HAL open science

Quantization of cellular automata

Pablo Arrighi, Vincent Nesme

To cite this version:

Pablo Arrighi, Vincent Nesme. Quantization of cellular automata. JAC 2008, Apr 2008, Uzès, France. pp.204-215. hal-00274002

HAL Id: hal-00274002

https://hal.science/hal-00274002v1

Submitted on 17 Apr 2008

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Journées Automates Cellulaires 2008 (Uzès), pp. 204-215

QUANTIZATION OF CELLULAR AUTOMATA

PABLO ARRIGHI [1] AND VINCENT NESME [2]

[1] Université de Grenoble
LIG, 46 Avenue Félix Viallet
38031 Grenoble Cedex FRANCE
E-mail address: pablo.arrighi@imag.fr

[2] Technische Universität Braunschweig
IMaPh, Mendelssohnstraße 3
38106 Braunschweig DEUTSCHLAND
E-mail address: vincent.nesme@tu-bs.de

Abstract. Take a cellular automaton, consider that each configuration is a basis vector in some vector space, and linearize the global evolution function. If lucky, the result could actually make sense physically, as a valid quantum evolution; but does it make sense as a quantum cellular automaton? That is the main question we address in this paper. In every model with discrete time and space, two things are required in order to qualify as a cellular automaton: invariance by translation and locality. We prove that this locality condition is so restrictive in the quantum case that every quantum cellular automaton constructed in this way — i.e., by linearization of a classical one — must be reversible. We also discuss some subtleties about the extent of nonlocality that can be encountered in the one-dimensional case; we show that, even when the quantized version is non local, still, under some conditions, we may be unable to use this nonlocality to transmit information nonlocally.

Introduction

After some tries [9, 4, 5, 1] at defining and studying quantum cellular automata, it is now believed to be fairly well understood how reversible quantum cellular automata (RQCA) should be defined, and what their basic properties are. As with classical cellular automata (CA), there are two levels on which RQCA are defined: as local transition functions or as global evolutions. The definition of RQCA proposed in [8] focuses only on the properties of the global evolution, based on the two essential points of invariance by translation and locality. It was also proved in the same paper that each reversible cellular automaton could be "quantized" in a natural way, and the result would be a RQCA. Furthermore, it was proved that RQCA can be implemented with local means, thereby reinforcing the parallel with CA; this was first done in the one-dimensional case [8, 2], the result being later

2000 ACM Subject Classification: F.1.1.

Key words and phrases: cellular automata, quantum cellular automata, open cellular automata, quantization, locality, localization.

creative commons

extended to the general case [3]. Also, they involve no measurement procedure; the global evolution of a RQCA can be described by a unitary operator, while its decomposition as layers of local operations consists only of small unitary transformations.

We would like now to extend this framework to include cases where the global evolution is no longer described by a unitary operator, but by an isometry. This would be the first step in the investigation of nonreversible quantum cellular automata (NRQCA). The main problem with this topic, nowadays, is that there is no practical definition for such things. Our aim is to provide such a definition and work out the basic properties of NRQCA. Invariance by translation and locality as defined in [2] are still properties that NRQCA should obviously have. In this paper we will ask and answer this question: when does the quantization of a CA have these properties? Since the translational invariance comes freely, the real question is: when is the quantization local?

Section 1 will be devoted to the mandatory definitions. We will be quick as we assume the reader is familiar with the basics of CA and somewhat familiar with quantum computing. We then show with theorem 2.1 that the locality — more precisely, the *uniform* locality, cf. definition 1.7 — of the quantization is equivalent to reversibility, therefore extending the results presented in [8, 2], and proving that no NRQCA can be constructed in this way. In Section 3, we discuss the one-dimensional case. We show that, in some cases, even if the quantization is not uniformly local, it can still be local in a weaker sense which forbids some kinds of long-distance communications.

1. Definitions

We will now introduce the basic definitions of quantum cellular automata. For technical reasons, we will work mainly with finite configurations. This is because they are countable, as opposed to infinite configurations, and we want to have vector spaces of countable dimension, so as to simplify the formalism of [8]. This distinction between finite and infinite configurations is not so important, as was shown in [2]; anyway, we are only interested in locality conditions for quantizations of CA. We do not restrict the dimension of the space, which will be some positive integer d. We denote q the quiescent state, and Σ the rest of the alphabet, assuming $q \notin \Sigma$; the union of Σ and $\{q\}$ is denoted $q\Sigma$. The sets of finite configurations is denoted $\mathcal{C}_f$; it contains the elements of $(q\Sigma)^{\mathbb{Z}^d}$ that are equal to q almost everywhere on $\mathbb{Z}^d$.

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 $\mathcal{C}_f$ is a countably infinite set.

Definition 1.1 (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 $\mathcal{H}_{\mathcal{C}_f}$.

We used here Dirac notation. Likewise, $\langle c|$ denotes the dual of $|c\rangle$, i.e. the linear form on $\mathcal{H}_{\mathcal{C}_f}$ such that for all $d \in \mathcal{C}_f$, $\langle c| (|d\rangle)$, which is noted $\langle c|d\rangle$, is equal to δ_{cd}. These notations may then be combined the other way around, $|c\rangle\langle c'|$ being the linear transformation of $\mathcal{H}_{\mathcal{C}_f}$ such that $|c\rangle\langle c'||d\rangle$ is, quite naturally, equal to $\langle c'|d\rangle|c\rangle$.

States on $\mathcal{H}_{\mathcal{C}_f}$ are nonnegative hermitian operators of trace 1. For instance, for each superposition of configurations $|\psi\rangle$, $|\psi\rangle\langle\psi|$ is a state, called in this case a *pure* state. Physically, states describe the actual state of matter; they bear all the information that can be measured in the system. The cells of our CA are in the pure state $|\psi\rangle\langle\psi|$ when what lies on them is, with certainty, the superposition $|\psi\rangle$. Actually, each state can be approximated by convex combinations of pure states. It means that the actual physical state of our CA at some moment can be described as a (possibly infinite) sum $\sum_i p_i|\psi_i\rangle\langle\psi_i|$, where the p_i's are positive, $\sum_i p_i = 1$ and the $|\psi_i\rangle$'s are pairwise orthogonal.

We will be manipulating isometries a lot. Unitary operators should be well-known, but isometries are probably somewhat less familiar, so let us write down their definition. A linear operator $G : \mathcal{H}_{\mathcal{C}_f} \longrightarrow \mathcal{H}_{\mathcal{C}_f}$ is *isometric* if and only if $\{G|c\rangle \mid c \in \mathcal{C}_f\}$ is an orthonormal family of $\mathcal{H}_{\mathcal{C}_f}$. This can also be expressed simply using the adjoint $G^\dagger$ of G. By definition, when G is a endomorphism of $\mathcal{H}_{\mathcal{C}_f}$, $G^\dagger$ is the endomorphism of $\mathcal{H}_{\mathcal{C}_f}$ such that for every $|\varphi\rangle, |\psi\rangle \in \mathcal{H}_{\mathcal{C}_f}$, $\langle\varphi|G|\psi\rangle = \langle\psi|G^\dagger|\varphi\rangle$. This way, $G^\dagger$ is indeed always unique; however, it is defined if and only if G is continuous. When G is isometric, G is of course continuous, and actually, G is isometric iff $G^\dagger G = \mathrm{Id}_{\mathcal{C}_f}$. If, moreover, G is onto, it is said to be *unitary*; so G is unitary if and only if $G^\dagger G = GG^\dagger = \mathrm{Id}_{\mathcal{C}_f}$.

Now, we are talking about CA, whose one important feature is shift-invariance. The definition of shift-invariance in a quantum context, with all these linearizations, is actually no more tedious than in the classical case; here it is.

Definition 1.2 (Shift-invariance)**.**
Consider the shift operation which takes configuration $\ldots c_{i-1}c_ic_{i+1}\ldots$ to $\ldots c'_{i-1}c'_ic'_{i+1}\ldots$ 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. 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 $G\sigma = \sigma G$.

The second important feature of CA is their locality. In the classical case, we know that the locality is equivalent to the continuity of the global evolution on infinite configurations. Unfortunately, there does not seem to be such a result in the quantum case; at least it is not obvious what the right topology on superpositions of configurations should be. Therefore, the definition of locality proposed in [8] is more concrete. It explicitly states that to know the state of some region of the space after an iteration of the CA, you only need to know the state of a slightly larger region beforehand. In the classical case, you would trivially deduce from this property that the global evolution stems from a local transition rule. In the quantum case however, things are not so simple as entanglement suddenly comes into play, and when G is unitary it turns out [8, 2, 3] you need to keep things locally reversible.

To give the actual definition of locality, we first need to introduce some vocabulary. First, we will make abundant use throughout this paper of the Minkowski sum. For two subsets $\mathcal{A}$ and $\mathcal{B}$ of $\mathbb{Z}^d$, the Minkowski sum of $\mathcal{A}$ and $\mathcal{B}$, noted $\mathcal{A} + \mathcal{B}$, is the set $\{a + b/a \in \mathcal{A}, b \in \mathcal{B}\}$. $\mathcal{A} - \mathcal{B}$ is naturally the Minkowski difference, $\{a - b/a \in \mathcal{A}, b \in \mathcal{B}\}$.

$\mathcal{H}_{\mathcal{C}_f}$ has a natural structure of tensor product. Namely, for a subset $\mathcal{A}$ of $\mathbb{Z}^d$, let us note $\mathcal{C}_f(\mathcal{A})$ the set of the finite words on $\mathcal{A}$. Then $\mathcal{H}_{\mathcal{C}_f}$ is naturally isomorphic to $\mathcal{H}_{\mathcal{C}_f(\mathcal{A})} \otimes \mathcal{H}_{\mathcal{C}_f(\overline{\mathcal{A}})}$, where $\overline{\mathcal{A}}$ denotes the complementary of $\mathcal{A}$ in $\mathbb{Z}^d$ and $\mathcal{H}_{\mathcal{C}_f(\mathcal{A})}$ is the Hilbert space whose canonical basis is indexed by the elements of $\mathcal{C}_f(\mathcal{A})$. That being said, there are two more definitions we need before moving on. The first one should be familiar, it is also known as "trace out" and occurs whenever a quantum system can be divided into two subsystems. Informally, if a system S can be written as the tensor product of two

subsystems A and B, and given a state ρ on S, you can chose to ignore completely what is going on B and restrict your universe to A. The state you get on A is then the restriction of ρ to A.

Definition 1.3 (Reduction)**.** Let ρ be a state over $\mathcal{H}_{\mathcal{C}_f}$ and $\mathcal{A}$ a subset of $\mathbb{Z}^d$. One can write $\rho = \sum_i \sigma_i \otimes \tau_i$, where the σ_i's and τ_i's are respectively operators over $\mathcal{H}_{\mathcal{C}_f(\mathcal{A})}$ and $\mathcal{H}_{\mathcal{C}_f(\overline{\mathcal{A}})}$. Then $\rho|_{\mathcal{A}}$, the *reduction* of ρ to $\mathcal{A}$, is a state on $\mathcal{H}_{\mathcal{C}_f(\mathcal{A})}$ defined as $\sum_i \mathrm{Tr}\,(\tau_i)\,\sigma_i$; this does not depend on the way ρ was decomposed in the first place. ∎

The following definition is the dual of the last one. Why it is its dual will appear in proposition 1.6.

Definition 1.4 (Localization)**.** A linear endomorphism of $\mathcal{H}_{\mathcal{C}_f}$ is *localized* in a subset $\mathcal{A}$ of $\mathbb{Z}^d$ if it is of the form $A \otimes \mathrm{Id}$, where A is an endomorphism of $\mathcal{H}_{\mathcal{C}_f(\mathcal{A})}$ and Id is the identity on $\mathcal{H}_{\mathcal{C}_f(\overline{\mathcal{A}})}$.

We can now explain the duality going on here with this lemma, which is stated and proved as lemma 3 in [2].

Lemma 1.5 (Duality)**.**
Let $\mathcal{H}_0$ and $\mathcal{H}_1$ be Hilbert spaces, with $\mathcal{H}_0$ of finite dimension p. Let A, ρ, ρ' denote some elements of $\mathcal{L}(\mathcal{H}_0 \otimes \mathcal{H}_1)$ with ρ, ρ' having reductions $\rho|_0, \rho'|_0$ over $\mathcal{H}_0$. We then have that A is localized in $\mathcal{H}_0$ iff

"for every states ρ and ρ', if $\rho|_0 = \rho'|_0$ then $Tr(A\rho) = Tr(A\rho')$".

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

"if A is localized in $\mathcal{H}_0$, then $Tr(A\rho) = Tr(A\rho')$". ∎

The proposition 1.6 we introduce next comes from theorem 3 in [2]. It entails structural reversibility, i.e. the fact that the inverse function of a RQCA is also a RQCA. Since we want now to talk about nonunitary operators, we have to restate it for general linear operators. We also have to extend the domain of localization of this operator from one cell to a set of cells. It will also serve as a definition of locality for linear endomorphisms over $\mathcal{H}_{\mathcal{C}_f}$ — which is not to be confused with localization. Note that the hypothesis of continuity for G provides the existence of its adjoint $G^\dagger$.

It defines the locality "at somewhere" in the space. Intuitively, a global transition is said to be local at some locus if the physical state in this locus after the transition depends only on the physical state on a neighbourhood of this locus beforehand (this is point (i) of the proposition). Equivalently, one could say that the result of each measure done on this locus after the transition could be predicted beforehand by measures performed on its neighbourhood (that would be point (ii)).

Proposition 1.6 (Structural reversibility)**.**
Let G be a continuous linear endomorphism of $\mathcal{H}_{C_f}$, $\mathcal{A}$ and $\mathcal{N}$ respectively a subset and a finite subset of $\mathbb{Z}^d$. Suppose $G^\dagger$ The two properties are equivalent:

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

(ii) *For every operator A localized in $\mathcal{A}$, $G^\dagger A G$ is localized in $\mathcal{A} + \mathcal{N}$.*

When G satisfies these properties, we say that G is local at $\mathcal{A}$ with neighbourhood $\mathcal{N}$. If only $\mathcal{A}$ is given, we say that G is local at $\mathcal{A}$ if there exists a finite subset $\mathcal{N}$ of $\mathbb{Z}^d$ such that G is local at $\mathcal{A}$ with neighbourhood $\mathcal{N}$.

If G is unitary, the following items are equivalent to (i) and (ii).

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

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

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 1.5 and our hypothesis that $\left(G\rho G^\dagger\right)|_{\mathcal{A}} = \left(G\rho' G^\dagger\right)|_{\mathcal{A}}$. 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 $\rho|_{\mathcal{A}+\mathcal{N}} = \rho'|_{\mathcal{A}+\mathcal{N}}$, this means, again according to lemma 1.5, that $G^\dagger AG$ is localized on the cells in $\mathcal{A}+\mathcal{N}$.
$[(ii) \Rightarrow (i)]$. Suppose (ii) and $\rho|_{\mathcal{A}+\mathcal{N}} = \rho'|_{\mathcal{A}+\mathcal{N}}$. Then, for every operator B localized on the cells in $\mathcal{N}$, lemma 1.5 gives $\mathrm{Tr}\,(B\rho) = \mathrm{Tr}\,(B\rho')$, so for every operator A localized on cell 0, we get:

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

Again by lemma 1.5, this means $\left(G\rho G^\dagger\right)|_0 = \left(G\rho' G^\dagger\right)|_0$.
Let us now assume G is unitary.
$[(ii) \Rightarrow (iv)]$. 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 $G^\dagger$. ∎

We can now say that again in a mathematically rigorous way: a RQCA is a unitary operator on $\mathcal{H}_{\mathcal{C}_f}$ that is shift-invariant and local at the central cell. Indeed, in this case, the assumption of locality at the central cell implies the locality at each finite subset $\mathcal{A}$ of $\mathbb{Z}^d$. Moreover, this locality is uniform, in the sense that a same neihbourghood $\mathcal{N}$ can be chosen for all $\mathcal{A}$'s. However, if we remove this hypothesis of unitarity, things are not so simple and we have to make stronger hypotheses; hence the following definitions.

Definition 1.7 (Locality)**.** A continuous linear endomorphism G of $\mathcal{H}_{\mathcal{C}_f}$ is *everywhere local* if, for every finite subset $\mathcal{A}$ of $\mathbb{Z}^d$, G is local at $\mathcal{A}$. It is *uniformly local* if there exists a finite subset $\mathcal{N}$ of $\mathbb{Z}^d$ such that for every finite subset $\mathcal{A}$ of $\mathbb{Z}^d$, G is local at $\mathcal{A}$ with neighbourhood $\mathcal{N}$.

2. Linearization of Classical Automata

Let $F : \mathcal{C}_f \to \mathcal{C}_f$ be a cellular automaton on finite configurations, $\widetilde{F} : \mathcal{H}_{\mathcal{C}_f} \to \mathcal{H}_{\mathcal{C}_f}$ its linearization. For it to have a physical meaning and earn its name of "quantization", it should be an isometry, i.e. F should be one-to-one. We will nevertheless make a seemingly weaker assumption; we only assume $\widetilde{F}^\dagger$ to be defined, in order to be able to apply definition 1.7 and ask when $\widetilde{F}$ is local; it turns out that this condition actually implies the injectivity of F.

In order for $\widetilde{F}^\dagger$ to be defined, we have to assume that $\widetilde{F}$ is continuous. Beware that this notion of continuity has nothing to do with any kind of topology on the set of words, and is therefore not related to the continuity of F, which is true by definition of a CA. For $\widetilde{F}$ to be continuous means that it is bounded on the unit sphere of $\mathcal{H}_{\mathcal{C}_f}$. This is equivalent to saying that F is one-to-one. To verify this, let us first assume F is one-to-one. Then $\widetilde{F}^\dagger$ is isometric, and consequently continuous. Let us now assume F is not one-to-one. Since F is defined on the finite configurations, for every n, there exists $x_n \in \mathcal{C}_f$ such that x_n has a number of antecedents μ_n greater than n — just repeat as many times as needed some finite configuration having several antecedents. But then $\frac{1}{\sqrt{\mu_n}} \sum_{y \in \mathcal{C}_f / F(y) = x_n} |y\rangle$ is a unit vector whose image by $\widetilde{F}$, $\sqrt{\mu_n}|x_n\rangle$, has norm $\sqrt{\mu_n}$; hence, $\widetilde{F}$ is not bounded on the unit sphere, i.e. not continuous. To close this chapter on $\widetilde{F}^\dagger$, note that when it exists, it is defined as such:

$$\widetilde{F}^\dagger |a\rangle = \sum_{u \in \mathcal{C}_f / F(u) = a} |u\rangle.$$

We therefore assume from now on that F is one-to-one. So, if you are given a word w in the image of F, there is a unique $u \in \mathcal{C}_f$ such that $F(u) = w$. In general though, u can not be computed locally from w. If it were possible to do that, the cellular automaton would be, by definition, reversible, and thus, according to [8], its linearization would be a *bona fide* reversible quantum cellular automaton.

We will be monitoring XOR as an example, for which we will allow the quiescent state q to be renamed 0, the only letter in Σ being 1. XOR acts exactly as the usual XOR: it sums modulo 2 the bits in its neighbourhood $\{0; 1\}$. Of course, XOR is not reversible, since $11\ldots1$ and $00\ldots0$ are sent locally on the same word. It is one-to-one on finite configurations, though, while not surjective. It was already stated in proposition 1 of [2] that the quantization of nonreversible automata that are bijective on finite configurations could not be local, but that left the case of such automata as XOR unsettled. The following theorem does the job.

Theorem 2.1. *Suppose F is one-to-one. Then $\widetilde{F}$ is uniformly local if and only if F is reversible.*

Proof. Let us first briefly justify that when F is reversible, $\widetilde{F}$ is uniformly local. This is essentially what states the lemma 4 of [8], though in this case it is the automaton as defined on infinite configurations that is quantized. It is quite straightforward to adapt the statement and the proof of this lemma to our formalism, to get the same result: if F admits a neighbourhood $\mathcal{N}_C$ and an inverse neighbourhood $\mathcal{N}_I$, then $\mathcal{N}_C - \mathcal{N}_C + \mathcal{N}_I$ is a neighbourhood $\overline{\mathcal{N}}$; this is actually a direct consequence of lemma 3.2. However, there is a much simpler proof that such a neighbourhood exists. First, decompose your automaton

into block permutations, with auxiliary bits if needed. Linearize then each of these block permutations. The composition of all these local unitary transformations is then $\widetilde{F} \otimes \mathrm{Id}$, where Id is the identity on the auxiliary qubits, and the block decomposition from which it is constructed is a witness that $\widetilde{F}$ is uniformly local.

We now prove the other implication, in a way that can be seen as a generalization of the argument presented page 7 of [2]. It proceeds by contraposition, so let us first of all assume F is not reversible. We will prove that for every set $\mathcal{N}$ there exists a set $\mathcal{A}$ such that $\widetilde{F}$ cannot satisfy the condition (i) of proposition 1.6; this will mean that $\widetilde{F}$ is not uniformly local.

Let $\mathcal{N}$ be a finite subset of $\mathbb{Z}^d$. Since F is not reversible, there exists a finite subset $\mathcal{B}$ of $\mathbb{Z}^d$ such that $F(x)|_{\mathcal{B}-\mathcal{N}} = F(y)|_{\mathcal{B}-\mathcal{N}}$ but $x|_{\mathcal{B}} \neq y|_{\mathcal{B}}$. Let $\mathcal{A} = \left\{s \in \mathbb{Z}^d / F(x)|_s \neq F(y)|_s\right\}$; since $F(x)$ and $F(y)$ both are finite configurations, $\mathcal{A}$ is finite.

Let $|\varphi_\pm\rangle$ denote the superpositions of configurations $\frac{|x\rangle \pm |y\rangle}{\sqrt{2}}$, and let $\rho_\pm$ be the pure states $|\varphi_\pm\rangle\langle\varphi_\pm|$. We are now going to prove that $\rho_+|_{\mathcal{A}+\mathcal{N}} = \rho_-|_{\mathcal{A}+\mathcal{N}}$, while $\left(\widetilde{F}\rho_+\widetilde{F}^\dagger\right)\Big|_{\mathcal{A}} \neq \left(\widetilde{F}\rho_-\widetilde{F}^\dagger\right)\Big|_{\mathcal{A}}$.

Since $F(x)$ and $F(y)$ are equal on $\mathcal{B}-\mathcal{N}$, $\mathcal{A}+\mathcal{N}$ does not intersect $\mathcal{B}$, so x and y differ on some point on the complement of $\mathcal{A}+\mathcal{N}$. Considering the partition of $\mathbb{Z}^d$ into $\mathcal{A}+\mathcal{N}$ and $\overline{\mathcal{A}+\mathcal{N}}$, we can thus write $|x\rangle = |x_1\rangle \otimes |x_2\rangle$ and $|y\rangle = |y_1\rangle \otimes |y_2\rangle$, where $x_1, y_1 \in \mathcal{C}_f\left(\mathcal{A}+\mathcal{N}\right)$, $x_2, y_2 \in \mathcal{C}_f\left(\overline{\mathcal{A}+\mathcal{N}}\right)$, and $x_2 \neq y_2$. We then have

$$\begin{aligned}
\rho_\pm|_{\mathcal{A}+\mathcal{N}} &= \frac{1}{2}\left(|x\rangle\langle x| \pm |x\rangle\langle y| \pm |y\rangle\langle x| + |y\rangle\langle y|\right)|_{\mathcal{A}+\mathcal{N}} \\
&= \frac{1}{2}\left(\begin{array}{c} |x_1\rangle\langle x_1| \otimes |x_2\rangle\langle x_2| \pm |x_1\rangle\langle y_1| \otimes |x_2\rangle\langle y_2| \\ \pm|y_1\rangle\langle x_1| \otimes |y_2\rangle\langle x_2| + |y_1\rangle\langle y_1| \otimes |y_2\rangle\langle y_2| \end{array}\right)\Bigg|_{\mathcal{A}+\mathcal{N}} \\
\rho_\pm|_{\mathcal{A}+\mathcal{N}} &= \frac{1}{2}\left(|x_1\rangle\langle x_1| + |y_1\rangle\langle y_1|\right).
\end{aligned}$$

Thus, the reductions of ρ_+ and ρ_- and $\mathcal{A}+\mathcal{N}$ are indeed equal. Now, $\widetilde{F}\rho_\pm\widetilde{F}^\dagger = |\psi_\pm\rangle\langle\psi_\pm|$, where $|\psi_\pm\rangle = \frac{|F(x)\rangle \pm |F(y)\rangle}{\sqrt{2}}$. Since $F(x)$ and $F(y)$ coincide on $\overline{\mathcal{A}}$, we actually have $\widetilde{F}\rho_\pm\widetilde{F}^\dagger = \sigma_1 \otimes \sigma_\pm$, where σ_1 is a (pure) state over $\mathcal{H}_{\mathcal{C}_f(\overline{\mathcal{A}})}$, and the $\sigma_\pm$'s are states over $\mathcal{H}_{\mathcal{C}_f(\mathcal{A})}$. The reductions of $\widetilde{F}\rho_\pm\widetilde{F}^\dagger$ to $\mathcal{A}$ are then $\sigma_\pm$, which are distinct states since ρ_+ and ρ_- where distinct to begin with. ∎

Another way to present this proof is to appeal to the perennial Alice and Bob. We start with the state ρ_+. Alice and Bob have access to some cells of $\mathbb{Z}^d$, meaning that they can conjugate the state on $\mathcal{H}_{\mathcal{C}_f}$ with unitary operators, as long as these unitary operators are localized in the region of the space they were assigned. So let Alice and Bob's regions be respectively $\mathcal{A}$ and $\mathcal{B}$ as encountered in the proof of theorem 2.1. We will see how they can communicate through the use of $\widetilde{F}$, even though their regions could be at quite a large distance from each other, depending on $\mathcal{N}$.

Since $x|_{\mathcal{B}} \neq y|_{\mathcal{B}}$, Bob is able to transform at will ρ_+ into ρ_-, by performing a *controlled phase-shift* on some cell where x and y differ. What that means informally is that, since Bob is able to tell the difference between x and y in his area, he can introduce a dissimetry between $|x\rangle$ and $|y\rangle$. Of course he could simply transform $|y\rangle$ by changing the letters of y is

some cells or something like that, but that would not allow him to communicate any faster than in the classical case. So what Bob does is to change $|y\rangle$ into $-|y\rangle$, something more immaterial, purely quantum and, in a way "delocalized", that will allow Alice to catch his message, which is one bit of information : "did I or didn't I change ρ_+ into ρ_-?". After Bob did his thing, $\widetilde{F}$ is applied to the state.

Now, Alice being able to actually read the message is due to the fact that her region contains all the cells where $F(x)$ and $F(y)$. As explained in the proof of theorem 2.1, the state after $\widetilde{F}$ has been applied is a tensor product of a state on $\mathcal{A}$ and a state on $\overline{\mathcal{A}}$, the state on $\overline{\mathcal{A}}$ not depending on the prior actions of Bob; therefore, the state on $\mathcal{A}$ does depend on them, so Alice must have a way to distinguish between them — in this case she just has to perform a so-called *swap-test*. Let us see for instance what happens with XOR. Consider these two words in $\mathcal{C}_f$:

$$\begin{aligned} x &= \ldots 0000000000000000\ldots \\ y &= \ldots 0011111111111100\ldots \end{aligned}$$

Their images are

$$\begin{aligned} F(x) &= \ldots 0000000000000000\ldots \\ F(y) &= \ldots 0100000000000100\ldots \end{aligned}$$

Now put Bob on the middle of the stripe, and Alice at the two cells where the 1's are in $F(y)$. By following the protocol described in the proof of theorem 2.1, Bob can indeed send a bit of information to Alice. There is no doubt that this is a correct proof that $\widetilde{\mathrm{XOR}}$ is not uniformly local, but one might argue that this idea of an "Alice" surrounding Bob makes little sense: surely if Alice can be present at two faraway places in the stripe at the same time, it means he must have some way to go from one place to the other, and since in the middle stands Bob, why would she bother using $\widetilde{\mathrm{XOR}}$ to send her message? Cannot we find another protocol where Alice stands either on the left or on the right of Bob, but on only one side at a time? Actually, no, we cannot, and this is related to the fact that $\widetilde{\mathrm{XOR}}$, while not uniformly local, is still everywhere local: if Bob is forbidden the access to the cells located between Alice's positions, then he cannot transmit her any message. The proof of this assertion is the object of the next section.

3. Everywhere Locality in the One-dimensional Case

The question is: when is the quantization of a one-to-one CA everywhere local? We are going now to give a proof that in the one-dimensional case, it is equivalent to the openness of F_∞, the extension of F to the set $\mathcal{C}_\infty$ of infinite configurations; so let us fix the dimension d to 1 for this section.

First, it might be useful to remind what it means for F_∞ to be open. $\mathcal{C}_\infty$ comes with the usual topology; namely, a base of open sets is given by the sets $\{v \in \mathcal{C}_\infty / v_{\mathcal{A}} = w_{\mathcal{A}}\}$, for $w \in \mathcal{C}_\infty$ and $\mathcal{A}$ a finite subset of Z^d. By definition, F_∞ is *open* if for every open subset O of $\mathcal{C}_\infty$, $F_\infty(O)$ is open.

Proposition 3.1. *$\widetilde{F}$ is everywhere local if and only if F_∞ is open.*

Proof. We will appeal to [7]. According to its theorem 5.45, F_∞ is open iff it is left and right-closing. The definitions of left and right-closingness may be found in definition 5.38. First, x and y in $\mathcal{C}_\infty$ are said to be *left-asymptotic* (respectively *right-asymptotic*) when

there is some $n \in \mathbb{Z}$ such that for every $k < n$ (resp. $k > n$), $x_k = y_k$. By definition, F_∞ is left-closing (respectively right-closing) if, for every $x, y \in \mathcal{C}_\infty$ that are left-asymptotic (resp. right-asymptotic), if $F(x) = F(y)$ then $x = y$. We now translate these conditions on de Bruijn diagrams.

Let us recall briefly what we mean by Bruijn diagrams. Let n be an integer such that $[-n; n+1]$ is a neighbourhood for F. We note F_0 the function from $(q\Sigma)^{[-n;n+1]}$ to $q\Sigma$ which computes locally F on cell 0, from the knowledge of the stripe on $[-n; n+1]$. Then the associated de Bruijn diagram is a graph whose vertices are indexed by the pairs $(u, v) \in q\Sigma^{[-n;n]} \times q\Sigma^{[-n;n]}$. There is an edge from (u, v) to (u', v') if and only if

- for $i \in [-n; n[$, $u_{i+1} = u'_i$ and $v_{i+1} = v'_i$
- $F_0(u_{-n}u_{-n+1} \dots u_n u'_n) = F_0(v_{-n}v_{-n+1} \dots v_n v'_n)$.

The first thing we want to note is that the strongly connected component (SCC) of (q, q) in the de Bruijn diagram includes the diagonal Δ of $q\Sigma^{[-n;n]} \times q\Sigma^{[-n;n]}$, i.e. the elements of the form (u, u).

To each pair of words $(u, v) \in \mathcal{C}_\infty \times \mathcal{C}_\infty$ such that $F(u) = F(v)$ is associated a bi-infinite path on the de Bruijn diagram, and vice-versa. In this respect, we see that "F_∞ is left-closing" is equivalent to "every infinite path starting from Δ stays forever in Δ", while "F_∞ is left-closing" is the dual statement that "every bi-infinite path ending in Δ is completely included in Δ". Thus, F_∞ is open iff there is no connection, in or out, between Δ and any cycle of the de Brujin diagram not included in Δ.

Now, what does it mean on this diagram for $\widetilde{F}$ to be everywhere local? If we follow the proof of theorem 2.1, we see this means that there exists an integer k such that for every integer n, if $F(x)$ is known on $\overline{[-n; n]}$, then $x \in \mathcal{C}_f$ is determined on $\overline{[-n-k; n+k]}$. On the de Bruijn diagram, it means that there exists an integer k such that any path starting from (q, q) must stay in X until k steps before the end, and that every path ending in (q, q) must stay in X after k steps. This also means that X is not connected to any cycle not included in Δ.

Suppose F_∞ is not open. Without loss of generality, we assume there is a path from a cycle not included in Δ to Δ. This cycle is given by two distinct finite words v and v' of same length such that $F(\dots vvvv \dots) = F(\dots v'v'v'v' \dots)$; the path from this cycle to (q, q) is given by two words of same lenght w and w', such that $F(\dots vvvwqqq \dots) = F(\dots v'v'v'w'qqq \dots)$. Let $[-n; n]$ be a neighbourhood for F and k a positive integer. Now consider the finite configurations $x_k = \dots qqqv^k wqqq \dots$ and $y_k = \dots qqqv'^k w'qqq \dots$, where the first letter of the first v has position 0. Almost everywhere, (x_k, y_k) follows a path on the de Bruijn diagram. The only points where (x_k, y_k) does not follow an edge of this diagram is at the transition between cells -1 and 0. So $\mathcal{A}_k = \{i \in \mathbb{Z} / F(x_k) \neq F(y_k)\}$ is included in $[-n-1; n]$, and does not depend on k when k is large enough; let's define $\mathcal{A} = \lim_{k \to \infty} \mathcal{A}_k$. Let $\mathcal{B}_k \subseteq \mathbb{Z}$ be the singleton consisting of the rightmost cell where x_k and y_k differ. Since $v \neq v'$, its emplacement is at least $k - 1$. Let $\mathcal{N}$ be a finite subset of $\mathbb{Z}$; for a large enough k, we have the following properties:

- $F(x_k)|_{\mathcal{B}_k - \mathcal{N}} = F(y_k)|_{\mathcal{B}_k - \mathcal{N}}$
- $x_k|_{\mathcal{B}_k} \neq y_k|_{\mathcal{B}_k}$
- $\mathcal{A} = \{i \in \mathbb{Z} / F(x_k) \neq F(y_k)\}$.

Then, according to the proof of theorem 2.1, $\widetilde{F}$ is not local at $\mathcal{A}$ with neigbourhood $\mathcal{N}$. Since we showed that there exists $\mathcal{A}$ such that this is true for any $\mathcal{N}$, we have indeed just proven that $\widetilde{F}$ is not everywhere local.

Now, what remains to prove is that when F_∞ is open, $\widetilde{F}$ is everywhere local. To do that we will strengthen a little bit the lemma 4 of [8]. But first we need to explain a property of one-dimensional open automata. Suppose F_∞ is open and let $\mathcal{A}$ be a finite subset of $\mathbb{Z}$ and x and y two words such that $F(x)|_{\overline{\mathcal{A}}} = F(y)|_{\overline{\mathcal{A}}}$. Say $\mathcal{A}$ is included in $[-n;n]$, $[-k;k]$ is a neighbourhood for F and l is the number of vertices in the de Bruijn diagram. If we look at (x,y) as a run in this diagram, then we follow edges except perhaps in $[-n-k;n+k]$. But since there are no loops connected in one way or another do Δ, and we have to join Δ at $\pm\infty$, this means we are always in Δ except perhaps in $[-n-k-l;n+k+l]$, to give a rough bound. So there exists a finite subset $\mathcal{N}_I$ of $\mathbb{Z}$, which does not depend on x nor y — though it may depend on $\mathcal{A}$ — such that $x|_{\overline{\mathcal{A}+\mathcal{N}_I}} = y|_{\overline{\mathcal{A}+\mathcal{N}_I}}$. Now all is needed to complete the proof is the next (and last) lemma, which, as announced, is but a gentle strengthening of the lemma 4 of [8].

Lemma 3.2. *Let F be a one-to-one automaton with neighbourhood $\mathcal{N}_C$. Let $\mathcal{A}$ and $\mathcal{N}_I$ be finite subsets of $\mathbb{Z}$ such that for all $x,y \in \mathcal{C}_f(\mathbb{Z})$, if $F(x)|_{\overline{\mathcal{A}}} = F(y)|_{\overline{\mathcal{A}}}$, then $x|_{\overline{\mathcal{A}+\mathcal{N}_I}} = y|_{\overline{\mathcal{A}+\mathcal{N}_I}}$. Suppose $\mathcal{N}_C$ and $\mathcal{N}_I$ contain 0. Then $\widetilde{F}$ is local at $\mathcal{A}$ with neighbourhood $\mathcal{N} = \mathcal{N}_C - \mathcal{N}_C + \mathcal{N}_I$.*

Proof. Let $\mathcal{A} \subseteq \mathbb{Z}^d$. Let ρ and ρ' be states over $\mathcal{H}_{\mathcal{C}_f}$ such that $\rho|_{\mathcal{A}+\mathcal{N}} = \rho'|_{\mathcal{A}+\mathcal{N}}$. We have to prove $\left(\widetilde{F}\rho\widetilde{F}^\dagger\right)|_{\mathcal{A}} = \left(\widetilde{F}\rho'\widetilde{F}^\dagger\right)|_{\mathcal{A}}$.

Let us write $\rho = \sum_{a,b\in\mathcal{C}_f} \lambda_{a,b}|a\rangle\langle b|$ and $\rho' = \sum_{a,b\in\mathcal{C}_f} \lambda'_{a,b}|a\rangle\langle b|$. Then

$$\rho|_{\mathcal{A}+\mathcal{N}} = \sum_{a,b/a_{\overline{\mathcal{A}+\mathcal{N}}}=b_{\overline{\mathcal{A}+\mathcal{N}}}} \lambda_{a,b}|a_{\mathcal{A}+\mathcal{N}}\rangle\langle b_{\mathcal{A}+\mathcal{N}}| = \sum_{x,y\in A^{\mathcal{A}+\mathcal{N}}} \left(\sum_{u\in A^{\overline{\mathcal{A}+\mathcal{N}}}} \lambda_{x.u,y.u}\right)|x\rangle\langle y|.$$

Ergo, the hypothesis $\rho|_{\mathcal{A}+\mathcal{N}} = \rho'|_{\mathcal{A}+\mathcal{N}}$ may be translated as

$$\forall x,y \in A^{\mathcal{A}+\mathcal{N}} \quad \sum_{u\in A^{\overline{\mathcal{A}+\mathcal{N}}}} \lambda_{x.u,y.u} = \sum_{u\in A^{\overline{\mathcal{A}+\mathcal{N}}}} \lambda'_{x.u,y.u}.$$

For $x,y \in A^{\mathcal{A}+\mathcal{N}}$, let $\alpha(x,y)$ be the set of couples (a,b) of words in $\mathcal{C}_f$ such that $a_{\mathcal{A}+\mathcal{N}} = x$, $b_{\mathcal{A}+\mathcal{N}} = y$ and $a_{\overline{\mathcal{A}+\mathcal{N}}} = b_{\overline{\mathcal{A}+\mathcal{N}}}$. Then the hypothesis is equivalent to

$$\forall x,y \in A^{\mathcal{A}+\mathcal{N}} \quad \sum_{(a,b)\in\alpha(x,y)} \lambda_{a,b} = \sum_{(a,b)\in\alpha(x,y)} \lambda'_{a,b}. \tag{3.1}$$

Let us now try translating our aim in the same way. First we have

$$\widetilde{F}\rho\widetilde{F}^\dagger = \sum_{a,b\in\mathcal{C}_f} \lambda_{a,b}|F(a)\rangle\langle F(b)| = \sum_{c,d\in F(\mathcal{C}_f)} \lambda_{F^{-1}(c),F^{-1}(d)}|c\rangle\langle d|$$

$$\left(\widetilde{F}\rho\widetilde{F}^\dagger\right)|_{\mathcal{A}} = \sum_{c,d\in F(\mathcal{C}_f)/c_{\overline{\mathcal{A}}}=d_{\overline{\mathcal{A}}}} \lambda_{F^{-1}(c),F^{-1}(d)}|c_{\mathcal{A}}\rangle\langle d_{\mathcal{A}}|$$

$$\left(\widetilde{F}\rho\widetilde{F}^\dagger\right)|_{\mathcal{A}} = \sum_{z,t\in A^{\mathcal{A}}} \left(\sum_{u\in A^{\overline{\mathcal{A}}}} \lambda_{F^{-1}(z.w),F^{-1}(t.w)}\right)|z\rangle\langle t|.$$

So what we want to prove is that, for every z and t in $A^{\mathcal{A}}$,

$$\sum_{w\in A^{\overline{\mathcal{A}}}} \lambda_{F^{-1}(z.w),F^{-1}(t.w)} = \sum_{w\in A^{\overline{\mathcal{A}}}} \lambda'_{F^{-1}(z.w),F^{-1}(t.w)},$$

with the convention that these numbers are 0 when F^{-1} is not appliable. For $z,t\in A^{\mathcal{A}}$, let $\beta(z,t)$ be the set of couples (a,b) of words in $\mathcal{C}_f$ such that $F(a)_{\mathcal{A}}=z$, $F(b)_{\mathcal{A}}=t$ and $F(a)_{\overline{\mathcal{A}}}=F(b)_{\overline{\mathcal{A}}}$. What we want to prove from (3.1) is the equivalent to

$$\forall z,t\in A^{\mathcal{A}} \sum_{(a,b)\in\beta(z,t)} \lambda_{a,b} = \sum_{(a,b)\in\beta(z,t)} \lambda'_{a,b}. \tag{3.2}$$

We will prove this by showing that for each $z,t\in A^{\mathcal{A}}$, there is some set $\gamma(z,t)$ such that $\beta(z,t)=\coprod_{(x,y)\in\gamma(z,t)}\alpha(x,y)$, ie $\beta(z,t)$ is the disjoint union of the $\alpha(x,y)$'s for (x,y) in $\gamma(z,t)$.

On the one hand, it is quite immediate by definition that, when $(x,y)\neq(x',y')$, $\alpha(x,y)$ and $\alpha(x',y')$ are disjoint. On the other hand, by hypothesis, every (a,b) of $\beta(z,t)$ is in some $\alpha(x,y)$, so that $\gamma(z,t)$ may be found in this simple way: for each (a,b) in $\beta(z,t)$, find the unique $(x_{a,b},y_{a,b})$ such that (a,b) is in $\alpha\left(x_{a,b},y_{a,b}\right)$, and then define $\gamma(z,t)$ to be the set of all these (x,y)'s you found. The only problem is that you could add unwanted (a,b)'s by doing so; we need only checking that this is not the case. In other words, we have to prove that whenever the intersection between $\alpha(x,y)$ and $\beta(z,t)$ is nonempty, then the former is included in the latter.

So, let (a,b) be an en element of $\alpha(x,y)\cap\beta(z,t)$ and (a',b') an other element of $\alpha(x,y)$. First of all, since a and a' coincide on $\mathcal{A}+\mathcal{N}$ (where they are equal to x), and in particular on $\mathcal{A}+\mathcal{N}_C$, then $f(a)$ and $f(a')$ coincide on $\mathcal{A}$, thus $F(a')_{\mathcal{A}}=F(a)_{\mathcal{A}}=z$. Likewise, of course, $F(b')_{\mathcal{A}}=t$.

Then, by hypothesis and since $\mathcal{A}$ is finite and $F(a)_{\overline{\mathcal{A}}}=F(b)_{\overline{\mathcal{A}}}$, a and b coincide on $\overline{\mathcal{A}+\mathcal{N}_I}$, not only on $\overline{\mathcal{A}+\mathcal{N}}$. This implies that x and y must coincide on $(\mathcal{A}+\mathcal{N})\cap\overline{\mathcal{A}+\mathcal{N}_I}$, and as a consequence a' and b' do also coincide on $\overline{\mathcal{A}+\mathcal{N}_I}$; thus $F(a')$ and $F(b')$ coincide on $\overline{\mathcal{A}+\mathcal{N}_I-\mathcal{N}_C}$.

Lastly, since a and a' coincide on $\mathcal{A}+\mathcal{N}=\mathcal{A}+\mathcal{N}_C-\mathcal{N}_C+\mathcal{N}_I$, so do $F(a)$ and $F(a')$ on $\mathcal{A}-\mathcal{N}_C+\mathcal{N}_I$. Likewise, $F(b)$ and $F(b')$ coincide on that same interval. However, $F(a)$ and $F(b)$ coincide on $\overline{\mathcal{A}}$, by hypothesis; ergo, $F(a')$ and $F(b')$ coincide on $\overline{\mathcal{A}}\cap(\mathcal{A}-\mathcal{N}_C+\mathcal{N}_I)$. Put it together, you finally get that $F(a')$ and $F(b')$ coincide on $\overline{\mathcal{A}}$; Q.E.D. ∎

XOR_∞ being, as can be checked easily on its de Bruijn diagram, open, it is thus everywhere local, which also means Alice has to surround Bob in order to receive his long-distance calls. On the contrary, the modified version of XOR that was defined in the definition 11 of [2] is not open on the infinite configurations, which is why we were able to find a protocol where Bob and Alice lie on two distinct sides of the stripe.

4. Conclusion

Starting only with the assumption that we should be able to use the adjoint of $\widetilde{F}$, this implied it should be isometric, thus convey a physical meaning as a valid quantum evolution. If we then add the constraint that it should be uniformly local — something that you would certainly expect a cellular automaton to verify in any model — it turns out F has to be reversible, so that $\widetilde{F}$ is part of the already well-known class of RQCA. This is

good news in a way: the notion of a RQCA is a robust one; however, it could nevertheless be considered a downside. Indeed, as stated in the introduction, RQCA are now believed to be fairly well understood, so the next challenge is understanding nonreversible quantum cellular automata. It would certainly have been of great help to be able to construct such NRQCA by quantizing nonreversible CA. Alas, this paper shows that such a thing is impossible. Quantizing one-dimensional open non-reversible automata certainly provides puzzling entities, but no quantum CA; there remains however an interesting open question about the generalization of proposition 3.1 to higher dimensions.

Then again, the most important question right now is: what are NRQCA? Can they be defined from their global evolution in a reasonably simple way? This question, in its most general form, includes the same one concerning randomized automata instead of quantum ones, since classical randomness is part of the quantum world, and as far as we know this question has been little studied. Let us ask it in a more precise way: what is the property on the global evolution of probability distributions that characterizes randomized cellular automata, i.e. those transformations that can be written as a finite number of layers, each of them consisting of a tiling of identical blocks performing some local random transformation?

Acknowledgements

We would like to thank Guillaume Theyssier for pointing out useful references and Reinhard Werner for asking the right questions and providing useful advices and encouragement. Also, a special thanks to the reviewer who remarked that a proof was absent and another one unclear, two remarks leading to the discovery of two mistakes in the first version of the paper, which led in turn to substantial rewriting. Our best hope is not to have introduced too many new mistakes in the process.

References

[1] P. Arrighi, *An alegraic study of unitary one-dimensional quantum cellular automata*, Proceedings of MFCS 2006, LNCS 4162 (2006), 122–133, arXiv:quant-ph/0512040v2

[2] P. Arrighi, V. Nesme, R. Werner, *One-dimensional quantum cellular automata over finite, unbounded configurations*, arXiv:0711.3517v1.

[3] P. Arrighi, V. Nesme, R. Werner, *N-dimensional Quantum Cellular Automata*, arXiv:0711.3975v1

[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] P. Kůrka, *Topological dynamics of cellular automata, Codes, Systems and Graphical Models* (B. Marcus and J. Rosenthal, eds.), The IMA Volumes in Mathematics and its Applications, 123, 447–386, Springer-Verlag, Berlin 2001.

[8] B. Schumacher, R. F. Werner, *Reversible quantum cellular automata*, arXiv:quant-ph/0405174.

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

This work is licensed under the Creative Commons Attribution-NoDerivs License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nd/3.0/.