

On the Periods of Spatially Periodic Preimages in Linear Bipermutive CA

Automata 2015 - June 8-10 - Turku

Luca Mariot, Alberto Leporati

Dipartimento di Informatica, Sistemistica e Comunicazione
Università degli Studi Milano - Bicocca
l.mariot@campus.unimib.it, alberto.leporati@unimib.it

June 10, 2015

Outline

Problem Statement

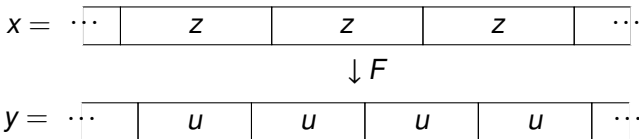
Preimages Periods in Generic BCA

Linear BCA Preimages and Concatenated LRS

Conclusions and Future Directions of Research

Spatially Periodic Preimages in Surjective CAs

- ▶ Let $F : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$ be a (CA) with $|A| = q$, and let $y \in A^{\mathbb{Z}}$ be a **spatially periodic configuration** of period $p \in \mathbb{N}$ defined by a finite word $u \in A^p$, i.e. $y = {}^\omega u^\omega$
- ▶ If F is surjective, it is known that each preimage x of y under F is spatially periodic as well [Hedlund73, Cattaneo00]



- ▶ What are the periods of preimages $x \in F^{-1}(y)$?

Assumptions and Problem Statement

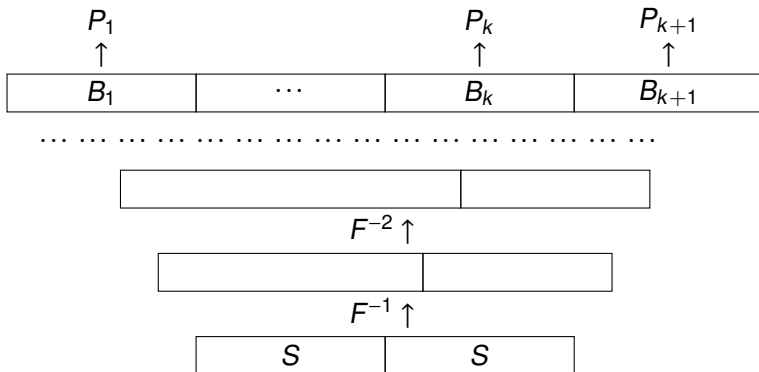
- ▶ We focus our attention on the class of bipermutive CA (BCA)
- ▶ A CA $F : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$ induced by a local rule $f : A^{2r+1} \rightarrow A$ is **bipermutive** if, by fixing the first (the last) $2r$ coordinates of f , the resulting restriction $f_{R,z} : A \rightarrow A$ ($f_{L,z} : A \rightarrow A$) is a permutation on A

Problem PBCAP - Periods of BCA Preimages

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

Motivation: BCA-based Secret Sharing Scheme

- Motivation for solving PBCAP: find the maximum number of players in a BCA-based **Secret Sharing Scheme** [Mariot14]



Outline

Problem Statement

Preimages Periods in Generic BCA

Linear BCA Preimages and Concatenated LRS

Conclusions and Future Directions of Research

Preimage Computation in BCA

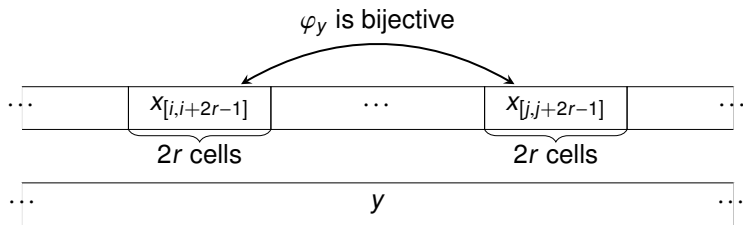
- ▶ Let $F : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$ be a BCA with local rule $f : A^{2r+1} \rightarrow A$, and let $y \in A^{\mathbb{Z}}$ be a configuration
- ▶ Additionally, let $x_{[i,i+2r-1]} \in A^{2r}$ be the $2r$ -cell block placed at position $i \in \mathbb{Z}$ of a preimage $x \in F^{-1}(y)$
- ▶ The remainder of x is determined by the following equation:

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

Preimages Periods in Generic BCA (1/2)

Lemma

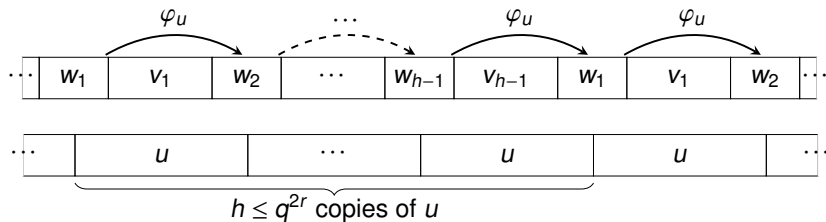
Let $F : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$ be a BCA with local rule $f : A^{2r+1} \rightarrow A$. Given a configuration $y \in A^{\mathbb{Z}}$ and $i, j \in \mathbb{Z}$, for all $x \in F^{-1}(y)$ there exists a permutation φ_y between the blocks $x_{[i, i+2r-1]}$ and $x_{[j, j+2r-1]}$.



Preimages Periods in Generic BCA (2/2)

Proposition

Let $F : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$ be a BCA with local rule $f : A^{2r+1} \rightarrow A$ 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 of x is $m = p \cdot h$, where $h \in \{1, \dots, q^{2r}\}$.



Outline

Problem Statement

Preimages Periods in Generic BCA

Linear BCA Preimages and Concatenated LRS

Conclusions and Future Directions of Research

Linear BCA

- ▶ We now assume that the alphabet is a **finite field**, that is, $A = \mathbb{F}_q$ where q is a power of a prime
- ▶ A CA $F : \mathbb{F}_q^{\mathbb{Z}} \rightarrow \mathbb{F}_q^{\mathbb{Z}}$ is *linear* if its local rule $f : \mathbb{F}_q^{2r+1} \rightarrow \mathbb{F}_q$ is a **linear combination** of the neighborhood $x \in \mathbb{F}_q^{2r+1}$:

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

for a certain vector $c = (c_0, c_1, \dots, c_{2r}) \in \mathbb{F}_q^{2r+1}$

- ▶ **Remark:** if $c_0, c_{2r} \neq 0$, then a linear CA is also bipermutive (LBCA)

Linear Recurring Sequences

- ▶ Given $a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_q$, a **linear recurring sequence** (LRS) of order k is a sequence $s = s_0, s_1, \dots$ of elements in \mathbb{F}_q satisfying

$$s_{n+k} = a_0 s_n + a_1 s_{n+1} + \dots + a_{k-1} s_{n+k-1} \quad \forall n \in \mathbb{N}$$

- ▶ A LRS is generated by a **Linear Feedback Shift Register** (LFSR)
- ▶ The **characteristic polynomial** of s is defined as

$$a(X) = X^k - a_{k-1}X^{k-1} - a_{k-2}X^{k-2} - \dots - a_0$$

- ▶ The **period** of s equals the **order** of the **minimal polynomial** $m(X)$, which depends on $a(X)$ and the initial terms of s

Characterising LBCA Preimages as Concatenated LRS

(1/2)

- ▶ Given a LBCA F , a preimage $x \in F^{-1}(y)$ of y can be considered as a LRS of order $k = 2r$ “disturbed” by y
- ▶ Let c_0, \dots, c_{2r} be the coefficients of the local rule f , and set
 - ▶ $d = c_{2r}^{-1}$
 - ▶ $a_i = -d \cdot c_i$ for $i \in \{0, \dots, 2r - 1\}$
- ▶ Moreover, define sequence v as the **r-shift** of y , that is, $v_n = y_{n+r}$ for $n \in \mathbb{N}$
- ▶ Case (a) of the preimage recurrence equation becomes

$$x_{n+k} = a_0 x_n + a_1 x_{n+1} + \dots + a_{k-1} x_{n+k-1} + d v_n \quad \forall n \geq 2r$$

Characterising LBCA Preimages as Concatenated LRS

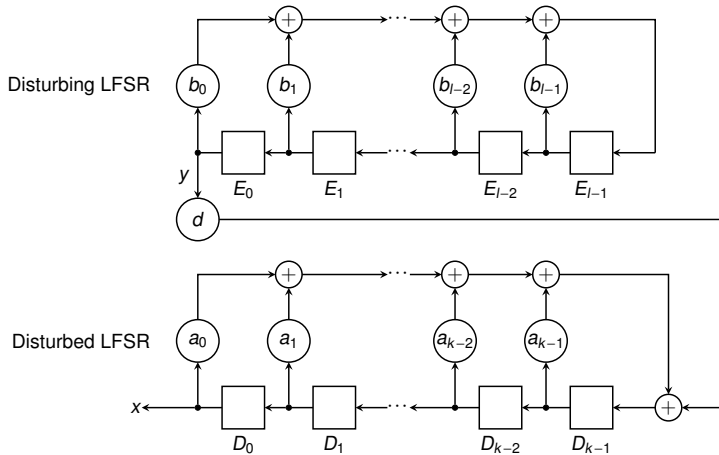
(2/2)

- ▶ **Remark:** If y is spatially periodic of period p , then sequence $v = \{v_n\}_{n \in \mathbb{N}}$ is a LRS of a certain order $l \in \mathbb{N}$:

$$v_{n+l} = b_0 v_n + b_1 v_{n+1} + \cdots + b_{l-1} v_{n+l-1} \quad \forall n \in \mathbb{N}$$

- ▶ In the worst case, v will be generated by the “trivial” LRS of order $l = p$ which cyclically shifts a word of length p
- ▶ We define x as the **concatenation** $s \leftarrow v$ of the LRS s induced by the local rule f and the LRS v which is the r -shift of y

LBCA Preimage Generation By Concatenated LFSR



Characteristic Polynomial of Concatenated LRS

Theorem

Let $s \leftarrow v$ be the concatenation of LRS s and v , and let $a(X), b(X) \in \mathbb{F}_q[X]$ be the characteristic polynomials of s and v . Then, $a(X) \cdot b(X)$ is a characteristic polynomial of $s \leftarrow v$.

Proof (Idea):

- ▶ Decompose $s \leftarrow v$ as the sum of sequence s without disturbance and the **0-concatenation** $s \leftarrow_0 v$, where the LFSR of s is initialised to 0
- ▶ Determine the **generating function** of $s \leftarrow_0 v$ [Chassé93], and then apply the fundamental identity of formal power series to find the characteristic polynomial of $s \leftarrow v$

Single Preimage Period Computation

Input: An LBCA F with local rule $f : \mathbb{F}_q^{2r+1} \rightarrow \mathbb{F}_q$, a spatially periodic configuration $y \in \mathbb{F}_q^{\mathbb{Z}}$ and a block $x_{[0,2r-1]}$ of $x \in F^{-1}(y)$

1. Find the minimal polynomial $b(X) = X^l - b_{l-1}X^{l-1} \dots - b_0$ of the LRS $v = \{v_n = y_{n+r}\}_{n \in \mathbb{N}}$
2. Set the characteristic polynomial $a(X)$ associated to f to $a(X) = X^k - a_{k-1}X^{k-1} - \dots - a_0$
3. Compute the characteristic polynomial $c(X) = a(X) \cdot b(X)$
4. Determine the minimal polynomial $m(X)$, using the characteristic polynomial $c(X)$ and the block $x_{[0,2r-1]}$
5. Compute the order of $m(X)$, and output it as the period of x

Periods Characterization for Irreducible Polynomials

Complete characterization of the periods of y when both $a(X)$ and $b(X)$ are **irreducible**:

Theorem

- ▶ Let $a(X)$ be the characteristic polynomial associated to $f_{R,Z}^{-1}$, and suppose that $a(X)$ has order e
- ▶ 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 $v = \{v_n = y_{n+r}\}_{n \in \mathbb{N}}$
- ▶ Assume that both $a(X)$ and $b(X)$ are irreducible

$\Rightarrow F^{-1}(y)$ contains one configuration of period p and $q^k - 1$ configurations of period m , where $m = \text{lcm}(e, p)$.

Outline

Problem Statement

Preimages Periods in Generic BCA

Linear BCA Preimages and Concatenated LRS

Conclusions and Future Directions of Research






Results Summary

- ▶ When the CA is only bipermutive, the preimages periods of a spatially periodic configuration y are multiple of the period of y
- ▶ In the case of LBCA, the preimages periods can be studied in terms of concatenated LRS
- ▶ Using the characteristic polynomial of the corresponding concatenated LRS, we derived an algorithm to compute the period of a single preimage
- ▶ In the particular case where both the characteristic polynomial induced respectively by the local rule and y are irreducible, we showed a characterization of the periods of all preimages of y

Future Directions

- ▶ Generalise the results with respect to the t -th iterate F^t
- ▶ Consider **nonlinear** rules. In this case, the preimage is generated by a **Nonlinear Feedback Shift Register** (NFSR) disturbed by a LFSR
- ▶ Results on the nonlinear case could have an impact on the cryptanalysis of the stream cipher Grain [Hell08]
- ▶ Investigate the preimages periods under the action of generic surjective CA and multi-dimensional CA

References

-  Cattaneo, G., Finelli, M., Margara, L.: Investigating topological chaos by elementary cellular automata dynamics. *Theor. Comp. Sci.* 244, 219–241 (2000)
-  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)
-  Hedlund, G.A.: Endomorphisms and Automorphisms of the Shift Dynamical Systems. *Mathematical Systems Theory* 7(2), 138–153 (1973)
-  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)
-  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)