Nivat's conjecture and pattern complexity in algebraic subshifts

Jarkko Kari, Etienne Moutot

Nivat's Conjecture and pattern complexity in algebraic subshifts[*]

Jarkko Kari[1] and Etienne Moutot[1,2]

[1]Department of Mathematics and Statistics, University of Turku
[2]LIP, ENS de Lyon – CNRS – UCBL – Université de Lyon

Abstract

We study Nivat's conjecture on algebraic subshifts and prove that in some of them every low complexity configuration is periodic. This is the case in the Ledrappier subshift (the 3-dot system) and, more generally, in all two-dimensional algebraic subshifts over $\mathbb{F}_p$ defined by a polynomial without line polynomial factors in more than one direction. We also find an algebraic subshift that is defined by a product of two line polynomials that has this property (the 4-dot system) and another one that does not.

1 Introduction and preliminaries

The European Association for Theoretical Computer Science, EATCS, celebrated its 25th anniversary at ICALP 1997 in Bologna. The keynote address was given by Maurice Nivat. His talk – titled "Towards a History of Automata: Why Were They Introduced? What Are They Good for?" – suggested the following intriguing problem that has become known as Nivat's conjecture: If an infinite two-dimensional grid has been colored in such a way that, for some $n, m \in \mathbb{N}$, the number of distinct $n \times m$ patterns is at most nm, is the coloring necessarily periodic in some direction? The conjecture has attracted wide interest, but it has turned out to be difficult and remains still unsolved today.

A number of partial results and related observations have been made. Periodicity has been established if the number of $n \times m$ patterns is at most αnm for progressively larger and larger constants $\alpha < 1$: First for $\alpha = 1/144$ in [5], then for $\alpha = 1/16$ in [11], and finally for the best known constant $\alpha = 1/2$ in [3]. It is also known that having at most $2n$ patterns of size $2 \times n$ and having at most $3n$ patterns of size $3 \times n$ imply periodicity [12, 4]. In [7] we introduced an algebraic approach that leads to the following asymptotic result: A non-periodic coloring of the grid can only have finitely many pairs (n, m) such that the number of distinct $n \times m$ patterns is at most nm. Of course Nivat's conjecture claims that there are no such pairs.

In this paper we continue with our algebraic approach and prove that Nivat's conjecture holds on colorings that come from certain algebraically defined sets, including the Ledrappier subshift [9]. In fact we prove a stronger statement that in

---

these sets periodicity is implied if for any shape – not necessarily a rectangle – the number of patterns of that shape is at most the size of the shape. Even more: if a coloring has any non-trivial annihilator over $\mathbb{Z}$ (terms explained below) then it is periodic.

To make the statement precise we recall some terminology. For a finite alphabet A, colorings $c \in A^{\mathbb{Z}^2}$ of the two-dimensional grid by elements of A are called (two-dimensional) *configurations*. Typically we use notation $c_{\mathbf{n}}$ for the color $c(\mathbf{n}) \in A$ of cell $\mathbf{n} \in \mathbb{Z}^2$. Basic operations on $A^{\mathbb{Z}^2}$ are *translations*: for any $\mathbf{t} \in \mathbb{Z}^2$ the translation $\tau_{\mathbf{t}} : A^{\mathbb{Z}^2} \longrightarrow A^{\mathbb{Z}^2}$ by $\mathbf{t}$ is defined by $\tau_{\mathbf{t}}(c)_{\mathbf{n}} = c_{\mathbf{n}-\mathbf{t}}$, for all $c \in A^{\mathbb{Z}^2}$ and all $\mathbf{n} \in \mathbb{Z}^2$. We call a configuration c *periodic* if $\tau_{\mathbf{t}}(c) = c$ for some non-zero $\mathbf{t} \in \mathbb{Z}^2$, and we call $\mathbf{t}$ a *vector of periodicity*. If there are two linearly independent vectors of periodicity then c is *two-periodic*. In this case it is easy to see that there are horizontal and vertical vectors of periodicity $(k, 0)$ and $(0, k)$ for some $k \neq 0$, and consequently a vector of periodicity in every rational direction. We call c *one-periodic* if it is periodic but not two-periodic.

Colorings $p \in A^D$ of a finite shape $D \subset \mathbb{Z}^d$ are called D-*patterns*, or simply patterns. The set of D-patterns that appear in a configuration c is denoted by $P(c, D)$, that is,

$$P(c, D) = \{\tau_{\mathbf{t}}(c)_{|D} \mid \mathbf{t} \in \mathbb{Z}^2 \ \}.$$

We say that c has *low complexity* with respect to shape D if $|P(c, D)| \leq |D|$, and we call c a *low complexity configuration* if it has low complexity with respect to some finite D. Otherwise c is a *high complexity configuration*. Low complexity configurations come up naturally in practical setups, e.g. in crystallography particles may attach to each other only in very limited ways. Moreover, there are interesting mathematical problems associated to them, including the famous Nivat's conjecture discussed above:

Conjecture (Maurice Nivat 1997)**.** *Let $c \in A^{\mathbb{Z}^2}$ be a two-dimensional configuration. If c has low complexity with respect to some rectangle $D = \{1, \ldots, n\} \times \{1, \ldots, m\}$ then c is periodic.*

The analogous claim in dimensions higher than two fails, as does an analogous claim in two dimensions for many other shapes than rectangles [1].

To study the conjecture algebraically we replace the colors by integers, or elements of some other integral domain R, and express the configuration c as a formal power series $c(X, Y)$ over two variables X and Y in which the coefficient of monomial $X^i Y^j$ is $c_{i,j}$, for all $i, j \in \mathbb{Z}$. Note that the exponents of the variables range from $-\infty$ to $+\infty$. In the following also polynomials may have negative powers of variables so all polynomials considered are actually Laurent polynomials. Let us denote by $R[X^{\pm 1}, Y^{\pm 1}]$ and $R[[X^{\pm 1}, Y^{\pm 1}]]$ the sets of such polynomials and power series, respectively, with coefficients in domain R. We call a power series $c \in R[[X^{\pm 1}, Y^{\pm 1}]]$ *finitary* if its coefficients take only finitely many different values. Since we color the grid using finitely many colors, configurations are identified with finitary power series.

Multiplying configuration $c \in R[[X^{\pm 1}, Y^{\pm 1}]]$ by a monomial corresponds to translating it, and the periodicity of the configuration by vector $\mathbf{t} = (n, m)$ is then equivalent to $(X^n Y^m - 1)c = 0$, the zero power series. More generally, we say that polynomial $f \in R[X^{\pm 1}, Y^{\pm 1}]$ *annihilates* power series c if the formal product fc is the zero power series. The set of polynomials that annihilates a power series is a polynomial ideal, and is denoted by

$$\mathrm{Ann}_R(c) = \{f \in R[X^{\pm 1}, Y^{\pm 1}] \mid fc = 0\}.$$

We observed in [7] that, in the case $R = \mathbb{Z}$, if a configuration has low complexity with respect to some shape then it is annihilated by some non-zero polynomial $f \neq 0$. The proof works unchanged for an arbitrary field R.

Lemma 1 ([7]). *Let R be a field or $R = \mathbb{Z}$. Let $c \in R[[X^{\pm 1}, Y^{\pm 1}]]$ be a low complexity configuration. Then $Ann_R(c)$ contains a non-zero polynomial.*

One of the main results of [7] states that, in the case $R = \mathbb{Z}$, if a configuration c is annihilated by a non-zero polynomial then it has annihilators of particularly nice form:

Theorem 2 ([7]). *Let $c \in \mathbb{Z}[[X^{\pm 1}, Y^{\pm 1}]]$ be a configuration (a finitary power series) annihilated by some non-zero polynomial.*
Then there exists non-zero $(i_1, j_1), \ldots, (i_m, j_m) \in \mathbb{Z}^2$ such that

$$(X^{i_1} Y^{j_1} - 1) \cdots (X^{i_m} Y^{j_m} - 1) \in Ann_{\mathbb{Z}}(c).$$

Unlike Lemma 1 this theorem does not generalize to all cases when R is a field.

For a polynomial $f = \sum a_{i,j} X^i Y^j$, we call $\mathrm{supp}(f) = \{(i,j) \mid a_{i,j} \neq 0\}$ its *support*. A *line polynomial* is a polynomial with its terms aligned all on the same line: f is a line polynomial in direction $\mathbf{u} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$ if and only if $\mathrm{supp}(f)$ contains at least two elements and for some $\mathbf{n} \in \mathbb{Z}^2$ we have $\mathrm{supp}(f) \subseteq \{\mathbf{n} + r\mathbf{u} \mid r \in \mathbb{Q}\}$. Note that the annihilator provided by Theorem 2 is a product of line polynomials. A central feature of line polynomials is that any configuration that is annihilated by a line polynomial is periodic in the direction of the line polynomial [7].

If R is a finite field and if $f \in R[X^{\pm 1}, Y^{\pm 1}]$ is a non-zero polynomial then we define the set

$$X_f = \{c \in R[[X^{\pm 1}, Y^{\pm 1}]] \mid fc = 0\}$$

of all configurations that f annihilates and call it the *algebraic subshift* defined by f. It is a subshift of finite type (SFT, see [10] for the symbolic dynamics terminology). We have that $c \in X_f \iff f \in \mathrm{Ann}_R(c) \iff fc = 0$.

By Lemma 1 all low complexity configurations belong to algebraic subshifts when the symbols are renamed as elements of a finite field. It is thus enough to consider Nivat's conjecture on elements of algebraic subshifts: if the conjecture is false then there is a counter example configuration that belongs to an algebraic subshift. This is the approach taken in this work. We consider various algebraic subshifts and see whether low complexity implies periodicity in these subshifts. When this is the case we say that the subshift has the *generalized Nivat property*. We prove that an algebraic subshift X_f has the generalized Nivat property if the defining polynomial f does not have line polynomial factors in two different directions.

The paper is organized as follows. In Section 2 we consider as a particular example the well known Ledrappier subshift, also known as the 3-dot system, and prove that any low complexity configuration in the Ledrappier subshift is periodic. In Section 3 we generalize this result to all algebraic subshifts where the defining polynomial does not have line polynomial factors in more than one direction. This includes, for example, the space-time diagrams of all additive cellular automata over finite fields. In Section 4 we consider the 4-dot system defined by polynomial $(1 + X)(1 + Y)$ over $\mathbb{F}_2$ and prove that it also has the generalized Nivat property although the defining polynomial has horizontal and vertical line polynomial factors, while the analogous system defined by $(1 + X^2)(1 + Y^2)$ does not have the property.

3

2 The Ledrappier Subshift

The Ledrappier subshift, or the 3-dot system, consists of the configurations over the binary alphabet $\mathbb{F}_2$ that are annihilated by the polynomial $1 + X + Y \in \mathbb{F}_2[X^{\pm 1}, Y^{\pm 1}]$.

Definition 1 ([9])**.** *The* Ledrappier subshift L *is the algebraic subshift X_{f_L} over $\mathbb{F}_2$ defined by the annihilator $f_L = 1 + X + Y$.*

In this work we relate the generalized Nivat property to the number of line polynomial factors of the defining annihilator. It turns out that f_L has none.

A visual way of seeing if a polynomial has a line polynomial factor is to look at the shape of the convex hull of its support: the convex hull has parallel sides in the directions of its line polynomial factors. To be more precise, we need some definitions of discrete geometry. The closed half plane in a direction $\mathbf{v} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$ is the set $\overline{H}_{\mathbf{v}} = \{\mathbf{x} \in \mathbb{Z}^2 \mid \mathbf{x} \cdot \mathbf{v} \geq 0\}$, and the open half plane $H_{\mathbf{v}}$ is defined analogously to contain those $\mathbf{x} \in \mathbb{Z}^2$ that satisfy $\mathbf{x} \cdot \mathbf{v} > 0$. The boundary of the half plane is $\overline{H}_{\mathbf{v}} \setminus H_{\mathbf{v}}$. We say that a finite set $D \subseteq \mathbb{Z}^2$ has an *outer edge* perpendicular to $\mathbf{v} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$ if there is $\mathbf{x} \in D$ such that $D \subseteq \mathbf{x} + \overline{H}_{\mathbf{v}}$ and there are at least two elements of D on the boundary $\mathbf{x} + (\overline{H}_{\mathbf{v}} \setminus H_{\mathbf{v}})$. See Fig. 1 for an illustration.
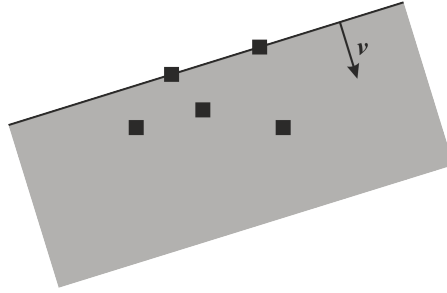

Figure 1: The set of black cells has an outer edge perpendicular to vector $\mathbf{v}$.

Lemma 3. *Let g, h be non-zero polynomials such that $supp(g)$ has an outer edge perpendicular to $\mathbf{v}$. Then also $supp(gh)$ has an outer edge perpendicular to $\mathbf{v}$.*

Proof. Let vector $\mathbf{u} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$ be perpendicular to $\mathbf{v}$. By the hypotheses of the lemma there are $\mathbf{x} \in \mathbb{Z}^2$ and a line polynomial α in the direction $\mathbf{u}$ such that $supp(g) \subseteq \mathbf{x} + \overline{H}_{\mathbf{v}}$ and $supp(g - \alpha) \subseteq \mathbf{x} + H_{\mathbf{v}}$. Here α contains the terms of g along the boundary of the half plane $\mathbf{x} + H_{\mathbf{v}}$. Analogously, for any non-zero polynomial h there exists $\mathbf{y} \in \mathbb{Z}^2$ and polynomial $\beta \neq 0$ that is either a monomial or a line polynomial in the direction $\mathbf{u}$ such that $supp(h) \subseteq \mathbf{y} + \overline{H}_{\mathbf{v}}$ and $supp(h - \beta) \subseteq \mathbf{y} + H_{\mathbf{v}}$. But then $supp(gh) \subseteq \mathbf{x} + \mathbf{y} + \overline{H}_{\mathbf{v}}$ and $supp(gh - \alpha\beta) \subseteq \mathbf{x} + \mathbf{y} + H_{\mathbf{v}}$. Because $\alpha\beta$ is a line polynomial in the direction $\mathbf{u}$, this proves that the support of gh has an outer edge perpendicular to $\mathbf{v}$. $\square$

Corollary 4. *If $f \neq 0$ has a line polynomial factor in the direction $\mathbf{u}$ then $supp(f)$ has outer edges perpendicular to $\mathbf{v}$ and $-\mathbf{v}$, where $\mathbf{v}$ is a vector perpendicular to $\mathbf{u}$.*

Proof. A line polynomial g in the direction $\mathbf{u}$ has outer edges perpendicular to $\mathbf{v}$ and $-\mathbf{v}$. The claim then follows directly from Lemma 3. $\square$

Because the convex hull of $\mathrm{supp}(f_L)$ is a triangle, it does not have parallel outer edges and therefore no line polynomial factors.

Corollary 5. *Polynomial $f_L = 1 + X + Y$ has no line polynomial factors.*

Remark. In fact, it is very easy to see that f_L is an irreducible polynomial, which directly implies Corollary 5.

Now we can prove that the Ledrappier subshift has the generalized Nivat property.

Theorem 6. *Any low complexity $c \in X_{f_L}$ is periodic.*

Proof. In this proof we are going to need annihilators of c over $\mathbb{F}_2$ and over $\mathbb{Z}$. We interpret c as a configuration over $\mathbb{Z}$ using the renaming $\mathbb{F}_2 \longrightarrow \mathbb{Z}$ that maps $0_{\mathbb{F}_2} \mapsto 0_{\mathbb{Z}}$ and $1_{\mathbb{F}_2} \mapsto 1_{\mathbb{Z}}$. We write $\mathrm{Ann}_{\mathbb{Z}}(c)$ for the annihilator ideal of the configuration over $\mathbb{Z}$ obtained after this renaming. We are going to prove the following stronger statement: if $\mathrm{Ann}_{\mathbb{Z}}(c)$ contains a non-zero polynomial then c is periodic. The result then follows from Lemma 1.

Let $c \in L$ be non-periodic. We first prove that $\mathrm{Ann}_{\mathbb{F}_2}(c)$ is the principal ideal generated by f_L, that is, for every $g \in \mathrm{Ann}_{\mathbb{F}_2}(c)$ there exists $\alpha \in \mathbb{F}_2[X^{\pm 1}, Y^{\pm 1}]$ such that $g = \alpha f_L$. First, let $g \in \mathrm{Ann}_{\mathbb{F}_2}(c)$ be a proper polynomial which means that all exponents of variables are non-negative. Because $X = 1 + Y + f_L$ we can eliminate variable X: there exists a polynomial $\alpha(X, Y)$ and a polynomial $\beta(Y)$ in variable Y only such that $g = \alpha(X, Y)f_L + \beta(Y)$. Because both f_L and g are annihilators of c, $\beta(Y) \in \mathrm{Ann}_{\mathbb{F}_2}(c)$ as well.

If $\beta \neq 0$ then it is either a single monomial (in which case $c = 0$) or a line polynomial annihilator of c. Any configuration with a line polynomial annihilator is periodic in the direction of the polynomial. We conclude that $\beta = 0$ so that $g = \alpha f_L$, as claimed.

Consider then arbitrary $g \in \mathrm{Ann}_{\mathbb{F}_2}(c)$ with possibly some negative exponents. Because $g = X^i Y^j g'$ for some $i, j \in \mathbb{Z}$ and a proper polynomial $g' \in \mathrm{Ann}_{\mathbb{F}_2}(c)$, we conclude that also in this case g is a multiple of f_L, and therefore we have that $\mathrm{Ann}_{\mathbb{F}_2}(c)$ is the principal ideal generated by f_L.

Now it remains to show that $\mathrm{Ann}_{\mathbb{Z}}(c)$, the set of annihilators over $\mathbb{Z}$, is trivial. Suppose by contrary that there is a non-zero annihilator in $\mathrm{Ann}_{\mathbb{Z}}(c)$. By Theorem 2 there exists non-zero $(i_1, j_1), \ldots, (i_m, j_m) \in \mathbb{Z}^2$ such that $(X^{i_1}Y^{j_1} - 1) \cdots (X^{i_m}Y^{j_m} - 1) \in \mathrm{Ann}_{\mathbb{Z}}(c)$. By performing computations modulo two instead, we have that $(X^{i_1}Y^{j_1} - 1) \cdots (X^{i_m}Y^{j_m} - 1) \in \mathrm{Ann}_{\mathbb{F}_2}(c)$. But then this polynomial, which only has line polynomial factors, is a multiple of f_L. All factors of line polynomials are line polynomials in the same direction (or monomials) so that all irreducible factors of f_L are line polynomials, contradicting Corollary 5. Here we used the fact that every polynomial can be factored uniquely into its irreducible factors [2]. $\qquad\square$

3   Annihilators with Few Line Polynomial Factors

One of the key element in the proof of Theorem 6 is the fact that we can find an annihilator with one variable eliminated from it. It turns out that this is something we can do with other annihilators than f_L, and to do so we will use some parts of *elimination theory*, so-called resultants. Everything needed to understand this paper will be introduced but for more, Cox's book [2] is a good introduction.

3.1 Resultant

Usually resultant are defined for proper polynomials, so in order to stick with usual definitions we define them likewise. We will still use them for talking about Laurent polynomials, which is not a problem since from a Laurent polynomial annihilator we can always obtain a proper one by multiplying it by a suitable monomial.

Let R be a field, e.g. $R = \mathbb{F}_p$ for a prime p, and let $K = R[Y]$ be the ring of polynomials with one variable Y. Then $K[X] = R[X, Y]$ is the ring of polynomials with two variables over R. Resultant can be defined for polynomials with more than two variables, but two is all we need here. Resultant can be defined formally as a determinant of some matrix with coefficients in K, but for our purpose, all we need to know is that for any $f, g \in R[X, Y]$, there exists a polynomial $\mathrm{Res}_X(f, g) \in R[Y]$ in variable Y only with the following two properties:

Property 1. *The polynomials f and g have a common factor in $R[X, Y]$ if and only if $Res_X(f, g) = 0$.*

Property 2. *There exist $\alpha, \beta \in R[X, Y]$ such that*

$$\alpha f + \beta g = Res_X(f, g).$$

The second property exactly states that we can find a linear combination of f and g that eliminates variable X.

Lemma 7. *Let c be a power series over a field R. If c is annihilated by two non-zero polynomials f and g with no common factors then c is two-periodic.*

Proof. Using Property 2, let $\alpha, \beta \in R[X, Y]$ be such that

$$\alpha f + \beta g = \mathrm{Res}_X(f, g).$$

Because f and g are both annihilators of c so is $\mathrm{Res}_X(f, g)$. Because f and g have no common factors, Property 1 tells us that $\mathrm{Res}_X(f, g) \neq 0$. We found an annihilator which is a line polynomial or a monomial (only with variable Y) so c must be periodic along Y.

Symmetrically, there also exist $\gamma, \delta \in R[X, Y]$ such that

$$\gamma f + \delta g = \mathrm{Res}_Y(f, g).$$

Again, $\mathrm{Res}_Y(f, g) \neq 0$, so c is also periodic along X. □

Remark. In [8] we analyzed the structure of annihilator ideals of configurations over $\mathbb{Z}$, and an analogous result for the case of $\mathbb{Z}$ follow from those considerations. We included here the simple proof above for the sake of completeness, and in order to cover also the case of arbitrary coefficient fields.

3.2 Main Result

Now we can easily generalize Theorem 6. We consider an algebraic subshift X_f over a finite field $\mathbb{F}_p$ defined by an annihilator $f \in \mathbb{F}_p[X^{\pm 1}, Y^{\pm 1}]$. A configuration $c \in \mathbb{F}_p[[X^{\pm 1}, Y^{\pm 1}]]$ will also be interpreted as a configuration over $\mathbb{Z}$ by mapping the symbols by $a_{\mathbb{F}_p} \mapsto a_{\mathbb{Z}}$ for all $a \in \{0, 1, \ldots, p-1\}$. Then, as in the proof of Theorem 6, we can define both $\mathrm{Ann}_{\mathbb{F}_p}(c)$ and $\mathrm{Ann}_{\mathbb{Z}}(c)$, and use the fact that any $g \in \mathrm{Ann}_{\mathbb{Z}}(c)$ is also in $\mathrm{Ann}_{\mathbb{F}_p}(c)$ when its coefficients are reduced modulo p.

Theorem 8. *Let $c \in X_f$ for a polynomial $f \in \mathbb{F}_p[X^{\pm 1}, Y^{\pm 1}]$, and suppose that $Ann_{\mathbb{Z}}(c)$ contains a non-zero polynomial.*

- *If f has no line polynomial factors then c is two-periodic.*

- *If all line polynomial factors of f are in the same direction then c is periodic in this direction.*

Proof. By Theorem 2 there exists non-zero $(i_1, j_1), \ldots, (i_m, j_m) \in \mathbb{Z}^2$ such that $(X^{i_1}Y^{j_1} - 1) \cdots (X^{i_m}Y^{j_m} - 1) \in \text{Ann}_{\mathbb{Z}}(c)$. By performing computations modulo p instead, we have that $g(X, Y) = (X^{i_1}Y^{j_1} - 1) \cdots (X^{i_m}Y^{j_m} - 1) \in \text{Ann}_{\mathbb{F}_p}(c)$.

If f has no line polynomial factors then f and g do not have any common factors. By Lemma 7 then c is two-periodic. This proves the first claim.

Suppose then that all line polynomial factors of f are in the same direction. Let h be the greatest common divisor of f and g so that we can write $f = f'h$ and $g = g'h$ where f' and g' do not have common factors. Note that h is a line polynomial: as a factor of g h is a product of line polynomials, and as a factor of f these line polynomials are all in the same direction.

Because $c' = hc$ is annihilated by both f' and g' it follows from Lemma 7 that c' is two-periodic. In particular, there is a line polynomial h' in the direction of h that annihilates c'. We have $hh' \in \text{Ann}_{\mathbb{F}_p}(c)$ so that c is annihilated by the line polynomial hh' and is therefore periodic in this direction. $\qquad \square$

Using Lemma 1 we now immediately get that algebraic subshifts defined by an annihilator with at most one line polynomial factor have the generalized Nivat property.

Corollary 9. *Let $c \in X_f$ for a polynomial $f \in \mathbb{F}_p[X^{\pm 1}, Y^{\pm 1}]$ whose line polynomial factors are all in the same direction. If c has low complexity then it is periodic.*

Remark. Elements of the Ledrappier subshift are exactly the space-time diagrams of the one-dimensional XOR cellular automaton. More generally, the algebraic subshift X_f defined by a polynomial of the form $f(X, Y) = Y - g(X) \in \mathbb{F}_p[X^{\pm 1}, Y^{\pm 1}]$ consists exactly of the space-time diagrams of the one-dimensional additive cellular automaton over $\mathbb{F}_p$ whose local rule is given by $g(X)$. See Section 9 of [6] for a short discussion about additive cellular automata. If $g(X)$ has at least two terms then the support of f has triangular shape and therefore f has no line polynomial factors. If $g(X)$ has one term then f itself is a line polynomial. In any case, Theorem 8 and Corollary 9 hold for the space-time diagrams of all one-dimensional additive cellular automata over field $\mathbb{F}_p$.

4 Square Annihilators

After Corollary 9, it is natural to take a look at configurations annihilated by polynomials with line polynomial factors in more directions. It turns out that already products of two line polynomials include examples with and without the generalized Nivat property. We first prove that the 4-dot system defined by $(1 + X)(1 + Y)$ over $\mathbb{F}_2$ has the generalized Nivat property and then we show that the system defined by $(1 + X^2)(1 + Y^2)$ does not.

4.1 The 4-dot system

Definition 2. *The* 4*-dot system* S *is the algebraic subshift* X_{f_S} *over* $\mathbb{F}_2$ *defined by the annihilator* $f_S = 1 + X + Y + XY = (1 + X)(1 + Y)$.

Theorem 10. *Every low complexity* $c \in X_{f_S}$ *is periodic.*

Proof. Similarly as before, we are going to prove the more general statement that if c has a non-trivial annihilator p_0 over $\mathbb{Z}$ then it is periodic.

We first observe that $c = h + v$ for $h, v \in \mathbb{F}_2[[X^{\pm 1}, Y^{\pm 1}]]$ that are $(1, 0)$-periodic and $(0, 1)$-periodic, respectively. Indeed, we can take $h_{i,j} = c_{0,j}$ and $v_{i,j} = c_{i,0} + c_{0,0}$, for all $i, j \in \mathbb{Z}$. Because $(1 + X^i)(1 + Y^j)$ is a multiple of $(1 + X)(1 + Y)$ over $\mathbb{F}_2$, polynomial $(1 + X^i)(1 + Y^j)$ annihilates c, for all $i, j \in \mathbb{Z}$. This means that $c_{i,j} = c_{0,j} + c_{i,0} + c_{0,0} = h_{i,j} + v_{i,j}$.

Using the periodicity of h and v we can write $h = \mathbb{1}(X)s(Y)$ and $v = t(X)\mathbb{1}(Y)$, with $\mathbb{1}(X) = \sum_{i \in \mathbb{Z}} X^i$ and s, t two formal series depending only one one variable. Let us define another binary configuration d by

$$d(X, Y) = t(X)s(Y).$$

In other words, d is the configuration that has ones where both h and v have ones:

$$d_{i,j} = \begin{cases} 1 \text{ if } h_{i,j} = v_{i,j} = 1 \\ 0 \text{ otherwise} \end{cases}.$$

Interpreted in $\mathbb{Z}$, we have

$$c = h + v - 2d.$$

This is the case since the two sides are identical modulo two and both sides only contain values 0 and 1.

Consider next the polynomial

$$p = p_0(X - 1)(Y - 1)$$

over $\mathbb{F}_2$. Because p_0 annihilates c, and $X - 1$ and $Y - 1$ annihilate h and v, respectively, we have that $pc = ph = pv = 0$. Therefore $pd = 0$ as well, which can be written as

$$p(X, Y)t(X)s(Y) = 0,$$

emphasizing the variable dependencies of the polynomials. We have the following two cases:

Case 1: Suppose that $p(X, Y)t(X) = 0$. In $p(X, Y)$ we collect together terms with the same power of variable Y, obtaining

$$p(X, Y) = \sum_{j \in \mathbb{Z}} Y^j p_j(X)$$

where at least some $p_j(X)$ is a non-zero polynomial. We have

$$\sum_{j \in \mathbb{Z}} Y^j p_j(X)t(X) = 0.$$

This is an identity of formal power series so that $p_j(X)t(X) = 0$ for all $j \in \mathbb{Z}$. But then also $p_j(X)v = p_j(X)t(X)u(Y) = 0$, so that v is annihilated by a non-zero

horizontal line polynomial (or a non-zero monomial) $p_j(X)$. We conclude that v is horizontally periodic. But then also $c = h + v$ is horizontally periodic as a sum of two horizontally periodic configurations.

Case 2: Suppose that $p(X,Y)t(X) \neq 0$. Now we collect in $p(X,Y)t(X)$ together variables with the same power of variable X, obtaining

$$p(X,Y)t(X) = \sum_{i \in \mathbb{Z}} X^i q_i(Y),$$

where at least some $q_i(Y)$ is a non-zero polynomial. Note that all $q_i(Y)$ are polynomials because powers of the variable Y only come from the polynomial $p(X,Y)$. Because

$$0 = p(X,Y)d(X,Y) = p(X,Y)t(X)s(Y) = \sum_{i \in \mathbb{Z}} X^i q_i(Y)s(Y),$$

we have that $q_i(Y)s(Y) = 0$ for all $i \in \mathbb{Z}$. Analogously to case 1 above, this implies that h is vertically periodic, and therefore also c is vertically periodic. $\quad\square$

4.2 An algebraic subshift without the generalized Nivat property

For some polynomials with two line polynomial factors, the associated subshift does not have the generalized Nivat property. This is typically the case when the annihilating polynomial allows the use of sublattices.

Theorem 11. *There exists a configuration c over $\mathbb{F}_2$ annihilated by $f_T = (1 + X^2)(1 + Y^2)$ which is not periodic but has low complexity.*

Proof. Let us take $c = h + v$, with

$$h_{i,j} = \begin{cases} 1 \text{ if } j = 0 \text{ and } i \text{ even} \\ 0 \text{ otherwise} \end{cases} \quad \text{and} \quad v_{i,j} = \begin{cases} 1 \text{ if } i = 1 \text{ and } j \text{ even} \\ 0 \text{ otherwise} \end{cases}.$$

Visually, c is the superposition of a horizontal and a vertical line on two disjoint sublattices, see Fig. 2. Clearly h is one-periodic with periodicity vector $(2,0)$ and v is one-periodic with periodicity vector $(0,2)$. Their sum c is not periodic.

The periodicity of h and v directly implies that f_T annihilates c: h being $(2,0)$-periodic $(1 + X^2)h = 0$ and, analogously, v being $(0,2)$-periodic $(1 + Y^2)v = 0$. This means that $f_T c = (1 + X^2)(1 + Y^2)h + (1 + X^2)(1 + Y^2)v = 0$.

The last thing we have to check is that c has low complexity, i.e, there is a shape D such that $P_c(D) \leq |D|$. It is sufficient to take D to be the scattered 3x3 square, as shown in Fig. 3. Patterns of shape D in c will only contain values from one of the four sublattices, depending on the parity of its position. If D is superimposed with sublattices 3 or 4, the pattern is blank. With sublattice 1, it can only contain values from h, so it can have four different values: blank, and the horizontal line crossing at the top, the middle or the bottom. If it is on sublattice 2, then it has values from v, and here again there are four different possibilities. Counting the blank shape only once, we obtain $P_c(D) = 1 + 3 + 3 = 7 < 9 = |D|$.

$\quad\square$

Figure 2: Sublattices of c and shape D superimposed. The horizontal line is from h and the vertical one from v.
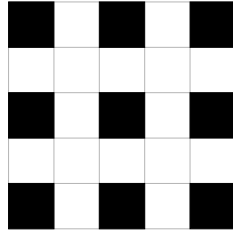

Figure 3: The shape D of low complexity.

5 Conclusions

To prove Nivat's conjecture it is enough to consider configurations of two-dimensional algebraic subshifts over $\mathbb{F}_p$. We prove that simplest subshifts do not contain a counter example to the conjecture, and they even have the stronger property that any configuration that has low complexity with respect to any finite shape is periodic. It remains open to characterize which algebraic subshifts have this generalized Nivat property. It remains also an interesting algorithmic problem to decide for a set of at most $|D|$ allowed patterns of shape D, for some finite $D \subseteq \mathbb{Z}^2$, whether there is a configuration all of whose D-patterns are among the allowed patterns. We do not know if this emptyness problem of low complexity subshifts of finite type is decidable in general, but if the given patterns come from one of the algebraic subshifts studied in this work then the emptyness problem is decidable by a standard argument because any configuration with these patterns must be periodic. We also ask whether the generalized Nivat property may fail for other reasons than having the support of the defining polynomial in a proper sublattice of $\mathbb{Z}^2$.

References

[1] J. Cassaigne. Subword complexity and periodicity in two or more dimensions. In G. Rozenberg and W. Thomas, editors, *Developments in Language Theory*, pages 14–21. World Scientific, 1999.

[2] D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 4th edition, 2015.

[3] V. Cyr and B. Kra. Nonexpansive $\mathbb{Z}^2$-subdynamics and Nivat's conjecture. *Trans. Amer. Math. Soc.*, 367(9):6487–6537, 2015.

[4] V. Cyr and B. Kra. Complexity of short rectangles and periodicity. *European Journal of Combinatorics*, 52:146 – 173, 2016.

[5] C. Epifanio, M. Koskas, and F. Mignosi. On a conjecture on bidimensional words. *Theor. Comput. Sci.*, 1-3(299), 2003.

[6] J. Kari. Theory of cellular automata: A survey. *Theoretical Computer Science*, 334(1):3 – 33, 2005.

[7] J. Kari and M. Szabados. An Algebraic Geometric Approach to Nivat's Conjecture. In *Automata, Languages, and Programming - 42nd International Colloquium, ICALP 2015, Kyoto, Japan, July 6-10, 2015, Proceedings, Part II*, pages 273–285, 2015.

[8] J. Kari and M. Szabados. An Algebraic Geometric Approach to Nivat's Conjecture. preprint arXiv:1605.05929, May 2016.

[9] F. Ledrappier. Un champ markovien peut être d'entropie nulle et mélangeant. *C. R. Acad. Sci. Paris Sér. A-B*, 287(7):A561–A563, 1978.

[10] D. Lind and B. Marcus. *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press, 1995.

[11] A. Quas and L. Q. Zamboni. Periodicity and local complexity. *Theor. Comput. Sci.*, 319(1-3):229–240, 2004.

[12] J. W. Sander and R. Tijdeman. The rectangle complexity of functions on two-dimensional lattices. *Theor. Comput. Sci.*, 270(1-2):857–863, 2002.