Primitive roots of bi-periodic infinite pictures

Nicolas Bacquey

Primitive roots of bi-periodic infinite pictures

Nicolas Bacquey

GREYC - Université de Caen Basse-Normandie / ENSICAEN / CNRS
Campus Côte de Nacre, Boulevard du Maréchal Juin
CS 14032 CAEN cedex 5, FRANCE

Abstract. This paper defines and studies the notion of *primitive root* of a bi-periodic infinite picture, that is a rectangular pattern that tiles the bi-periodic picture and contains exactly one representative of each equivalence class of its pixels. This notion extends to dimension 2 the notion of primitive root of a bi-infinite periodic word.
We prove that, for each bi-periodic infinite picture P,
- there exists at least one primitive root of P;
- there are at most two ordered pairs of positive integers (m, n) such that every primitive root of P has size $m \times n$;
- for each such pair (m, n), every rectangular pattern of size $m \times n$ extracted from P is a primitive root of P.

We also discuss some additional properties of primitive roots.

1 Introduction: Primitive words in dimension 1 and 2

In the field of formal languages, primitive words are finite words that are not a power of a smaller word. These words are a well studied subject, with an array of open problems related to them. For instance, it is unknown if the language of all primitive words is context-free (see *e.g.* [5] or [7] for more matter on primitive languages). In this paper, we will define an extension of that notion over words of dimension 2, *i.e.* pictures over a finite alphabet. It is important to note that we will consider rectangular words *as part of a bi-periodic, infinite picture* instead of independently from their surroundings. Informally speaking, we will say that primitive rectangular words will be the smallest rectangular words with which we will be able to rebuild the whole infinite picture by translation.

A trivial extension of the notion of primitive words would be to say that a rectangular word is primitive if it is primitive in both directions. However, our twist in the definition will allow us to consider a broader array of primitive words than this trivial extension.

The work presented in this paper originated from the field of Cellular Automata, which are a massively parallel computational model (see [4] or [6]). Our initial goal was to design an algorithm able to perform leader election over infinite periodical pictures [1,2]. We noticed that the set of leaders of an infinite picture constitute a lattice, and that this lattice could be used to delimit finite rectangular words.

Those particular words, which are the *primitive roots* we will discuss in this article, appear to have very interesting properties that closely relate to formal language theory. We will first formally define those primitive roots, then we will

give a tight upper bound to their number (they are not unique up to a shift, as it happens with languages of dimension 1). Finally, we will discuss some of their most interesting properties.

2 Context and definitions

We will now introduce a few definitions that will lead to the proper definition of a primitive root of a bi-dimensional picture.

Definition 1 (pictures). *Let Σ be a finite alphabet, we call* picture *a function $P : \mathbb{Z}^2 \to \Sigma$. We say that a picture P is* bi-periodic *if there is a pair of non-collinear vectors $(x_0, y_0), (x_1, y_1) \in \mathbb{Z}^2$ called a* period *of P such that*
$\forall (x, y) \in \mathbb{Z}^2$*:*
$P(x + x_0, y + y_0) = P(x, y)$
$P(x + x_1, y + y_1) = P(x, y)$.
In the context of pictures, an element $p \in \mathbb{Z}^2$ is called a pixel.

All along this article, every picture we talk about will be bi-periodic, except when noted otherwise.

Definition 2 (shift functions). *We introduce the* horizontal shift function σ_h *and the* vertical shift function σ_v *defined over pictures as follows :*
$\forall (x, y) \in \mathbb{Z}^2$
$\sigma_h(P)(x, y) = P(x + 1, y)$
$\sigma_v(P)(x, y) = P(x, y + 1)$.

Figure 1 illustrates the action of these functions over a bi-periodic picture. It is immediate to see that those functions are invertible, and that they commute with each other.

2	1	2	1	2	1	2	1
1	0	1	0	1	0	1	0
1	2	1	2	1	2	1	2
0	1	0	1	0	1	0	1
2	1	2	1	2	1	2	1
1	0	1	0	1	0	1	0
1	2	1	2	1	2	1	2
0	1	0	1	0	1	0	1

(a) The original picture P

0	1	0	1	0	1	0	1
2	1	2	1	2	1	2	1
1	0	1	0	1	0	1	0
1	2	1	2	1	2	1	2
0	1	0	1	0	1	0	1
2	1	2	1	2	1	2	1
1	0	1	0	1	0	1	0
1	2	1	2	1	2	1	2

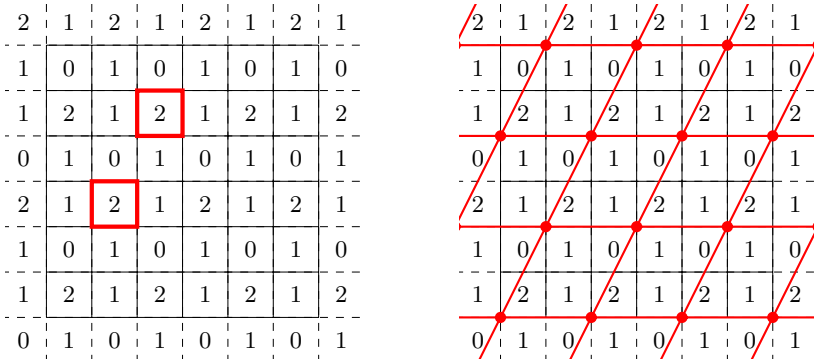
(b) A new picture $\sigma_h^{-1} \circ \sigma_v^{-1}(P)$

Fig. 1: Illustration of the shift function over a picture.

Definition 3 (equivalent pixels). *We say that two pixels* $p_1 = (x_1, y_1)$ *and* $p_2 = (x_2, y_2)$ *of a picture* P *are* equivalent *if the transformation that translates* p_1 *onto* p_2 *leaves the picture unchanged,* i.e. *if* $\sigma_h^{x_2-x_1} \circ \sigma_v^{y_2-y_1}(P) = P$. *In that case, we note* $p_1 \sim p_2$.

We note that this definition actually corresponds to an equivalence relation. It is easy to see that the following lemma holds for equivalence classes of pixels:

Lemma 1. *For any bi-periodic picture* P, *there exists a finite number of equivalence classes of pixels of that picture. Moreover, each of these equivalence classes contains an infinite number of pixels. Finally, the equivalence class of pixel* $(0, 0)$ *constitutes an* integer lattice of dimension 2, i.e. *a sub-group of* $(\mathbb{Z}^2, +)$ *(see Figure 2b).*



(a) Two equivalent pixels. (b) The equivalent pixels lattice.

Fig. 2: Similar pixels and their induced lattice.

Definition 4 (rectangular patterns). *Let* P *be a picture over* Σ, *we call* rectangular pattern *of size* $m \times n$ *extracted at* (x_0, y_0) *the following function :*

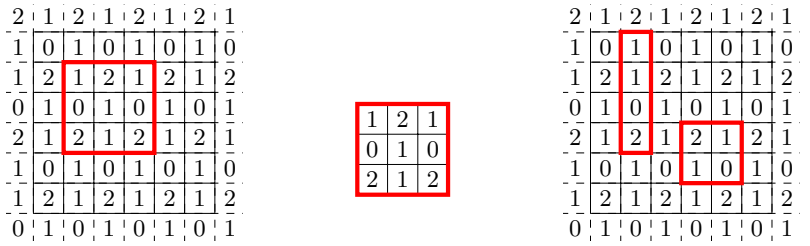
$$R_{x_0,y_0} : [\![0, m-1]\!] \times [\![0, n-1]\!] \to \Sigma$$
$$(x, y) \mapsto P(x + x_0, y + y_0)$$

Definition 5 (primitive root). *We say that a rectangular pattern* R_{x_0,y_0} *of size* $m \times n$ *is a* primitive root *of the picture* P *if it contains exactly one representative of each equivalence class of pixels of the picture,* i.e.
$\forall (x, y) \in \mathbb{Z}^2,\ \exists! (x', y') \in [\![0, m-1]\!] \times [\![0, n-1]\!]$ *such that* $(x, y) \sim (x_0 + x', y_0 + y')$.

Figure 3 gives an example of primitive roots of a picture.

The following lemma holds directly from the previous definition :

Lemma 2. *All primitive roots of a given picture have the same area, which is the number of equivalence classes of that picture.*



(a) The original picture P

(b) The rectangular pattern of size 3×3 extracted at $(1, 2)$

(c) Primitive roots of picture P

Fig. 3: Rectangular patterns in a bi-periodic picture.

Let us notice that these definitions can be adapted to pictures of dimension 1, *i.e.* words over Σ. It can be easily seen that primitive roots exactly are primitive words in that context.

We also notice that our definition of primitive root is non-constructive. Our first non-trivial result is that these primitive roots indeed exist.

Theorem 1 (existence of primitive roots). *Let P be a bi-periodic picture, then primitive roots can be extracted from P.*

Proof (Theorem 1). This proof will use *Hermite normal form* of square matrices, which are a well studied tool of linear algebra. Simply put, an integer matrix H is said to be in Hermite normal form if

- it is lower triangular
- its diagonal entries are positive
- in every column, the entries below the diagonal are non-negative and smaller than the ones on the diagonal.

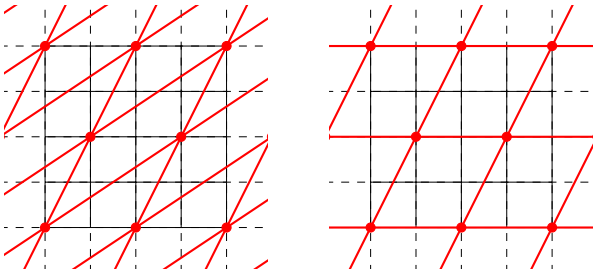
For any integer matrix M, it is known that there exists a unique integer matrix H in Hermite normal form such that $H = U \times M$, where U is unimodular with integer coefficients. We will also use notions related to *integer lattices*, such as the fundamental domain of a lattice. More references about Hermite normal form and lattices can be found in [3].

Let us consider the integer lattice $\mathcal{L}$ formed by the equivalence class of pixel $(0, 0)$ (See Lemma 1). Let us call $\mathcal{B}$ a basis of that lattice (see Figure 4a), and let $\mathcal{B}'$ be the family of vectors whose matrix is the Hermite normal form of the matrix associated with $\mathcal{B}$ (see [3]). Without loss of generality we can assume that $\mathcal{B}' = \begin{pmatrix} \alpha & 0 \\ \beta & \gamma \end{pmatrix}$.
Because of the properties of Hermite transformation (*i.e.* the matrix U is unimodular), it is clear that $\{(\alpha, 0), (\beta, \gamma)\}$ is also a basis of $\mathcal{L}$ (see Figure 4b).

Let $\mathcal{F}$ be the fundamental domain of $\mathcal{L}$ associated with basis $\mathcal{B}'$ (see [3]). More precisely, let us consider the pixels within $\mathcal{F}$. Clearly, because $\mathcal{B}'$ is a basis of $\mathcal{L}$, there must be exactly one representative of each equivalence class among them (see Figure 4c).

Let also $\mathcal{R}$ be the rectangular pattern of size $\alpha \times \gamma$ extracted from P at position $(0,0)$ (see Figure 4c). It appears that $\mathcal{R}$ contains exactly the same equivalence classes as $\mathcal{F}$, because each pixel of $\mathcal{R}$ is either a pixel of $\mathcal{F}$ or the translation by a vector $(-\alpha, 0)$ of a pixel of $\mathcal{F}$ (that translation preserves equivalence classes, since $(\alpha, 0)$ is a vector of $\mathcal{B}'$).

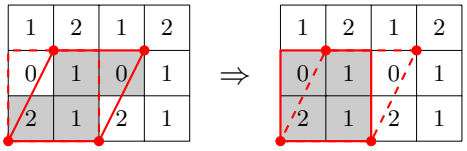
We therefore know that $\mathcal{R}$ contains exactly one representative of each equivalence class of P, which makes it a primitive root. □



$\mathcal{B} = \begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix}$ $\mathcal{B}' = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}$

(a) The original lattice $\mathcal{L}$ with an unspecified base

(b) The same lattice with an Hermite normal form base



(c) Transforming the fundamental domain $\mathcal{F}$ of $\mathcal{B}'$ into a rectangular pattern $\mathcal{R}$

Fig. 4: Illustration of primitive root construction.

We note that the construction of such primitive roots is non-trivial in the general case: The naive algorithm that takes an arbitrary rectangular pattern that contains at least (resp. at most) one representative of each equivalence class and shrinks it (resp. expands it) until it contains exactly one representative does not work. Figure 5 gives counter-examples, in the form of rectangular patterns that contain at least (resp. at most) one representative of each class, and cannot be shrunk (resp. expanded).

3 Main result

Now that we have proved that there exist primitive roots in any bi-periodic picture, we will describe them exactly. In order to achieve this, we will need the following lemma:

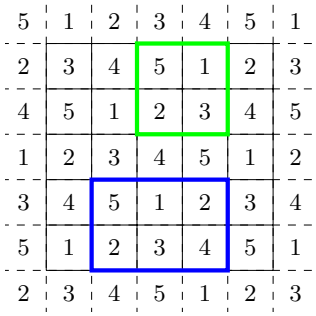


Fig. 5: Counter-examples to the naive algorithm.

Lemma 3. *Let $\mathcal{R}$ be a primitive root of a bi-periodic picture P, then $\mathcal{R}$ tiles P by translation.*

This lemma is illustrated by Figure 6, and can be easily proved by noticing that a translation of $\mathcal{R}$ can be constructed around each pixel of P (because $\mathcal{R}$ contains at least one representative of each equivalence class), and that these translations cannot overlap (those representatives must be unique in $\mathcal{R}$). This tiling can also be obtained by copying $\mathcal{R}$ on each point of the lattice $\mathcal{L}$ defined previously.

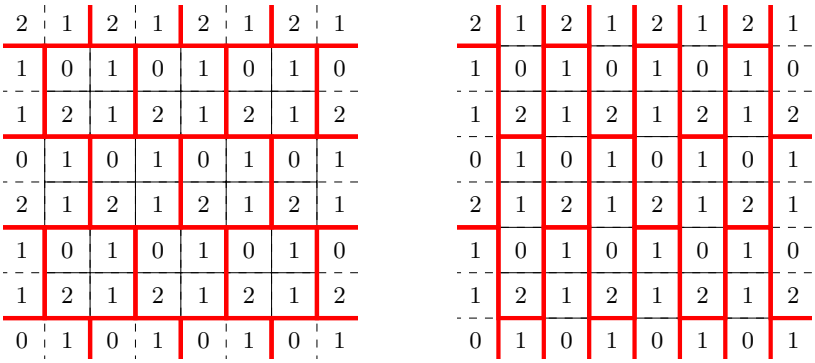


Fig. 6: Tilings of a bi-periodic picture by its primitive roots.

We can now introduce our second theorem, which gives us a more precise characterization of the primitive roots of a picture.

Theorem 2. *let P be a bi-periodic picture, and let $S \subset \mathbb{N}^2$ be the set of all possible sizes for primitive roots of P (more precisely, $S = \{(m,n);\ \exists R_{x,y}$ a primitive root of P of size $m \times n\}$), then:*

- $\|S\| \leq 2$ *(there are at most two different sizes for primitive roots).*

– $\forall (m,n) \in S;\ \forall (x,y) \in \mathbb{Z}^2$ *if* $R_{x,y}$ *is the rectangular pattern of size* $m \times n$ *extracted from* P *at* (x,y)*, then* $R_{x,y}$ *is a primitive root of* P *(that is, primitive roots can be extracted from anywhere provided that they are of appropriate size).*

Proof (Theorem 2). We will prove the first point of Theorem 2 by associating a matrix in Hermite normal form to each primitive root of picture P, and by considering what it implies.

Let R_{x_0,y_0} be a primitive root of P of size $m \times n$. Thanks to Lemma 3, we know that there exists a tiling of P by R. We consider two particular vectors of that tiling, which are illustrated on Figure 7 and defined thereafter:

– Let $V_1 = (m, -y_1)$ where y_1 is the smallest positive integer such that $(x_0, y_0) \sim (x_0 + m, y_0 - y_1)$.
– Let $V_2 = (x_2, n)$ where x_2 is the smallest positive integer such that $(x_0, y_0) \sim (x_0 + x_2, y_0 + n)$.

Because R tiles the picture, it is clear that we have $0 \leq y_1 < n$ and $0 \leq x_2 < m$. We will now prove that we have either $y_1 = 0$ or $x_2 = 0$.

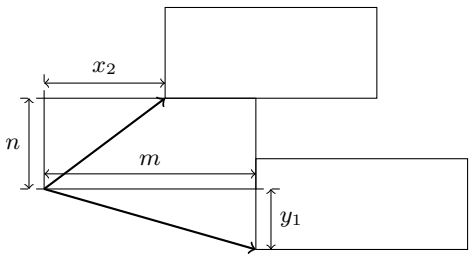


Fig. 7: The particular tiling vectors associated to a given primitive root.

Indeed, if we have $y_1 \neq 0$ and $x_2 \neq 0$, that would mean there exists a rectangular "hole" of size $x_2 \times y_1$ in the tiling (see Figure 8). Because we have $x_2 < m$ and $y_1 < n$, that means it is impossible to fit a translation of R into that hole, therefore a contradiction with the fact that R tiles the picture. We now have either $V_1 = (m, 0)$ or $V_2 = (0, n)$.

It is important to note that, as they are non-colinear, V_1 and V_2 constitute a basis of the lattice $\mathcal{L}$ associated with P. Up to a re-ordering of the dimensions, we can suppose without loss of generality that $V_1 = (m, 0)$ and $V_2 = (x_2, n)$. Let us consider the matrix $\mathcal{B} = \begin{pmatrix} m & 0 \\ x_2 & n \end{pmatrix}$.

It is the matrix of a basis of $\mathcal{L}$, and it happens to be in Hermite normal form (because $0 \leq x_2 < m$). It means that every (m, n) eligible to be the size of a primitive root must be the couple of diagonal coefficients of the matrix of a basis of $\mathcal{L}$ in Hermite normal form (up to a reordering of the dimensions). We know that such a matrix is unique (see [3]), and that there exist 2 reorderings of 2 dimensions ($2! = 2$). Therefore, it means that the couple (m, n) can only have at most two different values, giving us the first point of the theorem.

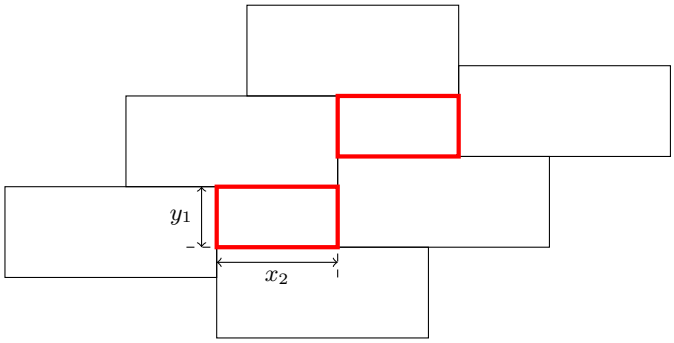


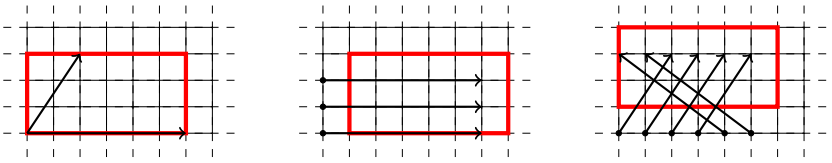
Fig. 8: An illustration of what the tiling would look like if $y_1 \neq 0$ and $x_2 \neq 0$.

Now to prove the second point, we will only prove that if R_{x_0,y_0} is a primitive root of size $m \times n$, then the rectangular patterns R'_{x_0+1,y_0} and R''_{x_0,y_0+1} of same size also are. The second point would then automatically follow by induction.

Let therefore R_{x_0,y_0} be a primitive root of P of size $m \times n$. Let also V_1 and V_2 be the particular vectors defined earlier. We assume without loss of generality that $V_1 = (m, 0)$ and $V_2 = (x_2, n)$.

Figure 9 shows that both R'_{x_0+1,y_0} and R''_{x_0,y_0+1} contain the same equivalence classes as R_{x_0,y_0}. Indeed, in both cases there exists a bijection between the equivalence classes of the original pattern and those of the new one; this bijection is a translation by particular vectors which conserve the equivalence classes of a pixel.

In the case of R'_{x_0+1,y_0}, the vectors are either V_1 or $(0, 0)$ (see Figure 9b). In the case of R''_{x_0,y_0+1}, the vectors are V_2, $V_2 - V_1$ or $(0, 0)$ (see Figure 9c). As R'_{x_0+1,y_0} and R''_{x_0,y_0+1} contain the same equivalence classes as R_{x_0,y_0} and also are rectangular patterns, it means that they also are primitive roots of P. □



(a) The original primitive root and its translation vectors V_1 and V_2.

(b) The new pattern R'_{x_0+1,y_0}

(c) The new pattern R''_{x_0,y_0+1}

Fig. 9: Translation of a primitive root preserves its equivalence classes. Here we have $V_1 = (6, 0)$ and $V_2 = (2, 3)$.

Note that the upper bound stated in Theorem 2 is tight, as there are pictures for which the primitive roots can have 2 different sizes (in fact, most of them). An example is given on Figure 3c.

The second point of Theorem 2 can give us all the primitive roots of a given picture. An example of its application is given on Figure 10.

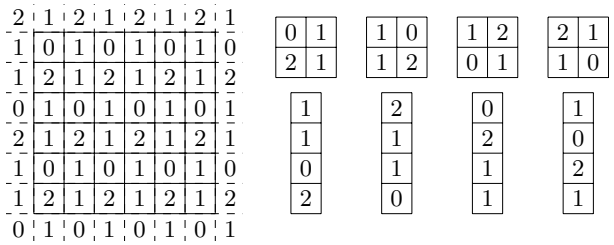


Fig. 10: Here are given all the primitive roots of the example picture.

4 Discussion about the root extracting function

In this section, we will study some interesting properties of the function $\mathcal{F}$ that maps a bi-periodic picture to the set of its primitive roots, or equivalently (as Theorem 2 states) the set of sizes of its primitive roots.

More formally, we can say that $\mathcal{F} : \Sigma^{\mathbb{Z}^2} \to (\mathbb{N}^2)^2$. Note that $\mathcal{F}(P)$ is only defined if its argument P is a *periodic* picture.

4.1 Computability of function $\mathcal{F}$

The first and perhaps most interesting result is that function $\mathcal{F}$ is indeed computable, even if its argument is an infinite object (more precisely, an infinite object with finite support, but whose size is unknown). A few computational models can reasonably process an input whose size is infinite, but the computability of this function has been proved with the model of Cellular Automata, which is one of those models (See *e.g.* [4] or [6] for general matters on Cellular Automata).

This computability result will not be extensively discussed here, as it would easily double the size of this article and has already been proved in [2]. However, note that this result could also adapt to classical computational models with finite input, such as Turing Machines. In that case it becomes quasi trivial, because the only relevant way to describe the input picture would be to give one of its periods (not necessarily the shortest one). If the period is known, then a straightforward application of the construction given in the proof of Theorem 1 would immediately give the primitive roots of the picture.

4.2 Injectivity in the general case

It is immediate to see that two bi-periodic pictures which are shifts of each other have exactly the same set of primitive roots, so the injectivity of function $\mathcal{F}$ is clearly disproved. However, it would be interesting to see what happens if the pictures are defined up to a shift, which is a reasonable assumption.

It appears that the function $\mathcal{F}$ is not injective either in that case. Indeed, Figure 11 proves it by giving two different bi-periodic pictures that have exactly the same set of primitive roots. We can infer that the mere knowledge of its primitive roots is not sufficient to deduce a whole bi-periodic picture; one would also need the tiling vectors of a given root.

An attentive reader may have noticed that both pictures shown on Figure 11 are rotations of each other, and that the set of their primitive roots is invariant by rotation. This reader could ask if the injectivity of function $\mathcal{F}$ is true if the pictures are defined up to a rotation. Unfortunately, it is not the case, as there exist more complex counterexamples which are not equivalent by rotation.

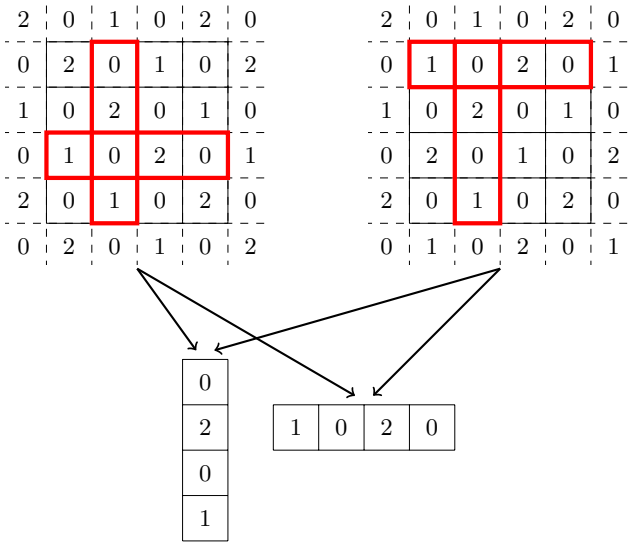


Fig. 11: Illustration of the non-injectivity of the root extracting function: both pictures have the same set of primitive roots (all the primitive roots are shifts of the ones presented on the figure).

4.3 Bijectivity in the case of a double root

Now let us consider what happens when there is only one possible size for the primitive root. This case happens when the Hermite normal form of the matrix associated with P is diagonal instead of simply triangular. An example of that case is shown on Figure 12.

If R_{x_0,y_0} is a double root of the picture P of size $m \times n$, it means that the translation vectors associated with R_{x_0,y_0} are horizontal and vetical ($V_1 = (m, 0)$ and $V_2 = (0, n)$). In that case, the original picture can be rebuilt P by merely translating R_{x_0,y_0} along V_1 and V_2. This means that $\mathcal{F}$ is bijective if there is a double root, provided the picture is defined up to a translation.

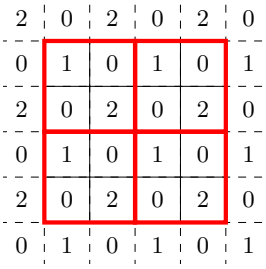


Fig. 12: When there is only one possible size for the primitive roots of a picture, the inverse function exists and is trivial.

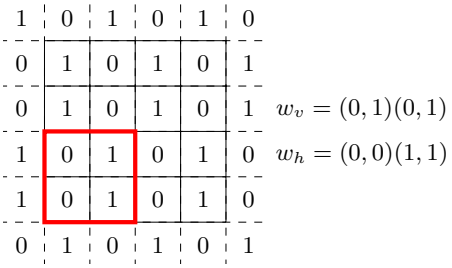


Fig. 13: A primitive root can be seen as a one-dimensional vertical word w_v over the alphabet of horizontal tuples of Σ, or as a horizontal word w_h over the alphabet of vertical tuples of Σ.

4.4 Properties of the primitive roots

It can be interesting to study the relation between the primitive roots we defined in this article with *primitive words* of dimension 1 (see *e.g.* [7]). In particular, if P is a picture over an alphabet Σ and R_{x_0,y_0} is a root of P of size $m \times n$, R can be seen as a horizontal word over the alphabet Σ^n, or as a vertical word over the alphabet Σ^m (as shown on Figure 13). It appears that at least one of these words is primitive in their particular alphabet (the proof is quite simple, and uses once again the fact that either V_1 or V_2 have a null component).

Conversely, one could ask if any rectangular pattern that is either "horizontally primitive" or "vertically primitive" can be the primitive root of a certain bi-periodic picture. It seems to be the case, but we were not able to find a formal proof of that property.

5 Conclusion and perspectives

Although the definition of a primitive root is non-constructive, this article succeeds in exhibiting all of them for every bi-periodic picture, and shows some of their properties. Now let us review the remaining points that could lead to future works.

5.1 Open problems

As stated earlier, we still don't know if every two-dimensional word that fits our naive precondition (*i.e.* being either horizontally primitive or vertically primitive) can be the primitive root of a picture. Deciding that property could lead to a characterization of the 2-dimensional language of potential primitive roots. Even if we don't know much about that language, we still have some lower bounds about its recognizability (it obviously is as hard to recognize as the language of primitive words, which is its restriction to dimension 1).

5.2 Primitive roots in higher dimensions

An immediate extension of our work would be to extend it to pictures of dimension higher than 2. All the definitions scale nicely, up to the definition of a multi-dimensional primitive root, as a hyper-parallelogram containing exactly one representative of each equivalence class of pixels. The existence of such primitive roots also holds, due to the same argument used in the proof of Theorem 1, only using the Hermite normal form of matrices of higher dimensions.

However, Theorem 2 seems harder to prove; it would state that *for a multi-periodic picture of dimension d, there are at most $d!$ possible sizes for its primitive roots*. We know how to construct pictures that have at least $d!$ different sizes of primitive roots ($d!$ is the number of linear orders of the d dimensions). In order to prove that this bound is a maximum, we miss a statement that would be equivalent to "at least one of the translating vectors have a null component" in higher dimensions. Note that this problem is a purely geometric one; it only relates to the tiling of the space by translations of a hyper-parallelogram, and does not relate to formal languages. The subject of properties of primitive roots of higher dimensions is also left unexplored.

References

1. Nicolas Bacquey. Complexity classes on spatially periodic cellular automata. In Ernst W. Mayr and Natacha Portier, editors, *31st International Symposium on Theoretical Aspects of Computer Science*, volume 25 of *LIPIcs*, pages 112–124, 2014.
2. Nicolas Bacquey. Leader election on two-dimensional periodic cellular automata. *currently submitted*, 2015.
3. Henri Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag Berlin Heidelberg, 1993.
4. Marianne Delorme and Jacques Mazoyer. *Cellular Automata: a parallel model*, volume 460. Springer Science & Business Media, 1998.
5. Pál Dömösi, S Horváth, and M Ito. Formal languages and primitive words. *Publ. Math. Debrecen*, 42(3–4):315–321, 1993.
6. Jarkko Kari. Theory of cellular automata: A survey. *Theoretical Computer Science*, 334(1-3):3–33, 2005.
7. H Petersen. On the language of primitive words. *Theoretical Computer Science*, 161(1):141–156, 1996.