One-dimensional quantum cellular automata over finite, unbounded configurations.

Pablo Arrighi,1 Vincent Nesme,2∗ and Reinhard Werner2‡

1Université de Grenoble,
LIG, 46 Avenue Félix Viallet, 38031 Grenoble Cedex, France.
2Technical University of Braunschweig,
IMAPH, Mendelsohnstr. 3, 38106 Braunschweig, Germany.

One-dimensional quantum cellular automata (QCA) consist in a line of identical, finite dimensional quantum systems. These evolve in discrete time steps according to a local, shift-invariant unitary evolution. By local we mean that no instantaneous long-range communication can occur. In order to define these over a Hilbert space we must restrict to a base of finite, yet unbounded configurations. We show that QCA always admit a two-layered block representation, and hence the inverse QCA is again a QCA. This is a striking result since the property does not hold for classical one-dimensional cellular automata as defined over such finite configurations. As an example we discuss a bijective cellular automata which becomes non-local as a QCA, in a rare case of reversible computation which does not admit a straightforward quantization. We argue that a whole class of bijective cellular automata should no longer be considered to be reversible in a physical sense. Note that the same two-layered block representation result applies also over infinite configurations, as was previously shown for one-dimensional systems in the more elaborate formalism of operators algebras [9]. Here the proof is made simpler and self-contained, moreover we discuss a counterexample QCA in higher dimensions.

PACS numbers: 03.67.Lx, 03.67.-a, 03.65.-w, 05.30.-d
Keywords: Symbolic dynamics, complex systems, intrinsic universality, complex systems, translation-invariant dynamics, Ising models

One-dimensional cellular automata (CA) consist in a line of cells, each of which may take one in a finite number of possible states. These evolve in discrete time steps according to a local, shift-invariant function. When defined over infinite configurations, the inverse of a bijective CA is then itself a CA, and this structural reversibility leads to a natural block decomposition of the CA. None of this holds over finite, yet possibly unbounded, configurations.

Because CA are a physics-like model of computation it seems very natural to study their quantum extensions. The flourishing research in quantum information and quantum computer science provides us with appropriate context for doing so, both in terms of the potential implementation and the theoretical framework. Right from the very birth of the field with Feynman’s 1986 paper, it was hoped that QCA may prove an important path to realistic implementations of quantum computers [6] – mainly because they eliminate the need for an external, classical control and hence the principal source of decoherence. Other possible aims include providing models of distributed quantum computation, providing bridges between computer science notions and modern theoretical physics, or anything like understanding the dynamics of some quantum physical system in discrete spacetime, i.e. from an idealized viewpoint. Studying QCA rather than quantum Turing machines for instance means we bother about the spatial structure of things [2], whether for the purpose of describing a quantum protocol, modelling a quantum physical phenomena, or again taking into account the spatial parallelism inherent to the model.

One-dimensional quantum cellular automata (QCA) consist in a line of identical, finite dimensional quantum systems. These evolve in discrete time steps according to a local, shift-invariant unitary evolution. By local we mean that information cannot be transmitted faster than a fixed number of cells per time step. Because the standard mathematical setting for quantum mechanics is the theory of Hilbert spaces, we must exhibit and work with a countable basis for our vectorial space. This is the reason why we restrict to finite, unbounded configurations. An elegant alternative to this restriction is to abandon Hilbert spaces altogether and use the more abstract mathematical setting of $C^*$-algebras [3] – but here we seek to make our proofs self-contained and accessible to a wider community, including those computer scientists with an interest in quantum computation. Our main result is that QCA can always be expressed as two layers of an infinitely repeating unitary gate even over such finite configurations. The existence of such a two-layered block representation implies of course that the inverse QCA is again a QCA. Our result is mainly a simplification of the same theorem over infinite configurations as expressed with operators algebra [9]. Unfortunately an example QCA disproves the theorem in further dimensions – at least in its present form.

It is a rather striking fact however that QCA admit the two-layered block representation in spite of their being defined over finite, unbounded configurations. For
most purposes this saves us from complicated unitary tests such as \([1,3,5]\). But more importantly notice how this is clearly not akin to the classical case, where a CA may be bijective over such finite configurations, and yet not structurally reversible. In order to clarify this situation we consider a perfectly valid, bijective CA but whose inverse function is not a CA. It then turns out that its quantum version is no longer valid, as it allows superluminal signalling. Hence whilst we are used to think that any reversible computation admits a trivial quantization, this turns out not to be case in the realm of cellular automata. Curiously the non-locality of quantum states (entanglement) induces more structure upon the cellular automata – so that its evolution may remain local as an operation (no-superluminal signalling). Based upon these remarks we prove that an important, well-studied class of bijective CA may be dismissed as not physically reversible.

Outline. We reorganize a number of known mathematical results around the notion of subsystems in quantum theory (Section I). Thanks to this small theory we prove the reversibility/block structure theorem in an elementary manner (Section III). In the discussion we show why the theorem does not hold as such in further dimensions; we exhibit superluminal signalling in the XOR quantum automata, and end with a general theorem discarding all injective, non surjective CA over infinite configurations as unphysical (Section III).

I. A SMALL THEORY OF SUBSYSTEMS

Definition 1 (Algebras)
Consider \(A \subseteq M_n(\mathbb{C})\). We say that \(A\) is an algebra of \(M_n(\mathbb{C})\) if and only if it is closed under weighting by a scalar \((\cdot)\), addition \((+)\), matrix multiplication \((\cdot)\), adjoint \((\dagger)\). Moreover for any \(S\) a subset of \(M_n(\mathbb{C})\), we denote by \(\mathcal{C}(S)\) its closure under the above-mentioned operations.

Note that algebras as above-defined are really just \(C^*\)-algebras over finite-dimensional systems.

Definition 2 (Subsystem algebras)
Consider \(A\) an algebra of \(M_n(\mathbb{C})\). We say that \(A\) is a subsystem algebra of \(M_n(\mathbb{C})\) if and only if there exists \(p,q \in \mathbb{N} / pq = n \) and \(U \in M_n(\mathbb{C}) / U^\dagger U = UU^\dagger = I\) such that \(UAU^\dagger = M_{p}(\mathbb{C}) \otimes I_q\).

Definition 3 (Center algebras)
For \(A\) an algebra of \(M_n(\mathbb{C})\), we note \(\mathcal{C}(A) = \{A \in A \mid \forall B \in A BA = AB\}\). \(\mathcal{C}(A)\) is also an algebra of \(M_n(\mathbb{C})\), which is called the center algebra of \(A\).

Theorem 1 (Characterizing one subsystem)
Let \(A\) be an algebra of \(M_n(\mathbb{C})\) and \(\mathcal{C}(A) = \{A \in A \mid \forall B \in A BA = AB\}\) its center algebra. Then \(A\) is a subsystem algebra if and only if \(\mathcal{C}(A) = \mathbb{C}I\).

Proof. The argument is quite technical and its understanding not mandatory for understanding the rest of the paper. Its presentation is based on \([2]\). See also \([3]\) for a proof within the setting of general \(C^*\)-algebras.

Consider some set \(P = \{P_i\}_{i=1}^p\) such that:

(i) \(\forall i = 1 \ldots p\ P_i \in A\);

(ii) \(\forall i,j = 1 \ldots p\ P_i P_j = \delta_{ij} P_i \in A\).

Moreover we take \(P\) is maximal, i.e. so that there is no set \(Q = \{Q_i\}\) verifying conditions (i), (ii) and such that \(P \subseteq Q\), with \(P, Q\) the closures of \(P, Q\). Note that:

(iii) \(\sum_{i=1}^p P_i = I\),

otherwise \(I - \sum_{i=1}^p P_i\) may be added to the set.

First we show that

\(\forall i\ [P_i AP_i = CP_i]\). 

Intuitively this is because the contrary would allow us to refine the subspaces defined by \(P_i\) into smaller subspaces, and hence go against the fact that \(P\) is maximal. Formally consider some \(M \in A\) such that \(P_i MP_i \not\subseteq P_i\). If \(M\) is proportional to a unitary let \(N = M + M^\dagger\), else let \(N = M^\dagger M\). In any case we have \(P_i NP_i \not\subseteq P_i\) with \(N\) hermitian. Note that \(H = P_i NP_i\) is also hermitian, and has support in the subspace \(P_i\), hence we can write \(H = \sum_k \lambda_k Q_k\) with the \(Q_k\)'s orthogonal projectors such that \(\sum_k Q_k = P_i\) and the \(\lambda_k\)’s distinct real numbers. Any such \(Q_k\) is part of \(A\), since \(Q_k = \frac{1}{\lambda_k} M_{P_i}(\mathbb{C})\otimes I_{\lambda_k - \lambda_j}\).

Consider the set \(Q = \{P_i\} \cup k\{Q_k\}\). It satisfies condition (i), (ii) but \(P \subseteq Q\), which is impossible.

Second we show that

\(\forall i,j\ [P_i AP_j \neq 0]\).

Intuitively this is because the contrary would split \(A\) into the direct sum of two matrix algebras, and hence go against the fact that \(\mathcal{C}(A) = \mathbb{C}I\). Formally write \(i \sim j\) whenever this is the case. The relation \(\sim\) is reflexive by Eq. \([1]\), transitive by multiplicative closure of \(A\), and symmetric since

\(P_i AP_j \neq 0 \Rightarrow (P_i AP_j)^\dagger \neq 0 \Rightarrow (P_j A^\dagger P_i) \neq 0 \Rightarrow (P_j AP_i) \neq 0\).

Say there is an equivalence class \(J \subset 1 \ldots p\) and let \(P_J = \sum_{i \in J} P_i\), \(P_J = \sum_{j \in J} P_j\). Then

\(AP_j = (P_i + P_j)AP_j = P_j AP_j = P_j A\) symmetrically.

and so \(P_J \in \mathcal{C}(A)\), which is impossible.

Third we show that for all \(A\), for all \(i,j = 1 \ldots p\), if we let \(M = P_i AP_j\) then

\(\exists \lambda \in \mathbb{C}\ [M^\dagger M = \lambda P_i \wedge MM^\dagger = \lambda P_j]\). 

(3)
Indeed, Eq. (1) gives $M^\dagger M = \lambda P_i$ and $MM^\dagger = \mu P_j$. But then $\lambda^2 P_i = M^\dagger MM^\dagger M = \mu M^\dagger P_j M = \mu P_i$, hence $\lambda$ equals $\mu$.

**Fourth** we show that

$$\forall i, j \quad [\text{Tr}(P_i) = \text{Tr}(P_j) = \text{some constant } q]. \quad (4)$$

For each $i, j$ take some $A \in \mathcal{A}$ verifying Eq. (2). Let $M = P_i AP_j$. By Eq. (3) there is a complex number $\lambda$ such that we have $P_i = \lambda MM^\dagger$ and $P_j = \lambda M^\dagger M$. Then the equality follows from $\text{Tr}(\lambda MM^\dagger) = \text{Tr}(\lambda M^\dagger M)$.

**Fifth** consider some unitary $U$ which takes those $\{P_i\}_{i=1 \ldots p}$ into one-zero orthogonal diagonal matrices $I = \{I_i\}_{i=1 \ldots p}$ with $I_i = |i\rangle \langle i| \otimes I_q$. Note that this is always possible since the $\{P_i\}_{i=1 \ldots p}$ form an orthogonal (ii), complete (iii) set of projectors of equal dimension by Eq. (4). We show that

$$\forall A \in UAU^\dagger \forall i, j \quad [I_i A I_j = |i\rangle \langle j| \otimes A_{ij}]$$

with $A_{ij} A_{ij}^\dagger = A_{ij}^\dagger A_{ij} \propto I_q$. \quad (5)

The line stems from the form of $I_i$, i.e., $I_i A I_j$

$$= \sum_{pqkl} A_{pqkl} (|i\rangle \langle p| \otimes I_q) (|q\rangle \langle k| \otimes I_q) (|j\rangle \langle l| \otimes I_q)$$

$$= \sum_{kl} A_{ijkl} (|i\rangle \langle k| \otimes I_q) (|j\rangle \langle l|) = |i\rangle \langle j| \otimes (\sum_{kl} A_{ijkl} |k\rangle \langle l|).$$

For the second line let $M = I_i A I_j$. By Eq. (3) there is a complex number $\lambda$ such that we have both $I_i = \lambda MM^\dagger$ and $I_j = \lambda M^\dagger M$. But then

$$|i\rangle \langle i| \otimes I_q = I_i = \lambda MM^\dagger = \lambda (|i\rangle \langle j| \otimes A_{ij}) (|i\rangle \langle j| \otimes A_{ij}^\dagger)$$

$$= \lambda |i\rangle \langle i| \otimes A_{ij} A_{ij}^\dagger$$

and hence $\lambda A_{ij} A_{ij}^\dagger = I_q$, and symmetrically for $\lambda A_{ij}^\dagger A_{ij} = I_q$.

Finally consider some unitary $V = \sum_i |i\rangle \langle i| \otimes A_{ii}$, where $U^\dagger AU$ is some matrix verifying Eq. (2), and rescaled so that Eq. (5) makes $A_{ij}$ it unitary. We show that

$$\forall M \in VUAV^\dagger \forall i, j \quad [I_i M I_j = |i\rangle \langle j| \otimes A_{ij}]$$

with $\lambda$ a complex number.

For a better understanding of $V$ notice that

$$V = \sum_i |i\rangle \langle i| \otimes A_{ii}$$

$$= \sum_i (|i\rangle \langle 1| \otimes I_q) (|1\rangle \langle i| \otimes A_{ii})$$

$$= \sum_i (|i\rangle \langle 1| \otimes I_q) I_i A I_i$$

Consider $B = V^\dagger MV$. It belongs to $UAU^\dagger$ and by Eq. (5) it is of the form

$$B = \sum_{ij} |i\rangle \langle j| \otimes B_{ij}.$$ 

Now $I_i M I_j$

$$= I_i V B V^\dagger I_j$$

$$= (|i\rangle \langle 1| \otimes I_q) I_i A I_j (|1\rangle \otimes I_q)$$

$$= (|i\rangle \langle 1| \otimes I_q) I_i (|1\rangle \otimes I_q)$$

$$= \lambda (|i\rangle \langle 1| \otimes I_q) (|1\rangle \langle I_q) (|1\rangle \otimes I_q)$$

$$= \lambda |i\rangle \langle j| \otimes I_q.$$



**Theorem 2 (Characterizing several subsystems)**

Let $\mathcal{A}$ and $\mathcal{B}$ be commuting algebras of $M_n(\mathbb{C})$ such that $\mathcal{A}B = M_n(\mathbb{C})$. Then there exists a unitary matrix $U$ such that $U\mathcal{A}U^\dagger$ is $M_p(\mathbb{C}) \otimes I_q$ and $U\mathcal{B}U^\dagger$ is $I_p \otimes M_q(\mathbb{C})$, with $pq = n$.

**Proof.**

First, let us note that $\mathcal{C}_A$ includes $\mathcal{C}_B$. Next, the elements of $\mathcal{C}_A$ commute by definition with all matrices in $\mathcal{A}$, but also with all matrices in $\mathcal{B}$, since $\mathcal{A}$ and $\mathcal{B}$ commute. Therefore, as $\mathcal{A}B = M_n(\mathbb{C})$, $\mathcal{C}_A$ is equal to $\mathcal{C}_B$. Thus, according to proposition 1, $\mathcal{A}$ is a subsystem algebra. For simplicity matters, and without loss of generality, we will assume that $\mathcal{A}$ is actually equal to $M_p(\mathbb{C}) \otimes I_q$ for some $p$ and $q$ such that $pq = n$. Now for the same reasons $\mathcal{B}$ is also a subsystem algebra. Because it commutes with $\mathcal{A}$ it must act on a disjoint subsystem as $\mathcal{A}$. And since together they generate $M_n(\mathbb{C})$, there is no other choice but to have $\mathcal{B}$ actually equal to $I_p \otimes M_q(\mathbb{C})$. 

**Definition 4 (Restriction Algebras)**

Consider $\mathcal{A}$ an algebra of $M_p(\mathbb{C}) \otimes M_q(\mathbb{C}) \otimes M_r(\mathbb{C})$. For $A$ an element of $\mathcal{A}$, we write $A_{1\cdot}$ for the matrix $Tr_{02}(A)$. Similarly we call $A_{\cdot 1\cdot}$ the restriction of $\mathcal{A}$ to the middle subsystem, i.e. the algebra generated by the matrices of the set $\{Tr_{02}(A) \mid A \in \mathcal{A}\}$.

**Lemma 1 (Restriction of commuting algebras)**

Consider $\mathcal{A}$ an algebra of $M_p(\mathbb{C}) \otimes M_q(\mathbb{C}) \otimes I_r$ and $\mathcal{B}$ an algebra of $I_p \otimes M_q(\mathbb{C}) \otimes I_r(\mathbb{C})$. Say $\mathcal{A}$ and $\mathcal{B}$ commute. Then so do $\mathcal{A}_{1\cdot}$ and $\mathcal{B}_{\cdot 1\cdot}$.

**Proof.**

In the particular case where $\mathcal{A}$ and $\mathcal{B}$ have only subsystem 1 in common we have

$$\forall A \in \mathcal{A}, B \in \mathcal{B} \quad pr_{Tr02}(AB) = Tr_{02}(A)Tr_{02}(B). \quad (6)$$

Indeed take $A = \sum_i \alpha_i (\sigma_i \otimes \tau_i \otimes I)$ and $B = \sum_j \beta_j (I \otimes \mu_j \otimes \nu_j)$. We have

$$pr_{Tr02}(AB) = Tr_{02}(\sum_{ij} \rho \alpha_i \tau_i \beta_j (\nu_j \otimes \mu_j \otimes \nu_j))$$

$$= (\sum_i \rho \alpha_i Tr(\tau_i) \beta_j (\nu_j \otimes \mu_j \otimes \nu_j))$$

$$= Tr_{02}(A)Tr_{02}(B).$$
Now $A_{|1}$ is generated by $\{\text{Tr}_{02}(A) \mid A \in A\}$, and $B_{|1}$ is generated by $\{\text{Tr}_{02}(B) \mid B \in B\}$. Since commutation is preserved by $\ast$, $+$, $\alpha$, and $\dagger$ all we need to check is that the generating elements commute. Consider $A_{|1}$ an element of $A_{|1}$ and take $A$ such that $A_{|1} = \text{Tr}_{02}(A)$. Similarly take $B_{|1}$ and $B$ such that $B_{|1} = \text{Tr}_{02}(B)$. We have $A_{|1}B_{|1} = \text{Tr}_{02}(A)\text{Tr}_{02}(B) = \text{pr} \cdot \text{Tr}_{02}(AB) = \text{pr} \cdot \text{Tr}_{02}(BA) = \text{Tr}_{02}(B)\text{Tr}_{02}(A) = B_{|1}A_{|1}$. □

Lemma 2 (Restriction of generating algebras)
Consider $A$ an algebra of $M_p(C) \otimes M_q(C) \otimes \mathbb{I}_r$ and $B$ an algebra of $\mathbb{I}_p \otimes M_q(C) \otimes M_r(C)$. Say $AB_{|1} = M_p(C)$. Hence we have that $A_{|1}B_{|1} = M_p(C)$.

Proof.
$AB_{|1}$ is generated by $\{\text{Tr}_{02}(AB) \mid A \in A, B \in B\}$. However by Eq. (6) this is the same as $\{\text{Tr}_{02}(A)\text{Tr}_{02}(B) \mid A \in A, B \in B\}$, which generates $A_{|1}B_{|1}$. □

Lemma 3 (Duality)
Let $\mathcal{H}_0$ and $\mathcal{H}_1$ be Hilbert spaces, with $\mathcal{H}_0$ of dimension $p$. Let $A, p, p'$ denote some elements of $\mathcal{L}(\mathcal{H}_0 \otimes \mathcal{H}_1)$ with $p, p'$ having partial traces $\rho_{0}, \rho'_{0}$ over $\mathcal{H}_0$. We then have that $A \in M_p(C) \otimes \mathbb{I}$ is equivalent to

$$\forall \rho, \rho' \quad |\rho|_{0} = \rho'_{0} \implies \text{Tr}(\rho) = \text{Tr}(\rho')$$

Moreover we have that $\rho_{0} = \rho'_{0}$ is equivalent to

$$\forall A \in M_p(C) \otimes \mathbb{I} \quad |\text{Tr}(A) = \text{Tr}(A')|$$

Proof.
Physically the first part of the lemma says that “measurement is local if and only if it depends only upon the reduced density matrices”. $[\Rightarrow]$. Suppose that $A = A_{0} \otimes \mathbb{I}_{1}$. In this case we have $\text{Tr}(A) = \text{Tr}(A_{0}\rho_{0})$. Assuming $\rho_{0} = \rho'_{0}$ yields $\text{Tr}(A) = \text{Tr}(A_{0}\rho_{0}) = \text{Tr}(A_{0}\rho'_{0}) = \text{Tr}(A').$

$[\Leftarrow]$. Let’s write $A = \sum_{i,j} |i\rangle \langle j | \otimes B_{ij}$, with $|i\rangle$ and $|j\rangle$ ranging over some unitary basis of $\mathcal{H}_0$. If $A$ is not of the form $A_{0} \otimes \mathbb{I}_{1}$, then for some $i$ and $j$, $B_{ij}$ is not a multiple of the identity. Then there exist unit vectors $|x\rangle$ and $|y\rangle$ of $\mathcal{H}_1$ such that $\langle x| B_{ij} |x\rangle \neq \langle y| B_{ij} |y\rangle$. In other words, $\text{Tr}(B_{ij} |x\rangle \langle x|) \neq \text{Tr}(B_{ij} |y\rangle \langle y|)$. If we now consider $\rho = |j\rangle \langle i | \otimes |x\rangle \langle x|$ and $\rho' = |j\rangle \langle i | \otimes |y\rangle \langle y|$, we get what we wanted, i.e. $\rho_{0} = \rho'_{0}$ but $\text{Tr}(A) \neq \text{Tr}(A')$. Physically the second part of the lemma says that “two reduced density matrices are the same if and only if their density matrices cannot be distinguished by a local measurement”. $[\Rightarrow]$. This “$[\Rightarrow]$” is actually exactly the same as the first one, so we have already proved it.

$[\Leftarrow]$. Supposing $\text{Tr}(A) = \text{Tr}(A')$ for $A = |j\rangle \langle i | \otimes \mathbb{I}$ yields $\rho_{0} = \rho'_{0}$. Hence $\rho_{ij} = \text{Tr}(|j\rangle \langle i \rho_{0}|) = \text{Tr}(A) = \text{Tr}(A') = \text{Tr}(|j\rangle \langle i \rho'_{0}|) = \rho'_{ij}$. Because we can do this for all $ij$ we have $\rho_{0} = \rho'_{0}$. □

II. BLOCK STRUCTURE

We will now introduce the basic definitions of one-dimensional QCA.

In what follows $\Sigma$ will be a fixed finite set of symbols (i.e. ‘the alphabet’, describing the possible basic states each cell may take) and $q$ is a symbol such that $q \notin \Sigma$, which will be known as ‘the quiescent symbol’, which represents an empty cells. We write $q\Sigma = \{q\} \cup \Sigma$ for short.

Definition 5 (finite configurations)
A (finite) configuration $c$ of over $q\Sigma$ is a function $c : \mathbb{Z} \rightarrow q\Sigma$, with $i \mapsto c(i) = c_{i}$, such that there exists a (possibly empty) interval $I$ verifying $i \in I \implies c_{i} \in q\Sigma$ and $i \notin I \implies c_{i} = q$. The set of all finite configurations over $\{q\} \cup \Sigma$ will be denoted $C_{f}$.

Whilst configurations hold the basic states of an entire line of cells, and hence denote the possible basic states of the entire QCA, the global state of a QCA may well turn out to be a superposition of these. The following definition works because $C_{f}$ is a countably infinite set.

Definition 6 (superpositions of configurations)
Let $H_{c_{f}}$ be the Hilbert space of configurations, defined as follows. To each finite configuration $c$ is associated a unit vector $|c\rangle$, such that the family $(|c\rangle)_{c \in C_{f}}$ is an orthonormal basis of $H_{c_{f}}$. A superposition of configurations is then a unit vector in $H_{c_{f}}$.

Definition 7 (Unitarity)
A linear operator $G : H_{c_{f}} \rightarrow H_{c_{f}}$ is unitary if and only if $(G|c\rangle |c \in C_{f})$ is an orthonormal basis of $H_{c_{f}}$.

Definition 8 (Shift-invariance)
Consider the shift operation which takes configuration $c = \ldots c_{-1}c_{i}c_{i+1} \ldots$ to $c' = \ldots c'_{i-1}c'_{i+1} \ldots$ where for all $i c'_{i} = c_{i+1}$. Let $G : H_{c_{f}} \rightarrow H_{c_{f}}$ be its linear extension to superpositions of configurations. A linear operator $G : H_{c_{f}} \rightarrow H_{c_{f}}$ is said to be shift invariant if and only if $G\sigma = \sigma G$.

Definition 9 (Locality)
A linear operator $G : H_{c_{f}} \rightarrow H_{c_{f}}$ is said to be local with radius $\frac{1}{t}$ if and only if for any $\rho, \rho'$ two states over $H_{c_{f}}$, and for any $i \in \mathbb{Z}$, we have

$$\rho_{i, i+1} = \rho'_{i, i+1} \implies G\rho G^{\dagger}_{|i} = G\rho' G^{\dagger}_{|i}. \quad (7)$$

In the classical case, the definition would be that the letter to be read in some given cell $i$ at time $t+1$ depends only the state of the cells $i$ and $i+1$ at time $t$. This seemingly restrictive definition of locality is known in the classical case as a $\frac{1}{2}$-neighborhood cellular automaton. This is because the most natural way to represent such
an automaton is to shift the cells by \( \frac{1}{2} \) at each step, so that the state of a cell depends on the state of the two cells under it, as shown in figure 1. This definition of locality is actually not so restrictive, since by grouping cells into ‘supercells’ one can construct a \( \frac{1}{2} \)-neighborhood CA simulating the first one. The same thing can easily be done for QCA, so that this definition of locality is essentially done without loss of generality. Transposed to a quantum setting, we get the above definition: to know the state of cell number \( i \), we only need to know the state of cells \( i \) and \( i + 1 \) before the evolution.

We are now set to give the formal definition of one-dimensional quantum cellular automata.

**Definition 10 (QCA)**

A one-dimensional quantum cellular automaton (QCA) is an operator \( G : \mathcal{H}_{C_1} \to \mathcal{H}_{C_j} \) which is unitary, shift-invariant and local.

The next theorem provides us with another characterization of locality, more helpful in the proofs. But more importantly it entails structural reversibility, i.e. the fact that the inverse function of a QCA is also a QCA. Actually this theorem works for \( n \)-dimensional QCA as well as one.

**Theorem 3 (Structural reversibility)**

Let \( G \) be a unitary operator of \( \mathcal{H}_{C_1} \) and \( \mathcal{N} \) a finite subset of \( \mathbb{Z} \). The two properties are equivalent:

(i) For every states \( \rho \) and \( \rho' \) over the finite configurations, if \( \rho|_{\mathcal{N}} = \rho'|_{\mathcal{N}} \) then \( (G\rho G^\dagger)|_0 = (G\rho' G^\dagger)|_0 \).

(ii) For every operator \( A \) localized on cell 0, then \( G^\dagger AG \) is localized on the cells in \( \mathcal{N} \).

(iii) For every states \( \rho \) and \( \rho' \) over the finite configurations, if \( \rho|_{-\mathcal{N}} = \rho'|_{-\mathcal{N}} \) then \( (G^\dagger \rho G)|_0 = (G^\dagger \rho' G)|_0 \).

(iv) For every operator \( A \) localized on cell 0, then \( GAG^\dagger \) is localized on the cells in \( -\mathcal{N} \).

When \( G \) satisfies these properties, we say that \( G \) is local at 0 with neighbourhood \( \mathcal{N} \).

**Proof.**

\([i] \Rightarrow (ii)\). Suppose (i) and let \( A \) be an operator acting on cell 0. For every states \( \rho \) and \( \rho' \) such that \( \rho|_{\mathcal{N}} = \rho'|_{\mathcal{N}} \), we have \( \text{Tr} \left( AG\rho G^\dagger \right) = \text{Tr} \left( AG\rho' G^\dagger \right) \), using lemma 3 and our hypothesis that \( (G\rho G^\dagger)|_0 = (G\rho' G^\dagger)|_0 \). We thus get \( \text{Tr} \left( G^\dagger AG\rho \right) = \text{Tr} \left( G^\dagger AG\rho' \right) \). Since this is true of every \( \rho \) and \( \rho' \) such that \( \rho|_{\mathcal{N}} = \rho'|_{\mathcal{N}} \), this means, again according to lemma 3, that \( G^\dagger AG \) is localized on the cells in \( \mathcal{N} \).

\([ii] \Rightarrow (i)\). Suppose (ii) and let \( A \) be an operator acting on cell 0. Consider some operator \( M \) acting on a cell \( i \) which does not belong to \( -\mathcal{N} \). According to our hypothesis we know that \( G^\dagger MG \) does not act upon cell \( 0 \), and hence it commutes with \( A \). But \( AB \leftarrow GAG^\dagger GBG^\dagger = GAG^\dagger \) is a morphism, hence \( G^\dagger MG \) is also commutes with \( GAG^\dagger \). Because \( M \) can be chosen amongst to full matrix algebra \( M_d(\mathbb{C}) \) of cell \( i \), this entails that \( GAG^\dagger \) must be the identity upon this cell. The same can be said of any cell outside \( -\mathcal{N} \).

\([iv] \Rightarrow (ii)\), \([iii] \Rightarrow (iv)\), \([iii] \Leftarrow (iv)\) are symmetrical to \([ii] \Rightarrow (iv)\), \([i] \Rightarrow (ii)\), \([i] \Leftarrow (i)\] just by interchanging the roles of \( G \) and \( G^\dagger \).

Now this is done we proceed to prove the structure theorem for QCA over finite, unbounded configurations. This is a simplification of [10]. The basic idea of the proof is that in a cell at time \( t \) we can separate what information will be sent to the left at time \( t + 1 \) and which information will be sent to the right at time \( t + 1 \). But first of all we shall need two lemmas. These are better understood by referring to Figure 2.

**Lemma 4** Let \( \mathcal{A} \) be the image of the algebra of the cell 1 under the global evolution \( G \). It is localized upon cells \( 0 \) and \( 1 \), and we call \( \mathcal{A}|_1 \) the restriction of \( \mathcal{A} \) to cell 1. Let \( \mathcal{B} \) be the image of the algebra of the cell 2 under the global evolution \( G \). It is localized upon cells \( 1 \) and \( 2 \), and we call \( \mathcal{B}|_1 \) the restriction of \( \mathcal{B} \) to cell 1.

There exists a unitary \( U \) acting upon cell 1 such that \( U\mathcal{A}|_0 U^\dagger \) is of the form \( M_p(\mathbb{C}) \otimes I_q \) and \( U\mathcal{B}|_1 U^\dagger \) is of the form \( I_p \otimes M_q(\mathbb{C}) \), with \( pq = d \).

**Proof.**

\( \mathcal{A} \) and \( \mathcal{B} \) are indeed localized as stated due to the locality of \( G \) and a straightforward application of lemma 3 with \( \mathcal{N} = \{0,1\} \), which we can apply at position 1 and 2 by shift-invariance.
Lemma 5
Let $\mathcal{B}$ be the image of the algebra of the cell 2 under the global evolution $G$. It is localized upon cells 1 and 2, and we call $B_{1}$ the restriction of $\mathcal{B}$ to cell 1 and $B_{2}$ the restriction of $\mathcal{B}$ to cell 2.

We have that $\mathcal{B} = B_{1} \otimes B_{2}$.

Proof. 
We know that $\mathcal{B}$ is isometric to $M_{q}(\mathbb{C})$ and we know that $B_{1} \otimes B_{2} \subset \mathcal{B}$. But then by the previous lemma applied upon cell 1 we also know that $B_{1}$ is isometric to $M_{p}(\mathbb{C})$ and if we apply it to cell 2 then we have that $B_{2}$ is isometric to $M_{q}(\mathbb{C})$. Hence the inclusion is an equality.

\[ AB \rightarrow GAG^{\dagger}GBG^{\dagger} \]

Moreover by lemma 3, the antecedents of the operators localized in cell 1 are all localized in cells 1 and 2. Plus they all have an antecedent because $G$ is surjective. Hence $AB_{1}$ is the entire cell algebra of cell 1, i.e. $M_{q}(\mathbb{C})$.

So now we can apply Theorem 2 and the result follows.

\[ V \]

\[ U \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]

\[ \]
due to the quiescent boundaries. □

Note that this structure could be further simplified if we were to allow ancillary cells [1].

III. QUANTIZATIONS AND CONSEQUENCES

The structure theorem for QCA departs in several important ways from the classical situation, giving rise to a number of apparent paradoxes. We begin this section by discussing some of these concerns in turns. Each of them is introduced via an example, which we then use to derive further consequences or draw the limits of the structure theorem.

Bijective CA and superluminal signalling.

First of all, it is a well-known fact that not all bijective CA are structurally reversible. The XOR CA is a standard example of that.

Definition 11 (XOR CA)

Let $C_f$ be the set of finite configurations over the alphabet $q\Sigma = \{0, 1\}$. For all $x, y$ in $q\Sigma$, let $\delta(xy) = x, \delta(xq) = q,$ and $\delta(qy) = x \oplus y$ otherwise. We call $F : C_f \rightarrow C_f$ the function mapping $c = \ldots c_{i-1}c_ic_{i+1}\ldots \rightarrow c' = \ldots \delta(c_{i-1}c_i)c_{i+1}\ldots$.

The XOR CA is clearly shift-invariant, and local in the sense that the state of a cell at $t+1$ only depends from its state and that of its right neighbour at $t$. It is also bijective. Indeed for any $c' = \ldots qqc'_{k+1}\ldots$ with $c_{k}$ the first non quiescent cell, we have $c_k = q$, $c_{k+1} = c'_k$, and therefor for $l \geq k+1$ we have either $c_{l+1} = c_l \oplus c'_l$ if $c'_l \neq q$, or again $c_{l+1} = q$ otherwise, etc. In other words the antecedent always exists (surjectivity) and is uniquely derived (injectivity) from left till right. But the XOR CA is not structurally reversible. Indeed for some $c' = \ldots 00000000\ldots$ we cannot know whether the antecedent of this large zone of zeroes is another large zone of zeroes or a large zone of ones – unless we deduce this from the left border as was previously described... but the left border may lie arbitrary far.

So classically there are bijective CA whose inverse is not a CA, and thus who do not admit any n-layered block representation at all. Yet surely, just by defining $F$ over $H_{C_f}$ by linear extension (e.g. $F(\alpha|\ldots 01\ldots + \beta|\ldots 11\ldots)) = \alpha.F|\ldots 01\ldots \beta.F|\ldots 11\ldots$) we ought to have a QCA, together with its block representation, hence the apparent paradox.

In order to lift this concern let us look at the properties of this quantized $F = \delta(abcd)$ linear map: $\delta(abcd) = (b \oplus a.c).c$. We call $F : C_f \rightarrow C_f$ the function mapping $c = \ldots c_{i-1}c_ic_{i+1}\ldots \rightarrow c' = \ldots \delta(c_{i-1}c_i)c_{i+1}\ldots$.

This is best described by Figure 7.

The Toffoli CA is clearly shift-invariant, and of radius 1/2. Let us check that its inverse is also of radius 1/2. For instance say we seek to retrieve $(c,d)$. $c$ is easy of course. By shift-invariance retrieving $d$ is like retrieving $b$. But since we have $a$ and $d$ in cleartext we can easily
substract $a.d$ from $b \oplus a.d$. Now why does it not have a two-layered block representation without cell grouping? Remember the toffoli gate is the controlled-controlled-NOT gate. Here $b$ is NOTed depending upon $a$ and $c$, which pass through unchanged, same for $d$ with the left and right neighbouring subcells, etc. So actually the Toffoli CA is just two layers of the toffoli gate, as we have shown in Figure 5. But we know that the toffoli gate cannot be obtained from two bit gates in classical reversible electronics, hence there cannot be a two-layered block representation without cell grouping.

So classically there exists some structurally reversible CA, of radius $1/2$, whose inverse is also of radius $1/2$, but do not admit a two-layered block representation without cell grouping. Yet surely, just by defining $F$ over $\mathcal{H}_C$, by linear extension we ought to have a QCA, together with its block representation, and that construction does not need any cell grouping, hence again the apparent paradox.

Once more let us take a step back. The Toffoli CA is yet another case where exploiting quantum superpositions of configurations enables us to have information flowing faster than in the classical setting, just like for the XOR CA. But unlike the XOR CA, the speed of information remains bounded in the Toffoli CA, and so up to cell grouping it can still be considered a QCA. Therefore we reach the following proposition.

**Proposition 2 (Quantum information flows faster)**

Let $F : \mathcal{C}_f \rightarrow \mathcal{C}_f$ be a CA and $F : \mathcal{H}_C \rightarrow \mathcal{H}_C$, the corresponding QCA, as obtained by linear extension of $F$. Information may flow faster in the the quantized version of $F$.

This result is certainly intriguing, and one may wonder whether it might contain the seed of a novel development quantum information theory, as opposed to its classical counterpart.

**No-go for n-dimensions.**

Finally, it is again well-known that in two-dimensions there exists some structurally reversible CA which do not admit a two-layered block representation, even after a cell-grouping. The standard example is that of Kari [8]:

**Definition 13 (Kari CA)** Let $\mathcal{C}_f$ be the set of finite configurations over the alphabet $\{0,1\}^9$, with $0^9$ is now taken as the quiescent symbol. So each cell is made of 8 bits, one for each cardinal direction (North, North-East...), plus one bit in the center, as in Figure 6. At each time step, the North bit of a cell undergoes a NOT only if the cell lying North has center bit equal to 1, the North-East bit of a cell undergoes a NOT only if the cell lying North-East has center bit equal to 1, and so on. Call $F$ this CA.

This is clearly shift-invariant, local and structurally reversible. Informally the proof that the Kari CA does not admit a a two-layered block representation, even if we group cells into supercells, runs as follows [8]:

- Suppose $F$ admits a decomposition into $U$ and $V$ blocks;
- Consider cells $x, y, z$ such that they are all neighbours; $x, y$ are in the same $V$-block but not $z$; $x$ and $y, z$ are not in the same $U$-block, as in Figure 6.
- Consider $c_1$ the configuration with 1 as the center bit of $x$ and zero everywhere. Run the $U$-blocks, the hatched zone left of Figure 7 represents those cells which may not be all zeros;
- Consider the configuration obtained from the previous $Uc_1$ by putting to zero anything which lies not the $V$-block of $z$, as in Figure 7. Call it $c'$, and let $c$ be defined as the antecedent of $c$ under a run of the $U$-blocks;
- On the one hand we know that $F(c)$ is obtained from a run of the $V$-blocks from $c'$. In the left $V$-block there are just zeroes so $F(c)$ has only zeroes, in particular the North bit of the $y$ cell is 0. But the right $V$-block is exactly the same as that of $Uc_1$, and so we know that the North-West bit of the $y$ cell of $F(c)$ is 1, as in the left of Figure 8.
- On the other hand since $c'$ has zeroes everywhere but in the above $U$-block, the same is true of $c$, as shown right of the Figure 8. A consequence of this is that the North bit of the $y$ cell must be equal to the North-West bit of the $z$ cells, as they are both obtained from the same function of the center bit of the $x$ cell;
- Hence the contradiction.

Now by defining $F$ over $H_{C_f}$, by linear extension we have a QCA, and the proof applies in a very similar fashion, the contradiction being that the state of the North qubit of the $y$ cell must be equal to the state of the North-West bit of the $z$ cells, whether these are mixed states or not. Hence we have a counterexample to the higher-dimensional case of the Theorem in [9]. We reach the following proposition.

**Proposition 3 (No-go for n-dimensions)** There exists some 2-dimensional QCA which do not admit a two-layered block representation.

Understanding the structure of the $n$-dimensional QCA is clearly the main challenge that remains ahead of us.

**Acknowledgements**

We would like to thank Jacques Mazoyer, Torsten Franz, Holger Vogts, Jarkko Kari, Jérôme Durand-Lose, Renan Fargetton, Philippe Jorrand for a number of helpful conversations.

---

[1] P. Arrighi, *Intrinsically universal one-dimensional quantum cellular automata*, MFCS’07, (2007).
[2] P. Arrighi, R. Fargetton, *Intrinsically universal one-dimensional quantum cellular automata*, DCM’07, (2007).
[3] O. Bratteli, D. Robinson, *Operators algebras and quantum statistical mechanics 1*, Springer, (1987).
[4] C. Dürr, H. LêThanh, M. Santha, *A decision procedure for well formed quantum cellular automata*, Random Structures and Algorithms, 11, 381–394, (1997).
[5] C. Dürr, M. Santha, *A decision procedure for unitary quantum linear cellular automata*, SIAM J. of Computing, 31(4), 1076–1089, (2002).
[6] R. P. Feynman, *Quantum mechanical computers*, Found. Phys. 16, 507-531, (1986).
[7] D. Gijswijt, *Matrix algebras and semidefinite programming techniques for codes*, Ph.D. thesis, University of Amsterdam, 2005.
[8] J. Kari, *On the circuit depth of structurally reversible cellular automata*, Fundamenta Informaticae, 34, 1-15, (1999).
[9] B. Schumacher, R. F. Werner, *Reversible quantum cellular automata*, arXiv:quant-ph/0405174.
[10] D. J. Shepherd, T. Franz, R. F. Werner, *Universally programmable quantum cellular automata*, Phys. Rev. Lett., 97, 020502 (2006).
[11] J. Watrous, *On one-dimensional quantum cellular automata*, Complex Systems 5(1), 19–30, (1991).