Periodicity in Additive Cellular Automata

Lieven Le Bruyn*

Dpt. Mathematics and Computer Sciences
University of Antwerp
UIA, Belgium

December 1987 - 87-25

Abstract.

We study the relation between spatial and temporal periods of any infinite additive one-dimensional cellular automata. The connection with the period of the generating polynomial gives an efficient algorithm to compute $\alpha(n)$.

Key Words and phrases.

Parallelprocessing, additive cellular automata, periodic configurations.

Subject Classification.

68D20, 68D30, 13M10.

* Research associate of NFWO (Belgium)

Periodicity in Additive Cellular Automata

Lieven Le Bruyn
Dept. of Mathematics and Computer Sciences
University of Antwerp, UIA, Belgium

1. Introduction

Cellular automata are structures evolving on a lattice according to a definite deterministic local law. They were first introduced by Von Neumann [12] and Ulam [11] as examples of simple structures presenting some of the features of life. Recently, there is some renewed interest in them due to the popularity of artificial intelligence and parallel computing on the one hand and their suitability to simulate complex physical phenomena on the other hand. We refer the reader to [8], [9], [13-14] for more details.

Some cellular automata have a simplifying additivity property, i.e. their local transition rules are linear. A class of finite additive cellular automata has been studied in a recent paper by Martin, Odlyzko and Wolfram [8]. A general framework for additive cellular automata will be presented in a joint paper with M. Van den Bergh [6].

In this paper we concentrate on the problem for a configuration to be periodic in time for any type of infinite onedimensional additive cellular automaton. In a recent paper Cordovil, Dilao and da Costa [4] proved that such configurations necessarily have to be periodic in space, too. The generic spatial periodicity for a configuration of temporal period n is denoted by $\alpha(n)$. In [4] a very time consuming algorithm was given to compute $\alpha(n)$. In this paper we show that $\alpha(n)$ is precisely the period of the polynomial $\tau^n - 1$ as defined in [2]. Berlekamps algorithm to compute the period of any polynomial is recalled and adapted to the special case of interest to us. Besides providing an efficient algorithm, it also gives short arguments for some of the results from [4] and explains the large numerical values for $\alpha(n)$ in the tables of [4].

Personally, it came as a surprise that deep number theoretical problems such as the factorization of generalized Mersenne numbers arise naturally from the study of cellular automata.

2. The problem

Because it does not complicate our life, we will generalise the setting of [4] to any finite field. As remarked above a general treatment of additive or linear cellular automata will be presented in [6].

Let $\mathbb{F}_q$ be the finite field of characteristic p on $q = p^r$ for some $r \in \mathbb{N}$ elements. Of course, $\mathbb{F}_z = \{0,1\}$ is the case of prime interest to cellular automatists. With $\mathbb{F}_q^{\mathbb{Z}}$ one denotes the vectorspace of $r \in \mathbb{Z}$ elements. Of course, $\mathbb{F}_2 = \{0,1\}$ is the case of prime interest On $\mathbb{F}_q^{\mathbb{Z}}$ we have the shift operator $\sigma : \mathbb{F}_q^{\mathbb{Z}} \rightarrow \mathbb{F}_q^{\mathbb{Z}}$ defined by $(\sigma x)_i = x_{i+1}$.

With $\mathbb{F}_q[\sigma, \sigma^{-1}]$ we will denote the $\mathbb{F}_q$-algebra of linear functions finitely generated by the automorphisms $\{\sigma^r : r \in \mathbb{Z}\}$. For every $\tau \in \mathbb{F}_q[\sigma, \sigma^{-1}]$ we call the ordered pair $= (\mathbb{F}_q^{\mathbb{Z}}, \tau)$ the onedimensional infinite cellular automaton defined over $\mathbb{F}_q$ with linear time evolution rule τ, that is if the configuration at time t is given by $x(t) = \{x(t)_i : i \in \mathbb{Z}\}$ then at the next clock pulse we have $x(t+1)$ where $x(t+1)_i = (\tau.x(t))_i$. Some well known of these cellular automata (over $\mathbb{F}_2$) are Wolfram's rule 90 where $\tau = \sigma + \sigma^{-1}$ or rule 150 where $\tau = \sigma^{-1} + 1 + \sigma$. Generalizing [4,def 2.2] we define

Definition : Let $\mathcal{A} = (\mathbb{F}_q^{\mathbb{Z}}, \tau)$ be an additive cellular automaton as defined above and let $n \geq 1$ be a natural number. We say that a configuration x of $\mathcal{A}$ has temporal period n if and only if $\tau^n x = x$. In this case we say that x is a periodic orbit of $\mathcal{A}$. The spatial period $\alpha(x)$ of the configuration x is defined to be the smallest natural number r such that $x_{i+r} = x_i$ for all $i \in \mathbb{Z}$ if it exists or $\alpha(x) = \infty$ other wise. With $\alpha(n)$ we denote the largest $\alpha(x)$ from all the configurations x of $\mathcal{A}$ with temporal period n.

We will now briefly discuss the Cordovil-Dilao-da Costa algorithms to compute

$\alpha(n)$. If $\tau = \Sigma_{i=m'}^{m"} \lambda_i \sigma^i$ with $\lambda_{m'}, \lambda_{m"} \neq 0$ they denote $s(\tau) = m" - m'$ and define $\gamma(\tau) = s(\tau + 1)$ if $\tau + 1 \neq 0$ and $\gamma(1) = 1$. Then $\gamma(\tau)$ is called the breath of the transition rule τ. Suppose x is a configurat ion of $\mathcal{A} = (\mathbb{F}_2^{\mathbb{Z}}, \tau)$ with temporal period n. Then from [4, 2.3.1] the entries are uniquely determined by the $\gamma(\tau^n)$ entries $\{X_0, X_1, ..., X_{\gamma(\tau^n)-1}\}$. Let $X' \in \mathbb{F}_2^{\gamma(\tau^n)}$ such that for every $0 \leq i \leq \gamma(\tau^n) - 1$ we have $(X')_i = X_i$ then there exists a linear endomorphism of $\mathbb{F}_2^{\gamma(\tau^n)}$, say L, such that for every $m \in \mathbb{Z}$ and every $0 \leq i \leq \gamma(\tau^n) - 1$ we have in the canonical basis of $\mathbb{F}_2^{\gamma(\tau^n)}$: $(L^m x')_i = x_i$. With respect to this basis the matrix corresponding to L has the form

$$A = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & 0 & \ldots & 0 & a_2 \\ \vdots & \vdots & \vdots & & & \vdots \\ 0 & 0 & 0 & \ldots & 1 & a_{\gamma(\tau^n)-1} \end{bmatrix}$$

where the a_i can be determined from τ by [4 , 2.3.1.]. One says that A (resp. L) is the companion matrix (resp. linear application) of the configurations of $\mathcal{A}$ with temporal period n. The main result [4, Th. 2.10] then states that $\alpha(n)$ is the smallest positive natural number such that $A^{\alpha(n)} = I$ the identity matrix. Moreover, if d divides n then by [4, Cor. 2.11] $\alpha(d)$ divides $\alpha(n)$ and if $n = 2^r d$ then $\alpha(n) = 2^r \alpha(d)$.

Cordovil, Dilao and da Costa then risk the conjecture that there are no other properties for $\alpha(n)$, i.e. there are no short cuts in the algorithm for general τ and general n other than those coming from the divisibility properties mentioned above.

3. An efficient algorithm to compute $\alpha(n)$

In this section we will reduce the problem of finding periodic configurations to that of finding zero divisors in finite groupalgebra over $\mathbb{F}_q$. This will allow us to identify $\alpha(n)$ with the period of a polynomial.

Let $X = \{X_i : i \in \mathbb{Z}\}$ be a configuration of an additive infinite onedimensional cellular automaton $\mathcal{A} = (\mathbb{F}_q^{\mathbb{Z}}, \tau)$ which is temporal cyclic of order n and spatial temporal of period $\alpha(x) \geq \gamma(\tau^n)$. Since x is totally determined by its entries $\{X_0, X_1, ..., X_{\alpha(X)-1}\}$ we can consider it as an element of the finite group algebra $\mathbb{F}_q[\mathbb{Z}/\alpha(X)\mathbb{Z}] = \mathbb{F}_q[\sigma]/(\sigma^{\alpha(X)} - 1)$. Since X is of temporal period n and $\alpha(X) \geq \gamma(\tau^n)$, then temporal behaviour of X is fully determined by its representant in

$\mathbb{F}_q[\mathbb{Z}/\alpha(X)\mathbb{Z}]$ with respect to multiplication with τ in $\mathbb{F}_q[\mathbb{Z}/\alpha(X)\mathbb{Z}]$ where we denote by τ the image of $\sigma^{-m'}\tau$ in $\mathbb{F}_q[\mathbb{Z}/\alpha(X)\mathbb{Z}]$. The condition of being temporal period of order n then translates into $(\tau^n - 1).X = 0$ in $\mathbb{F}_q[\mathbb{Z}/\alpha(X)\mathbb{Z}]$. Since the structure of these group algebras can be totally described (e.g. in case $p \not| \alpha(X)$ it is just the direct sum of extension fields of $\mathbb{F}_q$ corresponding to the irreducible factors of the cyclotomic polynomial $\sigma^n - 1$; in general one first has to divide out the Jacobson radical, see e.g. [1] for more details) it is perfectly possible to describe all temporal period n configurations with spatial period $\alpha(X)$.

However, if we do not want to know all periodic configuration, but only $\alpha(n)$ we do not really need to know the structures of the group algebras $\mathbb{F}_q[\mathbb{Z}/m\mathbb{Z}]$ for $m \in \mathbb{N}$.

Following [2, p.150] we define the period of a polynomial $\gamma(\sigma) \in \mathbb{F}_q[\sigma]$ with coefficients in the finite field $\mathbb{F}_q$ to be the smallest natural number j such that $\gamma(\sigma)$ divides $\sigma^j - 1$ in the unique factorization domain $\mathbb{F}_q[\sigma]$. In view of the foregoing remarks it is then easy to see that :

THEOREM : Let $\mathcal{A} = (\mathbb{F}_q^{\mathbb{Z}}, \tau)$ be a cellular automaton defined over the finite field $\mathbb{F}_q$ with transition function $\tau = \Sigma_{i=m'}^{m}, \lambda_i \sigma^i$ and denote $t = \sigma^{-m'}\tau \in \mathbb{F}_q[\sigma]$. Then, for any natural number n the spatial period parameter $\alpha(n)$ coincides with the period of the polynomial $t^n - 1$ in $\mathbb{F}_q[\sigma]$.

Fortunately, there is an efficient algorithm to compute the period of any polynomial [2, ch.6] due to E. Berlekamp. For the convenience of the reader we will briefly outline the main steps.

Suppose that $\gamma(\sigma) = \Pi_{i=1}^{k}(f_i(\sigma))^{m_i}$ is a factorization of the polynomial $\gamma(\sigma)$ in irreducible factors. Assume that the irreducible polynomial $\gamma_i(\sigma)$ has period n_i over $\mathbb{F}_q$ (which is of characteristic p), then the period of $\gamma(\sigma)$ is the least common multiple of the n_i multiplied with the least power of p which is not less than any of the m_i, [2,th 6.21]. So, the period of a polynomial is determined by the periods of its irreducible factors. Using Berlekamps factorization algorithm [2, 6.1] or [5] it is perfectly possible to factorize binary polynomials of degree ≤ 10.000. Since we only need to factorize polynomials of the form $t^n - 1$ in $\mathbb{F}_q[\sigma]$ we can speed up things by first factorizing the cyclotomic polynomial $\sigma^n - 1$ which can be done very fast by considering polynomials of the form $g = \Sigma_{k \in K}\sigma^k$ where K is any set of numbers which is closed under multiplication by q modulo n and computing by Euclid's algorithm the greatest common divisor of $\sigma^n - 1$ and $g - s$ for $s \in \mathbb{F}_q$, see

[2, 6.4] for more details. The case $\mathbb{F}_q = \mathbb{F}_2$ is especially easy to handle. Once we know a factorization of $\sigma^n - 1$ we replace σ in the factors by τ and factorize these polynomials further.
Since $\sigma^d - 1$ divides $\sigma^n - 1$ iff d/n and since $\tau^{p^a d} - 1 = (\tau^d - 1)^{p^a}$ we immediately obtain from the above discussion the following generalization of [4, Cor.2.11].

COROLLARY : Let $\mathcal{A} = (\mathbb{F}_q^{\mathbb{Z}}, \tau)$ be an infinite onedimensional additive cellular automaton defined over the finite field $\mathbb{F}_q$ where $q = p^r$ and let d and n be two positive natural numbers. Then, if $d/n, \alpha(d)/\alpha(n)$; in particular $\alpha(1)$ divides $\alpha(n)$. Moreover, if $n = d$ and $\gamma(\tau) \geq 1$ then $\alpha(n) = p^a \alpha(d)$.

We still have to determine the period of an irreducible polynomial $f(\sigma)$ in $\mathbb{F}_q[\sigma]$. Since the period of $f(\sigma)$ is equal to the multiplicative order of its roots it has to be a factor of $q^m - 1$ if the degree of $f(\sigma)$ is m. Therefore, the first step is to find a complete factorization of the integer $q^m - 1 = \prod_i p_i^{e_i}$ into prime numbers p_i. We can then determine whether the period is a multiple of $p_i^{e_j}$ by calculating the residue of $\sigma^{(q^m-1)/p_i^{e_j}}$ modulo $f(\sigma)$. This can be implemented as in [2,6.2]. Repeating this procedure for all prime factors of $q^m - 1$ we can determine the period of $f(\sigma)$.
Note that the hardest part in this algorithm is to find the complete factorization of the generalized Mersenne numbers $q^m - 1$. At this moment, there are very powerfull algorithms to factorize large (say about a hundreth digits) numbers e.g. by Lenstra's factorization method using elliptic curves [7], see also [10] for a discussion of other algorithms. However, again there is a considerable shortcut in the case of prime interest to us, that is $\mathbb{F}_q = \mathbb{F}_2$. Then, we have to factorize $2^m - 1$. Over the years a huge amount of knowledge is accumulated about the factorization of these Mersenne numbers. For instance Brillhart and Selfridge [3] gave already in 1967 the complete factorization of all such numbers with $m \leq 136$. Since then the factorization tables are significantly extended, see for example [10,tables] which contain the complete factorizations for $m \leq 260$. So, we can bypass this problem by referring to the tables. Sometimes, $2^m - 1$ is itself a prime number (a so called Mersenne prime) hence the period has to be $2^m - 1$ explaining some of the large values of $\alpha(n)$ in the tables of [4].
It came as a surprise to me that determining the spatial parameter $\alpha(n)$ of infinite onedimensional additive cellular automata for moderatly large values of n needs deep number theoretical results such as the factorization of generalized Mersenne numbers $q^m - 1$.

References

[1] : Alperin J. ; Local representation theory , Cambridge Lect Notes (1985)

[2] : Berlekamp E. ; Algebraic coding theory , Mc Graw Hill series in system science (1968)

[3] : Brillhart J.,Selfridge J.L. ; Some factorizations of $2^n + / -1$ and related results, Math.Comp. 21 (1967) 87-96

[4] : Cordovil R.,Dilao R.,Noronha da Costa A. ; Periodic orbits for additive cellular automata, Discrete Comp. Geometry 1 (1986) 277-288

[5] : Knuth D. ; The art of computer programming vol 2

[6] : Le Bruyn L., Van den Bergh M. ; Linear cellular automata , an algebraic treatment , in preparation

[7] : Lenstra H.W. ; Factoring integers with elliptic curves, Ann. of Math. to appear

[8] : Martin O.,Odlyzko A.,Wolfram S. ; Algebraic properties of cellular automata, Comm. Math. Phys. 93 (1984) 219-258

[9] : Pries W.,Thanailakis A.,Card H.C. ; Group properties of cellular automata and VLSI applications, IEEE Trans Comp C-35 (1986) No 12,1013-1024

[10] : Riesel, Prime numbers and computer methods for factorization, Birkhauser (1985)

[11] : Ulam S. ; Some ideas and prospects in biomathematics, Ann. Rev. Biomath. 255 (1974)

[12] : Von Neumann J. ; in 'Theory of Self-reproducing automata' (Burks A.W. ed) Univ of Illinois Press Urbana (1966)

[13] : Wolfram S. ; Statistical mechanics of cellular automata, Rev. Mod. Phys. 55 (1983) 601-644

[14] : Wolfram S. ; Computation theory of cellular automata, Comm.Math.Phys. 96 (1984) 15-57