Int. Journ. of Unconventional Computing, Vol. 7, pp. 223–244
Reprints available directly from the publisher
Photocopying permitted by license only

One-Dimensional Quantum Cellular Automata

PABLO ARRIGHI[1,2], VINCENT NESME[3] AND REINHARD WERNER[4]

[1]*Université de Grenoble, Laboratoire LIG, 220 rue de la chimie, 38400 Saint-Martin-d'Hères, France*

[2]*École Normale Supérieure de Lyon, Laboratoire LIP, 46 allée d'Italie, 69364 Lyon cedex 07, France*

[3]*Quantum information theory, Universität Potsdam, Karl-Liebknecht-Str. 24/25, 14476 Potsdam, Germany*

[4]*Leibniz Universität Hannover, Institut für theoretische Physik, Appelstr. 2, 30167 Hannover, Germany*

Received: September, 2009. Accepted: December, 2010

We define and study quantum cellular automata (QCA). We show that they are reversible and that the neighborhood of the inverse is the opposite of the neighborhood. We also show that QCA always admit, modulo shifts, a two-layered block representation. 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 [18]. Here the proof is simpler and self-contained, moreover we discuss a counterexample QCA in higher dimensions.

Keywords: cellular automata, quantum, neighborhood, block representation

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 causal, 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 [11] – 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 or the spatial parallelism of things [2], either for the purpose of describing a quantum protocol, or to model a quantum physical phenomena [16].

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 causal, shift-invariant unitary evolution. By causal 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 only consider 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 [7] – but here we want our proofs to be self-contained and accessible to the Computer Science community. Our main result is that QCA can always be expressed as two layers of an infinitely repeating unitary gate including local unitaries and partial shifts, even over such finite configurations. Our proof method is mainly a drastic simplification of that of the same theorem over infinite configurations, adapted to finite unbounded configurations. Moreover in its present form the theorem over infinite configurations is stated for n-dimensions [18], which we prove is incorrect by presenting a two-dimensional QCA which does not admit a two-layered block representation.

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 [9, 10, 1]. 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 the case in the realm of cellular automata. Curiously the nonlocality of quantum states (entanglement) induces more structure upon the cellular automata – so that its evolution may remain causal 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 provide a simple axiomatic presentation of QCA (Section 1). We reorganize a number of known mathematical results around the notion of subsystems in quantum theory (Section 2). Thanks to this small theory we prove the reversibility/block structure theorem in an elementary manner (Section 3). Lastly, 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 4). It turns out that these considerations have already led to further works, which we point out. Indeed, this paper is the journal version of a conference paper [6]; it aims at providing a self-contained, all-proofs-included, more formal presentation of the same results, with updated references.

1 AXIOMATICS OF QCA

We will now introduce the basic definitions of one-dimensional QCA. In what follows Σ 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 1 (finite configurations).
A (finite) configuration *c over $q + \Sigma$ is a function $c : \mathbb{Z} \longrightarrow q + \Sigma$, with $i \longmapsto c(i) = c_i$, such that there exists a (possibly empty) interval I verifying $i \in I \Rightarrow c_i \in q + \Sigma$ and $i \notin I \Rightarrow c_i = q$. The set of all finite configurations over $\{q\} \cup \Sigma$ will be denoted $\mathcal{C}_f$.*

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. Since $\mathcal{C}_f$ is countable, the following definition works.

Definition 2 (superpositions of configurations).
Let $\mathcal{H}_{\mathcal{C}_f}$ 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 $(|c\rangle)_{c \in \mathcal{C}_f}$ is an orthonormal basis of $\mathcal{H}_{\mathcal{C}_f}$. A superposition of configurations *is then a unit vector in $\mathcal{H}_{\mathcal{C}_f}$.*

This space of QCA configurations is the same one as in [20, 9, 10, 1]. It is isomorphic to the cyclic one considered in [15], but fundamentally different from the finite, bounded periodic space of [19] and the infinite setting of [18].

Definition 3 (Unitarity).
A linear operator $G : \mathcal{H}_{\mathcal{C}_f} \longrightarrow \mathcal{H}_{\mathcal{C}_f}$ *is* unitary *if and only if* $\{G|c\rangle \mid c \in \mathcal{C}_f\}$ *is an orthonormal basis of* $\mathcal{H}_{\mathcal{C}_f}$.

Definition 4 (Shift-invariance).
Consider the shift operation which takes configuration $c = \ldots c_{i-1}c_ic_{i+1}\ldots$ *to* $c' = \ldots c'_{i-1}c'_ic'_{i+1}\ldots$ *where for all* i $c'_i = c_{i+1}$. *Let* $\sigma : \mathcal{H}_{\mathcal{C}_f} \longrightarrow \mathcal{H}_{\mathcal{C}_f}$ *be its linear extension to superpositions of configurations. A linear operator* $G : \mathcal{H}_{\mathcal{C}_f} \longrightarrow \mathcal{H}_{\mathcal{C}_f}$ *is said to be* shift invariant *if and only if* $G\sigma = \sigma G$.

Definition 5 (Causality).
A linear operator $G : \mathcal{H}_{\mathcal{C}_f} \longrightarrow \mathcal{H}_{\mathcal{C}_f}$ *is said to be* causal *with radius* $\frac{1}{2}$ *if and only if for any* ρ, ρ' *two states over* $\mathcal{H}_{\mathcal{C}_f}$, *and for any* $i \in \mathbb{Z}$, *we have*

$$\rho|_{i,i+1} = \rho'|_{i,i+1} \quad \Rightarrow G\rho G^\dagger|_i = G\rho' G^\dagger|_i. \tag{1}$$

where we have written $A|_S$ *for the matrix* $Tr_{\bar{S}}(A)$, *i.e. the partial trace obtained from A once all of systems that are not in S have been traced out.*

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 on the state of the cells i and $i+1$ at time t. This seemingly restrictive definition of causality 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 causality is actually not so restrictive, since by grouping cells into 'supercells' and composing with shifts 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 causality 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.

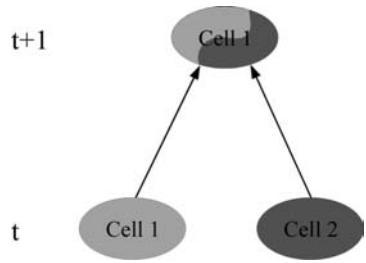

FIGURE 1
A $\frac{1}{2}$-neighborhood CA

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

Definition 6 (QCA).
A one-dimensional quantum cellular automaton (QCA) is an operator $G : \mathcal{H}_{\mathcal{C}_f} \longrightarrow \mathcal{H}_{\mathcal{C}_f}$ *which is unitary, shift-invariant and causal.*

This is clearly the natural axiomatic quantization of the notion of cellular automata. An almost equivalent definition in the litterature is phrased in terms of homomorphism of a C^*-algebra [18]. On the other hand the definitions in [20, 9, 10, 15, 19, 1, 17] are not axiomatic, in the sense that they all make particular assumptions about the form of the local action of G, and G is then defined as a composition of these actions. The present work justifies some of these assumptions [17] to some extent.

The next theorem provides us with another characterization of causality, 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. This theorem works for n-dimensional QCA as well as one. We are not aware of a rigorous proof of this fact for n-dimensional QCA in the previous litterature.

Theorem 1 (Structural reversibility).
Let G *be a unitary operator of* $\mathcal{H}_{\mathcal{C}_f}$ *and* $\mathcal{N}$ *a finite subset of* $\mathbb{Z}$*. The four properties are equivalent:*

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

(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 ρ *and* ρ' *over the finite configurations, if* $\rho|_{-\mathcal{N}} = \rho'|_{-\mathcal{N}}$ *then* $\left(G^\dagger \rho G\right)|_0 = \left(G^\dagger \rho' G\right)|_0$.

(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 causal at* 0 *with neighbourhood* $\mathcal{N}$*. Here* $-\mathcal{N}$ *take the opposite of each of the elements of* $\mathcal{N}$.

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

operator A localized on cell 0, we get:

$$\begin{aligned}\mathrm{Tr}\left(AG\rho G^\dagger\right) &= \mathrm{Tr}\left(G^\dagger AG\rho\right)\\ &= \mathrm{Tr}\left(G^\dagger AG\rho'\right)\\ &= \mathrm{Tr}\left(AG\rho' G^\dagger\right)\end{aligned}$$

Again by lemma 3, this means $\left(G\rho G^\dagger\right)|_0 = \left(G\rho' G^\dagger\right)|_0$.
$[(ii) \Rightarrow (iv)]$. 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 $AB \mapsto GAG^\dagger GBG^\dagger = GABG^\dagger$ is a morphism, hence $GG^\dagger MGG^\dagger = M$ 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 $[(ii) \Rightarrow (iv)]$, $[(i) \Rightarrow (ii)]$, $[(ii) \Leftarrow (i)]$ just by interchanging the roles of G and $G^\dagger$. □

2 A SMALL THEORY OF SUBSYSTEMS

The purpose of this section is to provide a series of mathematical results about 'When can something be considered a subsystem in quantum theory?'. Let us work towards making this sentence more precise. The 'something' will be an matrix algebra (a C^*-algebra over a finite-dimensional system):

Definition 7 (Algebras).
Consider $\mathcal{A} \subseteq M_n(\mathbb{C})$. We say that $\mathcal{A}$ is an algebra *of $M_n(\mathbb{C})$ if and only if it is closed under weighting by a scalar (.), addition (+), matrix multiplication ($*$), adjoint (†). Moreover for any S a subset of $M_n(\mathbb{C})$, we denote by curly $\mathcal{S}$ its closure under the above-mentioned operations.*

The key issue here is that the notion of subsystem is usually a base-dependent one, i.e. one tends to say that $\mathcal{A}$ is a subsystem if $\mathcal{A} = M_p(\mathbb{C}) \otimes \mathbb{I}_q$, but this depends on a particular choice of basis/tensor decomposition. Let us make the definition base-independent, artificially at first.

Definition 8 (Subsystem algebras).
Consider a subalgebra $\mathcal{A}$ of $M_n(\mathbb{C})$. We say that $\mathcal{A}$ is a subsystem algebra *of $M_n(\mathbb{C})$ if and only if there exists $p, q \in \mathbb{N}$ / $pq = n$ and $U \in M_n(\mathbb{C})$ / $U^\dagger U = UU^\dagger = \mathbb{I}_n$ such that $U\mathcal{A}U^\dagger = M_p(\mathbb{C}) \otimes \mathbb{I}_q$.*

We now work our way towards simple characterizations of subsystem algebras.

Definition 9 (Center algebras).
For $\mathcal{A}$ an algebra of $M_n(\mathbb{C})$, we note $\mathcal{C}_\mathcal{A} = \{A \in \mathcal{A} \mid \forall B \in \mathcal{A}\ BA = AB\}$. $\mathcal{C}_\mathcal{A}$ is also an algebra of $M_n(\mathbb{C})$, which is called the center algebra *of $\mathcal{A}$.*

Theorem 2 (Characterizing one subsystem).
Let $\mathcal{A}$ be an algebra of $M_n(\mathbb{C})$ and $\mathcal{C}_\mathcal{A} = \{A \in \mathcal{A} \mid \forall B \in \mathcal{A}\ BA = AB\}$ its center algebra. *Then $\mathcal{A}$ is a subsystem algebra if and only if $\mathcal{C}_\mathcal{A} = \mathbb{C}\mathbb{I}_n$.*

Proof. The argument is quite technical and its understanding not mandatory for understanding the rest of the paper. Its presentation is based on [12]. See also [7] for a proof within the setting of general C^*-algebras.
$[\Rightarrow]$.
$\mathcal{C}_{M_p(\mathbb{C})} = \mathbb{C}\mathbb{I}_p$ because the center algebra of a full matrix algebra is just the identity and its multiples. Hence $\mathcal{C}_{M_p(\mathbb{C})\otimes\mathbb{I}_q} = \mathbb{C}\mathbb{I}$, i.e the center algebra of a subsystem algebra is also just the identity and its multiples.
$[\Leftarrow]$.
CONSIDER some set $P = \{P_i\}_{i=1\ldots p}$ such that:
(i) $\forall i = 1 \ldots p\ P_i \in \mathcal{A}$;
(ii) $\forall i, j = 1 \ldots p\ P_i P_j = \delta_{ij} P_i \in \mathcal{A}$.
Moreover we take P is maximal, i.e. so that there is no set $Q = \{Q_i\}$ verifying conditions (i), (ii) and such that $\mathcal{P} \subset \mathcal{Q}$, with $\mathcal{P}$, $\mathcal{Q}$ the closures of P, Q. Note that:
(iii) $\sum_{i=1\ldots p} P_i = \mathbb{I}$,
otherwise $\mathbb{I} - \sum_{i=1\ldots p} P_i$ may be added to the set.
FIRST we show that

$$\forall i \quad [P_i \mathcal{A} P_i = \mathbb{C} P_i]. \tag{2}$$

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 $M \in \mathcal{A}$ such that $P_i M P_i \not\propto P_i$. If M is proportional to a unitary let $N = M + M^\dagger$, else let $N = M^\dagger M$. In any case we have $P_i N P_i \not\propto P_i$ with N hermitian. Note that $H = P_i N P_i$ 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 λ_k's distinct real numbers. Any such Q_k is part of $\mathcal{A}$, since $Q_k = \dfrac{H \prod_{l\neq k} (H - \lambda_l \mathbb{I})}{\lambda_k \prod_{l\neq k} (\lambda_k - \lambda_i)}$. Consider the set $Q = P/\{P_i\} \cup_k \{Q_k\}$. It satisfies condition (i), (ii) but $\mathcal{P} \subset \mathcal{Q}$, which is impossible.
SECOND we show that

$$\forall i, j \quad [P_i \mathcal{A} P_j \neq 0]. \tag{3}$$

Intuitively this is because the contrary would split $\mathcal{A}$ into the direct sum of two matrix algebras, and hence go against the fact that $\mathcal{C}_\mathcal{A} = \mathbb{C}\mathbb{I}$. Formally

write $i \sim j$ whenever this is the case. The relation $\sim$ is reflexive by Eq. (2), transitive by multiplicative closure of $\mathcal{A}$, and symmetric since

$$\begin{aligned} P_i \mathcal{A} P_j \neq 0 &\Rightarrow (P_i \mathcal{A} P_j)^\dagger \neq 0 \\ &\Rightarrow (P_j \mathcal{A}^\dagger P_i) \neq 0 \\ &\Rightarrow (P_j \mathcal{A} P_i) \neq 0. \end{aligned}$$

Say there is an equivalence class $J \subset 1 \dots p$ and let $P_I = \sum_{i \notin J} P_i$, $P_J = \sum_{j \in J} P_j$. Then

$$\begin{aligned} \mathcal{A} P_J &= (P_I + P_J) \mathcal{A} P_J \\ &= P_J \mathcal{A} P_J \\ &= P_J \mathcal{A} \quad \text{symmetrically.} \end{aligned}$$

and so $P_J \in \mathcal{C}_\mathcal{A}$, which is impossible.

THIRD we show that for all A, for all $i, j = 1 \dots p$, if we let $M = P_i A P_j$ then

$$\exists \lambda \in \mathbb{C} \quad [M^\dagger M = \lambda P_i \wedge M M^\dagger = \lambda P_j]. \tag{4}$$

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

FOURTH we show that

$$\forall i, j \quad [\mathrm{Tr}(P_i) = \mathrm{Tr}(P_j) = \text{some constant } q]. \tag{5}$$

For each i, j take some $A \in \mathcal{A}$ verifying Eq. (3). Let $M = P_i A P_j$. By Eq. (4) there is a complex number λ such that we have $P_i = \lambda M M^\dagger$ and $P_j = \lambda M^\dagger M$. Then the equality follows from $\mathrm{Tr}(\lambda M M^\dagger) = \mathrm{Tr}(\lambda M^\dagger M)$.

FIFTH consider some unitary U which takes those $\{P_i\}_{i=1\dots p}$ into one-zero orthogonal diagonal matrices $I = \{\mathbf{I}_i\}_{i=1\dots p}$ with $\mathbf{I}_i = |i\rangle\langle i| \otimes \mathbb{I}_q$. Note that this is always possible since the $\{P_i\}_{i=1\dots p}$ form an orthogonal (*ii*), complete (*iii*) set of projectors of equal dimension by Eq. (5). We show that

$$\begin{aligned} \forall A \in U \mathcal{A} U^\dagger \, \forall i, j \quad & [\mathbf{I}_i A \mathbf{I}_j = |i\rangle\langle j| \otimes A_{ij}] \\ & \text{with } A_{ij} A_{ij}^\dagger = A_{ij}^\dagger A_{ij} \propto \mathbb{I}_q. \end{aligned} \tag{6}$$

The first line stems from the form of I, i.e. $\mathbf{I}_i A \mathbf{I}_j$

$$= \sum_{pqkl} A_{pqkl}(|i\rangle\langle i| \otimes \mathbb{I}_q)(|p\rangle\langle q| \otimes |k\rangle\langle l|)(|j\rangle\langle j| \otimes \mathbb{I}_q)$$
$$= \sum_{kl} A_{ijkl}(|i\rangle\langle j| \otimes |k\rangle\langle l|) = |i\rangle\langle j| \otimes (\sum_{kl} A_{ijkl}|k\rangle\langle l|).$$

For the second line let $M = \mathbf{I}_i A \mathbf{I}_j$. By Eq. (4) there is a complex number λ such that we have both $\mathbf{I}_i = \lambda M M^\dagger$ and $\mathbf{I}_j = \lambda M^\dagger M$. But then

$$|i\rangle\langle i| \otimes \mathbb{I}_q = \mathbf{I}_i =$$
$$\lambda M M^\dagger = \lambda(|i\rangle\langle j| \otimes A_{ij})(|i\rangle\langle j| \otimes A_{ij}^\dagger)$$
$$= \lambda |i\rangle\langle j| \otimes A_{ij} A_{ij}^\dagger$$

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

FINALLY consider some unitary $V = \sum_i |i\rangle\langle i| \otimes A_{1i}$, where $U^\dagger A U$ is some matrix verifying Eq. (3), and rescaled so that Eq. (6) makes A_{1j} it unitary. We show that

$$\forall M \in V U \mathcal{A} U^\dagger V^\dagger \, \forall i, j \quad [\mathbf{I}_i M \mathbf{I}_j = |i\rangle\langle j| \otimes \lambda \mathbb{I}_q]$$
$$\text{with } \lambda \text{ a complex number.}$$

For a better understanding of V notice that

$$V = \sum_i (|i\rangle\langle i| \otimes A_{1i})$$
$$= \sum_i (|i\rangle\langle 1| \otimes \mathbb{I}_q)(|1\rangle\langle i| \otimes A_{1i})$$
$$= \sum_i (|i\rangle\langle 1| \otimes \mathbb{I}_q)\mathbf{I}_1 A \mathbf{I}_i$$

Consider $B = V^\dagger M V$. It belongs to $U \mathcal{A} U^\dagger$ and by Eq. (6) it is of the form $B = \sum_{ij} |i\rangle\langle j| \otimes B_{ij}$. Now $\mathbf{I}_i M \mathbf{I}_j$

$$= \mathbf{I}_i V B V^\dagger \mathbf{I}_j$$
$$= (|i\rangle\langle 1| \otimes \mathbb{I}_q)\mathbf{I}_1 A \mathbf{I}_i B \mathbf{I}_j A^\dagger \mathbf{I}_1 (|1\rangle\langle j| \otimes \mathbb{I}_q)$$
$$= (|i\rangle\langle 1| \otimes \mathbb{I}_q)\lambda \mathbf{I}_1 (|1\rangle\langle j| \otimes \mathbb{I}_q)$$
$$= \lambda(|i\rangle\langle 1| \otimes \mathbb{I}_q)(|1\rangle\langle 1| \otimes \mathbb{I}_q)(|1\rangle\langle j| \otimes \mathbb{I}_q)$$
$$= \lambda |i\rangle\langle j| \otimes \mathbb{I}_q \qquad \square$$

Next we give two simple conditions for some algebras $\mathcal{A}$ and $\mathcal{B}$ to be splitted as a tensor product, namely commutation and generacy.

Theorem 3 (Characterizing several subsystems).
Let $\mathcal{A}$ and $\mathcal{B}$ be commuting algebras of $M_n(\mathbb{C})$ such that $\mathcal{AB} = M_n(\mathbb{C})$. Then there exists a unitary matrix U such that, $U\mathcal{A}U^\dagger$ is $M_p(\mathbb{C}) \otimes \mathbb{I}_q$ and $U\mathcal{B}U^\dagger$ is $\mathbb{I}_p \otimes M_q(\mathbb{C})$, with $pq = n$.

Proof.
First, let us note that $\mathcal{C}_\mathcal{A}$ includes $\mathbb{C}\mathbb{I}_n$. Next, the elements of $\mathcal{C}_\mathcal{A}$ 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 $\mathcal{AB} = M_n(\mathbb{C})$, $\mathcal{C}_\mathcal{A}$ is equal to $\mathbb{C}\mathbb{I}_n$. Thus, according to proposition 2, it is a subsystem algebra. For simplicity matters, and without loss of generality, we will assume that $\mathcal{A}$ is actually equal to $M_p(C) \otimes \mathbb{I}_q$ 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 $\mathbb{I}_p \otimes M_q(\mathbb{C})$. □

Often however we want to split some algebras $\mathcal{A}$ and $\mathcal{B}$ as a tensor product, not over the union of the subsystems upon which they act, but over the intersection of the subsystems upon which they act. The next definition and two lemmas will place us in a position to do so.

Definition 10 (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 $A|_1$ for the matrix $Tr_{02}(A)$, i.e. the partial trace obtained from A once systems 0 and 2 have been traced out. Similarly so we call $\mathcal{A}|_1$ the restriction of $\mathcal{A}$ to the middle subsystem, i.e. the algebra generated by $\{Tr_{02}(A) \,|\, A \in \mathcal{A}\}$.

Notice that this definition of Restriction of linear maps is nothing but the trace out, whereas Restriction of algebras is nothing but the closure of the trace outs of its constituent linear maps. Hence this definition naturally generalizes to other subdivisions of a Hilbert space into a tensor product of Hilbert spaces. Notice also that these Restriction algebras contain, in general, less elements than the Support algebras defined in [18], whose definition is more involved. It turns out that we will not need support algebras in this paper.

Now, when we restrict our commuting algebras to the subsystem they have in common, their restrictions still commute:

Lemma 1 (Restriction of commuting algebras).
Consider $\mathcal{A}$ an algebra of $M_p(\mathbb{C}) \otimes M_q(\mathbb{C}) \otimes \mathbb{I}_r$ and $\mathcal{B}$ an algebra of $\mathbb{I}_p \otimes M_q(\mathbb{C}) \otimes M_r(\mathbb{C})$. Suppose $\mathcal{A}$ and $\mathcal{B}$ commute. Then so do $\mathcal{A}|_1$ and $\mathcal{B}|_1$.

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

$$\forall A \in \mathcal{A}, B \in \mathcal{B} \quad pr.\,\mathrm{Tr}_{02}(AB) = \mathrm{Tr}_{02}(A)\mathrm{Tr}_{02}(B). \tag{7}$$

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

$$\begin{aligned} pr.\,\mathrm{Tr}_{02}(AB) &= \mathrm{Tr}_{02}\Big(\sum_{ij} pr\alpha_i\beta_j.(\sigma_i \otimes \tau_i\mu_j \otimes \nu_j)\Big) \\ &= \Big(\sum_i r\alpha_i.\,\mathrm{Tr}(\sigma_i).\,\tau_i\Big)\Big(\sum_j p\beta_j.\,\mathrm{Tr}(\nu_j).\,\mu_j\Big) \\ &= \mathrm{Tr}_{02}(A)\mathrm{Tr}_{02}(B). \end{aligned}$$

Now $\mathcal{A}|_1$ is generated by $\{\mathrm{Tr}_{02}(A) \mid A \in \mathcal{A}\}$, while $\mathcal{B}|_1$ is generated by $\{\mathrm{Tr}_{02}(B) \mid B \in \mathcal{B}\}$. Since commutation is preserved by $*$, $+$, $\alpha.$ and $\dagger$ all we need to check is that the generating elements commute. Consider $A|_1$ an element of $\mathcal{A}|_1$ and take A such that $A|_1 = \mathrm{Tr}_{02}(A)$. Similarly take $B|_1$ and B such that $B|_1 = \mathrm{Tr}_{02}(B)$. We have $A|_1B|_1 = \mathrm{Tr}_{02}(A)\mathrm{Tr}_{02}(B) = pr.\,\mathrm{Tr}_{02}(AB) = pr.\,\mathrm{Tr}_{02}(BA) = \mathrm{Tr}_{02}(B)\mathrm{Tr}_{02}(A) = B|_1A|_1$. □
Moreover when we restrict our generating algebras to the subsystem they have in common, theirs restrictions generate the subsystem.

Lemma 2 (Restriction of generating algebras).
Consider $\mathcal{A}$ an algebra of $M_p(\mathbb{C}) \otimes M_q(\mathbb{C}) \otimes \mathbb{I}_r$ and $\mathcal{B}$ an algebra of $\mathbb{I}_p \otimes M_q(\mathbb{C}) \otimes M_r(\mathbb{C})$. Suppose $\mathcal{AB}|_1 = M_p(\mathbb{C})$. Then we have that $\mathcal{A}|_1\mathcal{B}|_1 = M_p(\mathbb{C})$.

Proof.
$\mathcal{AB}|_1$ is generated by $\{\mathrm{Tr}_{02}(AB) \mid A \in \mathcal{A}, B \in \mathcal{B}\}$. However by Eq. (7) this is the same as $\{\mathrm{Tr}_{02}(A)\mathrm{Tr}_{02}(B) \mid A \in \mathcal{A}, B \in \mathcal{B}\}$, which generates $\mathcal{A}|_1\mathcal{B}|_1$. □

This last lemma will let us switch from the notion of localized observable to the notion of partial density matrix, and hence serve to express locality both ways.

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

$$\forall \rho, \rho' \quad [\rho|_0 = \rho'|_0 \Rightarrow Tr(A\rho) = Tr(A\rho')].$$

Moreover we have that $\rho|_0 = \rho'|_0$ is equivalent to

$$\forall A \in M_p(\mathbb{C}) \otimes \mathbb{I} \quad [Tr(A\rho) = Tr(A\rho')].$$

Proof.
Physically the first part of the lemma says that "a 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 $\mathrm{Tr}\,(A\rho) = \mathrm{Tr}\,(A_0(\rho|_0))$. Assuming $\rho|_0 = \rho'|_0$ yields $\mathrm{Tr}\,(A\rho) = \mathrm{Tr}\,(A_0\rho|_0) = \mathrm{Tr}\left(A_0(\rho'|_0)\right) = \mathrm{Tr}\left(A\rho'\right)$.
[$\Leftarrow$]. 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 $A_0 \otimes \mathrm{Id}_1$, 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, $\mathrm{Tr}\left(B_{ij}|x\rangle\langle x|\right) \neq \mathrm{Tr}\left(B_{ij}|y\rangle\langle y|\right)$. 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 $\mathrm{Tr}\,(A\rho) \neq \mathrm{Tr}\left(A\rho'\right)$.
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 $\mathrm{Tr}\,(A\rho) = \mathrm{Tr}\left(A\rho'\right)$ for $A = |j\rangle\langle i| \otimes \mathbb{I}$ yields $\rho|_{0_{ij}} = \mathrm{Tr}\,(|j\rangle\langle i|\rho|_0) = \mathrm{Tr}\,(A\rho) = \mathrm{Tr}\left(A\rho'\right) = \mathrm{Tr}\left(|j\rangle\langle i|\rho'|_0\right) = \rho'|_{0_{ij}}$. Because we can do this for all ij we have $\rho|_0 = \rho'|_0$. □

3 BLOCK STRUCTURE

Now this is done we proceed to prove the structure theorem for QCA over finite, unbounded configurations. This is a simplification of [18]. 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.

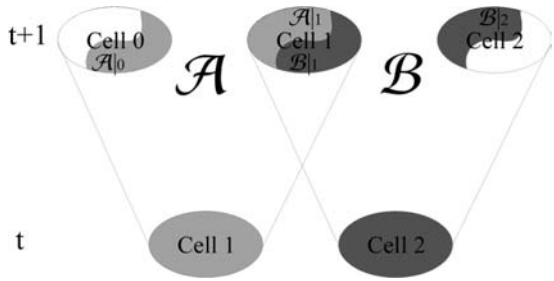

FIGURE 2
Definitions of the algebras for the proof of the structure theorem.

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 $U\mathcal{A}|_0U^\dagger$ is of the form $M_p(\mathbb{C}) \otimes \mathbb{I}_q$ and $U\mathcal{B}|_1U^\dagger$ is of the form $\mathbb{I}_p \otimes M_q(\mathbb{C})$, with $pq = d$.*

Proof.
Note that q in the above lemma is an integer; it does not have anything to do with the quiescent symbol. $\mathcal{A}$ and $\mathcal{B}$ are indeed localized as stated due to the causality of G and a straightforward application of lemma 1 with $\mathcal{N} = \{0, 1\}$, which we can apply at position 1 and 2 by shift-invariance.
$\mathcal{A}$ and $\mathcal{B}$ commute because they are the image of two commuting algebras, those of Cell 1 and 2, via a morphism $AB \mapsto GAG^\dagger GBG^\dagger = GABG^\dagger$.
Moreover by lemma 1 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 $\mathcal{A}\mathcal{B}|_1$ is the entire cell algebra of cell 1, i.e. $M_d(\mathbb{C})$.
So now we can apply Theorem 3 and the result follows. □

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 $\mathcal{B}|_1$ the restriction of $\mathcal{B}$ to cell* 1 *and $\mathcal{B}|_2$ the restriction of $\mathcal{B}$ to cell* 2*.*
We have that $\mathcal{B} = \mathcal{B}|_1 \otimes \mathcal{B}|_2$.

Proof. We know that $\mathcal{B}$ is isometric to $M_d(\mathbb{C})$ and we know that $\mathcal{B}|_1 \otimes \mathcal{B}|_2 \subset \mathcal{B}$. But then by the previous lemma applied upon cell 1 we also know that $\mathcal{B}|_1$ is isometric to $M_q(\mathbb{C})$ and if we apply it to cell 2 then we have that $\mathcal{B}|_2$ is isometric to $M_p(\mathbb{C})$. Hence the inclusion is an equality. □

We now come to the statement of the structure theorem. The intuitive idea is that any QCA can be put in the form described in Figure 3. First, a row of U's splits the content of each cell into two subspaces, which are then reunited by a staggered row of V's, as described by Figure 4. There are two questions related to this representation which need to be discussed.

First, an infinite tensor product of unitary transformations is a priori ill-defined, and we have to explain why this one is well-defined. Given that the underlying space is the Hilbert space of configurations, this is essentially the same problem as defining a CA locally and having to justify why it does send finite configurations on finite configurations. The answer in the classical case is that its sends locally $q \cdots q$ on q. Similarly we will show that our local unitary transformations send $|q\rangle$ on $|q\rangle$.

The second issue is only an apparent one. Figure 3 looks like a composition of local unitary transformations, whereas it is well-known that in the classical case, only a CA of trivial index can be decomposed into a product of local unitaries without increasing the size of the alphabet (cf. for instance [13]). We already did some grouping and composing with shifts in order to give our QCA a minimal $\frac{1}{2}$ neighborhood, but we should need to add now partial shifts to compensate for the index. Actually, that is right, and the partial shifts are

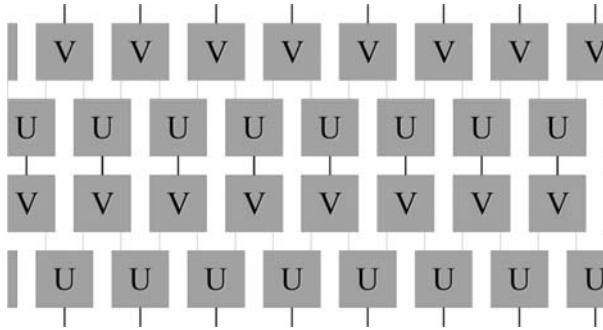

FIGURE 3
QCA with two-layered block representation (U, V). Each line represents a cell, which is a quantum system. Each square represents a unitary U/V which gets applied upon the quantum systems. Time flows upwards.

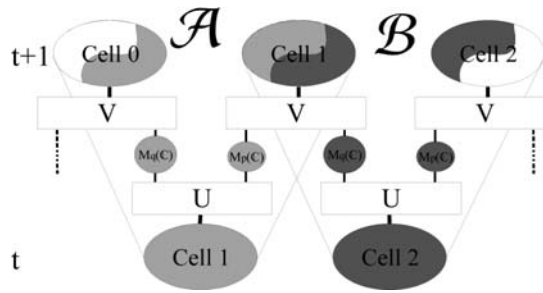

FIGURE 4
Zooming into the two-layered block representation. The unitary interactions U and V are alternated repeatedly as shown.

contained indeed in Figure 4, though not so openly. For instance, let us follow Cell 1. It is decomposed by U into a tensor product $M_q(\mathbb{C}) \otimes M_p(\mathbb{C})$, but while $M_p(\mathbb{C})$ "stays here" and will contribute to the update of Cell 1, $M_q(\mathbb{C})$ is sent to the left: therein lies the hidden partial shift.

Theorem 4 (Structure theorem).
Let G be a QCA with local cell dimension d. There exist integers p, q and unitary transformations $U : \mathbb{C}^d \to \mathbb{C}^q \otimes \mathbb{C}^p$ and $V : \mathbb{C}^q \otimes \mathbb{C}^p \to \mathbb{C}^d$ such that the G is computed by the assemblage described in Figure 3. More formally, let us denote for a matrix M and a natural integer n $M^{\otimes[-n;n]} = \cdots \otimes \mathrm{Id} \otimes M \otimes M \otimes \mathrm{Id} \otimes \cdots$ where the M's are in positions $-n, \ldots, n$, and let S be the partial shift of $(\mathbb{C}^q \otimes \mathbb{C}^p)^{\otimes \mathbb{Z}}$ sending the the first component one cell towards the left. Let $G_n = V^{\otimes[-n;n]} S U^{\otimes[-n;n]}$. Then for every $\xi \in \mathcal{H}_{C_f}$, $\lim_{n\to\infty} G_n \xi = G\xi$.

Proof.
Let $\mathcal{A}$ and $\mathcal{B}$ be respectively the images of the algebra of the cells 1 and 2 under the global evolution G. By virtue of lemma 4 we know that $\mathcal{A}$ and $\mathcal{B}$ are respectively isometric to $M_p(\mathbb{C}) \otimes \mathrm{Id}_q$ and $\mathrm{Id}_p \otimes M_q(\mathbb{C})$; let $V^\dagger$ be the unitary transformation over $\mathbb{C}^d$ which accomplishes this separation. From lemma 5, we know that $(V^\dagger \otimes V^\dagger)G$ maps the algebra of one cell into $\mathrm{Id}_p \otimes M_q(\mathbb{C}) \otimes M_p(\mathbb{C}) \otimes \mathrm{Id}_q$, so we can choose a unitary operator U over $\mathbb{C}^d$ which realizes this mapping by conjugation. By shift-invariance, the same V and U will do for every position in the line. Therefore $G = \left(\bigotimes V\right)\left(\bigotimes U\right)$ as in Fig. 4. The rest of the proof serves only to give a formal meaning to these infinite tensor products as unitary operators over $\mathcal{H}_{\mathcal{C}_f}$.

Let us consider $|q\rangle\langle q| \in M_d(\mathbb{C})$. Its image by $V^\dagger$, i.e. $V|q\rangle\langle q|V^\dagger$, is some one-dimensional projector in $M_p(\mathbb{C}) \otimes M_q(\mathbb{C})$. Now consider the state corresponding to the quiescent state on every cells. It is invariant by G, so this $V|q\rangle\langle q|V^\dagger$ has to be separable in $M_p(\mathbb{C}) \otimes M_q(\mathbb{C})$, because after applying independent U transformations on each side we get the everywhere quiescent state, which is unentangled. This means that $V|q\rangle\langle q|V^\dagger$ can be written as $|q_1\rangle\langle q_1| \otimes |q_2\rangle\langle q_2|$, where $|q_1\rangle$ and $|q_2\rangle$ are respectively unit vectors of $\mathbb{C}^p$ and $\mathbb{C}^q$. So we can assume that V maps $|q_1\rangle|q_2\rangle$ to $|q\rangle$. Moreover we know $U^\dagger\left(|q_2\rangle\langle q_2| \otimes |q_1\rangle\langle q_1|\right)U$ must be equal to $|q\rangle\langle q|$, so we can assume that U maps $|q\rangle$ to $|q_2\rangle|q_1\rangle$.

We can now give a meaning to the infinite product of unitary operators. For each n we consider the operator $\left(\bigotimes_{[-n,n]} U\right)$ where the U's are only applied on the portion $[-n, n]$ of the line. The action of $\left(\bigotimes U\right)$ is simply the limit of its images by $\left(\bigotimes_{[-n,n]} U\right)$, when n goes to infinity. That U maps $|q\rangle$ to $|q_2\rangle|q_1\rangle$ insures that this limit does exist. Indeed, for every finite configuration c, the sequence $\left(\bigotimes_{[-n,n]} U\right)|c\rangle$ will be ultimately constant, due to the quiescent boundaries. □

Note that this structure could be further simplified if we were to allow ancillary cells [1]. Therefore we have shown that one-dimensional QCA over finite, unbounded configurations admit a two-layered block representation. As we shall see n-dimensional QCA do not admit such a two-layered block representation, contrary to what was stated in [18]. Whilst the proof remains similar in spirit, it has the advantage of being remarkably simpler and self-contained, phrased in the standard setting of quantum theory, understandable without heavy prerequisites in C^*-algebras. The proof technique is rather different from that of [19], for whom G is essentially a finite-dimensional matrix and hence can necessarily be approximated by a quantum circuit.

4 CURRENT WORKS

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. This will lead us to three original propositions.

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

Definition 11 (mXOR CA).
Let $\mathcal{C}_f$ be the set of finite configurations over the alphabet $q + \Sigma = \{q, 0, 1\}$. For all x, y in $q + \Sigma$ Let $\delta(qx) = q$, $\delta(xq) = x$, and $\delta(xy) = x \oplus y$ otherwise. We call $F : \mathcal{C}_f \longrightarrow \mathcal{C}_f$ the function mapping $c = \ldots c_{i-1}c_ic_{i+1}\ldots$ to $c' = \ldots \delta(c_{i-1}c_i)\delta(c_ic_{i+1})\ldots$.

The mXOR CA is clearly shift-invariant, and causal 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 $c' = \ldots qqc'_kc'_{k+1}\ldots$ with c'_k the first non quiescent cell, we have $c_k = q$, $c_{k+1} = c'_k$, and thereon for $l \geq k+1$ we have either $c_{l+1} = c_l \oplus c'_l$ if $c'_l \neq q$, or once 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 mXOR CA is not structurally reversible. Indeed for some $c' = \ldots 000000000\ldots$ 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 $\mathcal{H}_{\mathcal{C}_f}$ by linear extension (e.g. $F(\alpha.|\ldots 01\ldots\rangle + \beta.|\ldots 11\ldots\rangle) = \alpha.F|\ldots 01\ldots\rangle + \beta.F|\ldots 11\ldots\rangle$) 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 $F : \mathcal{H}_{\mathcal{C}_f} \longrightarrow \mathcal{H}_{\mathcal{C}_f}$. It is indeed unitary as a linear extension of a bijective function, and it is shift-invariant for the same reason. Yet counter-intuitively it is non-causal. Indeed consider configurations $c_\pm = 1/\sqrt{2}.|\ldots qq\rangle(|00\ldots 00\rangle \pm |11\ldots 11\rangle)|qq\ldots\rangle$. We have $Fc_\pm = |\ldots qq00\ldots 0\rangle|\pm\rangle|qq\ldots\rangle$, where we have used the usual notation $|\pm\rangle = 1/\sqrt{2}.(|0\rangle \pm |1\rangle)$. Let i be the position of this last non quiescent cell. Clearly $(Fc_\pm)|_i = |\pm\rangle\langle\pm|$ is not just a function of $c|_{i,i+1} = (|0q\rangle\langle 0q| + |1q\rangle\langle 1q|)/2$, but instead depends upon this global $\pm$ phase. Another way to put it is that the quantized XOR may be used to transmit information faster than light. Say the first non quiescent cell is with Alice in Paris and the last non quiescent cell is with Bob in New York. Just by applying a phase gate Z upon her cell Alice can change c_+ into c_- at time t, leading to a perfectly measurable change from $|+\rangle$ to $|-\rangle$ for Bob. Again another way to say it is that operators localized upon cell 1 are not taken to operators localized

upon cells 0 and 1, as was the case for QCA. For instance take $\mathbb{I} \otimes Z \otimes \mathbb{I}$ localized upon cell 1. This is taken to $F(\mathbb{I} \otimes Z \otimes \mathbb{I})F^{\dagger}$. But this operation is not localized upon cells 0 and 1, as it takes $|\ldots qq00\ldots0\rangle|+\rangle|qq\ldots\rangle$ to $|\ldots qq00\ldots0\rangle|-\rangle|qq\ldots\rangle$, whatever the position i of the varying $|\pm\rangle$. Note that because the effect is arbitrarily remote, this cannot be reconciled with just a cell grouping. Notice also the curious asymmetry of the scenario, which communicates towards the right.

Such a behaviour is clearly not acceptable. Although it seemed like a valid QCA, F must bi discarded as non-physical. A phenomenon which seems causal classically may turn out non-causal in its quantum extension. Clearly this is due to the possibility of having entangled states, which allow for more 'non-local' states, and hence strengthens the consequences of no-signalling. This is the deep reason why QCA, even on finite configurations, do admit a block representation.

Now let us take a step back. If a CA is not structurally reversible, there is no chance that its QCA will be. Moreover according the current state of modern physics, quantum mechanics is the theory for describing all closed systems. Therefore we reach the following proposition, where the class B stands for the class of bijective but not structurally reversible CA upon finite configurations is known to coincide with the class of surjective but non injective CA upon infinite configurations, well-known to be quivalent to the class of bijective CA upon finite configurations but not upon infinite configuration.

Proposition 1 (Class B is not causally quantizable). *The quantization of a class B automata is not causal. It cannot be implemented by a series of finite quantum systems, isolated from the outside world.*

As far as CA are concerned this result removes much of the motivation of several papers which focus upon class B, since they become illegal physically in the formal sense above. As regards QCA the structure theorem also removes much of the motivation of the papers [9, 10, 15, 1], which contain unitary decision procedures for possibly non-structurally reversible QCA.

Faster quantum signalling.
Second, it is a well-known fact that there exists some $1/2$-neighbourhood, structurally reversible CA, whose inverse is also of $1/2$-neighbourhood, and yet which do not admit a two-layered block representation unless the cells are grouped into supercells. The Toffoli CA is a good example of that.

Definition 12 (Toffoli CA). *Let $\mathcal{C}_f$ be the set of finite configurations over the alphabet $\{00, 01, 10, 11\}$, with 00 now taken as the quiescent symbol. For all ab and cd taken in the alphabet let $\delta(abcd) = (b \oplus a.c)c$. We call $F : \mathcal{C}_f \longrightarrow \mathcal{C}_f$ the function mapping $c = \ldots c_{i-1}c_ic_{i+1}\ldots$ to $c' = \ldots \delta(c_{i-1}c_i)\delta(c_ic_{i+1})\ldots$. This is best described by Figure 5.*

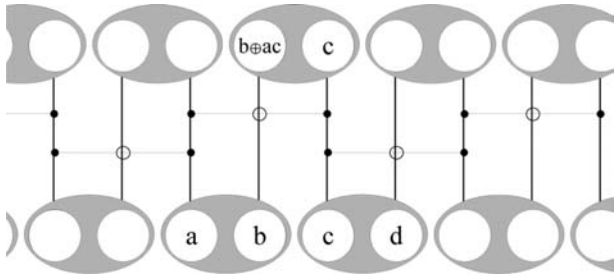

FIGURE 5
The Toffoli CA.

The Toffoli CA is clearly shift-invariant, and of $1/2$-neighbourhood. Let us check that its inverse is also of $1/2$-neighbourhood. For instance say we seek to retrieve (c,d). Retrieving c is immediate. By shift-invariance retrieving d is like retrieving b. But since we have a and c in cleartext we can easily substract $a.c$ from $b \oplus a.c$. 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 $1/2$-neighbourhood, whose inverse is also of $1/2$-neighbourhood, but do not admit a two-layered block representation without cell grouping. Yet surely, just by defining F over $\mathcal{H}_{\mathcal{C}_f}$ 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.

Again in order to lift this concern let us look at the properties of this quantized $F : \mathcal{H}_{\mathcal{C}_f} \longrightarrow \mathcal{H}_{\mathcal{C}_f}$. It is clearly unitary and shift-invariant. This time it is also causal, but counter-intuitively it turns out not to be of $1/2$-neighbourhood. Indeed from the formulation in terms of Toffoli gates as in Figure 5 one can show that the radius is $3/2$ in a quantum mechanical setting. For instance one can check that putting $|+\rangle$ in the a-subcell, $|-\rangle$ in the b-subcell, and either $|0\rangle$ or $|1\rangle$ in the c-subcell of Fig. 5 at time t will yield either $|+\rangle$ or $|-\rangle$ in the a-subcell at time $t+1$. Basically this arises because unlike in the classical case where the control bit always emerges unchanges of a Toffoli gate, when a control bit is in a superposition (like a in the example given) it may emerge from the Toffoli gate modified.

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 mXOR CA, the speed of information remains bounded in the Toffoli CA, and so up to cell grouping it can still be considered a QCA. The Toffoli CA is hence perfectly valid from a physical point of view, and causal, so long as we are willing to reinterprete what the maximal speed of information should be. Therefore we reach the following proposition.

Proposition 2 (Quantum information flows faster). *Let $F : \mathcal{C}_f \longrightarrow \mathcal{C}_f$ be a CA and $F : \mathcal{H}_{\mathcal{C}_f} \longrightarrow \mathcal{H}_{\mathcal{C}_f}$ 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. Recent works [4] have sought to provide quantified bounds on the extent in which this phenomenon can arise, answering the question: "Quantum information can sometimes flow faster than classical information, but when, and how much faster?". Interestingly, it turns out that these bounds characterize the Block neighbourhood of reversible CA, i.e. the minimal size of the blocks used for its block representation [13, 14].

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 [14]:

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, causal 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 [14]:

- 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;

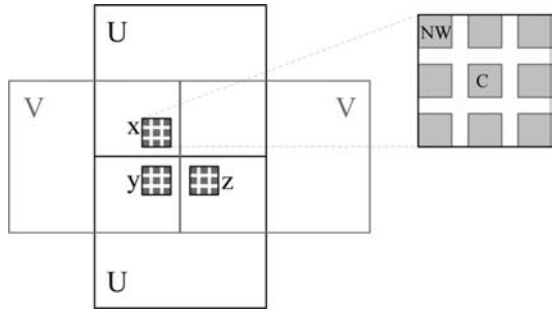

FIGURE 6
The Kari CA and the choice of x, y, z cells.

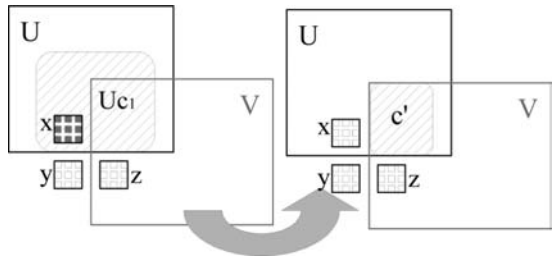

FIGURE 7
Uc_1 and c'.

- 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 z 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 ofs the center bit of the x cell;
- Hence the contradiction.

Now by defining F over $\mathcal{H}_{\mathcal{C}_f}$ 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

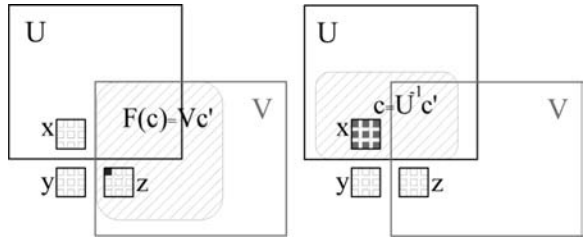

FIGURE 8
$F(c)$ and c: a contradiction.

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 [18]. 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.*

At this stage we must, however, introduce a word of caution. This entire paper has been concerned with exact block representations of a QCA G. In other words, the block representation we have contructed do not just *simulate* G, but rather it *implements exactly* G. In particular, we have not resorted to ancillary cells that may be used for storing intermediate results, nor changed the cells' dimension in order to achieve the block representation. In the field of reversible CA, this subtelty is known to make a big difference: with ancilla a number of block representations of n-dimensional RCA have been contructed [14, 8]; without ancilla this remains an open problem for $n > 2$ [13]. Hence, what can be said of block representations of QCA with ancillas? A recent result [5] provides a 2^n-layered construction, whereas another paper [3] reduces the number of layers down to 2.

Open problem.
The question that remains open to this day, is precisely that of exact block representations of n-dimensional QCA — just like in the classical case. Proposition 3 already tells us that the techniques of this paper cannot be directly exported, since the exact block representations is not going to be two-layered. Nevertheless, it could well be that the original linear-algebraic methods that have been developped in this line of research can help resolve this case, together with its classical counterpart.

ACKNOWLEDGEMENTS

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

REFERENCES

[1] P. Arrighi. (2006). Algebraic characterizations of unitary linear quantum cellular automata. In *Proceedings of MFCS, Lecture Notes in Computer Science*, volume 4162, page 122. Springer.

[2] P. Arrighi, R. Fargetton, and Z. Wang. (2009). Intrinsically universal one-dimensional quantum cellular automata in two flavours. *Fundamenta Informaticae*, 21:1001–1035.

[3] P. Arrighi and J. Grattage. (2009). Partitioned quantum cellular automata are intrinsically universal. Accepted for publication, Post-proceedings of the Physics and Computation workshop.

[4] P. Arrighi and V. Nesme. (2010). The Block Neighbourhood. In *Second Symposium on Cellular Automata "Journées Automates Cellulaires" (JAC 2010), Turku, December 2010, to be published in proceedings.*

[5] P. Arrighi, V. Nesme, and R. Werner. (2010). Unitarity plus causality implies localizability. *QIP 2010 and Journal of Computer and System Sciences, ArXiv preprint: arXiv:0711.3975*.

[6] P. Arrighi, V. Nesme, and R. F. Werner. (2008). Quantum cellular automata over finite, unbounded configurations. In *Proceedings of MFCS, Lecture Notes in Computer Science*, volume 5196, pages 64–75. Springer.

[7] 0. Bratteli and D. Robinson. (1987). *Operators algebras and quantum statistical mechanics 1*. Springer.

[8] J. 0. Durand-Lose. (2001). Representing reversible cellular automata with reversible block cellular automata. *Discrete Mathematics and Theoretical Computer Science*, 145:154.

[9] C. Durr, H. Le Thanh, and M. Santha. (1996). A decision procedure for well-formed linear quantum cellular automata. In *Proceedings of STACS 96, Lecture Notes in Computer Science*, pages 281–292. Springer.

[10] C. Durr and M. Santha. (1996). A decision procedure for unitary linear quantum cellular automata. In *Proceedings of the 37th IEEE Symposium on Foundations of Computer Science*, pages 38–45. IEEE.

[11] R. P. Feynman. (1986). Quantum mechanical computers. *Foundations of Physics (Historical Archive)*, 16(6):507–531.

[12] D. Gijswijt. (1977). Matrix algebras and semidefinite programming techniques for codes. Ph.d. thesis, University of Amsterdam.

[13] J. Kari. (1996). Representation of reversible cellular automata with block permutations. *Theory of Computing Systems*, 29(1):47–61.

[14] J. Kari. (1999). On the circuit depth of structurally reversible cellular automata. *Fundamenta Informaticae*, 38(1-2):93–107.

[15] D. Meyer, (1995). Unitarity in one dimensional nonlinear quantum cellular automata. ArXiv pre-print quant-ph/9605023.

[16] D. A. Meyer. (1996). From quantum cellular automata to quantum lattice gases. *J. Stat. Phys*, 85:551–574.

[17] C.A. Pérez-Delgado and D. Cheung. (2007). Local unreversible cellular automaton ableitary quantum cellular automata. *Physical Review A*, 76(3):32320.

[18] B. Schumacher and R. Werner, (2004). Reversible quantum cellular automata. ArXiv pre-print quant-ph/0405174.

[19] W. Van Dam. (1996). Quantum cellular automata. Masters thesis, University of Nijmegen, The Netherlands.

[20] J. Watrous. (1991). On one-dimensional quantum cellular automata. *Complex Systems*, 5(1):19—30.