Université de Grenoble

Habilitation à Diriger les Recherches

Quantum cellular automata

Pablo Arrighi

© 13^{th} *of June 2009*

Abstract

Quantum cellular automata (QCA) consist of an array of identical, finite dimensional, quantum systems. These evolve in discrete time steps according to a causal, shift-invariant unitary evolution. We review the literature of QCA, after having provided the necessary elements of Quantum Theory and some background of Cellular Automata.

We then move on to consider a graph with a single quantum system at each node. The entire compound system evolves in discrete time steps by iterating a global evolution U. We require that this global evolution U be unitary, in accordance with quantum theory, and that this global evolution U be causal, in accordance with special relativity. By causal we mean that information can only ever be transmitted at a bounded speed, the speed bound being quite naturally that of one edge of the underlying graph per iteration of U. We show that these unitary causal U can be implemented locally; i.e. it can be put into the form of a quantum circuit made up with more elementary operators – each acting solely upon neighbouring nodes.

We apply the above general result to n-dimensional quantum cellular automata in order to obtain a block representation of them. Hence we have shown their general, axiomatic definition still yields a unifying, operational representation of them. Some non-trivial consequences are explored, such as the fact that bijective non-reversible CA are not physical as closed systems, or that quantum information may travel faster than classical – within some fixed dynamics.

Finally we describe n-dimensional quantum cellular automata capable of simulating all others. By this we mean that the initial configuration and the local transition rule of any one-dimensional QCA can be encoded within the initial configuration of the universal QCA. Several steps of the universal QCA will then correspond to one step of the simulated QCA. The simulation preserves the topology in the sense that each cell of the simulated QCA is encoded as a group of adjacent cells in the universal QCA. The encoding is linear and hence does not carry any of the cost of the computation.

Acknowledgements

See printed copy of the thesis.

Collaborations and publications

- Section 3.2.3 presents the Curtis-Lyndon-Hedlund theorem in a way which was shown to me by Jacques Mazoyer.
- Sections 4.2, 4.3 and 5.1 are results from the paper *Unitarity plus causality implies locality*, co-authored with Vincent Nesme and Reinhardt Werner, see [18].
- Sections 5.3 and 5.4 are results from the paper *Quantum cellular automata over finite, unbounded configurations*, co-authored with Vincent Nesme and Reinhardt Werner, although Subsection 5.4.2 has later been improved thanks to an idea by Jarkko Kari, see [19].
- Sections 5.2 and 6.3 are results from the paper *Intrinsically universal n-dimensional quantum cellular automata*, co-authored with Jonathan Grattage, see [16].
- Sections 6.1 and 6.2 are results from the paper *Intrinsically universal one-dimensional quantum cellular automata in two flavours*, co-authored with Renan Fargetton and Zizhu Wang, see [15].
- Section 7.3 refers to work in progress with Gilles Dowek, see [12].

How to read this thesis

Besides this dissertation the documents presented in order to obtain the 'Habilitation à Diriger les Recherches' (HDR) include a selection of papers amongst [7, 19, 17, 18, 13, 15, 16, 12], which are direct contributions to the topic of Quantum Cellular Automata (QCA), but also amongst [5, 20, 21, 14, 22, 6, 23, 10, 9, 11, 47, 8], which fit only in the wider quantum information and quantum computation themes. This dissertation is intended as an introduction to the first set of papers. HDR dissertations can be written in different styles:

- Some provide background knowledge of the main results in the literature surrounding their topic. This is a way to place one's work into perspective, and also an opportunity to prepare a text which may reach a wider audience than the already acquainted specialist reviewing the dissertation (⊙).

- Some provide more intuitions and examples to their own main results. Again this is a way to place one's work into perspective, and to grant easier access to these results. Although the precise mathematical detail is usually left to the attached papers, this is an opportunity to show that real, technical work has been done (⟁).

- Others throw themselves at the more informal and personal level into directly explaining the motivations and the perspective of their work, and how these may fit in the grander scheme of scientific things. Unfortunately this sort of explanation can often be misinterpreted as incautious, unsubstantiated claims or mere boasting, in a community which is fashioned by higher standards of objectivity and mathematical rigour. That is, unless their author has reached a certain level of seniority. But after all the HDR is intended as a first step towards seniority, and scientific research is always a step in the unknown. So this is an opportunity to try and put words upon what we aim for but is not yet formal (⊛).

We have tried to provide three reading coherent paths to this dissertation, corresponding to the three above styles. Each section is marked by the corresponding symbol (⊙, ⟁, ⊛).

See printed copy of the thesis.

Contents

Chapter 1

Introduction

We can only see a short distance ahead,
but we can see plenty there that needs to be done.
—Alan Turing, Final sentence in his 'Computing Machinery and Intelligence'

A computer scientist may find that this dissertation is in physics, but a physicist may find that this dissertation is in computer science, and both will be right. The work presented here lies at the interface between theoretical computer science and theoretical physics. This interface is by no means thin, it was fundamental in the early days of computer science, and has recently come back into fashion in both communities. This chapter speaks freely about this interface and serves as a personal introduction to the themes explored in the thesis.

1.1 Physics in computer science ⊙⟁⊛

1.1.1 When computer science takes off...

I completed my Ph.D. thesis in one of the oldest computer science department in the world : the Computer Laboratory of the University of Cambridge. This place is dear to my heart of course, even though it looks just like a cold modern fortress of concrete, steel and glass – with only a couple of bricks to give it a British touch. Now walk in and there they are. Some pictures of a monster machine named EDSAC which was the glory of the lab in the 50's, and the actual small green door that was hiding this monster at the time – straight out of the past! On this door some white letters say 'Mathematical Laboratory'. This relic should make us humble : 60 years ago there was no computer science department at all. Computer science did not even exist. There was physics and there was mathematics. Surely at the time it was obvious to everyone that the notion of a computer was to describe a physical system, which one would prepare in an initial state, leave it to run under whatever physical law was applicable, and then observe the results with the hope that this might have accomplished something useful – such as breaking cryptographic codes.

In the 30's mathematicians began to abstract away the computing process from the contingencies of physical life, as they like to do for things in general. That is, if you ask a physicist the question 'What is a computer?' you expect some answer involving silicon, transistors and electromagnetic pulses. However, if you ask a mathematician the same question, the answer is likely to involve set theory, functions, and the natural numbers. This gave rise to 'models of computation', i.e. purely abstract, mathematical definitions of what computers are, such as the Minsky machine, Church's λ-calculus, the Turing machine, Von Neumann's cellular automata, and many others.
Remember the old joke about Trotskyists : 'one of them makes a party, two of them make a scission'. Well, mathematicians are not so much like that,

and the amazing thing is that all of these different models of computation soon turned out to be equivalent, i.e. the notion of a computer according to some mathematician X was able to simulate anything that the notion of a computer according to some mathematician Y was able to do. Church and then Turing in 1936 captured the belief that the community had reached a robust answer to the question 'What is a computer?' through their famous thesis : 'Anything that can reasonably be computed can be computed by a Turing machine'. This statement had the impact of a declaration of independence : the computing process was no longer contingent upon the physics implementing it. Computer science was born as a field in its own right.

How many times during my undergraduate studies have I heard the expression 'hardware-independence', and actually now that I lecture I find myself saying it. Surely it is not just a matter of stating our independence from other fields : 'hardware-independence' is one of the driving forces in the history of computer science. After all, practical computer scientists learn to program in a way which could not care less about the actual physical machines and networks upon which their distributed, communicating processes live. They learn high-level programming, virtual machines, sockets, encapsulation... Meanwhile, theoretical computer science continues to be anchored on models of computation. It seeks to see what functions can be computed under these models and which cannot : this is computability theory. It seeks to see what functions can be computed efficiently (using the notions of time and space provided by these models) and which cannot : this is complexity theory. And for all of these purposes the answers continue to appear relatively independent of the chosen model of computation – so that the result are not only hardware-independent, but often model-independent even. For this reason maybe models have not evolved so much, but theories about them have. Well this is not quite true, there are quite a few new models of computation (CCS, π-calculus, ...) accounting for the parallelism, concurrency etc., available with the rise of internet – but these are only here to cover new aspects of computer science, and previous results are not at stake.

1.1.2 ... and lands.

Meanwhile some physicists don't understand. Why are modern day computers so useless at predicting the outcome of some of their quantum physics experiments? On the one hand the theory behind computer science is rock solid, and it says that matrix multiplications come at a cost $\omega(l^2)$ in l, the length of the input vector. On the other hand the state of a quantum physical system is decribed by a vector of length l which is exponential in s, the actual size of the system. So the simulation of a quantum physical system on

a classical computer is much too costly. Aren't computers physical systems after all? Is it not the case that a quantum physical system should be able to simulate a physical system efficiently? Could it be that the theory behind computer science is correct, but that the underlying assumptions are wrong – i.e. that models of computation are not so independent from the physics after all? Feynman advocates these ideas [60]. Deutsch proposes a first model of 'quantum computation' [46]. Shor [123] and Grover [67] unravel the major impact that these models have on complexity theory. This is yet another case of physicists coming in to provide new means of computation, just like in the early days. However this time their help is embarassing, because it not only puts at stake some of the previous theoretical results computer science has had, it goes against everything computer science has strived for until then, namely 'hardware-independence'. In fact, the computing process has become physical again.

As computer scientists we can choose to ignore this incursion of physics within our realm. We can also choose to fix this, by conceiving new models of computation, abstracting ourselves away again from the physics, and then rebuilding a new computability theory and a new complexity theory; i.e. an updated theoretical computer science. Mostly, this is what quantum computer science is all about. Over the last twenty years there has been a number of quantizations of the classical models of computation, of which this work on quantum cellular automata could be considered an instance. Whilst computability was not so shaken by the advent of these models of quantum computation, complexity theory has undergone quite an overhaul, see for example [27].

1.2 Computer science in physics ⊛

As computer scientists we can also choose to take a less defensive attitude, and decide to lead our own incursion within physics. After all, now that frontiers are blurred, cultural exchanges can take place. Now that the computing process has become physical again, the converse question comes back into fashion : 'To what extent are physical processes... computational?'. A number of essays by renowned physicists such as Smolin [124], Brukner and Zeilinger [37] or Lloyd [88], raise this question. This is part of a bigger trend where theoretical physics departs from looking at 'matter' (particles interacting, scattering, forces, etc.) and seeks to look at 'information' (entropy, observation, information exchanges between systems, etc.), in an attempt to clarify its own concepts. There are many examples of this; we could mention for instance the huge impact that quantum information theory has had on

the understanding of foundational concepts such as entanglement [49] and decoherence [112]. But coming back to theoretical computer science, and excluding information theory for that matter, what concepts have we that could be of use to theoretical physics?

Are there models of computation which, once quantized, could yield interesting results in theoretical physics? We have mentioned that the standard models of classical computation turn out to be equivalent in terms of their basic ability to compute. Nevertheless, each of them has its own advantages, its own reason d'être. For example, the λ-calculus is popular as a model of computation because it establishes formal connections between computer science and logics. Hence quantizing this model may be a way to work out some 'quantum physical logic'. That would be quite useful of course, as quantum theory is often said to be rather counter-intuitive. These are the kind of ideas we are pursuing in [11, 8], along with many others in the community [1] – but they are not the topic of this thesis. Cellular Automata are a popular model of computation because of their ability to frame the computing process within space, e.g. within a 3D grid which mimics space as we know it. Hence quantizing this model could be of interest in order to work out some 'quantum theory in space and time'. That of course would be quite useful too, as quantum theory is hardly compatible with our common intuition of space and time (cf. entanglement, Einstein's 'spooky effects at a distance', the Bell inequalities, etc.). Quantum theory is commonly used in order to describe spatially distributed systems, but strictly speaking the Schrödinger equation is known to be inexact in that case. The correct way to do this is to switch to quantum field theory and the Dirac equation. But this remains unsatisfactory in many respect, due to the complexity, the lack of axiomatization and the lack of intuitions around this theory. In this thesis we are making some, humble and small, contribution to the understanding of 'quantum theory in space and time', via the notion of unitary causal operator in particular.

Are there concepts in computation theory which, once quantized, could be of interest to theoretical physics? The main concept in computation theory is universality. An instance of a model of computation is universal if it can simulate any other. I believe that it could be useful to port this concept into physics. One argument goes as follows. First, notice how often in theoretical physics it pays off to be 'hardware-independent' as well, i.e. to distinguish the actual physics (the particles and forces being described) from the mechanics (the mathematical theory used for the description) in which it is framed. Second, consider the extreme problem of trying to reconcile two rather different mechanics (quantum theory and general relativity, say) and, at the same time, trying to account for all known particles and forces in

those mechanics... and face that this is overambitious. Third, consider the other extreme of trying to reconcile both mechanics – but in the absence of any actual physics! This would be too trivial; of course there is no need for a frame if there is nothing to frame. Fourth, picture yourself tackling the problem of reconciling both mechanics in the presence of a reasonably small and yet complex physical phenomena. That way there will be 'something to frame'. Ponder your anxiety as you struggle to unify both theories and wonder whether the physical phenomena you have chosen is not too complicated already. And ponder your anxiety again, as you come close to unifying both theories and wonder whether the physical phenomena you have chosen is not too trivial, after all! The point here is that the concept of universality adresses exactly this issue. Finding out a *minimal, universal physical phenomena* will provide us with something simple to frame – so that the focus can be on reconciling both mechanics – and yet rich enough so as to have a guarantee that we can later fit some arbitrarily complex phenomena in this reconciled mechanics. Now, there are simple objections to these arguments:

- First, the fact that a universal Turing machine can simulate just about anything, e.g. even 22 football players on a pitch (if you buy the FIFA09 football video game that is) is not enough : what you want is to be able to simulate each of the 22 players independently in their own space. So, really the universal physical phenomena we are looking for should be more alike some elementary unit of computation that can be plugged together into a larger 3D network of them. Our notion of universality ought to account for space and interactions across space in a satisfactory manner.

- Second, the fact that the universal Turing machine is so slow at simulating quantum physical phenomena suggests that it is not rich enough. So, intuitively the universal physical phenomena we are looking for should be a universal model of *quantum* computation. Our notion of universality should take into account the *cost* of simulation.

In this thesis I formalise a notion of universality which fits both these criteria, namely intrinsic universality over quantum cellular automata. Of course we expect that there will still be objections to these arguments – but at least they will not be so simple!

1.3 The plan ⊙⏢⊛

This thesis can be viewed as an account of a number of steps along porting computer science universality into theoretical physics. It can be viewed in numerous other ways however, as there are several more established reasons to study Quantum Cellular Automata as we did. You will find these are enumerated at the start of Chapter 4. In Chapter 2 we introduce some elements of quantum theory. In Chapter 3 we overview some Cellular Automata results. In Chapter 4 we explain Quantum Cellular Automata. In Chapter 5 we study their structure. In Chapter 6 we study their universality. In Chapter 7 we explain some of the remaining steps to take, according to our judgement.

Chapter 2

Elements of quantum theory

Very interesting theory - it makes no sense at all.
—Groucho Marx

If you haven't found something strange during the day,
it hasn't been much of a day.
—John A. Wheeler

Here we present some reminders of linear algebra and the postulates of quantum theory, making it possible for anyone with a basic knowledge of vector spaces to follow the thesis. We explain separable Hilbert spaces together with their inner product and norm $\|.\|$, so as to state that states $|\psi\rangle$ in quantum theory are normalized vectors ($\||\psi\rangle\| = 1$) of these spaces. We explain operators and their adjoints †, so as to state that evolutions U in quantum theory are unitary operators ($UU^\dagger = U^\dagger U = \mathbf{I}$), and measurements are sets of operators $\{M_k\}$ such that $\sum_k M_k^\dagger M_k = \mathbf{I}$. We explain density matrices, tensors and traces, which are necessary notions in order to put two quantum systems aside, have them to interact, and later take them apart.

This chapter seeks to provide the minimal amount of linear algebra and quantum theory required in order to follow this thesis. The prerequisite is some basic working knowledge of vector spaces. If the reader has not had any previous contact with Hilbert spaces and foundations of quantum theory before, this will get him started just enough to go through the mathematics of the thesis. But he will lack a number of intuitions which surround and motivate this work, as well as a couple of proofs of standard theorems. The recommended remedy is reference [108].

2.1 Reminders of linear algebra ⊙

2.1.1 Vectors

Vector spaces, Inner product, Hilbert spaces

Dirac notation. Usually a vector $\mathbf{v}$ in a vector space $\mathcal{V}$ is denoted with its name in bold. Here instead of writing $\mathbf{v}$ we write $|v\rangle$, following the Dirac notation. More generally we write vectors as $|name\_of\_vec\rangle$, where $name\_of\_vec$ is just a name for the vector. E.g. $|0\rangle$ is just a vector whose name is zero. It is not to be confused with the null vector, which is the only one we still write in bold, $\mathbf{0}$.

Inner product. Consider a vector space $\mathcal{V}$ over the field of the complex numbers. As usual $(.,.) : \mathcal{V} \times \mathcal{V} \longrightarrow \mathbb{C}$ is an inner product for $\mathcal{V}$ if and only if it verifies the following set of axioms:

$$\begin{aligned} \forall|\psi\rangle\forall|\phi\rangle\forall|\chi\rangle\ (|\psi\rangle, |\phi\rangle + |\chi\rangle) &= (|\psi\rangle, |\phi\rangle) + (|\psi\rangle, |\chi\rangle) \\ \forall|\psi\rangle\forall|\phi\rangle\ (|\psi\rangle, |\phi\rangle) &= (|\phi\rangle, |\psi\rangle)^* \\ \forall|\psi\rangle\ (|\psi\rangle, |\psi\rangle) &\geq 0 \text{ with equality iff } |\psi\rangle = \mathbf{0}. \end{aligned}$$

Dirac notation continued. Following the Dirac notation let us write $\langle\psi|$ for the linear functional from $\mathcal{V}$ to $\mathbb{C}$ which takes a vector $|\phi\rangle$ as input, and yields the complex number $(|\psi\rangle, |\phi\rangle)$ as output. Of course by doing this we are introducing a new notation for the inner product $(|\psi\rangle, |\phi\rangle)$, namely $\langle\psi|(|\phi\rangle)$ or simply $\langle\psi|\phi\rangle$.

Norm and distance. The inner product induces a norm and a distance. The induced norm of a vector $|\psi\rangle$, denoted $|||\psi\rangle||$, is the non-negative real number $\sqrt{\langle\psi|\psi\rangle}$. The induced distance between two vectors $|\psi\rangle$ and $|\phi\rangle$ is $|||\psi\rangle - |\phi\rangle||$.

Generated vector space. Let S be a countable set, i.e. S is either finite or in bijection with $\mathbb{N}$. We denote by $\mathcal{V}_S$ the vector space generated by finite linear combinations of the vectors $(|e\rangle)_{e\in S}$, and endowed with an inner product such that the $(|e\rangle)_{e\in S}$ are orthonormal, i.e. $\langle e|e'\rangle = \delta ee'$.

Hilbert space. Consider a series of vectors $|\psi_n\rangle = \sum_{i=0\ldots n} \alpha_i|i\rangle$ but such that $\||\psi_{n+1}\rangle - |\psi_n\rangle\|$ ends up decreasing in n. By definition this is a Cauchy sequence of vectors in $\mathcal{V}_{\mathbb{N}}$. Here the situation is the same as that of rational numbers $\mathbb{Q}$. Recall that Cauchy sequences in $\mathbb{Q}$ may not have a their limit in $\mathbb{Q}$, and so if we want to call these limits 'something' we have no choice but to 'add them' to $\mathbb{Q}$. This process is called 'completion' and in the case of the rational numbers $\mathbb{Q}$ it yields the real numbers $\mathbb{R}$. If we do the same for a vectorial space $\mathcal{V}_S$, this yields the separable Hilbert space $\mathcal{H}_S$. For instance in the above example the Cauchy sequence of vectors $|\psi_n\rangle$ converges in $\mathcal{H}_{\mathbb{N}}$ – by definition of $\mathcal{H}_{\mathbb{N}}$ as the completion of $\mathcal{V}_{\mathbb{N}}$.

Hilbertian basis and separability. A Hilbert space in general is a vector space which is complete with respect to the distance induced by its inner product. Not all of them arise as the completion of some $\mathcal{V}_S$, however. If they do, they are called separable. Let us consider again the above Cauchy sequence of vectors $|\psi_n\rangle$, and call $|\psi\rangle$ its limit as n goes to infinity. Notice that because this $|\psi\rangle$ may be in $\mathcal{H}_{\mathbb{N}}$ but not in $\mathcal{V}_{\mathbb{N}}$, it is no longer expressible as a finite linear combination of the vectors $(|i\rangle)_{i\in\mathbb{N}}$, and so strictly speaking $(|i\rangle)_{i\in\mathbb{N}}$ is not a basis for $\mathcal{H}_{\mathbb{N}}$. However it is clear that $|\psi\rangle$ can be approached to an arbitrary precision by a finite linear combination of vectors in $(|i\rangle)_{i\in\mathbb{N}}$, and so in this sense $(|i\rangle)_{i\in\mathbb{N}}$ constitutes a hilbertian basis for $\mathcal{H}_{\mathbb{N}}$. Hence an equivalent way to define separability is to require that a Hilbert space admits a countable hilbertian basis, or equivalently again that it has a vector space of countable dimension as a dense subset. We are only interested in separable Hilbert spaces $\mathcal{H}_S$ in this thesis; in fact for most purposes we could have done just as well with $\mathcal{V}_S$. From now on whenever a $\mathcal{H}$ appears, this is a separable Hilbert space, and whenever we talk about a basis, this is a hilbertian basis.

Tensor spaces. Let $\mathcal{H}^A$ and $\mathcal{H}^B$ be two separable Hilbert spaces. Consider the set T of finite linear combinations of terms in $\{|\psi\rangle\otimes|\phi\rangle \;/\; |\psi\rangle \in \mathcal{H}^A \wedge |\phi\rangle \in \mathcal{H}^B\}$, together with the equivalence induced by the following set of axioms:

$$\lambda.|\psi\rangle \otimes |\phi\rangle = |\psi\rangle \otimes \lambda.|\phi\rangle = \lambda.(|\psi\rangle \otimes |\phi\rangle)$$
$$(|\psi\rangle + |\chi\rangle) \otimes |\phi\rangle = |\psi\rangle \otimes |\phi\rangle + |\chi\rangle \otimes |\phi\rangle$$
$$|\psi\rangle \otimes (|\phi\rangle + |\chi\rangle) = |\psi\rangle \otimes |\phi\rangle + |\psi\rangle \otimes |\chi\rangle.$$

It turns out that T together with this equivalence relation, i.e. the quotient space $T_{/=}$, forms a vector space. We equip $T_{/=}$ with an inner product $(.,.)^{AB}$ defined in terms of the inner products $(.,.)^A$ and $(.,.)^B$ as follows:

$$\forall|\psi\rangle\forall|\phi\rangle\forall|\psi'\rangle\forall|\phi'\rangle\ (|\psi\rangle\otimes|\phi\rangle,|\psi'\rangle\otimes|\phi'\rangle)^{AB} = (|\psi\rangle,|\psi'\rangle)^A(|\phi\rangle,|\phi'\rangle)^B$$

and by linearity for other vectors. Then $\mathcal{H}^A\otimes\mathcal{H}^B$, or simply $\mathcal{H}^{AB}$, is just the completion of $T_{/=}$ with respect to the norm induced by $(.,.)^{AB}$.
Really this tensor product construction is not as complicated as it seems. It is just a question of wanting to put two elements aside : if $|\psi\rangle$ is in $\mathcal{H}_{\{0,1\}}$ and $|\phi\rangle$ is in $\mathcal{H}_{\{0,1\}}$ then we can put them aside just by separating them by $\otimes$, as though it was a comma, so that $|\psi\rangle\otimes|\phi\rangle$ is in $\mathcal{H}_{\{0,1\}}\otimes\mathcal{H}_{\{0,1\}}$. There is only a slight edge to it. First of all we want to identify say $(|0\rangle+|1\rangle)\otimes|0\rangle$ with $(|0\rangle\otimes|0\rangle+|1\rangle\otimes|0\rangle)$. This is intuitive, because both cases correspond to a scenario where 'the first space can be zero or one, but the second is always one'. Second of all we notice that now the four basic scenarios are $|0\rangle\otimes|0\rangle$, $|0\rangle\otimes|1\rangle$, $|1\rangle\otimes|0\rangle$ and $|1\rangle\otimes|1\rangle$, and we are allowed linear combinations of them, so $|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle$ is in $\mathcal{H}_{\{0,1\}}\otimes\mathcal{H}_{\{0,1\}}$. Now this is interesting, because $|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle$ cannot be expressed as a $|\psi\rangle\otimes|\phi\rangle$; it is only a linear combination of such things.

2.1.2 Operators

Operators and adjoints. An operator A from $\mathcal{H}$ to $\mathcal{H}'$ is a linear function from elements of $\mathcal{H}$ to elements of $\mathcal{H}'$, i.e. $A(|\psi\rangle+|\phi\rangle)=A|\psi\rangle+A|\phi\rangle$. We say that $A^\dagger$ is the adjoint operator of A if and only if

$$\forall|\psi\rangle\forall|\phi\rangle\ (|\psi\rangle,A|\phi\rangle)=(A^\dagger|\psi\rangle,|\phi\rangle).$$

We can also sum operators together and weight them by a scalar in the obvious way.

Projectors. Let $\mathcal{H}$ be a subspace of $\mathcal{H}'$. We denote by $\mathcal{H}^T$ the subspace generated by those vectors in $\mathcal{H}'$ which are orthogonal to all of the vectors in $\mathcal{H}$. Then P is the projector over $\mathcal{H}$ if and only if $P|\psi\rangle=|\psi\rangle$ for $|\psi\rangle\in\mathcal{H}'$, and $P|\psi\rangle=\mathbf{0}$ for $|\psi\rangle\in\mathcal{H}'^T$. Say $\{|\psi_i\rangle\}$ is an orthonormal basis for $\mathcal{H}$. Then $P=\sum_i|\psi_i\rangle\langle\psi_i|$. Moreover note that being a projector for some subspace is equivalent to $P^2=P$.

Normal operators. Let A be an operator over $\mathcal{H}_S$. A is said to be normal if and only if $A^\dagger A=AA^\dagger$. Now take S as a finite set. Then by the spectral

decomposition theorem A is normal if and only if it can be written as

$$A = \sum_x \lambda_x P_x$$

where the projectors P_x verify $P_x P_{x'} = \delta_{xx'} P_x$ and the eigenvalues λ_x are distinct.

Hermitian matrices. Let H be an operator over $\mathcal{H}_S$. H is said to be hermitian if and only if $H = H^\dagger$. Now take S as a finite set. Then by the spectral decomposition theorem H is hermitian if and only if it is normal with eigenvalues in $\mathbb{R}$.

Positive matrices. Let ρ be an operator over $\mathcal{H}_S$. ρ is said to be positive if and only if $\forall|\psi\rangle\ \langle\psi|\rho|\psi\rangle \in \mathbb{R}^+$. Now take S as a finite set. Then by the spectral decomposition theorem ρ is positive if and only if it is normal with eigenvalues in $\mathbb{R}^+$. Hence projectors are positive, positive operators are hermitian, and hermitian operators are normal.

Unitary matrices. Let U be an operator over $\mathcal{H}_S$. U is said to be unitary if and only if $\forall|\psi\rangle\ \||U|\psi\rangle\| = \||U^\dagger|\psi\rangle\| = \||\psi\rangle\|$. This turns out to be equivalent to $UU^\dagger = U^\dagger U = \mathbf{I}$, or to the fact that a unitary operators will map orthonormal basis $\{|\psi_i\rangle\}$ into another orthonormal basis $\{U|\psi_i\rangle\}$. Hence unitary operators can be thought of as rotations/changes of bases. Now take S as a finite set. Then by the spectral decomposition theorem U is unitary if and only if it is normal with eigenvalues of modulus one.

Tensor of operators. Let A and B be operators upon $\mathcal{H}^A$ and $\mathcal{H}^B$ respectively. Then $A \otimes B$ is the operator upon the tensor space $\mathcal{H}^A \otimes \mathcal{H}^B$ such that

$$\forall|\psi\rangle\forall|\phi\rangle\ \Big(A \otimes B\Big)(|\psi\rangle \otimes |\phi\rangle) = (A|\psi\rangle) \otimes (B|\phi\rangle)$$

and by linearity for other vectors. Again notice that not all operators upon $\mathcal{H}^A \otimes \mathcal{H}^B$ are of the form $A \otimes B$, but all of them are linear combinations $\sum_i A_i \otimes B_i$.

Trace. Another common operation is to take the trace of an operator. Consider A an operator over $\mathcal{H}_S$. Then $\mathrm{Tr}(A)$ is defined to be $\sum_{e \in S} \langle e|A|e\rangle$, if this limit exists. Of course many operators do not have a trace, for instance the identity $\mathbf{I}$ over $\mathcal{H}_\mathbb{N}$ does not. Here are some useful properties.

Lemma 2.1 (Cyclicity, linearity, base independence, etc.)
Let A, B be operators over $\mathcal{H}$. We have $Tr(AB) = Tr(BA)$ and $Tr(A+B) = Tr(A) + Tr(B)$. Similarly $Tr(zA) = z\,Tr(A)$. If $\{|\psi_i\rangle\}$ is any orthonormal basis of $\mathcal{H}$ then we have: $Tr(A) = \sum_i \langle\psi_i|A|\psi_i\rangle$. Finally for all $|\psi\rangle$ and $|\phi\rangle$ we have $Tr(A|\psi\rangle\langle\phi|) = \langle\phi|A|\psi\rangle$.

2.2 Postulates of quantum theory ⊙

The presentation of quantum theory will be kept to the minimum : only the postulates are provided. Several key notions such as entanglement, separability, quantum operations, and key companion theorems such as Stinespring's representation theorem, Kraus' representation theorem, purification, UDV decomposition etc. are absent. Although strictly speaking they are not needed in order to follow this thesis, they are the landscape in which this thesis draws a path ; without them it is difficult to understand what it is we are striving for. The density matrix formalism, on the other hand, is explained in some detail, because it is indispensable in order to consider subsystems that are part of a bigger whole.

2.2.1 Upon pure states

Quantum theory is the theory of 'closed systems'. By closed system, we mean absolutely closed, i.e. the sheer interaction of the system with one particle from the outside world may have it to lose its 'quantum behaviour'. Thus quantum theory is usually applied to describe the behaviour of small objects, over short periods of time. One of the foundational principles of quantum theory is the 'superposition principle'. It states that if a quantum system may be observed to take states in S, then it may take states in any of the normal vectors of $\mathcal{H}_S$. This translates into the following postulate.

Postulate 1 (States)
The state of a quantum system is fully described by a normal vector $|\psi\rangle$ in $\mathcal{H}$.

For instance a system that may be observed to take states in $\{0, 1\}$, may actually take states in any of the normal vectors of $\mathcal{H}_{\{0,1\}}$, i.e. any $|\psi\rangle$ of the form $\alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$. This $|\psi\rangle$ is often referred to as a 'superposition' of $|0\rangle$ and $|1\rangle$, with 'amplitudes' α and β.

Since the states are normal vectors of $\mathcal{H}$, it is somewhat natural that evolutions in time should be norm-preserving linear operators over $\mathcal{H}$. This translates into the following postulate.

Postulate 2 (Evolutions)
The evolution of a quantum system in discrete time steps is fully described by a unitary evolution U over $\mathcal{H}$, i.e. if a quantum system has state $|\psi\rangle$, then at the next time step it will have state $U|\psi\rangle$.

Note that in the case when $\mathcal{H}$ is of finite dimension, any unitary operator U can be approximated to an arbitrary precision by a composition (in time with the usual operator composition, and in space with the tensor product) of quantum gates chosen in a universal set, such as $\{\textsc{Cnot}, \mathrm{H} \text{ and } \mathrm{P}\}$. See for instance [34, 108].

Actually quantum theory is not quite just the theory of 'closed systems'. This is because observing a quantum system does require some outside interaction with it, and of course if we were not allowed to observe any of it then quantum theory would be pointless. So the theory describes the way to measure a quantum system. But because observation 'opens up the system' to some extent, the system gets modified by this outside interaction – in quite an abrupt way as we now see.

Postulate 3 (Generalized measurements)
A generalized measurement upon an n-dimensional quantum system is described by a collection $\{M_k\}$ of measurement operators satisfying the completeness relation

$$\sum_k M_k^\dagger M_k = \mathbb{I}.$$

If the quantum system has state $|\psi\rangle$, then the probability that result m occurs is given by

$$p(k) = Tr(M_k^\dagger M_k |\psi\rangle\langle\psi|) = \langle\psi| M_k^\dagger M_k |\psi\rangle.$$

Then state of the system after the measurement is

$$|\psi'\rangle = M_k|\psi\rangle / \sqrt{\langle\psi| M_k^\dagger M_k |\psi\rangle} = M_k|\psi\rangle / \sqrt{p(k)}$$

Observation changes the system. This is a common place about quantum theory. Notice also the huge discrepancy between what can be learnt about a quantum system (some integer k) and what was the full description of the state of a quantum system (some normal vector of $\mathcal{H}$). In the case of $|\psi\rangle$ in $\mathcal{H}_{\{0,1\}}$ we can only ask rough questions such as 'are you $|0\rangle$ or are you $|1\rangle$', whereas $|\psi\rangle$ lives in a continuum of normal vectors of the form $\alpha|0\rangle + \beta|1\rangle$. Worse still we cannot ask that question without altering the state in an irreversible manner and 'collapse' it down to either $|0\rangle$ or $|1\rangle$, in a probabilistic manner.

The tensor product is the canonical way to take two Hilbert spaces and embed them in a bigger one. Hence it is natural that this should be the operation used in order to put two quantum systems aside.

Postulate 4 (Composite systems)
The state space of a composite physical system is the tensor product of the state space of the component physical systems.
Before the two systems have interacted in any manner if we have $|\psi\rangle$ *the state of system* A *and* $|\phi\rangle$ *the state of system* B*, then the joint system has density matrix* $|\psi\rangle \otimes |\phi\rangle$*.*

Consider the state $(|0\rangle + |1\rangle)/\sqrt{2}) \otimes |0\rangle$. By bilinearity this is equal to $(|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle)/\sqrt{2})$. Now consider applying the unitary gate CNOT, which is defined to map $|1\rangle \otimes |0\rangle$ to $|1\rangle \otimes |1\rangle$, $|1\rangle \otimes |1\rangle$ to $|1\rangle \otimes |0\rangle$, and leave $|0\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle$ unchanged. Then the state becomes $(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)/\sqrt{2})$. This is no longer a product state: it can no longer be written as $|\psi\rangle \otimes |\phi\rangle$ for a certain choice of $|\psi\rangle$ and $|\phi\rangle$. The two quantum systems, as they interacted through the CNOT gate, have become 'entangled'. This state lives in $\mathcal{H}^A \otimes \mathcal{H}^B$ and can no longer be thought of as an element of $\mathcal{H}^A \times \mathcal{H}^B$. Fine, but what if the second system was to be discarded, how would we describe the reminder in $\mathcal{H}^A$?

2.2.2 Upon mixed states

In order to consider a subsystem of a larger quantum system, and be able to speak of its state, we need to switch to the density matrix formalism. This formalism also arises naturally when one seeks for a canonical way to mix 'classical' probabilities with 'quantum' amplitudes.

Ensembles and canonicity issues

Say we want to mix 'classical' probabilities with 'quantum' amplitudes. A legitimate way to do this is to denote by $\{(p_0, |\psi_0\rangle), \ldots, (p_r, |\psi_r\rangle)\}$ the state of a quantum system which has state $|\psi_0\rangle$ with probability p_0, state $|\psi_1\rangle$ with probability p_1,... This works well and is called an 'ensemble state'. The principal weakness of ensemble states is their non-canonicity. That is, we may have two different ensemble states which are physically indistinguishable, and hence 'equal for all purpose'.

Example 1 *The ensembles* $\{(3/4, |0\rangle), (1/4, |1\rangle)\}$ *and* $\{(1/2, \sqrt{3/4}|0\rangle + \sqrt{1/4}|1\rangle), (1/2, \sqrt{3/4}|0\rangle - \sqrt{1/4}|1\rangle)\}$ *are undistinguishable physically.*

To prove these statements we need the theoretical tools provided next. Meanwhile, a challenge would be to find a generalized measurement $\{M_k\}$ which discriminates these ensembles (i.e. such that the $p(k)$ vary from one ensemble to the other) : it turns out that this is impossible.

Density matrices and canonicity

We now describe a more canonical formalism for 'mixing' 'classical' probabilities with 'quantum' amplitudes, but this implies changing the basic mathematical objects which we use in order to describe the states, moving from vectors to operators. As a consequence we need to rephrase all the postulates, as proposed by Von Neumann [137]. Only after that will we be able to show the equivalence between ensemble states and their postulates on the one hand, and density matrices and their postulates on the other hand.

Postulate 1'
The state of an n-dimensional quantum system is fully described by its density matrix ρ, which its a positive unit trace operator over $\mathcal{H}$.

Postulate 2'
The evolution of a quantum system in discrete time steps is fully described by a unitary evolution U over $\mathcal{H}$. I.e. if a quantum system has density matrix ρ, then at the next time step it will have density matrix $U\rho U^\dagger$.

Postulate 3'
A generalized measurement upon an n-dimensional quantum system is described by a collection $\{M_k\}$ of measurement operators $M_k \in M_{m\times n}(\mathbb{C})$ satisfying the completeness relation

$$\sum_k M_k^\dagger M_k = \mathbb{I}.$$

If the quantum system has density matrix ρ, then the probability that result k occurs is given by

$$p(k) = Tr(M_k^\dagger M_k \rho).$$

Then state of the system after the measurement is

$$\rho' = M_k \rho M_k^\dagger / Tr(M_k^\dagger M_k \rho) = M_k \rho M_k^\dagger / p(k)$$

Postulate 4'
The state space of a composite physical system is the tensor product of the space space of the component physical systems.

Before the two systems have interacted in any manner, if we have ρ^A is the density matrix of system A and ρ^B is the density matrix of system B, then the joint system has density matrix $\rho^A \otimes \rho^B$.
If a bipartite system has density matrix ρ^{AB} we call ρ^A the reduced density matrix of A, which corresponds to ignoring system B and whatever may happen to it. We have

$$\rho^A = Tr_B(\rho^{AB})$$

where $Tr_B(.)$ is defined to take $\tau^A \otimes \sigma^B$ into $Tr(\sigma)\tau$ and is extended to all other matrices over the tensor space by linearity.

Embedding

We now look at the equivalence between ensemble states and density matrices.

Lemma 2.2
Consider an ensemble state $E = \{(p_0, |\psi_0\rangle), \ldots, (p_r, |\psi_r\rangle)\}$, its corresponding density matrix $\rho_E = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, and a generalized measurement $\{M_k\}$. Postulate 3' on ρ_E yields the same measurement statistics as Postulate 3 on E. Moreover suppose outcome k occurs. Consider E' the ensemble state as given from E by Postulate 3, and its corresponding density matrix $\rho_{E'}$. Consider $(\rho_E)'$ the post-measurement density matrix as given from ρ_E by Postulate 3'. We have $(\rho_E)' = \rho_{E'}$.

Proof.

$$\begin{aligned}
p(k) &= \sum_i p_i \mathrm{Tr}(M_k^\dagger M_k |\psi_i\rangle\langle\psi_i|) = \mathrm{Tr}(M_k^\dagger M_k \sum_i p_i |\psi_i\rangle\langle\psi_i|) \\
&= \mathrm{Tr}(M_k^\dagger M_k \rho_S) \\
\rho_{E'} &= \sum_i p(i|k) \frac{M_k|\psi_i\rangle\langle\psi_i|M_k^\dagger}{p(k|i)} = \sum_i p_i \frac{M_k|\psi_i\rangle\langle\psi_i|M_k^\dagger}{p(k)} \\
&= \sum_i p_i \frac{M_k|\psi_i\rangle\langle\psi_i|M_k^\dagger}{\mathrm{Tr}(M_k^\dagger M_k \rho)} = \frac{M_k \rho M_k^\dagger}{\mathrm{Tr}(M_k^\dagger M_k \rho)} \\
&= (\rho_E)'
\end{aligned}$$

□

Physical interpretation. The density matrix $\rho = |\psi\rangle\langle\psi|$ is an alternative, equivalent notation to the state vector $|\psi\rangle$, but this representation has the advantage of being able to hold probability distributions over states, i.e. ρ_1

with probability p_1 and ρ_2 with probability p_2 has density matrix $p_1\rho_1 + p_2\rho_2$. This representation is canonical in the sense that if $\rho \neq \sigma$, then there exists a measurement yielding different measurement statistics upon these states.

Discussion : causality and the partial trace

Lemma 2.3 *Consider ρ a bipartite state and a measurement $\{M_k\}$ acting solely upon the second subsystem. We have:*

$$Tr_B(\rho) = Tr_B(\sum_k (\mathbb{I} \otimes M_k)\rho(\mathbb{I} \otimes M_k)^\dagger)$$

Proof Say $\rho = \sum_{ij} \alpha_{ij} A_i \otimes B_j$.

$$\begin{aligned}
\mathrm{Tr}_B(\sum_k (\mathbb{I} \otimes M_k)\rho(\mathbb{I} \otimes M_k)^\dagger) &= \sum_{ij} \alpha_{ij} \mathrm{Tr}_B(\sum_k A_i \otimes M_k B_j M_k^\dagger) \\
&= \sum_{ij} \alpha_{ij} A_i \otimes \mathrm{Tr}(\sum_k M_k B_j M_k^\dagger) \\
&= \sum_{ij} \alpha_{ij} A_i \otimes \mathrm{Tr}(\sum_k M_k^\dagger M_k B_j) \\
&= \sum_{ij} \alpha_{ij} A_i \otimes \mathrm{Tr}(B_j) \\
&= \mathrm{Tr}_B(\rho)
\end{aligned}$$

Physical content. Hence a quantum operation acting upon subsystem B cannot change the reduced density matrix of system A. This means that no 'spooky effect at a distance' of quantum mechanics can help communicate information faster than light.
Though it is true that $(1/\sqrt{2})(|00\rangle + |11\rangle)$, when measured in the canonical basis of the second subsystem, collapses to either $|00\rangle$ or $|11\rangle$, hereby instantaneously modifying the first system, it is also true that the reduced density matrix of system 1 remains $\mathbb{I}/2$ in the absence of the knowledge of the measurement outcome.
Though very different in its formulation, quantum mechanics remains coherent with special relativity in this sense : a local quantum operation upon B does not jeopardize causality between A and B. We could call this well-known lemma 'Locality implies causality'. One of the main contributions of this thesis is to deepen our understanding of the interplay between quantum theory and relativity, by demonstrating something which roughly speaking could be thought of as a converse to the above lemma, but in a more general setting.

Chapter 3

Cellular Automata

The sciences do not try to explain, they hardly even try to interpret, they mainly make models. By a model is meant a mathematical construct which, with the addition of certain verbal interpretations, describes observed phenomena. The justification of such a mathematical construct is solely and precisely that it is expected to work.

—*John Von Neumann*

We provide a rapid introduction to the theory of Cellular Automata (CA), focusing on those results which were influential in the development of Quantum Cellular Automata (QCA). In particular we insist upon the three different ways to define a CA, namely in terms of a local transition rule, a partitioned or block representation, or as a shift-invariant continuous function. We also discuss the influence of the chosen space of configurations upon these presentations. We discuss universal CA.

The field of Cellular Automata (CA) has far too many facets[1] for us to attempt a review. The thorough reader is recommended one of the many good introductions [44, 45, 81]. By contrast this Chapter will focus only on those theoretical results about CA which have had a strong influence in the development of Quantum Cellular Automata (QCA). Often we will only enumerate those results without proof. This is because they are of lesser interest for us when they do not have a known quantum counterpart, and when they do we prefer to provide the more general proof in the quantum setting, later in the thesis.

3.1 Motivations ⊙⊛

Cellular automata consist in an array of identical cells, each of which may take one in a finite number of possible states. The whole array evolves in discrete time steps by iterating a function Δ. Moreover this global evolution Δ is shift-invariant (it acts everywhere the same) and causal (information cannot be transmitted faster than some fixed number of cells per time step).

This model of computation is clearly physics-like [91], in the sense that it shares some fundamental symmetries of theoretical physics : homogeneity (invariance of the physical laws in time and space), causality, and often reversibility as we shall see. The way in which one programs cellular automata is also very physics-like, as often we construct 'signals'/'particles' and have them to 'interact'/'collide' with one another, plus we like to observe all of these things happening in a 'space-time diagrams', etc. Often demonstrating that a CA is universal for computation, for instance in the case of Conway's Game of Life, feels very much like building an entire computer from scratch, with wires, gates etc., in the 'virtual world' of the CA [50].

There are many models of computation around. Some of them are capable of modelling spatially distributed computation, as data exchanging processes (CCS, π-calculus...). But in such models space has nothing to do with space as we know it (with some places closer than other, kind of $3D$, etc.). They are not adequate in order to reason about simple space-sensitive synchronization problems such as the 'Firing Squad' [102, 94]. In contrast, CA model spatially distributed computation with space as we know it [131], and therefore they constitute a framework for studying and proving properties about such systems – by far the most established. Although there are

[1]The string 'Cellular Automata' gets 2740 citations in CiteSeer^X, 52100 in Google Scholar, and a Google rank of 637000.

some alternative models emerging, seeking for instance to formalize recent works on space-time computation, such as [55, 32]. Even then the influence of CA is strong [51]. CA have also been studied as possible architectures for real-world computers for instance in [131, 84]. This sort of research may soon get back into fashion as Moore's law will hit the quantum barrier and manufacturers be forced to switch to multicore architectures – and face the many timing problems that come along.

But CA are not just a model of computation. Born amongst theoretical physicists such as Ulam and Von Neumann [138], they are soon conceived as a possible model for particle physics, fluids, and the related differential equations. There are a lot of results on this approach up to this day, often under the name of Lattice-gas cellular automata [147, 143, 42, 117].

More generally, CA are one of the main theoretical tools of 'complex sciences', where one studies the emergence of complex, global behaviours as arising from simple local interactions [144]. There, CA have proved useful for modelling an incredible variety of things [145] ranging traffic jams [106] to demographics and regional development or consumption [38, 141]. But let us come back to sheer mathematics.

3.2 Definitions, properties and structures ⊙

We will now explain three different ways to present a CA, namely in terms of a local transition rule, a partitioned or block representation, or as a shift-invariant continuous function. Whenever relevant we will deal with two cases : CA over infinite configuration and CA over finite unbounded configurations. Why? Well when we later seek to quantize CA into QCA we shall see that this cannot be done over infinite configurations (or at least not in the standard formalism of quantum theory). So QCA are quantizations of finite configurations. Yet paradoxically it will turn out that their properties are much more alike those of CA over infinite configurations.

3.2.1 X : Local transition rule, global properties

Historically this presentation precedes the other two, hence it stands out as being the very definition of CA. For simplicity the definitions we provide are for one-dimensional CA, but the generalization to higher dimensions is straightforward. For simplicity also the definitions we provide are for radius

half CA (where the neighbourhood is fixed to be $\{0,1\}$), but since any CA can be put into that form this is without loss of generality [71, 33, 113]. In any case our discussion applies to CA in general.

Infinite case

In 1D the infinite configurations are amongst biinfinite words ${}^{\omega}\Sigma^{\omega}$.

Definition 3.1 (Infinite configurations)
An infinite configuration *c over Σ is a function $c : \mathbb{Z}^n \longrightarrow \Sigma$, with $(i_i, \ldots, i_n) \longmapsto c(i_i, \ldots, i_n) = c_{i_i \ldots i_n}$. The set of all infinite configurations over Σ will be denoted $\mathcal{C}_\infty^\Sigma$, of just $\mathcal{C}_\infty$ if Σ is fixed.*

The state of each pair of adjacent cells at time t determines the state of one cell at time $t+1$.

Definition 3.2 (CA over infinite configurations)
A cellular automaton over infinite configurations is defined by a function $\delta : \Sigma \times \Sigma \to \Sigma$ ("the local transition rule").
The induced global evolution *of the CA is as follows:*

$$\begin{aligned} \Delta : \mathcal{C}_\infty &\to \mathcal{C}_\infty \\ c &\mapsto \Delta(c) \\ \Delta(c) &= \bullet_{i \in \mathbb{Z}}\, \delta(c_i, c_{i+1}) \end{aligned}$$

where $\bullet$ stands for concatenation.

Finite unbounded case

In 1D finite unbounded configurations are of the form $\ldots qqwqq \ldots$.

Definition 3.3 (Finite unbounded configurations)
A (finite unbounded) configuration *c over Σ is a function $c : \mathbb{Z}^n \longrightarrow \Sigma$, with $(i_i, \ldots, i_n) \longmapsto c(i_i, \ldots, i_n) = c_{i_i \ldots i_n}$, such that there exists a (possibly empty) interval I verifying $(i_i, \ldots, i_n) \notin I \Rightarrow c_{i_i \ldots i_n} = q$. The set of all finite configurations over Σ will be denoted $\mathcal{C}_f^\Sigma$, of just $\mathcal{C}_f$ if Σ is fixed.*

Then the evolution of the CA must not send a finite configuration into an infinite one.

Definition 3.4 (CA over finite unbounded configurations)
A cellular automaton over finite unbounded configurations is defined by a

function $\delta : \Sigma \times \Sigma \to \Sigma$ *("the local transition rule").*
Moreover δ *must verify the quiescent stability condition:* $\delta(q, q) = q$.
The induced global evolution *of the CA is as follows:*

$$\begin{aligned} \Delta : \mathcal{C}_f &\to \mathcal{C}_f \\ c &\mapsto \Delta(c) \\ \Delta(c) &= \bullet_{i \in \mathbb{Z}} \, \delta(c_i, c_{i+1}) \end{aligned}$$

where $\bullet$ *stands for concatenation.*

Injectivity, surjectivity, reversibility

We see from the above definitions that the global evolution Δ is induced by a local transition rule δ in a straightforward way. Sometimes however it can be quite difficult to see what global properties are induced by what local transition rule. For instance knowing when δ induces a Δ that is injective, surjective or bijective is a hard question, which has received much attention. Moreover in case it is bijective the question whether the inverse function Δ^{-1} can itself be casted as a CA is again not as straightforward as it may seem. Actually it is quite surprising how much of the literature is dedicated to the study of these reversible cellular automata (RCA) - when reversibility is not so much of a crucial feature to have in classical computation [132]. A frequently encountered argument states that all consumption-less, zero-heat micro-mechanical device need be reversible. Another states that CA are physics-like models of computations, and hence they ought to be reversible [80]. But tracing back the origins [85] of these arguments, one finds essentially quantum physical considerations.

Let us summarize a few of these results, but the reader can refer to [81] for a more complete account.

- Injectivity, surjectivity, bijectivity and reversibility are all decidable for one-dimensional CA [3, 127]. But these properties become undecidable for higher-dimensional CA [77, 78]. This is true whether on finite unbounded or infinite configurations.

- Surjectivity of CA over infinite configurations is equivalent to injectivity over finite unbounded configuration [101, 104].

- Bijectivity implies reversibility for CA over infinite configurations [70], but nor over finite configurations.

Evolutions in quantum theory are unitary, and hence bijective. The fact that bijectivity is not even decidable for two-dimensional CA is a serious concern if we want to be able to define QCA in a rigorous and general manner – a question raised in [68]. Fortunately for us there are other presentations of CA.

3.2.2 Y : Partitioned and block representations

Another way to present CA is as a circuit, infinitely repeating across space in a translation-invariant manner, describing how to map one configuration into another. Of course if we allow for non-reversible gates in our circuit as well as cell (wire) duplication (fan-out), this is trivial and just comes back to the original definition : δ could just be seen as a $2\log_2(|\Sigma|)$ to $\log_2(|\Sigma|)$ bits gate, applied to every possible pair of adjacent cells. But if the perspective is to quantize CA in to QCA, we would like to disallow non-reversible gates as well as cell duplication [146]. These representations of CA were proposed by Margolus [91], hence they are sometimes referred to as 'Margolus neighbourhoods' or 'Margolus block partioning'. But is this block representation is applicable to any CA whose global evolution Δ is bijective? Let us see what the litterature has to say.

The infinite case

In the infinite case if a CA is bijective, it is reversible. In [79], Kari has shown that any one-dimensional or two-dimensional Reversible CA (RCA) can be expressed a composition of reversible gates (which are referred to as 'blocks' or 'permutations'), together with some partial shifts. In two-dimensions the proof is quite involved, the representation requires three layers of blocks, and it has been proved that this cannot be brought down to a two-layered block representation [80]. In higher dimensions we do not know if such block representations exist at all : this is an open problem. The only thing we know is that if such a block representation exists for n-dimensional CA, it needs have no more than $n+1$ layers of these blocks [80].

However maybe we do not ask for an exact representation, but are willing to encode our original cells into some larger ones (or equivalently to interleave some ancillary cells), as proposed in [52]. Then a relatively simple construction [80] shows that even n-dimensional RCA admit a two-layered block representation. But really what we are doing then is simulating the original RCA in a way which preserves the spatial layout of cells, with another, simpler RCA that we know admits a two-layered block representation.

In this sense the intrinsically universal RCA [53] also does the job. More on intrinsic universality later in this chapter.

Two layered block representations, in the particular case when these two layers are the same (only shifted), are called Partioned Cellular Automata. These have been studied extensively for instance in [103, 72].

The finite unbounded case

Bijectivity does not imply reversibility in the finite unbounded case. This is to say that the inverse function Δ^{-1} may not a cellular automata. Why? Shift-invariance of course will never be a problem, but causality is the problem. Now if Δ^{-1} is not even causal, this removes all hopes of having a block representation. Let us provide the reader with a well-known example of this for concreteness[2].

Example 2 (mXOR CA)
Let $\mathcal{C}_f$ be the set of finite configurations over the alphabet $\Sigma = \{q, 0, 1\}$. For all x, y in Σ Let $\delta(q, x) = q$, $\delta(x, q) = x$, and $\delta(x, y) = x \oplus y$ otherwise. Then $\Delta : \mathcal{C}_f \longrightarrow \mathcal{C}_f$ is the function mapping $c = \ldots c_{i-1}c_ic_{i+1}\ldots$ to $c' = \ldots \delta(c_{i-1}, c_i)\cdots\delta(c_i, c_{i+1})\ldots$.

The mXOR CA is clearly shift-invariant, and causal in the sense that the state of a cell at $t+1$ only depends upon 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. In other words the antecedent always exists (surjectivity) and is uniquely derived (injectivity) from left till right. But the mXOR CA is not reversible. Indeed for some large zone of zeroes $\ldots 000000000\ldots$ we cannot know whether the antecedent 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. For this same reason the mXOR does not have a block representation.

Actually, this is again a concern for us. When we seek to quantize CA into QCA, we will take those 'classical' finite unbounded configurations as a basis for the vectorial space of 'quantum configurations'. Will this entail that QCA can also be bijective-not-reversible? And why is it that things work out for infinite configurations and not for finite configurations, anyway? Next we look into this second question.

[2]We thank Jacques Mazoyer for pointing it out.

3.2.3 Z : Axiomatic route (⊙⟁⊛)

The two above presentations of classical CA have raised concerns on how be able to define QCA in a rigorous and general manner. Indeed because bijectivity of a CA is undecidable from its local transition rule, we would maybe have liked to define CA directly in terms of their block representation. But on the other hand we know that what seems to be their direct classical counterpart, i.e. bijective CA over finite unbounded configurations, do not even admit to a block representation. Hence we are left to consider the axiomatic presentation of CA.

The infinite case

In what follows we explain the well-known Curtis-Lyndon-Hedlund Theorem[70], using only elementary arguments. We endow the space of infinite configurations with the following metric. Intuitively two configurations are close to one another when the central part they have in common is large.

Definition 3.5 (Metric)

$$\begin{aligned} \textit{The function } d(.,.) : \mathcal{C} \times \mathcal{C} &\longrightarrow \mathbb{R}^+ \\ (c,c') &\mapsto d(c,c') = 0 < \quad \textit{if } c = c' \\ (c,c') &\mapsto d(c,c') = 1/2^k \\ &\qquad \textit{with } k = \min\{i \in \mathbb{N} \mid c_{-i\ldots i} \neq c'_{-i\ldots i}\} \end{aligned}$$

is a metric. It is such that $c, c' \in \mathcal{C}_\infty$ *and* $\varepsilon > 0$ *we have (with* $n = \lfloor \log_2(\varepsilon) \rfloor$*):*

$$d(c,c') < \varepsilon \Leftrightarrow c_{-n\ldots n} = c'_{-n\ldots n}.$$

Actually it is an ultrametric i.e. for all $a, b, c \in \mathcal{C}_\infty$, $d(a,c) = \max\{d(a,b), d(b,c)\}$. *Moreover it makes* $\mathcal{C}_\infty$ *compact.*

Proof.
[Non-negativity, symmetry, identity of indiscernibles] are obvious.
[Equivalence]

$$\begin{aligned} d(c,c') < \varepsilon &\Leftrightarrow d(c,c') = 1/2^k \text{ with } k \in \mathbb{N} \wedge 1/2^k < \varepsilon \\ &\Leftrightarrow k = \min\{j \in \mathbb{N} \mid c_{-i\ldots i} \neq c'_{-i\ldots i}\} \wedge 1/2^k < \varepsilon \\ &\Leftrightarrow_{l=k-1} \; c_{-l\ldots l} = c'_{-l\ldots l} \text{ with } l \in \mathbb{N} \wedge 1/2^{l+1} < \varepsilon \\ &\Leftrightarrow c_{-l\ldots l} = c'_{-l\ldots l} \text{ with } l = \lfloor -\log_2(\varepsilon) \rfloor. \end{aligned}$$

[Ultrametricity] Consider k such that $1/2^k = d(a,c)$ and l such that $1/2^l = d(a,b)$. By definition of the metric a, c differ only after index k and a, b differ only after index l. By supposition $k \leq l$ so that b, c differ only after index k. But then $d(b,c) = 1/2^k$ which is $d(a,c)$.
[Triangle inequality] is obvious from the ultrametricity.
[Compacity]. We need to show that any sequence $(c^{(k)})_{k\in\mathbb{N}}$ of configurations has a convergent subsequence. We construct the limit c recursively as follows:
$c_0 = \sigma$ with some $\sigma \in \Sigma$ such that $\#\{k \,|\, c_0^k = \sigma\} = \infty$.
$c_{-i-1\ldots i+1} = \sigma_l c_{-i\ldots i} \sigma_r$ with some $\sigma, \sigma' \in \Sigma$ such that $\#\{k \,|\, c^k_{-i-1\ldots i+1} = \sigma_l c_{-i\ldots i}\sigma_r\} = \infty$.
(An alternative proof path is to show that $d(.,.)$ is the product metric of the metric of the cells. Since the metric of the cells is compact the product metric is compact via Tychonoff's theorem.) □

Definition 3.6 (Continuity)
A function $F : \mathcal{C}_\infty \longrightarrow \mathcal{C}_\infty$ is continuous if and only if for all $c \in \mathcal{C}_\infty$ and $\varepsilon > 0$, there exists $\eta > 0$ such that for all $c' \in \mathcal{C}_\infty$:

$$d(c,c') < \eta \;\Rightarrow\; d(F(c), F(c')) < \varepsilon.$$

In other words a function $F : \mathcal{C}_\infty \longrightarrow \mathcal{C}_\infty$ is continuous if and only if for all $c \in \mathcal{C}_\infty$ and $n \in \mathbb{N}$, there exists $m \in \mathbb{N}$ such that for all $c' \in \mathcal{C}_\infty$:

$$c_{-m\ldots m} = c'_{-m\ldots m} \;\Rightarrow\; F(c)_{-n\ldots n} = F(c')_{-n\ldots n}.$$

Definition 3.7 (Uniform continuity)
A function $F : \mathcal{C}_\infty \longrightarrow \mathcal{C}_\infty$ is uniform continuous if and only if for all $\varepsilon > 0$, there exists $\eta > 0$ such that for all $c, c' \in \mathcal{C}_\infty$:

$$d(c,c') < \eta \;\Rightarrow\; d(F(c), F(c')) < \varepsilon.$$

In other words a function $F : \mathcal{C}_\infty \longrightarrow \mathcal{C}_\infty$ is continuous if and only if for all $n \in \mathbb{N}$, there exists $m \in \mathbb{N}$ such that for all $c, c' \in \mathcal{C}_\infty$:

$$c_{-m\ldots m} = c'_{-m\ldots m} \;\Rightarrow\; F(c)_{-n\ldots n} = F(c')_{-n\ldots n}.$$

Notice that rephrased in this manner, uniform continuity is really just a synonym for causality, i.e. the fact that information does not propagate faster than a fixed speed bound. So what is continuity on about, in terms of speed of information? Clearly it expresses a form of relaxed causality, where information does not propagate faster than a certain speed bound... but

this speed bound is allowed to vary. The question is : is there, still, a maximal speed of information under mere 'continuity'? If so this would equate continuity and uniform continuity. Here is a sufficient condition for that.

Theorem 3.1 (Heine)
If a function $F : \mathcal{X} \longrightarrow \mathcal{Y}$ is continuous and X is compact then F is uniformly continuous.

Proof. By contradiction. Say there exists $\varepsilon > 0$ such that for all η there exists c, c' such that $d(c, c') < \eta$ but $d(F(c), F(c')) \geq \varepsilon$. Take such an ε. Then for all $n \in \mathbb{N}$ one may choose c_n, c'_n such that

$$(i) \quad d(c_n, c'_n) < 1/n \quad \text{and} \quad (ii) \quad d(F(c_n), F(c'_n)) \geq \varepsilon.$$

Since the metric is compact we can extract from (c_n) a subsequence (c_{k_n}) which converges to some limit c. Condition (i) entails that (c'_{k_n}) also converges to c. Now by continuity of F there ought be $\eta > 0$ such that for all c':

$$d(c, c') < \eta \;\Rightarrow\; d(F(c), F(c') < \varepsilon/2.$$

But this is no longer the case. Indeed when taking n sufficiently large one has both $d(c, c_{k_n}) < \eta$ and $d(c, c'_{k_n}) < \eta$, but condition (ii) entails that $d(F(c_{k_n}), F(c))$ or $d(F(c'_{k_n}), F(c))$ is greater than $\varepsilon/2$. □

Theorem 3.2 (Curtis, Lyndon, Hedlund)
A function $F : \mathcal{C}_\infty \longrightarrow \mathcal{C}_\infty$ is continuous and shift-invariant if and only if it is the global evolution of a Cellular Automata.

Proof.
[⇒] Say F is continuous. From Theorem 3.1 we have that F is uniform continuous and so for all $n \in \mathbb{N}$ there exists $m \in \mathbb{N}$ and $f : \Sigma^m \longrightarrow \Sigma^n$ such that $[F(c)_{-n\ldots n} = f(c_{-m\ldots m})]$. Take $n = 0$ and fix the corresponding m. We have $F(c)_0 = f(c_{-m\ldots m})$, and by shift-invariance $F(c)_i = f(c_{-m+i\ldots m+i})$.
[⇐] Say $F(c)_i = f(c_{-m+i\ldots m+i})$. Consider some $\varepsilon > 0$, and let $k = \lfloor \log_2(\varepsilon) \rfloor$, $l = n + m$ and $\eta = 1/2^l$. Then for all $c, c' \in \mathcal{C}_\infty$ the condition $d(c, c') < \eta$ implies $c_{-l\ldots l} = c'_{-l\ldots l}$, which in turn implies $F(c)_{-k\ldots k} = F(c)_{-k\ldots k}$ as they are both equal to $f(c_{-m-n\ldots m-n})\cdots f(c_{-m+n\ldots m+n})$. Hence $d(F(c), F(c')) < \varepsilon$ and we have proved uniform continuity, which is stronger than continuity. □

Really what this theorem is saying is that CA are causal, shift-invariant functions. But instead of calling them 'causal' (a.k.a 'uniformly continuous'), the theorem just calls them 'continuous'. As we have seen continuity is a weaker condition than uniform continuity, but the two are made equivalent

through the compactness of the underlying metric. The reason why it is preferable to call then 'continuous' and not 'uniform continuous' is because this lets you use ready-made theorems from analysis, such as the fact that the inverse of a continuous function is a continuous function... hence the fact that bijective CA over infinite configurations are reversible!

The finite case

We can define the same metric for $\mathcal{C}_f$ as we did on $\mathcal{C}_\infty$. The metric then has all the same properties but compactness. Indeed the metric is not even complete, for instance consider the series of finite configurations $(c^{(k)})_{k\in\mathbb{N}}$ with $c^{(k)} = \ldots qq0^kqq\ldots$, centered on the first 0 say. This tends to $c = \ldots qq00\ldots$ but this is not in $\mathcal{C}_f$. As a consequence Heine's theorem no longer helps, i.e. there are continuous functions which are not uniformly continuous. The Curtis-Lyndon-Hedlund theorem must be played down as a consequence to take the following form.

Theorem 3.3
A function $F : \mathcal{C}_f \longrightarrow \mathcal{C}_f$ is uniformly continuous and shift-invariant if and only if it is the global evolution of a Cellular Automata.

Proof. Same as in the infinite case except that in the [⇒] direction we directly assume uniform continuity. □

To show that this is as good as it gets consider the following. Take $\Sigma = \{q, 0, 1\}$ and a function $F : \mathcal{C}_f \longrightarrow \mathcal{C}_f$ which parallely rewrites all subwords qwq (with $w \in \Sigma^*$) into $qw\bigoplus_i w_i$ (with $\oplus$ the exclusive or). In other words the function computes the xor of the bits of every binary strings it meets, and appends the result. The function is clearly shift-invariant: there is no preferred position in the evaluation of this function. It is also clearly continuous: for all configuration c and for all n we can always take m so that $-m\ldots m$ includes both $-n\ldots n$ and the interval domain of c, and have that for all c' such that $c'_{-m\ldots m} = c_{-m\ldots m}$, $F(c)_{-m\ldots m} = F(c')_{-m\ldots m}$. But clearly this is not a uniformly continuous function: the suitable m depends not only on the n but on c. And clearly this is not a cellular automata.

So, what this theorem is saying is that CA are causal, shift-invariant functions. The example right-above shows that over finite configurations we really need to call them 'causal' (a.k.a 'uniformly continuous'), and not just 'continuous', because the two are unequivalent given the lack of compactness of the underlying metric. Whilst this is still a solid axiomatization of CA over finite configurations, some results no longer follow. For instance, it is no longer the case that the inverse function of a causal function is a causal function, as discussed already through Example 2. Fixing this issue of

reversibility over finite unbounded configurations will be a major challenge when seeking to quantize CA into QCA.

3.3 Universalities ⊙

The most popular cellular automaton is Conway's 'Game of Life', a two-dimensional CA which has been proven to be universal for computation – in the sense that any algorithm can be encoded within its initial state and then be run by the cellular automaton's evolution. This was accomplished by simulating any Turing Machine (TM) within the automaton, and since Turing machines have long been regarded as pretty much the best definition of 'what an algorithm is' in classical computer science, this could have meant the end of the story to many people. Yet researchers in CA have always been looking for more than just running any algorithm, seeking to run distributed algorithms in a distributed manner, model some other phenomena together with their spatial structure, or make use of the spatial parallelism which is inherent to the model – as these are the features which are modelled by CA and not by Turing machines. And hence they have had to come back [24, 2, 93, 50] to the original meaning of the word 'universal', namely the ability for one instance of a computational model to be able to simulate all other instances of the very same computational model. The introduction of a partial order on CA via the notion of grouping [95] and subsequent generalizations of this notion [110, 129], have led to elegant and robust definitions of intrinsic universality, as an extremum of this partial order. Nowadays there is an impressive number results about intrinsically universal CA as reviewed for instance in [45, 110, 56] – i.e. results on cellular automata that are capable of simulating all others efficiently and directly. (Incidentally of course they can also simulate those CA which are capable of simulating the Turing machine.). In the non-reversible case some of the best constructions are given in [109, 111]. Closer to our setting there are, even, intrinsic universal Reversible CA constructions by Durand-Löse [53, 54]. Notice that the paper on intrinsic universal Reversible CA in more-than-one-dimensions came out before that in one-dimension, because the one-dimensional case is harder; due to the lack of space! (E.g. to implement wire-crossings). Notice also that the difficulty is to have an n-dimensional reversible CA simulate all other n-dimensional reversible CA and not, say, the $(n-1)$-dimensional reversible CA – otherwise we could use a history-keeping-dimension as in Toffoli [130].

We have seen how CA are not only a physics-like model of computation, but also a computer-science-like model of physical phenomena. Plus we have given an overview of the rich mathematical structure they have. To quite

some extent one can view this thesis as a port / generalization of several of these results to the quantum regime. We have also hinted at a few difficulties awaiting for us along that path.

Chapter 4

Quantum Cellular Automata

I think that modern physics has definitely decided in favor of Plato. In fact the smallest units of matter are not physical objects in the ordinary sense; they are forms, ideas which can be expressed unambiguously only in mathematical language.

—Werner Heisenberg,
as quoted in The New York Times Book Review, 8^{th} of March 1992.

We explain the concept of Quantum Cellular Automata, and go through the literature around that concept, discussing on criteria such as unitarity, causality, generality and operationality. Expanding upon the more recent axiomatic approach [120] we introduce the wider concept of unitary causal operators, and prove two fundamental properties about them. This leads us to a general, unitary and causal axiomatic definition of Quantum Cellular Automata – but operationality is left open in this chapter.

We mentionned that Von Neumann provided us with the modern axiomatization of quantum theory in terms of the density matrix formalism [137] in 1955, and the CA model of computation [138] in 1966 – but he did not bring the two together. Feynman did [60] in 1986, just as he was inventing the concept of a Quantum Computer. Besides the historical reason of wanting to continue the work of these visionnary scientists, let us enumerate the motivations that have brought people from different communities to the study of QCA (the first two are the original ones by Feynman, the last two have been expanded upon in Chapter 1) :

- *Implementation perspective.* QCA may prove an important path to realistic implementations of quantum computers – mainly because they eliminate the need for an external, classical control over the computation and hence the principal source of decoherence. This route is continuously under investigation [62, 86, 26, 133, 140, 136, 125, 126, 36, 105].

- *Simulation perspective.* Quantum computers were invented first as a mean to simulate efficiently other quantum physical systems – and this remains perhaps one of the most likely applications of quantum computation. But actually it may not be all that easy to encode the theoretical description of the quantum physical system into the quantum computer in a relevant manner, i.e. so that the quantum computer can provide an accurate and efficient simulation. QCA constitute a natural theoretical setting for this purpose, in particular via the works on Quantum Lattice-Gas Automata [128, 28, 98, 100, 30, 29, 59, 96, 135, 89].

- *CA perspective.* We have seen that one-dimensional CA consist of a line of cells, each of which may take one in a finite number of possible states, and evolving in discrete time steps according to a local transition rule, applied synchronously and homogeneously across space. Hence they account for many of the symmetries of physics. Because CA are a physics-like model of computation (a term coined by Margolus in [91]) it seems very natural to study their quantum extensions (and so he did in [92]).

- *Models of computation perspective.* Shaken by the avent of quantum computation theoretical computer science continues to wonder about 'What is a computer, ultimately?'. QCA provide a model of quantum computation which, just like CA, takes into account space as we know it. Hence they constitute a framework to model and reason about problems in spatially distributed quantum computation.

- *Theoretical physics perspecive.* QCA could provide helpful toy models for theoretical physics, as was also advocated for instance in [87], e.g. by providing bridges between computer science notions and modern theoretical physics – such as universality.

The field of Quantum Cellular Automata (QCA) is rapidly growing[1], but it should still possible to write a relatively thorough theory-oriented overview. Reviews of QCA are also found in [68, 4, 41, 142].

4.1 Early approaches ⊙⟁⊛

There are many cases of models of classical computation that have been ported to the realm of quantum computation, for instance Turing Machines (TM) yielding Quantum Turing Machines (QTM) [46, 27, 114], etc. When there is a unique definition of a concept X, and we need to quantize it into a concept QX, this usually is not so difficult. But think of a situation where you would have three equivalent definitions X, Y and Z of an exact same concept, and these quantize into three *inequivalent* definitions QX, QY, QZ. Which one should you choose?
As we discussed in Chapter 3, cellular automata can be presented from three different angles:

- their original definition is in terms of a local transition rule δ, whose repeated application across space yields the global evolution Δ (X);
- their partitioned and block representations (Y);
- their defining properties, namely continuous shift-invariant bijective maps (Z).

Following the short history of QCA we will examine the quantizations QX, QY and QZ in turn, before we answer the above question. This does not quite follow the chronological order, but almost.

4.1.1 QX : LQCA, CQCA

Linear QCA (LQCA)

One of the first well-studied notion of QCA was introduced by Watrous [139], and was later referred to as Linear Quantum Cellular Automata (LQCA) by

[1]The string 'Quantum Cellular Automata' fetches 26 papers on the ArXiv, there are about 60 papers that we know of, yet Citeseer^X yields 110 citations, Google Scholar gives 1690, and the Google Rank is 111000.

Dürr, Santha, Lêthanh [57, 58]. It corresponds to the natural quantization of the original presentation of classical CA, i.e. the one in terms of a local transition rule which is repeatedly applied across space (X). It goes as follows. First one needs to consider the set of finite unbounded configurations as in the classical setting (see Definition 3.3). These are all the possible basis states of the entire LQCA, but of course in general the states of a LQCA may be a superpositions of basis states, so we have:

Definition 4.1 (superpositions of (finite) configurations)
A superposition of (finite) configurations *is a normalized element of $\mathcal{H}_{\mathcal{C}_f}$, the Hilbert space of configurations.*

This definition works because $\mathcal{C}_f$ is a countably infinite set. Here we have used the notation $\mathcal{H}_S$ for the Hilbert space whose canonical orthonormal basis vectors are identified with the elements of the countable set S, see Chapter 2 for the formal details. Then the idea is that whereas in the classical setting the local transition rule is from Σ^2 to Σ (see Definition 3.4), it is now extended in order to be able to produce superpositions of symbols. In [7] we have simplified, without loss of generality, the original definition of LQCA in several ways. This yielded:

Definition 4.2 (LQCA)
A linear quantum cellular automaton (LQCA) is defined by a linear function $\delta : \mathcal{H}_\Sigma \otimes \mathcal{H}_\Sigma \to \mathcal{H}_\Sigma$ ("the local transition function").
Moreover δ must verify the following two properties:
- the quiescent stability condition: $\big[\delta|qq\rangle) = |q\rangle\big]$.
- the normalization condition:
$\forall w \in \Sigma^2$, $\big[||\delta|w\rangle|| = 1\big]$.
The induced global evolution of the LQCA is the linear operation defined by linear extension of its action upon the canonical orthonormal basis, as follows:

$$\begin{aligned} G : \mathcal{H}_{\mathcal{C}_f} &\to \mathcal{H}_{\mathcal{C}_f} \\ |c\rangle &\mapsto \Delta|c\rangle \\ G|c\rangle = \bigotimes_{i\in\mathbb{Z}} & G|c_i c_{i+1}\rangle \end{aligned}$$

(For comparison with the classical definitions of CA over finite unbounded configurations you must fix the alphabet Σ to be Σ and let 0 play the role of the quiescent state q.) So basically you look at each neighbourhood $c_i c_{i+1}$, compute a cell state $\delta|c_i c_{i+1}\rangle$, and then glue all of these cells together with a tensor. If the initial configuration is not a basis state but a superposition,

the definition also tells you how to handle it: by linearity. There are several problems, however, with this approach.

- This is not an operational definition. In practice you cannot look at overlapping neighbourhoods separately, compute the new cell states and then glue, because of the no-cloning theorem.

- There is no guarantee whatsoever that the global evolution G is unitary (e.g. take a δ that yields $|0\rangle$ always). Deciding of this unitarity is the complicated problem addressed by Dürr, Santha, Lêthanh in [57, 58], Meyer in [97] and which we have further simplified in [7]. Plus in 2D we know this will be undecidable [77], endangering all attempt of generalization to higher-dimensions as was noticed in [68].

- The definition is non-causal, because it allows for superluminal signalling, as we have later shown in [19] and will explain here in Subsection 5.4.1.

Nevertheless some particular instances LQCA are well-behaved. This is the case of the Partitioned QCA introduced by Watrous, and hence his result about QCA being able to simulate Quantum Turing Machines (QTM) still applies.

Continuous-time QCA (CQCA)

Another approach is to quantize classical CA as a line of quantum systems interacting with their nearest neighbour in continuous time, via a local translation-invariant hamiltonian. This is an intuitive approach as physicists have been studying this sort of models for years, in statistical quantum mechanics originally under the name of spin chains, Ising models and others, and then as candidate architectures for implementations of quantum computers [62, 86, 26, 133, 140]. Only recently, however, have they been studied in the more abstract frameworks provided by quantum information theory and quantum computer science – with for instance Bose addressing questions such as quantum information transport [31], Subrahmanyam, Lakshminarayan, Brennen and Williams looking at entanglement creation and transport [125, 126, 36], Vollbrecht, Cirac , Nagaj and Wocjan working out universality [136, 105]. With some variations all of these models revolve around the following definition [136]:

Definition 4.3 (CQCA)
A continuous-time quantum cellular (CQCA) is defined by $h : \mathcal{H}_\Sigma \otimes \mathcal{H}_\Sigma \to \mathcal{H}_\Sigma \otimes \mathcal{H}_\Sigma$ *a hamitonian over two cell sites.*

Moreover h must verify the quiescent stability condition: $\big[h|qq\rangle = \mathbf{0}\big]$.
The induced global evolution $G(t)$ of the continuous-time quantum cellular automaton is the unitary operator given by:

$$G : \mathcal{H}_{\mathcal{C}_f} \to \mathcal{H}_{\mathcal{C}_f}$$
$$G(t) = e^{-iHt} = \sum_n \frac{(-iH)^n}{n!}$$
$$\text{with} \quad H = \sum_i h_i$$

where h_i stands for h as acting over positions i and $i+1$.

There are a lot great things to be learnt about this definition, which avoids many of the drawbacks of LQCA as it is operational and the global evolution is guaranteed to be unitary. In particular in terms of finding practical implementation schemes for QCA, this is surely the way to go. Nevertheless from a purely theoretical point of view CQCA suffer the downside which most non-trivial models of continuous-time quantum mechanical systems that are spatially distributed share. Namely strictly speaking they also allow for superluminal-signalling – in some negligible, exponentially tailing off manner. Intuitively this is because even though in a δt of time each cell only interacts with its nearest-neighbour, this is non longer true for any finite period of time t. Indeed it is clear from the series form of Definition 4.3 that $G(t)$includes terms of the form H^n, and hence terms of the form $\prod_i h_i$. Rigorous analytical proofs of this can be hard, but can be found in [136, 125, 126]. Actually in the variations by [36, 105] this is not the case, because the evolution is actually given by two alternating hamiltonian. In this sense these last two models are actually more akin to the block representation approach to QCA we now explain.

4.1.2 QY : PQCA, BQCA

Due to all of the shortcomings we have mentioned above in terms of having an operational, unitary, and causal definition of QCA, several authors have switched to quantizing Partitioned or Block representations of CA (Y).

Partitioned QCA (PQCA)

Very early Watrous [139], Van Dam [134] and later Inokuchi and Mizoguchi[73] have introduced Partitioned QCA. This approach is the natural quantization of classical Partitioned CA, as discussed in Subsection 3.2.2. As usual we assume without loss of generality that the neighbourhood is of size two:

Definition 4.4 (Partitioned QCA) *A partitioned n-dimensional quantum cellular automaton (PQCA) is defined by a unitary operators U such that $U : \mathcal{H}_\Sigma^{\otimes 2^n} \longrightarrow \mathcal{H}_\Sigma^{\otimes 2^n}$, and $U|qq\dots qq\rangle = |qq\dots qq\rangle$, i.e. that takes 2^n cells into 2^n cells and preserve quiescence. Consider $G = (\bigotimes_{2\mathbb{Z}^n} U)$ the operator over $\mathcal{H}$. The induced global evolution is G at odd time steps, and σG at even time steps, where σ is a translation by one in all directions. Cf. Figure 4.1.*

The defining elementary unitary evolution U will be referred to as the scattering unitary, by analogy with quantum field theory. Hence the term 'U-defined QCA' is used in order to designate the PQCA with a scattering unitary U. As

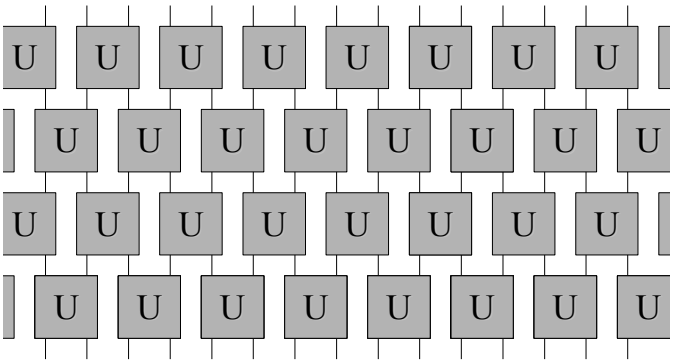

Figure 4.1: Partitioned one-dimensional QCA with scattering unitary U. Each line represents a quantum system, in this case a whole cell. Each square represents a scattering unitary U which gets applied upon two cells. Time flows upwards.

we have mentioned, they have shown that these can simulate the Quantum Turing Machine [139], or in a simpler way Quantum Circuits [134].

Block QCA (BQCA)

Soon afterwards VanDam [134], Brennen, Williams [36], Nagaj, Wocjan [105], Raussendorf [115], Schumacher, Werner [120], Karafyllidis [76] and Perez-Delgado, Cheung [41] have introduced Block QCA. These are quantizations of Block represented CA as discussed in Subsection 3.2.2. Most of the times, the authors propose to quantize two-layered block represented CA, i.e. we simply have :

Definition 4.5 (Block QCA) *A block n-dimensional quantum cellular automaton (BQCA) is defined by a two unitary operators U_0 and U_1 such that $U_i : \mathcal{H}_\Sigma^{\otimes 2^n} \longrightarrow \mathcal{H}_\Sigma^{\otimes 2^n}$, and $U_i|qq\dots qq\rangle = |qq\dots qq\rangle$, i.e. that take 2^n cells into*

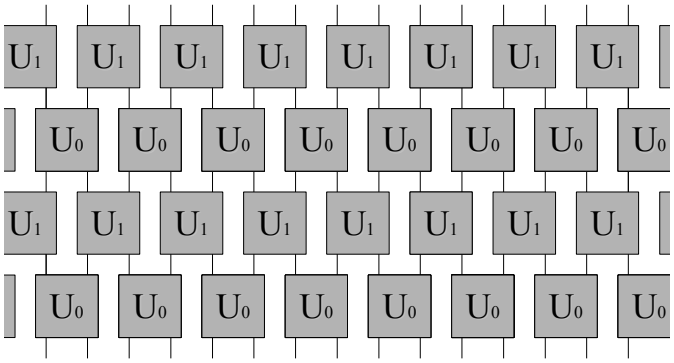

Figure 4.2: Block QCA. The elementary unitary evolutions U_0 and U_1 are alternated repeatedly as shown.

2^n cells and preserve quiescence. Consider $G_i = (\bigotimes_{2\mathbb{Z}^n} U_i)$ the operator over $\mathcal{H}$. The induced global evolution is G_0 at odd time steps, and σG_1 at even time steps, where σ is a translation by one in all directions. Cf. Fig. 4.2.

In one-dimension and at the cost of larger cells Shepherd, Franz and Werner have shown in [122] that two-layered Block QCA are capable of simulating l-layered BQCA (i.e. having $U_0, \ldots, U_l$) – and we have shown in [15] that PQCA are also capable of simulating these BQCA, as we explain in Subsection 5.2.2. On the other hand the definition of Block QCA for n-dimensions by Perez-Delgado and Cheung [41] is 2^n-layered, as we later explain in Subsection 5.2.1.

We have discussed the various problems related to the family of definitions QX, and so we ought to do the same with definitions QZ, except there is none of the previously mentioned problems with this family of definitions : they are operational, unitary, causal. The issue however is one of generality. Apart from in [120], these definitions appear to be quite ad hoc at first : Why should we believe that QCA in general are of the particular form introduced by [139], [134], [36], [105], [115] or [41]? Is it the case at all that all QCA admit a block representation? As we have explained in Subsection 3.2.2 this is not even always the case in the classical case. We postpone the answers to these questions to Chapter 5.

4.1.3 QZ : QW, RQCA

Due to all of the shortcomings we have mentioned above in terms of having a general definition of QCA, several authors have switched to quantizing axiomatic characterizations of CA (Z). The axiomatic characterization of CA

over infinite configurations is in terms of continuity and shift-invariance (cf. Theorem 3.2). But as we discussed earlier the axiomatic characterization of CA over finite unbounded configurations is only in terms of uniform continuity and shift-invariance (cf. Theorem 3.3), due to the lack of compactness of this space. We also explained that uniform continuity basically boils down to causality.
For QCA, even if we manage to define them over infinite configurations (which is difficult, but not impossible as we see next [120]) the induced vector space is unlikely to have a compact metric. Hence a good starting point for an axiomatic definition of QCA is just to require that they are causal, shift-invariant, and of course unitary for compliance with quantum theory. There has been two such approaches in the literature.

Quantum Walks : QW

Actually the very first to introduce the name Quantum Cellular Automata were Grössing and Zeilinger [66, 65], and they did taking that methodology. In their approach however the space upon which QCA were defined was quite different from everything we have discussed so far : it was made out of the superposition of all possible positions of a single cell, i.e. for instance in the case of a one-dimensional QCA this would be $\mathcal{H}_{\mathbb{Z}}$. Say we denote by $\mathcal{C}_1^2$ those configurations where cells are bits, but only one of them is one and the rest is zero, then clearly we have $\mathcal{H}_{\mathbb{Z}} \equiv \mathcal{H}_{\mathcal{C}_1^2} \subset \mathcal{H}_{\mathcal{C}_f^d}$. And so it becomes apparent that the QCA studied in [66, 65] are the one-particle-without-internal-degree-freedom-subcase of the more general finite-unbounded-number-of-particles-with-d-degrees-of-internal-freedom QCA we have been discussing so far.
Grössing and Zeilinger let their single particle evolve in discrete-time steps according to a global unitary. This global unitary must be band-diagonal, so as to prevent the particle from going too fast – this is how they formalize causality. Moreover the values within this band-diagonal unitary must repeat periodically – this is how they formalize shift-invariance.
Meyer showed that in the nearest-neighbour case, any such unitary is trivial [99]. He then moved on to notice that in order to obtain some non-trivial behaviour one can augment the radius of the neighbourhood, or equivalently require that the unitary commutes with squared shifts instead of single shifts... or equivalently just let this single particle have an internal degree of freedom, e.g. place yourself upon for instance $\mathcal{H}_2 \otimes \mathcal{H}_{\mathbb{Z}} \equiv \mathcal{H}_{\mathcal{C}_1^4}$. This paper gave rise to an enormous amount of literature, but under the more appropriate name of Quantum Walks [82]. The relationship between QCA and Quantum Walks is made explicit in [83, 69]. Hence quantum walks are the one-particle-subcase of the more general QCA we study here – and yet they

have some much to offer in terms of quantum algorithms [90] and physical modelling [98, 100].

Reversible Quantum Cellular Automata : RQCA

The first to take the axiomatic route for general QCA were Richter, Schumacher and Werner [116, 120]. In their approach however the space upon which QCA was defined was again different from everything we have discussed so far, as it allows infinite configurations. This point deserves an explanation. In QCA, each cell is a d-dimensional Hilbert space, and so the space of configurations is morally something alike "$\bigotimes_{\mathbb{Z}} \mathcal{H}_d$", but unfortunately this is not a Hilbert space (e.g. the scalar product may diverge in such a space). This is the reason why we have been working upon $\mathcal{H}_{\mathcal{C}_f}$ the Hilbert space generated by superpositions of finite, unbounded configurations (cf. Definition 4.1). By restricting to superpositions of finite unbounded configurations we are saying that the basis states include only a finite number of non quiescent cells, this is why we have been talking about finite-unbounded-number-of-particles-with-d-degrees-of-internal-freedom QCA earlier-on. However if one is willing to pay the price of abandoning Hilbert spaces (the traditional mathematical setting for quantum theory) and moving on to C^*-algebras (a more abstract operator space, see [35]) then it becomes possible to formalize a notion of QCA over infinite configurations. This is what Schumacher and Werner have done, formalizing that space first and then imposing that the evolution be causal and unitary in that particular language. They obtained that, in the one-dimensional case, any such RQCA can be put into the form of a BQCA as in Definition 4.5. Hence in the one-dimensional case their definition is not only an axiomatic one (ensuring unitarity and causality by definition) but also an operational one – as it turns out to be equivalent to that of [36, 105].
Hence this totally solved the problem of a rigorous definition of QCA over infinite configurations and in the one-dimensional case. Yet:

- Over finite unbounded configurations the situation was still unclear. In classical CA theory it is a well-known fact there are CA can be bijective from $\mathcal{C}_f$ to $\mathcal{C}_f$, and yet not admit to a representation in terms of blocks (permutations applied locally) and partial shifts (shifting subcells left or right) (cf. Subsection 3.2.2). And so, why should QCA as defined upon finite unbounded configurations admit a block representation – when their classical counterparts do not? Supposing that there is a finite although unbounded number of particles in the universe is a fairly

reasonable assumption, could such an assumption lead, as in the classical case, to more general forms of QCA? Can we get back to the Hilbert space setting of quantum theory and away from the C*-algebra setting, as in all of the other papers about QCA?

- Moreover in the n-dimensional case, whether upon finite unbounded or infinite configurations, there was no clear indication that this axiomatic definition would admit to a block representation – hence the pursuit of the particular yet rich case of Clifford Quantum Cellular Automata [119, 118, 107]. We had not yet the possibility to claim that a QCA definition that would be both general and operational had been reached.

This fundamental contribution, and its open problems, is the stage from which this thesis takes on to offer new results – the artificial line from which our discourse moves from past to present tense.

Faced with different quantizations of Cellular Automata, some of them non-causal (QX), some of them ad hoc (QY), it is our responsibility as theoreticians to pursue the more axiomatic route (QZ). And so we will now recast the definition of QCA in the more standard setting of the Hilbert space of superpositions of finite, unbounded configurations. This, however, can be done for general graphs and not just grids, leading us to the very general concept of unitary causal operators. We now explain the central role of that more general concept, before we formalize it and prove two of its properties.

4.2 Unitary causal operators ⊙⟁⊛

A physical system is described in quantum theory by state vectors (i.e. a unit vector) $|\psi\rangle$ in a separable Hilbert space $\mathcal{H}$, and it evolves from time t to time t' according to a unitary operator U (cf. Subsection 2.2.1). In general we only know a few things about unitary operators; that they preserve the norm and the inner product, which is equivalent to $U^\dagger U = U^\dagger U = \mathbb{I}$, or sending a base into a base (cf. Subsection 2.1.2). In finite dimension we also know that they can be decomposed as $\sum_x e^{i\lambda_x}|\phi_x\rangle\langle\phi_x|$, and that they can be approximated up to an arbitrary precision by a circuit made out of the universal quantum gates H, $Phase$, $Cnot$ [34, 108]. However in infinite dimensions spectral theory becomes quite complicated, and nothing tells us whether the operator can be expressed as a quantum circuit. Often it can be hard to give a meaningful / operational structure to the unitary operator.

Often infinite-dimensions arise in quantum theory from the fact that we are considering spatial degrees of freedom. The canonical example is that of the wavefunction of a particle on a line – whose state vector already lives in a Hilbert space of infinite dimensions. But physics then tells us something else about the evolution, namely that if the particle is well-localised within a region R at time t', it was nowhere to be found outside the region $R \pm c(t'-t)$ at time t. This is causality, and what causality says in general is that if we distinguish different 'places', some of them close to one another, some of them distant, and if the interval $(t'-t)$ is sufficiently small, then the state associated to some place x at time t' should only depend upon the state associated to the neighbours of x at time t.

What we are going to explain in this thesis is that infinite-dimensional unitary causal operators have, contrary to general infinite-dimensional unitary operators, a lot of structure.

To make this more specific we need to formalize what is meant by 'state associated to some place'. The simplest, rigorous, well established formalism for doing so is that of density matrices, tensor products, and partial traces (cf. Subsection 2.2.2). In this formalism the state of a physical system is described by a density matrix (i.e. a unit trace positive operator) ρ over $\mathcal{H}$. If space divides up into places A and B, then we have that $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$, but the point is that we can now recover the state associated to place A via a trace-out operation $\rho|_A = \mathrm{Tr}_B(\rho)$. And hence we can express causality by saying that if ρ taken to ρ' over a short enough period of time, then $\rho'|_x$ should be a function of $\rho|_{\mathcal{N}_x}$, with $\mathcal{N}_x$ designating the neighbours of x.

4.2.1 Formalization

So far in this intuitive motivation towards the concept of unitary causal operator we have been speaking about 'places, some of them close to one another, some of them distant'. As we seek to capture this idea in the most general, and yet simple and formal manner, we shall identify those 'places' with the nodes of an arbitrary graph, and say that two nodes are 'close' whenever they are related by an edge. We first need to make rigorous the idea of a graph, with a quantum system at each node.

Definition 4.6 (quantum labeled graph)
A quantum labeled graph (QLG) is a tuple $\Gamma = (\mathcal{V}, \mathcal{E}, \mathcal{H})$ *with:*
- $\mathcal{V}$*, the nodes (a countable set);*
- $\mathcal{E}$*, the edges (a subset of* $\mathcal{V} \times \mathcal{V}$*);*

- $\mathcal{H}$, the labels (a countable set of Hilbert spaces).
We denote by $\mathcal{N}_x = \{y \,|\, (x,y) \in \mathcal{E}\}$ the set of direct neighbours of the node x, with x an integer ranging over $\mathcal{V}$.

To each node x there is an associated alphabet Σ^x and hence an Hilbert space $\mathcal{H}^x = \mathcal{H}_{\Sigma^x}$. Now say the graph is infinite. The difficulty here is that as we have mentioned an infinite tensor product Hilbert spaces "$\bigotimes_{\mathbb{N}} \mathcal{H}^x$" is in general not a Hilbert space, so we must take the following detour :

Definition 4.7 ((finite) configurations)
A (finite) configuration c of a QLG $\Gamma = (\mathcal{V}, \mathcal{E}, \mathcal{H})$ is a function $c : \mathbb{N} \longrightarrow \mathbb{N}$, with $x \longmapsto c(x) = c_x$, such that:
- c_x belongs to Σ^x;
- the set $\{x \,|\, c_x \neq q\}$ is finite.
The set of all finite configurations of a QLG be denoted $\mathcal{C}_f$ again.

The idea is that finite configurations are the basic states of the quantum systems labelling the graph. The following definition works because $\mathcal{C}_f$ is countable (this generalizes Definition 4.1):

Definition 4.8 (superpositions of (finite) configurations)
We define $\mathcal{H}_{\mathcal{C}_f}$ be the Hilbert space of configurations of a QLG $\Gamma = (\mathcal{V}, \mathcal{E}, \mathcal{H})$, as follows: to each finite configurations 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 state vector *is a unit vector $|\psi\rangle$ in $\mathcal{H}_{\mathcal{C}_f}$. A* state *is a trace-one positive operator ρ over $\mathcal{H}_{\mathcal{C}_f}$.*

Note that $\mathcal{H}_{\mathcal{C}_f}$ is entirely defined by the set of Hilbert spaces $\mathcal{H} = (\mathcal{H}^x)$. From now on we will write $\mathcal{H}$ instead of $\mathcal{H}_{\mathcal{C}_f}$. Note also that the state ρ captures the state of the entire compound system, whereas $\rho|_x$ stands for the state which labels node x of the graph, where we introduce the notation $A|_{\mathcal{S}}$ for the matrix $\mathrm{Tr}_{\text{All but the systems in } \mathcal{S}}(A)$.

Definition 4.9 (Causality)
A linear operator $U : \mathcal{H} \longrightarrow \mathcal{H}$ is said to be causal *with respect to a quantum labeled graph Γ if and only if for any ρ, ρ' two states over $\mathcal{H}$, and for any $x \in \mathbb{Z}$, we have*

$$\rho|_{\mathcal{N}_x} = \rho'|_{\mathcal{N}_x} \quad \Rightarrow U(\rho)U^\dagger|_x = U(\rho')U^\dagger|_x. \tag{4.1}$$

In other words: to know the state of node number x, we only need to know the neighbouring of nodes $\mathcal{N}_x$. Unitarity is as usual:

Definition 4.10 (Unitarity)
A linear operator $G : \mathcal{H} \longrightarrow \mathcal{H}$ is unitary *if and only if $\{G|c\rangle \,|\, c \in \mathcal{C}_f\}$ is an orthonormal basis of $\mathcal{H}_{\mathcal{C}_f}$.*

Hence we have defined the main object of our discourse: unitary causal operators. This concept of unitary causal operator generalizes the two-systems definition by Beckman, Gottesman, Nielsen, Preskill [25] and the three-systems definition by Schumacher and Westmoreland [121].

4.2.2 Properties

Let us now give some important facts we have proved about unitary causal operators. These results may also be regarded as providing alternative formulations of the above notion causality (cf. Definition 4.9).

Proposition 4.1 expresses causality in the Heisenberg picture, as a condition on the evolution of observables. Whenever we say that a linear operator A is localised upon a region R, we mean that A is of the form $A_R \otimes \mathbb{I}_{\mathcal{V} \setminus R}$, i.e. it is the identity over anything that lies outside of R. Morally, A is an 'observable' in the following result.

Property 4.1 (Dual causality)
Let U be a causal linear operator with respect to a quantum labeled graph Γ. This is equivalent to saying that for every operator A localised upon node x, then $U^\dagger AU$ is localised upon the nodes in $\mathcal{N}_x$.

Proof. [$\Rightarrow$]. Suppose causality and let A be an operator localised upon node x. For every states ρ and ρ' such that $\rho|_{\mathcal{N}_x} = \rho'|_{\mathcal{N}_x}$, we have $(U\rho U^\dagger)\,|_x = (U\rho' U^\dagger)\,|_x$ and hence $\mathrm{Tr}\,(AU\rho U^\dagger) = \mathrm{Tr}\,(AU\rho' U^\dagger)$. We thus get $\mathrm{Tr}\,(U^\dagger AU\rho) = \mathrm{Tr}\,(U^\dagger AU\rho')$. Since this equality holds for every ρ and ρ' such that $\rho|_{\mathcal{N}_x} = \rho'|_{\mathcal{N}_x}$, what we are saying is that the $U^\dagger AU$ does not discriminate differences between ρ and ρ' whenever they lie outside of $\mathcal{N}_x$. In other words $U^\dagger AU$ is localised on the nodes in $\mathcal{N}_x$.
[$\Leftarrow$]. Suppose dual causality and $\rho|_{\mathcal{N}_x} = \rho'|_{\mathcal{N}_x}$. Then, for every operator B localised upon the nodes in $\mathcal{N}_x$, $\mathrm{Tr}\,(B\rho) = \mathrm{Tr}\,(B\rho')$, and so for every operator A localised upon node x, we get: $\mathrm{Tr}\,(AU\rho U^\dagger) = \mathrm{Tr}\,(U^\dagger AU\rho) = \mathrm{Tr}\,(U^\dagger AU\rho') = \mathrm{Tr}\,(AU\rho' U^\dagger)$. This entails $(U\rho U^\dagger)\,|_x = (U\rho' U^\dagger)\,|_x$. □

Proposition 4.2 expresses causality in terms of the inverse of the unitary causal operator U. Whenever we speak about the transpose of a quantum labeled graph Γ, we mean as usual the quantum labeled graph Γ^T which is obtained just by changing the direction of the edges. The neighbours of x in Γ^T are designated by $\mathcal{N}_x^T$.

Property 4.2 (Inverse causality)
Let U be a causal linear operator with respect to a quantum labeled graph Γ.

Then $U^\dagger$ is a causal operator with respect to the transposed quantum labeled graph Γ^T.

Proof. Suppose causality, let A be an operator localised upon node x, and choose M an operator localised upon a node y which does not lie in $\mathcal{N}_x^T$. That way x does not belong to $\mathcal{N}_y$. But according to Proposition 4.1 we know that $U^\dagger MU$ is localised upon $\mathcal{N}_y$, and hence $U^\dagger MU$ commutes with A. Now $A \mapsto UAU^\dagger$ is a morphism because $AB \mapsto UAU^\dagger UBU^\dagger = UABU^\dagger$, and so via this morphism we can also say that $UU^\dagger MUU^\dagger = M$ commutes with $UAU^\dagger$. An since M can be chosen amongst to full matrix algebra $M_d(\mathbb{C})$ of the node y, this entails that $UAU^\dagger$ must be the identity upon this node. The same can be said of any node outside $\mathcal{N}_x^T$. So $UAU^\dagger$ is localised upon $\mathcal{N}_x^T$ and we can conclude our proof via Proposition 4.1. □

We will provide some more general results on unitary causal operators in Chapter 5. For now let us come back to the canonical example of such unitary causal operators : QCA.

4.3 Axiomatics of Quantum cellular automata ⊙⟁⊛

After having taken this detour via the more general notion of unitary causal operator, the definition of QCA becomes an easy matter. For n-dimensional QCA the corresponding QLG is simply an n-dimensional grid with a Hilbert space $\mathcal{H}_\Sigma$ sitting at each node. In addition the unitary is required to be shift-invariant with respect to that grid, but this shift-invariance is formalized as expected:

Definition 4.11 (Shift-invariance)
Consider the shift operation, for $k \in \{1, \dots, n\}$, which takes configuration c to c' where for all $(i_1, \dots, i_n)$ we have $c'_{i_1 \dots i_k \dots i_n} = c_{i_1 \dots i_k+1 \dots i_n}$. Let $\sigma_k : \mathcal{H} \longrightarrow \mathcal{H}$ denote its linear extension. A linear operator $G : \mathcal{H} \longrightarrow \mathcal{H}$ is said to be shift invariant *if and only if $G\sigma_k = \sigma_k G$ for each k.*

And so we get to the following definition.

Definition 4.12 (QCA)
A n-dimensional quantum cellular automaton (QCA) is an shift-invariant unitary causal operator $G : \mathcal{H} \longrightarrow \mathcal{H}$ over a QLG $\Gamma = (\mathcal{V}, \mathcal{E}, \mathcal{H})$ with:
- $\mathcal{V} = \mathbb{Z}^n$ i.e. the nodes form a grid;
- $\mathcal{E} = \{x, x + z \mid x \in \mathbb{Z}^n \wedge z \in \{0, 1\}^n\}$ i.e. radius half;
- $\mathcal{H} = (\mathcal{H}_\Sigma)$ i.e. all cells are of a given finite dimension d.

What now? Quantum cellular automata (QCA) consist in an array of identical finite-dimensional quantum systems. The whole array evolves in discrete time steps by iterating a linear operator G. Moreover this global evolution G is shift-invariant (it acts everywhere in the same way), causal (information cannot be transmitted faster than some fixed number of cells per time step), and unitary (the condition required by the postulate of evolutions in quantum mechanics, akin to reversibility). This axiomatic definition is the natural 'quantization' of the classical definition. But contrary to its classical counterpart the axiomatic definition does not immediately yield a straightforward way of constructing /enumerating all of the instances of this model. This lack of operationality is the reason why QCA remained an excessively abstract, hard-to-grasp mathematical object for a while – leaving out a gap for more ad hoc, hands-on definitions. The results in the next chapter will give them a more concrete turn and finish to settle down this issue by reconciling different views.

Chapter 5

Structures

Time is what prevents everything from happening at once.
—John A. Wheeler, American J. of Physics, **46***, 323, (1978).*

We show that unitary causal operators can be implemented locally. This provides an operational meaning to the axiomatic definition of Quantum Cellular Automata, because it shows that QCA can be put into the form of an infinite tiling of more elementary, finite-dimensional unitary operations. We take some time to show how this reconciles most previous definitions of QCA. We derive some non-trivial consequences – such as the fact that quantum information goes faster than classical information. We end with a general discussion about this structure theorem.

We have seen that Quantum cellular automata can be given an elegant axiomatic definition in terms of shift-invariant unitary causal operators. But we have also seen that this axiomatic definition is not so operational : if we leave it there QCA would remain an excessively abstract, hard-to-grasp mathematical object.

5.1 Unitary causal operators continued ⊙⟁⊛

Let us consider the general setting of a graph with a single quantum system sitting at each node, and the entire compound system evolving in discrete time steps by according to a global evolution U. Moreover let us suppose that this global evolution U is unitary, in accordance with quantum theory, and that this global evolution U is causal, in accordance with special relativity. By causal we mean that information can only ever be transmitted at a bounded speed, the speed bound being quite naturally that of one edge of the underlying graph per iteration of U. These general unitary causal operators have been formalized in Section 4.2. We will now show that they have the remarkable property of being implementable locally; i.e. that they can be put into the form of a quantum circuit made up with more elementary operators – each acting solely upon neighbouring nodes.

Theorem 5.1 (Local representation)
Let U be a unitary causal operator with respect to a quantum labeled graph $\Gamma = (\mathcal{V}, \mathcal{E}, \mathcal{H})$. Then there exists D, (K_x), E, and $|\phi\rangle$ such that for all $|\psi\rangle$,

$$(\bigotimes D)(\prod K_x)(\bigotimes E)|\psi\rangle = |\phi\rangle \otimes U|\psi\rangle$$

where:

- *(K_x) is a collection of commuting unitary operators localised upon each neighbourhood $\mathcal{N}_x^T$;*

- *$D^\dagger, E$ are two isometric operators localised upon each node x, and whose actions depend only on $\dim(\mathcal{H}^x)$.*

Moreover:

- *If the $(\mathcal{H}^x)$ are all of finite dimensions, then the $(K_x), D^\dagger$ and E are finite dimensional operators;*

- *If* $U(\bigotimes|q\rangle) = (\bigotimes|q\rangle)$*, then* $|\phi\rangle = (\bigotimes|q\rangle)$*;*

- *If the* $(\mathcal{H}^x)$ *are all of infinite dimensions and* $U(\bigotimes|q\rangle) = (\bigotimes|q\rangle)$*, then we can choose to just have* $(\bigotimes D)(\bigotimes K_x)(\bigotimes E) = U|\psi\rangle$ *where* D *and* E *are also unitary.*

Proof. [Encoding]. The action of E upon node x is just to add an ancilla, i.e. $E|\psi_x\rangle = |q\rangle \otimes |\psi_x\rangle$. Hence if $\dim(\mathcal{H}^x)$ is finite then $E : \mathcal{H}^x \longrightarrow \mathcal{H}^x \otimes \mathcal{H}^x$ and E is an isometry, whereas if $\mathcal{H}^x$ is of infinite countable dimension then we can use any bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ so that $E : \mathcal{H}^x \longrightarrow \mathcal{H}^x$ and E is unitary.
[Product states]. Let us consider $|\psi\rangle \in \mathcal{H}$ having the form of a product state, i.e. so that $|\psi\rangle = \bigotimes|\psi_x\rangle$. We will show that $(\bigotimes D^\dagger)(\bigotimes K_x)(\bigotimes E)|\psi\rangle = U|\psi\rangle$, and then by linearity the result will be proved for entangled states also. This is because in general any state vector $|\phi\rangle$ can be written as a sum of $|\phi^i\rangle$, where each $|\phi^i\rangle$ is a product state $|\phi^i\rangle = \bigotimes|\phi^i_x\rangle$. Below we again use this form for $|\phi\rangle = U^\dagger(\bigotimes|q\rangle)$.
[Two tapes]. So E takes $|\psi\rangle$ into $(\bigotimes|q\rangle) \otimes (\bigotimes|\psi_x\rangle)$. Now since $(\bigotimes|q\rangle) = UU^\dagger(\bigotimes|q\rangle) = U|\phi\rangle$ we rewrite $E|\psi\rangle$ as:

$$\sum_i U(\bigotimes|\phi^i_x\rangle) \otimes (\bigotimes|\psi_x\rangle)$$

So initially our QLG has got two 'tapes', one which we call the 'computed tape' holding state $U(\bigotimes|\phi\rangle)$, and one which we call the 'uncomputed tape' holding state $(\bigotimes|\psi_x\rangle)$.
[Changing factors]. Now the idea is that the K_x will let us pass pieces of the uncomputed tape to the computed tape. Namely we want $K_xE|\psi\rangle$ is equal to:

$$\sum_i U\big(|\psi_x\rangle \otimes \bigotimes_{\mathcal{V}\setminus\{x\}} |\phi^i_y\rangle\big) \otimes \big(|\phi^i_x\rangle \otimes \bigotimes_{\mathcal{V}\setminus\{x\}} |\psi_y\rangle\big).$$

Let us simply take $K_x = U\,Swap_x\,U^\dagger$, meaning that we simply uncompute the computed tape, swap $|\psi_x\rangle$ for $|q\rangle$, and then compute it back. Clearly this does the job but does seem wrong, because it looks as though we are acting over the entire graph and not just $\mathcal{N}_x$. Yet this naive choice is actually the right one. Indeed since U is unitary causal with respect to Γ, then so is $U^\dagger$ with respect to Γ^T, by Proposition 4.2. And now since $U^\dagger$ is unitary causal over Γ^T, $U\,Swap_x\,U^\dagger$ must be localised upon $\mathcal{N}^T_x$, by virtue of Proposition 4.1. Note that the (K_x) commute with one another just because the $(Swap_x)$ commute with one another and $A \mapsto UAU^\dagger$ is a morphism.

[Decoding]. Of course we can reiterate this process until we get

$$\sum_i U(\bigotimes |\psi_x\rangle) \otimes (\bigotimes |\phi_x^i\rangle)$$

which is just $U|\psi\rangle \otimes |\phi\rangle$. Now we just need to swap the computed and uncomputed tapes to get $(|\phi\rangle \otimes U|\psi\rangle$. (In situations where $U^\dagger(\bigotimes |q\rangle) = |\phi\rangle$ is known and turns out to be a product state $\bigotimes |\phi_x\rangle$, then D can also locally undo the $|\phi\rangle$ so as to get $(\bigotimes |q\rangle) \otimes U|\psi\rangle = EU|\psi\rangle$. This is the case for instance in the standard situation when $U(\bigotimes |q\rangle) = (\bigotimes |q\rangle)$. If on top of that E was a unitary, D can also apply $E^\dagger$ and give back $U|\psi\rangle$.) □

Corollary 5.1 (Circuit representation)
Let U be a unitary causal linear operator with respect to a quantum labeled graph $\Gamma = (\mathcal{V}, \mathcal{E}, \mathcal{H})$. Then U can be expressed as a circuit of quantum operations each localised upon a neighbourhood $\mathcal{N}_x^T$, and having depth less or equal to $\deg(\Gamma)^2 + 2$.

Proof. By inspection of the proofs of Theorem 5.1 and using the following remarks. Since each K_x is localised upon $\mathcal{N}_x^T$, many of them can be done in parallel, namely whenever the corresponding neighbourhoods do not intersect. The question of how much can be done in parallel, i.e. how many layers of circuit are necessary, is equivalent to the $L(1,1)$-labeling problem for graphs, namely we want to colour the graph so that no neighbours nor next-neighbours have the same colours. This is known to require at most $\deg(\Gamma)^2$ colours [40]. The plus two is for E and D. □

The study of unitary causal operators was, for us, initially motivated by the study of quantum cellular automata. However the study of unitary causal operators may have older origins than QCA, for example it is clear that similar questions have arisen in axiomatic/algebraic quantum field theories [39]. The main difference in approach seems to be that AQFT tends to focus on continuous space and time. The authors are not aware, however, of a result akin to Theorem 5.1 in AQFT, which would allow one to structure the dynamics of the system in such a meaningful, operational manner. Thus the field of application of Theorem 5.1 seems much wider than just QCA.

5.2 Quantum cellular automata reconciled ⊙⏢

Nevertheless let us now specialize the representation we have obtained about general unitary causal operators, to their canonical example : n-dimensional

QCA – and then draw the consequences.

5.2.1 Multi-layers

Assuming that the QLG is an n-dimensional grid labelled with a Hilbert space $\mathcal{H}_\Sigma$ sitting at each node, and assuming that the global evolution G is shift-invariant with respect to this grid, we obtain the following.

Theorem 5.2 (n-dimensional QCA multi-layered block representation)

Let G be an n-dimensional QCA with alphabet Σ. Let E be an isometry from $\mathcal{H}_\Sigma \to \mathcal{H}_\Sigma \otimes \mathcal{H}_\Sigma$ such that $E|\psi_x\rangle = |q\rangle \otimes |\psi_x\rangle$. This mapping can be obviously extended to whole configurations, yielding a mapping $E : \mathcal{H}_{C_f^\Sigma} \to \mathcal{H}_{C_f^{\Sigma^2}}$. Then there exists a n-dimensional QCA H on alphabet Σ^2, such that $HE = EG$, and H admits an 2^n-layer block representation. Moreover H is of the form

$$H = (\bigotimes S)(\prod K_x) \tag{5.1}$$

where:

- *(K_x) is a collection of commuting unitary operators all identical up to shift, each localised upon each neighbourhood $\mathcal{N}_x$;*

- *S is the swap gate over $\mathcal{H}_\Sigma \otimes \mathcal{H}_\Sigma$, hence localised upon each node x.*

Proof. By inspection of the proof of Theorem 5.1 and using the following remarks. At each $x = (i_1, \ldots, i_n)$ step, $K_x = K_{i_1 \ldots i_n}$ is local to cells $\{i_1, i_1+1\} \times \ldots \times \{i_n, i_n+1\}$, uncomputed and computed tapes alike. Namely, whenever $(i_1, \ldots, i_n)$ and $(j_1, \ldots, j_n)$ are such that for every $k \in \{1, \ldots, n\}$, $|i_k - j_k| > 1$, then $K_{i_1 \ldots i_n}$ and $K_{j_1 \ldots j_n}$ can be performed in parallel. So we can first apply simultaneously all the $K_{i_1,\ldots,i_n}$'s where the i_k's are even. Then, as each element $x = (x_1, \ldots, x_n)$ can be written in a unique way as the sum of y with even coordinates and $z \in \{0,1\}^n$, we need $|\{0,1\}^n| = 2^n$ layers to apply all of the $K_{i_1,\ldots,i_n}$'s. Moreover by shift-invariance these $K_{i_1 \ldots i_n}$'s are just shifted version of the same K, so that each layer is just tiling of the space by a finite-dimensional unitary K. □

In Chapter Subsection 4.1.2 we have explained how several authors, given the apparent lack of operationality of the axiomatics of QCA, have defined them directly as quantizations of block representations of CA. Amongst those

various definitions only the one by Perez-Delgado and Cheung [41] is not two-layered. It stands out at this stage, as it just directly posits, after some interesting informal arguments, that they are of a form very akin to the one given by Equation (5.1).
In other words we have demonstrated that starting just from an axiomatic definition of QCA as in [120], one can derive a circuit-like structure for n-dimensional QCA, thereby extending the result of [120] to n dimensions. But we have also demonstrated that the operational definition of [41] can be given a rigorous axiomatics. And so by doing these two things we have shown that the definitions of [120] and [41] are actually equivalent up to ancillary cells.

5.2.2 Down to two layers : BQCA

Nevertheless for most authors [134, 36, 105, 115, 120, 76] quantizations of block representations of CA are two-layered. We called these 'BQCA' in Definition 4.5. Is there again an equivalence between our axiomatics of QCA and BQCA? One direction is easy. BQCA are unitary, causal, shift-invariant, and hence they fall under the spell of our axiomatics and Theorem 5.2. (Actually strictly speaking we need to group each hypercube of 2^n adjacent cells into a supercell, a detail that can be made formal as in Definition 6.3.) The other direction is less trivial. Can BQCA simulate any QCA of the form given by Theorem 5.2 – and hence any QCA?

Notice that in the form given by Theorem 5.2, each cell x at time t is successively involved in 2^n computations governed by a local unitary K, and whose aim is to compute the next state of a cell within radius half of x at time $t+1$. In 2 dimensions a cell x get involved with the cells West, North-West and North of it in order to work out its North-West successor, and then with the cells North, North-East, East in order to compute the North-East successor, and so on for the South-East and the South-West successors. In order to mimic this with a BQCA we can encode each original cell into 4 cells, arranging to that the original cell x starts in the North-West quadrant of the four cells. The first layer of the BQCA will consist in applying K and computing the North-West successor of x. The second layer of the BQCA will consist in moving the original cell x in the North-West quadrant. And so each full application of the evolution of the BQCA corresponds only to one layer ($\bigotimes K$). Hence it will take 4 steps for our BQCA to simulate one step of the QCA. Figure 5.1 provides a sketch of the method we use to accomplish this.

There are some technicalities to it. Whereas cell x is turning clockwise

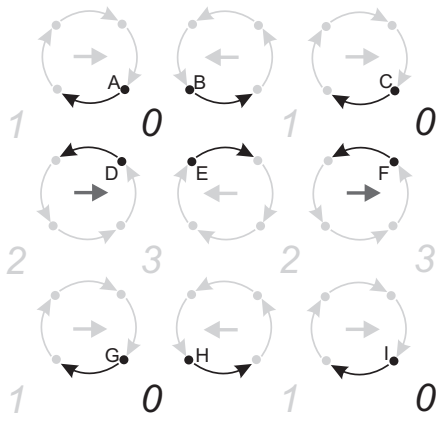

Figure 5.1: Sketch of a BQCA simulating a QCA. The original cell x has been coded into four cells, at the center. It starts of looking towards the North-West, because at time 0 it will compute its North-West successor, and then move clockwise. At time 1 it will compute its North-East successor etc.

in our example, the cell just North of it is turning anti-clockwise. Hence we need some ancillary data coding for the path to be taken by the original cell x within the 4 coding cells. Moreover remember that the form given by Theorem 5.2 finishes with a *Swap* between the 'computed tape', where the results have been stored and the 'uncomputed tape', i.e. what remains of the original cell after having computed all of its successors. Hence we need to keep track of the number of layers of K we have gone though – in order to trigger the *Swap* at the appropriate time. Finally this *Swap* needs to know where the results have been left. All of this has to be arranged spatially and efficiently – a good way to do so is described by Figure 5.2 and Figure 5.3.

In other words BQCA can simulate QCA up to a relatively simple encoding. We have shown this for two dimensions, but it is clear that our construct generalizes to n-dimensions. Hence QCA (as in Definition 4.12) provide a rigorous axiomatics for BQCA (as in Definition 4.5), and BQCA provide a convenient operational description of QCA.

5.2.3 Down to one scattering unitary : PQCA

In Chapter Subsection 4.1.2 we have explained how several authors [139, 134, 73] have defined quantizations of partitioned representations of CA. Is it again true that QCA (as in Definition 4.12) provide a rigorous axiomatics for PQCA (as in Definition 4.4), whereas PQCA provide a convenient operational description of QCA?

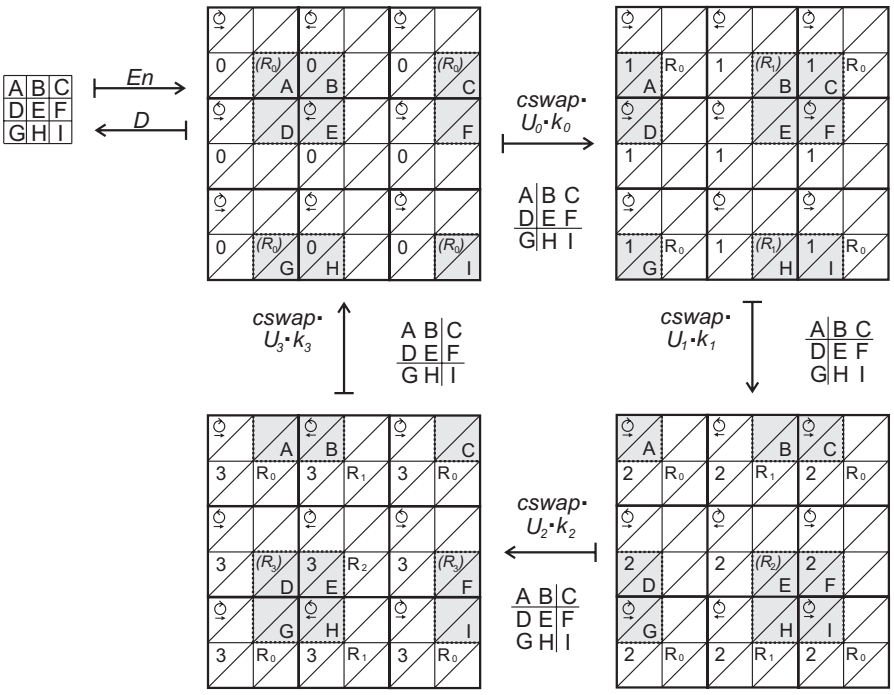

Figure 5.2: BQCA simulating a QCA. The grey areas denote the neighbourhood where the action of k_x, the first layer of the BQCA, will be significant – i.e. a group of four cells where it will perform a K_x operation so as to work out a successor. Where this successor is about to get stored is indicated by (R_x). At a next step we see that R_x has appeared, but also that registers have been reshuffled thanks to the second layer of the BQCA, which acts according to the rotation direction mark. The second layer also increases the clock count and includes the final swapping step, which only happens at time 3. There it makes sure that R_0 becomes A, R_1 becomes B, etc. Which registers are to be swapped with ont another can be worked out from the rotation and the $\leftarrow$, $\rightarrow$ marks. Each step is made formal by Figure 5.3.

Relying on the results of the above Subsection 5.2.2, we only need to show that PQCA can simulate BQCA. Both PQCA and BQCA are two-layered, the only difference is that for BQCA those two-layers may be different (e.g. compare Figures 4.1 and 4.2). So intuitively if a PQCA is U-defined, with a U which is capable of performing U_0 and U_1 alternatively as controlled by some ancillary, this will do the job. This is something we had done for one-dimension in [15] and we do for two dimensions in Figure 5.4, but it is clear that our construct generalizes to n-dimensions.

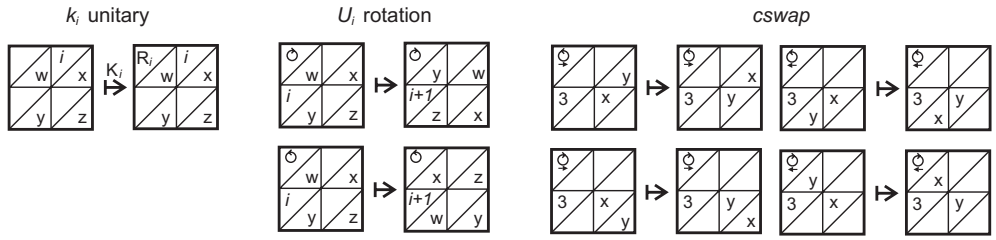

Figure 5.3: Operations used in figure 5.2. The k applies a K operation whenever some data is present (data carries an extra bit to distinguish it from $|q\rangle$, say.). The U operation simply reshuffles the data by rotating it in the direction given by the indicator in the top left (clockwise or anticlockwise), and increments the index counter. Lastly, *cswap* acts as the identity in all cases except when the index is 3, when it swaps the result of the computations with the data, ready for the next round.

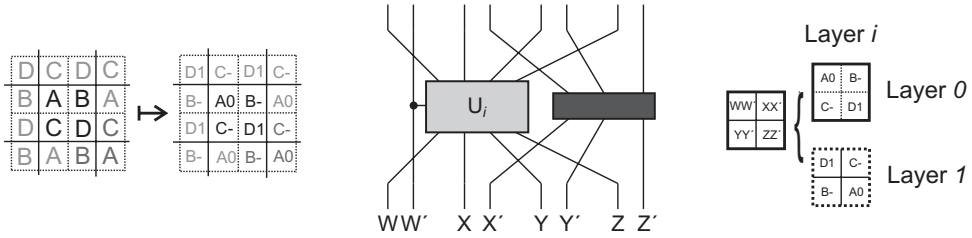

Figure 5.4: PQCA simulating a BQCA. The QCA is decorated with control qubits following a simple encoding procedure (*left*), which allow the scattering unitary U (*centre*) to act as either U_0 or U_1, according to the layer (*right*). The black box can be any unitary.

Hence the answer to the above question is yes : PQCA are the most canonical and yet general operational description of QCA. More generally this Section has demonstrated that the community has now got a well-axiomatized and yet concrete, operational notion of n-dimensional QCA.

5.3 Seeking for exact representations ⏢

So far we have worked out ways of representing the global evolution G of a QCA in terms of local finite-dimensional unitary operations repeated across space – but in doing so we have introduced ancilla cells. We have done so in a non-shocking way, i.e. one which preserves the topology, as we later formalize in Section 6.1. Nevertheless the representation obtained in such a way is not quite G, but only G up to some simple encoding into a larger

space. In this sense this is an non-exact representation. The situation is very akin to that of structure theorems for reversible cellular automata, as we explained in Section 3.2.2, were there are results for exact representations and non-exact representations. And so as in the classical case we may wish to study exact representations of G.
We obtain a positive and a negative result, reminiscent of the classical situation. The techniques in play for the positive result are quite different however from those used classically – they involve entertaining pieces of algebra.

5.3.1 Preliminaries : a small theory of subsystems

The purpose of this subsection 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 (equivalent to a C^*-algebra over a finite-dimensional system):

Definition 5.1 (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 ($\dagger$). 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 5.2 (Subsystem algebras)
Consider $\mathcal{A}$ an algebra 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 5.3 (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 5.3 (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. We skip the proof of this result which is attributed to Wedderburn, the argument being quite technical and its understanding not mandatory for the rest of the thesis. A proof can be found in [19] which is a revamped version of the presentation in [64]. See also [35] for a proof within the setting of general C^*-algebras. *Box*

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

Theorem 5.4 (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 5.3, 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 5.4 (Restriction Algebras)
Consider $\mathcal{A}$ an algebra of $M_p(\mathbb{C}) \otimes M_q(\mathbb{C}) \otimes M_r(\mathbb{C})$. For A an element of $\mathcal{A}$, we write $A|_1$ 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 $\{ Tr_{02}(A) \,|\, A \in \mathcal{A}\}$.

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

Lemma 5.1 (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

$$\forall A \in \mathcal{A}, B \in \mathcal{B} \quad pr.\mathrm{Tr}_{02}(AB) = \mathrm{Tr}_{02}(A)\mathrm{Tr}_{02}(B). \tag{5.2}$$

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

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

Now $\mathcal{A}|_1$ is generated by $\{\mathrm{Tr}_{02}(A) \,|\, A \in \mathcal{A}\}$, and $\mathcal{B}|_1$ is generated by $\{\mathrm{Tr}_{02}(B) \,|\, B \in \mathcal{B}\}$. 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 5.2 (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 $\{\mathrm{Tr}_{02}(AB) \,|\, A \in \mathcal{A}, B \in \mathcal{B}\}$. However by Eq. (5.2) this is the same as $\{\mathrm{Tr}_{02}(A)\mathrm{Tr}_{02}(B) \,|\, A \in \mathcal{A}, B \in \mathcal{B}\}$, which generates $\mathcal{A}|_1\mathcal{B}|_1$. □

5.3.2 Positive result for one dimension

Now this is done we proceed to prove an exact block representation theorem for QCA over finite, unbounded configurations. This is a simplification of [120]. The two-systems and three-systems case are also treated in [25] and [121]. 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 5.5.

Lemma 5.3 *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*

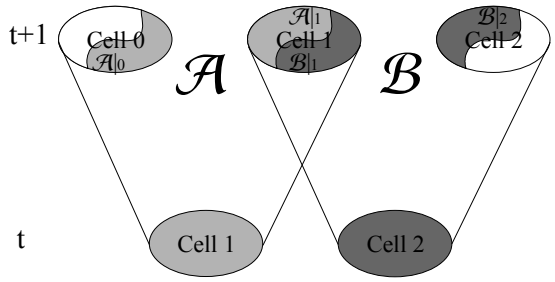

Figure 5.5: Definitions of the algebras for the proof of the structure theorem.

of $\mathcal{A}$ to cell 1.
Let $\mathcal{B}$ be the image of the algebra of the cell 2 *under the global evolution G. It is localized upon cells* 1 *and* 2*, and we call $\mathcal{B}|_1$ the restriction of $\mathcal{B}$ to cell* 1.
There exists a unitary U acting upon cell 1 *such that $U\mathcal{A}|_0U^\dagger$ 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 Propositions 4.1 and 4.2 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 Proposition 4.1 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 $\mathcal{AB}|_1$ is the entire cell algebra of cell 1, i.e. $M_d(\mathbb{C})$.
So now we can apply Theorem 5.4 and the result follows. □

Lemma 5.4 *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. □

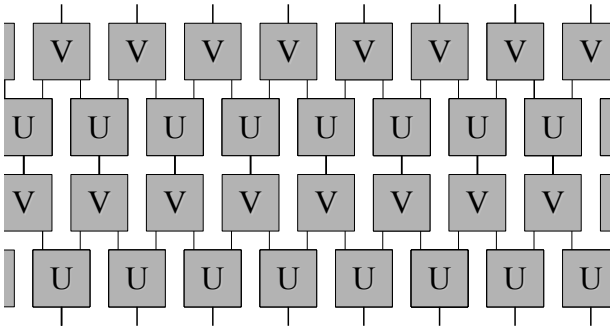

Figure 5.6: QCA with two-layered block representation (U, V). Each line represents a cell, which is a quantum system. Each square represents a unitary U/V which gets applied upon the quantum systems. Time flows upwards.

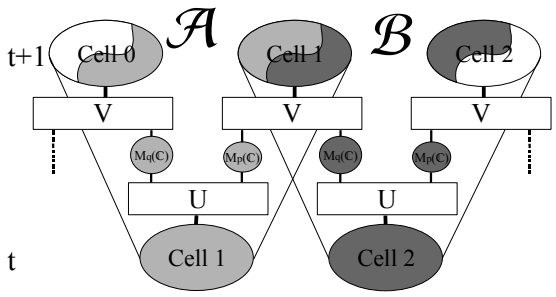

Figure 5.7: Zooming into the two-layered block representation. The unitary interactions U and V are alternated repeatedly as shown.

Theorem 5.5 (One-dimensional two-layered exact block representation)

Any one-dimensional QCA G is of the form described by Figures 5.6 and 5.7.

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 5.3 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 5.4, 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 $G = (\bigotimes V)(\bigotimes U)$ as in Fig. 5.7. 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 $U^\dagger(|q_2\rangle\langle q_2| \otimes |q_1\rangle\langle q_1|)U$ 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 $(\bigotimes U)$ 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. □
Therefore we have shown that one-dimensional QCA over finite, unbounded configurations admit a two-layered block representation. As we shall now see n-dimensional QCA do not admit such a two-layered block representation, contrary to what was stated in [120]. Whilst the proof remains very close in spirit to that of [120], it has the advantages of being remarkably simpler and self-contained, phrased in the standard setting of quantum theory, understandable without heavy prerequisites in C^*-algebras, and most of all is valid over finite unbounded configurations.

5.3.3 Negative result for n dimensions

Finally, and as we have explained in Section 3.2.2 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 [80]:

Definition 5.5 (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. 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.*

The proof can easily be ported to the quantum case, as discussed in the paper [19]. Hence we have a counterexample to the higher-dimensional case of the Theorem in [120]. We reach the following proposition.

Property 5.1 (No-go for n-dimensions) *There exists some 2-dimensional QCA which do not admit an exact two-layered block representation.*

5.4 Consequences of the structure theorems ⊙⍋⊛

We will now discuss two interesting consequences of the above discussed structure theorems, which have to do with the speed of quantum information. Both arise by following the same methodology: first we consider a classical CA F that is bijective over finite unbounded configurations ($\mathcal{C}_f$) taking a configuration c into $F(c)$, second we quantize it in the obvious to the Hilbert space of finite configurations ($\mathcal{H}_{\mathcal{C}_f}$) saying that it takes a configuration $|c\rangle$ into $F|c\rangle$ and any linear combination of configurations $\alpha|c\rangle+\beta|d\rangle$ into $\alpha F|c\rangle+\beta F|d\rangle$, third we make some observations. Because in classical CA we tend to use symbols in alphabet Σ rather than just integers in $0\dots d-1$ in order to keep track of cell states (see Chapter 3), we do the same here. Then the symbol q is back to be the dedicated symbol for the quiescent state, i.e. finite configurations are of the form $\dots qqwqq\dots$ and must remain finite configurations in the forward time evolution.

5.4.1 Bijective CA and superluminal signalling.

Classically there are bijective CA over finite unbounded configurations whose inverse is not a CA, and thus who do not admit any n-layered block representation at all. The mXOR CA is a standard example of that, which we have discussed already in Subsection 3.2.2. Yet surely, just by extending the definition of the mXOR linearly to the Hilbert space of finite configurations, we ought to have a QCA, together with its block representation, hence the apparent paradox. Here is the mathematical object in question:

Definition 5.6 (mXOR 'QCA')
Let $\mathcal{C}_f$ be the set of finite configurations over the alphabet $\Sigma = \{q, 0, 1\}$. For all x, y in Σ Let $\delta|qx\rangle = |q\rangle$, $\delta|xq\rangle = |x\rangle$, and $\delta|xy\rangle = |x \oplus y\rangle$ otherwise. We call $\Delta : \mathcal{H}_{\mathcal{C}_f} \longrightarrow \mathcal{H}_{\mathcal{C}_f}$ the linear operator mapping $|c\rangle = |\ldots c_{i-1}c_ic_{i+1}\ldots\rangle$ to $|c'\rangle = |\ldots\delta(c_{i-1}c_i)\delta(c_ic_{i+1})\ldots\rangle$.

In order to lift this concern let us look at the properties of this quantized Δ to see if this is indeed a QCA. It is indeed unitary as a linear extension of a bijective function, and it is shift-invariant as a linear extension of a shift-invariant function. Yet counter-intuitively it is non-causal. Indeed consider the configuration $d^x = |\ldots qq00\ldots0xqq\ldots\rangle$. It has antecedent $c^x = \Delta^{-1}d^x = |\ldots qqxx\ldots xxqq\ldots\rangle$. Now consider $c^\pm$ the superposition of the configurations c^0 and c^1. We have $c^\pm = 1/\sqrt{2}.|\ldots qq\rangle(|00\ldots00\rangle \pm |11\ldots11\rangle)|qq\ldots\rangle$, and hence $d^\pm = \Delta c^\pm = |\ldots qq00\ldots0\rangle|\pm\rangle|qq\ldots\rangle$, 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 $(\Delta c^\pm)|_i = |\pm\rangle\langle\pm|$ is not just a function of $c|_{i,i+1} = (|0q\rangle\langle 0q| + |1q\rangle\langle 1q|)/2$, but instead depends upon this more 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 $\Delta(\mathbb{I}\otimes Z\otimes\mathbb{I})\Delta^\dagger$. 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 – but this can be made more symmetrical for instance as we did in [17]. Such a behaviour is clearly not acceptable. Although at first it seemed like a

valid QCA, Δ must be discarded as non-physical. Here we are faced with a phenomenon which is causal classically and turns out non-causal in its trivial quantum extension. Clearly this is due to the possibility of having entangled states, which allow for more 'non-local' behaviours, and hence strengthen the consequences of no-signalling / causality. This is the reason why QCA, even on finite unbounded configurations, do admit a block representation. This is also the reason why LQCA, an early definition of QCA which was allowing this sort of quantization of CA, should be discarded as allowing non-physical behaviour (cf. Subsection 4.1.2).
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 unbounded, which is known to coincide with the class of surjective but non injective CA upon infinite configurations, which is again known to be equivalent to the class of bijective CA upon finite configurations but not upon infinite configuration (see Subsection 3.2.1).

Proposition 5.1 (Class B is not causally quantizable) *The quantization of a class B automata is not causal. Hence 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 this also removes much of the motivation behind the papers [57, 58, 97, 7], which contain unitary decision procedures for possibly non-structurally reversible QCA.

5.4.2 Faster quantum signalling.

Second, it is a well-known fact that there exists structurally reversible CA Δ of radius 1/2, but whose inverse CA Δ^{-1} has a larger neighbourhood, e.g. radius 3/2 [78]. Not all such examples are of interest, because often as we iterate Δ^n has radius $n+1/2$ and Δ^{-n} has radius $n+3/2$, and so this difference does not widen. This is not the case of the following example, which we owe to Kari, and whose inverse radius is $2n + 1/2$.

Definition 5.7 (Kari QCA) *Let $\mathcal{C}_f$ be the set of finite configurations over the alphabet $\{q, 0, 1\} \times \{0, 1, 2\}$, with $(q, 0)$ now taken as the quiescent symbol.*

So this can be seen as a two-tape one-dimensional CA, the upper tape having the same cell space as the mXOR, and the lower tape having cell dimension 3. *We call* $\Delta : \mathcal{H}_{\mathcal{C}_f} \longrightarrow \mathcal{H}_{\mathcal{C}_f}$ *the linear operator which we obtain as follows:*

- *first the upper tape undergoes the same evolutions as the mXOR, except that now each XOR gate is conditional to the numbers in the upper tape following each other – otherwise the symbol is left unchanged;*
- *second the lower tape is shifted to the right.*

So classically there exists these structurally reversible CA, of radius half, and whose inverse are of radius 3/2. Now just by defining Δ over $\mathcal{H}_{\mathcal{C}_f}$ by linear extension we ought to have a QCA, but combining Propositions 4.1 and 4.2 we know that Δ and $\Delta^\dagger$ should have the same radius, hence again the apparent paradox.
Again in order to lift this concern let us look at the properties of this quantized $\Delta : \mathcal{H}_{\mathcal{C}_f} \longrightarrow \mathcal{H}_{\mathcal{C}_f}$. It is indeed unitary and shift-invariant of course. This time it is also causal, but counter-intuitively it turns out not to be of 1/2-neighbourhood like its classical counterpart.
Indeed consider d^x a configuration with lower tape $|\ldots 00012012\ldots 01200\ldots\rangle$ and upper tape $|\ldots qq00\ldots 0xqq\ldots\rangle$. Its antecedent under Δ^{-1} has upper tape $|\ldots qq00\ldots 0xxxqq\ldots\rangle$. Its antecedent under Δ^{-2} has upper tape $|\ldots qq00\ldots 0xxx0xqq\ldots\rangle$. Etc. We do not need to know the exact form of the antecedent under $c^x = \Delta^{-n} d^x$, it suffices to notice that the first x and the last x lie at a distance $2n$. Say the first one is with Alice in Paris and the second one with Bob, in New York.
Again consider $c^\pm$ the superposition of the configurations c^0 and c^1. Again just by applying a phase gate Z upon her cell Alice can change c^+ into c^- at time t. But after n steps, the result will be $d^\pm = \Delta^n c^\pm$, which has upper tape $|\ldots qq00\ldots 0\rangle|\pm\rangle|qq\ldots\rangle$. And so her deeds are leading to a perfectly measurable change at time $t + n$ for Bob. Clearly this signal travels a two cells per time step, which is twice the speed of propagation of information which was achievable in the non-quantized version of this CA.
Once more let us take a step back. This Kari CA is another case where exploiting quantum superpositions of configurations enables us to have information flowing faster than in the classical setting, just like for the mXOR CA. But unlike the mXOR CA, the speed of information remains bounded in this CA, and so it can still be considered a QCA (up to cell grouping this is a radius half QCA). Therefore the Kari CA is perfectly valid from a physical point of view, and causal, so long as we are willing to reinterpret what the maximal speed of information should be. Therefore we reach the following proposition.

Proposition 5.2 (Quantum information flows faster) *Let $\Delta : \mathcal{C}_f \longrightarrow \mathcal{C}_f$ be a CA and $\Delta : \mathcal{H}_{\mathcal{C}_f} \longrightarrow \mathcal{H}_{\mathcal{C}_f}$ the corresponding QCA, as obtained by linear extension of Δ. Information may flow faster in the the quantized version of Δ.*

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.
Another possible interpretation of this result would be to say just like in the conclusion of Subsection 5.4.1 that this Kari CA is not possible to implement as a closed system... if the speed of information propagation of the radius half CA is to be interpreted as the speed of light c. Indeed as a closed system it would then admit a quantization – which we have seen would then yield a speed of information propagation of $2c$. In other words the forward evolution of this QCA, if implemented as a closed system, must take at least $2cs$ seconds, with s the distance separating the cells. Of course the lower tape could have been chosen to have cell dimension $d + 1 > 3$ instead of 3, leading to a speed if information propagation for the quantized CA of d times that of the classical CA. Then the forward evolution of this QCA, if implemented as a closed system, would need to be at least dcs seconds. This is counter-intuitive as we would have expected something logarithmic in d, but remember that this constraint comes not so much from the cost of comparing pairwise elements of the lower tape than the cost of having to implement d XORs in parallel and within a closed system. Still these are puzzling results which must be interpreted with caution; and yet it could be that modulo some assumptions there is here methodology to generate some non-trivial absolute speed bound for quantum computation. This route needs to be investigated further.

5.5 Discussion and some open questions ⊛

There are many situations in physics where we want to study a unitary operator U over a large Hilbert space $\mathcal{H}$, and struggle to obtain a practical representation for it. That may be for instance because the spectral theory of infinite-dimensional operators is rather intricate, or because we have no indication that the operator can be approximated via a combination of local unitary operators. Often, however, these infinite dimensional Hilbert spaces arise from the position degree of freedom of a particle. By virtue of the principle according to which information travels at bounded speed, we can then think about 'cutting space into different pieces' such that at each time step, the state of a piece depends solely on that of its neighbours. Whenever this

happens Theorem 5.1 applies and lets you write U as $(\bigotimes D^\dagger)(\bigotimes K_x)(\bigotimes E)$, where D and E are local to each piece and K_x is local to piece x and its neighbours.

And so this is saying something very general which we could dare to summarize by 'Unitarity plus causality implies locality'. If physical evolutions are implementable locally, this means we can focus on local interactions between physical elements, and the global evolution will just a composition of them. And so this statement bridges the gap somehow between general physical principles and the study of elementary interactions. Unfortunately there were several limiting assumptions to this structure theorem, which we now discuss.

A not so uncommon belief amongst theoretical physicists is that the universe being a closed system it should evolve unitarily. Nevertheless this is a rather unpractical view – any everyday physical system is an open system, noisy due to its interactions with the outside world, amongst which any measurement we may wish to do upon the system. And so it evolves not according to a unitary, but according to a quantum operation. Hence one of our most wanted open problem at the moment is to extend Theorem 5.1 to general quantum operations. Several cases of QCA under noise have been studied in [74, 75, 36].

A point which is also rather open to discussion is whether we are indeed allowed to divide up the universe into different 'places' whose state depend only on that of the closest neighbour, in the sort of abrupt and discrete manner which we use here. Having a fixed time arrow about which we take discrete time steps, or being able to account for isotropic phenomena are related questions. We would like to study the relationship between QCA and continuous-space continuous-time models, maybe building upon what has been done for Quantum Lattice Gas Automata [98, 100, 30, 29, 135, 89]. In general it is our intention to understand the extent in which 'causality implies locality' is a general principle in theoretical physics.

Chapter 6

Universalities

The Matrix is a system, Neo. That system is our enemy. When you're inside, you look around, what do you see? Businessmen, teachers, lawyers, carpenters. The very minds of people we're trying to save, but until we do, these people are still a part of that system and that makes them our enemy. You have to understand that most of these people are not ready to be unplugged. And many of them are so inert, so hopelessly dependent on the system that they will fight to protect it. Were you listening to me, Neo? Or were you looking at the woman in the red dress?
—Morpheus, in 'The Matrix'.

We reexplain the notion of intrinsic universality and provide a rigorous definition of it, this time in the context of QCA. We then show that for every dimension n, there is an n-dimensional QCA that is capable of simulating any other n-dimensional QCA – in a topology-preserving, direct manner. For this we have to distinguish the one-dimensional case from the more-than-one-dimensional case, which turns out to be easier. We discuss some possible improvements.

Studying QCA rather than Quantum Turing Machines (QTM) for instance means we bother about the spatial structure of things, whether for the purpose of describing a quantum protocol, modelling a quantum physical phenomena, taking into account the spatial parallelism inherent to the model, working out toy models of theoretical physics, etc... For any of these purposes it is again clear, just like in the classical case, that the kind of universality we require is in fact stronger than just the ability to simulate any QTM. I.e. we should be looking for an intrinsically universal QCA, i.e. a QCA which can simulate all others efficiently and directly.

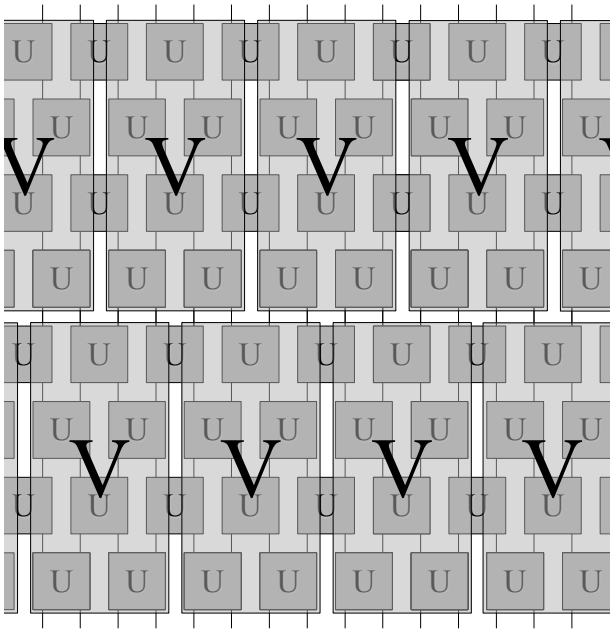

Figure 6.1: Intrinsic simulation of a QCA by another. (The QCA defined by U simulates the QCA defined by V. In this case we need two cells of the U-defined QCA in order to encode one cell of the V-defined QCA, and we need to run the U-defined QCA for four time steps in order to simulate one time step of the V-defined QCA. More generally the challenge is to come up with an initial configuration of the U-defined QCA so that it behaves just as the V-defined QCA with respect to the encoded initial configuration, after some fixed number of time steps. Clearly such an encoding will have to hold the configuration of the V-defined QCA as well as some way of describing the scattering unitary V.)

The closest related work is in the classical realm, where Durand-Lose [53, 54] has described a more-than-one-dimensional intrinsically universal

reversible cellular automaton, and later a one-dimensional intrinsically universal reversible cellular automaton. Our constructions will turn out to be a little simpler, but they cannot be substituted for his back in the classical realm, because reversible circuit universality requires at least one 3-bits gate if done without the help of quantum mechanics. In the realm of quantum computing Watrous [139] has proved that QCA are universal in the sense of Quantum Turing Machines. Then Shepherd, Franz and Werner [122] have defined a class of QCA where the scattering unitary U_i changes at each step i (CCQCA). Via this construct they have built a QCA of cell-dimension 12 which is universal in the circuit-sense. Universality in the circuit-sense had already been achieved by Van Dam [134], Cirac and Vollbrecht [136], Nagaj and Wocjan [105] and Raussendorf [115] – the latter uses a two-dimensional QCA but has this inspiring idea of programs crossing the data, with computation occurring in the interaction. To our knowledge there was no previous work on intrinsically universal quantum cellular automata before we tackled this issue in [15, 16].

6.1 Definitions ⊙⟁

The notion of intrinsic simulation of one CA by another was introduced in Subsection 3.3. In order to quantize this notion our main source of inspiration was [110]. The basic intuition is that in order to say 'G' simulates G' we translate the content of each cell of G into cells of G', run G', and then reverse the translation – and this three step process amounts to just running G. First we must make it clear what we mean by 'translate'. This translation should be simple (the cost of the computation will be carried over only by G'), it should preserve the topology (each cell of G is encoded into cells of G' in a way which preserves neighbours), and it should be faithful (the idea is that no information should be lost in translation). This latter requirement translates into a precise notion in quantum theory, which is that of an *isometry*, i.e. an inner product preserving evolution with $Enc^\dagger Enc = \mathbb{I}$. This same requirement is in line with the translation being a physical process, i.e. that an actual translating machine could be built, in theory. With this in mind we derive the following definitions.

Definition 6.1 (Isometric coding) *Consider $q + \Sigma$ and $q'' + \Sigma''$, two alphabets with distinguished quiescent states q and q'', and such that $|q + \Sigma| \leq |q'' + \Sigma''|$. Consider $\mathcal{H}_{q+\Sigma}$ and $\mathcal{H}_{q''+\Sigma''}$ the Hilbert spaces having these alphabets as their basis, and $\mathcal{H}_{\mathcal{C}_f^{q+\Sigma}}$, $\mathcal{H}_{\mathcal{C}_f^{q''+\Sigma''}}$ the Hilbert spaces of finite configurations over these alphabets.*

Let E be an isometric linear map from $\mathcal{H}_{q+\Sigma}$ to $\mathcal{H}_{q''+\Sigma''}$ which preserves quiescence, i.e. such that $E|q\rangle = |q''\rangle$. It trivially extends into an isometric linear map $Enc = (\bigotimes_{\mathbb{Z}^n} E)$ from $\mathcal{H}_{\mathcal{C}_f^{q+\Sigma}}$ into $\mathcal{H}_{\mathcal{C}_f^{q''+\Sigma''}}$, which we refer to as an isometric encoding.
Let D be an isometric linear map from $\mathcal{H}_{q''+\Sigma''}$ to $\mathcal{H}_{q+\Sigma} \otimes \mathcal{H}_{q''+\Sigma''}$ which also preserves quiescence, in the sense that $D|q''\rangle = |q\rangle \otimes |q''\rangle$. It trivially extends into an isometric linear map $Dec = (\bigotimes_{\mathbb{Z}^n} D)$ from $\mathcal{H}_{\mathcal{C}_f^{q''+\Sigma''}}$ into $\mathcal{H}_{\mathcal{C}_f^{q+\Sigma}} \otimes \mathcal{H}_{\mathcal{C}_f^{q''+\Sigma''}}$, which we refer to as an isometric decoding.
The isometries E and D define an isometric coding if the following condition is satisfied:

$$\forall |\psi\rangle \in \mathcal{H}_{\mathcal{C}_f^{q+\Sigma}},\ \exists |\phi\rangle \in \mathcal{H}_{\mathcal{C}_f^{q''+\Sigma''}} \quad / \quad |\psi\rangle \otimes |\phi\rangle = Dec\left(Enc|\psi\rangle\right).$$

(The understanding here is that Dec is morally an inverse function of Enc, but we may leave out some garbage $|\phi\rangle$ on the way.)

Definition 6.2 (Direct simulation) *Consider $q+\Sigma$ and $q''+\Sigma''$, two alphabets with distinguished quiescent states q and q'', and two QCA G and G'' over these alphabets. We say that G'' directly simulates G, if and only if there exists an isometric coding such that*

$$\forall i \in \mathbb{N},\ \forall |\psi\rangle \in \mathcal{H}_{\mathcal{C}_f^{q+\Sigma}},\ \exists |\phi\rangle \in \mathcal{H}_{\mathcal{C}_f^{q''+\Sigma''}} \quad / \quad (G^i|\psi\rangle) \otimes |\phi\rangle = Dec\left(G''^i\left(Enc|\psi\rangle\right)\right).$$

Unfortunately this is not enough for intrinsic simulation. Often we want to say that G' simulates G even though the translation:
- takes one cell of G into several, not just one cell of G';
- hence the quiescent symbol q becomes a quiescent word q';
- G' needs be run t times instead of just once.
All of these changes are made formal via the notion of grouping, as in the following definitions.

Definition 6.3 (Grouping) *Let G' be a QCA over alphabet $q'+\Sigma'$. Let s and t be two integers, q'' a word in $(q'+\Sigma')^{s^n}$, and $\Sigma'' = \Sigma'^{s^n}$. Consider the iterate global evolution G''^t up to a grouping of each hypercube of s^n adjacent cells into one supercell. If this operator can be considered to be a QCA G'' over $q''+\Sigma''$, then we say that G'' is an (s,t,q')-grouping of G'.*

Definition 6.4 (Intrinsic simulation) *Consider $q+\Sigma$ and $q'+\Sigma'$, two alphabets with distinguished quiescent states q and q', and two QCA G and G' over these alphabets. We say that G' intrinsically simulates G if and only if there exists G'' some grouping of G' such that G'' directly simulates G.*

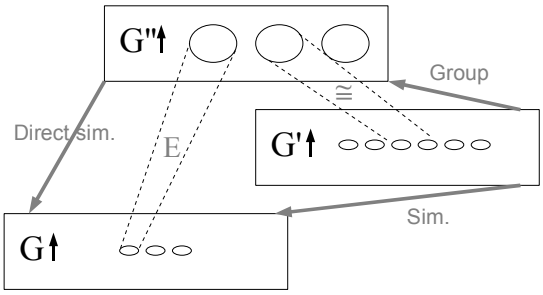

Figure 6.2: The notion of intrinsic simulation made formal.

In other words, G' intrinsically simulates G if and only if there exists some isometry E which translates each cell of G into s cells of G', such that if we then run G'^t and translate back, the whole process is equivalent to a run of G only. This understanding is captured by Fig. 6.2.

6.2 Intrinsically universal QCA : $1D$ case ⟁

In Section 4.3 we have recalled the formal definition of one-dimensional QCA, and in Section 5.2 we have shown that all have a simple circuit-like structure – i.e. they are expressible as PQCA. Ultimately the picture one needs to have in mind in order to follow this section is just that of Figure 4.1.
In Section 6.1 we have provided a formal definition for the notion of intrinsic simulation. But again the picture one needs to have in mind in order to follow this section is just that of Figure 6.1.
The purpose of this section is to find a particular U-defined QCA, and which is capable of intrinsically simulating any V-defined QCA, whatever the V. In order to describe that U-defined QCA we need to describe two things:
- How its cells are like (i.e. what are the vertical lines of Figure 4.1 composed of. What is the dimensionality of U?). By definition of QCA they are finite dimensional quantum systems of some fixed dimension d of course, but for clarity we will decompose these into subsystems of dimension d_i, and we will give names to these subsystems according to their purpose (i.e. the vertical lines of Figure 4.1 are 'buses').
- How U acts upon a pair of these cells, and more precisely upon the subsystems making up the pair of cells. We will say this informally, but we will also provide a formal circuit description of U, and check that such a U is indeed a unitary.

Before continuing with our detailed discussion of this precise intrinsically universal one-dimensional QCA, it is useful to make precise some of the vocabulary and conventions that will be encountered in the rest of the chapter. By a *subsystem* we mean a constituent of a cell that serves a specific function in our QCA. A subsystem may take many different *values*. Subsystems have their names written in bold. The term *signal* is used to refer to the value of a certain subsystem when it consistently travels between a cell and its left/right neighbour. In the space-time diagram of the QCA, a signal looks like a 'line' propagating through cells. Usually we take the name of a signal to be the name of the subsystem that takes those values.
This section will be organized as follows: first we give an intuitive idea about the mechanism we used to solve this problem, then we will explain different components of the QCA in detail, and finally we will see how this all fits together.

6.2.1 Intuition

The cells of our universal, U-defined, QCA will have a subsystem called **data** used for encoding one qubit of information about the state of a cell of the simulated, V-defined QCA. Hence one simulated cell (dotted oval in Figure 6.3) will in general be encoded as several adjacent simulating cells (small grey ovals in Figure 6.3). We also need to simulate the action of some arbitrary unitary V, and so the cells of our universal QCA will have a subsystem called **program**, holding some description of one of the elementary universal quantum gates that make up V. Hence V (dotted box in Figure 6.3) will in general be encoded as several adjacent simulating cells (small black ovals in Figure 6.3). Because V originally acts upon two cells, it is encoded in the surroundings of the two encoded cells.
During a first phase, as time unravels, the information held in the **data** subsystem of the encoded cells remain stationary, and so we can think of them as some stationary data signals. Meanwhile the information held in the **program** subsystems of the surroundings travels at lightspeed, and we can think of this as moving program signals. The program signals cross the data signals, leaving them unchanged, until they collide between one another. When that happens an elementary universal quantum gate is applied on the **data** subsystems (grey box in Figure 6.3), thereby implementing V. Which elementary universal quantum gate gets applied depends on the value of the colliding program signals. Where the elementary universal quantum gate gets applied depends on where the collision takes place.
During a second phase, we need to 'reload' this situation, with the added difficulty that V gets applied in a shifted manner. Hence we need to arrange

so that the left/right encoded cell travels left/right in order to meet with their right/left counterpart on the next site (travelling small grey ovals in Figure 6.3).

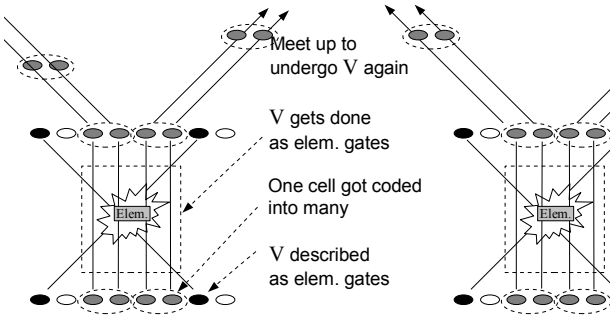

Figure 6.3: Outline of the simulation scheme.

We will explain how to do this in three steps. First we draw a background pattern which allows us to synchronize this whole process. Second we let some data signals flow upon this background. Third we let the program signals move upon the background, crossing and acting upon the data signals. Note that whenever we write $|dgp\rangle$ for the state of a cell, we mean that the subsystem **data** is in state $|d\rangle$, subsystem **program** is in state $|g\rangle$, subsystem **mode** is in state $|p\rangle$.

6.2.2 Ternary background pattern

First we seek to draw the *ternary background pattern* of Figure 6.4, where the large squares cycle through the three colours Light grey, Middle grey or Dark grey. The reason why this is useful will become clear in the next Subsection, for now it suffices to know that this ternary background pattern will help us synchronize the flow of the data signals as in Figure 6.3 and hence organize the computation as we add more interesting things to the initial configuration, i.e. the bottom of the diagram.
In order to achieve this ternary background pattern each cell must contain a 3-dimensional system to code for those three different colours. This is really the purpose of subsystem **mode**: when the **mode** equals 0, 1 or 2 the background colour is Light grey, Middle grey or Dark grey respectively. We must then place some signals at regular intervals, travelling at lightspeed and telling mode signals that they must change colour, and this is really role played by state $|1\rangle$ of subsystem **program**.

Let us show that the scattering unitary U which is given in Figure 6.9 does the job of generating Figure 6.4. Observe Figure 6.9 and notice that the content of the **mode** and **program** subsystems is always propagated unchanged by the scattering unitary U, to the right/left if it comes from the left/right. Moreover observe Figure 4.1 and notice that at the next layer the content of **mode** and **program** will again come up from the left/right and hence be propagated again to the right/left. Hence whatever value is in the **mode** or in the **program** subsystem it just travels at maximal speed, right or left, depending only upon its position in the initial configuration. This is just what we mean by 'a signal propagating at lightspeed'. In Subsection 6.2.5 we provide all extra information needed about Figure 6.9 so that the behaviour of U becomes fully-determined. We then state that $|1\rangle$ in the **program** subsystem is the control value required for the **+1 mod 3** to apply upon the **mode** subsystem. Hence the 'Change colour' signals are indeed implemented by setting some cells to have their subsystem **program** initialized at $|1\rangle$ as in Figure 6.4, and the 'Change colour' signals indeed propagates at lightspeed, changing the value of the mode signals travelling at lightspeed in the opposite direction.
Notice that later, when we will set the **data** subsystem to non-$|0\rangle$ values in order to code for simulated cells, or use up the other possible values of the **program** subsystem in order to code for elementary universal gates to be applied upon the coded simulated cells, this ternary background pattern will remain unaffected. This is obvious from Figure 6.9 and the fact that $|1\rangle$ is the only value of **program** which triggers the **+1 mod 3** gate.
The required widths of the Light grey and Middle grey zones of the initial configuration vary depending upon the V-defined QCA we are seeking to simulate, in a way which we explain in Subsection 6.2.3 and 6.2.4, respectively.

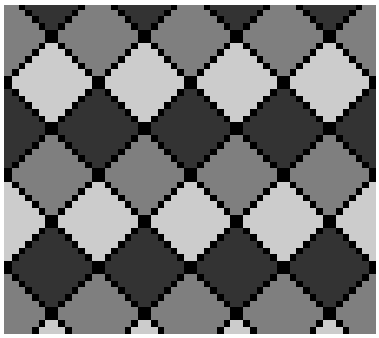

Figure 6.4: Ternary background pattern. Each small coloured square now represents the state of a cell at time t. This is unlike in the previous figures, where boxes would represent a unitary evolution. At the bottom we have the initial configuration. Time flows upwards as usual. Each configuration is determined by the one below by pairing up the small squares of the configuration below and applying the scattering unitary U to these pairs. The way they are paired up alternates in time: for odd steps cell 0 is paired with cell 1, cell 2 with cell 3, etc., whereas for even steps cell 1 is paired up with cell 2, cell 3 with cell 4, etc. The Light grey, Middle grey and Dark grey colours correspond to different values of the **mode** subsystem of the cells. They are separated by 'Change colour' signals, represented in Black. (With $|000\rangle$ in Light grey, $|001\rangle$ in Middle grey, $|002\rangle$ in Dark grey, and $|?1?\rangle$ in Black.)

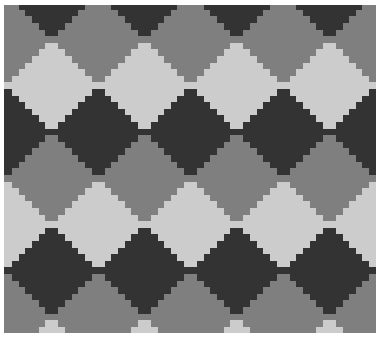

Figure 6.5: Ternary background pattern. This is the same as Figure 6.4 except we no longer show the 'Change colour signals'. (With $|??0\rangle$ in Light grey, $|??1\rangle$ in Middle grey, $|??2\rangle$ in Dark grey.)

6.2.3 Hexagonal data signals flow

Second we seek to draw the *hexagonal data signals flow* of Figure 6.6. That is we want to implement data signals, and would like that the data signals

remain stationary for a while, and then separate into a left moving and a right moving bunch of data signals, only to eventually rejoin their left and right counterparts in order to flow straight in time again, as was explained in Figure 6.3. As previously mentioned, the reason why we want to achieve this particular form of data signals flow is that it corresponds to the overall architecture of the QCA we are trying to simulate as in Figure 6.1, with the interaction unitary V taking its inputs as coming both from the left and the right, computing upon them, and spitting its outputs again both towards the left and the right for another run of V.
In order to achieve this each cell must contain another 3-dimensional subsystem to code for a data signal. This is really the purpose of subsystem **data**: when the **data** equals $|0\rangle$, $|1\rangle$ or $|2\rangle$ the cell carries no data, an encoded $|1\rangle$ or an encoded $|2\rangle$ respectively. We must then place the encoded data qubits in the Light grey coloured zones of the initial configuration, i.e. replacing the $|000\rangle$ cells by $|100\rangle$ cells in order to code for the presence of an encoded $|0\rangle$, and $|000\rangle$ by $|200\rangle$ in order to code for the presence of an encoded $|1\rangle$.
Let us show that the scattering unitary U which is given in Figure 6.9 does the job of generating Figure 6.6. The intuitive explanation will of course be that the Grey levels of the ternary background pattern are here to tell the data whether it can move or not, with the Middle and Dark grey forcing it to remain stationary, and the Light grey allowing it to move freely until they are gathered by a Middle grey funnel again. The more formal explanation relies on looking at the scattering unitary matrix U which is given in Figure 6.9 in order to understand when the value of the left/right **data** subsystem is propagated to the right/left, and when it is just left sitting on the left/right. This is what determines whether a data signal is stationary or moving at lightspeed. In order to have a complete answer to this question one must look at the definition of the S gate in Figure 6.9, as provided in Subsection 6.2.5. There we find that S swaps the left and right **data** subsystems but only if one of them is $|0\rangle$ (i.e. a data signal moves right/left only if there is no data signal there) and if the values of both **mode** subsystems are $|0\rangle$ (i.e. the Light grey zones of the ternary background pattern). Initially the data signals are in a Light grey zones, but they are stuck upon another, so they cannot move. Not even the ones on the left and right ends can move – due to the surrounding Middle grey zones. Clearly this stationary situation will be maintained until the ones on the left and right ends become surrounded by Light grey zones. During this period the data signals are freed two by two, with the one on the left end going to the left, and the one on the right end going to the right. Finally the first right moving data signal meets up with the first left moving data signal, and so they are stuck by one another for one step. But that one step is enough so that the second right/left moving

data signal rejoins the first, so that the second one also gets stuck against the first, and the first does not bounce back. When all of the right/left moving signals have done so we are back to the original situation. Hence this ability of the ternary background pattern to 'mold' the flow of data signals into the hexagonal shape of Figure 6.6.

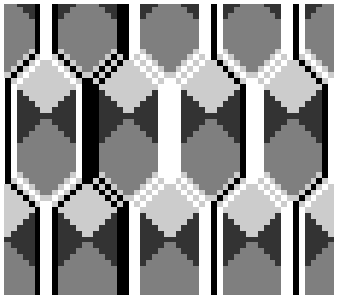

Figure 6.6: Molding the hexagonal data flow pattern. The ternary background of Figure 6.5 is now used to tell the data signals when it is they should stay stationary, and when it is they should move to go and meet their counterparts. We show the data signal as White for an encoded $|0\rangle$ qubit and Black for an encoded $|1\rangle$ qubit. (With $|0?0\rangle$ in Light grey, $|0?1\rangle$ in Middle grey, $|0?2\rangle$ in Dark grey, $|1??\rangle$ in White, $|2??\rangle$ in Black.)

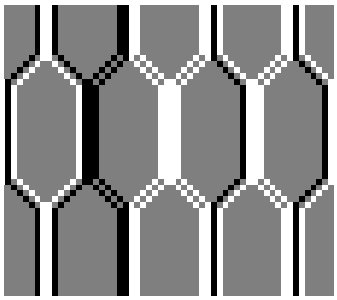

Figure 6.7: Hexagonal data flow pattern. This is the same as Figure 6.6 except we no longer show the ternary background. (With $|0??\rangle$ in Grey, $|1??\rangle$ in White, $|2??\rangle$ in Black.)

Notice that the required width of the Light grey zone of Figure 6.4 has now become apparent. Since the purpose of this Light grey zone is to encode the state of two cells of the simulated QCA, it needs to be twice as big as the number of qubits that are needed to encode one cell of the simulated, V-defined QCA.

6.2.4 Collision gates

Third we seek simulate the scattering unitary V, as in Figure 6.8. As was explained in Figure 6.3, the key idea here is that during the time the data signals are stationary, they may be crossed by program signals incoming from both their left and their right, and sometimes these program signals even collide against one another upon the data signals. The value of the colliding program signals is what will specify *what* should happen to the data signals, through a numbering of a set elementary universal quantum gates. The relative positions of the program signals is what will specify *where* this should happen, by determining where they collide.

In order to achieve this we must change some of the $|0\rangle$ values of the **program** subsystems of the Middle grey zones of the initial configuration, and allow them to take extra values $|2\rangle$ and $|3\rangle$. I.e. we will change some $|001\rangle$ cells into $|021\rangle$ or $|031\rangle$ cells and generate program signals carrying value $|2\rangle$ or $|3\rangle$, which will then travel at lightspeed, collide and so implement gates upon the data signals.

Let us show that the scattering unitary U which is given in Figure 6.9 does the job of generating Figure 6.8. We have already shown in Subsection 6.2.2 that the program signals travel at lightspeed, unaffected. The only thing we need to explain is what happens when they collide with one another. Again from Figure 6.9 and Subsection 6.2.5 we have that whenever two program signals (**xprogram** and **yprogram** are both $|2\rangle$ or $|3\rangle$) cross each other upon some data signals (**xdata** and **ydata** non-$|0\rangle$) then some elementary quantum gate is applied upon **xdata**$\otimes$**ydata** as given in Table 6.2. The mechanism is illustrated in Figure 6.8 but with essentially classical elementary gates – so that we may draw their effect.

Notice that the required width of the Middle grey zone of Figure 6.4 is starting to become apparent. Since the purpose of this Middle grey zone is to hold pairs of program signals, each pair coding for one of the elementary universal quantum gate implementing V, its size will depend will depend upon the number of elementary universal quantum gates of the circuit-description of V. However the exact size of those Middle grey zones will be determined in Subsection 6.2.6.

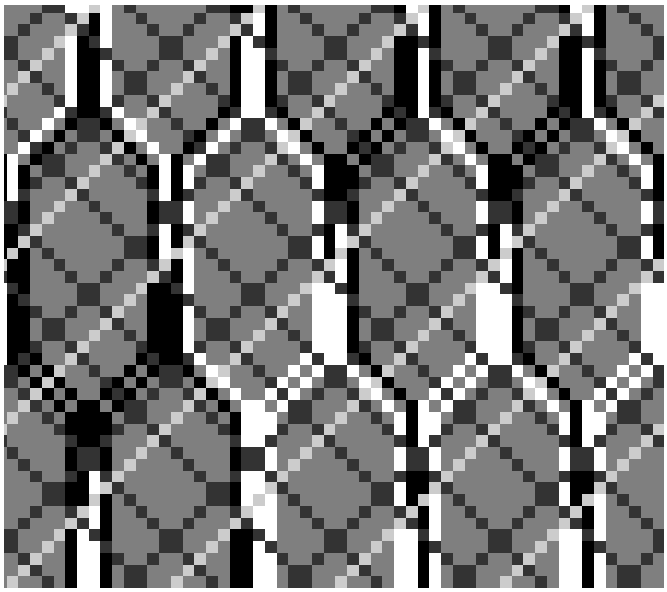

Figure 6.8: Circuitry. The Middle grey initial zone of Figure 6.7 has been modified in order to include two $|3\rangle$-valued program signals (here in Dark grey) and one $|2\rangle$-valued program signal (here in Light grey). This was done by changing two adjacent $|001\rangle$ to $|031\rangle$, and a $|001\rangle$ to $|021\rangle$. We can see that these program signals travel at lightspeed and sometimes collide. When they do so a two qubits elementary universal gate gets applied upon the data signals. The nature of the gate depends upon the values of the colliding program signals, whereas the position where the gate applies depends upon the place where the collision occurs. (Here whenever two $|3\rangle$-valued program signals intersect a $cNot$ gate get applied to the data signals below them, whereas whenever a $|2\rangle$-valued program signal meets a $|3\rangle$-valued program signal a $\mathbb{I} \otimes Not$ gets applied. With $|?3?\rangle$ in Dark grey, $|?2?\rangle$ in Light grey, $|20?\rangle$ and $|21?\rangle$ in White, $|20?\rangle$ and $|21?\rangle$ in Black, and the rest in Grey.)

6.2.5 The scattering unitary

So overall our universal, U-defined, QCA consists of a repeated application of one scattering unitary U as in Figure 4.1. Now follows the summarized description of the structure of the cells and the scattering unitary U.

Structure of the cells. In Figure 4.1 each vertical line does not represent just one qubit but a 36-dimensional quantum system made of the subsystems described in the following table.

Structure of the scattering unitary U. In Figure 4.1 the scattering unitary U takes two inputs $\mathbf{x}$ and $\mathbf{y}$, each of which decomposes into three subsystems

xdata, **xprogram**, **xmode** and **ydata**, **yprogram**, **yprogram** respectively, as mentioned. Therefore it could be given as a $36^2 \times 36^2$ matrix of complex numbers, yet fortunately it decomposes as in Figure 6.9.

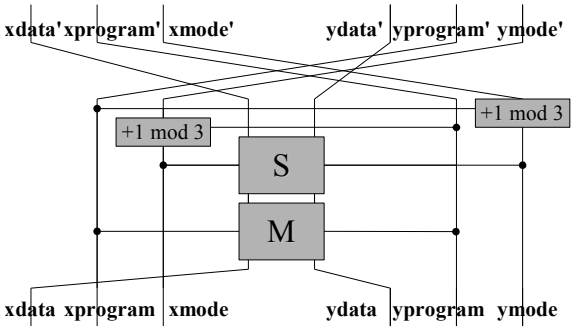

Figure 6.9: The scattering unitary U as a quantum circuit. The three left/right lines represent the three subsystems making up the left/right cell. Each square represents an elementary quantum gate being applied of these subsystems, conditional to the value of the control systems designated by the horizontal lines. Time flows upwards. The whole thing represents the scattering unitary U, it takes two cells and yields back two cells.

In this diagram horizontal lines are control lines. Let us explain what we mean by control lines in general, as this will provide us with the main step of the proof of the unitarity of U. Say that a box labelled B applies upon systems $S_1, \ldots, S_p$ whilst having an horizontal line crossing systems $T_1, \ldots, T_q$, then its effect is to apply the unitary evolution B_i whenever the control system is in state $|i\rangle$ – and linearly so. This being said we are now in a position to describe the three gates used, in terms of whatever canonical basis state their control systems may take. Of course the control systems do

Name	Size	Function
data	3	To hold one qubit of data of the QCA being simulated ($\|0\rangle$ ≡Empty, $\|1\rangle$ ≡Encoded $\|0\rangle$, $\|2\rangle$ ≡Encoded $\|1\rangle$).
program	4	To code for what quantum gate should be applied to the data ($\|0\rangle$ ≡Empty, $\|1\rangle$ ≡Change colour, $\|2\rangle/\|3\rangle$ ≡cf. Table 6.2)
mode	3	To synchronize the flow of the data signals ($\|0\rangle$ ≡Light grey $\|1\rangle$ ≡Middle grey, $\|2\rangle$ ≡Dark grey).

Table 6.1: Subsystems of cells of the universal QCA.

xprogram $\otimes$ **yprogram**	**Action of M**	
$\|22\rangle$	$Swap$	
$\|23\rangle$	$\mathbb{I} \otimes H$	Hadamard on the second qubit
$\|32\rangle$	$H \otimes \mathbb{I}$	Hadamard on the first qubit
$\|33\rangle$	$cPhase$	
$otherwise$	$\mathbb{I} \otimes \mathbb{I}$	

where $cPhase$ stands for $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/4} \end{pmatrix}$.

Table 6.2: The **M** gate.

not actually have to be in a basis state, by linear extension and the above lemma. We shall see that the first two gates are used really just to move the encoded data qubits around, whereas the last gate actually does perform the computation.

- The **+1 mod 3** gate. If **xprogram**$\neq |0\rangle$ and **yprogram**$= |4\rangle$, then **xmode** is incremented by one modulo three. Else this is the identity. (Symmetrically so swapping the roles of **x** and **y**.) This step's role is to increment the modes, which in turn synchronizes the flow of the data signals.

- The **S** gate. If **xprogram**$= |0\rangle$, and **yprogram**$= |0\rangle$, then permute $|01\rangle$ with $|10\rangle$ and $|02\rangle$ with $|20\rangle$. Else this is the identity. This means we are swapping **xdata** and **ydata** only if one of them is empty and the modes are 'White'. This step's role is to move the data when appropriate, in order to actually perform the flow of data.

- The **M** gate. If **xdata**$\neq |0\rangle$, **ydata**$\neq |0\rangle$, **xprogram**$= |2\rangle$ and **yprogram**$= |2\rangle$, then the system **xdata**$\otimes$**ydata** undergoes an elementary quantum gate according to the state of the system **xmode**$\otimes$**ymode** as in Table 6.2. This step's role is to apply a quantum gate upon two qubits of data, in order to perform the computation.

In the next subsection we show how this all fits together to obtain the intrinsic universality. Beforehand however, note that since we have described the evolution U as a combination of smaller unitary matrices via tensors,

composition and the control-construct, it is indeed unitary as required by Definition 4.4.

6.2.6 Results

First let us show that we have a universal set of gates available in the QCA. The set of gates which the M gate is able to perform upon the data qubits has been chosen to be universal in the traditional sense, i.e. any finite dimensional unitary evolution V can be approximated by tensors and compositions of these gates. We have not chosen the standard set [34] ($cNot$, H, $Phase$) so as to preserve the **xy** symmetry of the unitary evolution U and yet keep the dimension of **program** to a minimum, but it is easy to see that we can recover the standard set since

$$cNot|\psi\rangle = (\mathbb{I} \otimes H)(cPhase)^4(\mathbb{I} \otimes H)|\psi\rangle$$
$$|1\rangle \otimes Phase|\psi\rangle = cPhase|1\rangle \otimes |\psi\rangle$$

where the ancilla $|1\rangle$ can be brought over via applications of the $Swap$ gate.

Then according to the formal definition of U which we have given in Subsection 6.2.5 and the construction we have described informally in Subsections 6.2.1, 6.2.2, 6.2.3, 6.2.4 and formally in [15] we reach the following theorem.

Theorem 6.1 *There exists G' a U-defined QCA which is intrinsically universal QCA in the following sense. Let G be V-defined QCA such that V can be expressed as a quantum circuit C made of m gates acting upon $2n$ qubits. Then G' is able to intrinsically simulate G with space expansion factor $s = 4nm + 2 + 2n$ and time expansion factor $t = (3/2)s$.*

Note that if the scattering unitary V is only approximated with an error of $\epsilon = \max_{|\psi\rangle} \||V|\psi\rangle - C(V)|\psi\rangle\|$ by the quantum circuit $C(V)$, then this entails we are able to intrinsically approximate the evolution of s cells over t steps with an error bounded by $st\epsilon$ – again using supercells of size $s = 4nm + 2 + 2n$ and a time expansion of factor $t = (3/2)s$. This is the general statement that errors in quantum circuits grow no more than proportional to time and space [108], which stems from the fact that if $\|U - U'\| \leq \epsilon$ then $\|U^{\otimes s} - U'^{\otimes s}\| \leq s\epsilon$ and $\|U^t - U'^t\| \leq t\epsilon$.

Summarizing, we have constructed a one-dimensional QCA capable of simulating all others with linear overhead, exactly if the scattering unitaries they are made of decompose into a circuit of elementary quantum gates, and

approximately otherwise. This intrinsically universal QCA, is a Partitioned QCA (Figure 4.1) of cell-dimension 36 and whose scattering unitary we have given explicitly (Figure 6.9 and Subsection 6.2.5).

6.3 Intrinsically universal QCA : $> 1D$ case ⊙⏢⊛

6.3.1 Circuit universality versus intrinsic universality in higher dimensions

Intrinsic universality refers to the ability for one CA to simulate any other CA in a way which preserves the spatial structure of the simulated CA. Turing machine universality refers to the ability for one CA to simulate any Turing Machine, and hence run any algorithm; this is also known as computation-universality. Circuit universality refers to the ability of one CA to simulate any circuit. We mean the usual finitary combination of logical gates, e.g. NAND gates for classical circuits and CA, or TOFFOLI gates for reversible circuits and CA, etc. Informally, in the quantum setting, this means having a QCA which is capable of simulating a unitary evolution expressed as a combination of a universal set of quantum gates, such as the standard gate set: CNOT, PHASE, and HADAMARD.

An interesting question to ask is what is the relationship between these three notions of universality for CA [93, 50]? Clearly a computation universal CA is also a circuit universal CA, because circuits are simply finitary computations. Moreover, an intrinsic universal CA is also a computation universal CA, because it can simulate any CA; including computation universal CA. Hence intrinsic universality implies computation universality implies circuit universality. Could this be an equivalence?

In one-dimension we see immediately that this is not the case. Intuitively, computation universality requires more than circuit universality, namely the ability to loop the computation, which is not trivial to organise for a CA. Similarly, intrinsic universality requires more than computation universality, namely a property such as the ability to simulates various communicating Turing machines, not just one. In the classical setting there are formal results to distinguish them; see reference [110].

In n-dimensions there is a commonly held opinion in the CA community according to which circuit universality implies intrinsic universality, and hence all of these notions are equivalent, see for example reference [110]. Strictly speaking this is not true of course. For example, consider a 2-dimensional

CA which runs one-dimensional CA in parallel. If the one-dimensional CA is circuit/computation universal, but not computation/intrinsically universal, then so is the 2-dimensional CA. In the QCA setting it really seems that the 2-dimensional constructions in [41] and [115] are indeed circuit universal but not intrinsically universal – though we could be wrong, as non-universality is often even harder to prove than universality. And still this is worthwhile opinion to have.

Indeed as we have seem any CA admits a block representation, and for reversible CA these blocks are simply permutations (see Subsection 4.1.2). In Section 5.2 we saw that QCA also admit a block representation, and that these blocks are unitary matrices. This means we can express the evolution of any (Quantum/Reversible) CA as an infinite (quantum/reversible) circuit of (quantum/reversible) gates repeating across space. Hence the intuition that if a CA is circuit universal, and if it has the ability of wiring up together different pieces of circuits in different regions of space, then it can simulate the block representation of any CA, and hence it can simulate any CA in a way which preserves its spatial structure – it is intrinsically universal.

This is the route we will follow in order to construct our intrinsically universal n-dimensional QCA. First we will explain how to construct the 'wires' which can carry information across different regions of space. In this setting these are just signals travelling in space, which can be redirected or delayed by bouncing them off barriers, with each signal holding a qubit of information. Secondly, it will be explained how to construct the 'pieces of circuits', i.e. how to implement gates and combine them. One and two qubit gates will be implemented as obstacles to and collisions of these signals.

In order to give a formal completion to the proof, it is shown that since any n-dimensional QCA can be expressed as a PQCA, we can flatten this infinitely repeating two-layered circuit into space (i.e. so that at the beginning all the qubit carrying signals find themselves in pieces of circuits each implementing one of the scattering unitary of the first layer, and then they all synchronously exit and travel to pieces of circuits each implementing the scattering unitary of the second layer, etc.).

Ideally we would provide an algorithm for performing this flattening. We do not describe the process in too high a level of detail to maintain clarity, as per the corresponding classical literature. However, a good intuition of the flattening process for a 2-dimensional PQCA is presented in Figures 6.10 to 6.13. Clearly we can do the same in n-dimensions.

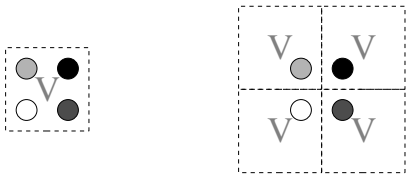

Figure 6.10: Flattening a PQCA into a UQCA. Consider four cells (white / light grey / dark grey / black) of a PQCA having scattering unitary V. The first layer PQCA applies V to these four cells (left), then the second layer applies V at the four corners (right). We need to flatten this so that the two-layers become non-overlapping.

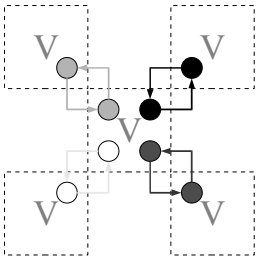

Figure 6.11: Flattening a PQCA into a UQCA. We now flatten the two layers from time to space. The first layer corresponds to the square at the centre. The second layer corresponds to the squares at the four corners. At the beginning the signals (white / light grey / dark grey / black) coding for the simulated cells find themselves in the square at the centre. They undergo V. Then they are directed towards the bottom left / top left / bottom right / top right squares at the corners, where they undergo V but are paired up with some other signals coding for other simulated cells. They are then directed back to the central square. This gets repeated.

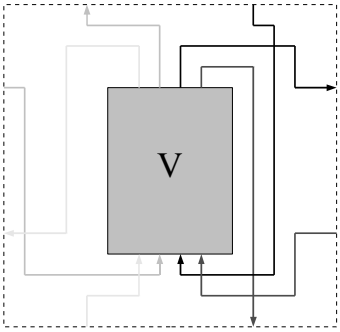

Figure 6.12: Flattening a PQCA into a UQCA. Within the central square of Figure 6.11, the incoming signals (white / light grey / dark grey / black) coding for the simulated cells are bunched together so as to undergo a circuit which implements V. Then they are then dispatched towards the four corners. This diagram does not make explicit a number of signal delays, which may be needed to ensure that they arrive synchronously at the beginning of the circuit implementing V.

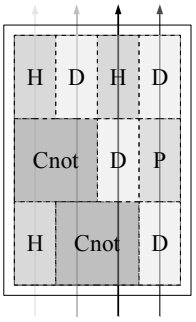

Figure 6.13: Flattening a PQCA into a UQCA: within the central rectangle of Figure 6.12 The circuit which implements V is itself a combination of smaller circuits for implementing a universal set of quantum gates such as CNOT, HADAMARD and the PHASE, together with Delays. These are implemented as explained in Subsections 6.3.2 and 6.3.3.

6.3.2 Qubit carrying signals and barriers

We begin by explaining how to code for signals travelling along the cardinal directions of space. Each cell requires two axis subsystems, x**-axis** and y-

axis which can be either empty, or hold a single qubit. The direction of propagation does not need to be signed, i.e. it suffices to know that a particle is travelling along some axis (e.g. the x-axis) and to know the parity of its position (e.g. on a left cell or a right cell) in order to know the direction in which it is travelling along the axis . This is because whenever a unitary interaction U acts upon a square of four cells, there is only one choice of cell for the propagation of the signal (e.g. a signal at the bottom right travelling along the x-axis can only move to the bottom left).
The ability to redirect these signals is also required, and this is achieved by 'bouncing' them off a barrier. It will be shown that this is all the structure required for our intrinsically universal U-defined QCA. We begin with an informal explanation of its dynamics. The movement operation is shown

Name	Size	Function
x**-axis**	3	Empty, or holding a qubit signal: ϵ,$\|0\rangle$, $\|1\rangle$.
y**-axis**	3	Empty, or holding a qubit signal: ϵ, $\|0\rangle$, $\|1\rangle$.
barrier	2	Empty, or holding an axis-change barrier: ϵ, $\times$.

Table 6.3: Subsystems of a cell dealing with qubit carrying signals and barriers.

in Figure 6.14, it acts on an entire neighbourhood of four cells. The effect of the **barrier** subsystem is given in Figure 6.15, and acts on individual cells; note that for now we assume that only one of the **axis** subsystem is carrying a qubit. Collisions, when two qubits are occupying the same cell, will be dealt with in the following section. The movement permutation is applied to the cell neighbourhood first, followed by the single cell operations.
Already, using only these operations we can easily delay (see Figure 6.16) and swap (see Figure 6.17) signals. For signals to be correctly synchronised, each operation takes 24 time-steps, and each qubit operates in a 4×16 cell grid so that they can be plugged together as in Figure 6.13.

6.3.3 Collisions and derived gates

Two qubit-carrying signals may meet and collide. No extra structure is required to enable this, it is simply modelled by both the x**-axis** and the y**-axis** subsystems of a single cell holding a qubit. In order to allow a universal set of gates to be implemented by our QCA, an extra meaning will now be attached to the collision of two signals : it is interpreted as the application of a two qubit gate. Indeed collisions between two signals will apply the either the Hadamard operation on both carried qubits, or the CPHASE gate

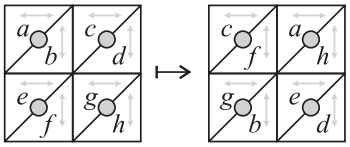

Figure 6.14: The rule for the basic movement of signals is presented here. Each cell is denoted by a single square split into three. The circle in the middle holds the **barrier** subsystem, while the top-left triangle holds the x**-axis** subsystem, and the bottom-right triangle holds the y**-axis** subsystem (as denoted by the grey arrows). Movement leaves the **barrier** subsystem unchanged, and acts as a simple permutation of the **axis** subsystems, shown in the diagram by the variables a to h. This operation is self-inverse on the basis states, and hence unitary.

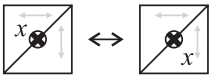

Figure 6.15: This diagram shows the effect of the **barrier** subsystem (×) when there is only one occupied axis, and the action is simply to exchange the axis subsystems. The barrier subsystem remains unchanged.

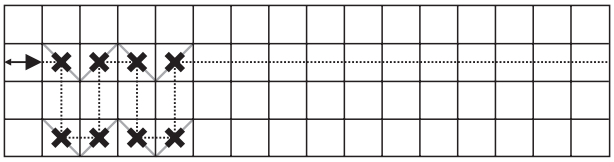

Figure 6.16: An 'identity circuit" configuration, a 4×16 configuration taking 24 time-steps made from two consecutive delay configurations. The dotted line shows the trajectory of the signal, and the arrow denotes the entry point and direction of signal propagation.

(controlled-phase, with the phase change defined as $e^{\frac{i\pi}{4}}$) on both carried qubits – depending upon whether there is or not a barrier. If a barrier is present the signals are also deflected, as expected; otherwise the signals continue on their original trajectory. Note that if we do not want a two qubit gate to apply, but simply want to cross-over the two signals, then the swap configuration of Figure 6.17 can be used. The operations for interpreting collisions are given in Figure 6.18, for when the **barrier** subsystem is empty, and Figure 6.19, for the case when a barrier is present.

From these building blocks a two qubit CPHASE gate configuration, and one qubit PHASE gate and HADAMARD gate configurations can be con-

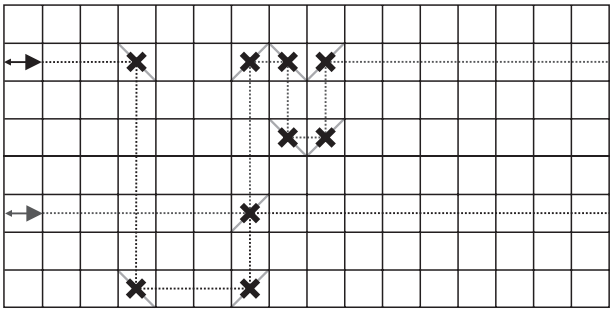

Figure 6.17: The 'swap circuit" configuration, an 8×16 configuration taking 24 time-steps which permutes the two inputs. Note that no cell contains two signals at the same time-step.

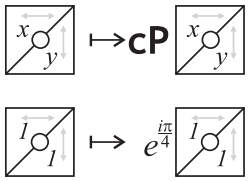

Figure 6.18: The collision of two signals when the **barrier** subsystem is empty also acts as a controlled phase (**cP**) operation on the qubits. If both axis signals are $|1\rangle$, then a global phase of $e^{i\pi/4}$ is added to the configuration. Note that all subsystems remain unchanged, and in all other cases this operation is simply the identity.

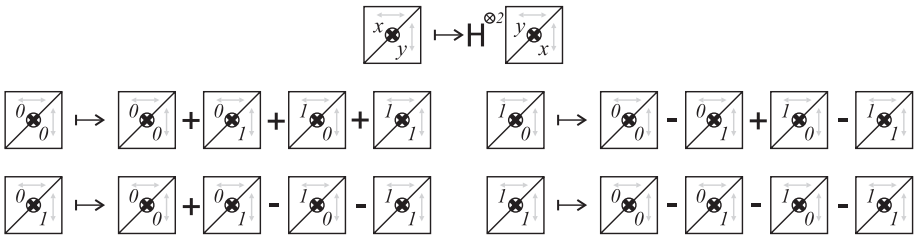

Figure 6.19: The collision of two signals when a **barrier** is present causes the Hadamard (**H**) operation to be applied to both qubits, causing the cell to move into a superposition of four cells. The signals are also deflected by the barrier, which is denoted by the exchanging of the **axis** subsystems. Normalisation factors of $\frac{1}{2}$ have been omitted for clarity.

structed, as shown in Figures 6.20, 6.21, and 6.22 respectively. Notice how each gate is implemented as a 4 by 16 grid for single qubit operations, and 8 by 16 grid for two qubit operations, with the signals entering on the second

of the four rows. This is so that these circuit configurations may be easily plugged together to form any circuit. The identity 'gate' is modelled by the delay configuration, given in Figure 6.16. To ensure that all signals are synchronised, each takes exactly 24 time-steps. When wiring together non-contiguous circuits several delay gates may be required in order to ensure all signals enter the second circuit at the same time-step.

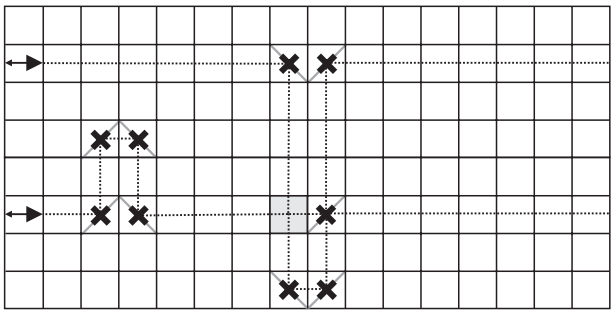

Figure 6.20: The 'cPhase circuit' configuration, an 8×16 configuration taking 24 time-steps which applies the controlled-phase operation to the two input qubits. This is achieved by delaying the second signal and redirecting the first, causing a collision at the highlighted cell. The qubits are then synchronised so that they exit at the same time along their original paths.

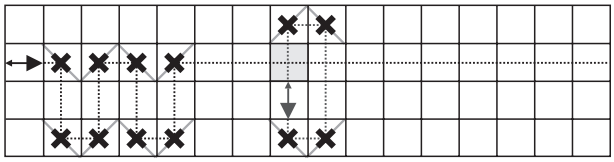

Figure 6.21: The 'Phase gate' configuration, a 4×16 configuration taking 24 time-steps. This configuration makes use of a signal, set to $|1\rangle$, which loops inside the grid every 8 time-steps, ensuring that it will collide with the signal that enters the configuration and causing it to act as the control qubit to a cPhase operation. This therefore acts as a phase rotation on the input qubit, which passes directly through. Note that after 24 time-steps the auxiliary signal has returned to its origin. The collision cell is highlighted in grey.

6.3.4 The scattering unitary

An intuitive explanation of what the scattering unitary U does to squares of four such cells has been provided in the previous sections. A formal descrip-

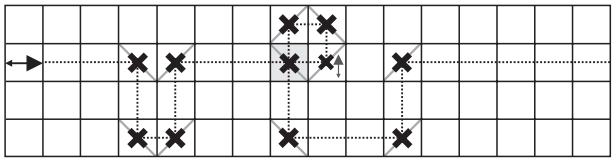

Figure 6.22: The 'Hadamard gate' configuration, a 4×16 configuration taking 24 timesteps which applies the Hadamard operation to the input signal. Like the 'Phase circuit' configuration, this configuration makes use of a looping signal, ensuring that it will collide with the signal that enters the configuration. The auxiliary signal in this circuit loops every 4 time-steps, and after the collision, which applies the Hadamard operation to both signals, the input signal is deflected by the barrier while the auxiliary continues looping. The input signal is then rerouted to exit along its original trajectory. The collision cell is highlighted in grey.

tion of U will now be given, and it is shown that it is indeed unitary.

The scattering unitary U takes four inputs **A**, **B**, **C**, and **D**, representing the four cells it operates on. Each of these decomposes into three subsystems: x**-axis**, y**-axis**, and **barrier** respectively, as already discussed. Therefore it could be given as a $18^4 \times 18^4$ matrix of complex numbers, yet fortunately it decomposes as in Figure 6.9. This circuit is essentially split into two sections: a permutation of the axis subsystems, and an application of a B operation on every cell, controlled by their own **barrier** subsystem. The permutation directly implements the neighbourhood movement rule given in Figure 6.14, while the B operation implements the single-cell rules for barriers and collisions given in Figures 6.15,6.18, and 6.19. The controlled-B operation can be further decomposed as in Figure 6.24, and is made up of three gates, all controlled by the **barrier** subsystem, that will now be discussed:

- **cP*** gate: This gate applies the cPhase operation to the **axis** subsystem on the subspaces where they are both not empty (i.e. they contain either $|0\rangle$ or $|1\rangle$). This operation is only applied if the cell does not contain a barrier; the **barrier** subsystem = ϵ. This fully implements the rule given in figure 6.18.

- **Axis permutation**: This gate simply permutes the values of the x**-axis** and y**-axis** subsystems of the cell, and is only applied if the cell contains a barrier. This implements the signal deflection rule given in Figure 6.15, and the collision signal deflection of the Hadamard collision rule given in Figure 6.19.

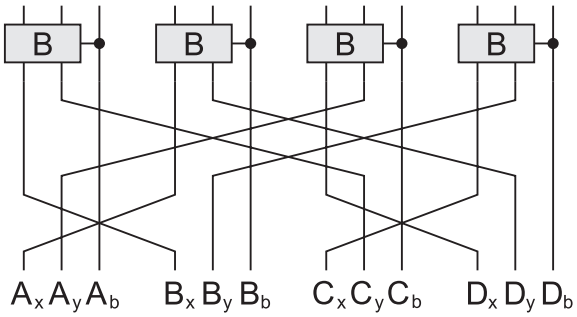

Figure 6.23: The scattering unitary U as a quantum circuit. Each cell, A, B, C, D, is split into its three subsystems, x**-axis**, x, y**-axis**, y, and **barrier**, b. The **axis** subsystems are first permuted following the scheme given in Figure 6.14, while the **barrier** subsystem simply passes through. The second stage sees the **barrier** subsystem of each cell act as the control for an operation B on the corresponding cells two **axis** subsystems. The action of the B circuit is further explained in Figure 6.24. Time flows upwards. The whole circuit represents the scattering unitary U; it takes four cells and yields back four cells.

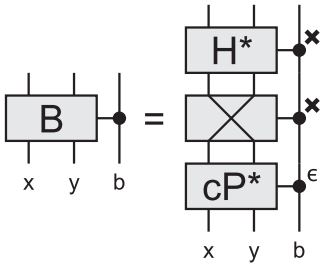

Figure 6.24: This circuit encodes the rules of this system that act upon only one cell. The first stage applies the cP^* operation, if the **barrier** subsystem is empty. cP^* is a modified cPhase operation that applies the cPhase operation in the subspace were both **axis** subsystems contain a qubit. Next, if a barrier is present, the second stage permutes the **axis** subsystems, x and y. Lastly, and again only if a barrier is present, the H^* operation is applied, which applies $H^{\otimes 2}$ if both **axis** subsystems contain a qubit. This completes the definition of the scattering unitary.

- $\mathbf{H}^*$ gate: This gate applies the Hadamard operation to both qubit signals stored in **axis** subsystems, and, like the $\mathbf{cP}^*$ operation, is the identity if either of these subsystems are empty. Again, it is only applied if the cell contains a barrier, and this operation, along with the axis permutation above, implements fully the Hadamard collision rule given in Figure 6.19.

This completes the formal definition of the scattering unitary U. Note that since we have described the evolution U as a combination of smaller unitary matrices via tensors, composition and the control-construct, it is indeed unitary as required by Definition 4.4.

Summarizing, we have constructed a two-dimensional QCA capable of simulating all others with linear overhead. This intrinsically universal QCA is a Partitioned QCA (Figure 4.1) of cell-dimension 18 and whose scattering unitary we have given explicitly (Figures 6.23, 6.24 and Subsection 6.3.4). We have done this construction is two-dimensions, but it is clear that it generalizes to n-dimensions.

6.4 Discussion and some open questions ⊛

Strong intrinsic universality. Notice how in the definition of intrinsic simulation (see Definition 6.4) $|q\rangle$ the quiescent state of the simulated QCA G gets encoded into words $|q''\rangle = E|q\rangle$, which in general may not be the same as $|q'^s\rangle$, i.e. s quiescent cells of the simulating QCA G'. In practice what this means is that with this notion of intrinsic simulation, we are indirectly assuming that the initial state of simulating QCA G' could be prepared in a non-finite configuration, i.e. one which does not end and begin with only q' symbols, but repeated q'' words instead. Formally this is not a problem, since G'' the (s, t, q')-grouping of G' remains a valid QCA with quiescent symbol q''. Yet, depending on the application, one may wonder whether this notion of intrinsic simulation is the appropriate notion. For instance, if the implementation of G' cannot be fed with q'' words left and right as the computation unravels, and if we do not know when the computation is supposed to stop, then this notion of intrinsic simulation may eventually fail, as illustrated by Figure 6.25.

This problem is not specific to QCA, and was discussed already for classical CA in [2, 45]. In order to solve this problem, they have come up with a second flavour to the notion of intrinsic universality, which we refer to as 'strong intrinsic universality'. For classical CA, however, having infinite

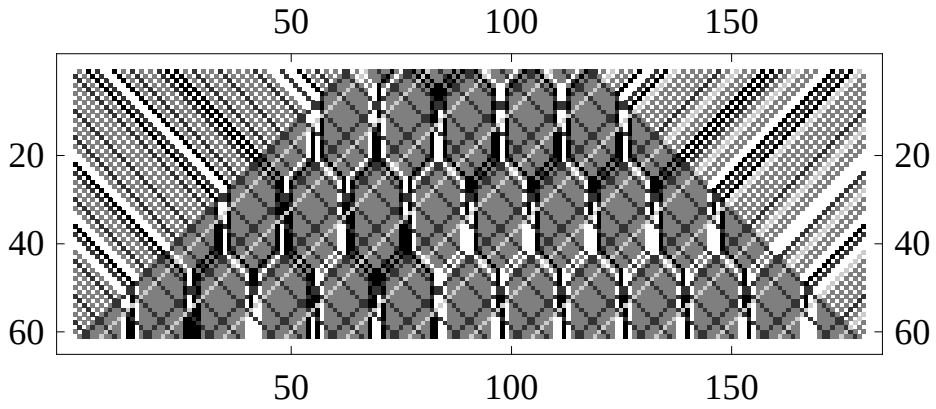

Figure 6.25: The ternary background pattern will shrink as the computation goes and the surrounding quiescent cells enter the computation region. Meanwhile, the data signals within the ternary background pattern may expand. At some point the data signals coding for the cells of the simulated QCA are no longer contained in the ternary background – the simulating QCA now fails to do the job.

configurations to start with is not such a big fuss – and therefore strong intrinsic universality has not been studied much. For QCA, however, we have explained that having finite unbounded configurations make the formalism much easier (although we could also have defined our Hilbert space over quasi-periodic configurations as in [97]) – and so strong intrinsic universality is more of an issue.

The challenge here is to construct a simulating QCA that has the ability to weave its background pattern as the computation proceeds. Actually, we have constructed such a one-dimensional strong intrinsic universal QCA in [15], which turns out to be a Partitioned QCA (Figure 4.1) of cell-dimension 15552 and whose scattering unitary we have given explicitly. A feeling of how it works is provided by Figure 6.26. Would it possible to achieve this same entertaining 'big bang effect' in the more-than-one-dimensional case?

Small cellular automata and the quest for a universal interaction in physics. Our Chapter 1 and the start of Chapter 4 discuss several motivations behind the study of QCA, but the introduction makes a particular point about how the

notion of universality should be ported from computer science to theoretical physics. Clearly the notion of universality that we are talking about for that research program is closer to intrinsic universality than computation universality : space matters. Hence with this first n-dimensional intrinsically universal construction (Section 6.3) we hope to have made a first contribution along that route. But although this QCA is universal, it probably is not so minimal : in comparison the simplest known nearest-neighbour intrinsically universal classical CA has cell dimension 4 [111]. Can we do better?

Small cellular automata and implementations of quantum computers. Another motivation that we have discussed in Chapter 1 is the one according to which QCA may be a good paradigm for an implementation of a quantum computer. If this is what we are interested in then we should be looking into the problem of identifying the simplest QCA capable of implementing any quantum circuit (intrinsic universality is no longer needed). This is what has been done in various ways in [134, 136, 105, 115, 122]. In the best case the cell dimension is 12, which is 10 more than in the classical case [43]. Can we do better?

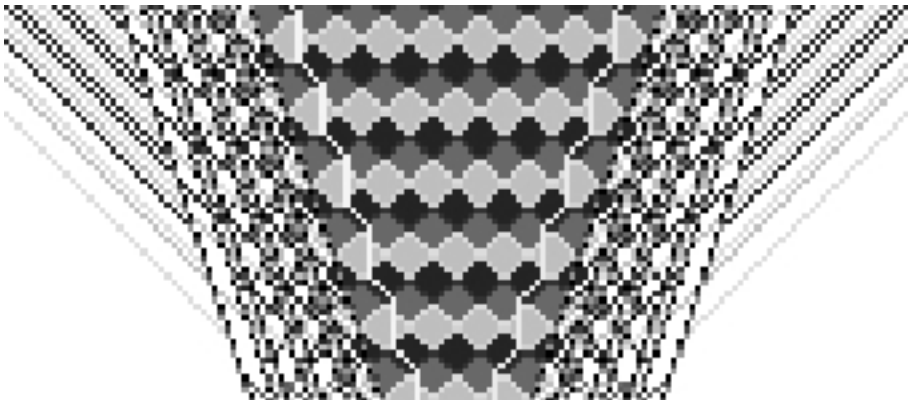

Figure 6.26: A run of the strongly intrinsically universal QCA. The ternary background pattern is produced by the four pairs of copy bands. Two data bits are shown as two white lines propagating through the ternary background pattern. In this example no quantum gates act on the data bits. Time flows upwards.

Chapter 7

Perspectives

There was nowhere to go but everywhere, so just keep on rolling under the stars.
—Jack Kerouac, On the road.

7.1 Summary ⊙⟁⊛

Contributions. In this thesis, some necessary linear algebra and the postulates of quantum theory have been explained, including the density matrix formalism. We reviewed the relevant Cellular Automata literature, and then the Quantum Cellular Automata literature. We introduced a notion of unitary causal operators (see Definition 4.9) and proved two important properties about them (Properties 4.2 and 4.1), as well as a structure theorem stating that they can always be implemented locally (see Theorem 5.1). Coming back to QCA, the notion of a unitary causal operator provides them with an elegant and general axiomatics (see Definition 4.12), and the structure theorem provides them with an operational, block representation (see Theorem 5.2). We pointed out some interesting consequences on bijective non-reversible CA over finite unbounded configurations (see Proposition 5.1) and on the speed of propagation of quantum information (see Proposition 5.2) – which raised some intriguing questions. Finally we formalised the notion of intrinsic simulation between n-dimensional QCA (see Definition 6.4), and provided universal instances of QCA with respect to this notion.
Open questions. As we presented the above results, we discussed several concrete open questions left to tackle. Because these were direct improvements on the results, it was easier to explain them 'inline'. These included:

- Seeking for exact block representations of more-than-one dimensional QCA (Section 5.3).
- Extending the structure theorem to quantum operations and not just unitary operators (Section 5.5).
- Investigating what may remain of the structure theorem in a continuous space setting (Section 5.5).
- Investigating the question of complexity bounds for parallel closed quantum computation (Subsection 5.4.2).
- Looking at strong intrinsic universality in more-than-one dimensional QCA (Section 6.4).
- Seeking a more minimal intrinsic universal QCA in more-than-one dimension (Section 6.4).
- Looking for a more minimal computation universal QCA (Section 6.4).

7.2 Applications ⟁⊛

Simulation and physical modelling. Our investigation of unitary causal operators has led us to a general 'unitarity plus causality implies locality' principle, which we have proved in a discrete-time, discrete space setting. Generalisations of this result to more continuous setting are crucially important if one wants to model continuous and isotropic quantum physical phenomena. Once modelled, these quantum physical phenomena could be simulated efficiently by a quantum computer – the reason why quantum computation was developed in the first place. This sort of theoretical issues, however, are echoing deep questions in axiomatic quantum field theory [39]. Perhaps a good angle of approach would be to look at the continuous limit of QCA dynamics as in the works which seek to have them simulate quantum field theoretical equations, i.e. [128, 28, 98, 100, 30, 29, 59, 96, 135, 89, 41].

Implementation of quantum computers. Our investigation of universal QCA illustrated the fact that computation in this setting does not require an external intervention / control. Before that our short presentation of quantum theory recalled the importance of keeping a system 'closed' in order to preserve its 'quantum behaviour'. Hence QCA may constitute a good paradigm for the implementation of a quantum computer – the reason why QCA were developed in the first place [61]. This route needs to be pursued further, following [62, 86, 26, 133, 140, 136, 125, 126, 36, 105]. Works like [136] in particular are able to throw a bridge between the language of computer science and the language of experimental physics language. For computer scientists, it would be beneficial to try and present more minimal computation universal QCA results to experimental physicists in this way.

7.3 A quantum extension of Gandy's theorem ⊛

The main result result of this work is that if some dynamics follow quantum theory (unitarity), and special relativity (causality) then it can be implemented locally. This entails several, almost philosophical consequence (abandoning our cautious scientific stance):

- If physical evolutions are implementable locally, this means that they can be given a very operational meaning in terms of operations over matrices and composition of them. Under some extra conditions, this could entail that they are computable.

- Conversely if physical evolutions were to be computable, this would explain why physics lends itself to being formalised by mathematics. This would call for computable reformulations of all physical laws, and reconcile the notions of physicality and computability in general. An enlightening discussion of these informal ideas can be found in [48].

These are intriguing questions, and we are actually exploring some aspects of them at a formal level in [12]. Indeed, the celebrated theorem of Gandy states that if the laws of physics are causal and homogeneous, and if the state space of each finite volume of space is a discrete set, then the evolution of any physical system is computable; and so the Church thesis must hold [63]. In the current state of physics, however, this theorem is clearly out-of-date, because of the common belief amongst physicists that each finite volume of space contains at least a finite dimensional quantum system – whose state space, due to the continuity of the complex amplitudes involved, is by no means isomorphic to a discrete set. However, although this continuity within finite-dimensional systems is a crucial ingredient of quantum theory, it turns out that to be quite innocuous as far as information storage is concerned. That is, it remains true somehow that each finite volume of space contains a finite amount of 'observable information'. Therefore it seems quite likely that the theorem of Gandy should continue to hold, even in a quantum setting.
We believe that the key mathematical ingredients we have used in this thesis in order to break down the global unitary evolution G of a n-dimensional QCA into elementary, finite-dimensional unitary operators ought to provide us with one of the crucial steps missing towards a quantum extension of Gandy's theorem [12]. Notice that what such a theorem would say (under a series of assumption such as causality, finite density, homogeneity etc.) that the Church thesis holds *because* physical phenomena are computable. Hence this would not just be a statement about the limits that physics imposes on computation, but conversely also a statement as 'To what extent are physical processes... computational'. We are not only arguing that computer science is about extracting from physics its ability to run a computation, we are also arguing that physics is about extracting from computer science its ability to run physical phenomena.

Bibliography

[1] S. Abramsky and B. Coecke. A Categorical Semantics of Quantum Protocols. In *Proceedings of LICS*, pages 415–425. IEEE Computer Society, 2004.

[2] J. Albert and K. Culik. A simple universal cellular automaton and its one-way and totalistic version. *Complex Systems*, 1:1–16, 1987.

[3] S. Amoroso and Y. N. Patt. Decision procedures for surjectivity and injectivity of parallel maps for tessellation structures. *Journal of Computer and Systems Sciences*, 6:448–464, 1972.

[4] B. Aoun and M. Tarifi. Introduction to quantum cellular automata. *Arxiv preprint quant-ph/0401123*, 2004.

[5] P. Arrighi. Quantum computation explained to my mother. In G. Rozenberg and A. Salomaa, editors, *Current Trends in Theoretical Computer Science: The Challenge of the New Century*. World Scientific, 2004.

[6] P. Arrighi. Quantum decoys. *International Journal of Quantum Information*, 2(3):341–351, 2004.

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

[8] P. Arrighi and A. Díaz-Caro. Scalar System F for Linear-Algebraic Lambda-Calculus: Towards a Quantum Physical Logic. In *Proceedings of QPL, to appear in Electronic Notes in Computer Science*, 2009.

[9] P. Arrighi and G. Dowek. Operational semantics for formal tensorial calculus. In *Proceedings of QPL*, volume 33, pages 21–38. Turku Centre for Computer Science General Publication, 2004.

[10] P. Arrighi and G. Dowek. A computational definition of the notion of vectorial space. *Electronic Notes in Theoretical Computer Science*, 117:249–261, 2005.

[11] P. Arrighi and G. Dowek. Linear-algebraic lambda-calculus: Higher-Order, Encodings, and Confluence. In *Proceedings of RTA, Lecture Notes in Compter Science*, page 17. Springer, 2008.

[12] P. Arrighi and G. Dowek. A quantum extention of Gandy's theorem (manuscript.). Current work., 2009.

[13] P. Arrighi and R. Fargetton. Intrinsically universal one-dimensional quantum cellular automata. In *Proceedings of DCM*, 2007.

[14] P. Arrighi and R. Fargetton. The Bloch representation of quantum states. In *To appear in Proceedings of QCMC*. AIP Conference series, 2008.

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

[16] P. Arrighi and John. Grattage. Intrinsically universal n-dimensional quantum cellular automata (manuscript.). To be submitted., 2009.

[17] P. Arrighi and V. Nesme. Quantizations of Cellular Automata. In B. Durand, editor, *First Symposium on Cellular Automata "Journées Automates Cellulaires" (JAC 2008), Uzès, France, April 21-25, 2008. Proceedings*, pages 204–215. MCCME Publishing House, Moscow, 2008.

[18] P. Arrighi, V. Nesme, and R. Werner. Unitarity plus causality implies locality. Arxiv preprint arXiv:0711.3975, 2007.

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

[20] P. Arrighi and C. Patricot. A note on the correspondence between qubit quantum operations and special relativity. *Journal of Physics A: Mathematical and General*, 36(20):L287–L296, 2003.

[21] P. Arrighi and C. Patricot. Conal representation of quantum states and non-trace-preserving quantum operations. *Phys. Rev. A*, 68:042310, 2003.

[22] P. Arrighi and C. Patricot. On quantum operations as quantum states. *Annals of Physics*, 311(1):26–52, 2004.

[23] P. Arrighi and L. Salvail. Blind quantum computation. *International Journal of Quantum Information*, 4(5):883–898, 2006.

[24] E. R. Banks. Universality in cellular automata. In *SWAT '70: Proceedings of the 11th Annual Symposium on Switching and Automata Theory (swat 1970)*, pages 194–215, Washington, DC, USA, 1970. IEEE Computer Society.

[25] D. Beckman, D. Gottesman, M. A. Nielsen, and J. Preskill. Causal and localizable quantum operations. *Phys. Rev. A*, 64(052309), 2001.

[26] S. C. Benjamin. Schemes for parallel quantum computation without local control of qubits. *Phys. Rev. A*, 61(2):020301, Jan 2000.

[27] E. Bernstein and U. Vazirani. Quantum complexity theory. In *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, pages 11–20. ACM New York, NY, USA, 1993.

[28] I. Bialynicki-Birula. Weyl, Dirac, and Maxwell equations on a lattice as unitary cellular automata. *Physical Review D*, 49(12):6920–6927, 1994.

[29] B. M. Boghosian and W. Taylor. Quantum lattice-gas model for the many-particle Schrödinger equation in d dimensions. *Phys. Rev. E*, 57(1):54–66, 1998.

[30] B. M. Boghosian and W. Taylor. Simulating quantum mechanics on a quantum computer. *Physica D*, 120(1-2):30–42, 1998.

[31] S. Bose. Quantum communication through spin chain dynamics: an introductory overview. *Contemporary Physics*, 48(1):13–30, 2007.

[32] O. Bournez and M.L. Campagnolo. A survey on continuous time computations. *New Computational Paradigms. Changing Conceptions of What is Computable*, pages 383–423, 2008.

[33] T. Boykett. Efficient exhaustive listings of reversible one dimensional cellular automata. *Theor. Comput. Sci.*, 325(2):215–247, 2004.

[34] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan. On universal and fault-tolerant quantum computing: A novel basis and a new constructive proof of universality for shor's basis. In *FOCS '99:*

Proceedings of the 40th Annual Symposium on Foundations of Computer Science, page 486, Washington, DC, USA, 1999. IEEE Computer Society.

[35] 0. Bratteli and D. Robinson. *Operators algebras and quantum statistical mechanics 1.* Springer, 1987.

[36] G. K. Brennen and J. E. Williams. Entanglement dynamics in one-dimensional quantum cellular automata. *Phys. Rev. A*, 68(4):042311, Oct 2003.

[37] C. Brukner and A. Zeilinger. Information and Fundamental Elements of the Structure of Quantum Theory. In *Time, Quantum and Information.*, pages 323–356. Springer, 2003.

[38] C. Bruun. *A model of consumption behaviour using cellular automata.* Aalborg University, 1996.

[39] D. Buchholz. Current trends in axiomatic quantum field theory. *Lect. Notes Phys.*, 558:4364, 2000.

[40] G. Chang, W.-T. Ke, D. Kuo, D. Liu, and R. Yeh. On $L(d, 1)$-labelings of graphs. *Discrete Mathematics*, 220:57–66, 2000.

[41] D. Cheung and C. A. Perez-Delgado. Local Unitary Quantum Cellular Automata. ArXiv pre-print arXiv:0709.0006.

[42] B. Chopard and M. Droz. *Cellular automata modeling of physical systems.* Cambridge University Press New York, 1998.

[43] M. Cook. Universality in elementary cellular automata. *Complex Systems*, 15(1):1–40, 2004.

[44] K. Culik, L. P. Hurd, and S. Yu. Computation theoretic aspects of cellular automata. *Physica D*, 45:357–378, 1990.

[45] M. Delorme. An Introduction to Cellular Automata, Cellular Automata: a Parallel Model. In *Mathematics and Its Applications.* Kluwer, 1999.

[46] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences (1934-1990)*, 400(1818):97–117, 1985.

[47] A. Díaz-Caro, P. Arrighi, M. Gadella, and J. Grattage. Measurements and confluence in quantum lambda calculi with explicit qubits. In *Proceedings of QPL, to appear in Electronic Notes in Computer Science*, 2008.

[48] G. Dowek. *Les Metamorphoses du calcul*. Le Pommier, 2007.

[49] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62:062314, 2000.

[50] B. Durand and Z. Roka. The Game of Life: universality revisited Research Report 98-01. Technical report, Ecole Normale Suprieure de Lyon, 1998.

[51] J. Durand-Lose. The signal point of view: from cellular automata to signal machines. In B. Durand, editor, *First Symposium on Cellular Automata "Journées Automates Cellulaires" (JAC 2008), Uzès, France, April 21-25, 2008. Proceedings*, pages 238–249. MCCME Publishing House, Moscow, 2008.

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

[53] J. O. Durand-Lose. Reversible cellular automaton able to simulate any other reversible one using partitioning automata. In *In latin'95, number 911 in Lecture Notes in Computer Science*, pages 23024–4. Springer, 1995.

[54] J. O. Durand-Lose. Intrinsic universality of a 1-dimensional reversible cellular automaton. In *Proceedings of STACS 97, Lecture Notes in Computer Science*, page 439. Springer, 1997.

[55] J. O. Durand-Lose. Black hole computation: implementation with signal machines. In C. S. Calude and J. F. Costa, editors, *International Workshop Physics and Computation, Wien, Austria, Agust 25-28*, Research Report CDMTCS-327, pages 136–158, 2008.

[56] J. O. Durand-Lose. Universality of Cellular Automata. In *Encyclopedia of Complexity and System Science*. Springer, 2008.

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

[58] C. Durr and M. Santha. 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, 1996.

[59] J. Eakins. Quantum cellular automata, the EPR paradox and the Stages paradigm. In *Proceedings of NATO ARW, The Nature of Time: Geometry, Physics and Perception*, 2003.

[60] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6):467–488, 1982.

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

[62] J. Fitzsimons and J. Twamley. Globally controlled quantum wires for perfect qubit transport, mirroring, and computing. *Physical Review Letters*, 97(9):90502, 2006.

[63] R. Gandy. Churchs thesis and principles for mechanisms. In *The Kleene Symposium*, Amsterdam, 1980. North-Holland Publishing Company.

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

[65] G. Grossing and A. Zeilinger. A conservation law in quantum cellular automata. *Physica D*, 31:70–77, 1988.

[66] G. Grössing and A. Zeilinger. Quantum cellular automata. *Complex Systems*, 2(2):197–208, 1988.

[67] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Found. Phys Phys Rev Lett*, 79:325, 1993.

[68] J. Gruska. *Quantum computing Advanced topics in computer science series.* McGraw-Hill companies, 1999.

[69] M. Hamada, N. Konno, and E. Segawa. Relation between coined quantum walks and quantum cellular automata. Arxiv preprint quant-ph/0408100, 2004.

[70] G. A. Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Math. Systems Theory*, 3:320–375, 1969.

[71] O. H. Ibarra and T. Jiang. On the computing power of one-way cellular arrays. In *Proceedings of ICALP 87*, page 550562, London, UK., 1987. Springer.

[72] K. Imai and K. Morita. A computation-universal two-dimensional 8-state triangular reversible cellular automaton. *Theoretical Computer Science*, 231(2):181–191, 2000.

[73] S. Inokuchi and Y. Mizoguchi. Generalized partitioned quantum cellular automata and quantization of classical CA. *International Journal of Unconventional Computing*, 1:0312102, 2005.

[74] N. Inui, S. Inokuchi, Y. Mizoguchi, and N. Konno. Statistical properties of a quantum cellular automaton. *Phys. Rev. A*, 72(3):032323, 2005.

[75] N. Inui, K. Nakamura, Y. Ide, and N. Konno. Effect of Successive Observation on Quantum Cellular Automaton. *Journal of the Physical Society of Japan*, 76(8):084001, 2007.

[76] I. G. Karafyllidis. Definition and evolution of quantum cellular automata with two qubits per cell. *Journal reference: Phys. Rev. A*, 70:044301, 2004.

[77] J. Kari. Reversibility of 2D cellular automata is undecidable. In *Cellular Automata: Theory and Experiment*, volume 45, pages 379–385. MIT Press, 1991.

[78] J. Kari. Reversibility and surjectivity problems of cellular automata. *J. Comput. Syst. Sci.*, 48(1):149–182, 1994.

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

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

[81] K. Kari. Theory of cellular automata: A survey. *Theor. Comp. Sc.*, 334:2005, 2005.

[82] J. Kempe. Quantum random walks: an introductory overview. *Contemporary Physics*, 44(4):307–327, 2003.

[83] N. Konno, K. Mistuda, T. Soshi, and HJ Yoo. Quantum walks and reversible cellular automata. *Physics Letters A*, 330(6):408–417, 2004.

[84] H. T. Kung and C. E. Leiserson. Systolic arrays (for VLSI). In *In Sparse Matrix Proceedings*, pages 256–282, 1978.

[85] R. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, 5(3):183–191, 1961.

[86] S. Lloyd. A potentially realizable quantum computer. *Science*, 261(5128):1569–1571, 1993.

[87] S. Lloyd. A theory of quantum gravity based on quantum computation. Arxiv preprint quant-ph/0501135, 2005.

[88] S. Lloyd. *Programming the universe*. Knopf, 2006.

[89] P. Love and B. Boghosian. From Dirac to Diffucion: decoherence in Quantum Lattice gases. *Quantum Information Processing*, 4:335–354, 2005.

[90] F. Magniez, M. Santha, and M. Szegedy. Quantum algorithms for the triangle problem. In *Proceedings of the sixteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 1109–1117. Society for Industrial and Applied Mathematics Philadelphia, PA, USA, 2005.

[91] N. Margolus. Physics-like models of computation. *Physica D: Nonlinear Phenomena*, 10(1-2), 1984. partiotioning, neighbourhood, energy.

[92] N. Margolus. Parallel quantum computation. In *Complexity, Entropy, and the Physics of Information: The Proceedings of the 1988 Workshop on Complexity, Entropy, and the Physics of Information Held May-June, 1989, in Santa Fe, New Mexico*, page 273. Perseus Books, 1990.

[93] B. Martin. Cellular automata universality revisited. In *Proceedings of FCT'97, in Lecture Notes in Computer Science*, pages 329–339. Springer, 1997.

[94] J. Mazoyer. A Six-State Minimal Time Solution to the Firing Squad Synchronization Problem. *Theoretical Computer Science*, 50:183–238, 1987.

[95] J. Mazoyer and I. Rapaport. Inducing an order on cellular automata by a grouping operation. In *Proceedings of STACS'98, in Lecture Notes in Computer Science*, pages 116–127. Springer, 1998.

[96] M. McGuigan. Quantum cellular automata from lattice field theories. Arxiv preprint quant-ph/0307176, 2003.

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

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

[99] D. A. Meyer. On the absence of homogeneous scalar quantum cellular automata. Arxiv pre-print quant-ph/9604011, 1996.

[100] D. A. Meyer. Quantum mechanics of lattice gas automata: boundary conditions and other inhomogeneities. *Journal of Physics A-Mathematical and General*, 31(10):2321–2340, 1998.

[101] E. F. Moore. Machine models of self-reproduction. In *In Mathematical Problems in Biological Sciences (Proceedings of Symposia in Applied Mathematics*. American Mathematical Society, 1962.

[102] E. F. Moore. The firing squad synchronization problem. In *in Sequential Machines, Selected Papers*, pages 213–214. Addison-Wesley, 1964.

[103] K. Morita. Computation-universality of one-dimensional one-way reversible cellular automata. *Inf. Process. Lett.*, 42(6):325–329, 1992.

[104] J. Myhill. The converse of Moore's Garden-of-Eden theorem. In *Proc. Am. Math. Soc*, pages 685–686. Press, 1963.

[105] D. Nagaj and P. Wocjan. Hamiltonian Quantum Cellular Automata in 1D. Arxiv preprint arXiv:0802.0886, 2008.

[106] K. Nagel and M. Schreckenberg. A cellular automaton model for freeway traffic. *J. Phys. I France*, 2:2221–2229, 1992.

[107] V. Nesme and J. Gütschow. On the fractal structure of the space-time diagrams of clifford cellular automata. manuscript, 2009.

[108] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, October 2000.

[109] N. Ollinger. The Quest for Small Universal Cellular Automata. In *Proceedings of ICALP '02, Lecture Notes in Computer Science*, pages 318–329. Springer, 2002.

[110] N. Ollinger. Universalities in cellular automata a (short) survey. In B. Durand, editor, *First Symposium on Cellular Automata "Journées Automates Cellulaires" (JAC 2008), Uzès, France, April 21-25, 2008. Proceedings*, pages 102–118. MCCME Publishing House, Moscow, 2008.

[111] N. Ollinger and G. Richard. A Particular Universal Cellular Automaton. In Turlough Neary, Damien Woods, Anthony Karel Seda, and Niall Murphy, editors, *CSP*, pages 267–278. Cork University Press, 2008.

[112] J. P. Paz and W. H. Zurek. Environment-induced decoherence and the transition from quantum to classical. *Lecture Notes in Physics*, pages 77–140, 2002.

[113] J. Pedersen. Cellular automata as algebraic systems. *Complex Systems*, 6:237–250, 1992.

[114] S. Perdrix. Partial observation of quantum Turing machine and weaker wellformedness condition. In *In proceedings of Joint Quantum Physics and Logic & Development of Computational Models (Joint 5th QPL and 4th DCM)*, 2008.

[115] R. Raussendorf. Quantum cellular automaton for universal quantum computation. *Phys. Rev. A*, 72(022301), 2005.

[116] S. Richter and R. F. Werner. Ergodicity of quantum cellular automata. *J. Stat. Phys*, 82:96–3, 1996.

[117] D.H. Rothman and S. Zaleski. *Lattice-gas cellular automata: simple models of complex hydrodynamics*. Cambridge University Press, 1997.

[118] D. M. Schlingemann, H. Vogts, and R. F. Werner. On the structure of Clifford quantum cellular automata. *Journal of Mathematical Physics*, 49:112104, 2008.

[119] D.M. Schlingemann. Remarks on the structure of Clifford quantum cellular automata. Arxiv preprint arXiv:0812.0714, 2008.

[120] B. Schumacher and R. Werner. Reversible quantum cellular automata. Arxiv pre-print quant-ph/0405174, 2004.

[121] B. Schumacher and M. D. Westmoreland. Locality and information transfer in quantum operations. *Quantum Information Processing*, 4(1):13–34, 2005.

[122] D. J. Shepherd, T. Franz, and R. F. Werner. A universally programmable quantum cellular automata. *Phys. Rev. Lett.*, 97(020502), 2006.

[123] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, pages 303–332, 1999.

[124] L. Smolin. *Three roads to quantum gravity*. Basic books, New York, 2001.

[125] V. Subrahmanyam. Entanglement dynamics and quantum-state transport in spin chains. *Phys Rev A*, 69:034304, 2004.

[126] V. Subrahmanyam and A. Lakshminarayan. Transport of entanglement through a Heisenberg–XY spin chain. *Physics Letters A*, 349(1-4):164–169, 2006.

[127] K. Sutner. De Bruijn graphs and linear cellular automata. *Complex Systems*, 5(1):19–30, 1991.

[128] K. Svozil. Are quantum fields cellular automata? *Physics Letters A*, 119(4):153–156, 1986.

[129] G. Theyssier. Captive cellular automata. In *Proceedings of MFCS 2004, in Lecture Notes in Computer Science*, pages 427–438. Springer, 2004.

[130] T. Toffoli. Computation and construction universality of reversible cellular automata. *J. of Computer and System Sciences*, 15(2), 1977. d+1 simulates d construction.

[131] T. Toffoli and N. Margolus. *Cellular Automata Machine A New Environment for Modelling*. MIT Press, Cambridge MA, 1987.

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

[133] J. Twamley. Quantum cellular automata quantum computing with endohedral fullerenes. *Phys. Rev. A*, 67(5):52318–52500, 2003.

[134] W. Van Dam. Quantum cellular automata. Master thesis, University of Nijmegen, The Netherlands, 1996.

[135] A.Y. Vlasov. On quantum cellular automata. Arxiv preprint quant-ph/0406119, 2004.

[136] K. G. H. Vollbrecht and J. I. Cirac. Reversible universal quantum computation within translation-invariant systems. *New J. Phys Phys Rev A*, 73:012324, 2004.

[137] J. von Neumann. *Mathematical foundations of quantum mechanics*. Princeton University Press, 1955.

[138] J. Von Neumann. *Theory of Self-Reproducing Automata*. University of Illinois Press, Champaign, IL, USA, 1966.

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

[140] Y. S. Weinstein and C. S. Hellberg. Quantum cellular automata pseudorandom maps. *Phys. Rev. A*, 69(6), 2004.

[141] R. White and G. Engelen. Cellular automata as the basis of integrated dynamic regional modelling. *Environment and Planning B*, 24:235–246, 1997.

[142] K. Wiesner. Quantum Cellular Automata. Arxiv preprint arXiv:0808.0679, 2008.

[143] D. A. Wolf-Gladrow. Lattice-Gas Cellular Automata and Lattice Boltzmann Models. In *Lecture Notes in Mathematics*. Springer, 2000.

[144] S. Wolfram. Computation Theory of Cellular Automata. *Comm. Math. Phys*, 96:15–57, 1984.

[145] S. Wolfram. A new kind of science. *Wolfram Media Inc.*, 2002.

[146] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[147] K. Zuse. Rechnender Raum. Elektronische Datenverarbeitung. *English Translation: Calculating Space, MIT Tech. Translation*, 8:336–344, 1967.