Discrete Mathematics and Theoretical Computer Science Proceedings **AA (DM-CCG)**, 2001, 079–094

Periodic Patterns in Orbits of Certain Linear Cellular Automata

André Barbé[1] and Fritz von Haeseler[2]

[1]*KU Leuven, Department of Electrical Engineering, Kasteelpark Arenberg 10, 3001 Leuven, Belgium*
[2]*CeVis, Universität Bremen, Universitätsallee 29, 28359 Bremen, Germany*

received February 4, 2001, revised April 20, 2001, accepted May 4, 2001.

We discuss certain linear cellular automata whose cells take values in a finite field. We investigate the periodic behavior of the verticals of an orbit of the cellular automaton and establish that there exists, depending on the characteristic of the field, a universal behavior for the evolution of periodic verticals.

Keywords: cellular automata, p-fold bifurcation of periods, finite fields

1 Introduction

Let p be a prime number, with $\mathbb{F}_q$ we denote the field of characteristic p with $q = p^m$ elements. The set of bidirectional sequences with values in $\mathbb{F}_q$ is denoted as $\mathbb{F}_q^{\mathbb{Z}} = \{\underline{c} = (c_i)_{i\in\mathbb{Z}} \mid c_i \in \mathbb{F}_q \text{ for all } i \in \mathbb{Z}\}$. The cellular automata under investigation in this paper are defined by a map

$$\begin{aligned} A_\phi : \mathbb{F}_q^{\mathbb{Z}} &\to \mathbb{F}_q^{\mathbb{Z}} \\ \underline{c} &\mapsto A_\phi(\underline{c}) = (\phi(c_{i-1}, c_i))_{i\in\mathbb{Z}}, \end{aligned}$$

where the map $\phi : \mathbb{F}_q^2 \to \mathbb{F}_q$ is defined as $\phi(a,b) = \alpha a + \beta b$ with $\alpha, \beta \in \mathbb{F}_q \setminus \{0\}$. The map ϕ is called *local evolution rule* or simply *local rule* of the cellular automaton A_ϕ.

For a given $\underline{c} \in \mathbb{F}_q^{\mathbb{Z}}$ we consider the iterates $A_\phi^j(\underline{c})$, $j \in \mathbb{N}$, of A_ϕ. The ϕ-*orbit* F of $\underline{c}$ under A_ϕ is considered as a two-dimensional sequence and we have

$$F = (F_{i,j})_{(i,j)\in\mathbb{Z}\times\mathbb{N}} = (A_\phi^j(\underline{c})_i)_{(i,j)\in\mathbb{Z}\times\mathbb{N}}.$$

Note that the orbit is uniquely determined by its *initial configuration* $\underline{c} = (F_{i,0})_{i\in\mathbb{Z}}$.

Referring to a standard graphical representation of the ϕ-orbit F (see Figure 1.), whereby the values of $F_{i,j}$ are plotted as colored cells placed on the grid with integer coordinates $(i, j) \in \mathbb{Z}\times\mathbb{N}$ (usually there is a one-to-one correspondence between colors and values), we define the *i-th vertical* V_i of the ϕ-orbit F as the one-dimensional sequence $V_i = (F_{i,j})_{j\in\mathbb{N}}$. Note that, due to the definition of the local rule ϕ, the knowledge of the i-th vertical V_i of a ϕ-configuration enables us to compute the vertical V_{i-1}. If additionally, we know the value of $F_{i+1,0}$, then it is also possible to compute the vertical V_{i+1} of F.

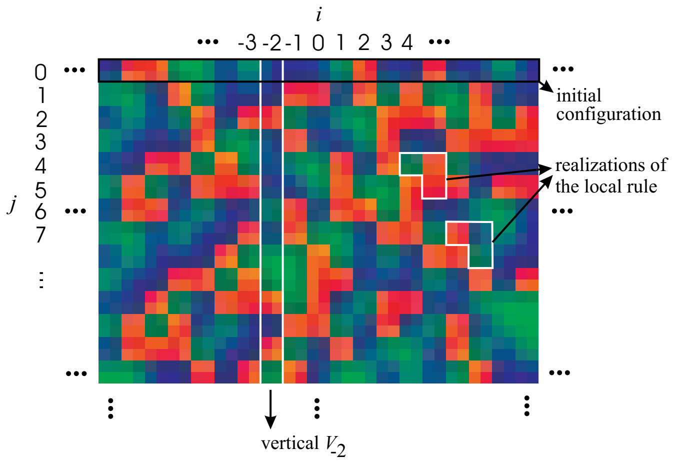

Fig. 1: Graphical representation of part of the orbit of a cellular automaton. The orbit is completely determined by its top row (the initial configuration of the cellular automaton), but also by, for example, the vertical V_{-2} and the initial configuration to the right of V_{-2}.

In this paper we will investigate periodic patterns of the verticals of a ϕ-orbit. In [1], it has been shown that for the case $q = 2$ and the local rule $\phi(a,b) = a+b$, the existence of one periodic vertical in a ϕ-orbit already ensures that all verticals are periodic. Hereby, periods may change by successive doubling while also the number of successive verticals with equal period (the bandwidth) doubles in size.

The goal of this paper is to discuss the more general case. In Section 2, we will discuss ϕ-orbits and their verticals. We will discuss how to (re)construct a ϕ-orbit from the knowledge of a vertical. Furthermore, we establish a certain dichotomy, namely, either all verticals of a ϕ-orbit are periodic or no vertical is periodic.

We introduce the period distribution of a ϕ-orbit and study its behavior in Section 3.

The main result of Section 3 generalizes the above mentioned result. We shall prove that there are only two different types of ϕ-orbits with a periodic vertical: either all verticals have the same period, or eventually the period as well as the bandwidth grow successively by a factor p.

2 Verticals of ϕ-orbits

In this section, we state some elementary properties of ϕ-orbits and their verticals. As already introduced, $\phi : \mathbb{F}_q^2 \to \mathbb{F}_q$ is defined as $\phi(a,b) = \alpha a + \beta b$ with α, $\beta \in \mathbb{F}_q \setminus \{0\}$.

If $F = (F_{i,j})_{(i,j)\in\mathbb{Z}\times\mathbb{N}}$ is a ϕ-orbit, i.e.,

$$\phi(F_{i-1,j}, F_{i,j}) = F_{i,j+1}$$

holds for all $(i,j) \in \mathbb{Z}\times\mathbb{N}$, then we consider its i-th vertical V_i as a power series

$$V_i = V_i(Y) = \sum_{j\in\mathbb{N}} F_{i,j} Y^j$$

with values in $\mathbb{F}_q$. The set of all power series is denoted as $\mathbb{F}_q(Y)$ and, as usual, the set of polynomials with values in $\mathbb{F}_q$ is denoted as $\mathbb{F}_q[Y]$.

Note that, since F is a ϕ-orbit, its shift $\sigma F = (F_{i+1,j})_{(i,j)\in\mathbb{Z}\times\mathbb{N}}$ along the X-axis is also a ϕ-orbit.

Associated to a local rule ϕ are two maps on the set of formal power series $\mathbb{F}_q(Y) = \{f(Y) = \sum_{j\in\mathbb{N}} f_j Y^j \mid f_j \in \mathbb{F}_q\}$. The first one is defined as

$$\begin{aligned} R_{\phi,\xi} &: \mathbb{F}_q(Y) \to \mathbb{F}_q(Y) \\ f(Y) &\mapsto \tfrac{\xi+\alpha Y f(Y)}{1-\beta Y}, \end{aligned} \tag{1}$$

where $\xi \in \mathbb{F}_q$ is a parameter, and is called the *right map of* ϕ, the second one is defined as

$$\begin{aligned} L_\phi &: \mathbb{F}_q(Y) \to \mathbb{F}_q(Y) \\ f(Y) &\mapsto \tfrac{(1-\beta Y) f(Y) - f(0)}{\alpha Y} \end{aligned} \tag{2}$$

and is called *left map of* ϕ. The next lemma collects some elementary properties of the left- and right map, respectively.

Lemma 2.1 *1. For all $f \in \mathbb{F}_q(Y)$ and for all $\xi \in \mathbb{F}_q$ one has*

$$L_\phi(R_{\phi,\xi}(f)) = f.$$

2. For every $f \in \mathbb{F}_q(Y)$ and for $\xi_0 = f(0)$ one has

$$R_{\phi,\xi_0}(L_\phi(f)) = f.$$

3. If F is a ϕ-orbit, then the following two assertions are true

$$\begin{aligned} R_{\phi,F_{i+1,0}}(V_i) &= V_{i+1} \\ L_\phi(V_i) &= V_{i-1} \end{aligned}$$

The proof is a simple consequence of the definitions. Assertion 1. of Lemma 2.1 shows that L_ϕ is the left inverse of all $R_{\phi,\xi}$, while assertion 2. ensures that one has to chose ξ properly to have $R_{\phi,\xi}(L_\phi(f)) = f$. The third assertion reads as: if V_i is the i-th vertical of a ϕ-orbit F, then $R_{\phi,F_{i+1,0}}(V_i)$ is the $(i+1)$-st vertical of F. In other words, the knowledge of the vertical i and the value of vertical V_{i+1} at zero allows us to construct all of the $i+1$-st vertical. The final assertion says that the application of L_ϕ to the i-th vertical of a ϕ-orbit gives the $(i-1)$-st vertical of the orbit.

If $f(Y) \in \mathbb{F}_q(Y)$ is a power series we say that $f = f(Y)$ is *periodic* if there exists a $T > 0$ such that $f_{j+T} = f_j$ holds for all $j \in \mathbb{N}$. The minimal positive T with this property is called the *minimal period* of f. Note that any period T of f is a multiple of the minimal period.

The next theorem shows that the existence of one periodic vertical in a ϕ-orbit F yields the periodicity of all verticals.

Theorem 2.2 *The ϕ-orbit F has a periodic vertical if and only if all verticals of F are periodic.*

Proof — The only thing we have to prove is that the existence of one periodic vertical implies the periodicity of all other verticals.

Let V_i be a vertical of F such that V_i is periodic. To prove the assertion it suffices to show that L_ϕ and $R_{\phi,\xi}$ preserve the periodicity. We begin with the left map L_ϕ. Let $f(Y) = \sum_{j\in\mathbb{N}} f_j Y^j \in F_q(Y)$ be periodic of period τ. By definition of $L_\phi(f)(Y) = \sum_{j\in\mathbb{N}} g_j Y^j$, we have

$$g_j = \frac{1}{\alpha}(-\beta f_j + f_{j+1})$$

for all $j \in \mathbb{N}$. This shows that $g_{j+\tau} = g_j$ for all $j \in \mathbb{N}$ and therefore the periodicity of $L(f)$.

To conclude the proof, we show that $R_{\phi,\xi}$ preserves periodicity. Let $f = f(Y) = \sum f_j Y^j$ be periodic of period τ and denote

$$R_{\phi,\xi}(f)(Y) = \sum r_j Y^j.$$

The definition of $R_{\phi,\xi}$ gives $r_0 = \xi$ and $r_{j+1} = \alpha f_j + \beta r_j$ for $j \in \mathbb{N}$. Using the recursive definition of r_j and the periodicity of $f(Y)$ one shows by induction that for all $l \in \mathbb{N}$

$$r_{l\tau} = \beta^{l\tau}\xi + \alpha\Delta\left(\beta^{(l-1)\tau} + \beta^{(l-2)\tau} + \ldots + \beta^{\tau} + 1\right),$$

with $\Delta = \beta^{\tau-1} f_0 + \beta^{\tau-2} f_1 + \ldots + \beta f_{\tau-2} + f_{\tau-1}$. The choice $l = \mathrm{ord}(\beta)p$, where $\mathrm{ord}(\beta)$ is the smallest positive integer t such that $\beta^t = 1$, gives $r_{\tau\mathrm{ord}(\beta)p} = r_0 = \xi$. The periodicity of f implies $f_{\tau\mathrm{ord}(\beta)p} = f_0$, therefore the recursive construction of the coefficients of $R_{\phi,\xi}$ yields the periodicity of $R_{\phi,\xi}$. ■

The following corollary collects some important properties of the left- and right map.

Corollary 2.3 *Let $f = f(Y) \in \mathbb{F}_q(Y)$ be periodic with minimal period τ.*

1. *The minimal period of $L_\phi(f)$ is a divisor of τ.*
2. *The minimal period of $R_{\phi,\xi}(f)$ is a multiple of the minimal period of f.*

Proof —

1. As we have already seen in the proof of Theorem 2.2, $L_\phi(f)$ has period τ. Therefore, the minimal period of $L_\phi(f)$ is a divisor of τ.
2. By 1. of Lemma 2.1, we have $L_\phi(R_{\phi,\xi}(f)) = f$, By the first assertion we have that the minimal period (which is equal to τ) of $L_\phi(R_{\phi,\xi}(f))$ is a divisor of the minimal period of $R_{\phi,\xi}(f)$. Therefore it follows that the minimal period of $R_{\phi,\xi}(f)$ is a multiple of τ.

■

For a ϕ-orbit F which has a periodic vertical (equivalently all verticals are periodic) we introduce the map $\pi_F : \mathbb{Z} \to \mathbb{N}$ by defining $\pi_F(i)$ as the smallest period of the i-th vertical of F. We call π_F the *period distribution* of F.

We extend the definition of π_F to any ϕ-orbit F by defining $\pi_F(i) = \infty$ if the i-th vertical is not periodic.

As a consequence of Theorem 2.2 we see that for a ϕ-orbit F we either have $\pi_F(i) = \infty$ for all $i \in \mathbb{Z}$ or $\pi_F(i) \in \mathbb{N}$ for all $i \in \mathbb{Z}$.

For ϕ-orbits with a periodic vertical we obtain the following

Corollary 2.4 *If F is a ϕ-orbit with a periodic vertical, then the period distribution π_F is monotonically increasing, i.e.,*

$$\pi_F(i_1) \leq \pi_F(i_2)$$

holds for all i_1, $i_2 \in \mathbb{Z}$ such that $i_1 \leq i_2$.

For a closer analysis of the period distribution we need to study the behavior of the left- and right map more closely.

The following lemma is elementary.

Lemma 2.5 *Let $f(Y) \in \mathbb{F}_q(Y)$ be periodic. If f is of the form*

$$f(Y) = \frac{P(Y)}{1 - Y^T}$$

with a polynomial $P(Y)$ of degree less than T, then f has period T. If f has period T, then there exists a polynomial $P(Y)$ with $\deg(P(Y)) < T$ such that

$$f(Y) = \frac{P(Y)}{1 - Y^T}.$$

We will now investigate the change of the minimal period under application of $R_{\phi,\xi}$ more closely.

Lemma 2.6 *Let $f(Y) \in \mathbb{F}_q(Y)$ such that*

$$f(Y) = \frac{P(Y)}{1 - Y^\tau}$$

is of minimal period τ and let $R_{\phi,\xi}$, L_ϕ be the right- and left map of a local rule $\phi(a,b) = \alpha a + \beta b$, where α, $\beta \in \mathbb{F}_q \setminus \{0\}$. The following statements are true.

1. *If $\operatorname{ord}(\beta)$ does not divide τ, then there exists a ξ_0 such that the minimal period of $R_{\phi,\xi_0}(f)$ is equal to τ and for all $\xi \neq \xi_0$ the minimal period is equal to $\operatorname{lcm}(\operatorname{ord}(\beta), \tau)$.*

2. *If $\operatorname{ord}(\beta)$ divides τ and $P(\beta^{-1}) = 0$, then the minimal period of $R_{\phi,\xi}(f)$ is equal to τ for all $\xi \in \mathbb{F}_q$.*

3. *If $\operatorname{ord}(\beta)$ divides τ and $P(\beta^{-1}) \neq 0$, then the minimal period of $R_{\phi,\xi}(f)$ is equal to $p\tau$ for all $\xi \in \mathbb{F}_q$.*

Proof — Since $f(Y)$ has minimal period τ we may assume that f is of the form

$$f(Y) = \frac{P(Y)}{1 - Y^\tau}$$

and, by the definition of $R_{\phi,\xi}$, see (1), we have

$$R_{\phi,\xi}(f)(Y) = \frac{\xi(1 - Y^\tau) + \alpha Y P(Y)}{(1 - \beta Y)(1 - Y^\tau)}. \tag{3}$$

1. If τ is not divisible by $\operatorname{ord}(\beta)$, then $1-\beta^{-\tau}\neq 0$. For $\xi_0=\frac{-\alpha\beta^{-1}P(\beta^{-1})}{1-\beta^{-\tau}}$, we have that β^{-1} is a zero of the polynomial $\xi(1-Y^\tau)+\alpha P(Y)$. Therefore $R_{\phi,\xi_0}(f)$ is of the form
$$R_{\phi,\xi_0}(f)(Y)=\frac{\overline{P}(Y)}{1-Y^\tau},$$
where $\overline{P}(Y)=\frac{\xi_0(1-Y^\tau)+\alpha YP(Y)}{1-\beta Y}$ is a polynomial of degree less than τ. By 2. of Corollary 2.3 and by Lemma 2.5, it follows that the minimal period of $R_{\phi,\xi_0}(f)$ is equal to τ.

   Now assume that $\xi\neq\xi_0$. Since β^{-1} is not a zero of $1-Y^\tau$ it follows that the polynomials $1-\beta Y$ and $1-Y^\tau$ are relatively prime. By Theorem 3.9 in [4], it follows that the order of the polynomial $(1-\beta Y)(1-Y^\tau)$ is equal to $\operatorname{lcm}(\operatorname{ord}(\beta),\tau)=l\tau$, $l>1$. In other words, there exists a polynomial $H(Y)$ such that $H(Y)(1-\beta Y)(1-Y^\tau)=1-Y^{l\tau}$. Since $1-\beta^{-l\tau}=0$, we have $1-Y^{l\tau}=(1-\beta Y)^sG(Y)$ with $s\geq 1$ and $G(\beta^{-1})\neq 0$ and therefore $H(Y)=(1-\beta Y)^{s-1}\overline{H}(Y)$, where $\overline{H}(Y)$ is a polynomial such that $\overline{H}(\beta^{-1})\neq 0$. Therefore (3) becomes
$$R_{\phi,\xi}(f)(Y)=\frac{(\xi(1-Y^\tau)+\alpha YP(Y))H(Y)}{1-Y^{l\tau}}.$$
   Since the degree of the numerator is less than $l\tau$, Lemma 2.5 applies, i.e., the period is equal to $l\tau$. By Corollary 2.3, a minimal period of $R_{\phi,\xi}(f)$ has to be a multiple of τ and also a divisor of $l\tau$. We therefore assume that the minimal period of $R_{\phi,\xi}(f)$ is equal to $l^*\tau$, where $1\leq l^*<l$ is a divisor of l. Under this assumption $R_{\phi,\xi}(f)$ is of the form
$$R_{\phi,\xi}(f)(Y)=\frac{Q(Y)}{1-Y^{l^*\tau}},$$
   i.e.,
$$R_{\phi,\xi}(f)(Y)=\frac{Q(Y)}{1-Y^{l^*\tau}}=\frac{(\xi(1-Y^\tau)+\alpha YP(Y)H(Y)}{1-Y^{l\tau}}.$$
   This gives
$$(\xi(1-Y^\tau)+\alpha YP(Y))H(Y)=\frac{Q(Y)(1-Y^{l\tau})}{1-Y^{l^*\tau}},$$
   using $H(Y)=(1-\beta Y)^{s-1}\overline{H}(Y)$ and $1-Y^{l\tau}=(1-\beta Y)^sG(Y)$ we obtain
$$(\xi(1-Y^\tau)+\alpha YP(Y))(1-\beta Y)^{s-1}\overline{H}(Y)=(1-\beta Y)^s\frac{G(Y)Q(Y)}{1-Y^{l^*\tau}}.$$
   The right hand side of the above equation has β^{-1} as a zero of order at least s. Since $\xi\neq\xi_0$ the left hand side has β^{-1} as a zero of order $s-1$. This gives a contradiction, therefore the minimal period of $R_{\phi,\xi}(f)$ is equal to $\operatorname{lcm}(\operatorname{ord}(\beta),\tau)$.

2. Due to the assumptions we have $(1-Y^\tau)=(1-\beta Y)G(Y)$ and $P(Y)=(1-\beta Y)\overline{P}(Y)$, where $\overline{P}$ has degree less than $\tau-1$. Therefore (3) becomes
$$R_{\phi,\xi}(f)(Y)=\frac{\xi G(Y)+\alpha Y\overline{P}(Y)}{1-Y^\tau},$$
   and the minimal period $R_{\phi,\xi}(f)(Y)$ is equal to τ.

3. Since $1 - Y^\tau$ is divisible by $1 - \beta Y$, there exists an $s \geq 1$ such that $1 - Y^\tau = (1-\beta Y)^s G(Y)$ with $G(\beta^{-1}) \neq 0$. Moreover, we have

$$(1 - Y^\tau)^p = 1 - Y^{p\tau} = (1-\beta Y)^{ps} G(Y)^p, \tag{4}$$

since $\mathbb{F}_q$ has characteristic p. Therefore (3) becomes

$$R_{\phi,\xi}(f)(Y) = \frac{\xi(1-Y^\tau) + \alpha Y P(Y)}{(1-\beta Y)^{s+1} G(Y)},$$

and using (4), we finally obtain

$$R_{\phi,\xi}(Y) = \frac{(\xi(1-Y^\tau) + \alpha Y P(Y))(1-\beta Y)^{p(s-1)-1} G(Y)^{p-1}}{1 - Y^{p\tau}}.$$

As the degree of the numerator is less then $p\tau$, the period of $R_{\phi,\xi}(f)$ is equal to $p\tau$. It remains to show that $p\tau$ is the minimal period. By Corollary 2.3, the minimal period has to be a multiple of τ. Since p is a prime number, we have to exclude τ as a minimal period.

If we suppose that the minimal period is τ, then we have

$$R_{\phi,0}(f)(Y) = \frac{H(Y)}{1-Y^\tau} = \frac{\xi(1-Y^\tau) + \alpha Y P(Y)}{(1-Y^\tau)(1-\beta Y)}$$

for a polynomial $H(Y)$. This implies that the polynomial $\alpha Y P(Y)$ is equal to $H(Y)(1-\beta Y) - \xi(1-Y^\tau)$, and therefore β^{-1} is a zero of $P(Y)$, which contradicts our assumption. Therefore the minimal period is equal to $p\tau$.

∎

3 Structure of the period distribution π_F

After the preparatory results in the previous chapter we will now study the period distribution π_F of a ϕ-orbit F with a periodic vertical.

As we have already seen in Corollary 2.4, the period distribution is monotonically increasing. We can therefore conclude that there exists an $i_0 \in \mathbb{Z}$ such that

$$\pi_F(i) = \pi_F(i_0)$$

holds for all $i \leq i_0$. Since L_ϕ maps periodic sequences of period $\pi(i_0)$ to periodic sequences of the same period, the sequence of iterates $L^n(V_{i_0})$, $n \geq 0$, satisfies $\pi_F(i_0 - n) = \pi_F(i_0)$ for all $n \in \mathbb{N}$, i.e., all verticals V_i, $i \leq i_0$ have the same minimal period. These facts imply that the sequence $(L_\phi^n(V_{i_0}))_{n\geq 0}$ is eventually periodic. In other words, there exists a maximal $i_1 = i_1(F) \leq i_0$ and a minimal positive $\sigma \in \mathbb{N}$ such that

$$V_{i-\sigma} = V_i$$

for all $i \leq i_1$.

Since a shift along the X-axis preserves the property of being a ϕ-orbit, we may always assume that $i_1(F)$ is equal to zero. I.e., from now on we assume that a ϕ-orbit F with a periodic vertical satisfies the following conditions

$$\begin{array}{l} 1.\ \pi_F(i) = \pi_F(0) = \tau_F \text{ for all } i \leq 0 \\ 2.\ \text{There exists a minimal } \sigma_F > 0 \text{ such that } V_{i-\sigma_F} = V_i \text{ for all } i \leq 0. \end{array} \tag{5}$$

The study of the period distribution is then reduced to a study of $\pi_F : \mathbb{Z} \to \mathbb{N}$ restricted to arguments being positive natural numbers.

Theorem 3.1 *Let F be a ϕ-orbit with a periodic vertical and initial configuration $\underline{c} = (c_i)_{i\in\mathbb{Z}}$. If the period distribution π_F is bounded, then the initial configuration $\underline{c}$ of F has period σ_F.*

Proof — It is no restriction to assume that F satisfies (5). Then we have have $V_{i-\sigma_F} = V_i$ for all $i \leq 0$. In particular, $c_{i-\sigma_F} = c_i$ for all $i \leq 0$.

By Corollary 2.4, $\pi_F : \mathbb{Z} \to \mathbb{N}$ is monotonically increasing. Since π_F is assumed to be bounded, it follows that π_F is eventually constant, i.e., there exist a i_0 such that $\pi_F(i_0) = \pi_F(i) = T$ for all $i \geq i_0$. In other words, the minimal period of V_i is equal to T for all $i \geq i_0$.

Since $V_{i_0} = L_\phi^n(V_{i_0+n})$ for all $n \in \mathbb{N}$ and since there are only finitely many periodic sequences $f(Y) \in \mathbb{F}_q(Y)$ with minimal period T, it follows that V_{i_0} is a periodic point of L_ϕ. By Corollary 2.3, L_ϕ does not increase the minimal period and since V_{i_0} is a periodic point of L_ϕ, it follows that the minimal period of $L_\phi^n(V_{i_0})$ is equal to T for all $n \in \mathbb{N}$.

For the choice $n = i_0$ we therefore obtain $\pi_F(0) = \pi_F(i_0)$ and therefore $T = \tau_F$. In other words, $\pi_F(i) = \tau_F$ for all $i \in \mathbb{Z}$.

The periodicity of $\underline{c}$ now follows from the fact that V_{i_0} belongs to the set $\{L_\phi^s(V_0) \mid s = 0, \ldots, \sigma_F - 1\}$. In fact, the period of $\underline{c}$ is equal to σ_F. ■

As a consequence of the above theorem we have a characterization of periodic points of the cellular automaton A_ϕ.

Corollary 3.2 *The initial configuration $\underline{c}$ is a periodic point of the cellular automaton A_ϕ if and only if the period distribution π_F of the ϕ-orbit F with initial configuration $\underline{c}$ is bounded.*

Proof — If $\underline{c}$ is a periodic point of period τ, then we have $\underline{c} = A_\phi^\tau(\underline{c})$. This implies that $\pi_F(i) = \tau$ for all $i \in \mathbb{Z}$.

Let F be the ϕ-orbit with initial configuration $\underline{c}$ such that π_F is bounded. By Theorem 3.1, it follows that $\pi_F(i) = \tau_F$ for all $i \in \mathbb{Z}$. Therefore $\underline{c}$ is a periodic point of the cellular automaton A_ϕ. ■

Moreover, if $\underline{c}$ is a periodic point of the cellular automaton A_ϕ, i.e., $A^n(\underline{c}) = \underline{c}$, then the sequence $\underline{c}$ is itself a periodic sequence.

The following corollary is obvious.

Corollary 3.3 *If F is a ϕ-orbit such that its initial configuration $\underline{c}$ is not a periodic sequence, then π_F is unbounded.*

The next theorem provides a necessary and sufficient criterion for the existence of a periodic vertical in a ϕ-orbit.

Theorem 3.4 *The ϕ-orbit F with initial configuration $\underline{c}$ has a periodic vertical if and only the initial configuration $\underline{c}$ satisfies the following two conditions*

1. *$\underline{c}$ is eventually periodic to the left, i.e., there exist i_0 and $T > 0$ such that $c_{i-T} = c_i$ hold for all $i \leq i_0$.*
2. *The initial sequence $\underline{\tilde{c}} = (\tilde{c}_i)_{i\in\mathbb{Z}}$ defined as $\tilde{c}_i = c_{i'}$, where $i \equiv i' \mod T$ and $i' \leq i_0$, is a periodic point of the cellular automaton A_ϕ.*

Proof — Let F be a ϕ-orbit with a periodic vertical. As we have already seen, the initial configuration $\underline{c}$ is periodic to the left, i.e., $c_{i-T} = c_i$ for a $T > 0$ and all $i \leq i_0$. By construction of the sequence $\underline{\tilde{c}}$, we see that $\underline{\tilde{c}}$ and $\underline{c}$ coincide for all $i \leq i_0$. Moreover, $A^n_\phi(\underline{c})$ and $A^n_\phi(\underline{\tilde{c}})$ coincide for all $i \leq i_0$ and for all $n \in \mathbb{N}$. Since all verticals V_i of F are periodic for all $i \leq i_0$, $\underline{\tilde{c}}$ is a periodic point of the cellular automaton.

Let F be a ϕ-orbit with initial configuration $\underline{c}$ which satisfies both assumptions. Then $A^n_\phi(\underline{\tilde{c}})$ and $A^n_\phi(\underline{c})$ coincide for all $i \leq i_0$ and all $n \in \mathbb{N}$. Since $\underline{\tilde{c}}$ is a periodic point of A_ϕ, the ϕ-orbit F has a periodic vertical. ■

For π_F unbounded we are interested in the growth behavior of π_F. To study this behavior we introduce the signature of a periodic sequence.

Definition 3.5 *Let $f(Y) \in \mathbb{F}_q(Y) = \frac{P(Y)}{1-Y^\tau}$ be periodic with minimal period $\tau \geq 1$. The* signature of f (w.r.t. ϕ) *is the triple $\mathrm{sig}_\phi(f) = (a,s,\tau)$, where $a \in \mathbb{N}$ satisfies $P(Y) = (1-\beta Y)^a Q(Y)$ and $Q(\beta^{-1}) \neq 0$ and $s \in \mathbb{N}$ satisfies $1 - Y^\tau = (1-\beta Y)^s G(Y)$ with $G(\beta^{-1}) \neq 0$.*

The understanding of the period distribution π_F relies on the change of the signature $\mathrm{sig}_\phi(V_i)$ under the application of $R_{\phi,\xi}$. The next theorem provides a complete list of possible changes of $\mathrm{sig}_\phi(f)$ under application of $R_{\phi,\xi}$.

Theorem 3.6 *Let $f(Y) \in \mathbb{F}_q(Y)$ be periodic and let $\rho = \mathrm{ord}(\beta)$.*

1. *If $\mathrm{sig}_\phi(f) = (a,0,\tau)$, $a \geq 0$, then there exists a $\xi_0 \in \mathbb{F}_q$ such that*
$$\mathrm{sig}_\phi(R_{\phi,\xi}(f)) = \begin{cases} (a^*,0,\tau) & \text{if } \xi = \xi_0 \\ (s-1,s,\mathrm{lcm}(\rho,\tau)) & \text{if } \xi \neq \xi_0, \end{cases}$$
where $a^* \geq 0$ and $s \geq 1$ satisfies $1 - Y^{\mathrm{lcm}(\rho,\tau)} = (1-\beta Y)^s G(Y)$ with $G(\beta^{-1}) \neq 0$.
2. *If $\mathrm{sig}_\phi(f) = (0,s,\tau)$ with $s \geq 1$, then*
$$\mathrm{sig}_\phi(R_{\phi,\xi}(f)) = ((p-1)s-1, ps, p\tau)$$
for all $\xi \in \mathbb{F}_q$.
3. *If $\mathrm{sig}_\phi(f) = (a,a,\tau)$ with $a \geq 1$, then there exists a $\xi_0 \in \mathbb{F}_q$ such that*
$$\mathrm{sig}_\phi(R_{\phi,\xi}(f)) = \begin{cases} (a^*,a,\tau) & \text{if } \xi = \xi_0 \\ (a-1,a,\tau) & \text{if } \xi \neq \xi_0, \end{cases}$$
where $a^* \geq a$.
4. *If $\mathrm{sig}_\phi(a,s,\tau)$ with $a > s \geq 1$, then*
$$\mathrm{sig}_\phi(R_{\phi,\xi}(f)) = \begin{cases} (a-1,s,\tau) & \text{if } \xi = 0 \\ (s-1,s,\tau) & \text{if } \xi \neq 0. \end{cases}$$

5. *If* $\mathrm{sig}_\phi(f) = (a,s,\tau)$ *with* $1 \le a < s$*, then*

$$\mathrm{sig}_\phi(R_{\phi,\xi}(f)) = (a-1,s,\tau)$$

for all $\xi \in \mathbb{F}_q$.

Proof — Using $P(Y) = (1-\beta Y)^a Q(Y)$ and $1 - Y^\tau = (1-\beta)^s G(G)$, where $a, s \ge 0$ and $Q(\beta^{-1})$, $G(\beta^{-1}) \neq 0$, we obtain for $R_{\phi,\xi}(f)$, see (1), the following expression

$$R_{\phi,\xi}(f)(Y) = R_{\phi,\xi}\left(\frac{P(Y)}{1-Y^\tau}\right) = \frac{\xi(1-\beta Y)^s + \alpha Y(1-\beta Y)^a Q(Y)}{(1-\beta Y)^{s+1} G(Y)}. \tag{6}$$

The proof is based on a discussion of the above formula for the different choices of the signature. Furthermore, note that the degree of the numerator is less than the degree of the denumerator.

1. The assumption $\mathrm{sig}_\phi(F) = (a,0,\tau)$, $a \ge 1$ implies that (6) becomes

$$R_{\phi,\xi}(f)(Y) = \frac{\xi(1-Y^\tau) + \alpha Y(1-\beta Y)^a Q(Y)}{(1-\beta Y)(1-Y^\tau)}.$$

Now 1. of Lemma 2.6 applies, i.e., there exists a ξ_0 such that $R_{\phi,\xi_0}(f)$ has minimal period τ, i.e., $\mathrm{sig}_\phi(R_{\phi,\xi_0}(f)) = (a^*,0,\tau)$, where $a^* \ge 0$.
If $\xi \neq \xi_0$, then by the same arguments given in the proof of 1. of Lemma 2.6, we have

$$R_{\phi,\xi}(f)(Y) = \frac{(\xi(1-Y^\tau) + \alpha Y P(Y))H(Y)}{1 - Y^{\mathrm{lcm}(\rho,\tau)}},$$

where $H(Y) = (1-\beta Y)^{s-1}\overline{H}(Y)$ and $\overline{H}(\beta^{-1}) \neq 0$ and s is such that $1 - Y^{\mathrm{lcm}(\rho,\tau)} = (1-\beta Y)^s G(Y)$. Therefore $\mathrm{sig}_\phi(R_{\phi,\xi}(f)) = (s-1, s, \mathrm{lcm}(\mathrm{ord}(\beta),\tau))$.

2. The assumption $\mathrm{sig}_\phi(f) = (0,s,\tau)$, $s \ge 1$ implies that (6) becomes

$$R_{\phi,\xi}(f)(Y) = \frac{\xi(1-\beta Y)^s G(Y) + \alpha Y Q(Y)}{(1-\beta Y)^{s+1} G(Y)}.$$

Since $s \ge 1$, it follows that $1 - \beta^{-\tau} = 0$, i.e., $\mathrm{ord}(\beta)$ is a divisor of τ.Therefore 3. of Lemma 2.6 applies, i.e., the minimal period of $R_{\phi,\xi}(f)$ is equal to $p\tau$ and we have

$$R_{\phi,\xi}(f)(Y) = \frac{(\xi(1-Y^\tau) + \alpha Y Q(Y))(1-\beta Y)^{(p-1)s-1} G(Y)^{p-1}}{1 - Y^{p\tau}}.$$

Since $\xi(1-\beta^{-\tau}) = 0$ for all $\xi \in \mathbb{F}_q$ and $Q(\beta^{-1}) \neq 0$, it follows that $\mathrm{sig}_\phi(R_{\phi,\xi}(f)) = ((p-1)s - 1, ps, p\tau)$.

3. The assumption $\mathrm{sig}_\phi(f) = (a,a,\tau)$, $a \ge 1$, implies that (6) is equal to

$$R_{\phi,\xi}(f)(Y) = \frac{(1-\beta Y)^a(\xi G(Y) + \alpha Y Q(Y))}{(1-\beta Y)^{a+1} G(Y)}.$$

The choice $\xi_0 = \frac{-\alpha\beta^{-1}Q(\beta^{-1})}{G(\beta^{-1})}$ increases the multiplicity of the zero β^{-1} of the numerator by one. This gives

$$R_{\phi,\xi_0}(f)(Y) = \frac{(1-\beta Y)^{a'}Q_1(Y)}{1-Y^\tau},$$

where $a' \geq a$. For $\xi \neq \xi_0$ we obtain

$$R_{\phi,\xi}(f)(Y) = \frac{(1-\beta Y)^{a-1}Q_1(Y)}{1-Y^\tau}.$$

4. The assumption $\mathrm{sig}_\phi(f) = (a,s,\tau)$, $a > s \geq 1$, implies that

$$R_{\phi,\xi}(f)(Y) = \frac{\xi(1-\beta Y)^{S-1}g(Y) + \alpha Y(1-\beta Y)^{a-1}Q(Y)}{1-Y^\tau}.$$

   The choice $\xi = 0$ leads to

$$R_{\phi,0}(f)(Y) = \frac{(1-\beta Y)^{a-1}Q_1(Y)}{1-Y^\tau}$$

   and for $\xi \neq 0$ we obtain, since $s < a$,

$$R_{\phi,\xi}(f)(Y) = \frac{(1-\beta Y)^{s-1}Q_1(Y)}{1-Y^\tau}.$$

5. The assumption $\mathrm{sig}_\phi(f) = (a,s,\tau)$, $s > a \geq 1$, transforms (6) into

$$R_{\phi,\xi}(f)(Y) = \frac{(1-\beta Y)^{a-1}Q_1(Y)}{1-Y^\tau},$$

   for all $\xi \in \mathbb{F}_q$, which proves the assertion.

■

The change of the signature allows a complete description of the growth of a nonconstant π_F.

Theorem 3.7 *Let F be a ϕ-orbit with a periodic vertical such that F satisfies (5) and $\pi_F : \mathbb{Z} \to \mathbb{N}$ is not bounded.*

1. *If the signature $\mathrm{sig}_\phi(V_0) = (a_0, s_0, \tau_0)$ satisfies $s_0 \geq 1$, then there exists an $i_0 \in \mathbb{Z}$ such that*

$$\pi_F(i) = p^{n+1}\tau_0,$$

   whenever $i_0 + (p^n - 1)s_0 \leq i < i_0 + (p^{n+1} - 1)s_0$ and $n \in \mathbb{N}$.

2. *If the signature $\mathrm{sig}_\phi(V_0) = (a_0, 0, \tau)$, then there exists an $i_0 \in \mathbb{Z}$ such that*

$$\pi_F(i) = \mathrm{lcm}(\mathrm{ord}(\beta), \tau_0)$$

   for i such that $i_0 \leq i < i_0 + S$ and

$$\pi_F(i) = p^{n+1}\mathrm{lcm}(\mathrm{ord}(\beta), \tau_0)$$

   for all i such that $i_0 + p^n s \leq i < i_0 + p^{n+1}s$ for $n \in \mathbb{N}$, where s is the multiplicity of the zero β^{-1} of the polynomial $1 - Y^{\mathrm{lcm}(\mathrm{ord}(\beta),\tau)}$.

Proof —

1. Since F has a periodic vertical and π_F is unbounded, there exists a minimal $i_0 > 0$ such that $\pi_F(i_0) > \pi_F(0)$. Because of this and because $s \geq 1$, it follows from Theorem 3.6 that the signature of the i_0-th vertical is given by $\mathrm{sig}_\phi(V_{i_0}) = ((p-1)s_0 - 1, ps_0, p\tau_0)$. Now 5. of Theorem 3.6 applies $((p-1)s_0-1)$-times, i.e., $\mathrm{sig}(V_{i_0+(p-1)s_0-1}) = (0, ps_0, p\tau_0)$. By 2. of Theorem 3.6, $\mathrm{sig}_\phi(V_{i_0+(p-1)s_0}) = ((p-1)ps_0 - 1, p^2 s_0, p^2\tau_0)$. An induction argument completes the assertion.

2. As above, there exists a minimal $i_0 \geq 1$ such that $\pi_F(i_0) > \pi_F(0)$. Since $\mathrm{sig}_\phi(V_0) = (a_0, 0, \tau_0)$ it follows from 1. of Theorem 3.6 that $\mathrm{sig}_\phi(V_{i_0}) = (s-1, s, \mathrm{lcm}(\mathrm{ord}(\beta), \tau_0))$, where $s \geq 1$. By 5. and 2. of Theorem 3.6, we have $\mathrm{sig}_\phi(V_{i_0+s-1}) = (0, s, \mathrm{lcm}(\mathrm{ord}(\beta), \tau_0))$ and $\mathrm{sig}_\phi(V_{i_0+s}) = ((p-1)s - 1, ps, p\,\mathrm{lcm}(\mathrm{ord}(\beta), \tau_0))$ and the arguments given under 1. apply.

■

Note that Theorem 3.7 remains true also if the ϕ-orbit F does not satisfy the requirements (5). By imposing the conditions (5) on the ϕ-orbit F we have guaranteed that we 'see' the complete scenario of period growth for positive values of i.

Examples

1. Figure 2 displays part of the ϕ-orbit of a CA with local rule $\phi(a,b) = a+b$ in $\mathbb{F}_2$, thus $\beta = \beta^{-1} = 1$. The periodic sequence enforced on the vertical V_0 is $\overline{10110}$, corresponding to $P(Y) = 1 + Y^2 + Y^3$. As the multiplicity of the zero β^{-1} in $P(Y)$ is 0, and 1 in $(1-Y^5)$, it follows that $\mathrm{sig}_\phi(V_0) = (0,1,5)$. Applying Theorem 3.5 gives the following evolution in the signature of $V_0, V_1, V_2, \ldots$:

$$(0,1,5)\ (0,2,10)\ (1,4,20)\ (0,4,20)\ (3,8,40)\ (1,8,40)\ (0,8,40)\ (15,16,80)\ \ldots$$

Thus the scenario of Theorem 3.7 is followed, with $i_0 = 1$.
2. Observe that, whereas $V_i = (F_{i,j})_{j\in\mathbb{N}}$ is a vertical for the ϕ-orbit of a cellular automaton with $\phi(a,b) = \alpha a + \beta b$, the *diagonal* sequence $D_i = (F_{i+j,j})_{j\in\mathbb{N}}$ can be considered as a "vertical" for the automaton with rule $\phi'(a,b) = \phi(b,a)$, whereby the application of $R_{\phi',\xi}$ now induces a propagation of the diagonal sequence to the left,i.e., $R_{\phi',\xi}(D_i) = D_{i-1}$, and $L_{\phi'}$ a propagation to the right: $L_{\phi'}(D_i) = D_{i+1}$. When considering both kinds of " verticals" simultaneously, it is nicer to display the orbit such that these "verticals" both appear in a symmetric fashion, as shown in Figure 3. This figure displays the ϕ-orbit of the cellular automaton with local rule $\phi(a,b) = a + 2b$ in $\mathbb{F}_3$, and enforces the periodic sequence $\overline{012}$ on the vertical V_0, and the periodic sequence $\overline{1221}$ on the diagonal D_0. The first cells of V_0 and D_0 are neighbouring cells of the top row. The local rule implies that D_0 and V_0 together define the whole orbit. The region to the left of V_0, i.e., $(V_i)_{i<0}$ is obtained by iteratively applying L_ϕ to V_0; the region to the right of D_0, i.e., $(D_i)_{i>0}$ by applying $L_{\phi'}$ to D_0. The evolution of the periods along $V_i, i > 0$ is governed by the map $R_{\phi,\xi}$, while the evolution of the periods along $D_i, i < 0$ is governed by $R_{\phi',\xi}$.

We first consider the evolution for the left verticals to the right of V_0. The rule is $\phi(a,b) = (a + 2b) \bmod 3$, and thus $\beta = \beta^{-1} = 2$. The periodic sequence V_0 is $P(Y) = Y + 2Y^2$, its period τ is equal to 3. The multiplicity of the zero $\beta^{-1} = 2$ is 0 in both $P(Y)$ and in $1 - Y^3$. Therefore, $\mathrm{sig}_\phi(V_0) = (0,0,3)$. We are now in case 1. of Theorem 3.6. As $\mathrm{ord}(\beta) = 2$ does not divide $\tau = 3$, and as $\xi = V_1(0) = 1 \neq \xi_0 = 2$ (see 1. of Lemma 2.6) and the multiplicity of $\beta^{-1} = 2$ in $1 - Y^{\mathrm{lcm}(\mathrm{ord}(\beta),\tau)} = 1 - Y^6 = (1-2Y)^3(1-Y^3)$ is 3, we find that $\mathrm{sig}_\phi(V_1) = (2,3,6)$. Further application of Theorem 3.6 produces the following evolution

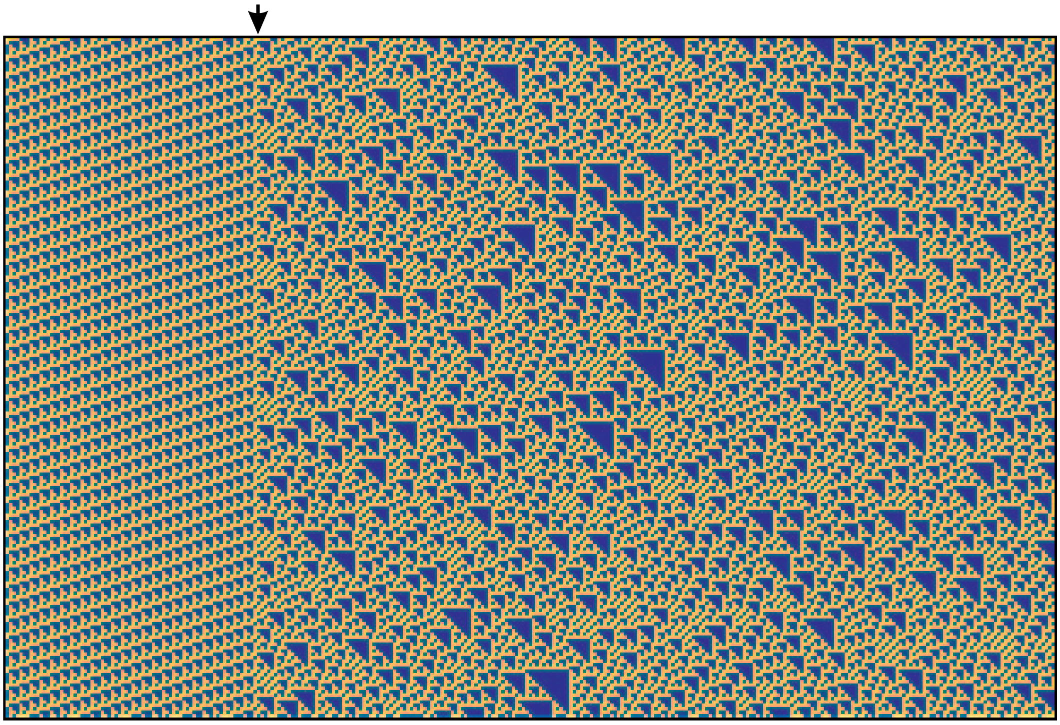

Fig. 2: Part of the ϕ-orbit of a cellular automaton with local rule $\phi(a,b) = a+b$ in $\mathbb{F}_2$ (310×200 pixels, evolution downwards, blue=0, yellow=1). The vertical V_0 indicated by the arrow is the periodic sequence $\overline{10110}$ with period 5. The period remains 5 for all verticals to the left of V_0. The initial configuration (top row) to the right of V_0 is a random sequence. When moving to the right, the period of the verticals starting at V_0 form the sequence 5,10,20,20,40,40,40,40, 80(8 times), 160(16 times), ... (doubling of period and bandwidth).

of sig_ϕ for $V_0, V_1, V_2, \ldots$:

$$(0,0,3)\ (2,3,6)\ (1,3,6)\ (0,3,6)\ (5,9,18)\ldots,$$

i.e., with $i_0 = 1$, we see that scenario 2 of Theorem 3.7 is followed.
For the evolution of the perid of $D_i, i \le 0$, we have to consider the rule $\phi'(a,b) = 2a+b$ corresponding to $\beta = \beta^{-1} = 1$. The periodic sequence D_0 is $P'(Y) = 1+2Y+2Y+Y^3 = (1-Y^2)(1+Y)$, hence the multiplicity of $\beta^{-1} = 1$ in $P'(Y)$ is 2, while it is 1 in $1-Y^4 = (1-Y)(1+Y+Y^2+Y^3)$. Thus $\text{sig}_{\phi'}(D_0) = (2,1,4)$. This gives, according to 4. in Theorem 3.6, as $\xi = D_{-1}(0) = 0$, that $\text{sig}_{\phi'}(D_{-1}) = (1,1,4)$. Then case 3. of Theorem 3.6 applies, with $\xi = D_{-2}(0) = 1 \neq \xi_0 = 2$, producing $\text{sig}_{\phi'}(D_2) = (0,1,4)$. This brings us in the case 2. of Theorem 3.6, and we finally get

$$(\text{sig}_{\phi'}(D_{-2}))_{i \le 0} = (2,1,4)\ (1,1,4)\ (0,1,4)\ (1,3,12)\ (0,3,12)\ (5,9,36)\ldots,$$

yielding the following evolution in the periods of the D_i to the left of D_0 starting from D_0:

$$4,4,4,12,12,36,36,36,36,108\ (12\text{ times}),\ldots.$$

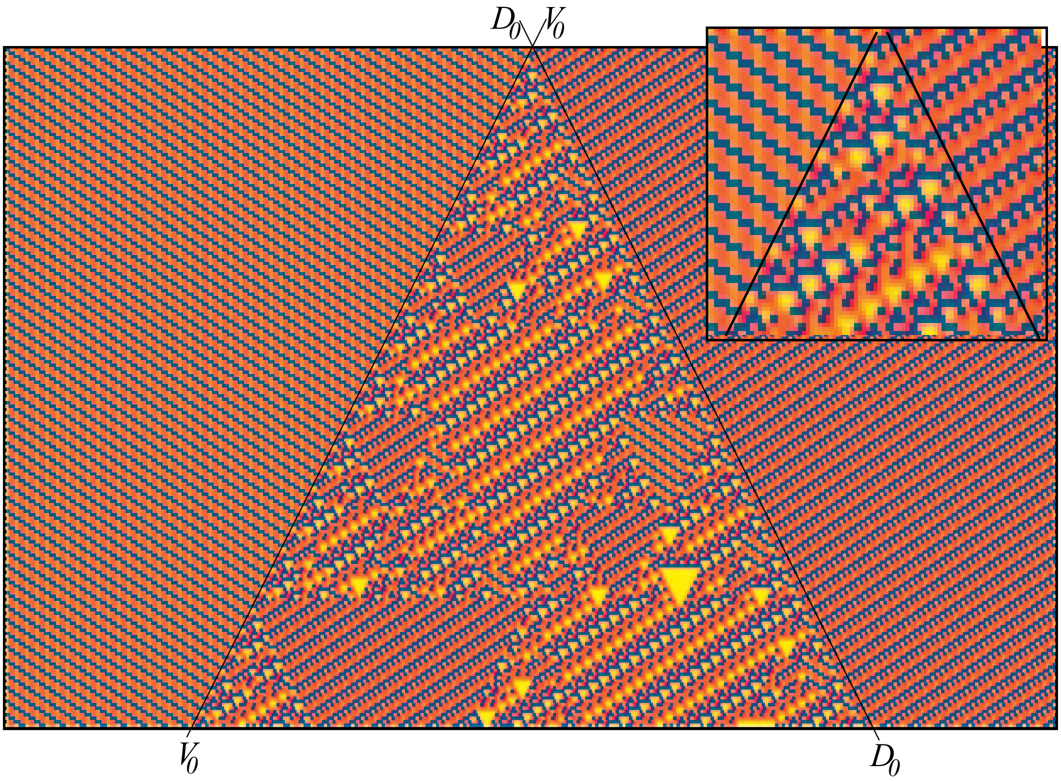

Fig. 3: Part of the ϕ-orbit of a cellular automaton with local rule $\phi(a,b) = a+2b$ in $\mathbb{F}_3$ in a symmetrized graphical representation (yellow=0, red=1, blue=3). The insert is an enlargement of the top of the triangular structure. The periodic sequence V_0 is $\overline{012}$, the periodic sequence D_0 is $\overline{1221}$. The periods of the $V_i, i \geq 0$ evolve according to the sequence 3,6,6,6,18,18,18,18,18,18, 54,... ; the periods of $D_i, i \leq 0$ evolve according to the sequence 4,4,4,12,12,36 (6 times), 108 (18 times),... (both sequences feature period and bandwidth triplings).

Hence, we see that scenario 1. of Theorem 3.7applies for $i_0 = -3$, i.e., $\pi_F(i) = 3^{n+1} \cdot 4$ for $-3-(3^n-1) \leq i \leq -3-(3^n+1-1)$.

Finally, we want to make some remarks about possible generalizations of the observed phenomena. It is obvious that some of the above results readily generalize to any finite ring $\mathcal{R}$ and a local rule $\phi : \mathcal{R}^2 \to \mathcal{R}$, with $\phi(a,b) = \alpha a + \beta b$ if α, β are units of the ring. Then Lemma 2.1, Theorem 2.2, and Corollaries 2.3, 2.4 remain true. More important, Theorem 3.1 also holds. Therefore, even in the situation of a finite ring, a ϕ-orbit has either a constant period distribution or an unbounded period distribution. However, the growth of the period distribution is not as simple as for the field case. E.g., If we consider the ring $\mathbb{Z}_6 = \mathbb{Z}/(6\mathbb{Z})$ with local rule $\phi_6(a,b) = a+b$, then the initial configuration $\underline{c} = (\ldots 0002000 \ldots)$ generates a ϕ_6-orbit F having the same period distribution as the ϕ_3-orbit generated by $(\ldots 0001000 \ldots) \in \mathbb{F}_3^{\mathbb{Z}}$ and local rule $\phi_3(a,b) = a+b$. On the other hand, the initial configuration $(\ldots 0003000 \ldots)$ generates a ϕ_6-orbit such that its period distribution is equal to the period distribution of the ϕ_2-orbit generated by $(\ldots 0001000 \ldots) \in \mathbb{F}_2^{\mathbb{Z}}$

and local rule $\phi_2(a,b) = a+b$. The initial configuration $(\ldots 0001000\ldots)$ generates a ϕ_6-orbit with period growth being a mixture of the 2-fold bifurcation and 3-fold bifurcation.

The assertions of the above mentioned results remain true even if the ring $\mathcal{R}$ is replaced by a finite set $\mathcal{G}$ and the local rule $\phi : \mathcal{G}^2 \to \mathcal{G}$ defines a quasigroup structure on $\mathcal{G}$, see [3] for quasigroups, and [2] for cellular automata and quasigroups.

Acknowledgements

This research was by the Concerted Action Project GOA-Mefisto of the Flemisch Community, FWO (Fund for Scientific Research Flanders) project G.0080.01, and by the Belgian Program on Interuniversity Attraction Poles of the Belgian Prime Minister's Office for Science Technology and Culture (IUAP P4-02). The second author thanks the DFG (Deutsche Forschungsgemeinschaft) for financial support.

References

[1] A. Barbé. Periodic patterns in the binary difference field, Complex Systems **2** (1988), 209–233.

[2] A. Barbé, F. von Haeseler. Cellular automata, quasigroups and symmetries, to appear in *Aequationes Mathematicae*.

[3] J. Dénes, A.D. Keedwell. Latin Squares and their Applications. Academic Press, New York, 1974.

[4] R. Lidl, H. Niederreiter. *Finite Fields*, Addison-Wesley, 1983.