An Algebraic Geometric Approach to Nivat's Conjecture

Jarkko Kari and Michal Szabados

Department of Mathematics and Statistics,
University of Turku, 20014 Turku, Finland

Abstract. We study multidimensional configurations (infinite words) and subshifts of low pattern complexity using tools of algebraic geometry. We express the configuration as a multivariate formal power series over integers and investigate the setup when there is a non-trivial annihilating polynomial: a non-zero polynomial whose formal product with the power series is zero. Such annihilator exists, for example, if the number of distinct patterns of some finite shape D in the configuration is at most the size $|D|$ of the shape. This is our low pattern complexity assumption. We prove that the configuration must be a sum of periodic configurations over integers, possibly with unbounded values. As a specific application of the method we obtain an asymptotic version of the well-known Nivat's conjecture: we prove that any two-dimensional, non-periodic configuration can satisfy the low pattern complexity assumption with respect to only finitely many distinct rectangular shapes D.

1 Introduction

Consider configuration $c \in A^{\mathbb{Z}^d}$, a d-dimensional infinite array filled by symbols from finite alphabet A. Suppose that for some finite observation window $D \subseteq \mathbb{Z}^d$, the number of distinct patterns of shape D that exist in c is small, at most the cardinality $|D|$ of D. We investigate global regularities and structures in c that are enforced by such local complexity assumption.

Let us be more precise on the involved concepts. As usual, we denote by $c_{\boldsymbol{v}} \in A$ the symbol in c in position $\boldsymbol{v} \in \mathbb{Z}^d$. For $\boldsymbol{u} \in \mathbb{Z}^d$, we say that c is $\boldsymbol{u}$-*periodic* if $c_{\boldsymbol{v}} = c_{\boldsymbol{v}+\boldsymbol{u}}$ holds for all $\boldsymbol{v} \in \mathbb{Z}^d$, and c is *periodic* if it is $\boldsymbol{u}$-periodic for some $\boldsymbol{u} \neq 0$. For a finite domain $D \subseteq \mathbb{Z}^d$, the elements of A^D are D-*patterns*. For a fixed D, we denote by $c_{\boldsymbol{v}+D}$ the D-pattern in c in position $\boldsymbol{v}$, that is, the pattern $\boldsymbol{u} \mapsto c_{\boldsymbol{v}+\boldsymbol{u}}$ for all $\boldsymbol{u} \in D$. The number of distinct D-patterns in c is the D-*pattern complexity* $P_c(D)$ of c. Our assumption of low local complexity is

$$P_c(D) \leq |D|, \tag{1}$$

for some finite D.

Nivat's conjecture

There are specific examples in the literature of open problems in this framework. *Nivat's conjecture* (proposed by M. Nivat in his keynote address in ICALP

1997 [Niv97]) claims that in the two-dimensional case $d = 2$, the low complexity assumption (1) for a rectangle D implies that c is periodic. The conjecture is a natural generalization of the one-dimensional Morse-Hedlund theorem that states that if a bi-infinite word contains at most n distinct subwords of length n then the word must be periodic [MH38]. In the two-dimensional setting for $m, n \in \mathbb{N}$ we denote by $P_c(m, n)$ the complexity $P_c(D)$ for the $m \times n$ rectangle D.

Conjecture 1 (Nivat's conjecture). If for some m, n we have $P_c(m, n) \leq mn$ then c is periodic.

The conjecture has recently raised wide interest, but it remains unsolved. In [EKM03] it was shown $P_c(m, n) \leq mn/144$ is enough to guarantee the periodicity of c. This bound was improved to $P_c(m, n) \leq mn/16$ in [QZ04], and recently to $P_c(m, n) \leq mn/2$ in [CK13b]. Also the cases of narrow rectangles have been investigated: it was shown in [ST02] and recently in [CK13a] that $P_c(2, n) \leq 2n$ and $P_c(3, n) \leq 3n$, respectively, imply that c is periodic.

The analogous conjecture in the higher dimensional setups $d \geq 3$ is false [ST00]. The following example recalls a simple counter example for $d = 3$.

Example 1. Fix $n \geq 3$, and consider the following $c \in \{0, 1\}^{\mathbb{Z}^3}$ consisting of two perpendicular lines of 1's on a 0-background, at distance n from each other: $c(i, 0, 0) = c(0, i, n) = 1$ for all $i \in \mathbb{Z}$, and $c(i, j, k) = 0$ otherwise. For D equal to the $n \times n \times n$ cube we have $P_c(D) = 2n^2 + 1$ since the D-patterns in c have at most a single 1-line piercing a face of the cube. Clearly c is not periodic although $P_c(D) = 2n^2 + 1 < n^3 = |D|$. Notice that c is a "sum" of two periodic components (the lines of 1's). Our results imply that any counter example must decompose into a sum of periodic components.　　　□

Periodic tiling problem

Another related open problem is the *periodic (cluster) tiling problem* by Lagarias and Wang [LW96]. A (cluster) tile is a finite $D \subset \mathbb{Z}^d$. Its co-tiler is any subset $C \subseteq \mathbb{Z}^d$ such that

$$D \oplus C = \mathbb{Z}^d. \tag{2}$$

The co-tiler can be interpreted as the set of positions where copies of D are placed so that they together cover the entire $\mathbb{Z}^d$ without overlaps. Note that the tile D does not need to be connected – hence the term "cluster tile" is sometimes used. The tiling is by translations of D only: the tiles may not be rotated.

It is natural to interpret any $C \subseteq \mathbb{Z}^d$ as the binary configuration $c \in \{0, 1\}^{\mathbb{Z}^d}$ with $c_{\boldsymbol{v}} = 1$ if and only if $\boldsymbol{v} \in C$. Then the tiling condition (2) states that C is a co-tiler for D if and only if the $(-D)$-patterns in the corresponding configuration c contain exactly a single 1 in the background of 0's. In fact, as co-tilers of D and $-D$ coincide [Sze98], this is equivalent to all D-patterns having a single 1.

We see that the set $\mathcal{C}$ of all co-tiler configurations for D is a *subshift of finite type* [LM95]. We also see that the low local complexity assumption (1) is

satisfied. We even have $P_\mathcal{C}(D) \le |D|$ where we denote by $P_\mathcal{C}(D)$ the number of distinct D-patterns found in the elements of the subshift $\mathcal{C}$.

Conjecture 2 (Periodic Tiling Problem). If tile D has a co-tiler then it has a periodic co-tiler.

This conjecture was first formulated in [LW96]. In the one-dimensional case it is easily seen true, but already for $d = 2$ it is open. Interestingly, it is known that if $|D|$ is a prime number then *every* co-tiler of D is periodic [Sze98] (see also our Example 2). The same is true if D is connected, that is, a polyomino [BN91].

Our contributions

We approach these problems using tools of algebraic geometry. Assuming alphabet $A \subseteq \mathbb{Z}$, we express configuration c as a formal power series over d variables and with coefficients in A. The complexity assumption (1) implies that there is a non-trivial polynomial that annihilates the power series under formal multiplication (Lemma 1). This naturally leads to the study of the annihilator ideal of the power series, containing all the polynomials that annihilate it. Using Hilbert's Nullstellensatz we prove that the ideal contains polynomials of particularly simple form (Theorem 1). In particular, this implies that $c = c_1 + \cdots + c_m$ for some periodic $c_1, \ldots, c_m$ (Theorem 2). This decomposition result is already an interesting global structure on c, but to prove periodicity we would need $m = 1$.

We study the structure of the annihilator ideal in the two-dimensional setup, and prove that it is always a radical (Lemma 5). This leads to a stronger decomposition theorem (Theorem 3). In the case of Nivat's conjecture we then provide an asymptotic result (Theorem 4): for any non-periodic configuration c there are only finitely many pairs $m, n \in \mathbb{N}$ such that $P_c(m, n) \le mn$.

Due to the strict page limit the proofs in the latter part of the paper are omitted.

2 Basic Concepts and Notation

For a domain R – which will usually be the whole numbers $\mathbb{Z}$ or complex numbers $\mathbb{C}$ – denote by $R[x_1, \ldots, x_d]$ the set of polynomials over R in d variables. We adopt the usual simplified notation: for a d-tuple of non-negative integers $\boldsymbol{v} = (v_1, \ldots, v_d)$ set $X^{\boldsymbol{v}} = x_1^{v_1} \ldots x_d^{v_d}$, then we write

$$R[X] = R[x_1, \ldots, x_d]$$

and a general polynomial $f \in R[X]$ can be expressed as $f = \sum a_{\boldsymbol{v}} X^{\boldsymbol{v}}$, where $a_{\boldsymbol{v}} \in R$ and the sum goes over finitely many d-tuples of non-negative integers $\boldsymbol{v}$. If we allow $\boldsymbol{v}$ to contain also negative integers we obtain *Laurent polynomials*, which are denoted by $R[X^{\pm 1}]$. Finally, by relaxing the requirement to have only finitely many $a_{\boldsymbol{v}} \ne 0$ we get *formal power series*:

$$R[[X^{\pm 1}]] = \Big\{ \sum a_{\boldsymbol{v}} X^{\boldsymbol{v}} \ \Big| \ \boldsymbol{v} \in \mathbb{Z}^d, \ a_{\boldsymbol{v}} \in R \Big\}.$$

Note that we allow negative exponents in formal power series.

Let d be a positive integer. Let us define a d-dimensional *configuration* to be any formal power series $c \in \mathbb{C}[[X^{\pm 1}]]$:

$$c = \sum_{\boldsymbol{v} \in \mathbb{Z}^d} c_{\boldsymbol{v}} X^{\boldsymbol{v}}.$$

A configuration is *integral* if all coefficients $c_{\boldsymbol{v}}$ are integers, and it is *finitary* if there are only finitely many distinct coefficients $c_{\boldsymbol{v}}$. In the case the coefficients are not given explicitly we denote the coefficient at position $\boldsymbol{v}$ by a subscript.

Classically in symbolic dynamics configurations are understood as elements of $A^{\mathbb{Z}^d}$. Because the actual names of the symbols in the alphabet A do not matter, they can be chosen to be integers. Then such a "classical" configuration can be identified with a finitary integral configuration by simply setting the coefficient $c_{\boldsymbol{v}}$ to be the symbol at position $\boldsymbol{v}$.

The first advantage of using formal power series is that a multiplication by a Laurent polynomial is well defined and results again in formal power series. For example, $X^{\boldsymbol{v}} c$ is a translation of c by the vector $\boldsymbol{v}$. Another important example is that c is periodic if and only if there is a non-zero $\boldsymbol{v} \in \mathbb{Z}^d$ such that $(X^{\boldsymbol{v}} - 1)c = 0$. Here the right side is understood as a constant zero configuration.

For a polynomial $f(X) = \sum a_{\boldsymbol{v}} X^{\boldsymbol{v}}$ and a positive integer n define $f(X^n) = \sum a_{\boldsymbol{v}} X^{n\boldsymbol{v}}$. The following example, and the proof of Lemma 2, use the well known fact that for any integral polynomial f and prime number p, we have $f^p(X) \equiv f(X^p) \pmod{p}$.

Example 2. Our first example concerns the periodic tiling problem. We provide a short proof of the fact – originally proved in [Sze98] – that if the size $p = |D|$ of tile D is a prime number then all co-tilers C are periodic. When the tile D is represented as the Laurent polynomial $f(X) = \sum_{\boldsymbol{v} \in D} X^{\boldsymbol{v}}$ and the co-tiler C as the power series $c(X) = \sum_{\boldsymbol{v} \in C} X^{\boldsymbol{v}}$, the tiling condition (2) states that $f(X)c(X) = \sum_{\boldsymbol{v} \in \mathbb{Z}^d} X^{\boldsymbol{v}}$. Multiplying both sides by $f^{p-1}(X)$, we get

$$f^p(X)c(X) = \sum_{\boldsymbol{v} \in \mathbb{Z}^d} p^{p-1} X^{\boldsymbol{v}} \equiv 0 \pmod{p}.$$

On the other hand, since p is a prime, $f^p(X) \equiv f(X^p) \pmod{p}$ so that

$$f(X^p)c(X) \equiv 0 \pmod{p}.$$

Let $\boldsymbol{v} \in D$ and $\boldsymbol{w} \in C$ be arbitrary. We have

$$0 \equiv [f(X^p)c(X)]_{\boldsymbol{w}+p\boldsymbol{v}} = \sum_{\boldsymbol{u} \in D} c(X)_{\boldsymbol{w}+p\boldsymbol{v}-p\boldsymbol{u}} \pmod{p}.$$

The last sum is a sum of p numbers, each 0 or 1, among which there is at least one 1 (corresponding to $\boldsymbol{u} = \boldsymbol{v}$). The only way for the sum to be divisible by p is by having each summand equal to 1. We have that $\boldsymbol{w} + p(\boldsymbol{v} - \boldsymbol{u})$ is in C for all $\boldsymbol{u}, \boldsymbol{v} \in D$ and $\boldsymbol{w} \in C$, which means that C is $p(\boldsymbol{v} - \boldsymbol{u})$-periodic for all $\boldsymbol{u}, \boldsymbol{v} \in D$. $\square$

The next lemma grants us that for low complexity configurations there exists at least one Laurent polynomial that annihilates the configuration by formal multiplication.

Lemma 1. *Let c be a configuration and $D \subset \mathbb{Z}^d$ a finite domain such that $P_c(D) \leq |D|$. Then there exists a non-zero Laurent polynomial $f \in \mathbb{C}[X^{\pm 1}]$ such that $fc = 0$.*

Proof. Denote $D = \{\boldsymbol{u_1}, \ldots, \boldsymbol{u_n}\}$ and consider the set

$$\{ (1, c_{\boldsymbol{u_1}+\boldsymbol{v}}, \ldots, c_{\boldsymbol{u_n}+\boldsymbol{v}}) \mid \boldsymbol{v} \in \mathbb{Z}^d \}.$$

It is a set of complex vectors of dimension $n+1$, and because c has low complexity there is at most $n = |D|$ of them. Therefore there exists a common orthogonal vector $(a_0, \ldots, a_n)$. Let $g(X) = a_1 X^{-\boldsymbol{u_1}} + \cdots + a_n X^{-\boldsymbol{u_n}}$, then the coefficient of gc at position $\boldsymbol{v}$ is

$$(gc)_{\boldsymbol{v}} = a_1 c_{\boldsymbol{u_1}+\boldsymbol{v}} + \cdots + a_n c_{\boldsymbol{u_n}+\boldsymbol{v}} = -a_0,$$

that is, gc is a constant configuration. Now it suffices to set $f = (X^{\boldsymbol{v}} - 1)g$ for arbitrary non-zero vector $\boldsymbol{v} \in \mathbb{Z}^d$. $\square$

3 Annihilating Polynomials and Decomposition Theorem

Lemma 1 motivates the following definitions. Let c be a configuration. We say that a Laurent polynomial f *annihilates* (or is an *annihilator* of) the configuration if $fc = 0$. Define

$$\mathrm{Ann}(c) = \{ f \in \mathbb{C}[X] \mid fc = 0 \}.$$

It is the set of all annihilators of c. Clearly it is an ideal of $\mathbb{C}[X]$. The zero polynomial annihilates every configuration; let us call an annihilator *non-trivial* if it is non-zero. Note that the configuration is periodic if and only if $X^{\boldsymbol{v}} - 1 \in \mathrm{Ann}(c)$ for some non-zero $\boldsymbol{v} \in \mathbb{Z}^d$.

We defined $\mathrm{Ann}(c)$ to consist of complex polynomials, so that we can later use Hilbert's Nullstellensatz directly, as it requires polynomial ideals over algebraically closed field. We shall however occasionally work with integer coefficients and Laurent polynomials when it is more convenient.

Recall that in the case of Nivat's conjecture and Periodic tiling problem we study finitary integral configurations, which by Lemma 1 have a non-trivial annihilator. Moreover there is an integer annihilating polynomial – actually for integral configurations $\mathrm{Ann}(c)$ is always generated by integer polynomials.

If $Z = (z_1, \ldots, z_d) \in \mathbb{C}^d$ is a complex vector then it can be plugged into a polynomial. In particular, plugging into a monomial $X^{\boldsymbol{v}}$ results in $Z^{\boldsymbol{v}} = z_1^{v_1} \cdots z_d^{v_d}$.

Lemma 2. *Let $c(X)$ be a finitary integral configuration and $f(X) \in \mathrm{Ann}(c)$ a non-zero integer polynomial. Then there exists an integer r such that for every positive integer n relatively prime to r we have $f(X^n) \in \mathrm{Ann}(c)$.*

Proof. Denote $f(X) = \sum a_{\boldsymbol{v}} X^{\boldsymbol{v}}$. First we prove the claim for the case when n is a large enough prime.

Let p be a prime, then we have $f^p(X) \equiv f(X^p) \pmod{p}$. Because f annihilates c, multiplying both sides by $c(X)$ results in

$$0 \equiv f(X^p)c(X) \pmod{p}.$$

The coefficients in $f(X^p)c(X)$ are bounded in absolute value by

$$s = c_{max} \sum |a_{\boldsymbol{v}}|,$$

where c_{max} is the maximum absolute value of coefficients in c. Therefore if $p > s$ we have $f(X^p)c(X) = 0$.

For the general case, set $r = s!$. Now every n relatively prime to r is of the form $p_1 \cdots p_k$ where each p_i is a prime greater than s. Note that we can repeat the argument with the same bound s also for polynomials $f(X^m)$ for arbitrary m – the bound s depends only on c and the (multi)set of coefficients $a_{\boldsymbol{v}}$, which is the same for all $f(X^m)$. Thus we have $f(X^{p_1 \cdots p_k}) \in \mathrm{Ann}(c)$. $\qquad\square$

Lemma 3. *Let c be a finitary integral configuration and $f = \sum a_{\boldsymbol{v}} X^{\boldsymbol{v}}$ a nontrivial integer polynomial annihilator. Let $S = \{ \boldsymbol{v} \in \mathbb{Z}^d \mid a_{\boldsymbol{v}} \neq 0 \}$ and define*

$$g(X) = x_1 \cdots x_d \prod_{\substack{\boldsymbol{v} \in S \\ \boldsymbol{v} \neq \boldsymbol{v_0}}} (X^{r\boldsymbol{v}} - X^{r\boldsymbol{v_0}})$$

where r is the integer from Lemma 2 and $\boldsymbol{v_0} \in S$ arbitrary. Then $g(Z) = 0$ for any common root $Z \in \mathbb{C}^d$ of $\mathrm{Ann}(c)$.

Proof. Fix Z. If any of its complex coordinates is zero then clearly $g(Z) = 0$. Assume therefore that all coordinates of Z are non-zero.

Let us define for $\alpha \in \mathbb{C}$

$$S_\alpha = \{ \boldsymbol{v} \in S \mid Z^{r\boldsymbol{v}} = \alpha \},$$
$$f_\alpha(X) = \sum_{\boldsymbol{v} \in S_\alpha} a_{\boldsymbol{v}} X^{\boldsymbol{v}}.$$

Because S is finite, there are only finitely many non-empty sets $S_{\alpha_1}, \ldots, S_{\alpha_m}$ and they form a partitioning of S. In particular we have $f = f_{\alpha_1} + \cdots + f_{\alpha_m}$.

Numbers of the form $1 + ir$ are relatively prime to r for all non-negative integers i, therefore by Lemma 2, $f(X^{1+ir}) \in \mathrm{Ann}(c)$. Plugging in Z we obtain $f(Z^{1+ir}) = 0$. Now compute:

$$f_\alpha(Z^{1+ir}) = \sum_{\boldsymbol{v} \in S_\alpha} a_{\boldsymbol{v}} Z^{(1+ir)\boldsymbol{v}} = \sum_{\boldsymbol{v} \in S_\alpha} a_{\boldsymbol{v}} Z^{\boldsymbol{v}} \alpha^i = f_\alpha(Z) \alpha^i$$

Summing over $\alpha = \alpha_1, \ldots, \alpha_m$ gives

$$0 = f(Z^{1+ir}) = f_{\alpha_1}(Z) \alpha_1^i + \cdots + f_{\alpha_m}(Z) \alpha_m^i.$$

Let us rewrite the last equation as a statement about orthogonality of two vectors in $\mathbb{C}^m$:

$$(f_{\alpha_1}(Z), \ldots, f_{\alpha_m}(Z)) \perp (\alpha_1^i, \ldots, \alpha_m^i)$$

By Vandermode determinant, for $i \in \{0, \ldots, m-1\}$ the vectors on the right side span the whole $\mathbb{C}^m$. Therefore the left side must be the zero vector, and especially for α such that $\boldsymbol{v_0} \in S_\alpha$ we have

$$0 = f_\alpha(Z) = \sum_{\boldsymbol{v} \in S_\alpha} a_{\boldsymbol{v}} Z^{\boldsymbol{v}}.$$

Because Z does not have zero coordinates, each term on the right hand side is non-zero. But the sum is zero, therefore there are at least two vectors $\boldsymbol{v_0}, \boldsymbol{v} \in S_\alpha$. From the definition of S_α we have $Z^{r\boldsymbol{v}} = Z^{r\boldsymbol{v_0}} = \alpha$, so Z is a root of $X^{r\boldsymbol{v}} - X^{r\boldsymbol{v_0}}$.

$\square$

Theorem 1. *Let c be a finitary integral configuration with a non-trivial annihilator. Then there are non-zero $\boldsymbol{v_1}, \ldots, \boldsymbol{v_m} \in \mathbb{Z}^d$ such that the Laurent polynomial*

$$(X^{\boldsymbol{v_1}} - 1) \cdots (X^{\boldsymbol{v_m}} - 1)$$

annihilates c.

Proof. This is an easy corollary of Lemma 3. The polynomial $g(X)$ vanishes on all common roots of $\mathrm{Ann}(c)$, therefore by Hilbert's Nullstellensatz there is n such that $g^n(X) \in \mathrm{Ann}(c)$. Note that any monomial multiple of an annihilator is again an annihilator. Therefore also

$$\frac{g^n(X)}{x_1^n \cdots x_d^n X^{nr\boldsymbol{v_0}(|S|-1)}}$$

is, and it is a Laurent polynomial of the desired form. $\square$

Multiplying a configuration by $(X^{\boldsymbol{v}} - 1)$ can be seen as a *"difference operator"* on the configuration. Theorem 1 then says, that there is a sequence of difference operators which annihilates the configuration. We can reverse the process: let us start by the zero configuration and step by step *"integrate"* until we obtain the original configuration. This idea gives the Decomposition theorem:

Theorem 2 (Decomposition theorem). *Let c be a finitary integral configuration with a non-trivial annihilator. Then there exist periodic integral configurations $c_1, \ldots, c_m$ such that $c = c_1 + \cdots + c_m$.*

Example 3. Recall the 3D counter example in Example 1. It is the sum $c_1 + c_2$ where $c_1(i, 0, 0) = 1$ and $c_2(0, i, n) = 1$ for all $i \in \mathbb{Z}$, and all other entries are 0. Configurations c_1 and c_2 are $(1, 0, 0)$- and $(0, 1, 0)$-periodic, respectively, so that $(X^{(1,0,0)} - 1)(X^{(0,1,0)} - 1)$ annihilates $c = c_1 + c_2$. $\square$

Example 4. The periodic configurations $c_1, \ldots, c_m$ in Theorem 2 may, for some configurations c, be necessarily non-finitary. Let $\alpha \in \mathbb{R}$ be irrational, and define three periodic two-dimensional configurations c_1, c_2 and c_3 by

$$c_1(i,j) = \lfloor i\alpha \rfloor, \qquad c_2(i,j) = \lfloor j\alpha \rfloor, \qquad c_3(i,j) = \lfloor (i+j)\alpha \rfloor.$$

Then $c = c_3 - c_1 - c_2$ is a finitary integral configuration (over alphabet $\{0, 1\}$), annihilated by the polynomial $(X^{(1,0)} - 1)(X^{(0,1)} - 1)(X^{(1,-1)} - 1)$, but it cannot be expressed as a sum of finitary periodic configurations. □

4 Structure of the Annihilator Ideal

In the rest of the paper we focus on two-dimensional configurations. We analyze $\mathrm{Ann}(c)$ using tools of algebraic geometry and provide a description of a polynomial ϕ which divides every annihilator. Moreover we show a theoretical result that $\mathrm{Ann}(c)$ is a radical ideal, which allows us to provide a stricter version of the Decomposition theorem for two-dimensional configurations.

The key ingredient needed for further analysis is the concept of a *line polynomial*. Let the *support* of a Laurent polynomial $f = \sum a_{\boldsymbol{v}} X^{\boldsymbol{v}}$ be defined as

$$\mathrm{supp}(f) = \{\, \boldsymbol{v} \in \mathbb{Z}^d \mid a_{\boldsymbol{v}} \neq 0 \,\}.$$

We say that f is a *line Laurent polynomial* if the support contains at least two points and all the points lie on a single line. Let us call a vector $\boldsymbol{v} \in \mathbb{Z}^d$ *primitive* if its coordinates don't have a common non-trivial integer factor. Then every line Laurent polynomial can be expressed as

$$f(X) = X^{\boldsymbol{v}'}(a_n X^{n\boldsymbol{v}} + \cdots + a_1 X^{\boldsymbol{v}} + a_0)$$

for some $a_i \in \mathbb{C}$, $n \geq 1$, $a_n \neq 0 \neq a_0$, $\boldsymbol{v}', \boldsymbol{v} \in \mathbb{Z}^d$, $\boldsymbol{v}$ primitive. Moreover, the vector $\boldsymbol{v}$ is determined uniquely up to the sign. We define the *direction* of a line Laurent polynomial to be the vector space $\langle \boldsymbol{v} \rangle \subset \mathbb{Q}^d$.

To simplify the notation, we prefer to write $\mathbb{C}[x, y]$ in the place of $\mathbb{C}[x_1, x_2]$. We begin by a sequence of lemmas with a result from algebra. Recall that an ideal A is *prime* whenever $ab \in A$ implies $a \in A$ or $b \in A$. An ideal is *radical* if $a^n \in A$ implies $a \in A$.

Lemma 4.

1. *Prime ideals in $\mathbb{C}[x, y]$ are maximal ideals, principal ideals generated by irreducible polynomials, and the zero ideal.*
2. *Every radical ideal $A \leq \mathbb{C}[x, y]$ can be uniquely written as a finite intersection of prime ideals $P_1, \ldots, P_k$ where $P_i \not\subset P_j$ for $i \neq j$. Moreover*

$$A = \bigcap_{i=1}^{k} P_i = \prod_{i=1}^{k} P_i.$$

Lemma 5. *Let c be a two-dimensional, finitary and integral configuration with a non-trivial annihilator. Then $\mathrm{Ann}(c)$ is radical.*

Our proof of Lemma 5 relies on the decomposition of two-dimensional radical ideals into a product of primes from Lemma 4, which fails in higher dimensions. However, we conjecture that Lemma 5 is true for higher dimensions as well.

Lemma 6. *Let c be as in Lemma 5. Then there exist polynomials $\phi_1, \ldots, \phi_m$ and an ideal $H \le \mathbb{C}[x, y]$ such that*

$$\mathrm{Ann}(c) = \phi_1 \cdots \phi_m H$$

where ϕ_i are line polynomials in pairwise distinct directions, and H is either an intersection of finitely many maximal ideals or $H = \mathbb{C}[x, y]$.
Moreover H is determined uniquely and ϕ_i are determined uniquely up to the order and multiplication by a constant.

Note that $H = \mathbb{C}[x, y]$ is not really a special case – it covers the case when H is the empty intersection. Let us denote the number m from Lemma 6 by $\mathrm{ord}(c)$. It is an important invariant of the configuration which provides information about its periodicity. A two-dimensional configuration is *doubly periodic* if there are two linearly independent vectors in which it is periodic. A configuration which is periodic but not doubly periodic is called *one-periodic*.

Theorem 3 (Strong decomposition theorem). *Let c, $m = \mathrm{ord}(c)$, and $\mathrm{Ann}(c) = \phi_1 \cdots \phi_m H$ be as in Lemma 6. Let $\phi = \phi_1 \cdots \phi_m$. Then there exist configurations $c_\phi, c_H, c_1, \ldots, c_m$ such that*

$$c = c_\phi + c_H$$
$$c_\phi = c_1 + \cdots + c_m,$$

where $\mathrm{Ann}(c_\phi) = \langle \phi \rangle$, $\mathrm{Ann}(c_H) = H$ and $\mathrm{Ann}(c_i) = \langle \phi_i \rangle$. Moreover c_ϕ and c_H are determined uniquely. Each c_i is one-periodic in the direction of ϕ_i, and c_H is doubly periodic.

Corollary 1. *Let c be as in Theorem 3. Then*

- *if $\mathrm{ord}(c) = 0$ the configuration is doubly periodic,*
- *if $\mathrm{ord}(c) = 1$ the configuration is one-periodic,*
- *if $\mathrm{ord}(c) \ge 2$ the configuration is non-periodic.*

5 Approaching Nivat's Conjecture

We already know that if a finitary integral configuration c satisfies the condition $P_c(m, n) \le mn$ for some positive integers m, n, then it has an annihilating polynomial. The Nivat's conjecture claims that such a configuration is periodic, that is, $\mathrm{ord}(c) \le 1$. Our approach is the contrapositive: assume that c is a finitary integral configuration which is non-periodic, that is, $\mathrm{ord}(c) \ge 2$. If c does not

have an annihilating polynomial, we have $P_c(m,n) > mn$ for all m and n, and we are done. So we assume c has an annihilating polynomial so that the theory developed so far applies to c. We want to prove that c has high local complexity.

Assuming $\mathrm{ord}(c) \geq 2$, let φ_1 and φ_2 be irreducible factors of ϕ_1 and ϕ_2. Any annihilator of c has a factor $f \in \mathrm{Ann}(c)$ that can be written as $f = \varphi_1 \varphi_2 f'$ such that $c_1 = \varphi_2 f' c$ and $c_2 = \varphi_1 f' c$ are one-periodic configurations in different directions. Moreover, a block in c determines smaller blocks in $\varphi_2 f' c$ and $\varphi_1 f' c$ because the multiplication by a polynomial is a local operation on the configurations. We next estimate the number of distinct blocks in one-periodic configurations in order to lower bound the number of slightly bigger blocks in c.

Complexity of One-periodic Configurations

Recall that for a finite domain $D \subset \mathbb{Z}^d$ we denote by $c_{\boldsymbol{v}+D}$ the pattern extracted from the position $\boldsymbol{v} \in \mathbb{Z}^d$ in c. Let us define a *line of D-patterns in direction* $\boldsymbol{u} \in \mathbb{Z}^d$ to be a set of the form

$$\mathcal{L} = \left\{ c_{\boldsymbol{v}+k\boldsymbol{u}+D} \mid k \in \mathbb{Z} \right\}$$

for some vector $\boldsymbol{v} \in \mathbb{Z}^d$.

It is easy to characterize irreducible factors of line polynomials – every line polynomial can be decomposed as

$$f(X) = X^{\boldsymbol{v}'}(a_n X^{n\boldsymbol{v}} + \cdots + a_1 X^{\boldsymbol{v}} + a_0)$$
$$= a_n X^{\boldsymbol{v}'}(X^{\boldsymbol{v}} - \lambda_1) \ldots (X^{\boldsymbol{v}} - \lambda_n)$$

where $a_0 \neq 0 \neq a_n$, $\boldsymbol{v}$ is a primitive vector and $\lambda_1, \ldots, \lambda_n$ are complex roots of the polynomial $a_n t^n + \cdots + a_1 t + a_0$. A Laurent polynomial of the form $X^{\boldsymbol{v}} - \lambda_i$ is irreducible. Therefore an irreducible polynomial factor of f either divides $X^{\boldsymbol{v}'}$, or has to be up to a multiplicative constant of the form $X^{\boldsymbol{v}''}(X^{\boldsymbol{v}} - \lambda_i)$ for some $\boldsymbol{v}'' \in \mathbb{Z}^d$.

The following two lemmas will be applied later on the one-periodic configurations $c_1 = \varphi_2 f' c$ and $c_2 = \varphi_1 f' c$, respectively. For a vector $\boldsymbol{v} = (v_1, v_2) \in \mathbb{Z}^2$ let us denote the size of a minimal rectangle that contains it by $Box(\boldsymbol{v}) := (|v_1|, |v_2|) \in \mathbb{Z}^2$.

Lemma 7. *Let c be a two-dimensional one-periodic configuration and $\boldsymbol{v}', \boldsymbol{v} \in \mathbb{Z}^2$, $0 \neq \lambda \in \mathbb{C}$ such that $\mathrm{Ann}(c) = \langle X^{\boldsymbol{v}'}(X^{\boldsymbol{v}} - \lambda) \rangle$. Let $(m,n) = Box(\boldsymbol{v})$. Then for any non-negative integers M, N there are at least $Mn + mN + mn$ disjoint lines of blocks $(M+m) \times (N+n)$ in c in the direction of $\boldsymbol{v}$.*

Lemma 8. *Let c be a two-dimensional one-periodic configuration and $\boldsymbol{u}', \boldsymbol{u} \in \mathbb{Z}^2$, $0 \neq \lambda \in \mathbb{C}$ such that $\mathrm{Ann}(c) = \langle X^{\boldsymbol{u}'}(X^{\boldsymbol{u}} - \lambda) \rangle$. Let $(m,n) = Box(\boldsymbol{u})$ and $\boldsymbol{v} \in \mathbb{Z}^2$ be a vector in a different direction than $\boldsymbol{u}$.*

If $\mathcal{L}$ is any line of blocks $(M+m) \times (N+n)$ in direction $\boldsymbol{v}$ in c, then

$$|\mathcal{L}| > \frac{Mn + mN}{S},$$

where S is the positive area of the parallelogram specified by vectors $\boldsymbol{u}$ and $\boldsymbol{v}$.

Putting Things Together

Applying Lemmas 7 and 8 on the configurations $c_1 = \varphi_2 f'c$ and $c_2 = \varphi_1 f'c$ provides the following lower bound for their common pre-image $c' = f'c$.

Lemma 9. *Let c' be a two-dimensional configuration such that*

$$\mathrm{Ann}(c') = \langle X^{\boldsymbol{v'}}(X^{\boldsymbol{v_1}} - \lambda_1)(X^{\boldsymbol{v_2}} - \lambda_2)\rangle$$

where $\lambda_1, \lambda_2 \in \mathbb{C}$ are non-zero, $\boldsymbol{v'}, \boldsymbol{v_1}, \boldsymbol{v_2} \in \mathbb{Z}^2$ and $\boldsymbol{v_1}, \boldsymbol{v_2}$ are primitive vectors. Denote $(m_i, n_i) = \mathrm{Box}(\boldsymbol{v_i})$. Then

$$P_{c'}(M + m_1 + m_2, N + n_1 + n_2) > \frac{(Mn_1 + m_1N)(Mn_2 + m_2N)}{m_1n_2 + m_2n_1}$$

for all non-negative integers M and N.

Let f be a Laurent polynomial in two variables and S its support. Let us extend the definition of the bounding box $\mathrm{Box}(\cdot)$ by setting

$$\mathrm{Box}(f) = (\max_{(a,b)\in S} a - \min_{(a,b)\in S} a, \max_{(a,b)\in S} b - \min_{(a,b)\in S} b).$$

Corollary 2. *Let c be a two-dimensional non-periodic finitary integral configuration and f its annihilator. Denote $(m,n) = \mathrm{Box}(f)$ and let $M \geq m, N \geq n$ be integers. Then:*

(a) $P_c(M, N) > (M - m)(N - n)$.
(b) If in the decomposition $\mathrm{Ann}(c) = \phi_1 \cdots \phi_{\mathrm{ord}(c)} H$ there are two ϕ_i, ϕ_j such that their directions are not horizontal or vertical, then $\exists \alpha > 1$:

$$P_c(M, N) > \alpha(M - m)(N - n).$$

(c) If $\mathrm{ord}(c) \geq 3$ then

$$P_c(M, N) > 2(M - m)(N - n).$$

The Main Result

Theorem 4. *Let c be a two-dimensional non-periodic configuration. Then $P_c(M, N) > MN$ holds for all but finitely many choices $M, N \in \mathbb{N}$.*

Corollary 3. *If c is a two-dimensional configuration such that $P_c(M, N) \leq MN$ holds for infinitely many pairs $M, N \in \mathbb{N}$, then c is periodic.*

The proof (details omitted) is structured as follows. Let c be non-periodic with a non-trivial annihilator, and let $\mathrm{Ann}(c) = \phi H$ be the decomposition of the annihilator as in Theorem 3, where $\phi = \phi_1 \cdots \phi_{\mathrm{ord}(c)}$. We consider different ranges of M and N.

Very thin blocks. Suppose N or M is so small that the support of ϕ does not fit inside the $M \times N$ rectangle. Then no annihilator of c fits inside the rectangle,

and as in Lemma 1 we see that $P_c(M, N) > MN$, no matter how large the other dimension of the rectangle is.

Thin blocks. Consider fixed N, large enough so that the support of ϕ fits inside a strip of height N. It can be shown that there exists M_0 such that for all $M > M_0$ we have $P_c(M, N) > MN$. Analogously for a fixed M.

Fat blocks. We prove that there are constants M_0 and N_0 such that for $M > M_0$ and $N > N_0$ we have $P_c(M, N) > MN$. This follows directly from Corollary 2(c) and (b), respectively, in the cases when $\mathrm{ord}(c) \geq 3$, or when $\mathrm{ord}(c) = 2$ and ϕ_1 and ϕ_2 are not horizontal or vertical. The cases when $\mathrm{ord}(c) = 2$ and ϕ_1 is vertical (or the symmetric cases) require more careful analysis. In particular, we use the observation that it is enough to consider two letter configurations:

Lemma 10. *In any non-periodic configuration $c \in A^{\mathbb{Z}^2}$, letters can be merged to obtain a non-periodic configuration $c' \in \{0, 1\}^{\mathbb{Z}^2}$. Then $P_{c'}(D) \leq P_c(D)$ for all finite $D \subseteq \mathbb{Z}^d$. In particular, if Nivat's conjecture holds on binary configurations it holds in general.*

It is clear that the three ranges of M and N above cover everything so that $P_c(M, N) \leq MN$ can hold only for a finite number of $M, N \in \mathbb{N}$.

References

[BN91]   D. Beauquier and M. Nivat. "On Translating One Polyomino to Tile the Plane". In: *Discrete & Computational Geometry* 6 (1991).

[CK13a]   V. Cyr and B. Kra. "Complexity of short rectangles and periodicity". In: *(submitted)* (2013). arXiv: `1307.0098 [math.DS]`.

[CK13b]   V. Cyr and B. Kra. "Nonexpansive $\mathbb{Z}^2$-subdynamics and Nivat's conjecture". In: *Trans. Amer. Math. Soc. (to appear)* (2013).

[EKM03]   C. Epifanio, M. Koskas, and F. Mignosi. "On a conjecture on bidimensional words". In: *Theor. Comput. Sci.* 1-3.299 (2003).

[LW96]   J. C. Lagarias and Y. Wang. "Tiling the Line with Translates of One Tile". In: *Inventiones Mathematicae* 124 (1996), pp. 341–365.

[LM95]   D. Lind and B. Marcus. *An Introduction to Symbolic Dynamics and Coding.* Cambridge University Press, 1995.

[MH38]   M. Morse and G. A. Hedlund. "Symbolic Dynamics". In: *American Journal of Mathematics* 60.4 (1938), pp. 815–866.

[Niv97]   M. Nivat. *Invited talk at ICALP, Bologna.* 1997.

[QZ04]   A. Quas and L. Q. Zamboni. "Periodicity and local complexity". In: *Theor. Comput. Sci.* 319.1-3 (2004), pp. 229–240.

[ST00]   J. W. Sander and R. Tijdeman. "The complexity of functions on lattices". In: *Theor. Comput. Sci.* 246.1-2 (2000), pp. 195–225.

[ST02]   J. W. Sander and R. Tijdeman. "The rectangle complexity of functions on two-dimensional lattices". In: *Theor. Comput. Sci.* 270.1-2 (2002), pp. 857–863.

[Sze98]   M. Szegedy. "Algorithms to Tile the Infinite Grid with Finite Clusters". In: *FOCS.* IEEE Computer Society, 1998, pp. 137–147.