

SOME ANSWER TO NIVAT'S CONJECTURE: A CHARACTERIZATION OF PERIODICITY WITH RESPECT TO BLOCK COMPLEXITY

FABIEN DURAND AND MICHEL RIGO

ABSTRACT. Nivat's conjecture is about the link between the pure periodicity of a subset M of \mathbb{Z}^2 , i.e., invariance under translation by a fixed vector, and some upper bound on the function counting the number of different rectangular blocks occurring in M . Attempts to solve this conjecture have been considered during the last fifteen years. Let $d \geq 2$. A legitimate extension to a multidimensional setting of the notion of periodicity is to consider sets of \mathbb{Z}^d definable by a first order formula in the Presburger arithmetic $\langle \mathbb{Z}; <, + \rangle$. With this latter notion and using a powerful criterion due to Muchnik, we solve an analogue of Nivat's conjecture and characterize sets of \mathbb{Z}^d definable in $\langle \mathbb{Z}; <, + \rangle$ in terms of some functions counting recurrent blocks, that is, blocks occurring infinitely often.

1. INTRODUCTION

A set $M \subseteq \mathbb{Z}^2$ is said to be *periodic* if there exists a non-zero vector $\mathbf{p} \in \mathbb{Z}^2$ such that for all $\mathbf{x} \in \mathbb{Z}^2$, \mathbf{x} belongs to M if and only if $\mathbf{x} + \mathbf{p}$ belongs to M . Periodic sets in dimension greater than one have been investigated recently in the spirit of the celebrated Morse-Hedlund theorem [9]. This is partly due to the so-called *Nivat's conjecture* [11] stated in 1997 and independently in [1].

Conjecture 1 (M. Nivat). *Let M be a subset of \mathbb{Z}^2 . If there exist $n_1, n_2 > 0$ such that the function p_M counting the number of distinct $n_1 \times n_2$ blocks occurring in M is such that $p_M(n_1, n_2) \leq n_1 n_2$, then M is periodic.*

Nivat's conjecture cannot be an equivalence because the converse does not hold: there exists a periodic set M in \mathbb{Z}^2 such that $p_M(n_1, n_2) > n_1 n_2$ for all n_1, n_2 [1, p. 49]. A weaker form of Nivat's conjecture is the following. Let $\alpha < 1$. If there exist $n_1, n_2 > 0$ such such that $p_M(n_1, n_2) \leq \alpha n_1 n_2$, then M is periodic. It was proven for $\alpha = 1/144$ in [7] and improved for $\alpha = 1/16$ in [14]. This latter result is a consequence of the following one.

Theorem 2. [14] *Let M be a subset of \mathbb{Z}^2 . If there exist $n_1, n_2 > 0$ such that the function counting the maximum number of distinct $n_1 \times n_2$ blocks occurring in a $2n_1 \times 2n_2$ block is $\leq \frac{n_1 n_2}{16}$, then M is periodic.*

For a survey on the relationships existing between periodicity and block complexity we refer to [4] and [17]. We can also mention [15]. In this paper, we do not consider this kind of "purely" periodic sets in \mathbb{Z}^2 or even \mathbb{Z}^d , with $d \geq 2$, i.e., we are not looking at sets M having a vector \mathbf{p} acting as "global" period. But we study what we consider as a natural extension of the notion of periodicity to a multidimensional setting. Indeed, when A. L. Semenov in [16] extended Cobham's theorem [5] to a

multidimensional setting, it turns out that the notion of periodicity he used was not the pure periodicity but sets in \mathbb{Z}^d which are defined by a first order formula of the Presburger arithmetic $\langle \mathbb{Z}; <, + \rangle$. It is important to observe that the subsets of \mathbb{N} which are defined by a first order formula in $\langle \mathbb{N}; =, + \rangle$ are exactly the ultimately periodic sets (i.e., finite union of arithmetic progressions). As an example, if

$$\varphi(x) := (x = 3) \vee ((\exists y)(x = 2y)) \vee ((\exists y)(x = 5y + 1))$$

is considered as a formula in $\langle \mathbb{N}; =, + \rangle$, then the set

$$M = \{x \in \mathbb{N} \mid \langle \mathbb{N}; =, + \rangle \models \varphi(x)\} = \{0, 2, 3, 4, 6, 8, 10, 11, 12, 14, 16, 18, 20, 21, \dots\}$$

is ultimately periodic: for $x \geq 4$, $x \in M$ if and only if $x + 10 \in M$. For a presentation of the sets in \mathbb{N}^d definable in the Presburger arithmetic $\langle \mathbb{N}; =, + \rangle$, see for instance the very nice survey [3]. Except for the scope of the variables, there is no fundamental difference between the structures $\langle \mathbb{N}; =, + \rangle$ and $\langle \mathbb{Z}; <, + \rangle$ and we can choose the more convenient one. Notice that in $\langle \mathbb{N}; =, + \rangle$, the relation $x \leq y$ can be easily defined by $(\exists z)(x + z = y)$ but this is no more true when x, y, z are possibly negative and this is the reason why the order relation $<$ has to be added to the Presburger arithmetic over \mathbb{Z} . Note that over $\langle \mathbb{Z}; <, + \rangle$ the formula $x = y$ can be defined by $\neg(x < y) \wedge \neg(y < x)$ and that $x = 0$ can be defined by $x + x = x$. To obtain a characterization of sets M in \mathbb{Z}^d defined by a first order formula of Presburger arithmetic, we estimate the function $R_M(n)$ of different blocks of size n occurring infinitely often in M . Collecting several results and observations about Presburger arithmetic and mainly applying the powerful criterion of Muchnik [10], we derive the following theorem.

Theorem 3. *Let M be a subset in \mathbb{Z}^d . This set is definable in $\langle \mathbb{Z}; <, + \rangle$ if and only if $R_M(n) \in \mathcal{O}(n^{d-1})$ and every section is definable in $\langle \mathbb{Z}; <, + \rangle$.*

If we apply this result recursively, we can express definability in Presburger arithmetic solely in terms of recurrent block complexity. More precisely, a set $M \subseteq \mathbb{Z}^d$ is definable in $\langle \mathbb{Z}; <, + \rangle$ if and only if $R_X(n) \in \mathcal{O}(n^{d-1})$ and for all $k \in \{1, \dots, d-1\}$ every $(d-k)$ -dimensional section has a recurrent block complexity in $\mathcal{O}(n^{d-k-1})$. In Section 2, we define the terminology. Section 3 contains several examples of definable and non-definable sets in \mathbb{Z}^2 to help the reader to develop some intuition about Presburger arithmetic and complexity. In Section 4 we prove the necessary condition relying mainly on the elimination of quantifiers in Presburger arithmetic. Observe that for $d = 1$ our main result corresponds to the celebrated Morse–Hedlund theorem: a set $M \subseteq \mathbb{Z}$ is periodic, i.e., there exists t such that, for all $x \in \mathbb{Z}$, $x \in M \Leftrightarrow x + t \in M$, if and only if there exists n such that $p_M(n) \leq n$ [9]. For $d = 2$ we give, in the first part of Section 5, a direct proof using a lemma already appearing in [7] and [14]. In the second part of Section 5, we treat the general multidimensional case relying on completely different techniques developed by Muchnik in [10].

2. SETTING UP THE FRAMEWORK

Let A be a finite alphabet and d be a positive integer. Let $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_d) \in \mathbb{Z}^d$. We consider the norm

$$\|\mathbf{x}\| = \sup_{1 \leq i \leq d} |\mathbf{x}_i|.$$

Let $k > 0$. We define the k -neighborhood of size k centered at \mathbf{x} by

$$(2.1) \quad \mathcal{B}(\mathbf{x}, k) := \{\mathbf{y} \in \mathbb{Z}^d \mid \|\mathbf{x} - \mathbf{y}\| < k\}.$$

Let $S \in A^{\mathbb{Z}^d}$ be an infinite d -dimensional word over A . It is convenient to consider S as a map $S : \mathbb{Z}^d \rightarrow A$. Let $S_{\mathbf{x}, k}$ denote the *finite block of size k* given by the restriction of S to the domain $\{\mathbf{x}\} + \llbracket 0, k-1 \rrbracket^d$. In this paper, when using notation like $\llbracket i, j \rrbracket$ with $i < j$, it has to be understood that we consider the set of integers $\{i, i+1, \dots, j\}$. If $k = 1$, we write $S_{\mathbf{x}}$ instead of $S_{\mathbf{x}, 1}$ to denote the letter in S pointed at \mathbf{x} . To compare blocks, the respective domains of $S_{\mathbf{x}, k}$ and $S_{\mathbf{y}, k}$ can both be identified with $\llbracket 0, k-1 \rrbracket^d$ and the two maps can be compared. Otherwise stated, we say that two blocks $S_{\mathbf{x}, k}$ and $S_{\mathbf{y}, k}$ of size k are equal if and only if the mappings are the same, i.e., for all \mathbf{v} such that $\mathbf{v} \in \llbracket 0, k-1 \rrbracket^d$, we have $S_{\mathbf{x}+\mathbf{v}} = S_{\mathbf{y}+\mathbf{v}}$. The *block complexity* of S is the map p_S counting for each n the number of different blocks $S_{\mathbf{x}, n}$ appearing in S , i.e.,

$$p_S : \mathbb{N} \rightarrow \mathbb{N} : n \mapsto \#\{S_{\mathbf{x}, n} \mid \mathbf{x} \in \mathbb{Z}^d\}.$$

The *recurrent block complexity* of S is the map R_S counting for each n the number of different blocks $S_{\mathbf{x}, n}$ appearing infinitely often in S . These blocks are called *recurrent blocks*. In other words, this latter function counts only the different blocks B of size n such that for all $L \in \mathbb{N}$, there exists $\mathbf{x} \in \mathbb{Z}^d$ verifying $\|\mathbf{x}\| \geq L$ and $S_{\mathbf{x}, n} = B$. The following inequalities are obvious

$$\forall n \geq 1, \quad R_S(n) \leq p_S(n) \leq (\#A)^{n^d}.$$

Remark 4. If the alphabet A is binary, say $A = \{0, 1\}$, then words in $A^{\mathbb{Z}^d}$ can be identified with subsets of \mathbb{Z}^d and the definitions and notation given above can be applied to subsets of \mathbb{Z}^d . For instance, we can speak of the recurrent block complexity of a subset of \mathbb{Z}^d .

For the sake of completeness, we recall some essential facts about sets definable by first order formulas in the Presburger arithmetic $\langle \mathbb{Z}; <, + \rangle$. For more details, we refer the reader to [2, 3, 10].

Remark 5. Recall that the subsets of \mathbb{N} definable in $\langle \mathbb{N}; =, + \rangle$ are exactly the ultimately periodic sets in \mathbb{N} . When taking a subset M of \mathbb{Z} definable in $\langle \mathbb{Z}; <, + \rangle$, we can consider the two subsets of \mathbb{N} ,

$$M \cap \mathbb{Z}_{\geq 0} \text{ and } -(M \cap \mathbb{Z}_{< 0}) = \{-x \mid (x \in M) \wedge (x < 0)\}$$

which are both definable in $\langle \mathbb{N}; =, + \rangle$ and therefore ultimately periodic. Consequently, if $M \subseteq \mathbb{Z}$ is definable in $\langle \mathbb{Z}; <, + \rangle$, there exist $N, p, q > 0$ (which are chosen minimal) such that for $x > N$, $x \in M$ if and only if $x + p \in M$ and for $x < -N$, $x \in M$ if and only if $x - q \in M$. Notice that even in dimension one, if $p \neq q$ or $N \neq 0$, then M which is definable in $\langle \mathbb{Z}; <, + \rangle$ cannot be “purely” periodic. As a trivial example, consider the set $M = \{0\} \subset \mathbb{Z}$ for which $p_M(n) = n + 1$ for all $n \geq 1$.

In this context, Presburger definability can be viewed as a natural extension of ultimate periodicity in dimensions higher than one. Before stating the so-called Muchnik's criterion, we need a few definitions.

Definition 6. A set $M \subseteq \mathbb{Z}^d$ is said to be *linear*, if there exist $\mathbf{x} \in \mathbb{Z}^d$ and a finite set (possibly empty) $V \subset \mathbb{Z}^d$ such that

$$M = \{\mathbf{x}\} + \sum_{\mathbf{v} \in V} \mathbb{N}\mathbf{v}.$$

A finite union of linear sets is a *semi-linear* set.

Let $M \subseteq \mathbb{Z}^d$, $i \in \{1, \dots, d\}$ and $c \in \mathbb{Z}$. The *section* $M_{i,c} \subseteq \mathbb{Z}^{d-1}$ is given by

$$M_{i,c} = \{(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_d) \mid (x_1, \dots, x_{i-1}, c, x_{i+1}, \dots, x_d) \in M\}.$$

Definition 7. Let $\mathbf{v} \in \mathbb{Z}^d \setminus \{\mathbf{0}\}$ and $M, X \subseteq \mathbb{Z}^d$. The set M is said to be *\mathbf{v} -periodic inside X* if for any $\mathbf{m}, \mathbf{m} + \mathbf{v} \in X$,

$$\mathbf{m} \in M \Leftrightarrow \mathbf{m} + \mathbf{v} \in M$$

(i.e., any two points inside X that differ by \mathbf{v} either both belong to M or both do not belong to M). We say \mathbf{v} is a *local period* for X . When V is a subset of \mathbb{Z}^d , we say M is *V -periodic inside X* if M is \mathbf{v} -periodic inside X for some $\mathbf{v} \in V$.

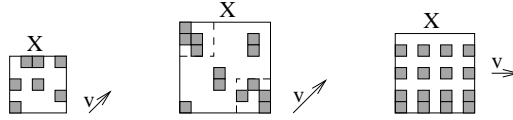


FIGURE 1. Three examples of \mathbf{v} -periodicity inside X .

As we will see definability in $\langle \mathbb{Z}; <, + \rangle$ can be expressed in terms of local periodicity as given in [3].

Definition 8. A set $M \subseteq \mathbb{Z}^d$ is said to be *locally periodic* if there exists a finite set $V \subset \mathbb{Z}^d \setminus \{\mathbf{0}\}$ such that for some $K > \sum_{\mathbf{v} \in V} \|\mathbf{v}\|$ and $L \geq 0$,

$$\forall \mathbf{x} \in \mathbb{Z}^d, \|\mathbf{x}\| \geq L, \exists \mathbf{v} \in V : M \text{ is } \mathbf{v}\text{-periodic inside } \mathcal{B}(\mathbf{x}, K).$$

In [10] an alternative definition of local periodicity is given, see also [2, 8].

Definition 9. Let $M \subseteq \mathbb{Z}^d$. If there exists a finite subset V of $\mathbb{Z}^d \setminus \{\mathbf{0}\}$ verifying: for all $K \geq 1$ there exists $L \in \mathbb{N}$ such that

$$\forall \mathbf{x} \in \mathbb{Z}^d, \|\mathbf{x}\| \geq L, \exists \mathbf{v} \in V : M \text{ is } \mathbf{v}\text{-periodic inside } \mathcal{B}(\mathbf{x}, K),$$

then we say that M *satisfies Muchnik's condition*.

As shown by the following theorem, these two definitions play similar role to characterize definability. The reader may already notice that the sections of M enter the picture.

Theorem 10. [10] *Let M be a subset of \mathbb{Z}^d . The following statements are equivalent.*

- (1) M is definable in $\langle \mathbb{Z}; <, + \rangle$,
- (2) M is semi-linear,
- (3) every section of M is definable in $\langle \mathbb{Z}; <, + \rangle$ and M is locally periodic,
- (4) every section of M is definable in $\langle \mathbb{Z}; <, + \rangle$ and M satisfies Muchnik's condition.

Remark 11. It is clear in Theorem 10 that condition (4) implies condition (3), i.e., Muchnik's condition implies local periodicity. The converse is not so obvious and as observed in [10, p. 1438], a close inspection of the proof of Theorem 10 reveals that assuming (3) is enough to derive the definability of M and that this definability implies Muchnik's condition.

Let A be a finite alphabet, $d \geq 1$ and $S \in A^{\mathbb{Z}^d}$ be a d -dimensional word over A . For each $a \in A$, we define the set

$$S^{-1}(a) := \{\mathbf{x} \in \mathbb{Z}^d \mid S_{\mathbf{x}} = a\}.$$

Definition 12. The word S is *definable* in $\langle \mathbb{Z}; <, + \rangle$ if and only if for all $a \in A$, the sets $S^{-1}(a)$ are definable in $\langle \mathbb{Z}; <, + \rangle$.

We can now recall our main result (stated in the introduction as Theorem 3).

Theorem. *Let M be a subset in \mathbb{Z}^d . This set is definable in $\langle \mathbb{Z}; <, + \rangle$ if and only if $R_M(n) \in \mathcal{O}(n^{d-1})$ and every section is definable in $\langle \mathbb{Z}; <, + \rangle$.*

The case $d = 1$ is equivalent to Morse–Hedlund theorem and was already discussed in Remark 5. Notice that the number of recurrent factors occurring in an ultimately periodic word in $\{0, 1\}^{\mathbb{N}}$ is bounded by a constant. The proof of Theorem 3 is given in Section 4 and Section 5. But prior to these developments, let us make a few immediate comments. Theorem 3 has an immediate application.

Corollary 13. *Let A be a finite alphabet and $d \geq 1$. A d -dimensional word $S \in A^{\mathbb{Z}^d}$ is definable in $\langle \mathbb{Z}; <, + \rangle$ if and only if $R_S(n) \in \mathcal{O}(n^{d-1})$ and every section is definable in $\langle \mathbb{Z}; <, + \rangle$.*

Let $k \in \{1, \dots, d-1\}$. A $(d-k)$ -dimensional section of $M \subseteq \mathbb{Z}^d$ is a subset of \mathbb{Z}^{d-k} where k components have been fixed to constants. So we define the set

$$M_{(i_1, \dots, i_k), (c_1, \dots, c_k)} = \{\mathbf{x} \in M \mid \mathbf{x}_j = c_j, \quad j = 1, \dots, k\}$$

viewed as a subset of \mathbb{Z}^{d-k} . If we apply Theorem 3 recursively, we get the following result expressing definability in Presburger arithmetic solely in terms of recurrent block complexity.

Corollary 14. *A set $M \subseteq \mathbb{Z}^d$ is definable in $\langle \mathbb{Z}; <, + \rangle$ if and only if $R_M(n) \in \mathcal{O}(n^{d-1})$ and, for all $k \in \{1, \dots, d-1\}$, every $(d-k)$ -dimensional section has a recurrent block complexity in $\mathcal{O}(n^{d-k-1})$.*

Using similar arguments as in Remark 5 we can replace in Theorem 3, Corollary 13 and Corollary 14, \mathbb{Z}^d by \mathbb{N}^d and $\langle \mathbb{Z}; <, + \rangle$ by $\langle \mathbb{N}; =, + \rangle$.

3. RUNNING EXAMPLES

We briefly give some examples that we hope could be helpful.

Example 15. Consider the set $M \subset \mathbb{Z}^2$ represented on the left in Figure 2 and defined by the formula

$$\varphi(x, y) := (x \geq 0) \wedge (y \geq 0) \wedge (\exists \lambda)((x, y) = \lambda(1, 1)) \wedge (\exists \lambda)((x, y) = (0, 1) + \lambda(1, 0)).$$

One can show that the block complexity p_M satisfies $p_M(n) \geq n^2$ for n large enough. A simple argument is to observe that the n^2 blocks of size n , $(i, j) + \llbracket 0, n-1 \rrbracket^2$ for $i, j \in \llbracket -n+1, 0 \rrbracket$ are all distinct. Local periodicity is clear with a set of periods

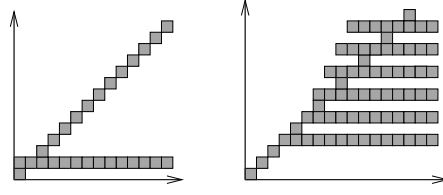


FIGURE 2. Examples of sets definable in Presburger arithmetic.

equal to $V = \{(1, 1), (1, 0)\}$, and, $K = 3$ and $L = 4$. Muchnik's condition is also obvious to check with the same set of periods. The recurrent block complexity is $R_M(n) = 3n$.

Example 16. Consider the set $M \subset \mathbb{Z}^2$ represented on the right in Figure 2 and defined by the formula

$$\begin{aligned} \varphi(x, y) := & (x \geq 0) \wedge (y \geq 0) \wedge ((\exists \lambda)((x, y) = \lambda(1, 1)) \\ & \vee (\exists \lambda)(\exists \mu)((x, y) = (4, 3) + \lambda(1, 0) + \mu(1, 2))). \end{aligned}$$

Notice that this set can also be defined with a quantifier-free formula $\psi(x, y) = (x \geq 0) \wedge (y \geq 0) \wedge (\psi_1(x, y) \vee \psi_2(x, y) \vee \psi_3(x, y))$ where

$$(3.1) \quad \begin{aligned} \psi_1(x, y) &:= (y \geq x) \wedge (2x \geq y + 5) \wedge (y \equiv 1 \pmod{2}), \\ \psi_2(x, y) &:= (y \geq x) \wedge (x \geq y), \\ \psi_3(x, y) &:= (x \geq y) \wedge (y \geq 3) \wedge (y \equiv 1 \pmod{2}). \end{aligned}$$

It is not difficult to compute that the recurrent block complexity is $R_M(n) = 7n - 1$ for all $n \geq 1$.

The following two examples will be used to see that our main result cannot be improved.

Example 17 (Fibonacci). Let $\mathcal{F} = (f_i)_{i \geq 0} = 0100101001 \dots$ be the Fibonacci word generated by the morphism $h : 0 \mapsto 01, 1 \mapsto 0$. It is well-known that $p_{\mathcal{F}}(n) = n + 1$. Now consider the word $\mathcal{G} = (g_i)_{i \in \mathbb{Z}}$ indexed by \mathbb{Z} and defined by

$$g_i = \begin{cases} f_i & \text{if } i \geq 0, \\ 1 & \text{otherwise} \end{cases}$$

$$g = \dots 11111111.0100101001 \dots$$

We have $p_{\mathcal{G}}(n) = 2n$. Consider the set $G \subset \mathbb{Z}^d$ defined by $\mathbf{x} \in G$ if and only if $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_d)$ is such that $g_{\mathbf{x}_1} = 1$. It is clear that G is locally periodic and that $R_G(n) = p_{\mathcal{G}}(n) = 2n$. None of the sections $G_{j,c}$ for $j \geq 2$ can be defined in $\langle \mathbb{Z}; <, + \rangle$. Indeed, the Fibonacci word is not ultimately periodic and therefore not definable in $\langle \mathbb{N}; =, + \rangle$.

Example 18 (Toeplitz'like set). Consider the set $T \subset \mathbb{Z}^2$ depicted in Figure 3 such that

$$(i, j) \in T \Leftrightarrow (i, j \geq 0) \wedge (\exists n > 0 : i = n2^{j+1}).$$

Each section is definable in $\langle \mathbb{Z}; <, + \rangle$ but the set is not locally periodic and does not satisfy Muchnik's condition. It is not difficult to see that $R_T(n) \geq n^2$ since the patterns represented in Figure 4 appear infinitely often. We call it *Toeplitz'like set* because, one can obtain the heights of the successive "heaps" as follows. At first step, consider the infinite word $(0?)^\omega = 0?0? \dots$, on the second step, replace

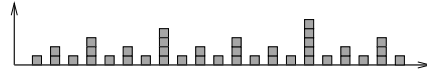


FIGURE 3. Toeplitz'like set.



FIGURE 4. Some blocks of size 3 occurring in T .

in order all the “?” symbols with the letters of the infinite word $(1?)^\omega$. On the $(n + 1)$ -th step, replace the remaining “?” with the letters of the word $(n?)^\omega$. This process generates an infinite word over the alphabet \mathbb{N} whose j -th element is the height of the j -th heap.

4. COMPLEXITY OF PRESBURGER DEFINABLE SETS

In what follows, as explained in Remark 4, we make no distinction between a subset of \mathbb{Z}^d and its characteristic word which belongs to $\{0, 1\}^{\mathbb{Z}^d}$. We consider indifferently complexity functions of both subsets of \mathbb{Z}^d and words indexed by \mathbb{Z}^d . To count the number of different blocks of size n it is convenient to use the following notation:

$$\mathcal{C}(\mathbf{x}, n) = \{\mathbf{y} \in \mathbb{Z}^d \mid \mathbf{y} = \mathbf{x} + \mathbf{z}, \mathbf{z} \in \llbracket 0, n - 1 \rrbracket^d\}.$$

One should avoid the confusion between the neighborhood $\mathcal{B}(\mathbf{x}, n)$ centered at \mathbf{x} given in (2.1) and this set $\mathcal{C}(\mathbf{x}, n)$ pointed at \mathbf{x} .

Proposition 19. *If $X \subseteq \mathbb{Z}^d$ is definable in $\langle \mathbb{Z}; =, + \rangle$, then $R_X(n) \in \mathcal{O}(n^{d-1})$.*

For a better understanding of the main arguments, we first give the proof for $d = 2$.

Proof. Let $X \subseteq \mathbb{Z}^2$ be definable in $\langle \mathbb{Z}; =, + \rangle$. We can assume [12, 13] that the formula defining X is a finite boolean combination of formulas of the kind

$$\lambda_i x + \mu_i y \geq \nu_i, \quad i \in \{1, \dots, r\} \quad \text{or} \quad \lambda_i x + \mu_i y \equiv \alpha_i \pmod{\beta}, \quad i \in \{1, \dots, s\}$$

where the $\alpha_i, \beta, \lambda_i, \mu_i, \nu_i$'s are integers (for an example, see for instance formula (3.1)). Therefore, except for a neighborhood of the origin, X is made up of finite number of regions delimited by two half (straight) lines. Inside such a region X is periodic (the period being determined with the constant β appearing in the formulas given above). In figure 5, no two lines have the same slope. Let us make this assumption first.

Let $n > 0$. Consider one region delimited by two lines $\lambda_i x + \mu_i y = \nu_i, i = 1, 2$. Since their slopes are different, there exists $s(n)$ such that for any \mathbf{x} of norm $\|\mathbf{x}\| > s(n)$, $\mathcal{C}(\mathbf{x}, n)$ intersects at most one line. The number of distinct blocks of size n lying completely in one region R is bounded by a constant r_R (due to the periodicity given by a finite number of congruence relations). The number of different blocks of size n intersecting two regions is bounded by $C n$ where the constant C depends on the periods within the two regions and the period on the line. Indeed the number of relative positions of a square of size n with respect to a given line is bounded by $2n$ (see Figure 6). For each such position, the number of different patterns within the two regions and on the line are bounded respectively by three constants r_1, r_2, r_3

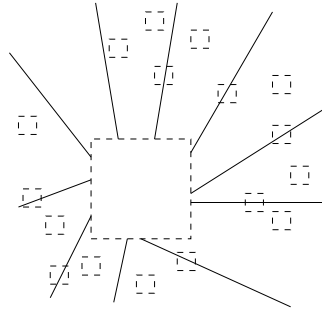


FIGURE 5. Regions in dimension 2.

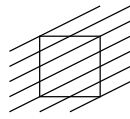


FIGURE 6. Intersection of a square and a line.

(one for each region and one for each line). This gives a number of different blocks bounded by $2r_1r_2r_3n$.

The conclusion follows from the fact that the number of regions is finite. If several lines have the same slope, then one can proceed using the same arguments. (Parallel lines does not increase the linear bound on the complexity, indeed, the number of relative positions of a square of size n with respect to given parallel lines is bounded by a Dn , for some D).

Now consider the general case.

Thanks to quantifier elimination in Presburger arithmetic [6], we can assume that the formula defining X is a finite disjunction of formulas $\varphi_i(x_1, \dots, x_d)$, $i = 1, \dots, k$, where each such formula is a conjunction of the form

$$(4.1) \quad \varphi_i(x_1, \dots, x_d) := \bigwedge_{j=1}^{\ell} t_{i,j}(x_1, \dots, x_d)$$

with

$$(4.2) \quad t_{i,j}(x_1, \dots, x_d) := \sum_{k=1}^d u_k^{(i,j)} x_k \geq c_{i,j}$$

or

$$(4.3) \quad t_{i,j}(x_1, \dots, x_d) := \sum_{k=1}^d u_k^{(i,j)} x_k \equiv e_{i,j} \pmod{\beta}$$

where all the occurring constants are integers. Notice that we can choose the same constant β in every modular equation occurring in the definition of X . Each φ_i defines a domain¹ of \mathbb{Z}^d intersected with a pattern². The following lemma is obvious.

Lemma 20. *The number of distinct blocks of size n for a set $X \subset \mathbb{Z}^d$ defined by a boolean combination of formulas of the kind $\sum_{k=1}^d u_k x_k \equiv e \pmod{\beta}$ is bounded by β^d .*

Let $\pi_{i,j}$ be the hyperplane having equation $\sum u_k^{(i,j)} x_k = c_{i,j}$ corresponding to (4.2). We define $\pi'_{i,j}$ as the vector subspace having equation $\sum u_k^{(i,j)} x_k = 0$. For the sake of simplicity, let us enumerate all the distinct hyperplanes occurring in the quantifier-free formula as $\Pi = \{\pi_1, \dots, \pi_t\}$ (with the corresponding vector subspaces denoted by π'_1, \dots, π'_t).

Let B be a recurrent block of size n , i.e., there exist infinitely many $\mathbf{y}_1, \mathbf{y}_2, \dots$ in \mathbb{Z}^d such that

$$B = X_{\mathbf{y}_1, n} = X_{\mathbf{y}_2, n} = \dots$$

Our aim is to estimate the number of distinct such blocks. Assume that for i large enough, $\mathcal{C}(\mathbf{y}_i, n)$ intersects³ no hyperplane in Π . Then it lies completely in a single domain. We can apply the previous lemma. There are at most β^d different such blocks for each domain and the number of domains is finite (and determined by the formula).

In what follows, we may therefore assume that all the blocks $X_{\mathbf{y}_i, n}$ intersects each of the hyperplanes π_1, \dots, π_j and no other, the \mathbf{y}_i belonging to the same domain D . We can do the reasoning for any subset of Π and any domain D (they are at most 2^t subsets of Π). For the sake of simplicity, we have chosen the first j elements in Π . Then, it suffices to prove, there exists a constant C , not depending on n , such that the number of pairwise distinct recurrent blocks $X_{\mathbf{y}, n}$ intersecting each of the hyperplanes π_1, \dots, π_j and no other, with $\mathbf{y} \in D$, is bounded by Cn^{d-1} .

Lemma 21. *Let B be a block of size n . If there exist infinitely many (different) vectors $\mathbf{y}_1, \mathbf{y}_2, \dots \in \mathbb{Z}^d$ such that, for all i , $\mathcal{C}(\mathbf{y}_i, n)$ intersects each of the hyperplanes π_1, \dots, π_j , then*

$$\dim(\pi'_1 \cap \dots \cap \pi'_j) \geq 1.$$

Proof. Assume to the contrary that the intersection of the vector subspaces $\pi'_1 \cap \dots \cap \pi'_j$ is reduced to $\{\mathbf{0}\}$. Therefore, for a given n , there are finitely many hypercubes $\mathbf{z} + [0, n]^d$ of size n intersecting simultaneously π_1, \dots, π_j , with $\mathbf{z} \in \mathbb{Z}^d$. \square

Now let us assume that $W = \pi'_1 \cap \dots \cap \pi'_j$ is a vector space of dimension $\ell \in \{1, \dots, d-1\}$. Let $(\mathbf{b}_1, \dots, \mathbf{b}_\ell)$ be a basis of W . We can suppose the entries of $\mathbf{b}_1, \dots, \mathbf{b}_\ell$ are integers and multiples of β .

The first idea is to show that a move parallel to W can only gives a constant number of distinct blocks.

¹We call *domain* any subset of \mathbb{Z}^d defined by a conjunction of formulas of the kind (4.2).

²We call *pattern* any subset of \mathbb{Z}^d defined by a conjunction of formulas of the kind (4.3).

³In what follows, when dealing with intersections, one should understand that the underlying hypercube considered as a convex body in \mathbb{R}^d does not intersect any hyperplane.

Lemma 22. *Suppose $\mathcal{C}(\mathbf{v}, n)$, $\mathbf{v} \in D$, intersects each of the hyperplanes π_1, \dots, π_j and no other. Then for all $\mathbf{w} = \alpha_1 \mathbf{b}_1 + \dots + \alpha_\ell \mathbf{b}_\ell$ with $\alpha_1, \dots, \alpha_\ell \in \mathbb{Z}$, $\mathcal{C}(\mathbf{v} + \mathbf{w}, n)$ intersects each of the hyperplanes π_1, \dots, π_j . Furthermore, if $\mathbf{v} + \mathbf{w} \in D$ and $\mathcal{C}(\mathbf{v} + \mathbf{w}, n)$ intersects no other hyperplane, then*

$$X_{\mathbf{v}, n} = X_{\mathbf{v} + \mathbf{w}, n}.$$

Proof. By definition of W , the hypercubes $\mathcal{C}(\mathbf{v}, n)$ and $\mathcal{C}(\mathbf{v} + \mathbf{w}, n)$ have the same relative position with respect to π_1, \dots, π_j . Moreover, since in each domain the pattern is given by congruence relations modulo β , we conclude thanks to the choice made for the basis (each of the components is a multiple of β). \square

Remark 23. There exist finitely many vectors of the kind $\alpha_1 \mathbf{b}_1 + \dots + \alpha_\ell \mathbf{b}_\ell$ belonging \mathbb{Z}^d with $(\alpha_1, \dots, \alpha_\ell) \in \mathbb{Q}^\ell \cap [-1, 1]^\ell$. This observation and the periodicity induced by the previous lemma lead to the following fact. Let $\mathbf{v} \in D$ be such that $\mathcal{C}(\mathbf{v}, n)$ intersects each of the hyperplanes π_1, \dots, π_j and no other. There exists a constant Q (independent of n) such that the number of pairwise distinct blocks $X_{\mathbf{v} + \mathbf{w}, n}$ is bounded by Q when $\alpha_1, \dots, \alpha_\ell \in \mathbb{Q}$ are such that $\mathbf{w} = \alpha_1 \mathbf{b}_1 + \dots + \alpha_\ell \mathbf{b}_\ell \in \mathbb{Z}^d$, $\mathbf{v} + \mathbf{w} \in D$ and $\mathcal{C}(\mathbf{v} + \mathbf{w}, n)$ intersects each of the hyperplanes π_1, \dots, π_j and no other.

Let $\mathbf{e}_1, \dots, \mathbf{e}_{d-\ell}$ be integer vectors such that $(\mathbf{e}_1, \dots, \mathbf{e}_{d-\ell}, \mathbf{b}_1, \dots, \mathbf{b}_\ell)$ is a basis of the space. The idea is now to move in a direction not parallel to W and show that we have $d - \ell$ degrees of freedom.

Lemma 24. *For all $i \in \{1, \dots, d - \ell\}$, there exists a constant $C_i > 0$ such that for all $\mathcal{C}(\mathbf{x}, n)$ intersecting π_1, \dots, π_j at some point $\mathbf{y} \in \mathbb{R}^d$, the following holds:*

- if $\mathcal{C}(\mathbf{x} + k\mathbf{e}_i, n)$ intersects π_1, \dots, π_j , then $|k| \leq C_i n$,
- if $|k| > C_i n$, then $\mathcal{C}(\mathbf{x} + k\mathbf{e}_i, n)$ does not intersect π_1, \dots, π_j .

Proof. Without loss of generality, we may assume $i = 1$. Since \mathbf{e}_1 does not belong to W , there exists $m \in \{1, \dots, j\}$ such that \mathbf{e}_1 does not belong to the vector subspace π'_m . In a system of coordinates built on the basis $(\mathbf{e}_1, \dots, \mathbf{e}_{d-\ell}, \mathbf{b}_1, \dots, \mathbf{b}_\ell)$, we may assume π_m has an equation of the kind

$$\alpha_1^{(m)} x_1 + \dots + \alpha_d^{(m)} x_d = c$$

and that $\mathbf{y} = (a_1, a_2, \dots, a_d)$ belongs to π_m . In this case, the equation of the corresponding vector subspace π'_m is $\alpha_1^{(m)} x_1 + \dots + \alpha_d^{(m)} x_d = 0$. The components of \mathbf{e}_1 in the basis $(\mathbf{e}_1, \dots, \mathbf{e}_{d-\ell}, \mathbf{b}_1, \dots, \mathbf{b}_\ell)$ are $(1, 0, \dots, 0)$ and they do not satisfy the equation of π'_m (otherwise, we would get that $\mathbf{e}_1 \in \pi'_m$). Therefore, $\alpha_1^{(m)}$ is non-zero.

We can determine the values of k such that $(a_1 + k, a_2 + \ell_2, \dots, a_d + \ell_d)$ belongs to π_m for some $\ell_2, \dots, \ell_d \in \llbracket -n, n \rrbracket$. Indeed, this latter point belongs to π_m if and only if

$$\exists \ell_2, \dots, \ell_d \in \llbracket -n, n \rrbracket : \alpha_1^{(m)} k + \alpha_2^{(m)} \ell_2 + \dots + \alpha_d^{(m)} \ell_d = 0.$$

That is, if and only if

$$k = -(\alpha_2^{(m)} \ell_2 + \dots + \alpha_d^{(m)} \ell_d) / \alpha_1^{(m)}.$$

Thus, it suffices to take

$$C_i = \sup_m \frac{d}{|\alpha_i^{(m)}|} \|\alpha^{(m)}\|,$$

where $\alpha^{(m)}$ is the vector whose coordinates are the $\alpha_i^{(m)}$. \square

We are now able to conclude this part of the proof. There are two kinds of recurrent blocks of size n . Those that do not intersect any hyperplane in Π and the others. Let us call $R_X^1(n)$ the number of blocks of the first kind and $R_X^2(n)$ the number of blocks of the second kind. Lemma 20 shows that $R_X^1(n)$ is less than the constant $2^t \beta^d$. To have a bound on $R_X^2(n)$, we make our reasoning only on the recurrent blocks $X_{\mathbf{y}_i, n}$ such that \mathbf{y}_i belongs to a given domain D and $\mathcal{C}(\mathbf{y}_i, n)$ intersects each of the hyperplanes π_1, \dots, π_j and no other (recall that there is only a constant number of such cases to take into account). Thanks to Lemma 22 and Remark 23, moving such a block in any direction parallel to W leads to a number of pairwise distinct blocks bounded by a constant. On the other hand, when moving in a direction spanned by $\mathbf{e}_1, \dots, \mathbf{e}_{d-\ell}$, Lemma 24 shows that we can have up to $\mathcal{O}(n^{d-\ell})$ pairwise distinct blocks of size n . Recall from Lemma 21 that $\ell = \dim W$ belongs to $\{1, \dots, d-1\}$. Furthermore, as suggested by the following example, the bound on R_X^2 is tight. Consider the hyperplanes having respectively equation $x_1 = x_2, x_2 = x_3, \dots, x_{d-\ell} = x_{d-\ell+1}$ defining $2^{d-\ell}$ regions having each a different pattern. \square

5. PROOF OF THE CONVERSE

In what follows, as explained in Remark 4, we make no distinction between a subset of \mathbb{Z}^d and its characteristic word which belongs to $\{0, 1\}^{\mathbb{Z}^d}$. We consider indifferently complexity functions of both subsets of \mathbb{Z}^d and words indexed by \mathbb{Z}^d .

5.1. An interesting lemma. The following lemma based on the pigeonhole principle is of particular importance in what follows. Proven in [14] for $d = 2$, we simply adapt it to our setting.

Lemma 25. *Let $M \subset \mathbb{Z}^d$ and $C > 0$ be such that $R_M(n) \leq Cn^{d-1}$ for all n . Let $n \in \mathbb{N}$. There exists $m_0 \in \mathbb{N}$ such that, for all m satisfying $m < n$ and $m^d - Cn^{d-1} \geq 1$, and all $\mathbf{z} = (\mathbf{z}_i)_{1 \leq i \leq d}$, with $\|\mathbf{z}\| \geq m_0 + m$, there exists a non-zero vector $\mathbf{v} = (\mathbf{v}_i)_{1 \leq i \leq d}$ with $\|\mathbf{v}\| \leq m$, verifying*

$$M_{\mathbf{z}-\mathbf{v}, n-m} = M_{\mathbf{z}, n-m} = M_{\mathbf{z}+\mathbf{v}, n-m}.$$

Proof. Far enough from the origin, every block is recurrent. Formally, take $n \in \mathbb{N}$. There exists m_0 such that if $\|\mathbf{x}\| \geq m_0$, then $M_{\mathbf{x}, n}$ is recurrent in M . Let m and $\mathbf{z} = (\mathbf{z}_i)_{1 \leq i \leq d}$ be such that $m < n$, $m^d - Cn^{d-1} \geq 1$ and $\|\mathbf{z}\| \geq m_0 + m$. If $\mathbf{y} \in \llbracket -m+1, 0 \rrbracket^d$, then $\|\mathbf{z} + \mathbf{y}\| \geq m_0$. Therefore, for all $\mathbf{y} \in \llbracket -m+1, 0 \rrbracket^d$, the blocks $M_{\mathbf{z}+\mathbf{y}, n}$ are recurrent. Since $R_M(n) < m^d$, by the pigeonhole principle, there exist two distinct integer vectors $\mathbf{y}, \mathbf{y}' \in \llbracket -m+1, 0 \rrbracket^d$ such that $M_{\mathbf{z}+\mathbf{y}, n} = M_{\mathbf{z}+\mathbf{y}', n}$. Let $\mathbf{v} = \mathbf{y} - \mathbf{y}'$. We observe that $\|\mathbf{v}\| \leq m$. Now consider \mathbf{x} in $\{\mathbf{z}\} + \llbracket 0, n-m-1 \rrbracket^d$, then \mathbf{x} and $\mathbf{x} + \mathbf{v}$ belong to $\{\mathbf{z} + \mathbf{y}\} + \llbracket 0, n-1 \rrbracket^d$, and, \mathbf{x} and $\mathbf{x} - \mathbf{v}$ belong to $\{\mathbf{z} + \mathbf{y}'\} + \llbracket 0, n-1 \rrbracket^d$. The situation is depicted in Figure 7. The conclusion follows from the fact that $M_{\mathbf{z}+\mathbf{y}, n} = M_{\mathbf{z}+\mathbf{y}-\mathbf{v}, n}$ and from the overlap of the two blocks. \square

The following corollary shows that Lemma 25 is ‘‘almost’’ sufficient to complete the proof of Theorem 3.

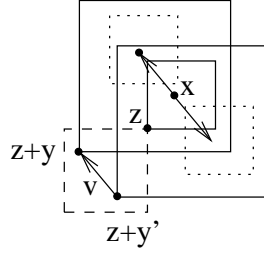


FIGURE 7. Sketch of the situation in Lemma 25.

Corollary 26. *Let $M \subseteq \mathbb{Z}^d$. Suppose there exists $C > 0$ such that $R_M(n) \leq Cn^{d-1}$ for all n . Then, for all large enough K there exists $L \geq 0$ such that*

$$\forall \mathbf{x} \in \mathbb{Z}^d, \|\mathbf{x}\| \geq L, \exists \mathbf{v}, \|\mathbf{v}\| \leq (2C)^{\frac{1}{d}}(5K)^{\frac{d-1}{d}} : M \text{ is } \mathbf{v}\text{-periodic inside } \mathcal{B}(\mathbf{x}, K).$$

Proof. The result is easy to obtain for $d = 1$. Thus we suppose $d \geq 2$. Consider the following maps $\alpha : n \mapsto (1 + Cn^{d-1})^{1/d}$, $\gamma : n \mapsto (2C)^{1/d}n^{\frac{d-1}{d}}$ and $\beta : n \mapsto (n - \gamma(n))/4$. Let n_0 be such that

- β is increasing on $[n_0, +\infty[$;
- $\gamma(n) < n$ for all $n \geq n_0$;
- $\gamma(n) \leq \beta(n - 1)$ for all $n \geq n_0$;
- $n \leq 5\beta(n - 1)$ for all $n \geq n_0$.

Let K, n be integers such that $K \geq \beta(n_0)$, $n \geq n_0 + 1$ and $\beta(n - 1) \leq K \leq \beta(n)$. Let m_0 be given by Lemma 25. Let m be an integer satisfying $\alpha(n) \leq m \leq \gamma(n)$. Notice that m satisfies the assumption of Lemma 25. We set $L = m_0 + m + 2K$. Let \mathbf{x} satisfying $\|\mathbf{x}\| \geq L$. Let $\mathbf{1}$ be the vector consisting of ones. From Lemma 25, since $\|\mathbf{x} - 2K\mathbf{1}\| \geq m_0 + m$, there exists a vector \mathbf{v} , with $\|\mathbf{v}\| \leq m$ such that $M_{\mathbf{x}-2K\mathbf{1}, n-m} = M_{\mathbf{x}-2K\mathbf{1}+\mathbf{v}, n-m}$. But as $n - m \geq n - \gamma(n) = 4\beta(n) \geq 4K$, we also have

$$M_{\mathbf{x}-2K\mathbf{1}, 4K} = M_{\mathbf{x}-2K\mathbf{1}+\mathbf{v}, 4K}.$$

Thus, M is \mathbf{v} -periodic inside $\mathcal{B}(\mathbf{x}, K)$. Moreover, from the choice of n_0 we obtain that

$$\|\mathbf{v}\| \leq m \leq (2C)^{1/d}n^{\frac{d-1}{d}} \leq (2C)^{1/d}(5\beta(n-1))^{\frac{d-1}{d}} \leq (2C)^{1/d}(5K)^{\frac{d-1}{d}}.$$

This completes the proof. \square

In order to obtain local periodicity as given in Definition 8 leading to a proof of Theorem 3, it would be nice that Corollary 26 implies the existence of a set $V \subset \mathbb{Z}^d$ such that $K > \sum_{\mathbf{v} \in V} \|\mathbf{v}\|$. This is the case in particular for $d = 2$ (as presented below). For $d \geq 3$ we are not able to give such a direct proof as for $d = 2$. Nevertheless this corollary is interesting because it provides us with a finite set of quite small local periods. We will use it when $d \geq 3$.

5.2. Proof of Theorem 3 for $d = 2$. The following two lemmata are also true in higher dimensions. The first one is another way to settle down the underlying idea of Lemma 25. Let $\mathbf{1}$ be the vector consisting of ones.

Lemma 27. *Let $M \subset \mathbb{Z}^2$. Suppose M is \mathbf{v} -periodic inside $\mathcal{B}(\mathbf{x}, n)$, for some $\mathbf{v} \neq 0$, $\|\mathbf{v}\| < n$, and is not \mathbf{w} -periodic for any \mathbf{w} with $\|\mathbf{w}\| < \|\mathbf{v}\|$. Then, the $\|\mathbf{v}\|^2$ blocks $M_{\mathbf{x}-n\mathbf{1}-\mathbf{z}, 2n+\|\mathbf{v}\|}$ with $\mathbf{z} \in \llbracket 0, \|\mathbf{v}\| - 1 \rrbracket^2$ are pairwise distinct.*

Proof. Suppose there exist two distinct vectors \mathbf{z}_1 and \mathbf{z}_2 in $\llbracket 0, \|\mathbf{v}\| - 1 \rrbracket^2$ such that $M_{\mathbf{x}-n\mathbf{1}-\mathbf{z}_1, 2n+\|\mathbf{v}\|}$ and $M_{\mathbf{x}-n\mathbf{1}-\mathbf{z}_2, 2n+\|\mathbf{v}\|}$ are equal. Let $\mathbf{w} = \mathbf{z}_1 - \mathbf{z}_2$. Then, $\|\mathbf{w}\| < \|\mathbf{v}\|$ and M is \mathbf{w} -periodic inside $\mathcal{B}(\mathbf{x}, n)$. \square

Lemma 28. *Let $n \in \mathbb{N}$, $M \subset \mathbb{Z}^2$ and $\mathbf{v}_1, \dots, \mathbf{v}_k, \mathbf{x}_1, \dots, \mathbf{x}_k$ be vectors of \mathbb{Z}^2 such that*

- (1) $\mathbf{0}, \mathbf{v}_1, \dots, \mathbf{v}_k$ are pairwise distinct;
- (2) $\ell = \max \|\mathbf{v}_i\| \leq n$;
- (3) for all i , M is \mathbf{v}_i -periodic inside $\mathcal{B}(\mathbf{x}_i, n)$ and is not \mathbf{w} -periodic inside $\mathcal{B}(\mathbf{x}_i, n)$ for any \mathbf{w} with $\|\mathbf{w}\| < \|\mathbf{v}_i\|$;
- (4) for all i , M is not \mathbf{v}_j -periodic inside $\mathcal{B}(\mathbf{x}_i, n)$ for $j < i$.

Then, we have

$$\# \{M_{\mathbf{x}_i-n\mathbf{1}-\mathbf{z}, 2n+\ell} \mid \mathbf{z} \in \llbracket 0, \|\mathbf{v}_i\| - 1 \rrbracket^2, 1 \leq i \leq k\} = \sum_{i=1}^k \|\mathbf{v}_i\|^2.$$

Proof. From Lemma 27, for all i , we have

$$\# \{M_{\mathbf{x}_i-n\mathbf{1}-\mathbf{z}, 2n+\|\mathbf{v}_i\|} \mid \mathbf{z} \in \llbracket 0, \|\mathbf{v}_i\| - 1 \rrbracket^2\} = \|\mathbf{v}_i\|^2$$

and thus, when considering possibly larger blocks, we get

$$\# \{M_{\mathbf{x}_i-n\mathbf{1}-\mathbf{z}, 2n+\ell} \mid \mathbf{z} \in \llbracket 0, \|\mathbf{v}_i\| - 1 \rrbracket^2\} = \|\mathbf{v}_i\|^2.$$

Let i, j be such that $1 \leq j < i \leq k$. It is sufficient to prove that, for all vectors $\mathbf{z}_i \in \llbracket 0, \|\mathbf{v}_i\| - 1 \rrbracket^2$ and $\mathbf{z}_j \in \llbracket 0, \|\mathbf{v}_j\| - 1 \rrbracket^2$, the blocks $M_{\mathbf{x}_i-n\mathbf{1}-\mathbf{z}_i, 2n+\ell}$ and $M_{\mathbf{x}_j-n\mathbf{1}-\mathbf{z}_j, 2n+\ell}$ are distinct.

Indeed, suppose there exist \mathbf{z}_i and \mathbf{z}_j such that $M_{\mathbf{x}_i-n\mathbf{1}-\mathbf{z}_i, 2n+\ell}$ and $M_{\mathbf{x}_j-n\mathbf{1}-\mathbf{z}_j, 2n+\ell}$ are equal. Then, since $\mathcal{B}(\mathbf{x}_i, n)$ is included in $\mathcal{B}(\mathbf{x}_i - n\mathbf{1} - \mathbf{z}_i, 2n + \ell)$, M would be \mathbf{v}_j -periodic inside $\mathcal{B}(\mathbf{x}_i, n)$. This contradicts our assumption (4). \square

Let us conclude with the proof of Theorem 3 for $d = 2$. Let $M \subset \mathbb{Z}^2$ such that for some C we have $R_M(n) \leq Cn$, for all n , and having all its sections definable in $\langle \mathbb{Z}; <, + \rangle$. Thanks to Theorem 10, it suffices to prove that M is locally periodic. Taking in Corollary 26 a large enough K , M satisfies the following property:

(P) there exist two positive integers K and L' such that

- (1) $\forall \mathbf{x} \in \mathbb{Z}^2, \|\mathbf{x}\| \geq L', \exists \mathbf{v}, \|\mathbf{v}\| \leq \sqrt{10CK} : M$ is \mathbf{v} -periodic inside $\mathcal{B}(\mathbf{x}, K)$;
- (2) $\sqrt{10CK} \leq K$;
- (3) $8 \log(K)^3 + \frac{3CK}{\log(K)} < K$.

Let L'' be such that if $\|\mathbf{x}\| \geq L''$, then the block $M_{\mathbf{x}, 3K}$ is recurrent. Let L be greater than $2K + L'' + L'$. We need the following lemma.

Lemma 29. *There exist vectors $\mathbf{x}_1, \dots, \mathbf{x}_k \in \mathbb{Z}^2$ and $V = \{\mathbf{v}_1, \dots, \mathbf{v}_k\} \subset \mathbb{Z}^2$ such that*

- (1) for all $\mathbf{x} \in \mathbb{Z}^2, \|\mathbf{x}\| \geq L$, there exists $\mathbf{v} \in V$ such that M is \mathbf{v} -periodic inside $\mathcal{B}(\mathbf{x}, K)$;

- (2) for all i , $\|\mathbf{v}_i\| \leq \sqrt{10CK}$;
- (3) $\mathbf{0}, \mathbf{v}_1, \dots, \mathbf{v}_k$ are pairwise distinct;
- (4) $\|\mathbf{x}_i\| \geq L$ for all i ;
- (5) for all i , M is \mathbf{v}_i -periodic inside $\mathcal{B}(\mathbf{x}_i, K)$ and is not \mathbf{w} -periodic inside $\mathcal{B}(\mathbf{x}_i, K)$ for any \mathbf{w} with $\|\mathbf{w}\| < \|\mathbf{v}_i\|$;
- (6) for all i , M is not \mathbf{v}_j -periodic inside $\mathcal{B}(\mathbf{x}_i, K)$ for $j < i$.

Proof. Let (\mathbf{u}_i) be a sequence consisting of all vectors of $\mathbb{Z}^2 \setminus \{\mathbf{0}\}$, appearing only once, which is non-decreasing with respect to their norms. Let R be the set of recurrent blocks of size K . Note that from Property **(P)** all elements of R are \mathbf{v} -periodic for some \mathbf{v} whose norm is less than $\sqrt{10CK}$. Let R_0 be the set of recurrent blocks of size K having \mathbf{u}_0 as a local period. Of course, R_0 can be empty. Let R_1 be the subset of $R \setminus R_0$ whose blocks have the local period \mathbf{u}_1 . Observe that these blocks do not have \mathbf{u}_0 as a local period. Continuing this way, we obtain finitely many non-empty subsets R_{i_1}, \dots, R_{i_k} of R such that

- (1) $R = \cup_{n=1}^k R_{i_n}$;
- (2) the blocks of R_{i_n} have \mathbf{u}_{i_n} as a local period;
- (3) for all $s \in \{1, \dots, k\}$ and $j < i_s$, \mathbf{u}_j is not a local period for blocks in R_{i_s} .

Property **(P)** ensures that for all s , $\|\mathbf{u}_{i_s}\| \leq \sqrt{10CK}$. We set $\mathbf{v}_s = \mathbf{u}_{i_s}$. For all s , there exists $\mathbf{x}_s \in \mathbb{Z}^2$ such that M is \mathbf{v}_s -periodic inside $\mathcal{B}(\mathbf{x}_s, K)$. The choice of L allows us to suppose $\|\mathbf{x}_s\| \geq L$. This concludes the proof. \square

Let $\ell = \max_{\mathbf{v} \in V} \|\mathbf{v}\|$. Lemma 29 provides us with vectors $\mathbf{x}_1, \dots, \mathbf{x}_k \in \mathbb{Z}^2$ and a set $V = \{\mathbf{v}_1, \dots, \mathbf{v}_k\} \subset \mathbb{Z}^2$ fulfilling the hypothesis of Lemma 28. To get local periodicity it remains to show that $\sum_{\mathbf{v} \in V} \|\mathbf{v}\| < K$. Applying Lemma 28, we obtain

$$\sum_{\mathbf{v} \in V} \|\mathbf{v}\|^2 \leq R_M(2K + \ell) \leq C(2K + \ell).$$

Using Property **(P)**, we deduce that $\ell \leq \sqrt{10CK} \leq K$. Hence

$$\sum_{\mathbf{v} \in V} \|\mathbf{v}\|^2 \leq 3CK.$$

Let $\delta_n = \#\{\mathbf{v} \in V \mid \|\mathbf{v}\| = n\}$. Then, we have

$$\log(K)^2 \sum_{n=\lfloor \log(K) \rfloor}^{\lfloor \sqrt{10CK} \rfloor} \delta_n \leq \sum_{n=1}^{\lfloor \sqrt{10CK} \rfloor} \delta_n n^2 = \sum_{\mathbf{v} \in V} \|\mathbf{v}\|^2 \leq 3CK.$$

Consequently, we get

$$\sum_{n=\lfloor \log(K) \rfloor}^{\lfloor \sqrt{10CK} \rfloor} \delta_n \leq \frac{3CK}{\log(K)^2}.$$

Hence, using Cauchy–Schwarz inequality, we deduce that

$$\begin{aligned} \sum_{n=\lfloor \log(K) \rfloor}^{\lfloor \sqrt{10CK} \rfloor} \delta_n n &= \sum_{n=\lfloor \log(K) \rfloor}^{\lfloor \sqrt{10CK} \rfloor} \sqrt{\delta_n} \sqrt{\delta_n} n \\ &\leq \left(\sum_{n=\lfloor \log(K) \rfloor}^{\lfloor \sqrt{10CK} \rfloor} \delta_n \right)^{1/2} \left(\sum_{n=\lfloor \log(K) \rfloor}^{\lfloor \sqrt{10CK} \rfloor} \delta_n n^2 \right)^{1/2} \leq \frac{3CK}{\log(K)}. \end{aligned}$$

Using the fact that, for all n ,

$$\delta_n \leq \#\{\mathbf{v} \in \mathbb{Z}^2 \mid \|\mathbf{v}\| = n\} = \# \bigcup_{i=-n}^n \{(i, n), (i, -n), (n, i), (-n, i)\} = 8n,$$

we deduce that

$$\begin{aligned} \sum_{\mathbf{v} \in V} \|\mathbf{v}\| &= \sum_{n=1}^{\lfloor \sqrt{10CK} \rfloor} \delta_n n \leq \sum_{n=1}^{\lfloor \log(K) \rfloor - 1} \delta_n n + \frac{3CK}{\log(K)} \\ &\leq 8 \sum_{n=1}^{\lfloor \log(K) \rfloor - 1} n^2 + \frac{3CK}{\log(K)} \leq 8 \log(K)^3 + \frac{3CK}{\log(K)} < K. \end{aligned}$$

This concludes the proof for $d = 2$.

Observe that this kind of computation gives nothing in dimension $d \geq 3$ because, given some constants a, b, c one should find some sufficiently large K and a function $\alpha(K)$ such that $a + b\alpha(K)^{d+1} + \frac{cK^{d-1}}{\alpha(K)} < K$. This is clearly not possible. But, maybe some of the above inequalities could be improved in order to have a direct proof for all $d \geq 3$. We leave this as an open question.

5.3. Proof of Theorem 3 in the general case. It remains to prove that if M is a subset in \mathbb{Z}^d such that $R_M(n) \in \mathcal{O}(n^{d-1})$ and every section is definable in $\langle \mathbb{Z}; <, + \rangle$, then it is definable in $\langle \mathbb{Z}; <, + \rangle$. Let us first recall some crucial results of Muchnik. For all $A \subset \mathbb{Z}^d$ and $\mathbf{v} \in \mathbb{Z}^d$, we define the *border of A in the direction \mathbf{v}* as

$$\mathbf{Bd}(A, \mathbf{v}) := \{\mathbf{x} \in A \mid \mathbf{x} + \mathbf{v} \notin A\}.$$

The following two lemmata show that it is sufficient to prove that, for some \mathbf{v} , the set $\mathbf{Bd}(M, \mathbf{v})$ is locally periodic.

Lemma 30. [10, Lemma 1.0] *Let $A \subset \mathbb{Z}^d$ and $\mathbf{v} \in \mathbb{Z}^d$. If all sections of A are definable, then all sections of $\mathbf{Bd}(A, \mathbf{v})$ are definable.*

Lemma 31. [10, Lemma 1.2] *Let $A \subset \mathbb{Z}^d$ and $\mathbf{v} \in \mathbb{Z}^d$. The set A is definable in terms of $\mathbf{Bd}(A, \mathbf{v})$, $\mathbf{Bd}(A, -\mathbf{v})$ and a finite number of sections of A , i.e., A can be defined by a formula that uses addition, order and unary predicates for the sets $\mathbf{Bd}(A, \mathbf{v})$, $\mathbf{Bd}(A, -\mathbf{v})$ and for a finite number of sections of A .*

The next lemma suggests to proceed by induction on the cardinality of the set of local periods to prove that $\mathbf{Bd}(M, \mathbf{v})$ is locally periodic.

Lemma 32. [10, Lemma 1.1] *Let $A \subset \mathbb{Z}^d$. Suppose there exist $K, L \geq 0$ and a finite set $V \subset \mathbb{Z}^d \setminus \{\mathbf{0}\}$ verifying that, for all $\mathbf{x} \in \mathbb{Z}^d$ with $\|\mathbf{x}\| \geq L$, the set A is V -periodic inside $\mathcal{B}(\mathbf{x}, K)$. Then, for all $\mathbf{v} \in \mathbb{Z}^d$ and all $\mathbf{x} \in \mathbb{Z}^d$ with $\|\mathbf{x}\| \geq L$, the set $\mathbf{Bd}(A, \mathbf{v})$ is $V \setminus \{\mathbf{v}, -\mathbf{v}\}$ -periodic inside $\mathcal{B}(\mathbf{x}, K)$.*

To complete the proof of Theorem 3 we will proceed by induction on the cardinality of V .

We will say that a set $M \subseteq \mathbb{Z}^d$ satisfies $\text{Hyp}(k)$ whenever :

- (1) there exists $C > 0$ such that, for all large enough $n \in \mathbb{N}$, $R_M(n) \leq Cn^{d-1}$;
- (2) all sections of M are definable;
- (3) there exist $K, L \geq 0$ and $V \subset \mathbb{Z}^d \setminus \{\mathbf{0}\}$ verifying
 - (a) $\forall \mathbf{x} \in \mathbb{Z}^d, \|\mathbf{x}\| \geq L, \exists \mathbf{v} \in V : M$ is \mathbf{v} -periodic inside $\mathcal{B}(\mathbf{x}, K)$,
 - (b) $\forall \mathbf{v} \in V, \|\mathbf{v}\| \leq (2C)^{\frac{1}{d}}(5K)^{\frac{d-1}{d}} < K$, and,
 - (c) $\#V = k$.

We note that, from Corollary 26, the subsets of \mathbb{Z}^d such that $R_M(n) \in \mathcal{O}(n^{d-1})$ and having all its sections definable in $(\mathbb{Z}; <, +)$, satisfy $\text{Hyp}(k)$ for some k . Hence, to complete the proof of Theorem 3 it is sufficient to prove that the following assertion $P(k)$ is true for all k .

$P(k) : \quad \text{If } M \subseteq \mathbb{Z}^d \text{ satisfies } \text{Hyp}(k), \text{ then it is definable.}$

If M satisfies $\text{Hyp}(1)$ then (3) corresponds to the local periodicity of M . Hence $P(1)$ is true.

Let $k \geq 1$ be such that $P(1), \dots, P(k)$ are true. Let M be a subset of \mathbb{Z}^d satisfying $\text{Hyp}(k+1)$. It remains to prove that M is definable. Let C, V, K and L be given by $\text{Hyp}(k+1)$ for M .

Lemma 33. *For all $\mathbf{v} \in \mathbb{Z}^d$ and $\epsilon > 0$ there exists n_0 such that if $n \geq n_0$, then $R_{\mathbf{Bd}(M, \mathbf{v})}(n) \leq (C + \epsilon)n^{d-1}$.*

Proof. It suffices to see that $R_{\mathbf{Bd}(M, \mathbf{v})}(n) \leq R_M(n + \|\mathbf{v}\|)$ for all $n \in \mathbb{N}$. □

Lemma 34. *For all $\mathbf{v} \in V$ the sets $\mathbf{Bd}(M, \mathbf{v})$ and $\mathbf{Bd}(M, -\mathbf{v})$ satisfy $\text{Hyp}(k)$.*

Proof. Let $\mathbf{w} \in \{\mathbf{v}, -\mathbf{v}\}$. From Lemma 33 there exists $\epsilon > 0$ such that

$$(2(C + \epsilon))^{\frac{1}{d}}(5K)^{\frac{d-1}{d}} < K \text{ and } R_{\mathbf{Bd}(M, \mathbf{w})}(n) \leq (C + \epsilon)n^{d-1}$$

for all large enough n . From Lemma 30 all sections of $\mathbf{Bd}(M, \mathbf{w})$ are definable. We take for $\mathbf{Bd}(M, \mathbf{w})$ the constants K, L and the set V of M . With Lemma 32 we know that $\mathbf{Bd}(M, \mathbf{w})$ is $V \setminus \{\mathbf{v}, -\mathbf{v}\}$ -periodic inside $\mathcal{B}(\mathbf{x}, K)$ for all \mathbf{x} with $\|\mathbf{x}\| \geq L$, and, thus satisfies $\text{Hyp}(k)$. □

We can now conclude the proof of Theorem 3. Let $\mathbf{v} \in V$. From Lemma 34, $\mathbf{Bd}(M, \mathbf{v})$ and $\mathbf{Bd}(M, -\mathbf{v})$ satisfy $\text{Hyp}(k)$. Then from $P(k)$ we deduce it is definable. Hence, from Lemma 31, M is definable.

REFERENCES

- [1] V. Berthé and L. Vuillon. Tilings and rotations on the torus: a two-dimensional generalization of Sturmian sequences. *Discrete Math.*, 223:27–53, 2000.
- [2] A. Bès. A survey of arithmetical definability. *Bull. Belg. Math. Soc. Simon Stevin*, suppl.:1–54, 2001. A tribute to Maurice Boffa.

- [3] V. Bruyère, G. Hansel, C. Michaux, and R. Villemaire. Logic and p -recognizable sets of integers. *Bull. Belg. Math. Soc.*, 1:191–238, 1994. Corrigendum, *Bull. Belg. Math. Soc.* **1** (1994), 577.
- [4] J. Cassaigne. Subword complexity and periodicity in two or more dimensions. In G. Rozenberg and W. Thomas, editors, *Developments in Language Theory 1999*, pages 14–21. World Scientific, 2000.
- [5] A. Cobham. On the base-dependence of sets of numbers recognizable by finite automata. *Math. Systems Theory*, 3:186–192, 1969.
- [6] H. B. Enderton. *A mathematical introduction to logic*. Academic Press, New York, 2001.
- [7] C. Epifanio, M. Koskas, and F. Mignosi. On a conjecture on bidimensional words. *Theoret. Comput. Sci.*, 299(1-3):123–150, 2003.
- [8] C. Michaux and R. Villemaire. Presburger arithmetic and recognizability of sets of natural numbers by automata: New proofs of Cobham's and Semenov's theorems. *Ann. Pure Appl. Logic*, 77:251–277, 1996.
- [9] M. Morse and G. A. Hedlund. Symbolic dynamics. *Amer. J. Math.*, 60:815–866, 1938.
- [10] A. A. Muchnik. The definable criterion for definability in Presburger arithmetic and its applications. *Theoret. Comput. Sci.*, 290(3):1433–1444, 2003.
- [11] M. Nivat. invited talk at icalp, bologna, 1997.
- [12] M. Presburger. Über die vollständigkeit eines gewissen systems der arithmetik ganzer zahlen, in welchem die addition als einzige operation hervortritt. *C. R. Premier congrès des Mathématiciens des pays slaves, Varsovie*, pages 92–101, 1929.
- [13] M. Presburger. On the completeness of a certain system of arithmetic of whole numbers in which addition occurs as the only operation. *Hist. Philos. Logic*, 12:225–233, 1991.
- [14] A. Quas and L. Zamboni. Periodicity and local complexity. *Theoret. Comput. Sci.*, 319:229–240, 2004.
- [15] J. W. Sander and R. Tijdeman. The rectangle complexity of functions on two-dimensional lattices. *Theoret. Comput. Sci.*, 270:857–863, 2002.
- [16] A. L. Semenov. The Presburger nature of predicates that are regular in two number systems. *Sibirsk. Mat. Z.*, 18(2):403–418, 479, 1977. In Russian. English translation in *Siberian J. Math.* **18** (1977), 289–300.
- [17] R. Tijdeman. Periodicity and almost-periodicity. In *More sets, graphs and numbers*, volume 15 of *Bolyai Soc. Math. Stud.*, pages 381–405. Springer, Berlin, 2006.

(F.D.)

UNIVERSITÉ DE PICARDIE JULES VERNE
 LABORATOIRE AMIÉNOIS DE MATHÉMATIQUES FONDAMENTALES ET APPLIQUÉES
 UMR 6140 CNRS UPJV
 33 RUE SAINT LEU
 80039 AMIENS CEDEX 01
 FRANCE.
E-mail address: fabien.durand@u-picardie.fr

(M.R.)

UNIVERSITÉ DE LIÈGE
 INSTITUT DE MATHÉMATIQUE
 GRANDE TRAVERSE 12 (B 37)
 B-4000 LIÈGE
 BELGIUM.
E-mail address: M.Rigo@ulg.ac.be