Nat Comput (2017) 16:367–381
DOI 10.1007/s11047-016-9586-x

Computing the periods of preimages in surjective cellular automata

Luca Mariot[1] · **Alberto Leporati**[1] · **Alberto Dennunzio**[1] · **Enrico Formenti**[2]

Published online: 16 November 2016

Abstract A basic property of one-dimensional surjective *cellular automata* (CA) is that any preimage of a *spatially periodic configuration* (SPC) is spatially periodic as well. This paper investigates the relationship between the periods of SPC and the periods of their preimages for various classes of CA. When the CA is only surjective and y is a SPC of least period p, the least periods of all preimages of y are multiples of p. By leveraging on the *De Bruijn graph representation* of CA, we devise a general algorithm to compute the least periods appearing in the preimages of a SPC, along with their corresponding multiplicities (i.e. how many preimages have a particular least period). Next, we consider the case of *linear* and *bipermutive* cellular automata (LBCA) defined over a *finite field* as state alphabet. In particular, we show an equivalence between preimages of LBCA and concatenated *linear recurring sequences* (LRS) that allows us to give a complete characterization of their periods. Finally, we generalize these results to LBCA defined over a *finite ring* as alphabet.

✉ Luca Mariot
luca.mariot@disco.unimib.it

Alberto Leporati
leporati@disco.unimib.it

Alberto Dennunzio
dennunzio@disco.unimib.it

Enrico Formenti
enrico.formenti@unice.fr

[1] Dipartimento di Informatica, Sistemistica e Comunicazione, Università degli Studi Milano-Bicocca, Viale Sarca 336, 20126 Milano, Italy

[2] Laboratoire I3S, Université Nice-Sophia Antipolis, 2000 Route des Colles, 06903 Sophia Antipolis, France

Keywords Cellular automata · Surjectivity · De Bruijn graph · Bipermutivity · Linear recurring sequences · Linear feedback shift registers

Mathematics Subject Classification 37B15 · 68Q80 · 94A55

1 Introduction

Cellular Automata (CA) are a parallel computational model that have been extensively studied as a particular type of discrete dynamical systems, where *cells* arranged on a regular lattice synchronously update their states according to their *neighbors* by means of a *local rule f*.

One of the most investigated aspects concerns the *temporally periodic* behavior of a CA, namely characterizing those integers $t \in \mathbb{N}$ such that, starting from a given configuration x of the cells, the CA returns to x after t applications of its *global rule* F; formally, $F^t(x) = x$.

On the other hand, *spatial periodicity* of CA is a much less researched topic. In this respect, one of the basic results is that if $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a surjective one-dimensional CA over alphabet A, $y \in A^{\mathbb{Z}}$ is a *spatially periodic configuration* (SPC) and $x \in F^{-1}(y)$ is a preimage of y, then x is also spatially periodic (see Cattaneo et al. 2000). This is a direct consequence of the *balancing* of surjective CA, which implies that every configuration can only have a finite number of preimages (see Hedlund 1969).

To our knowledge, there are no works in the literature that address the problem of actually characterizing the periods of SPC preimages. The aim of this paper, which is an extended version of Mariot and Leporati (2015), is to fill this gap by investigating the relation between the

periods of SPC and the periods of their preimages under the action of several classes of surjective CA.

Besides being interesting from a theoretical perspective, this research also has applications related to cryptography. In fact, determining the periods of SPC preimages under *bipermutive* CA corresponds to finding the maximum number of players allowed in the *secret sharing scheme* (SSS) proposed in Mariot and Leporati (2014). Furthermore, the theory of *concatenated linear recurring sequences*, which is a key tool used in the present paper to characterize the periods of preimages in *linear* and bipermutive CA, turns out to be useful also for studying the dynamics of *additive flowers*, a particular class of genetic regulatory networks introduced in Formenti et al. (2014).

A summary of the main contributions of the paper follows. Given a SPC $y \in A^{\mathbb{Z}}$ of least period $p \in \mathbb{N}$, we observe that in generic surjective CA the least period of a preimage $x \in F^{-1}(y)$ is a multiple of p, where the multiplier h ranges in $\{1, \ldots, q^{2r}\}$, with q being the size of the alphabet and r the radius of the CA (Lemmas 3 and 4). From this result, we also determine a first lower bound on the *multiplicity* of the least period of x, that is, how many other preimages of y have the same least period of x (Lemma 5). Successively, using the *De Bruijn graph representation* of CA, we introduce the notion of *u-closure graph* of a SPC y, whose cycles lengths turn out to be equivalent to the least periods of the preimages of y (Lemma 6). We thus describe an algorithm to build the u-closure graph starting from any surjective CA F and SPC y. The complexity of this procedure turns out to be exponential in the least period of y and in the radius of the CA. Remarking that the u-closure graph of a SPC under a bipermutive CA is composed only of disjoint cycles (Lemma 7), we narrow our attention to the special case of *linear bipermutive* CA (LBCA) defined over the *finite field* $\mathbb{F}_q$. In particular, we show that a preimage $x \in F^{-1}(y)$ is equivalent to a *concatenated linear recurring sequence* (CLRS), whose characteristic polynomial is the product of the characteristic polynomials respectively induced by the CA local rule and by configuration y (Theorem 6). Additionally, we present a procedure that given a $2r$-cell block of a preimage $x \in F^{-1}(y)$ as input determines the least period of x. Moreover, we characterize the multiplicities of the least periods under the tth *iterate* $F^{-t}(y)$ when the characteristic polynomial of the local rule is irreducible and does not divide the characteristic polynomial of y (Theorem 8). Finally, these results are generalized to LBCA defined over the *finite ring* $\mathbb{Z}_m$ (Theorem 9), using the *product CA conjugacy* described in Cattaneo et al. (2004).

The rest of this paper is organized 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 least periods of SPC preimages are multiples of the periods of their respective images, and introduces the notion of u-closure graph of a SPC along with the algorithm to compute the multiplicities of the least periods in surjective CA. Section 4 characterizes preimages of LBCA as concatenated linear recurring sequences and derives a characteristic polynomial for the latter. Section 5 presents an algorithm to compute the least period of a single LBCA preimage, characterizes the multiplicities of the least periods in the particular case where the characteristic polynomial of the local rule is irreducible and generalizes the previous results to LBCA defined over finite rings as alphabets. Finally, Sect. 6 summarizes the results presented throughout the paper and points out some additional further developments on the subject.

2 Basic definitions

2.1 Cellular automata

Let A be a finite alphabet having q symbols, and let A^n, A^* and $A^{\mathbb{Z}}$ respectively denote the set of all words over A having length $n \in \mathbb{N}$, the set of all finite words over A and the *full shift space* consisting of all bi-infinite words over A. Given $x \in A^{\mathbb{Z}}$ and $i, j \in \mathbb{Z}$ such that $i \leq j$ and $j - i + 1 = n$, by $x_{[i,j]}$ we denote the finite block $(x_i, \ldots, x_j) \in A^n$. For $k \in \mathbb{N}$, $\sigma^k(x)$ is the *k-left shift* of $x \in A^{\mathbb{Z}}$, where for all $i \in \mathbb{Z}$ the ith component of $\sigma^k(x)$ is defined as $\sigma^k(x)_i = x_{i+k}$. If $k = 1$, we simply write $\sigma(x)$.

Given $s \in \mathbb{N}$ and $u, v \in A^*$ such that $|u| \geq s$ and $|v| \geq s$, we define the *s-fusion operator* $\odot$ as in Sutner (1991):

$$u \odot v = z \Leftrightarrow \exists x \in A^s,\ u_0, v_0 \in A^* : u = u_0 x,\ v = x v_0,\ z = u_0 x v_0$$

that is, z is obtained by overlapping the right part of u and the left part of v of length s.

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 bi-infinite 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 rule f on the *neighborhood* $\{i - r, \ldots, i + r\}$.

The full shift space $A^{\mathbb{Z}}$ can be regarded as a compact metric space when endowed with the *Cantor distance*, defined for all $x, y \in A^{\mathbb{Z}}$ as follows:

$$d(x,y) = 2^{-i}, i = min\{j \in \mathbb{N} : x_j \neq y_j \vee x_{-j} \neq y_{-j}\}.$$

Intuitively, under the Cantor distance two configurations are near to each other if they agree on a large block centered around the origin. *Hedlund's theorem* (see Hedlund 1969) gives a particularly useful characterization of CA which leverages on this topological interpretation of the full shift space:

Theorem 1 *$F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a CA if and only if F is continuous with respect to the Cantor distance and commutes with the shift, i.e., $F(\sigma(x)) = \sigma(F(x))$ for all $x \in A^{\mathbb{Z}}$.*

A CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ can be represented by the *truth table* of its local rule f. Further, a local rule f can be indexed by its *Wolfram code*, which is the decimal representation of the output column in the truth table of f.

Another common way for representing a CA is by means of its *De Bruijn graph*. Given a finite alphabet A and $t \in \mathbb{N}$, the corresponding De Bruijn graph has vertex set A^t, and there exists a directed edge from $w_1 \in A^t$ to $w_2 \in A^t$ if and only if $w_1 = ax$ and $w_2 = xb$, where $a, b \in A$ and $x \in A^{t-1}$. In other words, two vertices are connected if and only if their respective words *overlap* respectively on the rightmost and the leftmost $t-1$ symbols. For the purposes of this paper, we give the following formal definition of De Bruijn graph associated to a CA based on the s-fusion operator:

Definition 2 Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a CA defined by a local rule $f : A^{2r+1} \to A$ of radius r. The *De Bruijn graph* associated to F is the directed labeled graph $G_{DB}(f) = (V, E, l)$ defined as follows:

- $V = A^{2r}$
- Given $v_1, v_2 \in V$, $(v_1, v_2) \in E$ if and only if there exists $z \in A^{2r+1}$ such that $z = v_1 \odot v_2$, where $\odot$ denotes the s-fusion operator with $s = 2r - 1$
- For all $(v_1, v_2) \in E$, the label function $l : E \to A$ is defined as $l(v_1, v_2) = f(v_1 \odot v_2)$

Figure 1 reports the De Bruijn graph associated to the CA $F : \{0,1\}^{\mathbb{Z}} \to \{0,1\}^{\mathbb{Z}}$ with elementary local rule 106 of radius $r = 1$, defined as $f_{106}(x_{i-1}, x_i, x_{i+1}) = x_{i-1} \cdot x_i \oplus x_{i+1}$.

Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a CA with local rule $f : A^{2r+1} \to A$. For all $m > 2r$, by $F_m : A^m \to A^{m-2r}$ we denote the restriction of F to input blocks of length m. The following Lemma, proved in Hedlund (1969), states that surjective CA are *balanced*, meaning that the sets of preimages on every restriction F_m all have the same cardinality:

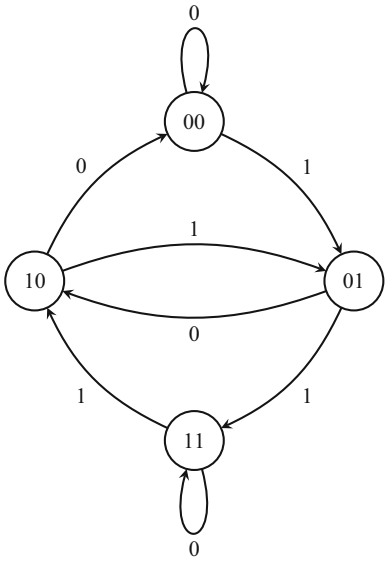

Fig. 1 De Bruijn graph associated to the CA F defined by rule 106

Lemma 1 *Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a surjective CA defined by a local rule $f : A^{2r+1} \to A$. Then, for all $m > 2r$ and for all $u \in A^{m-2r}$, it results that $|F_m^{-1}(u)| = q^{2r}$, where $q = |A|$. Additionally, for all $y \in A^{\mathbb{Z}}$, it holds that $|F^{-1}(y)| \leq q^{2r}$.*

One of the main classes of CA studied in this paper consists of *bipermutive* CA, defined as follows:

Definition 3 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* CA (BCA).

Bipermutivity may also be expressed in terms of the De Bruijn graph representation, by interpreting $G_{DB}(f)$ as a *finite state automaton*. To this end, if $l(v_1, v_2) = x$, define the transition function as $\delta(v_1, x) = v_2$. Then, F is bipermutive if and only if for all $v_1, v_2 \in V$ with $v_1 \neq v_2$ and for all $x \in A$, it holds that $\delta(v_1, x) \neq \delta(v_2, x)$, i.e. the De Bruijn graph is a *permutation automaton*.

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 $A = \mathbb{F}_q$, that is, A is the finite field of q elements with $q = \rho^{\alpha}$, where $\rho \in \mathbb{N}$ is a prime number (called the *characteristic* of $\mathbb{F}_q$) and $\alpha \geq 1$ is a positive integer.

Definition 4 Let $F : \mathbb{F}_q^{\mathbb{Z}} \to \mathbb{F}_q^{\mathbb{Z}}$ be a CA defined by a local rule $f : \mathbb{F}_q^{2r+1} \to \mathbb{F}_q$. Then, F is *linear* if there exists

$(c_0, \ldots, c_{2r}) \in \mathbb{F}_q^{2r+1}$ such that for all $(x_0, \ldots, x_{2r}) \in \mathbb{F}_q^{2r+1}$ the following equality holds:

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

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

One may easily check that if both c_0 and c_{2r} in Definition 4 are nonzero then a linear CA is bipermutive as well. Several results proved in this paper concern cellular automata which are both linear and bipermutive.

We now give the definition of *spatially periodic configuration* (SPC).

Definition 5 A configuration $x \in A^{\mathbb{Z}}$ is *spatially periodic* if there exists $P \in \mathbb{N}$, with $P \neq 0$, such that $\sigma^P(x) = x$. In particular, such a P is called a *period* of x. The smallest integer $p \in \mathbb{N}$ among all periods of x is called the *least period* of x.

Following the notation of Perrin and Pin (2004), we denote by $y = {}^{\omega} u^{\omega}$ the SPC $y \in A^{\mathbb{Z}}$ obtained as the bi-infinite concatenation of block $u \in A^*$ with itself. Moreover, given $v \in A^*$ such that $v = wzw$ where $w \in A^s$ and $z \in A^*$, by $x = {}^{\odot} v^{\odot}$ we denote the SPC $x \in A^{\mathbb{Z}}$ of least period $|wz|$ obtained by the bi-infinite s-fusion of block v with itself. Notice that if z is the empty word then ${}^{\odot}v^{\odot} = {}^{\omega} w^{\omega}$.

A proof of the following Lemma about preimages of SPC in surjective CA can be found in Cattaneo et al. (2000).

Lemma 2 *Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a surjective CA. Then, given a SPC $y \in A^{\mathbb{Z}}$, each preimage $x \in F^{-1}(y)$ is also spatially periodic.*

As a matter of fact, surjective CA satisfy an even stronger condition than the closure property implied by the Lemma above. In particular, the global map $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ of a CA is surjective if and only if its restriction F_p to the set of SPC is surjective (see Durand 1999). As a consequence, one can study other properties of surjective CA, for instance injectivity, by considering only their restriction to SPC. In the model-theoretic setting set forth in Sutner (2010), this means that the set of SPC is an elementary substructure of the full shift space $A^{\mathbb{Z}}$ for surjective CA.

Given $t \in \mathbb{N}$, by $F^{-t}(y)$ we denote the set of preimages of y under the tth *iterate* of F, that is, the set of configurations $x \in A^{\mathbb{Z}}$ such that $F^t(x) = y$. We call a preimage $x \in F^{-t}(y)$ a tth *ancestor* of 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 characterize the periods of preimages in LBCA. All the proofs of the facts and the theorems mentioned in this section may be found in Lidl and Niederreiter (1994).

Definition 6 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 $s = s_0, s_1, \ldots$ of elements in $\mathbb{F}_q$ which satisfies the following relation:

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

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 Fig. 2.Basically, a LFSR of order k is composed of k *delayed flip-flops* $D_0,\ D_1,\ \cdots,\ D_{k-1}$, each containing an element of $\mathbb{F}_q$. At each 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 with 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 Eq. (1). In the relevant literature, this kind of linear feedback shift registers are also called *Fibonacci* LFSR, as opposed to *Galois* LFSR where the adders are placed between one flip-flop and the other.

Notice that the output produced by the LFSR (that is, the LRS $s = s_0, s_1, \ldots$) is *ultimately periodic*, i.e. 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 $(s_n, s_{n+1}, \ldots, s_{n+k-1})$. Since all the components of such a 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 Lidl and Niederreiter (1994) it is proved that if $a_0 \neq 0$, then the sequence produced by the LFSR (or, equivalently, the corresponding LRS) is *periodic*, in the sense of Definition 5.

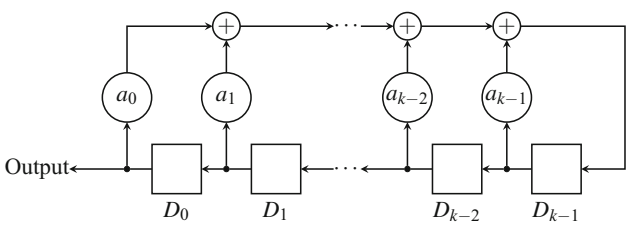

Fig. 2 Diagram of a linear feedback shift register

The *characteristic polynomial* $a(x) \in \mathbb{F}_q[x]$ of a kth order homogeneous LRS $s = s_0, s_1, \ldots$ is defined as:

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

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 characterize the period of s. In fact, in Lidl and Niederreiter (1994) 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 $s = s_0, s_1, \ldots$ is by means of its *generating function* $G(x)$, which is the formal power series defined as:

$$G(x) = s_0 + s_1 x + s_2 x^2 + \cdots = \sum_{n=0}^{\infty} s_n x^n \quad (3)$$

In this case, the terms $s_0, s_1, \ldots$ 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 kth order homogeneous LRS s can be expressed as a rational function:

$$G(x) = \frac{g(x)}{a^*(x)} = \frac{-\sum_{j=0}^{k-1}\sum_{i=0}^{j} a_{i+k-j} s_i x^j}{x^k a(1/x)}. \quad (4)$$

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

A given LRS $s = s_0, s_1, \ldots$ 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:

$$m(x) = \frac{a(x)}{\gcd(a(x), h(x))}, \quad (5)$$

where $a(x)$ is a characteristic polynomial of sequence s and $h(x) = -g^*(x)$ is the reciprocal of the initialization polynomial $g(x)$ appearing in Eq. (4), with the sign changed. In Lidl and Niederreiter (1994) 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 families of linear recurring sequences. Denote by $S(f(x))$ the set of LRS having $f(x)$ as characteristic polynomial. Given $s = s_0, s_1 \cdots \in S(f(x))$ and $t = t_0, t_1, \ldots \in S(f(x))$ define the sum of LRS $\sigma = s + t$ as $\sigma_n = s_n + t_n$ for all $n \in \mathbb{N}$, and for $c \in \mathbb{F}_q$ define the scalar multiplication $\mu = c \cdot s$ as $\mu_n = c \cdot s_n$ for all $n \in \mathbb{N}$. Under these two operations, the set $S(f(x))$ is a vector space over $\mathbb{F}_q$. The following theorem shows what is the characteristic polynomial of the direct sum of two families of LRS:

Theorem 2 *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 $f_2(x)$.*

From Theorem 2, the following result states how to compute the least periods of the sum of two LRS in the special case when their characteristic polynomials are coprime:

Theorem 3 *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 least period of σ is the least common multiple of p_1 and p_2.*

Finally, the following theorem characterizes the multiplicities of the least periods in $S(f(x))$ when $f(x)$ is the power of an irreducible polynomial:

Theorem 4 *Let $f(x) = g(x)^t$ with $g(x)$ monic and irreducible over $\mathbb{F}_q$ and such that $g(0) \neq 0$, $deg(g(x)) = k$, $ord(g(x)) = e$, and $t \in \mathbb{N}$ a positive integer. Let $s \in \mathbb{N}$ be the smallest integer such that $\rho^s \geq t$, where ρ is the characteristic of $\mathbb{F}_q$. If $t = 1$ the family of LRS $S(f(x))$ is composed of the following numbers of sequences with the following least periods:*

- *one sequence of least period 1*
- *$q^k - 1$ sequences of least period e*

For $t \geq 2$, $S(f(x))$ additionally contains the following numbers of sequences with the following least periods:

- *for $j \in \{1, \ldots, s-1\}$, $q^{k\rho^j} - q^{k\rho^{j-1}}$ sequences of least period $e\rho^j$*
- *$q^{kt} - q^{k\rho^s}$ sequences of least period $e\rho^s$*

3 Problems statement and basic results

In this section, we present some basic results concerning the periods of preimages of spatially periodic configurations in surjective CA. To this end, we begin by formally

stating the first main problem analyzed in this paper, generalized to the tth iterate case:

Problem 1 Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a surjective CA, $y \in A^{\mathbb{Z}}$ be a SPC of least period $p \in \mathbb{N}$ and $x \in F^{-t}(y)$ be a tth ancestor of y, for $t \in \mathbb{N}$. What is the least period of x?

Besides computing the period of a single preimage, we are also interested in counting the *multiplicities* of all least periods appearing in the set of preimages of a spatially periodic configuration, as described below:

Problem 2 Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a surjective CA, with $|A| = q$, and $y \in A^{\mathbb{Z}}$ be a SPC of least period $p \in \mathbb{N}$. For all multipliers $h \in \{1, \ldots, q^{2r}\}$, what is the number of preimages $N_h(y, F)$ of y under F having least period hp?

3.1 Periods of SPC preimages in surjective CA

We begin our analysis of Problem 1 by considering the general case where the CA is only surjective. To this end, we first show that if $y \in A^{\mathbb{Z}}$ is a SPC having least period $p \in \mathbb{N}$, then the least periods of its preimages are multiples of p.

Lemma 3 *Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a surjective CA, $y \in A^{\mathbb{Z}}$ be a spatially periodic configuration of least period $p \in \mathbb{N}$ and $x \in F^{-1}(y)$ be a preimage of y. Then, the least period $k \in \mathbb{N}$ of x is a multiple of p.*

Proof Suppose that k is not a multiple of p, and let $k = jp + r$ with $j = \lfloor k/p \rfloor$ and $0 < r < p$. Since x is spatially periodic of least period x, it follows that $\sigma^k(x) = x$. Moreover, by Hedlund's theorem $F(\sigma^t(x)) = \sigma^t(F(x))$ for all $t \in \mathbb{Z}$. Hence,

$$y = F(x) = F(\sigma^k(x)) = \sigma^k(F(x)) = \sigma^k(y)$$
$$= \sigma^{jp+r}(y) = \sigma^r(\sigma^{jp}(y)) = \sigma^r(y) \neq y$$

where the last inequality follows from the fact that $r < p$. Having obtained a contradiction, k is a multiple of p. □

By employing the *balancing* condition of surjective CA, the following result gives an upper bound on the value of the least period multiplier:

Lemma 4 *Let $|A| = q$ and let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a surjective CA defined by a local rule f of radius r. Further, let $y \in A^{\mathbb{Z}}$ be a SPC of least period $p \in \mathbb{N}$ and $x \in F^{-1}(y)$ be a preimage of y having least period $k = hp$. Then, $h \in \{1, \ldots, q^{2r}\}$.*

Proof The proof of Lemma 3 already implies that $h \geq 1$, so it suffices to show that $h \leq q^{2r}$.

Let $u \in A^p$ be a block of length p taken from y (hence $y = {}^{\omega} u^{\omega}$), and let $s = 2r$ and $Q = q^s$. By Lemma 1, we know that $|F_m^{-1}(u)| = Q$, where $m = p + s$. Hence, there are Q distinct blocks $x_1, x_2, \ldots, x_Q \in A^m$ such that $F_m(x_i) = u$ for all $i \in \{1, \ldots, Q\}$. Since $x \in F^{-1}(y)$ is spatially periodic of least period hp, there exists a block $v \in A^{hp+s}$ with $v = w_1 z w_1$ and $w_1 \in A^s$ such that $x = {}^{\odot} v^{\odot}$ and $F_{hp+s}(v) = u^h$ (see Fig. 3).As a consequence, block v is obtained by "gluing" together h blocks of $F_m^{-1}(u)$ using the s-fusion operator. Formally, this means that $v = \bigodot_{x_j \in S} x_j$, where $S \subseteq F_m^{-1}(u)$ and $|S| = h$. Recalling that $|F_m^{-1}(u)| = Q = |A|^s = |A|^{2r}$, it follows that $h \leq q^{2r}$. □

The following Corollary straightforwardly generalizes Lemma 4 to preimages under the tth iterate of F:

Corollary 1 *Let $|A| = q$, and let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a surjective CA defined by a local rule of radius r. Further, let $y \in A^{\mathbb{Z}}$ be a SPC of least period $p \in \mathbb{N}$ and $x \in F^{-t}(y)$ be a t-th ancestor of y. Then, the least period of x equals $k = \left(\prod_{i=1}^{t} h_i\right) \cdot p$, where $h_i \in \{1, \ldots, q^{2r}\}$ for all $i \in \{1, \ldots, t\}$.*

Proof We prove the result by induction on $t \in \mathbb{N}$. First, remark that the base case $t = 1$ corresponds to Lemma 4. For the induction step, assume that the condition holds up to $t - 1$, and consider a tth ancestor $x \in F^{-t}(y)$. Clearly, x can be expressed as a preimage of a preimage $x_{t-1} \in F^{-(t-1)}(y)$ under the $(t-1)$th iterate of F, i.e. $x \in F^{-1}(x_{t-1})$. By Lemma 4 we know that the least period of x is $k = h_t k_{t-1}$, where $h_t \in \{1, \ldots, q^{2r}\}$ and k_{t-1} is the least period of k_{t-1}. Further, by induction hypothesis we have $k_{t-1} = \left(\prod_{i=1}^{t-1} h_i\right) \cdot p$, where $h_i \in \{1, \ldots, q^{2r}\}$ for all $i \in \{1, \ldots, t-1\}$. Hence, it follows that $k = h_t \cdot \left(\prod_{i=1}^{t-1} h_i\right) \cdot p = \left(\prod_{i=1}^{t} h_i\right) \cdot p$. □

The following lemma gives a first lower bound on $N_h(y, F)$:

Lemma 5 *Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a surjective CA such that $|A| = q$, $y \in A^{\mathbb{Z}}$ a SPC of least period $p \in \mathbb{N}$, and $x \in F^{-1}(y)$ a preimage of y having least period hp, with $h \in \{1, \ldots, q^{2r}\}$. Then, $N_h(y, F) \geq h$.*

Proof Since x is a preimage of y, we have to show that there are at least $h - 1$ other preimages of y having least period hp. Given that $\sigma^p(y) = y$, by Hedlund's theorem we know that the following identity stands for all $i \in \mathbb{Z}$:

$$F(\sigma^{ip}(x)) = \sigma^{ip}(F(x)) = \sigma^{ip}(y) = y,$$

In particular, if $i \in \{1, \ldots, h-1\}$ then $\sigma^{ip}(x) \neq x$ (otherwise, this would contradict the hypothesis that x has least period hp). Thus, we can construct $h - 1$ distinct preimages of y by simply shifting x of ip coordinates, for

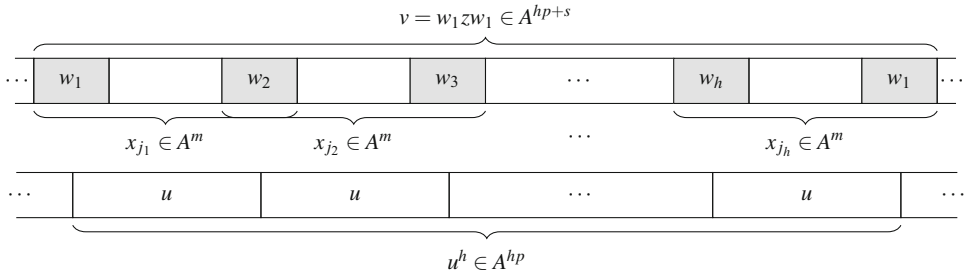

Fig. 3 Setting $s = 2r$, preimage x is generated by the bi-infinite s-fusion $x = {}^{\odot}\, v^{\odot}$ of block $v \in A^{hp+s}$, which is in turn obtained by the s-fusion of h blocks $x_{j_1}, \ldots, x_{j_h}$ in $F_m^{-1}(u)$. The *blocks shaded* in *gray* are the overlapping parts of length s between two consecutive blocks $x_{j_i}, x_{j_{i+1}}$

$i \in \{1, \ldots, h-1\}$. All these preimages have least period hp, hence it follows that $N_h(y, F) \geq 1 + h - 1 = h$. □

3.2 Graph characterization of preimages

We now introduce a graph-based method to study the periods of preimages in surjective CA. Given a CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ defined on an alphabet A such that $|A| = q$, and a configuration $y \in A^{\mathbb{Z}}$, a preimage $x \in F^{-1}(y)$ can be viewed as a *bi-infinite path* π labeled by y on the associated De Bruijn graph $G_{DB}(f)$, i.e. $\pi = \{v_i\}_{i \in \mathbb{Z}}$ such that $l(v_i, v_{i+1}) = y_i$ for all $i \in \mathbb{Z}$. In particular, by setting $s = 2r - 1$, preimage x can be defined as the bi-infinite s-fusion of the vertices visited by π, that is, $x = \bigodot_{v_i \in \pi} v_i$. If F is surjective, for all configurations $y \in A^{\mathbb{Z}}$ we can always find at least one bi-infinite path on $G_{DB}(f)$ labeled by y.

We now define a second graph which will be used to determine the least periods of the preimages and their numbers:

Definition 7 Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a surjective CA and let $G_{DB}(f)$ be its De Bruijn graph. Additionally, let $y \in A^{\mathbb{Z}}$ be spatially periodic of least period $p \in \mathbb{N}$, and let $u \in A^p$ be a block of length p of y, i.e. $y = {}^{\omega}\, u^{\omega}$. The *u-closure* of $G_{DB}(f)$ (also called the *unfolding* of $G_{DB}(f)$ along u) is the graph $\overline{G_{DB}^u}(f) = (V, E)$, where:

- $V = A^{2r}$
- Given $v_1, v_2 \in V$, $(v_1, v_2) \in E$ if and only if there exists a finite path $\pi = v_1, \ldots, v_2$ labeled by u on the De Bruijn graph $G_{DB}(f)$

As the next Lemma shows, the cycle structure of the u-closure graph is directly related to the least periods of the preimages of $y = {}^{\omega}\, u^{\omega}$ and their multiplicities.

Lemma 6 *Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a CA defined by local rule $f : A^{2r+1} \to A$, and let $y = {}^{\omega}\, u^{\omega} \in A^{\mathbb{Z}}$ for $u \in A^p$ be spatially periodic of least period $p \in \mathbb{N}$. Given $h \in \{1, \ldots, q^{2r}\}$, denote by $\mathscr{C}_h^u(f)$ the (possibly empty) set of distinct cycles of length h in the u-closure graph $\overline{G_{DB}^u}(f)$. Then, the number of preimages $x \in F^{-1}(y)$ of least period hp equals $N_h(y, F) = h \cdot |\mathscr{C}_h^u(f)|$.*

Proof Remark that an edge (w_1, w_2) of $\overline{G_{DB}^u}(f)$ represents the first and the last $2r$-cell blocks of a finite preimage $v \in F_{p+2r}^{-1}(u)$. Considering Fig. 3, this means that the blocks $w_1, \ldots, w_h, w_1$ occurring in $x \in F^{-1}(y)$ between the end and the beginning of a copy of u correspond to a cycle $c \in \mathscr{C}_h^u(f)$ of length h in $\overline{G_{DB}^u}(f)$. Thus, by Lemma 3 a single cycle $c \in \mathscr{C}_h^u(f)$ identifies h possible preimages of least period hp, depending from which vertex the path starts. Therefore, the number of preimages of least period hp is given by the number of distinct cycles of length h multiplied by h. □

In order to build the u-closure graph, it is possible to use a variation of *depth-first search* (DFS) in which the De Bruijn graph is explored up to depth p following only the paths labeled by u, without checking if a node has already been visited or not. In order to assess the time complexity of this procedure, observe first that the out-degree of each vertex $v \in A^{2r}$ in $G_{DB}(f)$ is $|A| = q$, and thus v can have at most q outgoing edges labeled by the same symbol $s \in A$. Consequently, starting from $v \in A^{2r}$ the DFS can visit at most the following number of vertices:

$$1 + q + q^2 + \cdots + q^p = \sum_{i=0}^{p} q^i = \frac{q^{p+1} - 1}{q - 1} = O(q^p).$$

In particular, the worst case occurs when for each symbol u_i of u each node in the ith level of the DFS tree has q outgoing edges labeled by u_i. Since the DFS must be called for all $v \in A^{2r}$, the time complexity for building the u-closure graph is thus $O(q^{2r} \cdot q^p) = O(q^{p+2r})$.

The u-closure graph contains at most q^{2r} edges, since u has exactly q^{2r} preimages under $F_{p+2r}^{-1}(u)$ and there can be at most a one-to-one correspondence between the prefixes and the suffixes of length $2r$ of these preimages. Thus, once the u-closure graph is built, a DFS visit can be employed to determine its cycles and their respective lengths in $O(q^{2r})$ steps. Starting from the De Bruijn graph

of a surjective CA as input, this means that the overall procedure to compute the least periods of the preimages of y and their cardinalities takes $O(q^{p+2r} + q^{2r})$ steps.

Notice that, in general, the u-closure of $G_{DB}(f)$ is not composed of disjoint cycles. Figure 4a, b report two examples of u-closure graphs for the CA F based on rule 106, the former corresponding to the configuration $y = {}^{\omega}011^{\omega}$ and the latter for $y = {}^{\omega}1000^{\omega}$.

In both cases, the resulting u-closure graphs have cycles with preperiods, and all $2r$-cell blocks in the preperiods cannot appear in any preimage of y (otherwise, the preimages containing them would not be spatially periodic, contradicting Lemma 2).

We now show that if the local rule is *bipermutive* then $\overline{G^u_{DB}}(f)$ is composed only of disjoint cycles:

Lemma 7 *Let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a surjective CA defined by a bipermutive local rule $f : A^{2r+1} \to A$. Then, for all spatially periodic configurations $y = {}^{\omega}u^{\omega}$ of least period $p \in \mathbb{N}$ with $u \in A^p$, the u-closure graph $\overline{G^u_{DB}}(f)$ is composed only of disjoint cycles.*

Proof Let $v \in A^{2r}$ be a vertex of the De Bruijn graph $G_{DB}(f)$. Since f is right permutive, the set of labelings $l(v, w_i)$ of the outgoing edges of v is a permutation on A. Hence, there exists exactly one path starting from v and labeled by u on the De Bruijn graph, which means that v has exactly one outgoing edge in the u-closure graph $G^u_{DB}(f)$. Analogously, since f is also left permutive, the set of labelings $l(w_i, v)$ of the incoming edges of v is a permutation on A as well. As a consequence, there is exactly one path ending in v and labeled by u on $G_{DB}(f)$, meaning that v has exactly one incoming edge $\overline{G^u_{DB}}(f)$. Since each vertex of the u-closure graph $\overline{G^u_{DB}}(f)$ has both in-degree and out-degree equal to 1, the thesis follows. □

A consequence of Lemma 7 is that the construction of the u-closure graph takes $\Theta(q^{2r} \cdot p)$ steps for bipermutive CA, since each call of the DFS on the De Bruijn graph returns only one path labeled by u. As an example, Fig. 5a, b depict the u-closure graphs for $y = {}^{\omega}011^{\omega}$ and $y = {}^{\omega}1000^{\omega}$ under the elementary bipermutive rule 150, which is defined as $f_{150}(x_{i-1}, x_i, x_{i+1}) = x_{i-1} \oplus x_i \oplus x_{i+1}$.

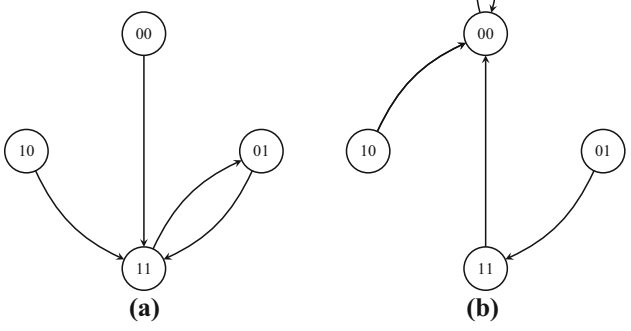

Fig. 4 Examples of u-closure graphs $\overline{G^u_{DB}}(f_{106})$ for the CA F based on the elementary rule 106. **a** $y = {}^{\omega}011^{\omega}$. **b** $y = {}^{\omega}1000^{\omega}$

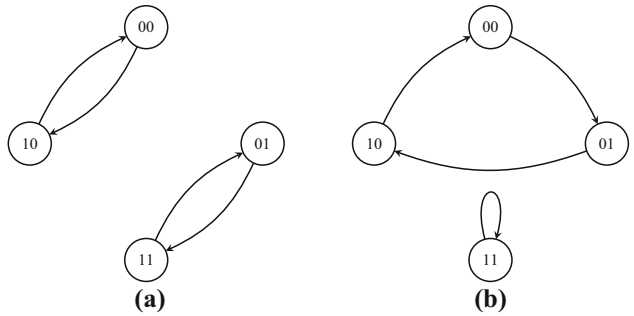

Fig. 5 Examples of u-closure graphs $\overline{G^u_{DB}}(f_{150})$ for the CA F based on the elementary rule 150. **a** $y = {}^{\omega}011^{\omega}$. **b** $y = {}^{\omega}1000^{\omega}$

As a concluding remark for this section, observe that the construction of the u-closure graph, as well as Lemma 6, can be generalized by induction to the tth iterate F^t. Of course, in this case both the construction of the graph and its visit become exponential in t, thus yielding a total complexity of $O(q^{p+2rt} + q^{2rt})$ for determining the multiplicities of the least periods in $F^{-t}(y)$. On the other hand, once the u-closure graph of $F^{-t}(y)$ has been built, it is not difficult to see that the number of tth ancestors $x \in F^{-t}(y)$ having least period hp are $h \cdot |\mathscr{C}^u_h(f)|$, where $h = \prod_{i=1}^{t} h_i$ by Corollary 1, with $h_i \in \{1, \ldots, q^{2r}\}$ for all $i \in \{1, \ldots, t\}$.

4 Linear bipermutive CA and linear recurring sequences

Lemma 7 suggests that both Problems 1 and 2 are easier to analyze in the bipermutive context, since BCA do not feature paths with preperiods in the u-closure graph. In this section, we narrow our attention to the class of LBCA, showing that in this case further information about the periods of preimages can be obtained. In particular, we characterize the preimages of LBCA as a particular kind of *concatenated linear recurring sequences*, and determine the corresponding *characteristic polynomials*.

4.1 LBCA preimages and concatenated LRS

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 $(c_0, \ldots, c_{2r}) \in \mathbb{F}_q^{2r+1}$, 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:

$$y = c_0x_0 + c_1x_1 + \cdots + c_{2r-1}x_{2r-1} + c_{2r}x_{2r}$$
$$x_{2r} = c_{2r}^{-1}(-c_0x_0 - c_1x_1 - \cdots - c_{2r-1}x_{2r-1} + y).$$

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

$$x_{2r} = a_0x_0 + a_1x_1 + \cdots + a_{2r-1}x_{2r-1} + dy. \tag{6}$$

Equation (6) 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 $z = (x_0, \ldots, x_{2r-1})$. 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 $x \in F^{-1}(y)$, for all $n > 2r$ it results that:

$$x_n = a_0x_{n-2r} + a_1x_{n-2r+1} + \cdots + a_{2r-1}x_{n-1} + dy_{n-r}, \tag{7}$$

and by setting $k = 2r$ and $v_n = y_{n+r}$ for all $n \in \mathbb{N}$, Eq. (7) can be rewritten as

$$x_{n+k} = a_0x_n + a_1x_{n+1} + \cdots + a_{k-1}x_{n+k-1} + dv_n. \tag{8}$$

Equation (8) 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 $v = v_0, v_1, \ldots$ as a linear recurring sequence of order $l \leq p$ defined by

$$v_{n+l} = b_0v_n + b_1v_{n+1} + \cdots + b_{l-1}v_{n+l-1}, \tag{9}$$

where $b_i \in \mathbb{F}_q$ for all $i \in \{0, \ldots, l-1\}$, 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 $s = s_0, s_1, \ldots$ is the kth order LRS satisfying the recurrence

$$s_{n+k} = a_0s_n + a_1s_{n+1} + \cdots + a_{k-1}s_{n+k-1}, \tag{10}$$

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 lth order LFSR multiplied by $d = c_{2r}^{-1}$, which produces the sequence v. Similarly to concatenated LRS, we call this system a *concatenation* of LFSR. Figure 6 depicts the block diagram of this concatenation.

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 Fig. 6, where the disturbing LFSR is initialized 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 $d = 1$.

4.2 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 Eq. (8) of x, but whose k initial terms $u_0, \cdots, u_{k-1}$ are set to 0.

Theorem 5 *Let $s = s_0, s_1, \ldots$ and $v = v_0, v_1, \ldots$ be the LRS respectively satisfying* Eqs. (9) *and* (10), *with $s_0 = x_0$, $\cdots$, $s_{k-1} = x_{k-1}$ and $v_0 = y_r, \ldots, v_{l-1} = y_{r+l-1}$. Further, let $x = s \leftsquigarrow v$ be the concatenation of s and v defined by* Eq. (8), *where $d = 1$, and 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 $u_0 = \cdots = u_{k-1} = 0$, for all $n \in \{0, \ldots, k-1\}$ it holds

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

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

$$\begin{aligned} s_k + u_k &= a_0s_0 + \cdots + a_{k-1}s_{k-1} \\ &\quad + a_0u_0 + \cdots + a_{k-1}u_{k-1} + v_0 \\ &= a_0x_0 + \cdots + a_{k-1}x_{k-1} + v_0 = x_k. \end{aligned}$$

For the induction step we assume $s_n + u_n = x_n$ for all n in the range $\{k, \ldots, m\}$. For $n = m + 1$, the sum $s_{m+1} + u_{m+1}$ is equal to:

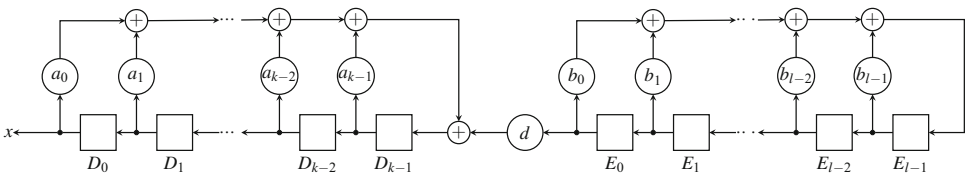

Fig. 6 Diagram of two concatenated LFSR

$$\begin{aligned} s_{m+1} + u_{m+1} &= a_0 s_{m-k+1} + \cdots + a_{k-1} s_m \\ &\quad + a_0 u_{m-k+1} + \cdots + a_{k-1} u_m + v_{m-k+1} \\ &= a_0 (s_{m-k+1} + u_{m-k+1}) + \cdots \\ &\quad + a_{k-1} (s_m + u_m) + v_{m-k+1}. \end{aligned} \tag{11}$$

By induction hypothesis, $s_{m-k+i} + u_{m-k+i} = x_{m-k+i}$ for all $i \in \{1, \ldots, k\}$. Hence, Eq. (11) can be rewritten as

$$s_{m+1} + u_{m+1} = a_0 x_{m-k+1} + \cdots + a_{k-1} x_m + v_{m-k+1} = x_{m+1}.$$

□

4.3 Characteristic polynomial of concatenated LRS

Theorem 5 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 Fig. 6, where the disturbed LFSR is initialized to zero, and the LRS produced by the *non-disturbed* LFSR, that is, the leftmost LFSR in Fig. 6 initialized to the values $x_0, \ldots, x_{k-1}$ without the feedback from the rightmost LFSR.

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 in Chassé (1990) 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 nth 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 Eq. (10). In particular, we will need the values of $A_n^{(0)}$ for $n \geq 0$, which can be computed by the following recurrence equation:

$$A_n^{(0)} = \begin{cases} \sum_{j=0}^{k-1} a_j A_{n-k+j}^{(0)}, & \text{if } n > 1 \\ 1, & \text{if } n = 1 \\ 0, & \text{if } n = 0 \end{cases} \tag{12}$$

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 1 *Let $u = s \leftsquigarrow_0 v$ be the 0-concatenation of the LRS s and v defined in* Theorem 5, *and let $V(x)$ be the generating function of v. Denoting by $\mathscr{A}(x)$ the generating function of the sequence $A = \{A_{n+1}^{(0)}\}_{n \in \mathbb{N}}$, the generating function of u is equal to*

$$U(x) = x \cdot \mathscr{A}(x) \cdot V(x). \tag{13}$$

Moreover, if $a(x) \in \mathbb{F}_q[x]$ is the characteristic polynomial of the sequence s associated to the recurrence Eq. (10), *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 6 *Let $s \leftsquigarrow v$ be the concatenation of LRS s and v defined by* Eq. (8) *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* Eqs. (10) *and* (9). *Then, $a(x) \cdot b(x)$ is a characteristic polynomial of $s \leftsquigarrow v$.*

Proof By Theorem 5 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 (Eq. 4) and Proposition 1, the following equalities hold:

$$S(x) = \frac{g_s(x)}{a^*(x)} \tag{14}$$

$$U(x) = \frac{x \cdot g_A(x) \cdot g_v(x)}{a^*(x) \cdot b^*(x)}, \tag{15}$$

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 Eq. (4). Hence, the generating function of $s \leftsquigarrow v$ is:

$$G(x) = S(x) + U(x) = \frac{g_s(x) \cdot b^*(x) + x \cdot g_A(x) \cdot g_v(x)}{a^*(x) \cdot b^*(x)}. \tag{16}$$

By applying again the fundamental identity of formal power series to Eq. (16), 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

$$c^*(x) = x^{k+l} \cdot \frac{1}{x^{k+l}} \cdot a(x) \cdot b(x) = a(x) \cdot b(x). \tag{17}$$

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

Theorem (6) 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:

$$\sigma_{n+k+l} = c_0\sigma_n + c_1\sigma_{n+1} + \cdots + c_{k+l-1}\sigma_{n+k+l-1}, \tag{18}$$

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

$$c_\mu = \sum_{i+j=\mu} a_i b_j, \text{ for} i \in \{0, \ldots, k\} \text{ and} j \in \{0, \ldots, l\}. \tag{19}$$

Additionally, the first $k = 2r$ initial terms $\sigma_0, \ldots, \sigma_{k-1}$ in Eq. (18) are initialized to the values in $x_{[0,2r-1]}$, while the remaining l ones are obtained using the recurrence Eq. (8). Hence, by applying the fundamental identity of formal power series, the numerator of Eq. (16) can also be expressed as:

$$g(x) = -\sum_{j=0}^{k-1}\sum_{i=0}^{j} c_{i+k-j}\sigma_i x^j. \tag{20}$$

As in the case of Lemmas 4 and 6, Theorem 6 can be easily extended to the tth iterate F^t for any $t > 1$. In this case, a tth ancestor $x \in F^{-t}(y)$ can be expressed by the following sequence of concatenated LRS:

$$x = s(t) \leftsquigarrow s(t-1) \leftsquigarrow \cdots \leftsquigarrow s(1) \leftsquigarrow v \tag{21}$$

where $s(i)$ belongs to the family of LRS $S(a(x))$ for all $i \in \{1, \ldots, t\}$. In other words, the tth ancestor $x \in F^{-t}(y)$ is obtained by concatenating t sequences generated by the characteristic polynomial $a(x)$ of the CA local rule, which are in turn concatenated with the r-left shift of configuration y. Notice that the preimage computation process, in this case, can be carried out by a *cascade* of concatenated LFSR, where the leftmost t ones all have the same characteristic polynomial but possibly different initialization values, while the rightmost one generates v.

Consequently, by iteratively applying Theorem 6, we obtain that the characteristic polynomial of $x \in F^{-t}(y)$ is

$$c(x) = a(x)^t \cdot b(x). \tag{22}$$

5 Applications to periods computation, multiplicities count and finite rings alphabets

To summarize the results discussed so far, in this section we explore the applications of the equivalence between LBCA preimages and CLRS presented in Sect. 4, starting from the most specific one and then generalizing. Specifically, in Sect. 5.1 we describe an algorithm which, given as inputs a SPC y of a LBCA over $\mathbb{F}_q$ and a $2r$-cell block of one of its preimages $x \in F^{-1}(y)$, computes the least period of x. On the other hand, Sect. 5.2 characterizes the multiplicities of the preimages of a SPC y in the particular case where the characteristic polynomial of the local rule is irreducible and it is not a factor of the polynomial of y. Finally, Sect. 5.3 generalizes the results presented in Sect. 4 to the case where the CA alphabet is a *finite ring*.

5.1 Computing the period of a single preimage

We now present a high-level procedure to compute the spatial period of a single preimage. Given a LBCA $F : \mathbb{F}_q^{\mathbb{Z}} \to \mathbb{F}_q^{\mathbb{Z}}$ defined by a 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. Compute the minimal polynomial $b(x)$ 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 Eq. (10).
3. Compute the polynomial $g(x)$ given by Eq. (20), and set $h(x) = -g^*(x)$.
4. Determine the minimal polynomial of the preimage by computing
$$m(x) = \frac{a(x) \cdot b(x)}{gcd(a(x) \cdot b(x), h(x))}. \tag{23}$$
5. Compute the order of $m(x)$, and output it as the least period of preimage x.

For step 1, the minimal polynomial of v can be found using the *Berlekamp-Massey algorithm* Massey (1969), 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 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* described in Berlekamp (1967), 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 Lidl and Niederreiter (1994):

Theorem 7 *Let $m(x) \in \mathbb{F}_q[x]$ be a polynomial of positive degree 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 $a \in \mathbb{F}_q$, $b_1, \ldots, b_n \in \mathbb{N}$ and $f_1(x), \ldots, f_n(x) \in \mathbb{F}_q[x]$ are distinct monic irreducible polynomials. Then $ord(m(x)) = e\rho^t$, where ρ is*

the characteristic of $\mathbb{F}_q$, $e = \mathrm{lcm}(ord(f_1(x)), \ldots, ord(f_n(x)))$ *and* t *is the smallest integer such that* $\rho^t \geq \max\{b_1, \ldots, b_n\}$.

Notice that Theorem 7 depends on the knowledge of the orders of the irreducible polynomials involved in the factorization of $m(x)$. A method to find the order of an irreducible polynomial that relies on the factorization of $q^D - 1$ is reported in Lidl and Niederreiter (1994). There exist several factorization tables for numbers in this form, especially for small values of q (see Wagstaff 2002).

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 150, defined as $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ for all $(x_1, x_2, x_3) \in \mathbb{F}_2^3$. Let $y \in \mathbb{F}_2^{\mathbb{Z}}$ be a SPC of least 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 minimal 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 initialization polynomial of Eq. (20) 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 Eq. (23) $c(x)$ 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 7 the least period of preimage x is $e2^t = 12$. Figure 7 shows the actual value of the block $x_{[0,11]}$ which generates preimage x.

	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	
⋯	1	0	1	0	0	0	0	1	0	1	1	1	1	0	⋯
⋯	0	0	1	1	0	0	1	1	0	0	1	1	0	0	⋯
	y_0	y_1	y_2	y_3	y_4	y_5	y_6	y_7	y_8	y_9	y_{10}	y_{11}	y_{12}	y_{13}	

Fig. 7 Block $x_{[0,11]}$ which generates preimage $x \in F^{-1}(y)$ under rule 150, computed using Eq. (7). Notice that $(x_{12}, x_{13}) = (x_0, x_1)$ and $(y_{12}, y_{13}) = (y_0, y_1)$. Hence, for all $n \geq 12$ and $n < 0$ the preimage will periodically repeat itself

The above procedure can be adapted to the case of tth ancestors $x \in F^{-t}(y)$ by setting the characteristic polynomial in step 2 to $a(x)^t$, according to Eq. (22). Clearly, at step 3 the computation of polynomial $g(x)$ defined in Eq. (20) becomes more expensive, since the sequence σ of Eq. (18) is now a $(kt + l)$-order LRS. Additionally, the complexity of step 5 grows exponentially in the degree D of the minimal polynomial $m(x)$ computed at step 4, since it depends on the factorization of $q^D - 1$.

5.2 Periods multiplicities

As a further application of Theorem 6, we characterize the least periods of preimages with respect to the tth iterate of LBCA in the special case where $a(x)$ is irreducible and relatively prime to $b(x)$.

Our characterization result, which is analogous to Theorem 4, is the following:

Theorem 8 *Let* $F : \mathbb{F}_q^{\mathbb{Z}} \to F_q^{\mathbb{Z}}$ *be a LBCA having local rule* $f : \mathbb{F}_q^{2r+1} \to \mathbb{F}_q$, *and let* $a(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_0$ *be the characteristic polynomial associated to* f, *where* $k = 2r$, *and* $ord(a(x)) = e$. *For* $t \in \mathbb{N}$, *let* $s \in \mathbb{N}$ *be the smallest integer such that* $\rho^s \geq t$, *where* ρ *is the characteristic of* $\mathbb{F}_q$. *Further, let* $y \in \mathbb{F}_q^{\mathbb{Z}}$ *be a spatially periodic configuration of least period* $p \in \mathbb{N}$, *and let* $b(x)$ *be the minimal polynomial of sequence* v *defined as* $v_n = y_{n+r}$ *for all* $n \in \mathbb{N}$. *If* $a(x)$ *is irreducible and does not divide* $b(x)$, *then*:

- *If* $t = 1$, $F^{-t}(y)$ *is composed of one sequence with least period* p *and* $q^k - 1$ *sequences with least period* $\mathrm{lcm}(e, p)$.
- *If* $t \geq 2$, $F^{-t}(y)$ *also contains* $q^{k\rho^j} - q^{k\rho^{j-1}}$ *sequences with least period* $\mathrm{lcm}(e\rho^j, p)$ *for* $j \in \{1, \ldots, s - 1\}$, *and* $q^{kt} - q^{k\rho^s}$ *sequences with least period* $\mathrm{lcm}(e\rho^s, p)$.

Proof Recall that by Eq. (22) $a(x)^t \cdot b(x)$ is a characteristic polynomial for all $x \in F^{-t}(y)$, which means that

$$F^{-t}(y) \subseteq S(a(x)^t \cdot b(x)). \tag{24}$$

Since $a(x)$ and $b(x)$ are coprime, it holds that

$$\mathrm{lcm}(a(x)^t, b(x)) = a(x)^t \cdot b(x). \tag{25}$$

Thus, on account of Theorem 2 and Eq. (25), the following equality holds:

$$S(a(x)^t \cdot b(x)) = S(a(x)^t) + S(b(x)). \tag{26}$$

Consequently, by Eqs. (24) and (26) we conclude that $F^{-t}(y) = S(a(x)) + v$, i.e. the set of preimages of y under F^{-t} is a coset of the vector space $S(a(x)^t) + S(b(x))$. In particular, $F^{-t}(y)$ is obtained by forming all possible sums

$u+v$ for $u \in S(a(x))$. Since $a(x)$ and $b(x)$ are coprime, Theorem 3 states that the least period of $u+v$ is $\mathrm{lcm}(l,p)$, where l is the least period of u. Finally, since $a(x)$ is irreducible, Theorem 4 characterizes the possible values of l and the corresponding numbers of sequences in $S(a(x)^t)$ attaining those values of l as least period, thus concluding the proof. □

5.3 LBCA over finite rings alphabets

In this section, we assume that $A = \mathbb{Z}_m$, where $\mathbb{Z}_m$ is the finite ring of residue classes modulo $m \in \mathbb{N}$. A CA $F : \mathbb{Z}_m^{\mathbb{Z}} \to \mathbb{Z}_m^{\mathbb{Z}}$ is linear and bipermutive if and only if the leftmost and rightmost coefficients c_0 and c_{2r} of its local rule are invertible over $\mathbb{Z}_m$, i.e. $\gcd(c_0, m) = \gcd(c_{2r}, m) = 1$.

Let us first consider the case where $m = q_1 q_2$ with q_1 and q_2 relatively prime. In Cattaneo et al. (2004), the authors showed that a LBCA $F : \mathbb{Z}_m^{\mathbb{Z}} \to \mathbb{Z}_m^{\mathbb{Z}}$ is *conjugated* to the function $G : \mathbb{Z}_{q_1}^{\mathbb{Z}} \times \mathbb{Z}_{q_2}^{\mathbb{Z}} \to \mathbb{Z}_{q_1}^{\mathbb{Z}} \times \mathbb{Z}_{q_2}^{\mathbb{Z}}$, which is defined for all $(x_1, x_2) \in \mathbb{Z}_{q_1}^{\mathbb{Z}} \times \mathbb{Z}_{q_2}^{\mathbb{Z}}$ as

$$G(x_1, x_2) = (F_{q_1}(x_1), F_{q_2}(x_2)), \tag{27}$$

where F_{q_1} and F_{q_2} denote the application of rule F respectively reduced modulo q_1 and q_2. In particular, the homomorphism which maps a configuration $x \in \mathbb{Z}_m^{\mathbb{Z}}$ to its pair of *factor configurations* $(x_1, x_2) \in \mathbb{Z}_{q_1}^{\mathbb{Z}} \times \mathbb{Z}_{q_2}^{\mathbb{Z}}$ is defined as

$$\psi(x) = ([x]_{q_1}, [x]_{q_2}), \tag{28}$$

where $[x]_{q_1}$ and $[x]_{q_2}$ respectively denote componentwise reduction modulo q_1 and q_2 of configuration x. The inverse homomorphism which recomposes a pair of configurations $(x_1, x_2) \in \mathbb{Z}_{q_1}^{\mathbb{Z}} \times \mathbb{Z}_{q_2}^{\mathbb{Z}}$ into a configuration $x \in \mathbb{Z}_m^{\mathbb{Z}}$ is defined as

$$\psi^{-1}(x_1, x_2) = x_2 + q_2[(x_1 - x_2)\hat{q}_2]_{q_1}, \tag{29}$$

where addition and subtraction are performed componentwise, and $\hat{q}_2$ is the multiplicative inverse of q_2 over $\mathbb{Z}_{q_1}$. Notice that $\hat{q}_2$ exists since $\gcd(q_1, q_2) = 1$.

The conjugacy can be extended to any $m \in \mathbb{N}$ as follows. First, let $m = \prod_{i=1}^{s} \rho_i^{\alpha_i}$ be the prime power factorization of m, and let $q_i = \rho_i^{\alpha_i}$ for all $i \in \{1, \ldots, s\}$. It follows that $\gcd(q_i, q_j) = 1$ for all $i \neq j$, since ρ_i and ρ_j are distinct prime numbers. The homomorphism $\psi_s : \mathbb{Z}_m^{\mathbb{Z}} \to \mathbb{Z}_{q_1}^{\mathbb{Z}} \times \cdots \times \mathbb{Z}_{q_s}^{\mathbb{Z}}$ is defined for all $x \in \mathbb{Z}_m^{\mathbb{Z}}$ as:

$$\psi_s(x) = ([x]_{q_1}, \ldots, [x]_{q_s}). \tag{30}$$

For the inverse homomorphism, observe that $q_1, \ldots, q_s$ induce two sequences of rings $\{R_2, \ldots, R_s\}$ and $\{Q_2, \ldots, Q_s\}$, where R_j and Q_j are defined for $j \in \{2, \ldots, s\}$ as:

$$R_j = \mathbb{Z}_{q_1}^{\mathbb{Z}} \times \cdots \times \mathbb{Z}_{q_j}^{\mathbb{Z}}, \tag{31}$$

$$Q_j = \mathbb{Z}_{m_j}^{\mathbb{Z}}, m_j = \prod_{i=1}^{j} q_i. \tag{32}$$

Likewise, values $q_1, \ldots, q_s$ induce a sequence of mappings $\{\psi_2^{-1}, \ldots, \psi_s^{-1}\}$ where for $j \in \{2, \ldots, s\}$ the inverse homomorphism $\psi_j^{-1} : R_j \to Q_j$ is defined for all $(x_1, \ldots, x_j) \in R_j$ as follows:

$$\psi_j^{-1}(x_1, \ldots, x_j) = \begin{cases} \psi^{-1}(x_1, x_2), & \text{if } j = 2 \\ \psi^{-1}(\psi_{j-1}^{-1}(x_1, \ldots, x_{j-1}), x_j), & \text{if } j > 2 \end{cases} \tag{33}$$

The following theorem shows how to compute the least periods of the preimages of a spatially periodic configuration under a linear and bipermutive CA $F : \mathbb{Z}_m^{\mathbb{Z}} \to \mathbb{Z}_m^{\mathbb{Z}}$.

Theorem 9 *Let $m = \prod_{i=1}^{s} q_i$ be a positive integer where $q_i = \rho_i^{\alpha_i}$ with ρ_i prime and $\alpha_i \geq 1$ for all $i \in \{1, \ldots, s\}$. Additionally, let $F : \mathbb{Z}_m^{\mathbb{Z}} \to \mathbb{Z}_m^{\mathbb{Z}}$ be a linear bipermutive CA, and let $y \in \mathbb{Z}_m^{\mathbb{Z}}$ be a spatially periodic configuration having least period $p \in \mathbb{N}$, with $p_1, \ldots, p_s \in \mathbb{N}$ respectively being the least periods of the factor configurations $y_1 = [y]_{q_1}, \ldots, y_s = [y]_{q_s}$. Then, given a preimage $x \in F^{-1}(y)$, the least period of x is $k = \mathrm{lcm}(k_1, \ldots, k_s)$, where $k_i = h_i p_i$ and $h_i \in \{1, \ldots, q_i^{2r}\}$ for all $i \in \{1, \ldots, s\}$.*

Proof We prove only the case $m = q_1 q_2$, the general case following by induction on the values q_i. Since F is linear and bipermutive, it follows that F is conjugated to the product CA G of Eq. (27) through the isomorphism defined in Eqs. (28) and (29). As a consequence,

$$F^{-1}(y) = F^{-1}(\psi^{-1}(y_1, y_2)) = \psi^{-1}(G^{-1}(y_1, y_2)).$$

Thus, the least period of $x \in F^{-1}(y)$ equals the least period of $\psi(x) = (x_1, x_2) \in G^{-1}(y_1, y_2)$.

Remark that $P \in \mathbb{N}$ is a period of (x_1, x_2) if and only if P is a period of both x_1 and x_2. By Lemma 4, x_1 and x_2 have least period $k_1 = h_1 p_1$ and $k_2 = h_2 p_2$ respectively, with $h_1 \in \{1, \ldots, q_1^{2r}\}$ and $h_2 \in \{1, \ldots, q_2^{2r}\}$. Since $k = \mathrm{lcm}(k_1, k_2)$ is a common multiple of k_1 and k_2, it follows that k is a period of both x_1 and x_2, and thus it is a period of (x_1, x_2) as well. Let us now suppose that k is not the least period of (x_1, x_2), i.e. there exists $k' < k$ such that $\sigma^{k'}(x_1, x_2) = (x_1, x_2)$. From the discussion above, it follows that k' is a period of both x_1 and x_2 as well, and thus k' is a common multiple of k_1 and k_2, contradicting the fact that $k = \mathrm{lcm}(x_1, x_2)$. □

As a final remark, observe that if ρ is prime then the ring of residue classes $\mathbb{Z}_\rho$ is a finite field. Consequently, if m has a square-free factorization $m = \prod_{i=1}^{s} \rho_i^{\alpha_i}$ with $\alpha_i = 1$ for all $i \in \{1, \ldots, s\}$, and $F : \mathbb{Z}_m^{\mathbb{Z}} \to \mathbb{Z}_m^{\mathbb{Z}}$ is a LBCA over $\mathbb{Z}_m$, the least periods of the tth ancestors $x \in F^{-t}(y)$ can be characterized by first determining the least periods of the factor preimages $[x]_{\rho_1}, \ldots, [x]_{\rho_s}$ using Theorem 8, and then by computing their least common multiple according to Theorem 9.

6 Conclusions

In this work, we studied the relation between the periods of spatially periodic configurations of surjective CA and the periods of their preimages. In the generic surjective case the periods of preimages are multiples of the periods of their respective images. Starting from this fact, we introduced a graph-theoretic method based on the De Bruijn representation of CA that allows one to compute the least periods of preimages and their multiplicities. Successively, by focusing on the linear and bipermutive case, we showed that every LBCA preimage can be characterized as a concatenated LRS, whose characteristic polynomial is the product of the characteristic polynomials which are associated to the component sequences. From this result, we derived an algorithm to compute the least period of a single LBCA preimage and we characterized the periods of all preimages along with their multiplicities, in the case where the characteristic polynomial of the local rule is irreducible. We finally showed how to generalize these results to LBCA defined over the finite ring $\mathbb{Z}_m$ as state alphabet.

There are several directions along which the present work can be extended and improved. As a matter of fact, this paper addressed two extreme cases of the preimages periods problem: the most generic one dealing with surjective CA, for which some facts and bounds can be derived, and the case of linear and bipermutive CA over finite fields, about which every major question can be settled by leveraging on the theory of linear recurring sequences. We remark that although the latter case refers to a highly-structured and specialized class of CA, it turns out to be very useful in applications related to cryptography, namely secret sharing schemes Mariot and Leporati (2015), and to genetic regulatory networks, specifically additive flowers Formenti et al. (2014).

Still, one can consider several intermediate classes between surjective CA and LBCA, one of the most interesting being bipermutive CA equipped with *nonlinear* local rules. Notice that the *affine* case can be still solved using the tools of concatenated LRS presented throughout this paper. Specifically, let $F : \mathbb{F}_q^{\mathbb{Z}} \to \mathbb{F}_q^{\mathbb{Z}}$ be a bipermutive CA with affine local rule $f : \mathbb{F}_q^{2r+1} \to \mathbb{F}_q^{\mathbb{Z}}$ of radius r, i.e. f is a linear combination of the neighborhood cells plus a constant $a \in \mathbb{F}_q$, meaning that the LRS associated to the inverse permutation $f_{R,z}^{-1}$ is *inhomogeneous*. Rewrite Eq. (1) by substituting $n+1$ in place of n:

$$s_{n+k+1} = a + a_0 s_{n+1} + \cdots + a_{k-1} s_{n+k}. \tag{34}$$

Subtracting Eqs. (34) and (1) yields the following equalities:

$$\begin{aligned} s_{n+k+1} - s_{n+k} &= a + a_0 s_{n+1} + \cdots + a_{k-1} s_{n+k} + \\ &\quad - a - a_0 s_n - \cdots - a_{k-1} s_{n+k-1} \\ &= b_0 s_n + \cdots + b_{k-1} s_{n+k-1} + b_k s_{n+k}, \end{aligned} \tag{35}$$

where $b_0 = -a_0$, $b_i = (a_i - a_{i-1})$ for $i \in \{1, \ldots, k-1\}$, and $b_k = (1 - a_{k-1})$. Hence, a kth order inhomogeneous LRS can be expressed as a $(k+1)$th order homogeneous LRS, which allows one to apply all the results proved in this paper about concatenated LRS to the affine case as well. From the CA point of view, this means that an affine local rule of radius r can be seen as a linear rule defined on a larger neighborhood, namely $\{i - r, \ldots, i + r + 1\}$.

Clearly, the above procedure cannot be applied to generic nonlinear rules, where the preimages are generated by a *Nonlinear Feedback Shift Register* (NFSR) disturbed by the LFSR which generates the configuration y. However, this case is interesting also from the cryptographic perspective, since the concatenation of NFSR and LFSR is the main primitive upon which the stream cipher Grain is based (see Hell et al. 2008). Hence, finding a general method to study the periods of preimages of nonlinear BCA could also be useful to cryptanalyze this cipher.

Successively, one could also consider classes of surjective CA more general than bipermutive CA. The *openness* property could be an interesting starting point to investigate, since configurations of open CA have a constant number of preimages, which can be viewed as a weaker condition than bipermutivity (where each configuration has exactly q^{2r} preimages). Hence, the openness property could induce some regularities on the structure of the u-closure graph that could simplify the analysis.

Concerning generic surjective CA, we also remark that the upper bound about the time complexity for the construction of the u-closure graph via DFS is not tight. As a matter of fact, the worst case mentioned in Sect. 3.2 cannot occur in surjective CA due to their balancing property, which implies that the DFS tree associated to a vertex can be balanced only up to a certain depth. Taking into account this fact, one could derive a better upper bound on the time complexity of the graph construction procedure.

Additionally, another interesting direction for future research is to investigate the connection between LBCA

preimages and *cyclic codes*. As Lidl and Niederreiter (1994) observe, linear recurring sequences can be used to generate codewords of cyclic codes, and this process can be implemented in LFSR. In particular, if we assume that the configuration y is *finite*, the preimage computation process under the action of a LBCA is very similar to the encoding scheme described in McEliece (2002).

Finally, a further extension concerns the period of a preimage of a totally spatially periodic configuration of a given linear CA in dimension $D \geq 2$. By *totally spatially periodic configuration* (TSPC) we mean a configuration $y \in A^{\mathbb{Z}^D}$ that is periodic with respect to each vector from a set of D linearly independent vectors. Remark that, if the CA is bipermutive according to Definition 8 in Dennunzio et al. (2014), then, by Propositions 25 and 15 in the same paper a TSPC always admits a totally spatially periodic preimage (in general, this fact is not assured for multidimensional CA). This is due to the so called *slicing* construction, which allows one to cut any D-dimensional configuration into slices of dimension $D-1$, and to see the given CA as a new one-dimensional CA operating on configurations made of slices. When the given CA is restricted on periodic configurations, the slicing construction gives a one-dimensional CA on a finite alphabet and a TSPC y becomes a one-dimensional SPC. So, the study of the spatial periodicity of a totally spatially periodic preimage of y can be reduced to that for the corresponding one-dimensional preimage in the obtained one-dimensional CA. By Proposition 22 in Dennunzio et al. (2014), if the given D-dimensional CA is bipermutive, then also the obtained one-dimensional CA is bipermutive. Therefore, except for very simple cases such as those in which all vectors of the CA neighborhood are pairwise linearly dependent, to lift the results from this paper to the D-dimensional setting it is required to guarantee that, if $A = \mathbb{Z}_m$ and the given D-dimensional CA is linear, then the obtained one-dimensional CA on the alphabet $\mathbb{Z}_m^s$ (for some power s depending on the periodicity of y) is linear with respect to some group operation to be investigated. Such a group operation is necessarily different from the usual one, but should preserve the main properties of linear CA.

Acknowledgements The authors wish to thank Ilkka Törma for suggesting that Lemma 4 holds in the general surjective case, and Marco Previtali for insightful comments about the computational complexity of the u-closure graph building procedure. Further, the authors are grateful to the anonymous reviewers for their helpful comments on how to improve the paper.

References

Berlekamp ER (1967) Factoring polynomials over finite fields. Bell Syst Tech J 46(8):1853–1859

Cattaneo G, Finelli M, Margara L (2000) Investigating topological Chaos by elementary cellular automata dynamics. Theor Comput Sci 244(1–2):219–241

Cattaneo G, Dennunzio A, Margara L (2004) Solution of some conjectures about topological properties of linear cellular automata. Theor Comput Sci 325(2):249–271

Chassé G (1990) Some remarks on a LFSR "disturbed" by other sequences. In: EUROCODE '90, international symposium on coding theory and applications, Udine, Nov 5–9, 1990, Proceedings, pp 215–221

Dennunzio A, Formenti E, Weiss M (2014) Multidimensional cellular automata: closing property, quasi-expansivity, and (un) decidability issues. Theor Comput Sci 516:40–59

Durand B (1999) Global properties of cellular automata. In: Cellular automata and complex systems, Springer, pp 1–22

Formenti E, Papazian C, Scribot PA (2014) Additive flowers. In: CIBB 2014

Hedlund GA (1969) Endomorphisms and automorphisms of the shift dynamical systems. Math Syst Theory 3(4):320–375

Hell M, Johansson T, Maximov A, Meier W (2008) The grain family of stream ciphers. In: New stream cipher designs—the eSTREAM finalists, pp 179–190

Lidl R, Niederreiter H (1994) Introduction to finite fields and their applications. Cambridge University Press, Cambridge

Mariot L, Leporati A (2014) Sharing secrets by computing preimages of bipermutive cellular automata. In: Cellular automata—11th international conference on cellular automata for Research and industry, ACRI 2014, Krakow, Sept 22–25, 2014. Proceedings, pp 417–426

Mariot L, Leporati A (2015) On the periods of spatially periodic preimages in linear bipermutive cellular automata. In: Cellular automata and discrete complex systems—21st IFIP WG 1.5 international workshop, AUTOMATA 2015, Turku, June 8–10, 2015. Proceedings, pp 181–195

Massey JL (1969) Shift-register synthesis and BCH decoding. IEEE Trans Inf Theory 15(1):122–127

McEliece R (2002) The theory of information and coding. Cambridge University Press, Cambridge

Perrin D, Pin JÉ (2004) Infinite words: automata, semigroups, logic and games, vol 141. Academic, Cambridge

Sutner K (1991) De Bruijn graphs and linear cellular automata. Complex Syst 5(1):19–30

Sutner K (2010) Cellular automata, decidability and phasespace. Fundam Inform 104(1–2):141–160

Wagstaff S (2002) Cunningham project. http://homes.cerias.purdue.edu/∼ssw/cun/index.html. Accessed 22 July 2016