On the Periods of Spatially Periodic Preimages in Linear Bipermutive Cellular Automata

Luca Mariot, Alberto Leporati

On the Periods of Spatially Periodic Preimages in Linear Bipermutive Cellular Automata

Luca Mariot and Alberto Leporati

Dipartimento di Informatica, Sistemistica e Comunicazione,
Università degli Studi Milano - Bicocca,
Viale Sarca 336/14, 20124 Milano, Italy
l.mariot@campus.unimib.it, alberto.leporati@unimib.it

Abstract. In this paper, we investigate the periods of preimages of spatially periodic configurations in linear bipermutive cellular automata (LBCA). We first show that when the CA is only bipermutive and y is a spatially periodic configuration of period p, the periods of all preimages of y are multiples of p. We then present a connection between preimages of spatially periodic configurations of LBCA and concatenated linear recurring sequences, finding a characteristic polynomial for the latter which depends on the local rule and on the configurations. We finally devise a procedure to compute the period of a single preimage of a spatially periodic configuration y of a given LBCA, and characterise the periods of all preimages of y when the corresponding characteristic polynomial is the product of two distinct irreducible polynomials.

Keywords: Linear bipermutive cellular automata, spatially periodic configurations, preimages, surjectivity, linear recurring sequences, linear feedback shift registers.

1 Introduction

It is known that if $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a surjective cellular automaton (CA) and $y \in A^{\mathbb{Z}}$ is a spatially periodic configuration, then all preimages $x \in F^{-1}(y)$ are spatially periodic as well [2]. However, to our knowledge there are no works in the literature addressing the problem of actually finding the periods of such preimages.

The aim of this paper is to study the relation between the periods of spatially periodic configurations and the periods of their preimages in the case of *linear bipermutive cellular automata* (LBCA). Given a spatially periodic configuration $y \in A^{\mathbb{Z}}$ of period p, we first prove that in generic bipermutive cellular automata (BCA) the period of a preimage $x \in F^{-1}(y)$ is a multiple of p, where the multiplier h ranges in $\{1, \cdots, q^{2r}\}$, with q being the size of the alphabet and r the radius of the BCA. We then show that, in the case of LBCA, a preimage $x \in F^{-1}(y)$ can be described as a *concatenated linear recurring sequence* (LRS) whose characteristic polynomial is the product of the characteristic polynomials respectively induced by the local rule f of the CA and by configuration y. Finally, we present a procedure which given a block $x_{[0,2r-1]}$ of a preimage $x \in F^{-1}(y)$ determines the period of x, and we characterise the periods of all q^{2r} preimages of y when their characteristic polynomial is the product of two irreducible polynomials.

This research was inspired from the problem of determining the maximum number of players allowed in a BCA-based secret sharing scheme presented in [10].

The rest of this paper is organised as follows. Section 2 recalls some basic definitions and facts about cellular automata, linear recurring sequences and linear feedback shift registers. Section 3 shows that the periods of spatially periodic preimages are multiples of the periods of their respective images, and characterises preimages of LBCA as concatenated linear recurring sequences. Section 4 focuses on the characteristic polynomial of concatenated LRS, while Section 5 presents an algorithm to compute the period of a single LBCA preimage and characterises the periods of all preimages of a spatially periodic configuration y in the particular case of irreducible characteristic polynomials. Finally, Section 6 summarises the results presented throughout the paper and points out some possible future developments on the subject.

2 Basic Definitions

2.1 Cellular Automata

Let A be a finite alphabet having q symbols, and let $A^{\mathbb{Z}}$ be the *full shift space* consisting of all biinfinite configurations over A. Given $x \in A^{\mathbb{Z}}$ and $i, j \in \mathbb{Z}$ with $i \leq j$, by $x_{[i,j]}$ we denote the finite block $(x_i, \cdots, x_j)$. In what follows, we focus our attention on *one-dimensional cellular automata*, formally defined below:

Definition 1. *A* one-dimensional cellular automaton *is a function $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ defined for all $x \in A^{\mathbb{Z}}$ and $i \in \mathbb{Z}$ as:*

$$F(x)_i = f(x_{[i-r,i+r]}) \ ,$$

where $f : A^{2r+1} \to A$ is the local rule *of the CA and $r \in \mathbb{N}$ is its* radius.

From a dynamical point of view, a CA can be considered as a biinfinite array of *cells* where, at each time step $t \in \mathbb{N}$, all cells $i \in \mathbb{Z}$ simultaneously change their *state* $s_i \in A$ by applying the local rule f on the *neighbourhood* $\{i-r, \cdots, i+r\}$.

The main class of CA studied in this paper consists of *bipermutive* CA, defined as follows:

Definition 2. *A CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ induced by a local rule $f : A^{2r+1} \to A$ is called* left permutive *(respectively,* right permutive*) if, for all $z \in A^{2r}$, the restriction $f_{R,z} : A \to A$ (respectively, $f_{L,z} : A \to A$) obtained by fixing the first (respectively, the last) $2r$ coordinates of f to the values specified in z is a permutation on A. A CA which is both left and right permutive is said to be a* bipermutive cellular automaton *(BCA).*

Another class of CA which can be defined by endowing the alphabet with a group structure is that of *linear* (or *additive*) cellular automata. We give the definition for the particular case in which A is a finite field. Thus, we have $A = \mathbb{F}_q$ with $q = \rho^\alpha$, where $\rho \in \mathbb{N}$ is a prime number (called the *characteristic* of $\mathbb{F}_q$) and $\alpha \in \mathbb{N}$.

Definition 3. *A CA $F : \mathbb{F}_q^{\mathbb{Z}} \to \mathbb{F}_q^{\mathbb{Z}}$ with local rule $f : \mathbb{F}_q^{2r+1} \to \mathbb{F}_q$ is* linear *if there exists $(c_0, \cdots, c_{2r}) \in \mathbb{F}_q^{2r+1}$ such that f can be defined for all $(x_0, \cdots, x_{2r}) \in \mathbb{F}_q^{2r+1}$ as:*

$$f(x_0, \cdots, x_{2r}) = c_0 \cdot x_0 + \cdots + c_{2r} \cdot x_{2r} \ ,$$

where $+$ and $\cdot$ respectively denote sum and product over $\mathbb{F}_q$.

One easily checks that if both c_0 and c_{2r} in Definition 3 are nonzero then a linear CA is bipermutive as well. Most of the results proved in this paper concern cellular automata which are both linear and bipermutive.

A configuration $x \in A^{\mathbb{Z}}$ is called *spatially periodic* if there exists $p \in \mathbb{N}$ such that $x_{n+p} = x_n$ for all $n \in \mathbb{Z}$, and the least p for which this equation holds is called the *period* of x. In this case, x is generated by the *biinfinite concatenation* of a string $u \in A^p$ with itself, denoted by ${}^{\omega}u^{\omega}$. A proof of the following result about preimages of spatially periodic configurations in surjective CA can be found in [2].

Lemma 1. *Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a surjective CA. Then, given a spatially periodic configuration $y \in A^{\mathbb{Z}}$, each preimage $x \in F^{-1}(y)$ is also spatially periodic.*

This lemma is a consequence of a theorem proved by Hedlund [7], which states that every configuration $x \in A^{\mathbb{Z}}$ has a finite number of preimages under a surjective CA. In the same work, Hedlund showed that bipermutive CA are also surjective. Indeed, given a BCA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ induced by a local rule $f : A^{2r+1} \to A$ and a configuration $y \in A^{\mathbb{Z}}$, a preimage $x \in F^{-1}(y)$ is determined by first setting in x a block of $2r$ cells $x_{[i,i+2r-1]} \in A^{2r}$, with $i \in \mathbb{Z}$. Then, denoting by $f^{-1}_{R,z} : A \to A$ and $f^{-1}_{L,z} : A \to A$ the inverses of the permutations obtained by respectively fixing the first and the last $2r$ coordinates of f to $z \in \mathbb{A}^{2r}$, for all $n \geq i + 2r$ and $n < i$ the value of x_n is determined through the following recurrence equation:

$$x_n = \begin{cases} f^{-1}_{R,z(n)}(y_{n-r}), \text{ where } z(n) = x_{[n-2r,n-1]}, & \text{if } n \geq i + 2r \quad \text{(a)} \\ f^{-1}_{L,z(n)}(y_{n+r}), \text{ where } z(n) = x_{[n+1,n+2r]}, & \text{if } n < i \quad \text{(b)} \end{cases} \tag{1}$$

As a consequence, by Lemma 1 the preimages of spatially periodic configurations under a BCA are spatially periodic as well. Moreover, since a preimage of y is uniquely determined by a $2r$-cell block using Equation (1), it follows that y has exactly q^{2r} possible preimages in $F^{-1}(y)$.

We now formally state the problem analysed in the remainder of this paper:

Problem. Let $y \in A^{\mathbb{Z}}$ be a spatially periodic configuration of period $p \in \mathbb{N}$. Given a BCA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$, find the relation between p and the spatial periods of the preimages $x \in F^{-1}(y)$.

2.2 Linear Recurring Sequences and Linear Feedback Shift Registers

We now recall some basic definitions and results about the theory of linear recurring sequences and linear feedback shift registers, which will be useful to characterise the periods of preimages in LBCA. All the proofs of the theorems mentioned in this section may be found in the book by Lidl and Niederreiter [9].

Definition 4. *Given $k \in \mathbb{N}$ and $a, a_0, a_1, \cdots, a_{k-1} \in \mathbb{F}_q$, a* linear recurring sequence *(LRS) of order k is a sequence $s = s_0, s_1, \cdots$ of elements in $\mathbb{F}_q$ which satisfies the following relation:*

$$s_{n+k} = a + a_0 s_n + a_1 s_{n+1} + \cdots + a_{k-1} s_{n+k-1} \quad \forall n \in \mathbb{N} \ . \tag{2}$$

The terms $s_0, s_1, \cdots, s_{k-1}$ which uniquely determine the rest of the LRS are called the *initial values* of the sequence. If $a = 0$ the sequence is called *homogeneous*, otherwise it is called *inhomogeneous*. In what follows, we will only deal with homogeneous LRS.

A linear recurring sequence can be generated by a device called *linear feedback shift register* (LFSR), depicted in Figure 1. Basically, a LFSR of order k is composed of

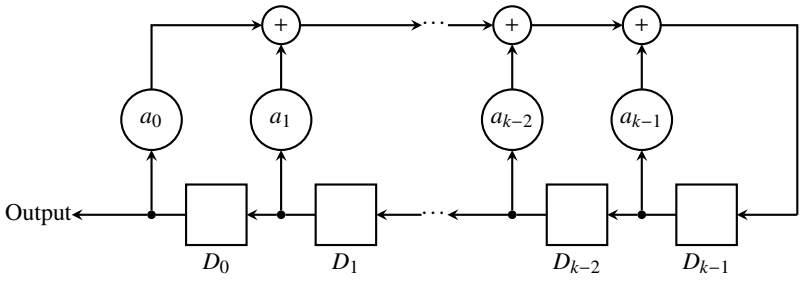

Fig. 1: Diagram of a linear feedback shift register of length k.

k delayed flip-flops $D_0, D_1, \cdots, D_{k-1}$, each containing an element of $\mathbb{F}_q$. At each time step $n \in \mathbb{N}$, the elements $s_n, s_{n+1}, \cdots, s_{n+k-1}$ in the flip-flops are shifted one place to the left, and D_{k-1} is updated by the linear combination $a_0 \cdot s_n + \cdots + a_{k-1} \cdot s_{n+k-1}$, which corresponds to the linear recurrence defined in Equation (2).

It is straightforward to observe that the output produced by the LFSR (that is, the LRS $s = s_0, s_1, \cdots$) must be *ultimately periodic*, that is, there exist $p, n_0 \in \mathbb{N}$ such that for all $n \geq n_0$, $s_{n+p} = s_n$. In fact, for all $n \in \mathbb{N}$ the state of the LFSR is completely described by the vector $(s_n, s_{n+1}, \cdots, s_{n+k-1})$. Since all the components of such vector take values in $\mathbb{F}_q$, which is a finite set of q elements, after at most q^k shifts the initial value of the vector will be repeated. In particular, in [9] it is proved that if $a_0 \neq 0$, then the sequence produced by the LFSR (or, equivalently, the corresponding LRS) is *periodic*, i.e., it is ultimately periodic with preperiod $n_0 = 0$.

An important parameter of a k-th order homogeneous LRS $s = s_0, s_1, \cdots$ is its *characteristic polynomial* $a(x) \in \mathbb{F}_q[x]$, defined as:

$$a(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_0 \quad . \tag{3}$$

The *multiplicative order* of the characteristic polynomial, denoted by $ord(a(x))$, is the least integer e such that $a(x)$ divides $x^e - 1$, and it can be used to characterise the period of s. In fact, in [9] it is shown that if $a(x)$ is irreducible over $\mathbb{F}_q$ and $a(0) \neq 0$, then the period p of s equals $ord(a(x))$, while in the general case where $a(x)$ is reducible $ord(a(x))$ divides p.

A common way of representing a LRS $s = s_0, s_1, \cdots$ is by means of its *generating function* $G(x)$, which is the formal power series defined as:

$$G(x) = s_0 + s_1 x + s_2 x^2 + \cdots = \sum_{n=0}^{\infty} s_n x^n \tag{4}$$

In this case, the terms $s_0, s_1, \cdots$ are called the *coefficients* of $G(x)$. The set of all generating functions over $\mathbb{F}_q$ can be endowed with a ring structure in which sum and product are respectively pointwise addition and convolution of coefficients. The *fundamental identity of formal power series* states that the generating function $G(x)$ of a k-th order homogeneous LRS s can be expressed as a rational function:

$$G(x) = \frac{g(x)}{a^*(x)} = \frac{-\sum_{j=0}^{k-1}\sum_{i=0}^{j} a_{i+k-j} s_i x^j}{x^k a(1/x)} \quad . \tag{5}$$

where $g(x)$ is the *initialisation polynomial*, which depends on the k initial terms of sequence s (in which we set $a_k = -1$), while $a^*(x) = x^k a(1/x)$ is the *reciprocal characteristic polynomial* of s.

It is easy to see that a given LRS $s = s_0, s_1, \cdots$ over $\mathbb{F}_q$ satisfies several linear recurrence equations. Hence, several characteristic polynomials can be associated to s, one for each recurrence equation which s satisfies. The *minimal polynomial* $m(x)$ associated to s is the characteristic polynomial which divides all other characteristic polynomials of s, and it can be computed as follows:

$$m(x) = \frac{a(x)}{\gcd(a(x), h(x))} \quad , \tag{6}$$

where $a(x)$ is a characteristic polynomial of s and $h(x) = -g^*(x)$ is the reciprocal of the initialisation polynomial $g(x)$ appearing in Equation (5), with the sign changed. In [9] it is proved that the period of s equals the order of its minimal polynomial $m(x)$.

In order to study the periods of preimages of LBCA, we also need some results about the sum of linear recurring sequences. Let $s = s_0, s_1, \cdots$ and $t = t_0, t_1, \cdots$ be homogeneous LRS over $\mathbb{F}_q$. The *sum sequence* $\sigma = s + t$ is defined as $\sigma_n = s_n + t_n$, for all $n \in \mathbb{N}$.

Theorem 1. *Let σ_1 and σ_2 be two homogeneous LRS having minimal polynomials $m_1(x), m_2(x) \in \mathbb{F}_q[x]$ and periods $p_1, p_2 \in \mathbb{N}$, respectively. If $m_1(x)$ and $m_2(x)$ are relatively prime, then the minimal polynomial $m(x) \in \mathbb{F}_q[x]$ of the sum $\sigma = s + t$ is equal to $m_1(x) \cdot m_2(x)$, while the period of σ is the least common multiple of p_1 and p_2.*

The following theorem gives a characterisation of the periods of LRS associated to an irreducible characteristic polynomial.

Theorem 2. *Let $S(a(x))$ be the set of all homogeneous linear recurring sequences over $\mathbb{F}_q$ with irreducible characteristic polynomial $a(x) \in \mathbb{F}_q[x]$, and let e be the multiplicative order of $a(x)$. Then, $S(a(x))$ contains one sequence of period 1 and $q^k - 1$ sequences of period e.*

3 Preliminary Results

3.1 Preimages Periods in Generic BCA

We begin our analysis of Problem 2.1 by considering the general case where only bipermutivity holds. To this end, we first show a relation between finite blocks in the preimages of BCA.

Lemma 2. *Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a BCA with local rule $f : A^{2r+1} \to A$. Then, given a configuration $y \in A^{\mathbb{Z}}$ and $i, j \in \mathbb{Z}$, for all $x \in F^{-1}(y)$ there exists a permutation between the blocks $x_{[i,i+2r-1]}$ and $x_{[j,j+2r-1]}$.*

Proof. Without loss of generality, let us assume $i < j$. Since y is fixed and F is bipermutive, for all $x_{[i,i+2r-1]} \in A^{2r}$ define $\varphi_y : A^{2r} \to A^{2r}$ as $\varphi_y(x_{[i,i+2r-1]}) = x_{[j,j+2r-1]}$, where for each $n \in \{j, \cdots, j+2r-1\}$ the value of x_n is computed by applying case (a) of Equation (1)*. We have to show that φ_y is a permutation on A^{2r} (Figure 2).*

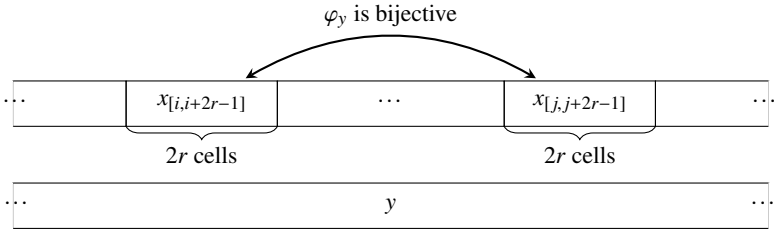

Fig. 2: By fixing y, function φ_y is a A^{2r}-permutation.

For all possible values of block $x_{[j,j+2r-1]}$, the value of $x_{[i,i+2r-1]}$ is uniquely determined by applying case (b) of Equation (1)*. As a consequence, under φ_y each image has a unique preimage, and thus φ_y is bijective.* □

Using Lemma 2, the following useful information about the periods of spatially periodic preimages in BCA can be deduced:

Proposition 1. *Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a BCA with local rule $f : A^{2r+1} \to A$ and let $y \in A^{\mathbb{Z}}$ be a spatially periodic configuration of period $p \in \mathbb{N}$. Given a preimage $x \in F^{-1}(y)$, the period $m \in \mathbb{N}$ of x is a multiple of p. In particular, it holds that $m = p \cdot h$, where $h \in \{1, \cdots, q^{2r}\}$.*

Proof. Since y is spatially periodic of period p, we have that $y = {}^{\omega}u^{\omega}$ for a certain $u \in A^p$. Given a preimage $x \in F^{-1}(y)$, denote by $w_1 \in A^{2r}$ the block $x_{[i-r,i+r-1]}$, where $i \in \mathbb{Z}$ is such that $y_i = y_{i+p} = u_1$. In other words, w_1 is a $2r$-cell block of x placed across the boundary between two copies of u in y (see Figure 3). By Lemma 2 we know that block u fixes a permutation $\varphi_u : A^{2r} \to A^{2r}$ which maps block w_1 to $w_2 = x_{[i+p-r,i+p+r-1]}$. More in general, observe that for all $j \geq 2$ the permutation which associates block $w_j = x_{[i+pj-r,i+pj+r-1]}$ to $w_{j+1} = x_{[i+p(j+1)-r,i+p(j+1)+r-1]}$ is always φ_u, the reason being that the block below w_j and w_{j+1} is a repetition of u. Since $|A| = q$, the permutation φ_u can be composed by at most one cycle of length q^{2r}. This means that, after at most $h \leq q^{2r}$ applications of φ_u, block $w_h = x_{[i+ph-r,i+ph+r-1]}$ will be equal to w_1, and from then on the preimage will periodically repeat itself. Thus, it results that $x_n = x_{n+ph}$ for all $n \in \mathbb{Z}$, from which we deduce that the period of x is $p \cdot h$. □

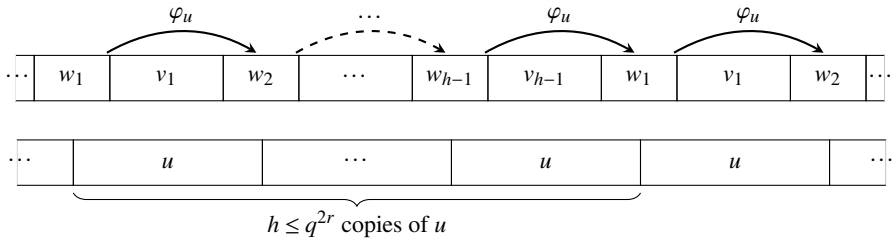

Fig. 3: After at most $h \leq q^{2r}$ applications of φ_u, the $2r$-cell block w_1 will be repeated. At this point, the subsequent p-cell block in the preimage will be a copy of $v_1 w_2$.

3.2 Characterising LBCA Preimages By LRS Concatenation

Proposition 1 limits the possible values of the periods attained by preimages of spatially periodic configurations in BCA. In what follows we show that, by narrowing the analysis to the class of LBCA, further information about the periods of preimages can be obtained.

Let $F : \mathbb{F}_q^{\mathbb{Z}} \to \mathbb{F}_q^{\mathbb{Z}}$ be a LBCA of radius r with local rule $f : \mathbb{F}_q^{2r+1} \to \mathbb{F}_q$ defined by a vector $(c_0, \cdots, c_{2r}) \in \mathbb{F}_q^{2r+1}$, where $c_0 \neq 0$ and $c_{2r} \neq 0$. Given $x \in \mathbb{F}_q^{2r+1}$ and $y = f(x)$, the following equalities hold:

$$\begin{aligned} y &= c_0 x_0 + c_1 x_1 + \cdots + c_{2r-1} x_{2r-1} + c_{2r} x_{2r} \\ x_{2r} &= c_{2r}^{-1}(-c_0 x_0 - c_1 x_1 - \cdots - c_{2r-1} x_{2r-1} + y) \ . \end{aligned}$$

Setting $d = c_{2r}^{-1}$ and $a_i = -d \cdot c_i$ for all $i \in \{0, \cdots, 2r-1\}$, we obtain

$$x_{2r} = a_0 x_0 + a_1 x_1 + \cdots + a_{2r-1} x_{2r-1} + dy \ . \tag{7}$$

Equation (7) defines the inverse $f_{R,z}^{-1}$ of the permutation $f_{R,z} : \mathbb{F}_q \to \mathbb{F}_q$ obtained by fixing the first $2r$ coordinates of f to the values of $z = (x_0, \cdots, x_{2r-1})$. Hence, given a configuration $y \in \mathbb{F}_q^{\mathbb{Z}}$ and the $2r$-cell block $x_{[0,2r-1]} \in \mathbb{F}_q^{2r}$ in a preimage $x \in F^{-1}(y)$, case (a) of Equation (1) yields

$$x_n = a_0 x_{n-2r} + a_1 x_{n-2r+1} + \cdots + a_{2r-1} x_{n-1} + dy_{n-r} \quad \forall n \geq 2r \ , \tag{8}$$

and by setting $k = 2r$ and $v_n = y_{n+r}$ for all $n \in \mathbb{N}$, Equation (8) can be rewritten as

$$x_{n+k} = a_0 x_n + a_1 x_{n+1} + \cdots + a_{k-1} x_{n+k-1} + dv_n \quad \forall n \geq 2r \ . \tag{9}$$

Equation (9) reminds the definition of a linear recurring sequence of order $k = 2r$, with the exception of term dv_n. However, if y is a spatially periodic configuration of period p then it is possible to describe the sequence $v = v_0, v_1, \cdots$ as a linear recurring sequence of order $l \leq p$ defined by

$$v_{n+l} = b_0 v_n + b_1 v_{n+1} + \cdots + b_{l-1} v_{n+l-1} \ , \tag{10}$$

where $b_i \in \mathbb{F}_q$ for all $i \in \{0, \cdots, l-1\}$, and the initial terms of the sequence are $v_0 = y_r$, $v_1 = y_{r+1}$, $\cdots$, $v_{l-1} = y_{r+l-1}$. In the worst case, the LRS v will have order $l = p$, and it will be generated by the trivial LFSR which cyclically shifts a word of length p.

As a consequence, preimage $x \in F^{-1}(y)$ is a linear recurring sequence of a special kind, where x_{n+k} is determined not only by the previous $k = 2r$ terms, but it is also "disturbed" by the LRS v. In particular, we define x as the *concatenation* of sequences s and v, which we denote by $s \leftsquigarrow v$, where $s = s_0, s_1, \cdots$ is the k-th order LRS satisfying the recurrence equation

$$s_{n+k} = a_0 s_n + a_1 s_{n+1} + \cdots + a_{k-1} s_{n+k-1} \quad , \tag{11}$$

and whose initial values are $s_0 = x_0$, $s_1 = x_1$, $\cdots$, $s_{k-1} = x_{k-1}$.

Equivalently, a preimage $x \in F^{-1}(y)$ is generated by a LFSR of order $k = 2r$ where the feedback is summed with the output of an l-th order LFSR multiplied by $d = c_{2r}^{-1}$, which produces sequence v. Similarly to concatenated LRS, we call this system a *concatenation* of LFSR. Figure 4 depicts the block diagram of this concatenation.

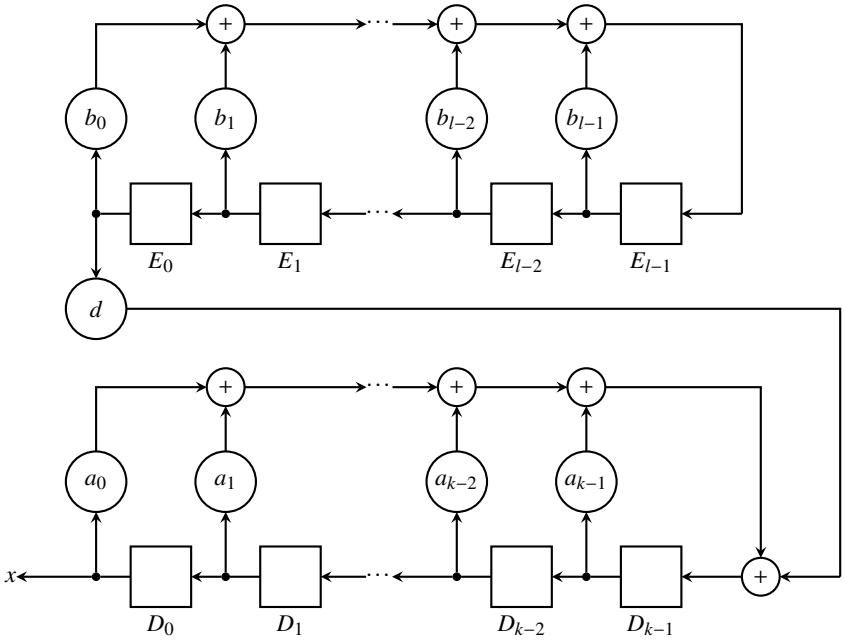

Fig. 4: Diagram of two concatenated LFSR.

In conclusion, we have shown that the periods of the preimages $x \in F^{-1}(y)$ are equivalent to the periods of the concatenated LRS generated by the LFSR in Figure 4, where the disturbing LFSR is initialised with the values y_r, $\cdots$, y_{r+l-1}. In particular, since multiplying the terms of a LRS by a constant does not change its period, in what follows we will assume $d = 1$.

4 Analysis of Concatenated LRS

4.1 Sum Decomposition of Concatenated LRS

In order to study the period of the concatenated linear recurring sequence $s \leftsquigarrow v$ giving rise to preimage $x \in F^{-1}(y)$, we first prove that it can be decomposed into the *sum* of two LRS: namely, sequence s and the 0-*concatenation* $u = s \leftsquigarrow_0 v$ satisfying the same recurrence Equation (9) of x, but whose k initial terms $u_0, \cdots, u_{k-1}$ are set to 0.

Theorem 3. *Let $s = s_0, s_1, \cdots$ and $v = v_0, v_1, \cdots$ be the LRS respectively satisfying Equations* (11) *and* (10)*, whose initial terms are respectively $s_0 = x_0, \cdots, s_{k-1} = x_{k-1}$ and $v_0 = y_r, \cdots, v_{l-1} = y_{r+l-1}$, and let $x = s \leftsquigarrow v$ be the concatenation of s and v defined by Equation* (9)*, where $d = 1$. Additionally, let $u = s \leftsquigarrow_0 v$ be the* 0*-concatenation of sequences s and v, where $u_0 = u_1 = \cdots = u_{k-1} = 0$. Then, $x_n = s_n + u_n$ for all $n \in \mathbb{N}$.*

Proof. Since $u_0 = u_1 = \cdots = u_{k-1} = 0$, for all $n \in \{0, \cdots, k-1\}$ it holds

$$s_n + u_n = s_n + 0 = x_n \quad .$$

Therefore, it remains to prove $x_n = s_n + u_n$ for all $n \geq k$. We proceed by induction on n. For $n = k$, we have

$$\begin{aligned} s_k + u_k &= a_0 s_0 + \cdots + a_{k-1} s_{k-1} + a_0 u_0 + \cdots + a_{k-1} u_{k-1} + v_0 = \\ &= a_0 x_0 + \cdots + a_{k-1} x_{k-1} + v_0 = x_k \quad . \end{aligned}$$

For the induction step we assume $s_n + u_n = x_n$ for $n \leq k$. The sum $s_{n+1} + u_{n+1}$ is equal to:

$$\begin{aligned} s_{n+1} + u_{n+1} &= a_0 s_{n-k+1} + \cdots + a_{k-1} s_n + a_0 u_{n-k+1} + \cdots + a_{k-1} u_n + v_{n-k+1} = \\ &= a_0 (s_{n-k+1} + u_{n-k+1}) + \cdots + a_{k-1} (s_n + u_n) + v_{n-k+1} \quad . \end{aligned} \tag{12}$$

By induction hypothesis, $s_{n-k+i} + u_{n-k+i} = x_{n-k+i}$ for all $i \in \{1, \cdots, k\}$. Hence, Equation (12) *can be rewritten as*

$$s_{n+1} + u_{n+1} = a_0 x_{n-k+1} + \cdots + a_{k-1} x_n + v_{n-k+1} = x_{n+1} \quad .$$

□

4.2 Characteristic Polynomial of Concatenated LRS

Theorem 3 tells us that a preimage $x \in F^{-1}(y)$ can be generated by the sum of two LRS: the LRS generated by the concatenated LFSR of Figure 4, where the disturbed LFSR is initialised to zero, and the LRS produced by the *non-disturbed* LFSR, that is, the lower LFSR in Figure 4 without the external feedback, initialised to the values $x_0, \cdots, x_{k-1}$.

We now show that this sum decomposition allows one to determine a characteristic polynomial of the concatenated sequence $x = s \leftsquigarrow v$. To this end, we first need a result proved by Chassé in [3] which concerns the generating function of the 0-concatenation $u = s \leftsquigarrow_0 v$. The proof stands on the observation that for all $n \in \mathbb{N}$, the n-th term of u is given by the linear combination $\sum_{i=0}^{n-1} A_n^{(i)} \cdot v_i$, where the terms $A_n^{(i)}$ depend only on the

coefficients a_j which define Equation (11). In particular, we will need the values of $A_n^{(0)}$ for $n \geq 0$, which can be computed by the following recurrence equation:

$$A_n^{(0)} = \begin{cases} \sum_{j=0}^{k-1} a_j A_{n-k+j}^{(0)} \ , \text{ if } \ n > 1 \\ 1 \ , \text{ if } \ n = 1 \\ 0 \ , \text{ if } \ n = 0 \end{cases} \tag{13}$$

where $k = 2r$ and $A_{n-k+j}^{(0)} = 0$ if $n - k + j < 0$. Using our notation and terminology, Chassé's result can thus be stated as follows:

Proposition 2. *Let $u = s \leftsquigarrow_0 v$ be the 0-concatenation of the LRS s and v defined in Theorem 3, and let $V(x)$ be the generating function of v. Denoting by $\mathcal{A}(x)$ the generating function of the sequence $A = \{A_{n+1}^{(0)}\}_{n\in\mathbb{N}}$, the generating function of u is*

$$U(x) = x \cdot \mathcal{A}(x) \cdot V(x) \ . \tag{14}$$

Moreover, if $a(x) \in \mathbb{F}_q[x]$ is the characteristic polynomial of the sequence s associated to the recurrence equation (11)*, then $a(x)$ is also a characteristic polynomial of A.*

We now prove that the characteristic polynomial of the concatenation $s \leftsquigarrow v$ is the product of the characteristic polynomials of s and v.

Theorem 4. *Let $s \leftsquigarrow v$ be the concatenation of LRS s and v defined by Equation* (9) *with $d = 1$, and let $a(x), b(x) \in \mathbb{F}_q[x]$ be the characteristic polynomials of s and v, respectively associated to the linear recurring equations* (11) *and* (10)*. Then, $a(x) \cdot b(x)$ is a characteristic polynomial of $s \leftsquigarrow v$.*

Proof. By Theorem 3 the concatenation of LRS s and v can be written as $s \leftsquigarrow v = s + u$, where $u = s \leftsquigarrow_0 v$ is the 0-concatenation associated to $s \leftsquigarrow v$. By applying the fundamental identity of formal power series (Equation (5)*) and Proposition 2, the following equalities hold:*

$$S(x) = \frac{g_s(x)}{a^*(x)} \tag{15}$$

$$U(x) = \frac{x \cdot g_A(x) \cdot g_v(x)}{a^*(x) \cdot b^*(x)} \ , \tag{16}$$

where $g_s(x)$, $g_A(x)$ and $g_v(x)$ are polynomials whose coefficients are computed according to the numerator in the RHS of Equation (5)*. Hence, the generating function of $s \leftsquigarrow v$ is:*

$$G(x) = \frac{g_s(x)}{a^*(x)} + \frac{x \cdot g_A(x) \cdot g_v(x)}{a^*(x) \cdot b^*(x)} = \frac{g_s(x) \cdot b^*(x) + x \cdot g_A(x) \cdot g_v(x)}{a^*(x) \cdot b^*(x)} \ . \tag{17}$$

By applying again the fundamental identity of formal power series to Equation (17)*, we deduce that the reciprocal of $c(x) = a^*(x) \cdot b^*(x)$ is a characteristic polynomial of $s \leftsquigarrow v$. Denoting by k and l the degrees of $a(x)$ and $b(x)$ respectively, it follows that $c(x) = x^{k+l} \cdot a(1/x) \cdot b(1/x)$, and thus the reciprocal of $c(x)$ is*

$$c^*(x) = x^{k+l} \cdot \frac{1}{x^{k+l}} \cdot a(x) \cdot b(x) = a(x) \cdot b(x) \ . \tag{18}$$

Therefore, $a(x) \cdot b(x)$ is a characteristic polynomial of $s \leftsquigarrow v$. □

Theorem (4) thus gives a characteristic polynomial for all preimages $x \in F^{-1}(y)$ of a spatially periodic configuration $y \in \mathbb{F}_q^{\mathbb{Z}}$. As a matter of fact, the polynomials $a(x)$ and $b(x)$ do not depend on the particular value of the block $x_{[0,2r-1]}$, but only on the local rule f and on configuration y, respectively. From the LFSR point of view, this means that a preimage $x \in F^{-1}(y)$ can be generated by a single LFSR implementing the $(k+l)$-th order recurrence equation

$$\sigma_{n+k+l} = c_0\sigma_n + c_1\sigma_{n+1} + \cdots + c_{k+l-1}\sigma_{n+k+l-1} \ , \tag{19}$$

where for all $\mu \in \{0, \cdots, k+l-1\}$ the term c_μ is the μ-th convolution coefficient in the multiplication $a(x) \cdot b(x)$ given by

$$c_\mu = \sum_{i+j=\mu} a_i b_j, \text{ for } i \in \{0, \cdots, k\} \text{ and } j \in \{0, \cdots, l\} \ . \tag{20}$$

Additionally, the first $k = 2r$ initial terms $\sigma_0, \cdots, \sigma_{k-1}$ in Equation (19) are initialised to the values in $x_{[0,2r-1]}$, while the remaining l ones are obtained using the recurrence equation (9). Hence, by applying the fundamental identity of formal power series, the numerator of Equation (17) can also be expressed as:

$$g(x) = -\sum_{j=0}^{k-1} \sum_{i=0}^{j} c_{i+k-j}\sigma_i x^j \ . \tag{21}$$

5 Further Results

5.1 Computing the Period of a Single Preimage

To summarise the results discussed so far, we now present a practical procedure to compute the spatial period of a single preimage. Given a LBCA $F : \mathbb{F}_q^{\mathbb{Z}} \to \mathbb{F}_q^{\mathbb{Z}}$ with local rule $f : \mathbb{F}_q^{2r+1} \to \mathbb{F}_q$ of radius $r \in \mathbb{N}$, a spatially periodic configuration $y \in \mathbb{F}_q^{\mathbb{Z}}$ and a $2r-$cell block $x_{[0,2r-1]} \in \mathbb{F}_q^{2r}$ of a preimage $x \in F^{-1}(y)$, the procedure can be described as follows:

1. Find the minimal polynomial $b(x) = x^l - b_{l-1}x^{l-1} \cdots - b_0$ of the linear recurring sequence v, where $v_n = y_{n+r}$ for all $n \in \mathbb{N}$.
2. Set the characteristic polynomial $a(x)$ associated to the inverse permutation $f_{R,z}^{-1}$ to $a(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_0$, where $k = 2r$ and the coefficients a_i are those appearing in the recurrence equation (11).
3. Compute the polynomial $g(x)$ given by Equation (21), and set $h(x) = -g^*(x)$.
4. Determine the minimal polynomial of the preimage by computing

$$m(x) = \frac{a(x) \cdot b(x)}{gcd(a(x) \cdot b(x), h(x))} \ . \tag{22}$$

5. Compute the order of $m(x)$, and output it as the period of preimage x.

For step 1, the minimal polynomial of v can be found using the *Berlekamp-Massey algorithm* [11], by giving as input to it the string composed by the first $2p$ elements of v, where p is the period of y (and hence the period of v as well). The time complexity of this algorithm is $O(p^2)$. Step 4 requires the computation of a greatest common divisor, which can be performed using the standard Euclidean division algorithm in $O(n^2)$ steps, where $n = max\{deg(a(x)b(x)), deg(h(x))\}$. Finally, the order of $m(x)$ in step 5 can be determined by first factorizing the polynomial, for example by using *Berlekamp's algorithm* [1] which has a time complexity of $O(D^3)$, where D is the degree of $m(x)$, if the characteristic ρ of $\mathbb{F}_q$ is sufficiently small. Once the factorization of $m(x)$ is known, $ord(m(x))$ can be computed using the following theorem proved in [9]:

Theorem 5. *Let $m(x) \in \mathbb{F}_q[x]$ be a polynomial having positive degree and such that $m(0) \neq 0$. Let $m(x) = a \cdot \prod_{i=0}^{n} f_i(x)^{b_i}$ be the canonical factorization of $m(x)$, where $a \in \mathbb{F}_q$, $b_1, \cdots, b_n \in \mathbb{N}$ and $f_1(x), \cdots, f_n(x) \in \mathbb{F}_q[x]$ are distinct monic irreducible polynomials. Then $ord(m(x)) = e\rho^t$, where ρ is the characteristic of $\mathbb{F}_q$, e is the least common multiple of $ord(f_1(x)), \cdots, ord(f_n(x))$ and t is the smallest integer such that $\rho^t \geq \max(b_1, \cdots, b_n)$.*

Notice that Theorem 5 depends on the knowledge of the orders of the irreducible polynomials involved in the factorization of $m(x)$. A method to determine the order of an irreducible polynomial is also described in [9], which relies on the factorization of $q^D - 1$. There exist several factorization tables for numbers in this form, especially for small values of q (see for example [4]).

We now present a practical application of the procedure described above. The computations in the following example have been carried out with the computer algebra system MAGMA.

Example 1. Let $F : \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ be the LBCA with local rule $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ of radius $r = 1$, defined as $f(x_1, x_2, x_3) = x_1 + x_2 + x_3$ for all $(x_1, x_2, x_3) \in \mathbb{F}_2^3$, which is the elementary rule 150. Let $y \in \mathbb{F}_2^{\mathbb{Z}}$ be a spatially periodic configuration of period $p = 4$ generated by the block $y_{[0,3]} = (0,0,1,1)$, and let $x_{[0,1]} = (1,0)$ be the initial 2-cell block of a preimage $x \in F^{-1}(y)$. Since $r = 1$, sequence v is generated by block $v_{[0,3]} = (0,1,1,0)$. Feeding the string $(0,1,1,0,0,1,1,0)$ to the Berlekamp-Massey algorithm yields the polynomial $b(x) = x^3 + x^2 + x + 1$, while the characteristic polynomial associated to rule 150 is $a(x) = x^2 + x + 1$. Hence, it follows that $c(x) = a(x) \cdot b(x) = x^5 + x^3 + x^2 + 1$ is a characteristic polynomial of the preimage. Since the first 5 elements of preimage x are $1,0,1,0,0$, the initialisation polynomial of Equation (21) is $g(x) = x^4 + x^3 + 1$, from which we deduce that $h(x) = x^4 + x + 1$. Considering that $h(x)$ is irreducible, the greatest common divisor of $c(x)$ and $f(x)$ is 1, and thus by Equation (22) $c(x)$ is also the minimal polynomial of the preimage. The factorization of $c(x)$ is $(x+1)^3(x^2 + x + 1)$, and the orders of $x + 1$ and $x^2 + x + 1$ are respectively 1 and 3, from which it follows that the least common multiple e is 3. Finally, the smallest integer t such that $2^t \geq 3$ is $t = 2$. Therefore, by applying Theorem 5 the period of preimage x is $e2^t = 12$. Figure 5 shows the actual value of the block $x_{[0,11]}$ which generates preimage x.

5.2 Characterisation of Periods When $a(x)$ and $b(x)$ Are Irreducible

As a further application of Theorem 4, we now show a complete characterisation of the periods of $x \in F^{-1}(y)$ in the special case where the characteristic polynomials $a(x)$

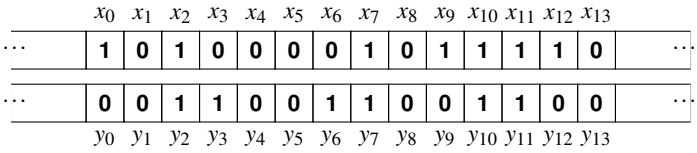

Fig. 5: Block $x_{[0,11]}$ which generates preimage $x \in F^{-1}(y)$ under rule 150, computed using case (a) of Equation (1). Notice that $(x_{12}, x_{13}) = (x_0, x_1)$ and $(y_{12}, y_{13}) = (y_0, y_1)$. Hence, for $n \geq 12$ and $n < 0$ the preimage will periodically repeat itself.

and $b(x)$ are irreducible. To this end, we first report an additional theorem proved in [9] which concerns the sum of families of LRS.

Theorem 6. *Let $f_1(x), f_2(x) \in \mathbb{F}_q$ be non-constant monic polynomials, and let $S(f_1(x))$ and $S(f_2(x))$ be the families of LRS whose characteristic polynomials are respectively $f_1(x)$ and $f_2(x)$. Denoting by $S(f_1(x)) + S(f_2(x))$ the family of all LRS $\sigma + \tau$ where $\sigma \in S(f_1(x))$ and $\tau \in S(f_2(x))$, it follows that $S(f_1(x)) + S(f_2(x)) = S(c(x))$, where $c(x)$ is the least common multiple of $f_1(x)$ and $f_2(x)$.*

Our characterisation result, which is analogous to Theorem 2, is the following:

Theorem 7. *Let $F : \mathbb{F}_q^{\mathbb{Z}} \to F_q^{\mathbb{Z}}$ be an LBCA having local rule $f : \mathbb{F}_q^{2r+1} \to \mathbb{F}_q$, and let $a(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_0 \in \mathbb{F}_q[x]$ be the characteristic polynomial associated to the inverse permutation $f_{R,z}^{-1}$, where $k = 2r$, $a_0, \cdots, a_{k-1}$ are the coefficients appearing in Equation (11) and $ord(a(x)) = e$. Further, let $y \in \mathbb{F}_q^{\mathbb{Z}}$ be a spatially periodic configuration of period $p > 1$, and let $b(x)$ be the minimal polynomial of sequence v, where $v_n = y_{n+r}$ for all $n \in \mathbb{N}$. If $a(x)$ and $b(x)$ are both irreducible and $a(x) \neq b(x)$, then $F^{-1}(y)$ contains one configuration of period p and $q^k - 1$ configurations of period m, where m is the least common multiple of e and p.*

Proof. By Theorem (4), $a(x) \cdot b(x)$ is a characteristic polynomial of the q^k preimages in $F^{-1}(y)$. Denote by $S(a(x))$ and $S(b(x))$ the sets of LRS having characteristic polynomials $a(x)$ and $b(x)$, respectively. Since $a(x)$ and $b(x)$ are both irreducible and $a(x) \neq b(x)$, by Theorem 6 it follows that $S(a(x) \cdot b(x)) = S(a(x)) + S(b(x))$. Hence, $F^{-1}(y)$ is a subset of $S(a(x)) + S(b(x))$, and as a consequence every preimage $x \in F^{-1}(y)$ can be written as $x = \sigma + \tau$, where $\sigma \in S(a(x))$ and $\tau \in S(b(x))$. In particular, by applying Theorem 2 it results that $S(a(x))$ is composed by one sequence of period 1 and $q^k - 1$ sequences of period e, while since $p > 1$ the sequence τ is necessarily one of the $q^l - 1$ sequences of period p of $S(b(x))$, where l is the degree of $b(x)$. Therefore, by making all possible sums for σ ranging in $S(a(x))$, Theorem 1 yields that $F^{-1}(y)$ is composed by one configuration having period p, which is the preimage $x = \sigma + \tau$ where σ has period 1, while the period of all the remaining $q^k - 1$ configurations is the least common multiple of e and p. □

6 Conclusions

In this work, we studied the relation between the periods of spatially periodic configurations of LBCA and the periods of their preimages, characterising the latter as concatena-

tions of linear recurring sequences. We remark that Theorem 4 can be straightforwardly generalised to the case $x^{(t)} \in F^{-t}(y)$, i.e. preimages of y with respect to the *t-th iterate* of the CA, where $t \in \mathbb{N}$. Indeed, it can be shown that $a(x)^t \cdot b(x)$ is a characteristic polynomial of $x^{(t)}$, which is thus generated by a "cascade" of concatenated LFSR where each LFSR is initialised to a block $x^{(i)}_{[0,2r-1]}$ of an intermediate preimage $x^{(i)} \in F^{-i}(y)$, for $i \in \{1, \cdots, t\}$. Of course in this case we have to take into account the fact that the running time of the procedure described in Section 5.1 grows exponentially in the degree D of the minimal polynomial $m(x)$, since it depends on the factorization of $q^D - 1$.

We conclude by discussing some possible future directions of research on the subject. A first idea is to generalise the results presented in this paper to *nonlinear* BCA, where the preimages are generated by a *Nonlinear Feedback Shift Register* (NFSR) disturbed by the LFSR which generates configuration y. We remark that this concatenation is also the main primitive upon which the stream cipher Grain is based [8]. Hence, finding a general method to study the periods of preimages of nonlinear BCA could also be useful to cryptanalyse this cipher. This study could be further generalised to generic surjective CA. In this regard, a possible starting point could be a result reported in [5], which implies that if $F : \mathbb{F}_q^{\mathbb{Z}} \to \mathbb{F}_q^{\mathbb{Z}}$ is a surjective linear CA, then there exists $t \in \mathbb{N}$ such that the t-th iterate F^t is bipermutive. Finally, a further extension of this research would be to analyse the periods of spatially periodic configurations in the case of multidimensional cellular automata, by considering suitable notions of bipermutivity such as the ones introduced in [6].

References

1. Berlekamp, E.R.: Factoring polynomials over finite fields. Bell Syst. Tech. J. 46, 1853–1859 (1967)
2. Cattaneo, G., Finelli, M., Margara, L.: Investigating topological chaos by elementary cellular automata dynamics. Theor. Comp. Sci. 244, 219–241 (2000)
3. Chassé, G.: Some remarks on a LFSR "disturbed" by other sequences. In: Cohen, G., Charpin. P. (eds.) EUROCODE '90. LNCS vol. 514, pp. 215–221. Springer, Heidelberg (1991)
4. The Cunningham Project, `http://homes.cerias.purdue.edu/~ssw/cun/index.html`
5. Dennunzio, A., Di Lena, P., Formenti, E., Margara, L.: On the directional dynamics of additive cellular automata. Theor. Comput. Sci. 410, 4823–4833 (2009)
6. Dennunzio, A., Formenti, E., Weiss, M.: Multidimensional cellular automata: closing property, quasi-expansivity, and (un)decidability issues. Theor. Comput. Sci. 516, 40–59 (2014)
7. Hedlund, G.A.: Endomorphisms and Automorphisms of the Shift Dynamical Systems. Mathematical Systems Theory 7(2), 138–153 (1973)
8. Hell, M., Johansson, T., Meier, W.: The Grain Family of Stream Ciphers. In: Robshaw, M., Billet, O. (eds.) New Stream Ciphers Designs. LNCS vol. 4986, pp. 179–190. Springer, Heidelberg (2008)
9. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press, Cambridge (1994)
10. Mariot, L., Leporati, A.: Sharing Secrets by Computing Preimages of Bipermutive Cellular Automata. In: Was, J., Sirakoulis, G.Ch., Bandini, S. (eds.): ACRI 2014. LNCS vol. 8751, pp. 417–426. Springer, Heidelberg (2014)
11. Massey, J.L.: Shift-register synthesis and BCH decoding. IEEE Trans. Inf. Theory 15, 122–127 (1969)