Laboratoire **B**ordelais de **R**echerche en **I**nformatique,
URA CNRS 1304,
Université Bordeaux I,
351, cours de la Libération,
33 405 TALENCE Cedex,
FRANCE.

Rapport de Recherche

Numéro 1135-96

Any Reversible Cellular Automaton Can be Represented with Block Permutations

Jérôme Olivier DURAND-LOSE*

LaBRI, URA CNRS 1304,
Université Bordeaux I,
351, cours de la Libération,
F-33 405 TALENCE Cedex,
FRANCE.

Abstract

Cellular Automata are mappings such that each cell is updated according to the states around it and a unique local function. Block Permutations are mappings that divide partitions regularly in rectangular blocks of states and make the same permutations on each block. We prove that any d-dimensional Reversible Cellular Automata (d-R-CA) can be expressed as the restriction of a composition of 2^d Block Permutations (BP). We exhibit such representation for any d-R-CA with 2^d BP of width $6r$. We also give a construction with $d+1$ BP, but with width $3(d+1)r$.

1 Introduction

Cellular Automata (CA) provide the most famous model for parallel phenomena, computations and architectures. They operate as iterative systems on d-dimensional infinite arrays, the underlying space is $\mathbb{Z}^d$. Each cell takes a value from a finite set of states $\mathcal{S}$. An iteration of a CA is the synchronous replacement of the state of every cell by the image of the states of neighboring cells according to a unique local function.

Reversible Cellular Automata (R-CA) are famous for modeling non-dissipative systems as well as for backtracking a phenomenon to its source. Reversibility is thought of as a means to save energy in computers. We refer the reader to the 1990 article of Toffoli and Margolus [8] to get a full introduction to the R-CA field (history, aims, uses, decidability ...) and a large bibliography. In this article, they make the following conjecture about R-CA :

Conjecture 1 [8, Conjecture 8.1] *Any cellular automaton can be expressed as a composition of block permutations.*

A block is a d-dimensional array of states. The lattice $\mathbb{Z}^d$ can be partitioned into regularly displayed blocks. A Block Permutation (BP) is a generalization of a permutation e over such a partition of $\mathbb{Z}^d$.

Kari [6] proves the Conj. 1 for dimensions 1 and 2. He uses $\mathcal{S}^2$ as the set of states for the BP during the simulation. At the end, he conjectures that:

Conjecture 2 [6, Conjecture 5.3] *Any d-dimensional cellular automaton can be expressed as a composition of 2^d block permutations.*

*e-mail: jdurand@labri.u-bordeaux.fr, http://www.labri.u-bordeaux.fr/~jdurand

In [2], we prove Conj. 1 for any dimension with $2^{d+1}-1$ BP of width $4r$. In this article, we prove Conj. 1 for any dimension with the number of permutations proposed by Kari, 2^d. Our constructive proof is based on the constructions made in [2] and the progressive erasing in Kari's proof. The size of the blocks is much greater than the neighborhood: $(6r, 6r, \ldots 6r)$, where r is the greater of the radii of the reversible CA and of its inverse. But the width of the block is constant: $6r$.

We give another construction with only $d+1$ BP. There is an important drawback to this: the width of the blocks is $3(d+1)r$ instead of $6r$. Within this construction, the origins of the BP are translated by $3r$ whereas before they take all values in $\{0, 3r\}^d$.

All definitions and proofs in this article can be read without any previous knowledge of the subject. The article is structured as follows. The definitions of Cellular Automata (CA), Block Permutations (BP) and reversibility are given in Section 2. In Section 3, for any reversible CA A, we exhibit 2^d BP such that the global function of A is a restriction of their composition. This proves the conjecture. In Sect. 4, we give a construction with only $d+1$ BP, but with wider blocks.

2 Definitions

Let d be a strictly positive integer. Cellular automata and block permutations define mappings over d-dimensional infinite arrays over a finite set of states $\mathcal{S}$. We denote $\mathcal{C} = \mathcal{S}^{\mathbb{Z}^d}$ the set of configurations. For any $x \in \mathbb{Z}^d$, σ_x is the shift by x: $\forall c \in \mathcal{C}, \forall i \in \mathbb{Z}^d, \sigma_x(c)_i = c_{i+x}$.

The set of integers $\{i, i+1, i+2, \ldots j\}$ is denoted $[\![i, j]\!]$. For any configuration c and any subset E of $\mathbb{Z}^d$, $c_{|E}$ is the restriction of c to E.

We denote $<$ and $\leq$ the following orders over $\mathbb{Z}^d$: $x < y \Leftrightarrow \forall k, x_k < y_k$ and $x \leq y \Leftrightarrow \forall k, x_k \leq y_k$. We denote $+$, mod, div and $.$ the pointwise vectorial addition, modulo, Eulerian division and multiplication over $\mathbb{Z}^d$. This means that: $\forall x, y \in \mathbb{Z}^d$, $\forall k$, $(x+y)_k = x_k + y_k$, $(x \bmod y)_k = x_k \bmod y_k$, $(x \operatorname{div} y)_k = x_k \operatorname{div} y_k$ and $(x \,.\, y)_k = x_k . y_k$.

2.1 Cellular Automaton

A *Cellular Automaton* (CA) A is defined by $(d, \mathcal{S}, r, f)$, where the *radius* r is a strictly positive natural number, and the *local function* f maps $\mathcal{S}^{(2r+1)^d}$ into $\mathcal{S}$. The *global function* of A, $\mathcal{G}_\mathrm{A}$, maps configurations into themselves as follows:

$$\forall c \in \mathcal{C},\ \forall i \in \mathbb{Z}^d,\ \mathcal{G}_\mathrm{A}(c)_i \ = \ f(c_{|i+[\![-r, r]\!]^d}) \ .$$

The new state of a cell depends only on the states of the cells which are at distance at most r.

2.2 Block Permutation

A *Block Permutation* (BP) is defined by $(d, \mathcal{S}, v, o, e)$ where the *size* v is an element of $\mathbb{Z}^d$ such that $1 \leq v$, and o is a coordinate modulo v (*i.e.*, $o \in \mathbb{Z}^d$ and $0 \leq o < v$). The *basic block* V is the following subset of $\mathbb{Z}^d$: $[\![0, v_1]\!] \times [\![0, v_2]\!] \times \cdots \times [\![0, v_d]\!]$. The function e is a permutation of $\mathcal{S}^V$. When all the lengths of the block are equal, we say that it is the *width* of the BP.

The block permutation of origin 0, T^0, is the following mapping over $\mathcal{C}$: for any $c \in \mathcal{C}$, for any $i \in \mathbb{Z}^d$, let $a = i \operatorname{div} v$ and $b = i \bmod v$ so that $i = a \,.\, v + b$, then $T^0(c)_i = e(c_{|a \,.\, v+V})_b$. In other words, the block which holds i in a regular partition issued from 0 is updated according to e. The same happens to all the blocks of this partition.

The *Block Permutation* of origin o, T_o is $\sigma_o \circ T^0 \circ \sigma_{-o}$. It is the same as before but with the partition is shifted by o.

We call *Block Permutation Automaton* or *Reversible Block Cellular Automaton* the composition of various BP with the same size and function e.

2.3 Reversibility

Both Cellular Automata and Block Permutations are synchronous and massively parallel mappings.

A Cellular Automaton A is *reversible* if and only if $\mathcal{G}_A$ is bijective and there is another CA B such that $\mathcal{G}_A^{-1} = \mathcal{G}_B$. Such an automaton B is called the inverse of A. Reversible CA are denoted R-CA.

Amoroso and Patt [1] give an algorithm which decides whether a 1-dimensional cellular automata is reversible or not. Kari [5] proves that the reversibility of CA is undecidable in greater dimensions.

By construction, block permutations are reversible. One simply uses the inverse permutation on the same partition to get the inverse block partition.

2.4 Simulation

Since CA are iterative, we use the following definition.

For any two functions $f : F \to F$ and $g : G \to G$, g *simulates* f if there exist two encoding functions $\alpha : F \to G$ and $\beta : G \to F$, space and time inexpensive compared to f and g, and a function $\varphi : \mathbb{N} \times F \to \mathbb{N}$ such that: $\forall x \in F, \forall n \in \mathbb{N}, f^n(x) = \beta \circ g^{\varphi(n,x)} \circ \alpha(x)$.

This corresponds to the commuting diagram of Fig. 1. The function g can be used instead of f for iterating.

$$\forall n \in \mathbb{N},\ 0 \leq n, \qquad \begin{array}{ccc} F & \xrightarrow{f^n} & F \\ {\scriptstyle\alpha}\downarrow & & \uparrow{\scriptstyle\beta} \\ G & \xrightarrow{g^{\varphi(n,.)}} & G \end{array}$$

Figure 1: g simulates f.

Simulation is a transitive relation. A simulation is in *linear time* τ if $\varphi(n, .) = \tau n$ for all natural n. If both f and g are invertible and g simulates f, by the unicity of predecessors, the function φ can be extended so that the equality $f^n = \beta \circ g^{\varphi(n,.)} \circ \alpha$ still holds for n negative.

An automaton simulates another if and only if its global function simulates the global function of the other.

3 Construction of the Block Partition Representation

Let A $= (\mathcal{S}, d, r, f)$ be a reversible cellular automaton. We prove that it is the product of 2^d block permutations. We consider that A^{-1} is known and that the radius r is large enough for both reversible cellular automata A and A^{-1}. Let $v = 6r$ be the width of all the BP that we built. We need some more definitions before going further on.

3.1 Notations

We use the set $\{0,1\}^d$ with the order $\prec$ defined as follows: first by the number of 1s, and then backward lexicographically. For example, $(0,0,\ldots 0) \prec (1,0,\ldots 0) \prec (0,1,0,\ldots 0) \prec \ldots \prec (0,0,\ldots 0,1) \prec (1,1,0,\ldots 0) \prec (1,0,1,0\ldots 0) \prec \ldots \prec (0,\ldots 0,1,1) \prec \ldots \prec (1,1,\ldots 1)$. Let succ (α) be the least element greater than α in $\{0,1\}^d$. We denote $\top$ for succ $((1,1,1,\ldots 1))$, it does not belongs to $\{0,1\}^d$ but is practical for writing. It should be noted that if 0s and 1s are permuted, exactly the reverse order is obtained. For any $\alpha \in \{0,1\}^d$, we define the shift ς_α to be $\sigma_{3r.\alpha}$, and $\#_1(\alpha)$ to be the number of 1 in α.

The set of symbols of the BP is $(\mathcal{S}_\mathrm{A} \cup \{-\})^2$ where $-$ is a symbol which does not belong to $\mathcal{S}_\mathrm{A}$ and means 'void'. The first component is the old state of the cell and the second component its new state. The next

sets correspond to where the old states are deleted and the new states are added:

$$\begin{aligned}
E^{\mathsf{O}}_{\beta} &= \prod_{1\le i\le d} [\![(2+2\beta_i)r,\, (4+4\beta_i)r-1]\!] \ , \\
F^{\mathsf{O}}_{\alpha} &= [\![0,\, (6r-1)]\!]^d \ \setminus \bigcup_{\beta\prec\alpha} E^{\mathsf{O}}_{\beta} \ , \\
E^{\mathsf{N}}_{\beta} &= \prod_{1\le i\le d} [\![(1+4\beta_i)r,\, (5+2\beta_i)r-1]\!] \ , \\
F^{\mathsf{N}}_{\alpha} &= \bigcup_{\beta\prec\alpha} E^{\mathsf{O}}_{\beta} \ .
\end{aligned}$$

Although it is not written for the sake of writing, the sets are supposed to be completed by all $6r$ shifts.

All E^{O}_{β} (E^{N}_{β}) are disjoint. Let $\overline{\beta}$ be the complement of β. The sets E^{O}_{β} and $E^{\mathsf{N}}_{\overline{\beta}}$ are equal up to a $3r$ shift. The set $F^{\mathsf{N}}_{\top}$ is equals to $[\![0,\, (6r-1)]\!]^d$ because:

$$\begin{aligned}
F^{\mathsf{N}}_{\top} &= \bigcup_{\beta\prec\top} E^{\mathsf{N}}_{\beta} = \bigcup_{\beta\in\{0,1\}^d} E^{\mathsf{N}}_{\beta} \\
&= \bigcup_{\beta\in\{0,1\}^d,\beta_1=0} E^{\mathsf{N}}_{\beta} \ \cup \bigcup_{\beta\in\{0,1\}^d,\beta_1=1} E^{\mathsf{N}}_{\beta} \\
&= [\![r,\, 7r-1]\!] \times \bigcup_{\beta'\in\{0,1\}^{d-1}} E^{\mathsf{N}}_{\beta'} \\
&\quad \cdots \\
&= [\![r,\, 7r-1]\!]^d \ .
\end{aligned}$$

It should not be forgotten that all is done in a $(6r)^d$-periodic space. We prove in the same way that $F^{\mathsf{O}}_{\top} = \emptyset$. It follows that the sets E^{O}_{β} (E^{N}_{β}) form a partition of the whole lattice $\mathbb{Z}^d$. Let:

$$\mathcal{F}_{\alpha}(c) \ = \ \left(c_{|F^{\mathsf{O}}_{\alpha}}, \mathcal{G}(c)_{|F^{\mathsf{N}}_{\alpha}}\right) \ .$$

This is a mix of old and new states of the configurations. It corresponds to the different steps that a configuration c has to travel to become $\mathcal{G}_A(c)$ within our construction.

Since $F^{\mathsf{O}}_{(0,0,\dots 0)} = [\![0,\, (6r-1)]\!]^d$ and $F^{\mathsf{N}}_{(0,0,\dots 0)} = \emptyset$, then $c \equiv (c,-) = \mathcal{F}_{(0,0,\dots 0)}(c)$ and $\mathcal{G}(c) \equiv (-,\mathcal{G}(c)) = \mathcal{F}_{\top}(c)$. We define the following sets of 'double configurations':

$$\forall \alpha \in \{0,1\}^d,\ \mathcal{C}_{\alpha} \ = \ \{\ \mathcal{F}_{\alpha}(c) \mid c \in \mathcal{C}\ \} \ .$$

3.2 Definitions of the Block Partitions

We construct block permutations which go from $\mathcal{F}_{(0,0,\dots 0)}(c)$ to $\mathcal{F}_{\top}(c)$. For any α in $\{0,1\}^d$, let $T_{\alpha} : \mathcal{C}_{\alpha} \to \mathcal{C}_{\mathrm{succ}(\alpha)}$, such that $T_{\alpha}(\mathcal{F}_{\alpha}(c)) = \mathcal{F}_{\mathrm{succ}(\alpha)}(c)$. The local transition is ϵ_{α} and the origin of the partition is $3r\,\alpha$. To prove that this is a function, we must prove that the states added are uniquely defined.

Lemma 3 *For any α, there is a block permutation T_{α} between $\mathcal{C}_{\alpha}$ and $\mathcal{C}_{\mathrm{succ}(\alpha)}$ such that $T_{\alpha}(\mathcal{F}_{\alpha}(c)) = \mathcal{F}_{\mathrm{succ}(\alpha)}(c)$.*

Proof. We are working in the block $\prod_{1\le i\le d} [\![(3\alpha_i)r,\, (6+3\alpha_i)r-1]\!]$. The added new states are in the cells which are in

$$E^{\mathsf{N}}_{\alpha} \ = \ \prod_{1\le i\le d} [\![(1+4\alpha_i)r,\, (5+2\alpha_i)r-1]\!] \ .$$

To compute the new states, we need the old states of the cells in

$$\prod_{1\le i\le d} [\![4\alpha_i\, r,\, (6+2\alpha_i)r-1]\!] \ .$$

These cells are in the block. Let x be such a cell. Let us prove that the old state of x is present in $\mathcal{F}_\alpha(c)$. For each i such that $\alpha_i = 1$, $4r \leq x_i \leq 8r-1$. By construction of the sets E^{O}_β, the ones which contain x must verify: $\forall i$, if $\alpha_i{=}1$ then $\beta_i{=}1$, thus $\alpha \preceq \beta$ so that $x \notin F^{\mathsf{O}}_\alpha$. This means that all the old states needed to compute the added new states are present and that e_α is a function.

Let us prove that e_α is one-to-one, or equivalently, that the erased states are uniquely defined. The erased states are in the cells $\prod_{1\leq i\leq d} [\![(2{+}2\alpha_i)r,\ (4{+}4\alpha_i)r{-}1]\!]$. To compute them from the new states and A^{-1}, we need the new states in the cells $\prod_{1\leq i\leq d} [\![(1{+}2\alpha_i)r,\ (5{+}4\alpha_i)r{-}1]\!]$. These cells are in the block. Let x be such a cell. For each i such that $\alpha_i{=}0$, $1r \leq x_i \leq 5r{-}1$. By construction of the sets E^{N}_β, the set in which x is found, must verify: $\forall i$, if $\alpha_i{=}0$ then $\beta_i{=}0$, thus $\beta \preceq \alpha$ so that $x \in F^{\mathsf{N}}_{\mathrm{succ}(\alpha)}$. This means that all the new states needed to compute the deleted old states are present in $\mathcal{F}_{\mathrm{succ}(\alpha)(C)}$. The transition e_α is one-to-one, T_α is a block permutation.

□

Since we have 2^d BP which go from $\mathcal{F}_{(0,0,\ldots 0)}(c)$ to $\mathcal{F}_{\mathsf{T}}(c)$:

Theorem 4 *Any d-dimensional reversible cellular automaton can be represented using 2^d block permutations.*

Lemma 5 *Any reversible cellular automaton can be represented by a reversible block cellular automaton.*

Proof. The cardinalities of the basic sets are $|E^{\mathsf{O}}_\beta| = \prod_{1\leq i\leq d}(2{+}2\beta_i)r = 2^{d-b}\,4^b\,r^d$ where b is the number of 1 of β. The sets E^{O}_β (E^{N}_β) form a partition of the torus. For any block, the number of new (old) states tells which α is to be used. The sets of blocks for each e_α inputs (outputs) are disjoint. Then all the partial definition of e_α are gathered in a unique e that is a one-to-one function and all BP in a unique BP T such that:

$$\forall c \in \mathcal{C},\ \mathcal{G}(c) \ = \ T_{(1,1,\ldots 1)} \circ \ldots T_{(1,0,\ldots 0)} \circ T_{(0,0,\ldots 0)}(c) \ .$$

This can be grouped in a reversible block cellular automaton:

$$\mathrm{B} \ = \ \left((\mathcal{S} \cup \{-\})^2,\ (6r, 6r, \ldots, 6r),\ 2^d,\ (3r\,\alpha)_{\alpha\in\{0,1\}^d},\ (\mathcal{S} \cup \{-\})^2 \right) \ .$$

The R-BCA B uses 2^d partitions to simulate the R-CA A. The last BP must maps $(- \times \mathcal{S})^{\mathbb{Z}^d}$ into $(\mathcal{S} \times -)^{\mathbb{Z}^d}$ in order to iterate the simulation.

□

Figure 2 shows how the new states are generated and the old states discarded in dimension 2. The left column indicates the distribution of new and old states inside $[\![0, 6r]\!]$. On the right it is depicted how the permutation operates on shifted blocks. The dotted lines indicates the distances r.

3.3 Composition of the BP's

In this subsection we collapse the states from $(\mathcal{S}_\mathrm{A} \cup \{-\})^2$ to $\mathcal{S}_\mathrm{A} \cup \mathcal{S}_\mathrm{A}^2$. This decreases the number of states and make iterating directly possible. We use the following Lemma:

Lemma 6 *In every partition, the positions of the cells with two CA states in each block are enough to determine α.*

Proof. If all cells are single, then $\alpha = (0, 0, \ldots 0)$.

Let ε^j be the following base of $\{0,1\}^d$: $\varepsilon^j_i{=}1$ if and only if $i{=}j$, otherwise $\varepsilon^j_i{=}0$. Let $\varphi^j = (3{+}3\alpha{+}\varepsilon^j)r$ be some element of $\mathbb{Z}^d$. Since the E^{O}_β ($E^{\mathsf{N}}_{\beta'}$) form a partition of the lattice, let us find the β (β') which corresponds to φ^j. From the definitions of E^{O}_β, the value of β depends only on α and each component depends only in the value on each direction. The relations between those elements of $\mathbb{Z}^d$ are summed up on Fig. 3.

Thus, if $\alpha \preceq \beta$, the old state of the cell φ^j is still present. If $\alpha_j{=}0$ then $\alpha \prec \beta'$, which means that the new state has not been added yet in the cell φ^j. If $\alpha_j{=}1$ then $\beta' \prec \alpha$, which means that the new state has been added in the cell φ^j.

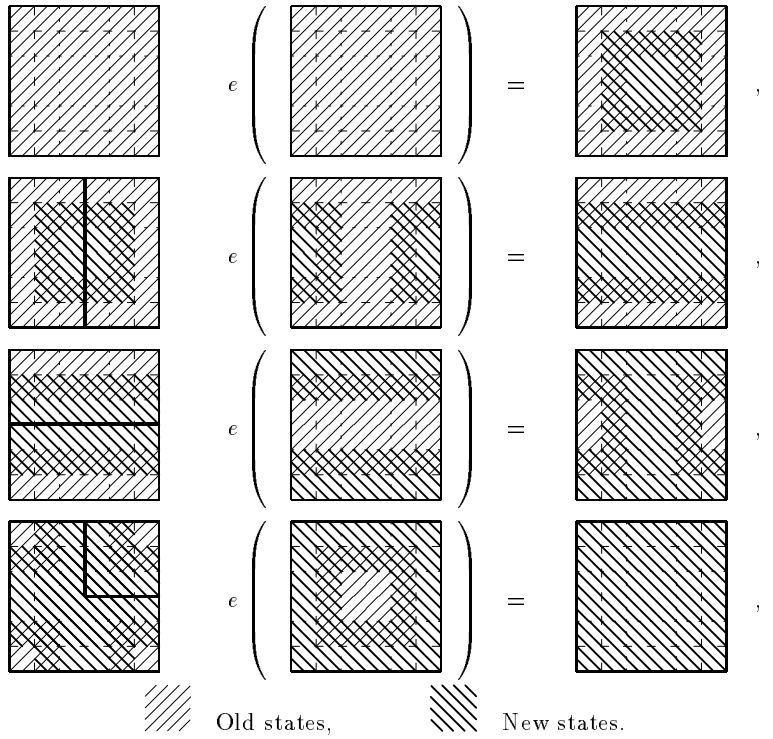

Figure 2: How states are generated and erased.

	α_i	φ_i^j	β_i	β'_i
$i \neq j$	0	3	0	0
	1	6	1	1
$i = j$	0	4	1	1
	1	7	1	0

Figure 3: Relations between α, φ^j, β and β'.

The coordinate of φ^j depends on α, but inside blocks of the α partition (the first shifted by $3\alpha\, r$), the $3\alpha\, r$ term disappears and only remains $\varphi^{j\,\prime} = (3{+}\varepsilon^j)r$, which is independent from α.

Altogether, the cell $(3{+}\varepsilon^j)r$ has two states if and only if $\alpha_j{=}1$ (*i.e.*, $\beta{\prec}\alpha$ and $\beta'{\prec}\alpha$). This means that simply by looking whether the states in the cells $(3{+}\varepsilon^j)r$ are single, the value of α can be guessed.

□

The sets $\mathcal{S}\times\{-\}$ and $\{-\}\times\mathcal{S}$ can both be collapsed onto $\mathcal{S}$ without losing the definition and injectivity of e. The set of states $(\mathcal{S}\cup\{-\})^2$ collapses on $\mathcal{S}\cup\mathcal{S}^2$. Apart from lowering the set of states, this allows the system to be iterated. This corresponds exactly to our simulation definition now.

4 Another Construction

In this Section, we built a representation with $d+1$ Block Permutations of width $3(d+1)r$.

4.1 New BP's

The following sets are used, $\forall \lambda \in \{0, 1, 2, \ldots d+1\}$:

$$\begin{array}{rcll} H^{\mathsf{N}}_\lambda & = & \bigcup_{0 \le \mu < \lambda} & \left(3\mu r + [\![r, 3(d+1)r - r - 1]\!]^d \right) \ , \\ H^{\mathsf{O}}_\lambda & = & \bigcup_{\lambda \le \mu < d+1} & \left(3\mu r + [\![r, 3(d+1)r - r - 1]\!]^d \right) \ . \end{array}$$

The sets are supposed to be completed by all $3(d+1)r$ shifts.

Lemma 7 *These sets verify the symmetry $H^{\mathsf{N}}_\lambda = -3r - H^{\mathsf{O}}_{d+1-\lambda}$ and the following equalities: $H^{\mathsf{N}}_0 = H^{\mathsf{O}}_{d+1} = \emptyset$ and $H^{\mathsf{N}}_{d+1} = H^{\mathsf{O}}_0 = \mathbb{Z}^d$.*

Proof. The symmetry and the equality with $\emptyset$ are obvious.
For the second part, we prove that $H^{\mathsf{N}}_d = \mathbb{Z}^d$, the last equality is done by symmetry. Let x be any element of the underlying lattice $\mathbb{Z}^d$. The $d+1$ sets $3\lambda r + [\![-r, r-1]\!]$ (for $\lambda \in [\![0, d]\!]$) are non-empty and disjoint. Since x has d coordinates, there exists a λ_0 such that no coordinate of x belongs to $3\lambda_0 r + [\![-r, r-1]\!]$. This means that all x_k belong to $3\lambda_0 r + [\![r, 3(d+1)r - r - 1]\!]$, thus $x \in H^{\mathsf{N}}_d$.

□

As before a wider set of states $(\mathcal{S} \cup -)^2$ is used during the composition. Let

$$\forall c \in \mathcal{C},\ \forall \lambda,\ \mathcal{H}_\lambda(c) = \left(c_{|H^{\mathsf{O}}_\lambda}\ ,\ \mathcal{G}(c)_{|H^{\mathsf{N}}_\lambda} \right) \ .$$

With Lem. 7, we have: $\mathcal{H}_0(c) = (c, -)$ and $\mathcal{H}_{d+1}(c) = (-, \mathcal{G}(c))$.

Let D_λ be a BP of width $3(d+1)r$ and origin $3\lambda r$. The local function e_λ is defined so that D_λ maps $\mathcal{H}_\lambda(c)$ into $\mathcal{H}_{\lambda+1}(c)$. The BP D_λ add new states and erase old states.

Let us prove that there is enough data in $\mathcal{H}_\lambda(c)$ to compute the new states. The states added belongs to:

$$\begin{array}{rcl} \Delta_\lambda & = & H^{\mathsf{N}}_{\lambda+1} \setminus H^{\mathsf{N}}_\lambda \\ & = & \left(3\lambda r + [\![r, 3(d+1)r - r - 1]\!]^d \right) \setminus \bigcup_{0 \le \mu < \lambda} \left(3\mu r + [\![r, 3(d+1)r - r - 1]\!]^d \right) \ . \end{array}$$

For any $x \in \Delta_\lambda$, $x \in 3\lambda r + [\![r, 3(d+1)r - r - 1]\!]^d$ and the origin of D_λ is $3\lambda r$. Then all the cells of the neighborhood of x and the old states needed to compute the new state of x are in the block $3\lambda r + [\![0, 3(d+1)r - 1]\!]^d$. Now, it only remains to verify that old states needed to compute the new states are still present.

For any μ in $[\![0, \lambda - 1]\!]$, since $x \notin 3\mu r + [\![r, 3(d+1)r - r - 1]\!]^d$, there is some index j_μ such that $x_{j_\mu} \notin 3\mu r + [\![r, 3(d+1)r - r - 1]\!]$. So x_{j_μ} is in $3\mu r + [\![-r, r-1]\!]$ (remember that all is $3(d+1)r$ periodic). And all j_μ must be different because the sets $3\mu r + [\![-r, r-1]\!]$ are disjoint.

Let y be any cell needed to compute x, y belongs to $x + [\![-r, r]\!]$. The cell y_{j_μ} must be in $3\mu r + [\![-2r, 2r-1]\!]$.

If y does not belong to H^{O}_λ then for all $\mu' \in [\![\lambda, d+1]\!]$, there is some $k_{\mu'}$ such that $y_{k_{\mu'}}$ does not belong to $\mu' r + [\![r, 3(d+1)r - r - 1]\!]$, or equivalently, $y_{k_{\mu'}} \in 3\mu' r + [\![-r, r-1]\!]$. Again all the $k_{\mu'}$ must be different.

Altogether, there are $d+1$ j_μ and $k_{\mu'}$ for d values so there are μ and μ' such that $j_\mu = k_{\mu'}$. Then the intersection of $3\mu r + [\![-2r, 2r-1]\!]$ and $3\mu' r + [\![-r, r-1]\!]$ is not empty. This means that $\mu' = \mu$. But, by definition of μ and μ', $\mu < \mu'$.

Thus y belongs to H^{O}_λ and the old states needed to compute the new state of x are present in the block.

Using the symmetry between H^{N} and H^{O}, the old states erased can be computed from the new states in $\mathcal{H}_{\lambda+1}(c)$.

The 3 BP in dimension 2 are given in Fig. 4.

4.2 Collapsing the States

We collapse again the states on $\mathcal{S}_{\mathrm{A}} \cup \mathcal{S}^2_{\mathrm{A}}$.

Lemma 8 *The BP is defined by the position of the double states.*

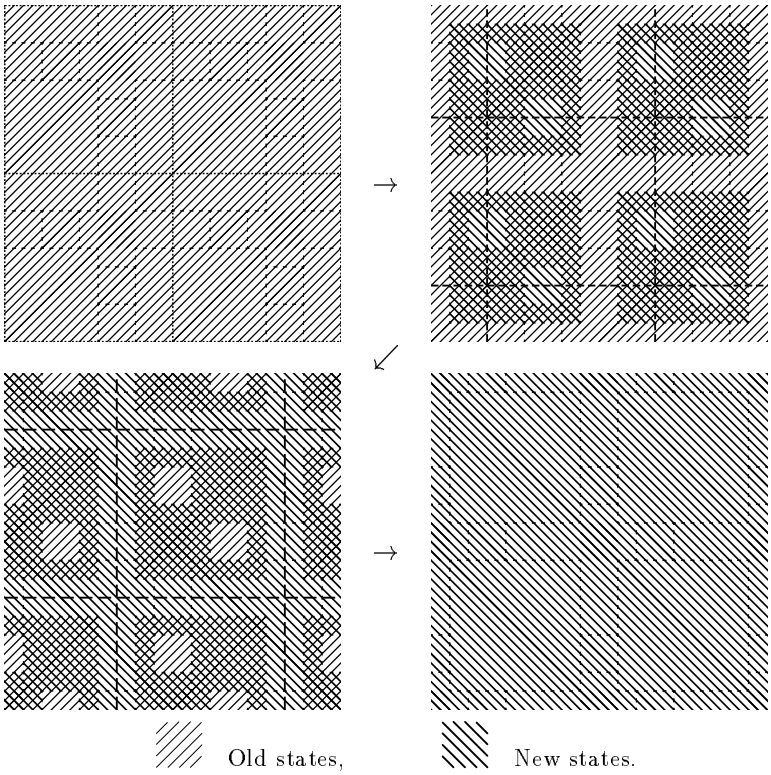

Figure 4: The 3 steps in dimension 2.

Proof. If all cells are single, then $\lambda = 0$.

Let ζ^i be the following vector:

$$\zeta^i \;=\; 3\lambda r \;+\; (-3,\, -6,\, -9\, \ldots, -3i,\, -3i, \cdots -3i) \;\; .$$

The vector ζ^i hold two states only if it belongs to both H_λ^{N} and H_λ^{O}. The equation

$$3\lambda r + (-3, -6, -9 \ldots, -3i, -3i, \cdots -3i) \in \; 3\lambda r + [\![\, r, 3(d+1)r - r - 1 \,]\!]^d$$

implies that ζ^i belongs to H_λ^{O} for $\lambda \leq d$, which is always the case. The vector ζ^i belongs to H_λ^{N} only if

$$\begin{aligned} 3\lambda r + (-3, -6, -9 \ldots, -3i, -3i, \cdots -3i) \quad &\in \quad \bigcup_{0 \leq \mu < \lambda} \quad \left(3\mu r + [\![\, r, 3(d+1)r - r - 1 \,]\!]^d\right) \;\; , \\ (-3, -6, -9 \ldots, -3i, -3i, \cdots -3i) \quad &\in \quad \bigcup_{-\lambda \leq \mu < 0} \quad \left(3\mu r + [\![\, r, 3(d+1)r - r - 1 \,]\!]^d\right) \;\; , \end{aligned}$$

which implies that $-3\lambda + 1 < -3i$, $i + 1 < \lambda$. Then λ is the maximum i such that ζ^i holds two states, plus two. If there is no such i then $\lambda = 1$.

Inside a block of the λ partition, ζ^i simplifies to $(-3, -6, -9 \ldots, -3i, -3i, \cdots -3i)$, which is independent of λ. As before, it is enough to know the position of the double states in a block to know which BP to use. □

With above Lemma, all local functions of the BP are compatible and can be grouped in a unique bijective local function and states can be collapsed. Altogether:

Theorem 9 *Any* R-CA *can be expressed as a composition of* $d+1$ BP *of width* $3(d+1)r$.

The origins of the partitions are: 0, $3r$, $6r$, $9r$ ... and $3dr$.

5 Conclusion

We prove conjectures 1 and 2. The proof is done in a rather technical way and is not so explicit and visible as the one in [2]. Nevertheless, we have improved the number of block permutations needed: 2^d instead of $2^{d+1}-1$. Generation and erasing are still done progressively. But they are made concurrently, not one after the other as in the first construction. The only drawback is that the size of the block is $(6r)^d$ instead of $(4r)^d$.

We modify the block permutations and the set of states used in order to have the possibility to iterate them.

We also give a construction with $d+1$ BP. But the width is $3(d+1)r$ instead of $6r$. This means that the size of the blocks are $(3(d+1)r)^d$ instead of $(6r)^d$. The complexity of the BP is the size of its table. It should be noted that if the number of BP is decreasing, the complexity is increasing: the exponent of the number of state is a factorial instead of an exponential.

As already noted by Kari [6], the fact that the BP representation can be effectively constructed does not contradict the undecidability of reversibility because the inverse CA is needed for the construction.

To have a BP allows one to use reversible circuitry in order to build R-CA. This was done in [2] to prove that, for $2 \leq d$, there exists one d-dimensional reversible CA able to simulate any d-dimensional R-CA.

Since the BP are compatible and the states are collapsed, the composition can be iterated directly. This defines a reversible block cellular automaton, also known as a CA with the Margolus neighborhood. The representation Th. 4 means that d-R-CA can be simulated by d-dimensional reversible block cellular automata. In [4], we use this to simulate d-R-CA with d-dimensional partitioned cellular automata (as defined by Morita [7]) and extend the result of [2] to dimension 1. Partitioned CA are CA whose set of states is a product set indexed by $[\![-r, r]\!]$. In this model, each part of a state is sent to one and only one of its neighbors.

References

[1] S. Amoroso and Y. Patt. Decision procedure for surjectivity and injectivity of parallel maps for tessellation structure. *Journal of Computer and System Sciences*, 6:448–464, 1972.

[2] J. O. Durand-Lose. Reversible cellular automaton able to simulate any other reversible one using partitioning automata. In LATIN *'95*, number 911 in Lecture Notes in Computer Science, pages 230–244. Springer-Verlag, 1995.

[3] J. O. Durand-Lose. *Automates Cellulaires, Automates à Partitions et Tas de Sable.* PhD thesis, LaBRI, 1996. In French.

[4] J. O. Durand-Lose. Intrinsic universality of a 1-dimensional reversible cellular automaton. In STACS *'97*, number 1200 in Lecture Notes in Computer Science, pages 439–450. Springer-Verlag, 1997.

[5] J. Kari. Reversibility and surjectivity problems of cellular automata. *Journal of Computer and System Sciences*, 48(1):149–182, 1994.

[6] J. Kari. Representation of reversible cellular automata with block permutations. *Mathematical System Theory*, 29:47–61, 1996.

[7] K. Morita. Reversible simulation of one-dimensional irreversible cellular automata. *Theoretical Computer Science*, 148:157–163, 1995.

[8] T. Toffoli and N. Margolus. Invertible cellular automata: A review. *Physica D*, 45:229–253, 1990.

Contents

Table of Symbols

Symbol	Definition	Page
d	Dimension of the lattice	2
$\mathcal{S}$	Set of states	2
CA	Cellular Automata	2
r	Radius of a CA	2
f	Local function of a CA	2
$\mathcal{G}$	Global function of a CA	2
BP	Block Permutation	2
v	Size of a BP	2
o	Origin of a BP	2
e	Local function of a BP	2
$\{0,1\}^d$, $\prec$	Set used for indexing in the first construction and the order used on it	3
succ (α)	Least element greater than α in $\{0,1\}^d$ for $\prec$	3
$\top$	succ $((1,1,1,\ldots 1))$	3
$\bot$	Added vacuum state	3
$E^{\mathsf{O}}, F^{\mathsf{O}}$	Set of deleted states	3
$E^{\mathsf{N}}, F^{\mathsf{N}}$	Set of added states	3
$\mathcal{F}_\alpha$	Step configuration in the first construction	4
$\mathcal{C}_\alpha$	Set of double configurations associated to α	4
ε^j, φ^j	Places to look for double states	5
H^{N},H^{O}	Where new and old states are held during the second construction	7
$\mathcal{H}_\lambda(c)$	Step configuration in the second construction	7
Δ_λ	Where new states are added in the second construction	7
ζ^i	Vector used to find the BP in the second construction	8