Bounds on Non-surjective Cellular Automata

Jarkko Kari[1], Pascal Vanier[2], and Thomas Zeume[3]

[1] University of Turku
jkari@utu.fi
[2] Laboratoire d'Informatique Fondamentale de Marseille
pascal.vanier@ens-lyon.fr
[3] Gottfried Wilhelm Leibniz Universität Hannover
thomas-zeume@web.de

Abstract. Cellular automata (CA) are discrete, homogeneous dynamical systems. Non-surjective one-dimensional CA have finite words with no preimage (called *orphans*), pairs of different words starting and ending identically and having the same image (*diamonds*) and words with more/fewer preimages than the average number (*unbalanced* words). Using a linear algebra approach, we obtain new upper bounds on the lengths of the shortest such objects. In the case of an n-state, non-surjective CA with neighborhood range 2 our bounds are of the orders $O(n^2)$, $O(n^{3/2})$ and $O(n)$ for the shortest orphan, diamond and unbalanced word, respectively.

1 Introduction

Non-surjective cellular automata (CA) have *Garden of Eden*-configurations: configurations without a preimage. By compactness, there exist also finite patterns that do not appear in any image configuration [2]. These we call *orphans*. The *Garden of Eden* -theorem by *E. F. Moore* [5] and *J. Myhill* [7] proves the existence of *mutually erasable* patterns in non surjective CA. These are two finite words such that two configurations, having the same prefix and suffix and only differing on those words, have the same image. Mutually erasable words are also called *diamonds*. The existence of diamonds is equivalent to being non-surjective. Non-surjectivity is also equivalent to the existence of finite words of the same size with a different number of preimages [2]. Patterns that do not have the average number of preimages are called *unbalanced*.

One will naturally think about the size of these objects. The objective of this paper is to bound the size of the smallest orphan, diamond and unbalanced word of any non-surjective one-dimensional CA, in terms of the number of states in the automaton. For dimensions greater than one, it is known that it is not decidable whether a given CA is surjective or not [3]. Therefore only bounds for one-dimensional CA will be studied: in higher dimensions no recursive bounds exist.

Using a standard blocking technique, one can convert any one-dimensional CA into a CA with the range-2 neighborhood, so we will only study the bounds in this range-2 case. The previously known bounds were an exponential bound

R. Královič and D. Niwiński (Eds.): MFCS 2009, LNCS 5734, pp. 439–450, 2009.

for shortest orphans, a quadratic bound for shortest diamonds and an $O(n^2 \ln n)$ bound for the shortest unbalanced words, where n is the number of states. These can be found in, or easily deduced from [9] and [6].

We will use tools based on linear algebra to obtain a linear upper bound for the size of the shortest unbalanced words, a quadratic bound for the size of the shortest orphans and an $2n^{\frac{3}{2}}$ bound for the length of the shortest diamonds. By using some combinatorial arguments, we are able to reduce the bounds for orphans and diamonds slightly. For all problems we also tried to bound the best possible upper bounds from below. However, the only non-constant lower bounds we found are for the case of shortest orphans.

The paper is organized as follows: In Section 2 we give the definitions of the main concepts, and in Section 3 we explain our basic linear algebra tools that we use to obtain bounds. In Section 4 we provide the bounds that the linear algebra approach immediately provides for the shortest orphans, diamonds and unbalanced words. All bounds are better than any previously known bounds. In the case of orphans the improvement is even from exponential to polynomial. In Section 5 we fine-tune the bounds by looking in detail at the first steps of the dimension reductions. In Section 6 we consider the algorithmic aspects and show that an orphan, a diamond and an unbalanced word can be found in polynomial time. Section 7 reports the existence for every $n \geq 2$ of an n-state range-2 CA whose shortest orphan is of length $2n - 1$. In contrast, for diamonds and unbalanced words we have no non-constant examples. Finally, in Section 8 we formulate open problems and discuss some related questions.

2 Definitions

A *configuration* is a function c that assigns a state from a finite *state set* S to every point in $\mathbb{Z}$. We denote the state of a point $p \in \mathbb{Z}$ of a configuration c by c_p. The set of all configurations is $S^{\mathbb{Z}}$. The *range-r neighborhood* is the tuple $N = (0, \ldots, r-1)$. A *local rule* is a function $f : S^{|N|} \to S$.

Formally, a *cellular automaton* G is a 3-tuple (S, N, f). At each time step a new configuration $G(c)$ is computed from c by updating the states with f at each point p:

$$G(c)_p = f(c_p, c_{p+1} \ldots, c_{p+r-1}) \text{ for all } p \in \mathbb{Z}.$$

The hereby defined function G is called the *global function* of the CA.

We will only consider range-2 CA G with a non-surjective global function throughout the whole paper. The generalization of our results to general range-r are quite straightforward, and will only be briefly discussed in Section 8.

Applications of the range-2 local rule $f : S \times S \longrightarrow S$ to finite words $w \in S^*$ will be denoted by the same symbol G as the global function. In this case

$$G(s_1 s_2 \ldots s_n) = t_1 t_2 \ldots t_{n-1}$$

where $t_i = f(s_i, s_{i+1})$ for all $i = 1, 2, \ldots, n-1$.

Configurations without a preimage are called *Garden of Eden*-configurations. We will be interested in *finite* words without a preimage, that is to say words u

for which there exists no word w such that $G(w) = u$. Such u exist if and only if the CA is non-surjective [2] and are called *orphans*.

By the *Garden of Eden*-theorem of *E. F. Moore* and *J. Myhill*, see [5] and [7], we know that non-surjective CA have configurations which differ only in a finite number of cells and which have the same image under G. We consider the finite differing part of such configurations: Two words $w = p\ c_1 \dots c_l\ s$ and $w' = p\ c'_1 \dots c'_l\ s \in S^{l+2}$ with $G(w) = G(w')$ are said to form a *diamond* if $(c_1, \dots, c_l) \neq (c'_1, \dots, c'_l)$. The length of the diamond is l. A cellular automaton has a diamond iff it is non-surjective.

There are $|S|^k$ different words of length k and $|S|^{k+1}$ different preimages for words of length k. We call G *k-balanced*, if all words of length k have the same number of predecessor words, i.e. $|G^{-1}(u)| = |S|$ for all $u \in S^k$. Words u with $|G^{-1}(u)| \neq |S|$ are called *unbalanced*. A CA has unbalanced words, iff it is non-surjective [2].

3 Linear Algebra Tools

3.1 Vectorial Interpretation of Sets

The proofs are mainly based on the vectorial interpretation of sets of states, introduced in [1] for the CA context: let us denote by $S = \{1, \dots, n\}$ the set of all states. A subset $X \subseteq S$ is interpreted as the 0-1 vector x in $\mathbb{R}^n$ whose i-th coordinate is 1 if $i \in X$ and 0 otherwise. The vectors corresponding to single element sets are the unit coordinate vectors e_i and they form a basis of the vector space $\mathbb{R}^n$.

We define $f_a : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ as the linear transformation such that

$$f_a(e_i) = \sum_{f(i,j)=a} e_j,$$

where f is the local transition function of the automaton and a a state. We define $\phi : \mathbb{R}^n \longrightarrow \mathbb{R}$ as the linear form defined by

$$\phi(x) = x \cdot (1, \dots, 1).$$

We call $\phi(x)$ the *weight* of a vector x since it is the sum of its coordinates. If $w = a_1 \dots a_k$ is a word[1] on the alphabet S, let f_w denote the composition $f_{a_k} \circ \dots \circ f_{a_1}$. The analogous notation for compositions is also used with any other family of functions indexed by letters of an alphabet.

Lemma 1. ***Balance*** *The following equality holds for all $x \in \mathbb{R}^n$:*

$$\sum_{a \in S} \phi(f_a(x)) = \phi(x)|S|$$

[1] The word could be empty, in which case $f_w(x) = x$.

Proof. For each e_i we have

$$\sum_{a \in S} f_a(e_i) = (1, 1, \ldots, 1)$$

because for each $j \in S$ there exists a unique $a \in S$ such that $f(i, j) = a$. By the linearity of ϕ we have

$$\sum_{a \in S} \phi(f_a(e_i)) = \phi(\sum_{a \in S} f_a(e_i)) = |S| = \phi(e_i)|S|.$$

Now, due to the linearity of f_a and ϕ this extends to any vector x of $\mathbb{R}^n$ in place of e_i. □

Note, that if x is a vector corresponding to $X \subseteq S$, then $\phi(f_w(x))$ is the number of preimages of w that start in a state of X. This can be proved by an easy induction on the length of w.

The main application of the balance lemma is the following: If $\phi(f_w(x)) \neq \phi(x)$ for some word w of length k then $\phi(f_u(x)) < \phi(x)$ and $\phi(f_{u'}(x)) > \phi(x)$ for some words u and u' of that same length k.

3.2 A Very Useful Lemma

For any $x \in \mathbb{R}^n$ with $\phi(x) > 0$ we want to establish an upper bound for the length of shortest words u, u' such that $\phi(f_u(x)) < \phi(x)$ and $\phi(f_{u'}(x)) > \phi(x)$. Therefore, the following lemma will be crucial. Strongly inspired by [8] and [4], it can be considered as the basis for all our results.

The lemma concerns affine subspaces of $\mathbb{R}^n$ and the minimal number of applications of given linear transformations that take a given point outside the subspace. Recall that an *affine subspace* of $\mathbb{R}^n$ of dimension d is a set $x + V$ where $x \in \mathbb{R}^n$ and $V \subseteq \mathbb{R}^n$ is a linear subspace of dimension d. In particular, singleton sets $\{x\}$ are affine subspaces of dimension 0. Affine subspaces relevant in our setup are the sets $\{x \in \mathbb{R}^n \mid \phi(x) = c\}$ of vectors having a fixed weight $c \in \mathbb{R}$. Their dimension is $n - 1$.

An *affine combination* of vectors is a linear combination where the coefficients sum up to one. Affine subspaces are closed under affine combinations of their elements, and conversely, any set closed under affine combinations is affine. The affine subspace *generated* by a set $X \subseteq \mathbb{R}^n$ of vectors consists of all affine combinations of elements of X.

Lemma 2. *Let A be an affine subspace of $\mathbb{R}^n$, and let $x \in A$. Let Σ be an alphabet and for every $a \in \Sigma$, let $\psi_a : \mathbb{R}^n \to \mathbb{R}^n$ be a linear transformation. Then, if there is a word w such that $\psi_w(x) \notin A$ then there exists such a word of length at most* $\dim A + 1$.

Proof. Consider the affine spaces $A_0 \subseteq A_1 \subseteq \ldots$ defined by $A_0 = \{x\}$, and A_{i+1} is generated by $A_i \cup \bigcup_{a \in S} \psi_a(A_i)$. Equivalently, A_i is generated by $\{\psi_w(x) \mid |w| \leq i\}$.

By definition, $A_{i+1} = A_i$ means that $\psi_a(A_i) \subseteq A_i$ for all $a \in \Sigma$. Hence if $A_{i+1} = A_i$ for some i, then $A_j = A_i$ for every $j \geq i$.

Let i be the smallest number such that $\psi_w(x) \notin A$ for some w of length i, that is, the smallest i such that $A_i \not\subseteq A$. This means that in $A_0 \subset A_1 \subset \cdots \subset A_i$ all inclusions are proper. In terms of dimensions of affine spaces we have that

$$0 = \dim A_0 < \dim A_1 < \cdots < \dim A_i.$$

This means that $\dim A_{i-1} \geq i-1$. But $A_{i-1} \subseteq A$ so that we also have $\dim A_{i-1} \leq \dim A$. We conclude that $i \leq \dim A + 1$. □

For our case we get the following corollary.

Corollary 1. *Let G be a non-surjective CA and $x \in \mathbb{R}^n$ a vector such that $\phi(x) > 0$. Then there exist words u, u' of length at most $n = |S|$ such that $\phi(f_u(x)) < \phi(x)$ and $\phi(f_{u'}(x)) > \phi(x)$.*

Proof. This is a direct application of Lemma 2. Let $\Sigma = S$, $\psi_a = f_a$ and $A = x + \ker \phi$. Note that A is an affine subspace of $\mathbb{R}^n$ of dimension $n-1$, and $\phi(f_w(x)) \neq \phi(x)$ iff $f_w(x) \notin A$. Since G is non-surjective, there exists an orphan v. As $f_v(e_i) = 0$ for all unit coordinate vectors e_i, we have $f_v(x) = 0$. In particular, $f_v(x) \notin A$. Thus, by Lemma 2, there exists a word w of length at most n such that $\phi(f_w(x)) \neq \phi(x)$. Now, Lemma 1 guarantees the existence of words u, u' of the same length $|w|$ with $\phi(f_u(x)) < \phi(x)$ and $\phi(f_{u'}(x)) > \phi(x)$. □

4 Basic Bounds

We will prove first a quadratic bound for the size of orphans using the previously defined linear algebraic tools.

Theorem 1. *If a range-2 non-surjective CA has n states, then it has an orphan of length at most n^2.*

Proof. We start with $x = (1, \ldots, 1)$. By applying Corollary 1, we know that there exists a word w of length at most n such that $\phi(f_w(x)) < \phi(x) = n$. As $f_w(x)$ is a vector of non-negative integers, $0 \leq \phi(f_w(x)) \leq \phi(x) - 1$. Repeating this argument on $f_w(x)$ in place of x, and continuing likewise, we successively decrease the weight of the vectors. After at most n iterations we obtain a vector of weight 0. Concatenating all words w gives an orphan of length at most n^2. □

We are not aware of any previously published polynomial bound for the length of the shortest orphan. An exponential bound 2^n can be easily seen by combinatorial arguments.

In [6], *Moothathu* proves an $O(n^2 \ln n)$ upper bound for the shortest unbalanced words and asks whether this can be improved. Our linear algebra tools lead straightforwardly to a better bound:

Theorem 2. *Let G be a non-surjective range-2 CA with n states. Then its shortest unbalanced words have at most length n.*

Proof. Let $x = (1, \ldots, 1)$. Because G is non-surjective, by Corollary 1 there is a word w of length n such that $\phi(f_w(x)) \neq \phi(x) = n$. Since $\phi(f_w(x))$ is the number of predecessors of w starting with an arbitrary state of S, we have that w is unbalanced. □

For diamonds also, we obtain a better bound than the previously existing one.

Theorem 3. *Let $G = (S, N, f)$ be a non-surjective range-2 CA with n states. Then $2(\lfloor\sqrt{n}\rfloor - 1)n + 2$ is an upper bound for shortest diamonds of G.*

Proof. Let $k = \lfloor\sqrt{n}\rfloor + 1$ and let $\diamond = p\ c_1 \ldots c_m\ s, p\ d_1 \ldots d_m\ s$ be a diamond of G where $c_1 \neq d_1$ and $c_m \neq d_m$. Let us denote $a = f(p, c_1) = f(p, d_1)$ and $b = f(c_m, s) = f(d_m, s)$. Let x be the $0/1$ -vector corresponding to $\{c_1, d_1\}$, so $\phi(x) = 2$.

By Corollary 1, we can successively increase the weight of x by reading words of length n. Thus there is a word w of length at most $(k-2)n$ such that $\phi(f_w(x)) \geq k$, i.e. there are more than k preimages of aw that start in p. If two of them end with the same letter, we already found a diamond. Therefore without loss of generality, we can assume that all of them have different last letters. Denote the set of these last letters by L. Symmetrically we can find a word $\widetilde{w}$ of length $(k-2)n$ with at least k preimages, where the preimages end either in c_m or d_m and have different first letters. We denote the set of first letters of those preimages by R.

As $|L \times R| = k^2 > n$, there are two distinct pairs $(l, r), (l', r') \in L \times R$ with $f(l, r) = f(l', r')$. Let $w_l, w_{l'}$ be words of length $|w|$ such that $G(p\ w_l\ l) = G(p\ w_{l'}\ l') = aw$. Analogously, let $w_r, w_{r'}$ be words of length $|\widetilde{w}|$ such that $G(r\ w_r\ s) = G(r'\ w_{r'}\ s) = \widetilde{w}b$. Then $p\ w_l\ l\ r\ w_r\ s$ and $p\ w_{l'}\ l'\ r'\ w_{r'}\ s$ form a diamond, and the length of the diamond is at most

$$|w_l\ l\ r\ w_r| = |w| + |\widetilde{w}| + 2 \leq 2(k-2)n + 2.$$ □

5 Improved Bounds

5.1 Improving the Algebraic Tools

We can improve Lemma 2 under conditions that apply for diamonds and orphans. The idea is to prove a lower bound for the dimension of the first affine subspace A_1. Let us call a $0/1$ -square matrix *k-regular* if every row and every column contains exactly k ones.

Lemma 3. *Let M be a k-regular 0/1 matrix of size $n \times n$, where $1 \leq k \leq n-1$. Then* $\operatorname{rank} M \geq \max\{\lceil\frac{n}{k}\rceil, \lceil\frac{n}{n-k}\rceil\}$.

Proof. It follows from the assumptions that every column contains k non-zero elements. To any collection of i columns one can then add another linearly independent column, provided $i < \frac{n}{k}$. This follows from the fact that some row r contains a zero in each of the i columns, so any column with a non-zero element

in row r is linearly independent of the i columns. Hence the rank of the matrix is at least $\frac{n}{k}$.

Analogously, the rank of the $(n-k)$-regular matrix $M' = \mathbf{1} - M$ is at least $\frac{n}{n-k}$, where $\mathbf{1}$ is the matrix that contains only ones. The ranks of M and M' are easily seen equal, so the result follows. □

Now we state an improvement of Corollary 1, that can be applied to diamonds and orphans of range-2 CA.

Corollary 2. *Let $G = (S, N, f)$ be a range-2 non-surjective CA with $S = \{1, \ldots, n\}$, and let x be a 0/1 -vector. Let $k = \phi(x)$ and assume that $1 \leq k \leq n-1$. If for all $s \in S$, $f_s(x)$ is a 0/1 -vector then there are words u, u' of length at most $n - \max\{\lceil \frac{n}{k} \rceil, \lceil \frac{n}{n-k} \rceil\} + 2$ with $\phi(f_u(x)) < \phi(x)$ and $\phi(f_{u'}(x)) > \phi(x)$.*

Proof. We follow the proof of Lemma 2 and use the same notation. Here, A is the affine space $x + \ker \phi$. Since G is not surjective, there is a w with $f_w(x) \notin A$. We give a lower bound for the dimension of A_1, the affine space generated by vectors x and $f_s(x)$ over all $s \in S$.

Define the 0/1 -matrix $M = (f_1(x), \ldots, f_n(x))$. Without loss of generality, we can assume that $\phi(f_s(x)) = k$ for all $s \in S$, as otherwise $f_s(x) \notin A$. Thus, every column of M contains exactly k ones and $n-k$ zeros. Further, as in the proof of Lemma 1 we see that the sum of the columns is $(k, k, \ldots, k)^T$ so the matrix M is k-regular.

Lemma 3 gives $r = \max\{\lceil \frac{n}{k} \rceil, \lceil \frac{n}{n-k} \rceil\}$ as a lower bound for the rank of M. Thus the affine subspace

$$A_1 = x + \langle \{ f_s(x) - x \mid s \in S \} \rangle$$

of Lemma 2 has at least dimension $r - 1$. Hence the chain of dimensions in Lemma 2 becomes

$$r - 1 \leq \dim A_1 < \ldots < \dim A_{i-1} \leq \dim A = n - 1$$

Hence $r + i - 3 \leq \dim A_{i-1} \leq n - 1$ and therefore there is an u with $|u| \leq n - r + 2$ and $\phi(f_u(x)) \neq \phi(x)$. The claim follows from Lemma 1. □

To obtain the bounds for the lengths of the shortest orphan and diamond, we apply the corollary above at each weight reduction step. This will lead to expressions of the form $\overline{H}_{k,n} = \sum_{i=1}^{k} \lceil \frac{n}{i} \rceil$. We immediately see that $\overline{H}_{k,n} > n \ln k$, since $\sum_{i=1}^{k} \frac{1}{i} > \ln k$. Further, we note that

$$\sum_{i=1}^{n-1} \max \left\{ \left\lceil \frac{n}{i} \right\rceil, \left\lceil \frac{n}{n-i} \right\rceil \right\} = 2\overline{H}_{\lfloor \frac{n-1}{2} \rfloor, n} + b$$

where $b = 2$ if n is even otherwise $b = 0$.

5.2 Improved Results

Combinatorial methods as well as Corollary 2 allow us to lower the bounds by looking at each weight reduction step. Let $F_a : 2^S \to 2^S$ be the set mapping

$$F_a(X) = \{y \in S \mid \exists x \in X : f(x, y) = a\}$$

for all $a \in S$ and $X \subseteq S$. Function F_a corresponds to the linear mapping f_a, with the difference that F_a ignores possible multiplicities.

The next lemma lowers the bound for the first step of weight reduction.

Lemma 4. *If G is non-surjective then there exists a letter a such that $|F_a(S)| < |S|$.*

Proof. If $F_a(S) = S$ for all $a \in S$ then $F_w(S) = S$ for all $w \in S^*$, so the CA would be surjective. □

For the second step and the last step of the weight reduction, Corollary 2 provides a reducing word of length at most 2. More generally, we have the following:

Lemma 5. *If $|X| = k$ and $1 \leq k \leq n-1$ then there exists a word u of length at most $n - \max\{\lceil \frac{n}{k} \rceil, \lceil \frac{n}{n-k} \rceil\} + 2$ such that $|F_u(X)| < |X|$.*

Proof. Let $x \in \mathbb{R}^n$ be the 0/1 -vector corresponding to set X. If $f_s(x)$ is not a 0/1 -vector for some $s \in S$ then either $\phi(f_s(x)) > k$ or $|F_s(X)| < k$. In both cases $|F_a(X)| < |X|$ for some $a \in S$.

If all $f_s(x)$ are 0/1 -vectors then the conditions of Corollary 2 are satisfied, so the bound follows from the Corollary. □

Now we easily get the following upper bounds for shortest orphans and diamonds.

Theorem 4. *Let $G = (N, S, f)$ be a non-surjective range-2 CA with $|S| = n$. Then $n^2 - 2\overline{H}_{\lfloor \frac{n-1}{2} \rfloor, n} + n - b - 1$ is an upper bound for the length of a shortest orphan, where $b = 2$ if n is even otherwise $b = 0$. Especially, a smallest orphan has at most length $n^2 - 2n \ln \lfloor \frac{n-1}{2} \rfloor + n$.*

Proof. We modify the proof of Theorem 1. We use Lemma 4 to improve the first reduction step and Lemma 5 on the remaining steps. We get the following upper bound for the length of a shortest orphan w:

$$\begin{aligned} |w| &\leq 1 + \textstyle\sum_{i=1}^{n-1} (n - \max\{\lceil \frac{n}{i} \rceil, \lceil \frac{n}{n-i} \rceil\} + 2) \\ &= 1 + (n-1)(n+2) - \textstyle\sum_{i=1}^{n-1} \max\{\lceil \frac{n}{i} \rceil, \lceil \frac{n}{n-i} \rceil\} \\ &= n^2 + n - 2\overline{H}_{\lfloor \frac{n-1}{2} \rfloor, n} - b - 1 \end{aligned}$$

where $b = 2$ if n is even otherwise $b = 0$. □

Theorem 5. *Let $G = (S, N, f)$ be a non-surjective range-2 CA with $|S| = n$, its shortest diamond has at most length $2(\lfloor \sqrt{n} \rfloor n - n \ln(\lfloor \sqrt{n} \rfloor) + 2\lfloor \sqrt{n} \rfloor - 2)$.*

Proof. We modify the proof of Theorem 3. Note, that the conditions of Corollary 2 are fulfilled for every increment of weight: If at any stage $f_s(x)$ is not a $0/1$ -vector then a diamond is found.

Thus the step increasing the weight from i takes a word of length at most $n - \lceil \frac{n}{i} \rceil + 2$. Therefore we obtain the upper bound

$$\sum_{i=2}^{k-1}(n - \left\lceil \frac{n}{i} \right\rceil + 2) = (k-2)(n+2) + n - \overline{H}_{k-1,n}$$

for the lengths of the words w and $\widetilde{w}$ in the proof of Theorem 3. Recall that $k = \lfloor \sqrt{n} \rfloor + 1$. We now obtain the result from this, the fact that $|w| + |\widetilde{w}| + 2$ is an upper bound for the length of the shortest diamond, and the fact that $\overline{H}_{k-1,n} > n \ln(k-1)$. □

6 Algorithms

The proof of Lemma 2 gives us algorithms for finding orphans, diamonds and unbalanced words whose running times are polynomial in the number of states.

Here, only one step will be described in Algorithm 1. That is to say, the algorithm is for obtaining from a vector x a word $w = w_1 \dots w_k$ such that $\phi(f_w(x)) < \phi(x)$. Note that we can easily have the converse, by only changing the inequality in the algorithm. The full algorithms can be easily deduced from this by looking at the proofs of Theorems 1, 2 and 3.

Algorithm 1. How to decrease the weight of a vector

Data: A non-surjective CA $G = (S, (0,1), f)$ and $x \in \{0,1\}^n \setminus 0^n$
Result: A word w with $\phi(f_w(x)) < \phi(x)$.
$F := \{(x, \epsilon)\}$ `% Set of independent vectors reached.`
while $\exists a \in S, \exists (x,w) \in F$ `such that` $f_a(x)$ `is not in the affine space generated by` F **do**
  if $\phi(f_a(x)) < \phi(x)$ **then**
    return wa ;
  end
  if $\phi(f_a(x)) = \phi(x)$ **then**
    $F := F \cup \{(f_a(x), wa)\}$;
  end
end

It is important to note that the algorithms based on this method will not necessarily find the shortest orphans, diamonds or unbalanced words. De Bruijn-graph based algorithms of [9] can be used to find a shortest diamond in polynomial time, using a breadth-first search on the product of the de Bruijn automaton with itself. Our algorithm above finds a shortest unbalanced word if the search in the **while** -loop is done in the breadth-first order, starting with vector $x = (1, 1, \dots, 1)$. We are not aware of a polynomial time method to find a shortest orphan.

7 Tightness

It is an interesting question to determine the best possible upper bounds for the lengths of shortest orphans, diamonds and unbalanced words. To see how tight our bounds are, we tried to discover families of CA with long shortest orphans, diamonds and unbalanced words.

For the shortest orphans we were able to construct, for every $n \geq 1$, an n-state, range-2 CA $\mathcal{A}_n$ whose shortest orphan has length $2n-1$. This example is still well below our quadratic upper bound, but we conjecture that $2n-1$ is the proper bound for the length of the shortest orphan. Through exhaustive search we verified that no 2, 3 or 4 state automaton exceeds this bound.

The transition table of $\mathcal{A}_n$ is given in figure 1. The state set is $S = \{0, 1, 2, \ldots, n-1\}$ and the local rule f is obtained from the function $f'(a, b) = b - a \pmod{n}$ by changing the entry $(0, 0)$ from 0 to 1.

f	0	1	...	$n-2$	$n-1$
0	$\underline{1}$	1	...	$n-2$	$n-1$
1	$n-1$	0	...	$n-3$	$n-2$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
$n-2$	2	3	...	0	1
$n-1$	1	2	...	$n-1$	0

Fig. 1. Local transition function of the automaton $\mathcal{A}_n$ which has a shortest orphan of length $2n-1$

Theorem 6. *For any number of states $n \geq 2$, the shortest orphan of automaton $\mathcal{A}_n$ has length $2n-1$.*

Proof. Word $w = 0(10)^{n-1}$ is an orphan: the only preimages of 0 are aa for $a \neq 0$, so a preimage of w cannot contain 0's and should be of the form

$$a\ a\ a+1\ a+1\ \ldots\ a-1\ a-1.$$

But such a word necessarily contains letter 0, a contradiction.

Let us prove that every word u of length $2n-2$ has a preimage. The related local rule $f'(a, b) = a - b \pmod{n}$ makes a CA surjective, so u has a preimage v under the local rule f'. Moreover, adding any constant $c \pmod{n}$ to all the letters of v provides another preimage of u under f'. Since the length of v is $2n-1$, some letter $s \in S$ appears at most once in v. Hence the preimage v' obtained by subtracting s from every letter of v contains at most one 0. But on such words f' and f are identical, so v' is a pre-image to u under f. □

Concerning the shortest diamond, a computer search found an 8-state CA whose shortest diamond is of length 6. No automata with longer shortest diamond has been found. For every $n \leq 6$ a CA with n states and a shortest diamond of length $n-1$ exists, and we conjecture this to be the optimal bound.

8 Conclusion and Open Problems

For all problems—size of a smallest unbalanced word, orphan and diamond—the linear algebra approach leads to better bounds than the ones obtained with combinatorial methods. For some of the problems, we decreased the upper bound further by looking closer into the dimensional argument of our approach. The results can be extended straightforward to arbitrary neighborhood ranges. For unbalanced words and orphans one can use exactly the same approach. For diamonds a standard blocking technique can be used.

The following table gives an overview of the results, for range-2 and the general range.

	$r = 2$	general r
Non-balanced word	n	n^{r-1}
Diamond	$2n^{\frac{3}{2}} - n \ln n + 2\sqrt{n} - 2$	$(r-1)(n^{\frac{3(r-1)}{2}} - n^{r-1}\frac{r-1}{2} \ln n)$
Orphan	$n^2 - 2n \ln \frac{n}{2} + n$	$n^{2(r-1)}$

We reported in Section 7 a family of n-state CA with shortest orphans of length $2n-1$, and also results of preliminary computer experiments. These lead us to formulate the following conjectures:

Conjecture 1. The tight upper bound of the length for the shortest orphan of an n -state non-surjective range-2 CA is $2n-1$.

Conjecture 2. The tight upper bound of the length for the shortest diamond of an n -state non-surjective range-2 CA is $n-1$.

An interesting related problem is the size of words for which many orphans occur. It can be seen rather easily that more than half of the words in S^l are orphans when l is exponential in the size of shortest orphans. Can a polynomial bound be obtained? This is relevant for the complexity of converting a given non-surjective CA to a lattice gas automaton, see [10].

References

1. Czeizler, E., Kari, J.: A tight linear bound on the neighborhood of inverse cellular automata. In: Caires, L., Italiano, G.F., Monteiro, L., Palamidessi, C., Yung, M. (eds.) ICALP 2005. LNCS, vol. 3580, pp. 410–420. Springer, Heidelberg (2005)
2. Hedlund, G.: Endomorphisms and automorphisms of shift dynamical systems. In: Mathematical Systems Theory, vol. 3, pp. 320–375. Springer, Heidelberg (1969)
3. Kari, J.: Reversibility and surjectivity problems of cellular automata. J. Comput. Syst. Sci. 48, 149–182 (1994)
4. Kari, J.: Synchronizing finite automata on eulerian digraphs. Theor. Comput. Sci. 295(1-3), 223–232 (2003)

5. Moore, E.F.: Machine models of self reproduction. In: Mathematical Society Proceedings of Symposia in Applied Mathematics, vol. 14, pp. 17–33 (1962)
6. Subrahmonian Moothathu, T.K.: Studies in Topological Dynamics with Emphasis on Cellular Automata. PhD thesis, Department of Mathematics and Statistics, School of MCIS, University of Hyderabad (2006)
7. Myhill, J.: The converse of Moore's garden-of-eden theorem. Proc. Amer. Math. Soc. 14, 685–686 (1963)
8. Pin, J.-E.: Utilisation de l'algèbre linéaire en théorie des automates. In: Actes du 1er Colloque AFCET-SMF de Mathématiques Appliquées, pp. 85–92. AFCET (1978)
9. Sutner, K.: Linear cellular automata and de bruijn automata. In: Mathematics and Its Applications 4, vol. 460, pp. 303–320. Kluwer, Dordrecht (1999)
10. Toffoli, T., Capobianco, S., Mentrasti, P.: When–and how–can a cellular automaton be rewritten as a lattice gas? Theor. Comput. Sci. 403, 71–88 (2008)