INSTITUTUL DE MATEMATICA
AL ACADEMIEI ROMANE

PREPRINT SERIES OF THE INSTITUTE OF MATHEMATICS
OF THE ROMANIAN ACADEMY

ISSN 0250 3638

A CELLULAR AUTOMATA ON A TORUS

by

C. I. COBELI, M. CRASMARU and A. ZAHARESCU

Preprint nr. 12/1998

BUCURESTI

A CELLULAR AUTOMATA ON A TORUS

by

C. I. COBELI*, M. CRASMARU** and A. ZAHARESCU***

August, 1998

---

* Mathematics Research Institute of Mathematics of the Romanian Academy, P.O. Box 1–764, RO–70700 Bucharest, Romania

e–mail: ccobeli@stoilow.imar.ro

** Vatra Dornei, 5975, Romania,

e–mail: mi@assist.cccis.ro

*** Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA and Mathematics Research Institute of Mathematics of the Romanian Academy P. O. Box 1–764, Bucharest, 70700, Romania,

e–mail: azah@math.mit.edu

A CELLULAR AUTOMATA ON A TORUS

BY CRISTIAN IOAN COBELI, MARCEL CRÂŞMARU AND ALEXANDRU ZAHARESCU

ABSTRACT. In this paper we prove a conjecture of Brian Thwaites concerning the evolution function of a certain cellular automata on a torus.

In the seventies, when more and more people had access to personal computers, John Conway's game of life became very popular. Since then, the study of this type of game grew up into the theory of cellular automata. In [5] (see also [2, page 311]) Brian Thwaites proposes a conjecture which leads to such a cellular automata.

Thwaites's conjecture is: *Given any finite sequence of rational numbers, take the positive differences of successive members (including differencing the last member with the first); iteration of this operation eventually produces a set of zeros if and only if the size of the set is a power of 2.*

Our aim in this note is to prove that Thwaites conjecture holds true.

Let $a_0, \ldots, a_{d-1}$ be the given d rational numbers, which we may think as the heights of d poles situated around a circle. These numbers are replaced at the next step by d rational numbers given by the difference in heights of successive poles, and then the process is repeated. Being an iteration of the same operation, it resembles Conway's life game.

Being an iteration of the same operation, it resembles Conway's life game. For now the field of play is a 1-dimensional torus and since, as we will see only finitely many numbers which depend on the initial configuration are involved, in the long run, we will end up with a cycle. Finding the lengths of these cycles, which depend mostly on d—the size of the torus, is the interesting problem. In other words, if d is a power of 2, Thwaites conjecture says that the length of any cycle is equal to 1 (the shortest possible) and in section 2 we indicate necessary and sufficient properties for d which will guarantee that the length of any cycle is either short or long. We discovered that there is a connection between this life game of Thwaites and arithmetic in cyclotomic fields. In section 2 we exploit this connection in order to obtain information

on the lengths of the above cycles. A criterion which tests if a given integer is a period for this evolution function is given in section 3.

1. Proof of Thwaites conjecture

We begin by making some notations which set the problem in a clearer framework. Let $a_0, \dots, a_{d-1}$ be the given rational numbers. For convenience, we *unpack* this ordered set of numbers by associating to it the infinite sequence $(a_0, a_1, \dots)$, where the components are defined by

$$a_k = a_{k+d} \qquad \text{for} \quad k \geq 0. \tag{1}$$

Let us denote by $\mathbb{Q}_d$ and by $\mathbb{N}_d$ the set of all the sequences with rational and natural components respectively, satisfying (1). The evolution function $\phi\colon \mathbb{Q}_d \to \mathbb{Q}_d$ is defined by $\phi(a_0, a_1, \dots) = (a'_0, a'_1, \dots)$, where

$$a'_k = |a_k - a_{k+1}| \qquad \text{for} \quad k \geq 0. \tag{2}$$

With these notations, Thwaites conjecture says that given an arbitrary sequence $(a_0, a_1, \dots) \in \mathbb{Q}_d$, then $\phi^{(n)}(a_0, a_1, \dots) = (0, 0, \dots)$ for all sufficiently large $n \in \mathbb{N}$ iff d is a power of 2. (Here $\phi^{(n)}$ is the repeated composition of n samples of ϕ.)

Let's note that all the components of $\phi^{(n)}(a_0, a_1, \dots)$ are nonnegative if $n \geq 1$ and by multiplying all the components of the initial sequence $(a_0, a_1, \dots)$ by the least common multiple of their denominators (note that only finitely many of them are distinct), we may assume that the evolution function has the domain and the range equal to $\mathbb{N}_d$.

Let $M = \max\{a_0, \dots, a_{d-1}\}$. By the definition of ϕ, it is easy to see that all the components of $\phi^{(n)}(a_0, a_1, \dots)$ are integers belonging to $[0, M]$. Because there are only finitely many such periodic sequences in $\mathbb{N}_d$, it follows that given any initial configuration $(a_0, a_1, \dots)$, the repeated application of the evolution function will eventually produce a cycle of sequences which keep repeating.

The next lemma shows that after sufficiently many steps we always end up with sequences with components having at most 2 distinct values.

Lemma 1. *Let d be a positive integer, $(a_0, a_1, \dots)$ a sequence of nonnegative integers satisfying (1) and suppose the function ϕ is defined as above. Then there is a positive integer a such that for sufficiently large n all the components of $\phi^{(n)}(a_0, a_1, \dots)$ belong to $\{0, a\}$.*

Proof. The proof is obtained by (inverse) induction. Let us look at a portion of the sequence of numbers we get at some step. We write them on a line as follows:

$$\ldots, b, \underbrace{0, \ldots, 0}_{s \text{ zeros}}, \underbrace{m, \ldots, m}_{u \text{ numbers}}, \underbrace{0, \ldots, 0}_{t \text{ zeros}}, c, \ldots \tag{3}$$

Here m is the maximum of the all our numbers at this step, b and c are nonzero, $m > b$, $m > c$, $s \geq 0$, $t \geq 0$, $u \geq 1$ and the part of the sequence that begins and ends with m contains only 0's or m's. Then, after at most $s + u + t$ steps, the maximum of the numbers that are produced out by this portion of the sequence will be $\leq \max\{m - b, m - c\} < m$. Of course at a given step the sequence of numbers we obtain might contain several subsequences of the form (3), but what happens is that after at most d steps the maximum of the numbers at that step will be strictly less than m.

The lemma then follows by induction.

By multiplying all the components of the initial configuration by a^{-1}, where a is given by Lemma 1, we may assume that after sufficiently many steps all the components of the sequences we obtain are 0 or 1. Then our operation (taking the positive differences of successive members of the sequence) is nothing else than addition in the group $(\mathbb{Z}/2\mathbb{Z}, +)$.

Now there is a transparent way to generalize the game by replacing $(\mathbb{Z}/2\mathbb{Z}, +)$ by a more general finite monoid and also by playing on a multidimensional field. The operation in this case is to take the sum (or product if the multiplicative notation is used) of the closest neighbors.

We only mention here that if we keep the same group $(\mathbb{Z}/2\mathbb{Z}, +)$, but play on a multidimensional torus, then we eventually obtain a sequence of zeros if and only if the size of one of the dimensions is a power of 2. This can be showed by following the same lines of proof.

Returning to our problem, let us observe that by starting with an arbitrary sequence of 0's and 1's, by applying repeatedly the evolution function, we obtain the following table which is filled with the beginning of the sequences obtained in the first few iterations.

Step	1	2	3	$\cdots$
0.	a_0	a_1	a_2	$\cdots$
1.	$a_0 + a_1$	$a_1 + a_2$	$a_2 + a_3$	$\cdots$
2.	$a_0 + a_2$	$a_1 + a_3$	$a_2 + a_4$	$\cdots$
3.	$a_0 + a_1 + a_2 + a_3$	$a_1 + a_2 + a_3 + a_4$	$a_2 + a_3 + a_4 + a_5$	$\cdots$
4.	$a_0 + a_4$	$a_1 + a_5$	$a_2 + a_6$	$\cdots$
5.	$a_0 + a_1 + a_4 + a_5$	$a_1 + a_2 + a_5 + a_6$	$a_2 + a_3 + a_6 + a_7$	$\cdots$
6.	$a_0 + a_2 + a_4 + a_6$	$a_1 + a_3 + a_5 + a_7$	$a_2 + a_4 + a_6 + a_8$	$\cdots$
7.	$a_0 + a_1 + \cdots + a_7$	$a_1 + a_2 + \cdots + a_8$	$a_2 + a_3 + \cdots + a_9$	$\cdots$
8.	$a_0 + a_8$	$a_1 + a_9$	$a_2 + a_{10}$	$\cdots$
9.	$a_0 + a_1 + a_8 + a_9$	$a_1 + a_2 + a_9 + a_{10}$	$a_2 + a_3 + a_{10} + a_{11}$	$\cdots$
10.	$a_0 + a_2 + a_8 + a_{10}$	$a_1 + a_3 + a_9 + a_{11}$	$a_2 + a_4 + a_{10} + a_{12}$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

Now it is easy to prove by induction that in the above table if $d = 2^m$ then the d-th row (and consequently all that follow after it) contains only $0'$s. Also, there are sequences of $0'$s and $1'$s, namely those containing an odd number of $1'$s, for which on the $(d-1)$-th row all the numbers are equal to 1. Thus, if d is a power of 2 and we start with an arbitrary set of $0'$s and $1'$s, then the process will produce $0'$s in d steps and only for particular a_k's in less then d steps.

The outcome in the case $d \neq 2^m$ can be also deduced easily by induction. Thus, if we start for example with the periodic sequence given by $a_0 = 1$ and $a_k = 0$ for $1 \leq k \leq d-1$, then 1 will always be the first number on the rows representing the steps of order a power of 2. Therefore, if d is not a power of 2 then there are sequences which will never produce a set of $0'$s.

We summarize our result in the following theorem which proves the Thwaites conjecture.

Theorem 1. *Let d be a positive integer and suppose the evolution function ϕ is defined as above. Then there is a rational number $r > 0$ such that the repeated application of ϕ to any initial sequence of rational numbers $(a_0, a_1, \dots)$ satisfying (1) will eventually produce a cycle of sequences with the property (1) with all their components in $\{0, r\}$. Moreover, the cycle will contain only the sequence $(0, 0, \dots)$ independently on the initial sequence if and only if d is a power of 2.*

2. The length of cycles

We assume in this section that the evolution function ϕ is defined on $\mathbb{U}_d$, where $\mathbb{U}_d$, is the set of all the sequences with components in

$\{0,1\}$, satisfying (1). This is not restrictive as we saw above and also has the advantage that it makes ϕ to be additive.

Theorem 1 shows that if d is a power of 2 then the length of any cycle is equal to 1. Suppose from now on that d is not a power of 2.

It is not difficult to prove by induction that $j-$th component of $\phi^{(n)}(a_0, a_1, \dots)$ is equal to

$$\sum_{k=0}^{n} \binom{n}{j} a_{j+k} \pmod 2.$$

Since ϕ is additive we need to see only the evolution of the sequence $\mathbf{e_0}$ with the components given by

$$\begin{cases} a_j = 1 & \text{if } j \equiv 0 \pmod d \\ a_j = 0 & \text{if } j \not\equiv 0 \pmod d \end{cases}.$$

Denote

$$S_d(n,r) = \sum_{\substack{1 \le k \le n \\ k \equiv r \pmod d}} \binom{n}{k}.$$

Then

$$\phi^{(n)}(\mathbf{e_0}) = \big(S_d(n,0),\ S_d(n,-1),\ S_d(n,-2),\ \dots\big) \pmod 2.$$

Therefore our problem is to study the behavior of the sums $S_d(n,r)$ (mod 2).

Let p be an odd prime divisor of d. The sum $S_p(n,r)$ can be written as

$$S_p(n,r) = S_d(n,r) + S_d(n,r+p) + S_d(n,r+2p) + \cdots + S_d\big(n, r + (\tfrac{d}{p} - 1)p\big).$$

This shows that if we prove that for any $n \ge 1$ there is an r such that $S_p(n,r) \not\equiv 0 \pmod 2$ then for no $n \ge 1$ we have that $S_d(n,r) \equiv 0 \pmod 2$ for all r.

For the sums with $d = p$ we prove the following:

Theorem 2. *Let p be an odd prime, ζ a primitive root of 1 of order p and $\mathcal{J}$ a prime ideal in $\mathbb{Z}[\zeta]$ which divides 2. Then, for any $n \ge 1$ which is a multiple of $\big(\mathbf{Norm}(\mathcal{J}) - 1\big)$, $S_p(n,r)$ is even if and only if $r \equiv 0 \pmod p$.*

Proof. Consider the polynomial $f(X) = (1+X)^n$ and let

$$f_{(n,r)}(X) = \frac{1}{p} \sum_{b \pmod p} \zeta^{-br} f(\zeta^b X).$$

Then $f_{(n,r)}(X)$ will pick up from $f(X)$ only the terms X^k with $k \equiv r \pmod p$. It follows that

$$f_{(n,r)}(1) = S(n,r).$$

Hence:

$$pS(n,r) = \sum_{b \pmod p} \zeta^{-br}(1+\zeta^b)^n. \tag{4}$$

Now since p is odd $S(n,r)$ will be even exactly when the right-hand-side of (4) is even. Note that for $b \equiv 0 \pmod p$ the corresponding term in the right-hand-side of (4) equals 2^n, which is even for $n > 0$. We are left then in (4) with the sum of terms with $1 \leq b \leq p-1$.

Let $\mathcal{J}$ be a prime ideal in $\mathbb{Z}[\zeta]$ which divides 2. Since the right-hand-side of (4) is a rational integer, it will be divisible by 2 if and only if it is divisible by $\mathcal{J}$. We know that $1+\zeta$ is a unit in $\mathbb{Z}[\zeta]$ (see Borevich-Shafarevich [1]) and so is any of its conjugates $1+\zeta^b$, $1 \leq b \leq p-1$. In particular none of them lies in $\mathcal{J}$. Now from the Little Fermat Theorem in $\mathbb{Z}[\zeta]$ it follows that

$$(1+\zeta^b)^{(\mathbf{Norm}(\mathcal{J})-1)} \equiv 1 \pmod{\mathcal{J}}.$$

for any $1 \leq b \leq p-1$. Then, for any n which is a multiple of $(\mathbf{Norm}(\mathcal{J})-1)$ we have:

$$(1+\zeta^b)^n \equiv 1 \pmod{\mathcal{J}}.$$

Therefore for such values of n the right-hand-side of (4) is

$$\equiv \sum_{1 \leq b \leq p-1} \zeta^{-br} \pmod{\mathcal{J}}.$$

If $r \equiv 0 (\text{mod } p)$ this last sum equals $p-1$, which is $\equiv 0 (\text{mod } \mathcal{J})$.

If $r \not\equiv 0 (\text{mod } p)$ then the sum equals -1, which is $\not\equiv 0 (\text{mod } \mathcal{J})$.

In conclusion, for any $n > 0$ which is a multiple of $(\mathbf{Norm}(\mathcal{J})-1)$, $S(n,r)$ is even if and only if $r \equiv 0 (\text{mod } p)$, which concludes the proof of the theorem.

Let's translate this in terms of our problem. Suppose we start with the initial configuration $\mathbf{e}_0$. Then after n steps, where n is a multiple of $(\mathbf{Norm}(J)-1)$, the outcome produced by the evolution function will be equal to $(1,1,1,\dots,)-\mathbf{e}_0$. In particular, this *"population"* never *"dies"*, so we proved again Thwaites conjecture for d which is not a power of 2. Moreover, we now know that the length of the cycle corresponding to the initial configuration $\mathbf{e}_0$ has to be a divisor of $(\mathbf{Norm}(J)-1)$.

There is a simple formula which can be used to compute this number $(\mathbf{Norm}(J)-1)$ in terms of p. It is known that 2 splits in $\mathbb{Z}[\zeta]$ into a

product $\mathcal{J}_1 \dots \mathcal{J}_r$ of distinct prime ideals. The norm of each of these ideals is 2^s, where s is the order of 2 mod p. Also $rs = p - 1$. Thus the number $(\mathbf{Norm}(\mathcal{J}) - 1)$ is the smallest number of the form $2^s - 1$ which is a multiple of p.

Note that from the additivity property of the evolution function ϕ it follows that $2^s - 1$ is a period for the corresponding life problem for any initial configuration with components 0 or 1.

Two more remarks:

1. The chain produced by an initial configuration with components 0 or 1 is not necessarily periodic from the beginning. It is periodic after we restrict to the subchain: $n \geq 1$. For $n = 0$ the configuration might not be the same as for $n = 2^s - 1$. Indeed, recall the term 2^n coming from the term $b = 0$ above, which adds a 1 to each component of the configuration. That's why, if we start with $\mathbf{e_0}$ in $2^s - 1$ steps we get $(1, 1, \dots) - \mathbf{e_0}$.

More generally, by the same additivity property, we deduce that if we start with a configuration from $\mathbb{U}_p$ which has k of the first p components equal to 1 and the other $p - k$ equal to 0 then, after $2^s - 1$ steps we get a a configuration which either equals the initial one, and this happens if k is even, or equals $(1, 1, \dots)$ minus the initial configuration and this happens if k is odd.

2. One can ask about *short* and *long* periods.

Short periods: $2^s - 1$ is always a multiple of p; it equals p when p is a Mersene prime. One doesn't know if there are infinitely many such primes. The first Mersenne primes are 3, 7, 31, 127, ... Note that for such a prime number p it follows from our results that for *any* initial configuration with components 0 and 1, not all equal to 0 and not all equal to 1, the length of the corresponding cycle is exactly p. For example, writing only the first p components of the sequences, the chain produced by the initial configuration $\mathbf{e_0}$ when $p = 3$ and $p = 7$ are:

$$(1,0,0) \to (1,0,1) \to (1,1,0) \to (0,1,1) \to (1,0,1) \to \cdots$$

and

$$\begin{aligned}(1,0,0,0,0,0,0) &\to (1,0,0,0,0,0,1) \to (1,0,0,0,0,1,0) \to \\ \to(1,0,0,0,1,1,1) &\to (1,0,0,1,0,0,0) \to (1,0,1,1,0,0,1) \to \\ \to(1,1,0,1,0,1,0) &\to (0,1,1,1,1,1,1) \to (1,0,0,0,0,0,1) \to \cdots\end{aligned}$$

respectively.

Long periods: $2^s - 1$ always divides $2^{p-1} - 1$; it equals $2^{p-1} - 1$ when 2 is a primitive root modulo p. Artin's conjecture, still unsolved, says that there are infinitely many such primes. The first prime numbers which satisfy Artin's conjecture are 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, ...

Below is the chain produced by the initial configuration $\mathbf{e_0}$ for $p = 5$. It is a cycle of length 15, as expected.

$$(1,0,0,0,0) \to (1,0,0,0,1) \to (1,0,0,1,0) \to (1,0,1,1,1) \to$$
$$\to (1,1,0,0,0) \to (0,1,0,0,1) \to (1,1,0,1,1) \to (0,1,1,0,0) \to$$
$$\to (1,0,1,0,0) \to (1,1,1,0,1) \to (0,0,1,1,0) \to (0,1,0,1,0) \to$$
$$\to (1,1,1,1,0) \to (0,0,0,1,1) \to (0,0,1,0,1) \to (0,1,1,1,1) \to$$
$$\to (1,0,0,0,1) \to \cdots$$

In the papers of Rajiv Gupta and M. Ram Murty [3] and Heath-Brown [4] on Artin's conjecture there are lemmas showing that for infinitely many primes p all the prime factors of the number $\frac{p-1}{2}$ are larger than $p^{1/4}$. This shows that there are primes p for which the lengths $2^s - 1$ of our periods are huge, more precisely they are larger than $2^{p^{1/4}}$.

However, $2^s - 1$ is not necessary the shortest period. For example, if $p = 11$ the length of the cycle produced by any configuration is 341, while $2^s - 1 = 2^{10} - 1 = 1023 = 3 \cdot 341$. Other examples can be found in the following Table.

d	length of cycle	s	$2^s - 1$	$d(2^{s/2} - 1)$
3	3	2	3	3
5	$15 = 5 \cdot 3$	4	15	15
7	7	3	7	
11	$341 = 11 \cdot 31$	10	$341 \cdot 3$	341
13	$819 = 13 \cdot 63$	12	$819 \cdot 5$	819
17	$255 = 17 \cdot 15$	8	255	255
19	$9709 = 19 \cdot 511$	18	$9709 \cdot 3^3$	9709
23	$2047 = 23 \cdot 89$	11	2047	
29	$475107 = 29 \cdot 16383$	28	$475107 \cdot 5 \cdot 113$	475107
31	31	5	31	
37	$3233097 = 37 \cdot 87381$	36	$3233097 \cdot 3 \cdot 5 \cdot 13 \cdot 109$	$3233097 \cdot 3$
41	$41943 = 41 \cdot 1023$	20	$41943 \cdot 5^2$	41943
43	$5461 = 43 \cdot 127$	14	$5461 \cdot 3$	5461
47	$8388607 = 47 \cdot 178481$	23	8388607	

We calculated the length of cycles for many other values of d and we found that when s is even the number $d(2^{s/2}-1)$, which is always a divisor of 2^s-1, is also a period. It would be interesting to know if this is true in general.

3. A MORE GENERAL EVOLUTION FUNCTION

In this section we introduce a more general evolution function and give a useful method to calculate its repeated composition by itself. Finally, we deduce a criterion which discerns if a given integer is or not the length of a cycle of chains produced by our original evolution function.

Let d be a positive integer and $\mathcal{S} = \{0,1\}^d$. We denote by $\rho(\mathbf{x})$ the circular rotation to the right of the vector $\mathbf{x} \in \mathcal{S}$ (e.g. for $d = 7$, $\rho(1,1,0,1,0,0,0) = (0,1,1,0,1,0,0)$) and $\cdot\colon \mathcal{S} \times \mathcal{S} \to \mathcal{S}$ the *xor* function (which is the componentwise addition mod 2).

Let $a_1, a_2, \ldots, a_s$ be s positive integers and define the evolution function $\phi\colon \mathcal{S} \to \mathcal{S}$ by

$$\phi(\mathbf{x}) = \rho^{(a_1)}(\mathbf{x}) \cdots \rho^{(a_s)}(\mathbf{x}).$$

Note that for $s = 2$, $a_1 = 0$ and $a_2 = 1$ we get our previous evolution function.

The following lemma adds together some properties of these functions.

Lemma 2. *For any nonnegative integers k, m, n and any $\mathbf{x}, \mathbf{y} \in \mathcal{S}$ we have:*

$$\begin{aligned}
&1.\rho(\mathbf{xy}) = \rho(\mathbf{x})\rho(\mathbf{y}),\\
&2.\phi(\mathbf{xy}) = \phi(\mathbf{x})\phi(\mathbf{y}),\\
&3.\phi\big(\rho(\mathbf{x})\big) = \rho\big(\phi(\mathbf{x})\big),\\
&4.\phi^{(m)}(\mathbf{xy}) = \phi^{(m)}(\mathbf{x})\phi^{(m)}(\mathbf{y}),\\
&5.\phi^{(m)}\big(\rho(\mathbf{x})\big) = \rho\big(\phi^{(m)}(\mathbf{x})\big),\\
&6.\phi^{(m)}\big(\rho^{(n)}(\mathbf{x})\big) = \rho^{(n)}\big(\phi^{(m)}(\mathbf{x})\big),\\
&7.\phi^{(2^k)}(\mathbf{x}) = \rho^{(2^k a_1)}(\mathbf{x}) \cdots \rho^{(2^k a_s)}(\mathbf{x}).
\end{aligned}$$

Proof. Everything follows easily by definitions and/or by induction.

As a consequence, we immediately obtain the following:

Corollary 1. *Suppose $d = 2^k$. Then, for any $\mathbf{x} \in \mathcal{S}$ and $n \geq 1$ we have that $\phi^{(d+n-1)}(\mathbf{x}) = \mathbf{0}$ if s is even and $\phi^{(nd)}(\mathbf{x}) = \mathbf{x}$ if s is odd.*

Remark. It is easy to see that the properties **1-7** from Lemma 2 do not depend essentially on $\mathcal{S}$. Thus we may replace $\{0,1\}$ by a more general monoid (a nilpotent one may be of particular interest), for which similar consequences still hold true.

Let

$$k = 2^{l_0} + 2^{l_1} + \cdots + 2^{l_\mu} \tag{5}$$

be the representation in base 2 of the positive integer k and assume $l_0 < \ldots < l_\mu$. We denote

$$r_{ij} \equiv 2^{l_i} a_j \pmod{d}, \quad 0 \leq r_{l_i j} \leq d-1 \tag{6}$$

for $0 \leq i \leq \mu$ and $1 \leq j \leq s$. The next proposition gives an algorithm for the calculation of $\phi^{(k)}(\mathbf{x})$ in $O_s(\log k)$ steps.

Proposition 1. *Let* $\mathbf{x} \in \mathcal{S}$ *and*

$$\mathbf{y_0} = \rho^{r_{01}}(\mathbf{x}) \cdots \rho^{r_{0s}}(\mathbf{x}).$$

Define inductively

$$\mathbf{y_j} = \rho^{r_{j1}}(\mathbf{y_{j-1}}) \cdots \rho^{r_{js}}(\mathbf{y_{j-1}})$$

for $1 \leq j \leq \mu$. *Then*

$$\phi^{(k)}(\mathbf{x}) = \mathbf{y}_\mu.$$

Proof. Let $k = k_1 + 2^{l_0}$. Using Lemma 2 we have

$$\begin{aligned}
\phi^{(k)}(\mathbf{x}) &= \phi^{(k_1+2^{l_0})}(\mathbf{x}) = \phi^{(k_1)}\Big(\phi^{(2^{l_0})}(\mathbf{x})\Big) \\
&= \phi^{(k_1)}\Big(\rho^{(2^{l_0}a_1)}(\mathbf{x}) \cdots \rho^{(2^{l_0}a_s)}(\mathbf{x})\Big) \\
&= \phi^{(k_1)}\Big(\rho^{(r_{01})}(\mathbf{x}) \cdots \rho^{(r_{0s})}(\mathbf{x})\Big) = \phi^{(k_1)}(\mathbf{y_0}).
\end{aligned}$$

Similarly, let $k_1 = k_2 + 2^{l_1}$. Then we have

$$\begin{aligned}
\phi^{(k_1)}(\mathbf{y_0}) &= \phi^{(k_2+2^{l_1})}(\mathbf{y_0}) = \phi^{(k_2)}\Big(\phi^{(2^{l_1})}(\mathbf{y_0})\Big) \\
&= \phi^{(k_2)}\Big(\rho^{(2^{l_1}a_1)}(\mathbf{y_0}) \cdots \rho^{(2^{l_1}a_s)}(\mathbf{y_0})\Big) \\
&= \phi^{(k_2)}\Big(\rho^{(r_{11})}(\mathbf{y_0}) \cdots \rho^{(r_{1s})}(\mathbf{y_0})\Big) = \phi^{(k_2)}(\mathbf{y_1}).
\end{aligned}$$

It is clear now that the proposition follows by induction following the same procedure.

A direct way to calculate $\phi^{(k)}(\mathbf{x})$ is given in the next theorem.

Theorem 3. *For any positive integer k represented as in* (5), *we have*

$$\phi^{(k)}(\mathbf{x}) = \prod_{1\le i_1,\dots,i_{\mu+1}\le s} \rho^{(r_{0\,i_1}+\dots+r_{\mu\,i_{\mu+1}})}(\mathbf{x}).$$

Proof. The proof is by induction on μ.

If $\mu = 0$, then $k = 2^{l_0}$ and by Lemma 2

$$\phi^{(2^{l_0})}(\mathbf{x}) = \rho^{(2^{l_0}a_1)}(\mathbf{x})\cdots\rho^{(2^{l_0}a_s)}(\mathbf{x}) = \rho^{(r_{01})}(\mathbf{x})\cdots\rho^{(r_{0s})}(\mathbf{x}).$$

Suppose the statement is true for $\mu - 1$. Let $k_1 = k - 2^{l_\mu}$. Then the representation of k_1 in base 2 has μ digits and we can apply to it the hypothesis of induction. Thus, by Lemma 2 we have

$$\begin{aligned}\phi^{(k)}(\mathbf{x}) &= \phi^{(2^{l_\mu}+k_1)}(\mathbf{x}) = \phi^{(2^{l_\mu})}\big(\phi^{(k_1)}(\mathbf{x})\big)\\ &= \phi^{(2^{l_\mu})}\Big(\prod_{1\le i_1,\dots,i_\mu\le s} \rho^{(r_{0\,i_1}+\dots+r_{\mu-1\,i_\mu})}(\mathbf{x})\Big).\end{aligned}$$

By the definition of $\phi(\mathbf{x})$, (6) and Lemma 2 this is

$$\begin{aligned}&= \prod_{j=1}^{s}\rho^{(2^{l_\mu}a_j)}\Big(\prod_{1\le i_1,\dots,i_\mu\le s} \rho^{(r_{0\,i_1}+\dots+r_{\mu-1\,i_\mu})}(\mathbf{x})\Big)\\ &= \prod_{j=1}^{s}\rho^{(r_{\mu j})}\Big(\prod_{1\le i_1,\dots,i_\mu\le s} \rho^{(r_{0\,i_1}+\dots+r_{\mu-1\,i_\mu})}(\mathbf{x})\Big)\\ &= \prod_{1\le i_1,\dots,i_{\mu+1}\le s} \rho^{(r_{0\,i_1}+\dots+r_{\mu\,i_{\mu+1}})}(\mathbf{x}),\end{aligned}$$

which concludes the proof of the theorem.

Now we apply this result to the particular evolution function from the previous sections. Thus, from now on we assume that $s = 2$, $a_1 = 0$ and $a_2 = 1$, that is $\phi(\mathbf{x}) = \mathbf{x}\rho(\mathbf{x})$.

Corollary 2. *Let $k = 2^{l_0} + 2^{l_1} + \dots + 2^{l_\mu}$ be the representation in base 2 of the positive integer k, where $l_0 < \dots < l_\mu$, and $\phi(\mathbf{x}) = \mathbf{x}\rho(\mathbf{x})$. Denote*

$$\mathcal{R}_k = \big\{r\colon r \equiv 2^{l_i} \pmod d,\ 0 \le r \le d-1,\ \textit{for some } 0 \le i \le \mu\big\}.$$

Then

$$\phi^{(k)}(\mathbf{x}) = \mathbf{x}\prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(\sum_{r\in R} r\right)}(\mathbf{x})$$

for any $\mathbf{x} \in \mathcal{S}$.

Proof. By Theorem 3

$$\phi^{(k)}(\mathbf{x}) = \prod_{1\le i_1,\dots,i_{\mu+1}\le 2} \rho^{(r_{0\,i_1}+\cdots+r_{\mu\,i_{\mu+1}})}(\mathbf{x}). \tag{7}$$

By (6) and our hypothesis $r_{j1} = 0$ and $r_{j2} \equiv 2^{l_j} \pmod d$, $0 \le r_{j2} < d$ for $0 \le j \le \mu$. The corollary then follows by isolating in (7) the term with $i_1 = \ldots = i_{\mu+1} = 1$, that is $\rho^{(0)}(\mathbf{x})\big(=\mathbf{x}\big)$ and using the fact that

$$\rho^{\left(\sum_{r\in\emptyset} r\right)}(\mathbf{x}) = \mathbf{0}.$$

From Corollary 2 we deduce a criterion for cycling. Thus, $\phi^{(k)}(\mathbf{x}) = \mathbf{x}$ is equivalent to

$$\prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(\sum_{r\in R} r\right)}(\mathbf{x}) = \mathbf{0}. \tag{8}$$

Starting with $\mathbf{x} = \mathbf{e_0} = (1,0,\dots,0)$, we get $\phi(\mathbf{e_0}) = \mathbf{e_0}\,\rho(\mathbf{e_0}) = (1,1,0,\dots,0) = \mathbf{e_1}$. Then, by (8) and Lemma 2, we deduce

$$\prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(\sum_{r\in R} r\right)}(\mathbf{e_0}) \cdot \prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(1+\sum_{r\in R} r\right)}(\mathbf{e_0}) = \mathbf{0},$$

which can be written as

$$\prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(\sum_{r\in R} r\right)}(\mathbf{e_0}) = \prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(1+\sum_{r\in R} r\right)}(\mathbf{e_0})$$

or

$$\prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(\sum_{r\in R} r\right)}(\mathbf{e_0}) = \rho\Big(\prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(\sum_{r\in R} r\right)}(\mathbf{e_0})\Big). \tag{9}$$

For any $m \in \{1,\dots,d\}$ let

$$\nu_{k,d}(m) = \#\{R \subset \mathcal{R}_k \colon \sum_{r\in\mathcal{R}} r \equiv m \pmod d\}.$$

Then (9) becomes

$$\prod_{m=1}^{d} \rho^{\nu_k(m)}(\mathbf{e_0}) = \rho\Big(\prod_{m=1}^{d} \rho^{\nu_k(m)}(\mathbf{e_0})\Big).$$

Since the only invariants of ρ are $(0,\dots,0)$ and $(1,\dots,1)$ we obtain the following:

Corollary 3. *A positive integer k is a period for $\phi(\mathbf{x}) = \mathbf{x}\rho(\mathbf{x})$ if and only if the numbers $\nu_{k,d}(m)$, $1 \le m \le d$ have the same parity.*

We checked the values of $\nu_{k,d}(m)$ with k the length of the shortest cycle for different values of d and we found some interesting "regularity" properties . Thus, $\nu_{k,d}(m)$ not only have the same parity but most of the time they are equal. Some nontrivial examples are:

1. If $d = 11$ then $k = 341 = 101010101_2$, $\nu_{341,11}(11) = 1$ and $\nu_{341,11}(m) = 3$ for $1 \leq m \leq 10$.

2. If $d = 13$ then $k = 819 = 1100110011_2$, $\nu_{819,13}(13) = 3$ and $\nu_{819,13}(m) = 5$ for $1 \leq m \leq 12$.

3. If $d = 19$ then $k = 9709 = 10010111101101_2$, $\nu_{9709,19}(19) = 25$ and $\nu_{9709,19}(m) = 27$ for $1 \leq m \leq 18$.

4. If $d = 43$ then $k = 5461 = 1010101010101_2$, $\nu_{5461,43}(43) = 1$ and $\nu_{5461,43}(m) = 3$ for $1 \leq m \leq 42$.

References

[1] Z. BOREVICH and I. SHAFAREVICH, *Number Theory*, Academic Press, New York, 1966.

[2] J. P. CAMPBELL, *Reviews,* Mathematics Magazine, Vol.**69**, No. 4 (October 1996) 311-313.

[3] R. GUPTA and M. RAM MURTY, *A Remark on Artin's conjecture,* Invent. Math. **78**, (1984), 127-130.

[4] D.R. HEATH-BROWN, *Artin's conjecture for primitive roots,* Quart. J. Math. Oxford (2), **37**, (1986), 27-38.

[5] B. THWAITES, *Two conjectures or how to win £*1100, Mathematical Gazette **80** (March 1996) 35-36.

C. I. COBELI, MATHEMATICS RESEARCH INSTITUTE OF THE ROMANIAN ACADEMY, P.O. BOX 1-764, BUCHAREST, 70700, ROMANIA
CCOBELI@STOILOW.IMAR.RO

M. CRÂŞMARU, VATRA DORNEI, 5975, ROMANIA
MI@ASSIST.CCCIS.RO

A. ZAHARESCU, DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA AND MATHEMATICS RESEARCH INSTITUTE OF THE ROMANIAN ACADEMY P.O. BOX 1-764, BUCHAREST, 70700, ROMANIA
AZAH@MATH.MIT.EDU