that $\mathrm{Sol}_{A,\mathbf{b}}$ is not bounded. Then there exists a partition of $\{1, \ldots, n\}$ in two sets I and J such that the following property holds: for every $i \in I$ (resp. $j \in J$), the set of values that appear in every vector of $\mathrm{Sol}_{A,\mathbf{b}}$ at position i (resp. j) is unbounded (resp. bounded).

Let i_0 be in I. We can define an infinite sequence of solutions of $\mathrm{Sol}_{A,\mathbf{b}}$, $(\mathbf{x}_r)_{r\in\mathbb{N}}$, where $\mathbf{x}_r = (x_{r,1}, \ldots, x_{r,n})$, such that, for every $r \in \mathbb{N}$, $x_{r,i_0} < x_{r+1,i_0}$ and the sequence $(x_{r,i_0})_{r\in\mathbb{N}}$ is unbounded. Consider now any other index, if exists, $i_1 \neq i_0$ in I. If the sequence $(x_{r,i_1})_{r\in\mathbb{N}}$ is bounded, then we do nothing. Otherwise we extract from the sequence $(\mathbf{x}_r)_{r\in\mathbb{N}}$, a subsequence $(\mathbf{x}'_r)_{r\in\mathbb{N}}$, which is unbounded also on the index i_1 and such that, for every $r \in \mathbb{N}$, $x'_{r,i_1} < x'_{r+1,i_1}$. By applying this argument finitely many times, we can obtain a subset I' of I and a sequence of solutions of $\mathrm{Sol}_{A,\mathbf{b}}$, $(\sigma_r)_{r\in\mathbb{N}}$, where $\sigma_r = (\sigma_{r,1}, \ldots, \sigma_{r,n})$, such that:

- for every $i \in I'$, the sequence $(\sigma_{r,i})_{r\in\mathbb{N}}$ is unbounded;
- for every $r \in \mathbb{N}$ and for every $i \in I'$, $\sigma_{r,i} < \sigma_{r+1,i}$;
- for every $i \in \{1, \ldots, n\} - I'$, the sequence $(\sigma_{r,i})_{r\in\mathbb{N}}$ is bounded.

Let $J' = \{1, \ldots, n\} - I'$. By compactness, we can extract from the previous sequence, a subsequence $(\hat{\sigma}_r)_{r\in\mathbb{N}}$, where $\hat{\sigma}_r = (\hat{\sigma}_{r,1}, \ldots, \hat{\sigma}_{r,n})$, such that, for every coordinate $i \in J'$, the sequence $(\hat{\sigma}_{r,i})_{r\in\mathbb{N}}$ is convergent. Therefore, for every $\epsilon > 0$, for every large enough positive integers $j < j'$, we have:

$$\forall\, i \in J', \quad \|\hat{\sigma}_{j',i} - \hat{\sigma}_{j,i}\| < \epsilon. \tag{9}$$

Let us consider the vector $\bar{\mathbf{z}} = (\bar{z}_1, \ldots, \bar{z}_n)$ such that:

$$\forall\, i \in J',\ \bar{z}_i = 0, \quad \forall\, i \in I',\ \bar{z}_i = \hat{\sigma}_{j',i} - \hat{\sigma}_{j,i}. \tag{10}$$

By the fact that $A(\sigma_{j'} - \sigma_j) = \mathbf{0}^t$ and by Eq. (9), one can easily check that $\|A\bar{\mathbf{z}}\| < c\epsilon$, for some constant c depending only on A. Observe now that, for every $i \in I'$, the sequence $(\sigma_{r,i})_{r\in\mathbb{N}}$ is unbounded. Therefore, without loss of generality, we can assume that $\bar{z}_i > 1$, for every $i \in I'$. Let $d = \sum_{i\in I'} \bar{z}_i$. It is easily seen that, by replacing in Eq. (10), each $\bar{z}_i,\ i \in I'$, with $\bar{z}_i/d$, we get a new vector $\mathbf{w}$ such that the inequality $\|A\mathbf{w}\| < c\epsilon/d$ holds. Since $A\mathbf{w} \in H_A$ and ϵ is arbitrary, this contradicts Proposition 4. This ends the proof. □

The next step is to determine a hypercube which contains the set $\mathrm{Sol}_{A,\mathbf{b}}$. To this aim we consider the following *linear programming problem* that we denote (Max A, $\mathbf{b}$, i):

- maximize the component x_i, where i is a given index, of the vector $\mathbf{x} = (x_1, \ldots, x_n)$ subject to:
- $A\mathbf{x} = \mathbf{b}$, and
- $\mathbf{x} \geq \mathbf{0}^n$.

We make use of the following theorem (*cf.* [21], Theorem 2.2).

Theorem 8. *Let B be a matrix in $\mathbb{Z}^{t\times n}$, with $n \geq t$, and let $\mathbf{f} = (f_1, \ldots, f_t)$, $\mathbf{d} = (d_1, \ldots, d_n)$ be integer vectors. Consider the linear programming problem in standard form given by:*

- *minimize $\mathbf{d} \cdot \mathbf{x} = \sum_{i=1}^{n} d_i x_i$, subject to:*
- *$B\mathbf{x} = \mathbf{f}$, and*
- *$\mathbf{x} \geq \mathbf{0}^n$.*

If an optimal solution exists, then there exists also an optimal solution $\mathbf{x}$ such that for every i, with $i = 1, \ldots, n$, $|x_i| \leq h\beta$, where h is a non-negative integer constant, depending only on the matrix B and the vector $\mathbf{d}$, and $\beta = \max_{1\leq j,i\leq n}\{|f_j|, |d_i|\}$.

Remark 5. More precisely, one can choose h as follows:

- let $g = \max_{1\leq i\leq t, 1\leq j\leq n,}\{|B_{ij}|\}$, where B_{ij} varies over the entries of the matrix B;
- let m be the rank of the matrix B;

then $h = m!\, g^{m-1}$.

We can now apply Theorem 8 to determine the hypercube which contains the set $\mathrm{Sol}_{A,\mathbf{b}}$.

Corollary 4. *Let A be a matrix in $\mathbb{Z}^{t\times n}$ satisfying (8) and let $\mathbf{b}$ be a vector in $\mathbb{Z}^t$. Set $\beta = \max_{1\le j\le t}\{|b_j|\}$, that is $\|\mathbf{b}\|_\infty$. Then there exists a non-negative integer constant h_A, depending only on the matrix A, such that the set $\mathrm{Sol}_{A,\mathbf{b}}$ is contained in the hypercube $x_i \le h_A\beta$, for $i = 1,\ldots,n$.*

Proof. By Proposition 5, the set $\mathrm{Sol}_{A,\mathbf{b}}$ is bounded in $\mathbb{R}^n_+$ so that Problem (Max A, $\mathbf{b}$, i) admits an optimal solution. Let $\mathbf{d}$ be the vector such that $\mathbf{d} \in \{0,-1\}^n$ and where the i-th component is -1 and all the others are 0. Then the claim follows from Theorem 8, by choosing the matrix A as B, the vector $\mathbf{b}$ as $\mathbf{f}$ and taking the vector $\mathbf{d}$ as above. □

Now we turn to the proof of our main result. For this purpose, we need some preliminary lemmas.

Let $\Lambda : \mathbb{Z}^t \longrightarrow \mathbb{N}$ be the map defined as:

$$\forall\, \mathbf{b} = (b_1,\ldots,b_t) \in \mathbb{Z}^t, \quad \Lambda(\mathbf{b}) = h_A \max_{1\le i\le t} |b_i|,$$

where h_A is the positive integer defined in Corollary 4. Consider the family Π of hyperplanes defined by the following equations:

- for every $i = 1,\ldots,t,\ x_i = 0,$
- for every i, j with $1 \le i < j \le t,\ x_i - x_j = 0$ and $x_i + x_j = 0,$

and let $\mathcal{P}$ be the family of polyhedral regions of $\mathbb{Z}^t$ defined by Π. The first two lemmas easily derive from the definition of $\mathcal{P}$.

Lemma 10. *For any region P of $\mathcal{P}$, there exist $\alpha_1,\ldots,\alpha_t \in \{\pm 1\}$, and j with $1 \le j \le t$, such that, for every $\mathbf{b} = (b_1,\ldots,b_t) \in P$:*

- $\forall\, i = 1,\ldots,t,\ |b_i| = (-1)^{\alpha_i} b_i,$
- $\Lambda(\mathbf{b}) = (-1)^{\alpha_j} h_A b_j.$

Remark 6. Lemma 10 shows the role of the family Π. Indeed, if $\mathbf{b} = (b_1,\ldots,b_t)$ is a vector of $\mathbb{Z}^t$, then, from the position of $\mathbf{b}$ w.r.t. the hyperplanes in Π one can determine for every components b_ℓ, b_m of $\mathbf{b}$, whether $|b_\ell| = b_\ell$ or $|b_\ell| = -b_\ell$ and whether $|b_\ell| \le |b_m|$ or $|b_\ell| > |b_m|$.

Lemma 11. *Let P be a region of $\mathcal{P}$. There exists a semi-linear set Z of $\mathbb{Z}^{t+n}$ such that, for every $\mathbf{b} = (b_1,\ldots,b_t) \in P$:*

$$\mathcal{S}_A(\mathbf{b}) = \mathcal{G}(|b_1|,\ldots,|b_t|, \Lambda(\mathbf{b}),\ldots,\Lambda(\mathbf{b})),$$

where $\mathcal{G} = \mathcal{G}_{Z,\,t_1,t_2}$ is the generalized growth function of Z with $t_1 = t$ and $t_2 = n$.

Proof. Let P be a region of $\mathcal{P}$. Let Z be the subset of all elements $\mathbf{z} = (z_1,\ldots,z_{t+n})$ of $\mathbb{Z}^{t+n}$ such that:

1. $z_i \ge 0$, for all $i = t+1,\ldots,t+n$;
2. $z_i = a_{i1}z_{t+1} + a_{i2}z_{t+2} + \cdots + a_{in}z_{t+n}$, for all $i = 1,\ldots,t$;
3. $(z_1,\ldots,z_t) \in P$.

It is easily seen that Z is semi-linear in $\mathbb{Z}^{t+n}$, as the clauses (1)–(2) above correspond to Presburger formulas and determine a semi-linear set X. Moreover, by Proposition 1, P is semi-linear in $\mathbb{Z}^t$ and therefore $P \times \mathbb{Z}^n$ is semi-linear in $\mathbb{Z}^{t+n}$. It follows that $Z = X \cap (P \times \mathbb{Z}^n)$ is semi-linear in $\mathbb{Z}^{t+n}$.

Let $\mathcal{G} = \mathcal{G}_{Z,\,t_1,t_2}$ be the generalized growth function of Z with $t_1 = t$ and $t_2 = n$.

We claim that, by the definition of Z for every $\mathbf{b} \in P$, with $\mathbf{b} = (b_1,\ldots,b_t)$, $\mathcal{G}(|b_1|,\ldots,|b_t|,\Lambda(\mathbf{b}),\ldots,\Lambda(\mathbf{b}))$ is the number of non-negative solutions of the Diophantine system:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdot \qquad\qquad\qquad\qquad \cdot \\ \cdot \qquad\qquad\qquad\qquad \cdot \\ \cdot \qquad\qquad\qquad\qquad \cdot \\ a_{t1}x_1 + a_{t2}x_2 + \cdots + a_{tn}x_n = b_t. \end{cases}$$

To see this recall that $\mathcal{G}(|b_1|,\ldots,|b_t|,\Lambda(\mathbf{b}),\ldots,\Lambda(\mathbf{b}))$ is the cardinality of the set Z' of all tuples $(b'_1,\ldots,b'_t,x_1,\ldots,x_n)$ which are in Z and such that $|b'_j| = |b_j|$, for $1 \le j \le t$, and $|x_i| \le \Lambda(\mathbf{b})$, for $1 \le i \le n$. For any such tuple $(b'_1,\ldots,b'_t,x_1,\ldots,x_n)$, observe that by clause (4) in the definition of Z, the tuple $(b'_1,\ldots,b'_t)$ must be in P. It follows, by Lemma 10, that the sign of every b'_j, with $j = 1,\ldots,t$, is constant in P and therefore is the same of b_j. We conclude that for every j, with $j = 1,\ldots,t$, $b'_j = b_j$. Therefore, by clauses (1) and (2) in the definition of Z if a vector $(b_1,\ldots,b_t,x_1,\ldots,x_n)$ is in Z' then it corresponds to a solution of the system above. On the other hand, the possible values of any x_i, with $i = 1,\ldots,n$, are restricted by the condition $x_i \le \Lambda(\mathbf{b})$. By Corollary 4, such restrictions include all non-negative solutions of the system. Therefore for every non-negative solution $(x_1,\ldots,x_n)$ of the system, the vector $(b_1,\ldots,b_t,x_1,\ldots,x_n)$ is in Z'. This ends the proof of the claim.

Therefore $\mathcal{S}_A(\mathbf{b}) = \mathcal{G}(|b_1|,\ldots,|b_t|,\Lambda(\mathbf{b}),\ldots,\Lambda(\mathbf{b}))$. □

Before continuing the proof, we need a technical lemma.

Lemma 12. *Let $G : \mathbb{N}^{t+n} \longrightarrow \mathbb{N}$ be a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^{t+n}$. Let h be a positive constant and let j_0 be an index with $1 \le j_0 \le t$. Let $G' : \mathbb{N}^t \longrightarrow \mathbb{N}$ be the map defined as:*

$$G'(b_1, \ldots, b_t) = G(b_1, \ldots, b_t, hb_{j_0}, \ldots, hb_{j_0}), \tag{11}$$

for every $\mathbf{b} = (b_1, \ldots, b_t) \in \mathbb{N}^t$. Then G' is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$.

Proof. Let $\Pi_G = \{\pi_1, \ldots, \pi_m\}$ be the family of planes of $\mathbb{R}^{t+n}$ associated with G. Recall that Π_G includes all the coordinate planes.
Now let $\pi(x_1, \ldots, x_t, x_{t+1}, \ldots, x_{t+n}) \equiv \beta_0 + \sum_{i=1,\ldots,t+n} \beta_i x_i = 0$ be a plane in Π_G. Then the plane:

$$\pi'(x_1, \ldots, x_t) \equiv \beta_0 + \sum_{i=1,\ldots,t} \beta_i x_i + \sum_{j=1,\ldots,n} h\beta_{t+j} x_{j_0} = 0$$

is a plane of $\mathbb{R}^t$. We define as $\Pi_{G'}$ the family of all such planes. It is obvious that all coordinates planes belong to $\Pi_{G'}$.

Let now $\bar{\mathbf{x}} = (\bar{x}_1, \ldots, \bar{x}_t)$ be a point in $\mathbb{N}^t$. Since G is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^{t+n}$, G associates to the point $\bar{\mathbf{x}}^{(\bullet)} \in \mathbb{N}^{t+n}$, with $\bar{\mathbf{x}}^{(\bullet)} = (\bar{x}_1, \ldots, \bar{x}_t, h\bar{x}_{j_0}, \ldots, h\bar{x}_{j_0})$, a unique quasi-polynomial q.

We want to show that the region of $\bar{\mathbf{x}}$ w.r.t. the planes in $\Pi_{G'}$ determines (*via* the transformation $\mathbf{x} \mapsto \mathbf{x}^{(\bullet)}$) q univocally. Let $\mathbf{x}$ be another element of the region of $\bar{\mathbf{x}}$ and let $\mathbf{x}^{(\bullet)} = (x_1, \ldots, x_t, hx_{j_0}, \ldots, hx_{j_0})$. Now, let $\pi \equiv \beta_0 + \sum_{i=1,\ldots,t+n} \beta_i x_i = 0$ be a plane in Π_G. Let π' be the corresponding plane of $\Pi_{G'}$. Then it is obvious that $\pi(\mathbf{x}^{(\bullet)}) > 0$ (or $\pi(\mathbf{x}^{(\bullet)}) = 0$, or $\pi(\mathbf{x}^{(\bullet)}) < 0$) if and only if $\pi'(\mathbf{x}) > 0$ (or, respectively, $\pi'(\mathbf{x}) = 0$, or, respectively, $\pi'(\mathbf{x}) < 0$). By the same argument, $\pi(\bar{\mathbf{x}}^{(\bullet)}) > 0$ (or $\pi(\bar{\mathbf{x}}^{(\bullet)}) = 0$, or $\pi(\bar{\mathbf{x}}^{(\bullet)}) < 0$) if and only if $\pi'(\bar{\mathbf{x}}) > 0$ (or, respectively, $\pi'(\bar{\mathbf{x}}) = 0$, or, respectively, $\pi'(\bar{\mathbf{x}}) < 0$). It follows that the region of $\bar{\mathbf{x}}$ w.r.t. $\Pi_{G'}$ determines q univocally.

Now, let $d > 0$ the period of q. A given point $\bar{\mathbf{x}} = (\bar{x}_1, \ldots, \bar{x}_t)$ in $\mathbb{N}^t$, gives rise to the $t + n$ remainders $(d_1, \ldots, d_t, d^{(\circ)}_{j_0}, \ldots, d^{(\circ)}_{j_0})$ modulo d, where $d^{(\circ)}_{j_0} \equiv hd_{j_0} \bmod d$.

Therefore we let correspond to q the quasi-polynomial $\bar{q} : \mathbb{N}^t \longrightarrow \mathbb{N}$, which has period d and to each sequence of remainders $(d_1, \ldots, d_t)$ modulo d associates the polynomial $\bar{q}_{(d_1,d_2,\ldots,d_t)} : \mathbb{N}^t \longrightarrow \mathbb{N}$, with rational coefficients, defined by:

$$\bar{q}_{(d_1,d_2,\ldots,d_t)}(x_1, \ldots, x_t) = q_{(d_1,d_2,\ldots,d_t,d^{(\circ)}_{j_0},\ldots,d^{(\circ)}_{j_0})}(x_1, \ldots, x_t, hx_{j_0}, \ldots, hx_{j_0}).$$

The piecewise quasi-polynomial G' on polyhedral regions in $\mathbb{N}^t$ is therefore completely specified and this ends the proof. $\square$

Now we continue with the proof of our main result.

Lemma 13. *Let P be a region of $\mathcal{P}$. Then there exists a piecewise quasi-polynomial F on polyhedral regions in $\mathbb{Z}^t$ such that, for every $\mathbf{b} \in P$, $\mathcal{S}_A(\mathbf{b}) = F(\mathbf{b})$.*

Proof. Let P be a region of $\mathcal{P}$. By Lemma 10, there exists an index j_0, with $1 \le j_0 \le t$ such that for every $\mathbf{b} = (b_1, \ldots, b_t) \in P$, $\Lambda(\mathbf{b}) = h_A|b_{j_0}|$.

By Lemma 11, there exists a semi-linear set Z of $\mathbb{Z}^{t+n}$ such that, for every $\mathbf{b} = (b_1, \ldots, b_t) \in P$:

$$\mathcal{S}_A(\mathbf{b}) = G(|b_1|, \ldots, |b_t|, \Lambda(\mathbf{b}), \ldots, \Lambda(\mathbf{b})) = G(|b_1|, \ldots, |b_t|, h_A|b_{j_0}|, \ldots, h_A|b_{j_0}|), \tag{12}$$

where G is the generalized growth function of Z with $t_1 = t$ and $t_2 = n$. By applying Theorem 5 to G, one has that G is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^{t+n}$.

By Lemma 12, there exists a piecewise quasi-polynomial G' on polyhedral regions in $\mathbb{N}^t$ such that, for every $\mathbf{b} = (b_1, \ldots, b_t) \in P$:

$$G'(|b_1|, \ldots, |b_t|) = G(|b_1|, \ldots, |b_t|, h_A|b_{j_0}|, \ldots, h_A|b_{j_0}|). \tag{13}$$

We want to show that there exists a $F : \mathbb{Z}^t \longrightarrow \mathbb{N}$, which is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{Z}^t$, such that for every $\mathbf{b} = (b_1, \ldots, b_t) \in P$ the following equality holds:

$$F(b_1, \ldots, b_t) = G'(|b_1|, \ldots, |b_t|). \tag{14}$$

First of all, recall that by Lemma 10 there exist $\alpha_1, \ldots, \alpha_t \in \{\pm 1\}$, such that for every $\mathbf{b} = (b_1, \ldots, b_t) \in P$:

$$\forall\, i = 1, \ldots, t,\ |b_i| = (-1)^{\alpha_i} b_i. \tag{15}$$

Let $\Pi_{G'} = \{\pi_1, \ldots, \pi_m\}$ be the family of planes of $\mathbb{R}^t$ associated with G'.

Recall that $\Pi_{G'}$ includes the coordinate planes, that is, the planes defined by the equations $x_\ell = 0,\ \ell = 0, \ldots, t$.
Now let $\pi(x_1, \ldots, x_t) \equiv \beta_0 + \sum_{i=1,\ldots,t} \beta_i x_i = 0$ be a plane in $\Pi_{G'}$. Then the plane:

$$\pi'(x_1, \ldots, x_t) \equiv \beta_0 + \sum_{i=1,\ldots,t} (-1)^{\alpha_i} \beta_i x_i = 0$$

is a plane of $\mathbb{R}^t$. We define as Π_F the family of all such planes. It is obvious that all coordinates planes belong to Π_F.

Let now $\bar{\mathbf{x}} = (\bar{x}_1, \ldots, \bar{x}_t)$ be a point in P. Since G' is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{N}^t$, G' associates to the point $\bar{\mathbf{x}}^{(\bullet)} = ((-1)^{\alpha_1}\bar{x}_1, \ldots, (-1)^{\alpha_t}\bar{x}_t)$ a unique quasi-polynomial q.

We want to show that the region of $\bar{\mathbf{x}}$ w.r.t. the planes in Π_F determines (*via* the transformation $\mathbf{x} \mapsto \mathbf{x}^{(\bullet)}$) q univocally. Let $\mathbf{x}$ be another element of the region of $\bar{\mathbf{x}}$ and let $\mathbf{x}^{(\bullet)} = ((-1)^{\alpha_1}x_1, \ldots, (-1)^{\alpha_t}x_t)$. Now, let $\pi \equiv \beta_0 + \sum_{i=1,\ldots,t+n} \beta_i x_i = 0$ be a plane in $\Pi_{G'}$. Let π' be the corresponding plane of Π_F. Then it is obvious that $\pi(\mathbf{x}^{(\bullet)}) > 0$ (or $\pi(\mathbf{x}^{(\bullet)}) = 0$, or $\pi(\mathbf{x}^{(\bullet)}) < 0$) if and only if $\pi'(\mathbf{x}) > 0$ (or, respectively, $\pi'(\mathbf{x}) = 0$, or, respectively, $\pi'(\mathbf{x}) < 0$). By the same argument, $\pi(\bar{\mathbf{x}}^{(\bullet)}) > 0$ (or $\pi(\bar{\mathbf{x}}^{(\bullet)}) = 0$, or $\pi(\bar{\mathbf{x}}^{(\bullet)}) < 0$) if and only if $\pi'(\bar{\mathbf{x}}) > 0$ (or, respectively, $\pi'(\bar{\mathbf{x}}) = 0$, or, respectively, $\pi'(\bar{\mathbf{x}}) < 0$). It follows that the region of $\bar{\mathbf{x}}$ w.r.t. Π_F determines q univocally.

Now, let $d > 0$ the period of q. If a given point $\bar{\mathbf{x}} = (\bar{x}_1, \ldots, \bar{x}_t)$ in $\mathbb{N}^t$, gives rise to the remainders $(d_1, \ldots, d_t)$ modulo d, then $\bar{\mathbf{x}}^{(\bullet)}$ determine the same remainders $(d_1, \ldots, d_t)$ modulo d.

Therefore we let correspond to q the quasi-polynomial $\bar{q} : \mathbb{Z}^t \longrightarrow \mathbb{N}$, which has period d and to each sequence of remainders $(d_1, \ldots, d_t)$ modulo d associates the polynomial $\bar{q}_{(d_1,d_2,\ldots,d_t)} : \mathbb{Z}^t \longrightarrow \mathbb{N}$, with rational coefficients, defined by:

$$\bar{q}_{(d_1,d_2,\ldots,d_t)}(x_1, \ldots, x_t) = q_{(d_1,d_2,\ldots,d_t)}((-1)^{\alpha_1}x_1, \ldots, (-1)^{\alpha_t}x_t).$$

The piecewise quasi-polynomial F on polyhedral regions in $\mathbb{Z}^t$ is therefore completely specified and this ends the proof. □

By using the previous lemma, we obtain the above mentioned version of the Theorem of Dahmen and Micchelli.

Theorem 9. *The function $\mathcal{S}_A$ of the Diophantine system $A\mathbf{x} = \mathbf{b}$ is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{Z}^t$.*

Proof. Let P be a region of $\mathscr{P}$. By Lemma 13, there exists a piecewise quasi-polynomial F_P on polyhedral regions in $\mathbb{Z}^t$ such that, for every $\mathbf{b} \in P$, $\mathcal{S}_A(\mathbf{b}) = F_P(\mathbf{b})$. Let us consider a new function F'_P which coincides with F_P on P and is identically 0 on the regions different from P. Then F'_P is still a piecewise quasi-polynomial on polyhedral regions in $\mathbb{Z}^t$. Let be the function $F = \sum_{P\in\mathscr{P}} F'_P$. By definition of the functions F'_P, with $P \in \mathscr{P}$, one has, for every $\mathbf{b} \in \mathbb{Z}^t$, $\mathcal{S}_A(\mathbf{b}) = F(\mathbf{b})$. On the other, hand, by Lemma 7, F is a piecewise quasi-polynomial on polyhedral regions in $\mathbb{Z}^t$ and this concludes the proof. □

Remark 7. As an immediate consequence of Proposition 2, we obtain that the function $\mathcal{S}_A$ of the Diophantine system $A\mathbf{x} = \mathbf{b}$ is a piecewise polynomial on simple sets in $\mathbb{Z}^t$.

As we have pointed out in the introduction of this paper, in the literature, the notion of partition function is usually related to that of *quasi-polynomials*. On the other hand, Remark 7 shows that, on a simple set in $\mathbb{Z}^t$, that is, *a translate of a free submonoid* of $\mathbb{Z}^t$, the partition function becomes as simple as a *polynomial*, a phenomenon which deserves, in our opinion, further investigations.

5. Final remarks

We remark that all the theorems of this paper are effective. In particular, if X is a semi-linear set of $\mathbb{N}^t$ or $\mathbb{Z}^t$, starting from a representation of X, we are able to effectively construct a polyhedral partition of $\mathbb{N}^t$ and a family of quasi-polynomials that describe the growth function of X as a piecewise quasi-polynomial. Similarly, starting from a matrix A, with integer entries, satisfying (8), we are able to effectively construct a polyhedral partition of $\mathbb{Z}^t$ and a family of quasi-polynomials that describe the partition function $\mathcal{S}_A$ as a piecewise quasi-polynomial.

Therefore, an interesting line of investigation could concern the evaluation of the complexity of the algorithms used in the constructions mentioned above.

Acknowledgements

We are indebted to Corrado De Concini for having given us a deep insight into the topics treated in this paper.
We also thank the anonymous referee for her (his) help in greatly improving a previous version of this paper.

References

[1] V. Baldoni, N. Berline, M. Vergne, Local Euler–Maclaurin expansion of Barvinok valuations and Ehrhart coefficients of a rational polytope, Contemp. Math. 452 (2008) 15–33.
[2] V. Baldoni, J.A. De Loera, M. Vergne, Counting integer flows in networks, Found. Comput. Math. 4 (2004) 277–314.
[3] A.I. Barvinok, A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed, Math. Oper. Res. 19 (1994) 769–779.
[4] M. Beck, S. Robins, Computing the Continuous Discretely, Springer, New York, 2007.
[5] E.T. Bell, Interpolated denumerants and Lambert series, Amer. J. Math. 65 (1943) 382–386.
[6] C. Choffrut, A. Frigeri, Definable sets in weak Presburger arithmetic, in: G. Italiano, E. Moggi, L. Laura (Eds.), Proc. 10th Italian Conference on Theoretical Computer Science ICTCS'07, World Scientific Pub. Co., Singapore, 2007, pp. 175–186.
[7] C. Choffrut, A. Frigeri, Deciding whether the ordering is necessary in a Presburger formula, Discrete Math. Theoret. Comput. Sci. 12 (2010) 21–38.
[8] F. D'Alessandro, A. de Luca, Obituary: Stefano Varricchio (1960–2008), Bull. Eur. Assoc. Theor. Comput. Sci. EATCS 96 (2008) 17.
[9] F. D'Alessandro, B. Intrigila, S. Varricchio, On the structure of the counting function of context-free languages, Theoret. Comput. Sci. 356 (2006) 104–117.

[10] F. D'Alessandro, B. Intrigila, S. Varricchio, The Parikh counting functions of sparse context-free languages are quasi-polynomials, Theoret. Comput. Sci. 410 (2009) 5158–5181.
[11] F. D'Alessandro, B. Intrigila, S. Varricchio, On some counting problems for semi-linear sets, in: 7th International Conference WORDS 2009, University of Salerno (Italy), September 2009.
[12] W. Dahmen, C.A. Micchelli, The number of solutions to linear Diophantine equations and multivariate splines, Trans. Amer. Math. Soc. 308 (1988) 509–532.
[13] C. De Concini, C. Procesi, Topics in Hyperplane Arrangements, Polytopes and Box-Splines, Springer, 2011.
[14] C. De Concini, C. Procesi, M. Vergne, Partition function and generalized Dahmen-Micchelli spaces, arXiv:math0805.2907.
[15] J.A. De Loera, The many aspects of counting lattice points in polytopes, Math. Semesterber. 52 (2005) 175–195.
[16] S. Eilenberg, M.-P. Schützenberger, Rational sets in commutative monoids, J. Algebra 13 (1969) 173–191.
[17] S. Ginsburg, The mathematical theory of context-free languages, Mc Graw-Hill, New York, 1966.
[18] S. Ginsburg, E.H. Spanier, Semigroups, Presburger formulas, and languages, Pacific J. Math. 16 (1966) 285–296.
[19] B. Grünbaum, Convex Polytopes, second ed., Springer-Verlag, New York, 2003.
[20] R. Ito, Every semi-linear set is a finite union of disjoint linear sets, J. Comput. Syst. Sci. 3 (1969) 221–231.
[21] C.H. Papadimitriou, K. Steiglitz, Combinatorial Optimization, Dover Publications, New York, 1998.
[22] R. Tyrrell Rockafellar, Convex Analysis, in: Princeton Mathematical Series, vol. 28, Princeton University Press, Princeton, NJ, 1970.
[23] J. Sakarovitch, Éléments de théorie des automates, Vuibert, Paris, 2003.
[24] A. Salomaa, M. Soittola, Automata-Theoretic Aspects of Formal Power Series, Springer-Verlag, New York, 1978.
[25] A. Schrijver, Theory of Linear and Integer Programming, John Wiley & Sons, Chichester, 1986.
[26] E. Sontag, Remarks on piecewise linear algebra, Pacific J. Math. 98 (1982) 183–201.
[27] B. Sturmfels, On vector partition functions, J. Combin. Theory Ser. A 71 (1995) 302–309.
[28] A. Szenes, M. Vergne, Residue formulae for vector partitions and Euler-Maclaurin sums, in: Formal Power Series and Algebraic Combinatorics (Scottsdale, AZ, 2001), Adv. Appl. Math. 30 (2003) 295–342.