Surjective Two-Neighbor Cellular Automata on Prime Alphabets*

Jarkko Kari[1] Ville Salo[1,2] Ilkka Törmä[1,2]

[1]University of Turku, Finland

[2]TUCS – Turku Center for Computer Science
{jkari,vosalo,iatorm}@utu.fi

August 2, 2013

Abstract

In this article, we present a simple proof for the fact that a surjective cellular automaton with neighborhood size 2 on a prime alphabet is permutive in some coordinate. We discuss the optimality of this result, and the existence of non-closing cellular automata of a given neighborhood and alphabet size.

1 Introduction

Cellular automata are topological dynamical systems that have a simple finite definition, and are discrete in both space and time. Formally, they are continuous self-maps of the space of infinite sequences over a finite alphabet. The dymamics of cellular automata can be very complex and unpredictable, and many fundamental questions about their properties are still open. In particular, the dynamics of surjective cellular automata have been extensively studied, but it is still unknown whether they always have a dense set of periodic points.

In this work-in-progress article, we study surjective cellular automata with small local neighborhoods. In particular, we show that if the neighborhood size is 2 and the size of the alphabet is a prime, the automaton is permutive in one of the coordinates. We try to optimize this result as much as possible, using computer searches and general constructions, and obtain an almost complete characterization of those alphabet-neighborhood size pairs which admit a non-closing cellular automaton.

*Research supported by the Academy of Finland Grant 131558

2 Definitions and Preliminaries

Let S be a finite set, called the *alphabet*, and denote by S^* the set of finite words over S. We endow $S^{\mathbb{Z}}$ with the product topology, making it a compact topological space. An element $x = (x_i)_{i\in\mathbb{Z}} \in S^{\mathbb{Z}}$ is called a *configuration*. For $i, j \in \mathbb{Z}$, we denote $x_{[i,j]} = x_i x_{i+1} \cdots x_j$. The *shift map* $\sigma : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$, defined by $\sigma(x)_i = x_{i+1}$, is a homeomorphism from $S^{\mathbb{Z}}$ to itself. A one-directional sequence $x \in S^{\mathbb{N}}$ (or $x \in S^{-\mathbb{N}}$) is *transitive* if every word in S^* occurs in it, and a configuration $x \in S^{\mathbb{Z}}$ is *doubly transitive* if both $x_{(-\infty,0]}$ and $x_{[0\infty)}$ are transitive.

A *cellular automaton* (CA for short) is a continuous function $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ that commutes with the shift: $f \circ \sigma = \sigma \circ f$. It is known [2] that a cellular automaton is given by a *local rule* $F : S^{\ell+r+1} \to S$ for some $\ell, r \in \mathbb{N}$ by $f(x)_i = F(x_{[i-\ell,i+r]})$. The numbers ℓ and r are called *left and right radii* of f, respectively. If we can take $\ell = 0$ and $r = 1$, we say f is a *radius-*$\frac{1}{2}$ CA. We say f is *permutive* in a coordinate $i \in [-\ell, r]$, if fixing a word $w \in S^{\ell+r+1}$ and permuting the letter w_i also permutes the image $F(w)$. If f is permutive in the leftmost (rightmost) coordinate of its neighborhood, we say it is left (right, respectively) permutive. We say f is *left (right) closing*, if $x_{[0,\infty)} = y_{[0,\infty)}$ ($x_{(\infty,0]} = y_{(\infty,0]}$, respectively) and $f(x) = f(y)$ implies $x = y$ for all $x, y \in S^{\mathbb{Z}}$. Finally, f is *preinjective* if $f(x) = f(y)$ and $x \neq y$ imply that $x_i \neq y_i$ for infinitely many $i \in \mathbb{Z}$.

The *image graph* of a CA $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ with radii ℓ and r is the labeled graph with vertex set $S^{\ell+r}$, and an edge from v to w with label $s \in S$ if and only if $v_{[1,\ell+r-1]} = w_{[0,\ell+r-2]}$ and $f(v_0 w) = s$. The *determinization* of said graph is given by the standard subset construction. Note that f is surjective iff every $u \in S^*$ occurs as the label of a path in the image graph of f.

The following result is classical, and can be found, for example, in [2] or [4].

Lemma 1. *Let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a surjective CA with left and right radii ℓ and r, respectively. Then $|f^{-1}(x)|$ is finite and bounded, and f is preinjective. If $x \in S^{\mathbb{Z}}$ is doubly transitive and $a \neq b \in f^{-1}(x)$, then a and b are also doubly transitive and $a_{[i,i+\ell+r-1]} \neq b_{[i,i+\ell+r-1]}$ for all $i \in \mathbb{Z}$. Moreover, there exists $M(f) \in \mathbb{N}$ such that $|f^{-1}(x)| = M(f)$ for every doubly transitive $x \in S^{\mathbb{Z}}$.*

3 Permutivity of Radius-$\frac{1}{2}$ Automata

For this section, we fix a surjective CA $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ with left and right radii ℓ and r, and denote $|S| = n$. When $x \in S^{\mathbb{N}}$, we write

$$f^{-1}(x) = \{y \in S^{\mathbb{N}} \mid \forall i \in \mathbb{N} : f({}^{\infty}0.y)_{\ell+i} = x_i\},$$

and symmetrically for $y \in S^{-\mathbb{N}}$. When $x \in S^{\mathbb{N}}$ ($y \in S^{-\mathbb{N}}$) is transitive, we write $L(f, x) = |f^{-1}(x)|$ ($R(f, y) = |f^{-1}(y)|$, respectively). Denote also

$M = M(f)$.

The following results (up to but not including Proposition 1) seem classical, but we have not been able to find a reference where they are presented in this form. Closely related results can be found in sections 14 and 15 of [2]. To our knowledge, Proposition 1 is a new result.

Lemma 2. *Both L and R are functions of f, ℓ and r only, and do not depend on the chosen transitive points. Writing $L(f)$ and $R(f)$ for these functions, we have $Mn^{\ell+r} = L(f)R(f)$.*

Proof. Let $x \in S^{-\mathbb{N}}$ and $y \in S^{\mathbb{N}}$ be transitive, and consider the set of points $A = xS^{\ell+r}y$. We have $|A| = n^{\ell+r}$, and since every element of A is doubly transitive, $|f^{-1}(A)| = Mn^{\ell+r}$. On the other hand, clearly $|f^{-1}(A)| = R(f,x)L(f,y)$. In particular, L and R are functions of f, ℓ and r only. □

Lemma 3. *Writing $L(f)$ and $R(f)$ as before, the functions $f \mapsto M(f)$, $f \mapsto L'(f) = \frac{L(f)}{n^\ell}$ and $f \mapsto R'(f) = \frac{R(f)}{n^r}$ are homomorphisms from the set of surjective CA on S to $\mathbb{Q}$ (and do not depend on the choice of ℓ and r), and $M = L'R'$.*

Proof. It is clear that L' and R' do not depend on the choice of ℓ and r, as increasing ℓ effectively multiplies L by n, and similarly for r and R. We then prove that L' is a homomorphism, the case of R' being symmetric. Let $g : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a surjective CA with left radius ℓ'. Let $x \in S^{\mathbb{N}}$ be transitive, so that $g^{-1}(x)$ is also transitive. Taking the left radius $\ell + \ell'$ for $f \circ g$, we then have $L(f \circ g) = |f^{-1}(g^{-1}(x))| = L(f)L(g)$. It follows that L' is a homomorphism, since it does not depend on the choice of the radii. □

From now on, denote $R = R(f)$ and $L = L(f)$, since f and its radii are fixed.

Lemma 4. *The inequalities $M \leq L, R \leq n^{\ell+r}$ hold.*

Proof. Let $x \in S^{\mathbb{Z}}$ be a configuration, and denote $|f^{-1}(x)| = k$. Then there exists $i \in \mathbb{Z}$ such that already $|f^{-1}(x_{[i,\infty)})| \geq k$. The inequalities $M \leq L$ and $M \leq R$ follow. The upper bounds follow from the equality $Mn^{\ell+r} = LR$ of Lemma 2. □

Lemma 5. *Let $x \in S^{\mathbb{N}}$ be transitive. If $a \neq b \in f^{-1}(x)$, then a and b differ in their $(r+\ell)$-prefix.*

Proof. Suppose not, let $y \in S^{-\mathbb{N}}$ be transitive and $c \in f^{-1}(y)$. Then $f(c.a) = f(c.b)$ is doubly transitive, but has two distinct preimages that agree on the interval $[0, \ell + r - 1]$, a contradiction by Lemma 1. □

By the above lemma, the numbers L and R are generalizations of the left and right Welch indices of reversible cellular automata, respectively, as defined in [1] (among others).

Proposition 1. *If $n = |S|$ is prime and f is a surjective radius-$\frac{1}{2}$ CA, then f is left or right permutive.*

Proof. Because $LR = Mn$, n is prime and $L, R \leq n$, we must have either $L = n$ or $R = n$. Without loss of generality we assume the former. Now, if $x \in S^{\mathbb{N}}$ is transitive and $s \in S$, every $s' \in S$ occurs as the leftmost symbol of a preimage of sx by Lemma 5. This means that for all $s, s' \in S$, there exists $s'' \in S$ such that $f(s', s'') = s$, and thus f is right permutive. $\square$

This proposition can be useful when trying to construct surjective cellular automata with some specific nontrivial properties, as it shows that radius-$\frac{1}{2}$ CA on prime alphabets are quite simple, and thus trivially possess or lack many interesting properties.

4 Other Neighborhoods and Alphabet Sizes

In this section, we study the case of non-prime alphabets and larger neighborhoods in the hope of generalizing Proposition 1. We proceed in the following two directions:

1. We study whether complicated surjective CA could somehow be 'decomposed' into more primitive components, preferably permutive CA.
2. With the help of computer searches, we try to enumerate the combinations of alphabet and neighborhood sizes in which all cellular automata must be permutive or closing in either direction.

In the first direction, we begin with the following definition.

Definition 1. *Let $n = k_1 k_2$, where $k_i \geq 2$. We say f is* track-reducible *if there exist two sets S_1 and S_2 with $|S_i| = k_i$, cellular automata g on S_1 and h on $S_1 \times S_2$ with $g \circ \pi_1 = \pi_1 \circ h$, and bijections $\alpha : S \to S_1 \times S_2$ and $\beta : S_1 \times S_2 \to S$ such that $f = \beta \circ h \circ \alpha$, where α and β are used as radius-*0 *cellular automata.*

Surjective track-reducible automata are easy to construct inductively as follows. First, let g be any surjective (perhaps track-reducible) CA in S_1. Then we can define h by choosing a coordinate $i \in \mathbb{Z}$ on the S_2-track and a neighborhood $N \subset \mathbb{Z}$ on the S_1-track, and for each $w \in S_1^N$, a CA h_w on S_2 that is left (or right) permutive in the coordinate i. Such a CA is always surjective, but if the direction of permutivity or the coordinate i is varied, it is not permutive. In the course of this section, however, we shall see that not all surjective cellular automata on non-prime alphabets are track-reducible.

For the second direction, we begin with the radius-$\frac{1}{2}$ case, and show that here Proposition 1 is optimal.

Proposition 2. *Let S be an alphabet. Then all surjective radius-$\frac{1}{2}$ CA on S are closing in either direction iff $|S|$ is prime.*

Proof. First, if $|S|$ is prime, then by Proposition 1, every radius-$\frac{1}{2}$ CA on S is permutive in either coordinate, thus closing.

Next, let $n \geq 3$ be arbitrary. We construct a left permutive radius-$\frac{1}{2}$ CA f_n on $\{0, \ldots, n-1\}$ which is not right closing. The local rules for f_n are $f_n(a, b) = a + b \bmod 2$ and $f_n(c, b) = c$ for all $a \in \{0, 1\}$, $b \in \{0, \ldots, n-1\}$ and $c \in \{2, \ldots, n-1\}$. Now f_n is left permutive, but the point ${}^\infty 2.0^\infty$ has preimages ${}^\infty 2.0^\infty$ and ${}^\infty 2.1^\infty$, so f_n is not right closing. Define also $g_n(a, b) = f_n(b, a)$, so that g_n is right permutive and not left closing.

Suppose $|S| = k_1 k_2$, where $k_i \geq 3$. The cellular automaton $f_{k_1} \times g_{k_2}$ on $\{0, \ldots, k_1 - 1\} \times \{0, \ldots, k_2 - 1\}$ is surjective, but not closing in either direction. Interpreting the state set as S, the claim follows for such S.

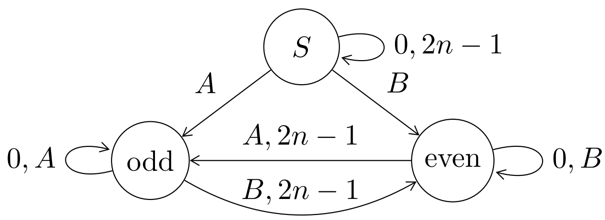
Finally, let $|S| = 2n$ for $n \in \mathbb{N}$, and assume $S = \{0, \ldots, 2n-1\}$. We construct a surjective radius-$\frac{1}{2}$ CA f on S which is not closing. First, define $A = \{1, 3, \ldots, 2n-3\}$ and $B = \{2, 4, \ldots, 2n-2\}$, so that A, B, $\{0\}$ and $\{2n-1\}$ form a partition of S. Define then f by

(a,b)	(s,s)	$(k-1,o)$	$(o,o+2k)$
$f(a,b)$	0	$k \in A$	

(a,b)	$(k-1,e)$	$(e,e+k)$	$(2n-2,o)$	$(2n-1,e)$
$f(a,b)$	$k \in B$		$2n-1$	

where $s \in S$, $o \in A \cup \{2n-1\}$ and $e \in \{0\} \cup B$ are arbitrary, and the sums are taken modulo $2n$. This is a generalization of the automaton defined in [3, Example 15].

The determinization of the image graph of f is



and it shows that f is surjective. However, the point ${}^\infty 0.1^\infty$ has the three preimages ${}^\infty 0.135\cdots$, ${}^\infty 0.357\cdots$ and ${}^\infty 1.357\cdots$ which show that f is neither right nor left closing. □

A simple computer search also shows that the automaton f constructed in the case $|S| = 4$ (the original example of [3]) is not track-reducible. Thus track-reducibility is not general enough to capture all radius-$\frac{1}{2}$ surjective cellular automata on composite alphabets.

For larger neighborhood sizes, we have the following.

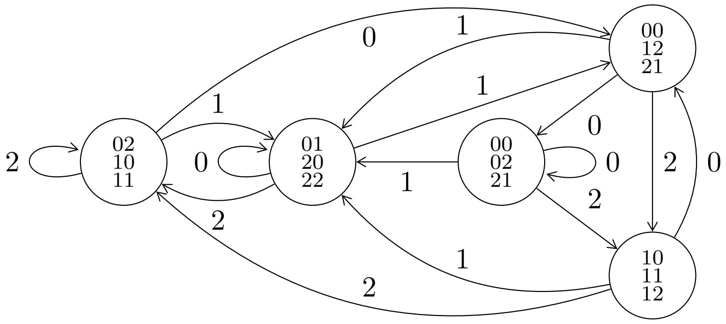
Example 1 (A non-closing surjective radius-1 CA with alphabet size at least 5)**.** *Let $n \geq 3$ and $S = \{(0,0),(0,1),(1,0),(1,1)\} \cup \{(i,i) \mid 2 \leq i < n\}$, and let f be the three-neighbor CA that simulates the automaton f_n (from the proof of Proposition 2) on the first track using the cells 0 and 1, and g_n on the second track using the cells -1 and 0. Then f is clearly surjective, but not closing in either direction.*

We show a three-state three-neighbor CA which is surjective, but not closing in either direction. This automaton was found by a computer search.

Example 2 (A non-closing surjective radius-1 CA with alphabet size 3)**.** *Consider the CA whose local rule is given by*

	00	01	02	10	11	12	20	21	22
0	0	1	0	2	2	1	1	0	1
1	0	1	2	2	2	0	1	0	1
2	1	0	2	2	2	2	0	1	0

It is surjective, since its determinized image graph contains the subgraph



Consider the points ${}^\infty 0.1^\infty$ and ${}^\infty 012.110^\infty$. The former has the preimages ${}^\infty 0.(2001)^\infty$ and ${}^\infty 0.(0120)^\infty$, while the latter has ${}^\infty 020.20^\infty$ and ${}^\infty 21.20^\infty$. This shows that the CA is neither left nor right closing.

Finally, we show the existence of a binary CA which is not closing in either direction. The construction is almost surely not optimal with respect to neighborhood size.

Example 3 (A non-closing surjective binary CA with neighborhood size 11)**.** *Consider the CA f on $\{0,1\}$ with neighborhood $\{-5,\dots,5\}$ defined by the rules $f(ab001cd001e) = c+e$ and $f(a001bc001de) = a+c$ for all $a,b,c,d,e \in \{0,1\}$, and $f(w) = w_5$ for all other $w \in \{0,1\}^{11}$. It is easy to check that given a configuration $x \in \{0,1\}^{\mathbb{Z}}$, we have $x_{[0,2]} = 001$ iff $f(x)_{[0,2]} = 001$.*

Consider a maximal subword w of the form $a_1b_1001a_2b_2001\cdots001a_nb_n$. A preimage for w is $a'_1b'_1001a'_2b'_2001\cdots001a'_{n-1}b'_{n-1}001a'_nb'_n$, where $a'_i, b'_1 \in$

Table 1: A table of closingness. The letter n denotes the size of the state set, while m is the size of the neighborhood. The label 'per' refers to left or right permutivity, 'clo' to left or right closingness, '?' to unknown and '-' to not necessarily closing. On each row, the leftmost '-' has been replaced by the number of the result that proves this fact.

$n \setminus m$	2	3	4	5	...	10	11
2	per	per	clo	?	...	?	Ex. 3
3	per	Ex. 2	-	-	...	-	-
4	Prop. 2	-	-	-	...	-	-
5	per	Ex. 1	-	-	...	-	-
6	Prop. 2	-	-	-	...	-	-
7	per	Ex. 1	-	-	...	-	-
8	Prop. 2	-	-	-	...	-	-
9	Prop. 2	-	-	-	...	-	-

$\{0,1\}$ *are given by* $a'_1 = a_1$, $b'_1 = b_1$, $a'_n = a_n$, $b'_n = b_n$, *and* $a'_i = a'_{i+1} + a_i \bmod 2$ *and* $b'_i = b'_{i-1} + b_i \bmod 2$ *for all* $i \in [2, n-1]$. *The preimages of other patterns are given by themselves, since cells can only change their state when surrounded by the* 001*-patterns in the specific way. Thus* f *is surjective. Also,* f *simulates the* $n = 3$ *automaton from Example 1 via the substitution* $(a,b) \mapsto 001ab$ *for* $a, b \in \{0,1\}$ *and* $(2,2) \mapsto 001000001$*, and it is then easy to see that it is not closing in either direction.*

Using a computer search, we have verified that all binary surjective CA with neighborhood size 4 are right or left closing. Also, all surjective elementary CA are left or right permutive (with the minimal neighborhood). The following cases are thus left open:

Question 1. *For* $5 \leq m \leq 10$*, does there exist a surjective binary CA of neighborhood size* m *which is not closing in either direction?*

References

[1] Eugen Czeizler and Jarkko Kari. A tight linear bound on the neighborhood of inverse cellular automata. In *Automata, languages and programming*, volume 3580 of *Lecture Notes in Comput. Sci.*, pages 410–420. Springer, Berlin, 2005.

[2] Gustav A. Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Math. Systems Theory*, 3:320–375, 1969.

[3] Petr Kurka. Topological dynamics of cellular automata. In Robert A. Meyers, editor, *Encyclopedia of Complexity and Systems Science*, pages 9246–9268. Springer, 2009.

[4] Douglas Lind and Brian Marcus. *An introduction to symbolic dynamics and coding.* Cambridge University Press, Cambridge, 1995.