Article review

One-dimensional quantum cellular automata over finite, unbounded configuration

by Pablo Arrighi, Vincent Nesme, and Reinhard Werner

Etienne Moutot

January 3, 2017

1 Introduction

Cellular automaton (CA) is a model of computation that use a local evolution rule to update iteratively a set of cells. Because of its connection with physics, the idea of generalizing this model with quantum effects was present very early, even already in the famous Feynman's 1982 paper [3]. Since then, a lot of different approaches have been tried to formalize the notion of quantum cellular automaton (QCA).

A one-dimensional classical cellular automaton consists in an infinite array of cells which can take different value in a (finite) set of states. This array evolves in time by successive applications of a local and shift-invariant function along all the array. The natural extension proposed by Watrous [6] is to allow cells to be in superposition of states, and the local function to be a unitary operator. Schumacher and Werner pointed out in [5] that this approach leads to a non-physical model, which means that the global evolution of the automata might not correspond to a unitary transformation. This non-unitary transformation might even lead the automaton to perform super-luminal signaling. The set of Watrous QCA is also not closed under composition and inverse, which are properties we would like to have for a "nice" computational model.

In order to rectify that, Schumacher and Werner proposed another model [5], based on a broader point of view, imposing the global evolution to be unitary. Using the mathematical notion of C^*-algebras [2] instead of Hilbert spaces, they made what they call an axiomatic definition of a QCA, imposing restrictions on the global evolution rather than on the local one (the constructive characterization, like Watrous did). They also proved a very strong result on their QCAs: not only they are reversible (they are by definition), but the inverse is also a QCA. This property is called structural reversibility. This is done thanks to a structure theorem, showing that all QCA have a very specific block-structure. It is a striking result because in the classical case, it is totally false: there exist some bijective classical CA whose inverse is not a valid CA.

The paper we are reviewing here ([1]) studies the particular case of QCA over finite configurations. In this case, it is still very surprising that QCAs over finite (but possibly unbounded) configurations are structurally reversible. The authors prove this theorem in an easier way than in [5], and then consider specific applications of it. Thanks to the locality condition (without which the model allows faster-than-light communication), the authors prove that a well-studied class of CA are not physically reversible. They also show that this definition of QCA allow some speedup in transmission of information in CAs. And finally they provide an example proving that the current structure theorem of [5] is false for dimensions higher than 1.

This report is organized as follow. First we take a look at the definition of a QCA in the finite configuration setting. We also sketch the proof of the main theorem of the paper. Then we explain the examples of the paper and their implications. We conclude with some remarks on this paper and what could be done to improve the results.

2 Definition of QCA

In this section we introduce the notion of one-dimensional QCA and the main theorem about them. In all this report Σ will denote a finite alphabet, which is all basic states cells of the automaton can take. $q\Sigma$will denote $q \cup \Sigma$ with $q \notin \Sigma$ denoting the empty cell.

Definition 1 (Finite configuration). *A finite* ***configuration*** *c over $q\Sigma$ is a function $c : \mathbb{Z} \to q\Sigma$ such that there exist an interval I (possibly empty) for which*

$$c_i = c(i) = \begin{cases} w \in q\Sigma & \text{if } i \in I \\ q & \text{if } i \notin I \end{cases} .$$

The set of all finite configurations over $q\Sigma$ will be denoted by $\mathcal{C}_f$.

Because we are only interested in the finite case, we will use the term configuration to designate a finite configuration.

These configurations are those a classical CA can take. In the quantum case however, the automaton could be in a superposition of these classical configurations.

Definition 2 (Superposition of configuration). *Let $\mathcal{H}_{\mathcal{C}_f}$ be the space of configurations of a QCA. It is defined as follows. We associate a vector $|c\rangle$ to each configuration c such that $(|c\rangle)_{c\in\mathcal{C}_f}$ is an orthonormal basis of $\mathcal{H}_{\mathcal{C}_f}$. A* ***superposition of configurations*** *is then a unit vector in $\mathcal{H}_{\mathcal{C}_f}$.*

Definition 3 (Unitary operator). *A linear opeator $G : \mathcal{H}_{\mathcal{C}_f} \to \mathcal{H}_{\mathcal{C}_f}$ 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). *Let s be the shift operation such that $s(c)_i = c_{i+1}$. Let σ be its linear extension to superposition of configurations. A linear operator G is said to be* ***shift-invariant*** *if and only if $G\sigma = \sigma G$.*

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

$$\rho|_{i,i+1} = \rho'|_{i,i+1} \implies G\rho G^*|_{i,i+1} = G\rho' G^*|_{i,i+1}$$

The classical notion of locality expresses the fact that the state of a cell i at a time $t+1$ depends only of the states of the cells i and $i+1$ at time t. This definition of locality is not so restrictive even if it looks so. In order to increase the "radius of dependency", one could group cells into bigger "supercells" and construct a QCA simulating a larger one, but which is local with radius $\frac{1}{2}$.

We now have all the notions to define a one-dimensional QCA:

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

Theorem 1. *The inverse of a QCA exists, and is a QCA.*

Proof idea. What is behind this theorem is a structure theorem, which provides a block decomposition for all QCAs. From this block decomposition it is straightforward to get the reversed QCA.

We start by focusing on two specific cells, say 1 and 2. The global idea is that for the cell 2 at time t, one could separate the information it will send to the cells 1 and 2 at time $t+1$.

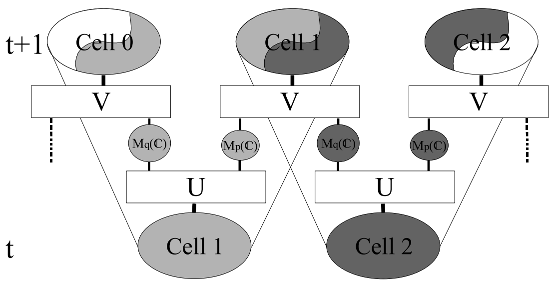

Figure 1: Picture of the block decomposition.

Without the details, Figure 1 gives a picture of the decomposition. The role of U is to separate the information that have to go to the left or right cell. Then V applies the transformation itself using information given by the left and right cells at time t. By shift-invariance, the construction made for a specific cell works for the whole automata.

Figure 2 gives a wider view of the decomposition, and with it, it is quite clear what the reversed QCA is: just take the inverse of the matrices U and V and apply them in the opposite order to get the time reversed. The resulting operator is again a QCA since it is local and duplicated along all the cells. $\square$

3 Consequences and examples

Because it differs from the classical case, this theorem seems to raise several paradoxes. In this section we discuss them with examples, and see some limits of the theorem.

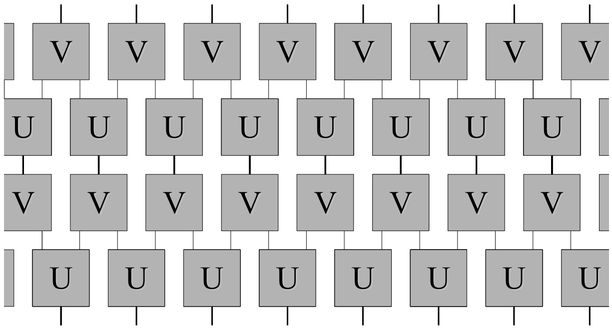

Figure 2: Wider image of the two-layered block representation. Time goes upwards and every (U, V) lines represent a time-step.

3.1 Bijective CA ans superluminal communications

Definition 7 (XOR CA)**.** *We consider the alphabet* $\Sigma = \{0, 1\}$*.* $\forall x, y \in q\Sigma$*, we define* δ *as:* $\delta(qx) = x$*,* $\delta(xq) = q$ *and* $\delta(xy) = x \oplus y$*. Let* F *be the operator applying* δ *on a configuration:* $F : \mathcal{C}_f \to \mathcal{C}_f$ *and maps* $\dots c_{i-1}c_ic_{i+1}\dots$ *to* $\dots\delta(c_{i-1}c_i)\delta(c_ic_{i+1})\dots$*.*

The XOR CA is clearly local and shift-invariant. Because it is defined on finite configurations, it is also bijective: the antecedent exists and can be uniquely determined from the left border of the nonempty region. But it is not structurally reversible: the antecedent could not be computed by a CA. Indeed, consider $c = \dots 000000000\dots$. c could be derived either from a large region of 0s or a large region of 1s, and the only way to determine it is to look at its left border. But because it can be arbitrarily far, a CA cannot separate the two cases in a constant number of steps.

Now comes the apparent paradox: this CA could be linearly extended to an equivalent QCA. Take for example $F : \mathcal{H}_{\mathcal{C}_f} \to \mathcal{H}_{\mathcal{C}_f}$ such that

$$F(\alpha\,|\dots 00\dots\rangle + \beta\,|\dots 10\dots\rangle) = \alpha F(|\dots 00\dots\rangle) + \beta F(|\dots 10\dots\rangle).$$

So, it would mean that there exists a block representation of the XOR CA. But if you look more carefully at the quantized Ff, it turns out that even if it is unitary and shift-invariant, it is not local. Consider the configurations

$$c_\pm = 1/\sqrt{2}\,|\dots qq\rangle\,(|00\dots 00\rangle \pm |11\dots 11\rangle).$$

Then $Fc_\pm = |\dots qq00\dots 00\rangle\,|\pm\rangle\,|qq\dots\rangle$ with $|\pm\rangle = \frac{|0\rangle\pm|1\rangle}{\sqrt{2}}$. If i is the position of the last non-empty cell, then $Fc_\pm|_i = |\pm\rangle\langle\pm|$ does not depend only on $c|_{i,i+1}$ but rather on the global "phase" of c, that is, a possibly unbounded part of c. Another way of seeing it is that the XOR QCA would allow faster-than-light communication. Indeed, if Alice has the first non-empty cell and Bob the last one (i), then Alice could change c_+ to c_- by just applying one phase gate $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ to her cell, leading Bob's cell to a change from $|+\rangle$ to $|-\rangle$, which is measurable since $|+\rangle$ and

$|-\rangle$ are orthogonal. Which leads to instantaneous communication between Alice and Bob.

More generally, a quantize version of a non-structurally reversible CA will not be structurally reversible. Hence we have:

Proposition 1 (Class B is not locally quantizable)**.** *We call B the class of bijective CA on finite configurations but not on infinite ones. Automata from this class do not admit a local quantization. Hence these automata cannot be implemented by a series of finite closed quantum systems.*

3.2 Faster quantum signalling

Some classical CAs do not admit a two-layered block representation unless cells are grouped into supercells. On example is the Toffoli CA (see Figure 3). It is clearly

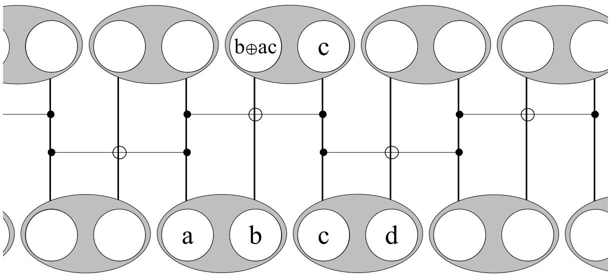

Figure 3: The Toffoli CA.

shift-invariant and local of radius 1/2. But to find its block representation we need to group cells. Indeed, b is switched depending on a and c. The Toffoli CA can be seen as two consecutive Toffoli gates, as shown in Figure 3. But it is known that these Toffoli gates cannot be obtained using two bits gates in classical reversible computation. Hence any block representation needs more than two classical gates, or two with cells grouping. So, in the classical setting, this CA is of radius 1/2, has an inverse of radius 1/2, but does not have a two-layered block representation without cell grouping.

Let F be the quantized version of the Toffoli CA. This time F is local, but again against intuition, F is not of radius 1/2 but 3/2. It means anyway that quantizing the Toffoli CA allows to have a faster communication than in the classical case. Unlike the XOR CA, this speedup does not break the light speed limit.

3.3 Higher dimensions

Unfortunately for dimensions higher than 2 there are examples of CA that are structurally reversible but that do not admit any two-layered bloc representation. One example is the Kari CA [4]: the original proof works the same for the quantum case. This leads to the following proposition:

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

This proposition does not mean that higer dimensional QCA are not all structurally reversible, it just means that they can have different structure from the one of the structure theorem, which hence fails to prove than any QCA is structurally reversible for dimensions higher than 1.

4 Conclusion

This paper proves in the simpler setting of finite configurations the result from [5]. This setting is still very expressive, and the finiteness of the configurations reflects better the physical reality of CA implementations. Using this theorem, it appears that some CA, like the XOR CA or the whole B class, are not physically reversible: even their quantum extension cannot be structurally reversed with the current definition of QCA.

The main limitation of this paper is that it treats only the one-dimensional case. A very challenging but interesting direction would be to find an equivalent structure theorem for higher-dimension QCAs. That would let us better understand how QCA works more generally, in some more complex cases than the one dimensional line. However, it is a very common fact that these kind of theories becomes very much harder to understand in dimensions greater than 1. Another possible direction follows from the remark in section 3.2: it could be interesting to study more precisely when the communication speedup do appears, and how big it is exactly. It is an interesting option since for CAs, communication speedup is synonymous of computational speedup.

Bibliography

[1] P. Arrighi, V. Nesme, and R. Werner. "One-Dimensional Quantum Cellular Automata over Finite, Unbounded Configurations". In: *Language and Automata Theory and Applications: Second International Conference, LATA 2008, Tarragona, Spain, March 13-19, 2008. Revised Papers*. Ed. by C. Martín-Vide, F. Otto, and H. Fernau. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 64–75. DOI: 10.1007/978-3-540-88282-4_8.

[2] O. Bratteli and D. W. Robinson. *Operator Algebras and Quantum Statistical Mechanics: C*- and W*- algebras, symmetry groups, decomposition of states*. Texts and Monographs in Physics. Springer-Verlag, 1979.

[3] R. P. Feynman. "Simulating physics with computers". In: *International Journal of Theoretical Physics* 21.6 (1982), pp. 467–488. DOI: 10.1007/BF02650179.

[4] J. Kari. "On the Circuit Depth of Structurally Reversible Cellular Automata". In: *Fundam. Inf.* 38.1,2 (Apr. 1999), pp. 93–107.

[5] B. Schumacher and R. F. Werner. "Reversible quantum cellular automata". In: *arXiv preprint quant-ph/0405174* (2004).

[6] J. Watrous. "On one-dimensional quantum cellular automata". In: *Proceedings of IEEE 36th Annual Foundations of Computer Science*. Oct. 1995, pp. 528–537. DOI: 10.1109/SFCS.1995.492583.