**Symmetry in**
**Self-Correcting Cellular Automata**

by
Nicholas Pippenger

Technical Report 92-8
April 1992

---

Department of Computer Science
University of British Columbia
Rm 333 - 6356 Agricultural Road
Vancouver, B.C.
CANADA V6T 1Z2

# Symmetry in Self-Correcting Cellular Automata

Nicholas Pippenger*

Department of Computer Science
The University of British Columbia
Vancouver, British Columbia V6T 1Z2
CANADA

**Abstract:** We study a class of cellular automata that are capable of correcting finite configurations of errors within a finite amount of time. Subject to certain natural conditions, we determine the geometric symmetries such automata may possess. In three dimensions the answer is particularly simple: such an automaton may be invariant under all proper rotations that leave the underlying lattice invariant, but cannot be invariant under the inversion that takes each configuration into its mirror image.

* This research was partially supported by an NSERC Operating Grant and an ASI Fellowship Award.

## 1. Introduction

The first clear formulation of the notion of a cellular automaton is apparently to be found in S. Ulam's address [U] to the International Congress of Mathematicians in 1950, where he attributes the model to J. von Neumann and himself. Cellular automata were subsequently made the basis for von Neumann's posthumously published work [N] on self-reproducing automata, which included among other things a construction of a "universal" cellular automaton.

We paraphrase Ulam's formulation as follows. We are given an infinite lattice of "cells", each with a finite number of connections to certain of its "neighbours" (including perhaps itself). Each cell is, at each moment of discrete time, in one of a finite number of possible "states". The states of the neighbours at each moment induce, in a specified manner, the state of the cell at the succeeding moment. This rule of transition is fixed deterministically. Throughout this paper we shall be concerned exclusively with the "Boolean" (or "binary") case, in which each cell has just 2 possible states.

In the years since this early work, many efforts have been made to find simple and natural universal cellular automata. Two of the most striking are J. H. Conway's "Life" (shown to be universal by R. W. Gosper; see [BCG]) and N. Margolus's "Billards" (based on a physical universal automaton devised by E. Fredkin; see [M]). Both are based on a 2-dimensional square lattice of cells. We shall not describe their transition rules in detail here, but merely observe that both possess remarkable symmetries. The rule of Life is invariant under translation in time and space, as well as under reflection and rotation in space. The rule of Billards is periodic with period 2 in time and space, with a parity condition linking these periodicities; translation in time and space, reflection and rotation in space, and reversal of time all amount to adjustment of the parity condition.

The results of this paper concern not universality, but rather a much simpler condition we shall call "self-correction". We shall say that a cellular automaton is *self-correcting* if, whenever it is started with all but finitely many of its cells in a common state, it reaches within finitely many steps the state with all its cells in that common state. Thus a self-correcting cellular automaton is one that can always eliminate a finite amount of "deviation" from an "ambient" state in a finite amount of time.

Neither Life nor Billiards is self-correcting; indeed, each has small "self-sustaining" configurations that have all but a finite positive number of cells in a common state, but for which these deviant cells are unaffected by the transition rule. (We do not require that a self-sustaining configuration be invariant under the transition rule: new cells may become deviant under the application of the rule.) A simple example a self-correcting cellular automaton is A. L. Toom's "Wedge" [T]. In this automaton, each cell adopts as its next state the majority of the current states of itself and its two nearest neighbours in the non-negative quadrant of which it forms the origin. This rule, and all others we shall consider in the remainder of this paper, is invariant under translation in time and space.

To see that Wedge is self-correcting, we consider an arbitrary finite set of initially deviant cells. By invariance under spatial translation, we may assume that the this set is contained in the non-negative quadrant, and indeed that it lies within a triangle having initial segments the non-negative axes as legs and a line segment with slope $-1$ as hypotenuse. Every cell outside this triangle has itself and at least one of its neighbours outside the triangle; thus these cells can never become deviant. Furthermore, each cell on the hypotenuse has both its neighbours outside the triangle; thus, though these cells may initially be deviant, they will be corrected to the ambient state during the first step. It follows that the set of deviant cells after the first step is contained in a triangle similar to the initial triangle, but with its intercepts reduced by 1. After finitely many steps, these intercepts become negative, and the triangle becomes empty.

The rule of Wedge does not have as much geometric symmetry as that of Life: it is not invariant under any rotation, and is only invariant under reflection through the main diagonal (and not under the other 3 reflections of the square). It does, however, have some other striking properties. First, it is "monotone": if some cells in the initial configuration are changed from one state to the other, none of the states of cells in the succeeding configuration will change from the other state to the first. Second, it is "self-dual"; that is, it is invariant under the exchange of the two states.

If we seek to combine the geometric symmetry of Life with the monotone, self-dual and self-correcting properties of Wedge, the following rule, which we call "Cross", is probably the first attempt that comes to mind. In this automaton, each cell adopts as its next state the majority of the current states of itself and its four nearest neighbours. It is clear, however, that four cells at the corners of a unit square form a self-sustaining configuration (since each cell has itself and two of its neighbours in the configuration), so Cross is not self-correcting, though it is montone, self-dual and symmetric under the full dihedral group of the square lattice.

The principal question addressed by this paper is how much geometric symmetry a monotone, self-dual and self-correcting rule can possess. We shall not confine ourselves to the square lattice, but more generally will consider the "hypercubic" lattice in $d \geq 2$

dimensions. (A simple argument shows that there is no monotone, self-dual and self-correcting rule for the 1-dimensional linear lattice, irrespective of geometric symmetry considerations.) In Section 2 we shall formulate this question more precisely.

In Section 3 we shall show that one symmetry, the "inversion" (or "antipodal involution", which simultaneously reverses all coordinates), is never possible for a monotone, self-dual and self-correcting rule. Indeed, given any monotone, self-dual rule invariant under inversion, we shall construct a finite self-sustaining configuration. This construction generalizes the self-sustaining configuration for Cross to a large class of rules.

In Section 4 we shall show that in an odd number $d \geq 3$ of dimensions, the inversion is the only forbidden symmetry. When $d$ is odd, the group of symmetries of the $d$-dimensional hypercube factors into a group of "proper rotations" and the group generated by the inversion. We shall construct a monotone, self-dual and self-correcting rule that is invariant under all proper rotation, and thus has the maximum allowed symmetry.

When $d$ is even, the situation is complicated by the fact that there is no longer a unique maximum group of symmetries that excludes the inversion, but rather there are many incomparable maximal groups. (For the 2-dimensional square lattice, for example, each of the 4 groups generated by a single reflection excludes the inversion, but any group containing two distinct reflections, or any rotation, includes the inversion.) It remains true that for any group excluding the inversion, there is a monotone, self-dual and self-correcting rule invariant under that group. This can be proved by essentially the same methods used in Section 4, with some modifications to deal with the richer variety of circumstances that can arise.

We should acknowledge at this point that all of the techniques employed in the following sections are taken from Toom's paper [T]. The sole contribution of the present paper is to derive their consequences as regards the forbidden and allowed geometric symmetries.

## 2. Cellular Automata

The cellular automata considered in this paper will satisfy the following five conditions. First, they are based on the "simple hypercubic lattice" with some number $d \geq 2$ of dimensions. That is, there is a "cell" situated at each point in $d$-dimensional Euclidean space with integral coordinates. We shall let $\mathbf{R}^d$ denote $d$-dimensional Euclidean space and $S = \mathbf{Z}^d$ the set of points with integral coordinates. Second, they evolve in discrete time from some initial moment. We shall let $T = \{0, 1, 2, \ldots\}$ denote the set of moments. Third, they will be "Boolean" (or "binary"). That is, each cell is at each moment in one of two possible states. We shall let $\mathbf{B} = \{0,1\}$ denote the set of states. Fourth, the evolution proceeds in accordance with a "transition rule", which is the same for every cell (translationally invariant in space) and every moment (translationally invariant in time). Fifth, this rule specifies the new state of a cell as a deterministic function of the state of some finite number of other cells at the immediately preceding moment in time.

A cellular automaton meeting these conditions can be specified by prescribing a list $x_1, \ldots, x_n \in \mathbf{Z}^d$ of displacements from a cell to the neighbours on which the new state of the cell depends, together with a Boolean function $f$ of $n$ arguments, which determines the state of this cell as a function of the states of the neighbours. Thus, the state of cell $y$ at time $t+1$ is are the states of cells $x_1 + y, \ldots, x_n + y$, respectively, at time $t$.

Once such an automaton has been specified, the "trajectory" (the state of every cell at every moment) is completely determined by the initial conditions (the state of every cell at the initial moment).

A transition rule $\varrho = (x_1, \ldots, x_n, f)$ is said to be *monotone* if $f$ is a monotone Boolean function; that is, if $f(a_1, \ldots, a_n) \leq f(b_1, \ldots, b_n)$ whenever $a_1 \leq b_1, \ldots, a_n \leq b_n$. If $f$ is monotone, then it can be written uniquely in *conjunctive normal form* as

$$f(a_1, \ldots, a_n) = \bigwedge_{I \in \mathcal{I}} \bigvee_{i \in I} a_i.$$

The disjunctions $\bigvee_{i \in I} a_i$ (or, by abuse of language, their sets $I$ of indices) for $I \in \mathcal{I}$ are called the *maxterms* of $f$; they correspond to sets of arguments that, if they are simultaneously assigned the value 0, are sufficient to force the value of $f$ to be 0. A monotone Boolean function $f$ can also be written uniquely in *disjunctive normal form* as

$$f(a_1, \ldots, a_n) = \bigvee_{I \in \mathcal{I}} \bigwedge_{i \in I} a_i.$$

The conjunctions $\bigwedge_{i \in I} a_i$ (or, by abuse of language, their sets $I$ of indices) for $I \in \mathcal{I}$ are called the *minterms* of $f$; they correspond to sets of arguments that, if they are simultaneously assigned the value 1, are sufficient to force the value of $f$ to be 1.

If $f$ is a Boolean function of $n$ arguments, the *dual* of $f$, denoted $f^*$, is defined by

$$f^*(a_1, \ldots, a_n) = \overline{f(\overline{a_1}, \ldots, \overline{a_n})}.$$

(Here $\overline{a}$ denotes the Boolean complement of $a$.) Roughly speaking, $f^*$ is obtained from $f$ by interchanging the roles of the Boolean values 0 and 1. In particular, if $f$ is monotone, then $f^*$ is obtained from $f$ by interchanging the roles of maxterms and minterms.

A transition rule $\varrho = (x_1, \ldots, x_n, f)$ is said to be *self-dual* if $f$ is a self-dual Boolean function; that is, if $f^* = f$. If a monotone Boolean function $f$ is self-dual, its maxterms are the same as its minterms. In this case we may refer to them simply as *terms*. Furthermore, any two terms must have an argument (or, by abuse of language, an index) in common; for if not, the arguments of one term could be assigned the value 0, forcing the value of the function to be 0, and the arguments of another term could simultaneously be assigned the value 1, forcing the function to be 1.

If $f$ is a Boolean function of $n$ arguments and $\pi$ is a permutation of the set $\{1, \ldots, n\}$, the *image* of $f$ under $\pi$, denoted $f^\pi$, is defined by

$$f^\pi(a_1, \ldots, a_n) = f(a_{\pi^{-1}(1)}, \ldots, a_{\pi^{-1}(n)}).$$

(Here $\pi^{-1}$ denotes the inverse of the permutation $\pi$.) We shall say that $f$ is *invariant* under $\pi$ if $f^\pi = f$. The set of all permutations under which a Boolean function $f$ is invariant forms a group (under composition of permutations), which we shall denote $\mathrm{Sym}(f)$. We shall say that $f$ is *symmetric* if it is invariant under all permutations.

If $n = 2m+1$ is odd, then by the *majority* of $n$ arguments we shall mean the monotone and self-dual Boolean function whose terms are all subsets comprising $m+1$ of the $2m+1$ arguments. The majority function is symmetric.

An *isometry* of $\mathbf{Z}^d$ is a permutation of the points of $\mathbf{Z}^d$ that preserves Euclidean distances between pairs of points. A *rotation* of $\mathbf{Z}^d$ is a permutation of the points of $\mathbf{Z}^d$ that fixes the origin $(0, \ldots, 0)$, and therefore induces an isometry of the $2^d$ vertices $(\pm 1, \ldots, \pm 1)$ of the hypercube centered at the origin. Any isometry of $\mathbf{Z}^d$ can be uniquely expressed as a translation of $\mathbf{Z}^d$ followed by a rotation. We shall denote by $\mathrm{O}(d, \mathbf{Z})$ the group of rotations of $\mathbf{Z}^d$.

A rotation of $\mathbf{Z}^d$ can be uniquely expressed as a permutation of the $d$ coordinate axes, followed by a reversal of some subset of these axes. (A permutation of the coordinates is effected by a transformation matrix whose entries are 0's, except for $d$ entries that are 1's, with a single 1 in each row and each column. A reversal of some coordiates is effected by a transformation matrix whose entries are 0's, except for the $d$ entries on the main diagonal, which are either 1's or $-1$'s. The determinant of the matrix of a rotation is either 1 or $-1$.) Since there are $d!$ permutations of $\{1, \ldots, d\}$ and $2^d$ subsets of $\{1, \ldots, d\}$, there are $d!\,2^d$ rotations in $\mathrm{O}(d, \mathbf{Z})$.

For a rotation, the permutation of the coordinates may be either even or odd, and the number of reversed coordinates may be either even or odd. We shall say that a rotation is *proper* if the parity of the permutation and the parity of the number of reversal are either both even or both odd. (The determinant of the matrix of a proper rotation is 1.) Since there $d!/2$ permutations of each parity and $2^{d-1}$ subsets of each parity, there are $d!\,2^{d-1}$ proper rotations. We shall denote by $\mathrm{SO}(d,\mathbf{Z})$ the group of proper rotations of $\mathbf{Z}^d$.

By the *inversion* of $\mathbf{Z}^d$ we shall mean the rotation that reverses all $d$ coordinates (while permuting them according to the identity permutation). (The matrix of the inversion has $d$ entries $-1$ on the main diagonal, with all other entries being 0.) If $d$ is even, the inversion is a proper rotation. If $d$ is odd, every rotation can be uniquely expressed as a proper rotation followed by either the inversion or the identity rotation.

Two transition rules $\varrho = (x_1, \ldots, x_n, f)$ and $\sigma = (y_1, \ldots, y_n, g)$ are said to be *equivalent*, denoted $\varrho \equiv \sigma$, if there is a permutation $\pi$ of $\{1, \ldots, n\}$ such that $x_1 = y_{\pi(1)}, \ldots, x_n = y_{\pi(n)}$ and $f = g^\pi$. Equivalent transition rules give rise to identical trajectories when started with identical initial configurations, and thus determine the "same" cellular automaton.

If $\varrho = (x_1, \ldots, x_n, f)$ is a transition rule and $r \in \mathrm{O}(d,\mathbf{Z})$ is a rotation, we shall denote by $\varrho^r$ the transition rule defined by

$$\varrho^r = \big(r(x_1), \ldots, r(x_n), f\big).$$

We shall say that $\varrho$ is *invariant* under $r$ if $\varrho^r \equiv \varrho$. The rotations under which a transition rule $\varrho$ is invariant for a group, which we shall denote $\mathrm{Sym}(\varrho)$.

A configuration (that is, an assignment of Boolean values to each cell) is said to *deviate finitely* from the Boolean value $a$ if there are only finitely many $y \in S$ such that the state of cell $y$ is different from $a$. A trajectory (that is, an assignment of Boolean values to each cell at each moment) is said to *deviate finitely* from the Boolean value $a$ if there are only finitely many $(y,t) \in S \times T$ such that the state of cell $y$ at time $t$ is 1. A transition rule $\varrho$ is said to be *self-correcting* if, for each Boolean value $a$, every initial configuration that deviates finitely from $a$ evolves under $\varrho$ to a trajectory that deviates finitely from $a$.

An initial configuration is said to be *self-sustaining* for a transition rule $\varrho$ if (1) the initial configuration deviates finitely from 0, and (2) every cell that is in state 1 in the initial configuration is in state 1 at every time in the trajectory to which the initial configuration evolves under $\varrho$.

### 3. Forbidden Symmetry

*Theorem 3.1:* Let $\varrho$ be a monotone, self-dual rule that is invariant under inversion. Then there exists a finite self-sustaining configuration for $\varrho$.

Let $B \subseteq \mathbf{Z}^d$ be finite. We shall denote by $\text{Conv}(B) \subseteq \mathbf{R}^d$ the *convex hull* of $B$, which is compact. Let $A \subseteq \mathbf{R}^d$ be a compact convex set. For $\alpha \in \mathbf{R}$, shall denote by $\alpha A$ the compact convex set $\{\alpha x : x \in A\}$. If $A' \in \mathbf{R}^d$ is another compact convex set, we shall denote by $A + A'$ the compact convex set $\{x + x' : x \in A, x' \in A'\}$. The operation "+" thus defined is associative and commutative, and has the compact convex set $\{0\}$ as neutral element.

We shall need several lemmas for the proof. The first two involve the notion of an "obtuse" set.

A set $A \subseteq \mathbf{R}^d$ will be called *obtuse* for a set $B \subseteq \mathbf{Z}^d$ if every translate of $A$ that meets $\text{Conv}(B)$ meets $B$ itself.

*Lemma 3.2:* For every finite set $B$, there is a compact set $A$ that is obtuse for $B$.

*Proof:* Suppose that $B$ contains $k$ points. Let $A = -(k-1)\text{Conv}(B)$. Suppose that $A + z$ meets $\text{Conv}(B)$. Then $z \in k\text{Conv}(B)$. Thus $y = \sum_{y \in B} \alpha_y y$, where the coefficients $\alpha_y$ are non-negative and sum to $k$. We must have $\alpha_x \geq 1$ for some $x \in B$. Thus we have $z = x + \sum_{y \in B} \beta_y y$, where $\beta_x = \alpha_x - 1$ and $\beta_y = \alpha_y$ for $y \neq x$. Thus the coefficients $\beta_y$ are non-negative and sum to $k - 1$. This means that $z \in x + (k-1)\text{Conv}(B)$, which implies $x \in z + A$. $\triangle$

*Lemma 3.3:* For every finite set $\mathcal{B} = \{B_1, \ldots, B_l\}$ of finite sets $B_1, \ldots, B_l \subseteq \mathbf{Z}^d$, there is a compact set $A$ that is obtuse for each set $B_j \in \mathcal{B}$.

*Proof:* By Lemma 3.2, for each $B_j \in \mathcal{B}$, there is a set $A_j \subseteq \mathbf{R}^d$ that is obtuse for $B_j$. The set $A = A_1 + \cdots + A_l$ is obtuse for each $B_j \in \mathcal{B}$. $\triangle$

Since the rule $\varrho = (x_1, \ldots, x_n, f)$ is monotone, the Boolean function $f$ may be expressed as a conjunction of maxterms. These maxterms are disjunctions of arguments of $f$, but we may regard them as subsets of the set $\{x_1, \ldots, x_n\}$, since the arguments are the states of the cells at these displacements.

*Lemma 3.4:* Let $\varrho = (x_1, \ldots, x_n, f)$ be monotone, self-dual and invariant under inversion. If $B \subseteq \{x_1, \ldots, x_n\}$ is a term of $f$, then $0 \in \text{Conv}(B)$.

*Proof:* Since $\varrho$ is invariant under inversion, $-B$ is also a term of $f$. Since $\varrho$ is self-dual, these two terms must have an element $x$ in common. Since $x \in -B$, we have $-x \in B$. Thus we can express 0 as $\frac{1}{2}x + \frac{1}{2}(-x)$, which proves that $0 \in \text{Conv}(B)$. $\triangle$

*Proof of Theorem 3.1:* Let $\mathcal{B} = \{B_1, \ldots, B_l\}$ be the set of terms of $\varrho$. Using Lemma 3.3, let $A \subseteq \mathbf{R}^d$ be a compact set that is obtuse for each term $B_j \in \mathcal{B}$. The set $Y = A \cap \mathbf{Z}^d$ is finite, since $A$ is compct and $\mathbf{Z}^d$ is discrete. We shall show that $Y$ is a self-sustaining configuration for $\varrho$.

To do this, it will suffice to show that if $y \in Y$ is a cell of the configuration and $B \in \mathcal{B}$ is a term, then there exists a displacement $x \in B$ such that $x + y \in Y$ is also a cell of the configuration. Since $y \in Y$, we have $y \in A$, which implies $0 \in A - y$. By Lemma 3.4, we have $0 \in \mathrm{Conv}(B)$. Thus the translate $A - y$ of $A$ meets $\mathrm{Conv}(B)$. Since $A$ is obtuse for $B$, $A - y$ meets $B$ as well, say in the element $x$. Since $x \in A - y$, we have $x + y \in A$. Since $x \in B \subseteq \mathbf{Z}^d$ and $y \in Y \subseteq \mathbf{Z}^d$, we also have $x + y \in \mathbf{Z}^d$. Thus $x + y \in Y$. $\triangle$

## 4. Allowed Symmetry

*Theorem 4.1:* For every odd $d \geq 3$, there is a self-correcting rule that is monotone, self-dual and invariant under all proper rotations.

For brevity, let $R = \mathrm{SO}(d, \mathbf{Z})$ be the group of proper rotations. Let $m = d!\, 2^{d-2}$ (which is a positive integer, since $d \geq 3$). The group $R$ has order $2m$.

Define the displacement $\xi \in \mathbf{Z}^d$ by

$$\xi = (1, 2, \ldots, d).$$

For $\eta \in \mathbf{Z}^d$, we shall denote by

$$\mathrm{Orb}_R(\eta) = \{g\eta : r \in R\}$$

the *orbit* of $\eta$ under $R$. Let

$$\Xi = \mathrm{Orb}_R(\xi).$$

Since only the identity element of $R$ fixes $\xi$, the orbit $\Xi$ has cardinality $2m$.

Let $n = 2m + 1$. Let define $x_1, \ldots, x_n \in \mathbf{Z}^d$ so that $\{x_1, \ldots x_n\} = \Xi \cup \{0\}$ (the actual correspondence is immaterial). Let $f : \mathbf{B}^n \to \mathbf{B}$ be the majority of $n$ Boolean arguments, and set $\varrho = (x_1, \ldots, x_n, f)$. It is clear that $\varrho$ is monotone, self-dual and invariant under all proper rotations. We shall show that $\varrho$ is self-correcting.

Let

$$L = \mathrm{Lin}(\mathbf{Z}^d, \mathbf{R})$$

denote the set of linear *forms* defined on $\mathbf{Z}^d$ and taking values in $\mathbf{R}$. For $\psi \in L$ and $\eta \in \mathbf{Z}^d$, we shall denote by $\psi\eta$ the value of the form $\psi$ for the point $\eta$.

We define the action of the group $R$ on $L$ by taking $(r\psi)\eta = \psi(r^{-1}\eta)$ for $r \in R$, $\psi \in L$ and $\eta \in \mathbf{Z}^d$. For $\psi \in L$, we shall define

$$\mathrm{Orb}_R(\psi) = \{r\psi : r \in R\}$$

to be the orbit of $\psi$ under $R$.

For $2 \le i \le d$, let $a_i = i$ and $b_i = 4i - 7$. Let

$$c = \sum_{2 \le i \le d} a_i b_i.$$

Since $d \ge 3$, we have $c \ge 17$.

*Lemma 4.2:* If $\pi$ is a permutation of $\{2, \ldots, d\}$, then

$$\sum_{2 \le i \le d} a_i b_{\pi(i)} \le c,$$

and if $\pi$ is not the identity permutation, then

$$\sum_{2 \le i \le d} a_i b_{\pi(i)} \le c - 4.$$

*Proof:* Since $a_2, \ldots, a_d$ and $b_2, \ldots, b_d$ are both increasing sequences, $\sum_{2 \le i \le d} a_i b_{\pi(i)}$ is maximized by taking $\pi$ to be the identity permutation, in which case the sum is by definition $c$. If $\pi$ differs from the identity by the transposition of two adjacent indices, the sum is reduced by 4, and any further transpositions of adjacent elements reduce the sum still further. Since any permutation can be obtained by a sequence of transpositions of adjacent elements, the lemma follows. $\triangle$

Define the form $\phi \in L$ by

$$\phi = (2 - c, b_2, \ldots, b_d).$$

Let

$$\Phi = \mathrm{Orb}_R(\phi).$$

Since only the identity of $R$ fixes $\psi$, the set $\Phi$ has cardinality $2m$.

*Lemma 4.3:* For $\psi \in \Phi$, we have

$$\#\{\eta \in \Xi : \psi\eta \ge 2\} \ge m + 1.$$

*Proof:* Since $\psi\eta$, as $\eta$ runs through $\Xi$, and $\phi\eta$, as $\eta$ runs through $\Xi$, comprise the same terms in different sequences, it suffices to prove that

$$\#\{\eta \in \Xi : \phi\eta \ge 2\} \ge m + 1.$$

The $2m$ elements $\eta = (\eta_1, \ldots, \eta_d)$ of $\Xi$ fall into two classes: the $m$ for which $\eta_1$ is positive, and the $m$ for which $\eta_1$ is negative. At least one element from the first class, namely $\eta = \xi$ satisfies $\phi\eta \geq 2$: the first term of the inner product $\sum_{1\leq i\leq d} \phi_i\xi_i$ is $2 - c$, and the sum of the remaining terms is by definition $c$. is Thus it will suffice to show that, for every element $\eta$ from the second class, we have $\phi\eta \geq 2$.

First suppose $\eta = -1$. Then the first term of the inner product $\sum_{1\leq i\leq d} \phi_i\eta_i$ is $c - 2$, so it will suffice to show that the sum of the remaining terms is at least $4 - c$. The absolute values $|\eta_2|, \ldots, |\eta_d|$ are a permutation of $\xi_2, \ldots, \xi_d$. If this permutation is not the identity permutation, then by Lemma 4.2 we have

$$\sum_{2\leq i\leq d} \phi_i|\eta_i| \leq c - 4,$$

and thus

$$\sum_{2\leq i\leq d} \phi_i\eta_i \geq 4 - c,$$

as claimed. If this permutation is the identity permutation, then not all of the terms in the sum $\sum_{2\leq i\leq d} \phi_i\eta_i$ can be negative (since we must have $\eta_i = -\xi_i$ for an even number of indices $i$ in the range $1 \leq i \leq d$). It follows that

$$\sum_{2\leq i\leq d} \phi_i\eta_i \geq 4 - c,$$

since the sum would have value $-c$ if all the terms were negative, and changing the sign of the term with smallest absolute value increases the sum by 4. Thus if $\eta_1 = -1$, we have $\phi\eta \geq 2$.

Finally, if $\eta_1 \leq -2$, the first term of the inner product $\sum_{1\leq i\leq d} \phi_i\eta_i$ is at least $2c - 4$. The absolute value of the sum of the remaining terms is at most $c$, and thus we have $\phi\eta \geq c - 4 \geq 13$ in this case. $\triangle$

*Lemma 4.4:* For any $y \in \mathbf{Z}^d$, we have

$$\sum_{\psi\in\Phi} \psi y = 0.$$

*Proof:* For any $1 \leq i \leq d$ and $1 \leq j \leq d$, exactly $m$ of the forms $\psi \in \Phi$ have $\psi_i = \phi_j$, and the remaining $m$ have $\psi_i = -\phi_j$. $\triangle$

*Proof of Theorem 4.1:* Let $y \in \mathbf{Z}^d$ be a cell. We shall associate with $y$ a value $\mathrm{Val}(y) \in \mathbf{Z}$ as follows:

$$\mathrm{Val}(y) = \max\{\psi y : \psi \in \Phi\}.$$

Since the maximum of $\psi y$ over $\psi \in \Phi$ is be at least the average, which vanishes by Lemma 4.4, we have $\mathrm{Val}(y) \geq 0$.

Let $Y \subseteq \mathbf{Z}^d$ be a finite set of cells. We shall associate a value $\mathrm{Val}(Y) \in \mathbf{Z} \cup \{-\infty, +\infty\}$ as follows. If $Y$ is empty, we take $\mathrm{Val}(Y) = -\infty$. If $Y$ is not empty, we take

$$\mathrm{Val}(Y) = \max\{\mathrm{Val}(y) : y \in Y\}.$$

We observe that $\mathrm{Val}(Y) < 0$ implies $Y = \emptyset$, since $\mathrm{Val}(Y) \geq 0$ for $y \in \mathbf{Z}^d$.

Let $Y$ be the set of deviant cells at some time $t$, and let $Y'$ be the set of deviant cells at the immediately succeeding time $t+1$. It is clear that if $Y$ is finite, then so is $Y'$, since the rule $\varrho$ has finite neighbourhood. We shall show that

$$\mathrm{Val}(Y') \leq \mathrm{Val}(Y) - 2. \tag{1}$$

If $Y'$ is empty, then (1) is trivial. If $Y'$ is not empty, take $y' \in Y'$ such that $\mathrm{Val}(y') = \mathrm{Val}(Y')$. Then take $\psi \in \Phi$ such that $\psi y' = \mathrm{Val}(y')$. By Lemma 4.3, there are at least $m+1$ displacements $\eta \in \Xi$ such that $\psi\eta \geq 2$, and thus such that $\mathrm{Val}(y'+\eta) \geq \psi(y'+\eta) \geq \mathrm{Val}(y')+2$. Since $y'$ is deviant at time $t+1$, at least $m+1$ of its neighbours $y'+x_1, \ldots, y'+x_n$ are deviant at time $t$. One of these might be $y'$ itself, but at least $m$ must be of the form $y'+\eta$ for $\eta \in \Xi$. Since $(m+1)+m > \#\Xi$, there exists $\eta \in \Xi$ such that $\mathrm{Val}(y'+\eta) \geq \mathrm{Val}(y')+2$ and $y \in Y$. Thus we have $\mathrm{Val}(Y) \geq \mathrm{Val}(y'+\eta) \geq \mathrm{Val}(y')+2 = \mathrm{Val}(Y')+2$, which completes the proof of (1).

If there is initially a finite set $Y$ of deviant cells, then $\mathrm{Val}(Y)$ is initially finite. Since $\mathrm{Val}(Y)$ decreases by at least 2 at each time step, it must eventually become negative. At this moment the set of deviant cells must be empty. $\triangle$

## 5. References


[BCG] E. R. Berlekamp, J. H. Conway and R. K. Guy, *Winning Ways, for Your Mathematical Plays*, Academic Press, London, 1982.

[M] N. Margolus, "Physics-Like Models of Computation", *Physica D*, 10 (1984) 81–95.

[N] J. von Neumann, *Theory of Self-Reproducing Automata*, A. W. Burks (editor), University of Illinois Press, Urbana, IL, 1966.

[T] A. L. Toom, "Stable and Attractive Trajectories in Multicomponent Systems", R. L. Dobrushin and Ya. A. Sinai (editors), *Multicomponent Random Systems*, Marcel Dekker, New York, NY, 1980.

[U] S. Ulam, "Random Processes and Transformations", *Proc. ICM*, 1950, II, 254–275.