Bounds on the speedup in quantum signaling

Pablo Arrighi, Vincent Nesme, Reinhard F. Werner

,

Bounds on the Speedup in Quantum signalling

Pablo Arrighi,[1] Vincent Nesme,[2] and Reinhard F. Werner[3]

[1]*Aix-Marseille Univ., LIF, F-13288 Marseille Cedex 9, France*[*]

[2]*LIG, Université Joseph Fourier, Grenoble, France*[†]

[3]*Institut für Theoretische Physik, Leibniz Universität, Hannover, Germany*

Given a discrete reversible dynamics, we can define a quantum dynamics, which acts on basis states like the classical one, but also allows for superpositions of them. It is a curious fact that in the quantum version, local changes in the initial state, after a single dynamical step, can sometimes can be detected much farther away than classically. Here we show that this effect is no use for generating faster signals. In a run of many steps the quantum propagation neighborhood can only increase by a constant fringe, so there is no asymptotic increase in speed.

Keywords: quantum cellular automata, neighborhood, block representation

[*] pablo.arrighi@univ-amu.fr

[†] vincent.nesme@imag.fr

I. INTRODUCTION

It is well known that a unitary quantum walk on a lattice propagates much faster than its classical counterpart: where the classically walking particle is expected to travel a distance of the order of $\sqrt{t}$ in t steps, the quantum particle travels ballistically, covering a distance of the order of t. The comparison is not entirely fair, because as soon as randomness in the form of decoherence is introduced the quantum walk also slows down to diffusive scaling. In this paper, as in [25], we study the complementary fair case, namely propagation in a non-random, fully reversible classical dynamical system and its quantum counterpart.

The classical dynamical system here will be a Cellular Automaton. Cellular automata (CA), first introduced by von Neumann [28], consist of an array of identical cells, each of which may take one of a finite number of possible states. The entire array evolves in discrete time steps by applying the same local transition function everywhere, synchronously. CA are used in Computer Science to model space-sensitive problems such as self-reproduction or synchronization, but they also arise quite naturally in applied mathematics and physics, as discrete models and numerical schemes for PDEs. In the context of this paper the cells need not be arranged in a grid, and the local transition function need not be the same everywhere: by CA we really mean just discrete time discrete space dynamics.

The quantum counterpart of this dynamical system will similarly be a Quantum Cellular Automaton (QCA). Indeed, because CA are a physics-like model of computation [20], Feynman [11], and later Margolus [21], suggested early in the development of Quantum Computing that quantizing this model was important. For two main reasons. First, they are a natural framework in which to cast the quantum simulation of a quantum system [6, 22]. Secondly, because they seem advantageous as an implementation architecture for a quantum computer [17, 27]: in QCA computation occurs without extraneous (unnecessary) control, hence eliminating a source of noise. There are yet other reasons to study QCA: as a model of distributed quantum computation, as a mathematical framework in order to grasp the interplay between entanglement and causality [2, 3][12], or even as yielding toy models of quantum spacetime [18]. QCA are the natural multi-particle extensions of Quantum Walks. But again, in the context of this paper the cells do not need to be arranged in a grid, and the evolution does not need to act the same everywhere: by QCA we really mean just a discrete time discrete space quantum dynamics. Actually, since we specifically look at QCA arising from quantizing CA, their state space will be akin to a Hilbert space whose basis states are

labelled by the configurations of the classical CA, and their unitary dynamics will be completely determined by the by the linear extension of the classical CA.

In both the quantum and classical settings there is a clear notion of localization, i.e., observables associated to each cell or a group of cells, and therefore we can directly compare propagation properties. We will see that a large quantum speedup is possible, in the sense that the quantum propagation neighbourhood can be much larger than the classical one. On the other hand we show that this gain cannot be realized in every step: in the long run of t steps the neighborhood gain does not increase with t. Therefore, the asymptotic speed of propagation is the same in QCA and CA.

The first upper bound on the quantum propagation neighborhood was given in [24] (compare to (1) below) in the context of proving that the above procedure for "quantizing" a CA is well-defined. However, no examples showing the quality of the bound were given. The theory was further developed in [1, 4]. In particular, an interpretation of the quantum neighborhood in terms of the classical CA, called the "block neighborhood" was given in [1]. Our bound for the asymptotic case crucially depends on the bound on block neighborhoods derived there.

Our paper is organized as follows. We begin with an example, the XOR-CA, which shows, paradoxically, an infinite speedup. Although the classical dynamics is local, the quantum system can carry signals arbitrarily far in a single step. In the definition of [24] the quantum system is thus not a QCA. The analysis of this extreme case helps us to explain the origin of the speedups discussed in this paper, and also highlights the importance of the classical inverse neighborhood (which is infinite in this example). We then make our mathematical setting precise, in particular excluding such pathologies and giving a more formal definition of the neighborhoods. We show in our second basic example, the Toffoli-CA, a quantum neighborhood twice as large as the classical one. We then state the best known bounds on the single-step quantum neighborhood. The effect of asymptotic loss of speedup is also first explained in the example of the Toffoli-CA, accompanied by a general theorem to this effect.

II. THE XOR-CA: INFINITE SPEEDUP?

A Cellular Automaton (CA) is a function from configurations to configurations. Configurations are themselves functions, which associate, to each point of the lattice, a state in a finite set. In our first example we take the lattice to be $\mathcal{Z}$, and the finite set to be $\Sigma = \{\_, 0, 1\}$. The set

of infinite configurations $\mathcal{C}$ is then the set of functions from $\mathcal{Z}$ to Σ. The set of finite configurations $\mathcal{C}_f$ is more restricted: it contains only those configurations $c = \cdots c_{-1}c_0c_1c_2\cdots$ such that there are only a finite number of $c_i \neq \_$. The symbol $\_$ is called the quiescent state. This restriction to finite configurations is a standard assumption for the CA and Turing machines computational models, to exclude infinite parallel computation or uncomputable input configurations. The dynamical transformation f is given in terms of a local transition rule δ applied to the contents of each cell and its right neighbor. It is based on the XOR gate, i.e., addition mod 2, which we denote by $\oplus$: for $x, y \in \{0, 1\}$, $\delta(\_\, x) = \_$, $\delta(x\_\,) = x$, and $\delta(xy) = x \oplus y$. The induced, global, classical dynamics f thus takes the configuration $c = \cdots c_{i-1}c_ic_{i+1}\cdots$ to the configuration $f(c) = \cdots\delta(c_{i-1}c_i)\delta(c_ic_{i+1})\cdots$. The infinite configurations $\ldots 000\ldots$ and $\ldots 111\ldots$ have the same image, namely $\ldots 000\ldots$, hence f is not bijective over $\mathcal{C}$ the set of infinite configurations. However, one can easily work out that it is bijective over the set of finite configurations $\mathcal{C}_f$. Hence its quantization Q_f, or "linear extension" defined on basis states as $Q_f|c\rangle = |f(c)\rangle$, is a perfectly valid unitary operator from $\mathcal{H}_{\mathcal{C}_f}$ to $\mathcal{H}_{\mathcal{C}_f}$, where $\mathcal{H}_{\mathcal{C}_f}$ is the Hilbert space having $\mathcal{C}_f$ as its orthonormal basis. So f is a well-defined cellular automaton, and everything seems to suggest that Q_f is a perfectly valid quantization of f, i.e. a quantum cellular automaton (QCA). But no: surprisingly Q_f violates the causality condition for QCAs in [24]. That is, it allows to transmit information arbitrarily far in a single step [4].

Indeed, for $x = 0$ or 1, consider the configuration $d^x = \cdots \_\_\, 00\cdots 0x\_\_\cdots$, where the dots in the middle stand for some long segment of the lattice, say of size L. It has antecedent $c^x = f^{-1}(d^x) = \cdots \_\_\, xx\cdots xx\_\_\cdots$. Now consider the two superposition states $|c^\pm\rangle = (|c^0\rangle \pm |c^1\rangle)/\sqrt{2}$ and their images $|d^\pm\rangle = Q_f|c^\pm\rangle$:

$$|c^\pm\rangle = \tfrac{1}{\sqrt{2}}|\cdots \_\_\,\rangle \otimes \big(|00\cdots 00\rangle \pm |11\cdots 11\rangle\big) \otimes |\_\_\,\cdots\rangle$$
$$|d^\pm\rangle = |\cdots \_\_\, 00\cdots 0\rangle \otimes |\pm\rangle \otimes |\_\_\,\cdots\rangle$$

where we used the usual notation $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

Let us now describe how one can transmit information between arbitrarily distant parties in just one step of this dynamics. The line is prepared in the state c_+ with the first non quiescent cell in Alice's lab in Paris and the last non quiescent cell with Bob in New York. Then Alice either leaves the state unchanged or performs a *local change* by applying a phase gate Z to her cell, changing c^+ into c^-. Then one XOR-CA is performed leading to either $|d^+\rangle$ or $|d^-\rangle$, and hence a perfectly measurable change from $|+\rangle$ to $|-\rangle$ for Bob, despite him being arbitrarily far remote.

This infinite speedup is intuitively unphysical. To make this intuition precise let us try to implement the XOR-CA with local gates satisfying the natural constraints that (1) each gate operates on a well defined subset of the system qubits and possibly some locally available ancillas, (2) in each clock cycle these subsets of simultaneously operating gates do not overlap, to avoid double use of quantum information and hence illegal cloning and (3) there are finitely many clock cycles. Any automaton built in this way is *structurally reversible*: we can invert it, by inverting the steps in each clock cycle, and the inverse is again a cellular automaton. This is precisely what the problem with this XOR-CA: although f has an inverse on finite configurations, this inverse is not itself a CA, i.e. there is no upper bound on the number of cells one has to look at in order to compute the antecedent. In fact, the same situation always arises whenever a CA f is one-to-one on finite configurations, but fails to be one-to-one on infinite configurations. This is because of a deep theorem in CA theory [13], which relies on the compactness of $\mathcal{C}$ equipped with a certain metric, and the characterization of CA as continuous functions with respect to that metric, in order to prove that if f is a CA over $\mathcal{C}$ and has an inverse, then f^{-1} is itself a CA over $\mathcal{C}$.
We will assume in the rest of the paper that both f and f^{-1} are CAs, i.e., have finite neighborhoods $\mathcal{N}(f)$ and $\mathcal{N}(f^{-1})$, and we will provide lower and upper bounds for the neighborhoods of the corresponding Q_f. In the lower bound both $\mathcal{N}(f)$ and $\mathcal{N}(f^{-1})$ appear. Porting this lower bound argument back to the $\mathcal{N}(f^{-1})$ infinite case, implies that the above XOR-CA trick can always be applied. In other words, any CA which is bijective over finite configurations but not over infinite configurations, has a infinite $\mathcal{N}(f^{-1})$, and hence an infinite $\mathcal{N}(Q_f)$.

III. SETTING AND ONE-STEP BOUND

A. Classical state space and evolutions

For the general points we want to make the structure of the lattice X which labels the cells is largely irrelevant. Although our examples are drawn from one-dimensional lattices, any dimension is fine, and translation invariance is also not needed. We only require that the system be organized in a set X of cells, and that the classical content of cell $x \in X$ be taken from a finite alphabet Σ_x, which may depend on x. For any subset A of X, we denote by $\Sigma_A = \prod_{x\in A} \Sigma_x$ the set of configurations on A. When A is not mentioned, it is understood to be the whole set X, so that a configuration c is an element of $\mathcal{C} = \Sigma_X$; a classical evolution is a function $f : \mathcal{C} \to \mathcal{C}$.

B. Neighborhoods

Neighborhoods $\mathcal{N}(.)$ are defined in an operational way which applies to the classical and quantum side alike, namely as the set of pairs (x, y) such that a state change at x after one step of the dynamics can make a detectable difference at y. To any evolution f over classical configurations, we can thus associate a neighborhood $\mathcal{N}(f)$, so that $(x, y) \in \mathcal{N}(f)$ if and only if there exists two configurations c, d which differ only at cell x and such that $f(c)_y \neq f(d)_y$. Then an evolution f is called a (non translation-invariant) *cellular automaton* (CA for short) if, for all y, the set $\mathcal{N}(f)(y) = \{x|(x, y) \in \mathcal{N}(f)\}$ is finite, so that the update of cell y can be computed from finitely many c_x.

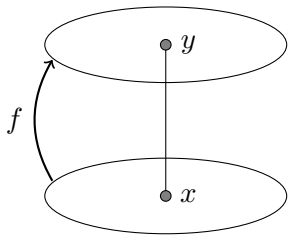

FIG. 1. $(x, y) \in \mathcal{N}(f)$ means that, in at least one case, knowing c_x is essential to determining $f(c)_y$. In other words, it means that there exists an antecedent configuration c such that changing the cell x will change the cell y of the image configuration $f(c)$.

In this paper, we assume that f is one-to-one, and that both f and f^{-1} are CA. Under these assumptions, another neighborhood scheme introduced in [4], namely the Block Neighborhood $\mathcal{BN}(.)$, is also finite. This notion arises naturally when we demand that the local mechanism that implements f be itself one-to-one, and wonder about its minimal size. To any evolution f of the classical configurations, we can thus associate a block neighborhood $\mathcal{BN}(f)$, so that "$(x, y) \in \mathcal{BN}(f)$" translates to "$x$ is in the range of minimal local reversible gate which computes y", for the dynamics f. Formally, the definition of $\mathcal{BN}(f)(x)$ is given in Fig. 2.

C. Quantum state space and evolutions

To each $x \in X$ we associate a Hilbert space $\mathcal{H}_x$, endowed with an orthonormal basis $\{|a\rangle|a \in \Sigma_x\}$. The local observable algebra associated to a cell x is $\mathcal{A}_x = L(\mathcal{H}_x)$. To each finite subset I of X we associate $\mathcal{A}_I = \bigotimes_{x \in I} \mathcal{A}_x$; if $I \subseteq J$, there is a natural embedding of $\mathcal{A}_I$

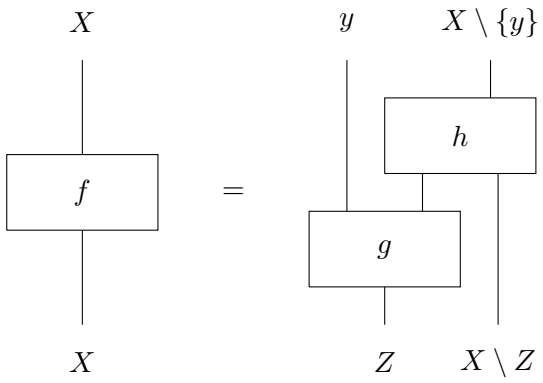

FIG. 2. $\mathcal{BN}(f)(y)$ is the smallest $Z \subseteq X$ such that f can be semilocalized, i.e. decomposed in such a way, with g and h bijective. Note that X and Z denote neither antecedents nor images of f; they are sets of cells. For instance, the left hand side reads "the image of a configuration on X by f is a configuration on X" and not "$f(X) = X$".

into $\mathcal{A}_J$. The limit of this system of inclusions is called the local algebra, and denoted $\mathcal{A}$; for all practical purposes an element $A \in \mathcal{A}$ can be thought of as a local operation $A = A_I \otimes Id_{X\setminus I}$ with I a finite subset of X [8]. A quantum evolution Q is just an automorphism $Q : \mathcal{A} \to \mathcal{A}$, i.e. a linear operator such that $Q(AB) = Q(A)Q(B)$ [24], but a more concrete view is to say that it maps any $A \in \mathcal{A}$ into $Q(A) = U^\dagger AU \in \mathcal{A}$ for some unitary operator U. Informally, this U can be thought of as acting on "$\bigotimes_{x\in X} \mathcal{H}_x$", i.e. it evolves the superpositions of configurations, in the Shrödinger picture. Again to any quantum evolution Q, we can associate a neighborhood $\mathcal{N}(Q)$, so that "$(x, y) \in \mathcal{N}(Q)$" translates to "$x$ can influence y", for the quantum evolution Q. Formally, by definition, $(x, y) \notin \mathcal{N}(Q)$ iff $Q(\mathcal{A}_y) \subseteq \mathcal{A}_{X\setminus\{x\}}$.

D. Quantization

In this paper, we are interested specifically in the quantum evolutions Q_f obtained by quantizing an evolution f. Intuitively, such a Q_f arises as follows. First, consider U_f the linear extension of f, which maps $\sum_i \alpha_i|c^i\rangle$ into $\sum_i \alpha_i|f(c^i)\rangle$. Then, let $Q_f(A)$ be ${U_f}^\dagger A U_f$. The problem with this approach is that U_f is not itself a member of $\mathcal{A}$, and so it is not clear whether Q_f makes sense as an operator over $\mathcal{A}$. In fact this fails to be the case for the XOR-CA.

In order reach a rigorous definition, we rely on the assumptions that not only f is bijective, but also that $\mathcal{N}(f)(x)$ and $\mathcal{N}(f^{-1})(x)$ are finite for every $x \in X$, so that f has finite block

neighborhood $\mathcal{BN}(f)$ [4]. Then Q_f will be well-defined, as it will map elements of $\mathcal{A}_y$ into elements of $\mathcal{A}_{\mathcal{BN}(f)(y)}$ and be an automorphism. More precisely, given some A in $\mathcal{A}_y$, consider the decomposition of f into bijections g and h with g over $\mathcal{BN}(f)(y)$ as in Fig. 2, and let U_g be the linear extension of g. We define $Q_f(A)$ to be ${U_g}^\dagger A U_g$, which is an element of $\mathcal{A}_{\mathcal{BN}(f)(y)}$ since so is U_g. Next we extend Q_f to the whole of $\mathcal{A}$ by demanding that it be an automorphism. Notice that this definition is consistent with the intuition that $Q_f(A)$ be ${U_f}^\dagger A U_f$, since for A in $\mathcal{A}_y$, we have ${U_f}^\dagger A U_f = {U_g}^\dagger A U_g$ as is clearly shown by Fig. 3. This definition of quantization coincides with that of [24].

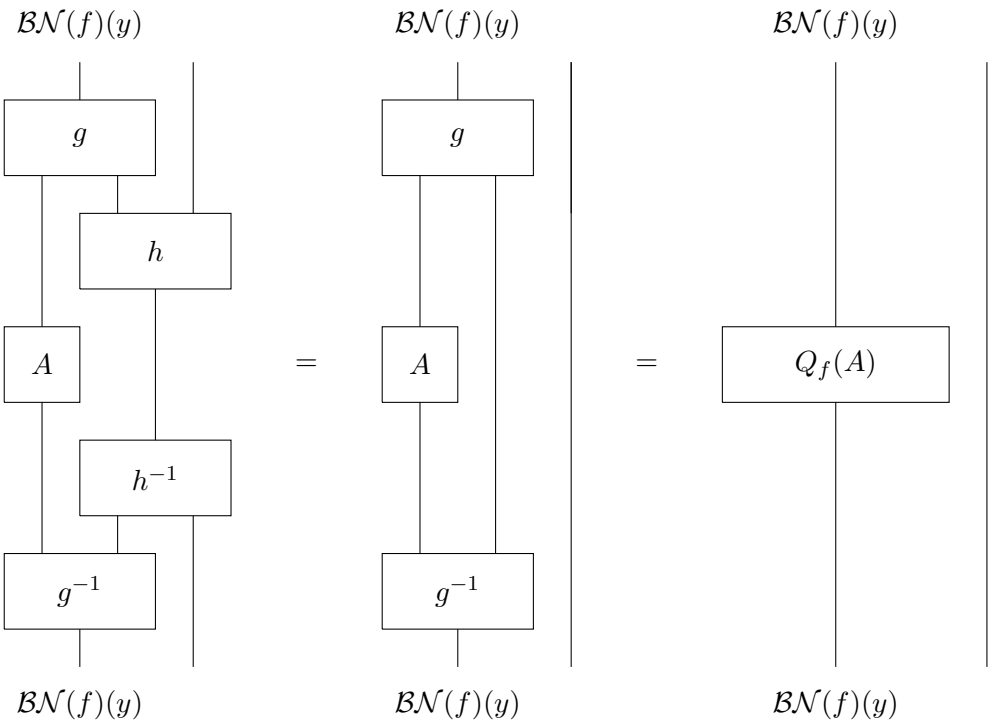

FIG. 3. Let A act on y. Intuitively $Q_f(A)$ is ${U_f}^\dagger A U_f$, but this is not always local. However if $\mathcal{BN}(f)(y)$ is finite, U_f decomposes into U_g and U_h, and ${U_f}^\dagger A U_f$ yields the left picture. The U_h cancel out (middle), and the remainder ${U_g}^\dagger A U_g$ makes for a good, local definition of $Q_f(A)$.

E. Quantum versus block neighborhoods

Figure 3 provides a definition of Q_f, but it also gives a justification that $\mathcal{N}(Q_f)$, the *quantum neighborhood* of f, is included in $\mathcal{BN}(f)$. Moreover, as is proven in the appendix, we have the converse inclusion $\mathcal{N}(Q_f) \supseteq \mathcal{BN}(f)$. Quantum and block neighborhoods are thus, as it was

hinted in [1] but never actually proven, the same thing.

Proposition 1. *Let $f : \mathcal{C} \to \mathcal{C}$ be bijective and such that for every $x \in X$, both $\mathcal{N}(f)(x)$ and $\mathcal{N}(f^{-1})(x)$ are finite. Then its quantization $Q_f : \mathcal{A} \to \mathcal{A}$ fulfills $\mathcal{N}(Q_f) = \mathcal{B}\mathcal{N}(f)$.*

Compare this with [10], which states that semicausality (i.e. "the system y can only be influenced by $\mathcal{N}(Q)(Y)$") and semilocalizability (i.e. "the system y can be computed by a circuit of automorphisms of the form of Fig. 2") are equivalent in the quantum regime. Our proposition is very closely related to that statement; more precisely, it can be seen as its classical counterpart, although neither result is directly derived from the other. In the remainder of this paper, it will allow us to generalize the results of [1] to the quantum setting, as corollaries.

F. Bounds on the Quantum Neighborhood

To state the bounds, we introduce a composition of neighborhood sets, by which $(x, z) \in \mathcal{N}_1\mathcal{N}_2$ means that for some y we have $(x, y) \in \mathcal{N}_1$ and $(y, z) \in \mathcal{N}_2$. If the $\mathcal{N}_i$ are the graphs of functions, this is just the composition of functions. Moreover, this operation matches the composition of automata, so that $\mathcal{N}(fg) \subseteq \mathcal{N}(g)\mathcal{N}(f)$. By $\mathcal{N}^T$ we denote the transpose, i.e., the set of pairs (y, x) with $(x, y) \in \mathcal{N}$. Notice that the transposition, as it does with matrices, reverses the order of composition : $(\mathcal{N}_1\mathcal{N}_2)^T = \mathcal{N}_2^T\mathcal{N}_1^T$.

Lemma 4 of [24] can then be expressed as such:

$$\mathcal{N}(f) \subseteq \mathcal{N}(Q_f) \subseteq \mathcal{N}(f)\mathcal{N}^T(f)\mathcal{N}^T(f^{-1}) \,. \tag{1}$$

A crucial property of quantum neighborhoods is that $\mathcal{N}(Q^{-1}) = \mathcal{N}^T(Q)$ [5]. This is somewhat surprising, since in the classical case there is not even a bound on the size of $\mathcal{N}(f^{-1})$ in terms of $\mathcal{N}(f)$. Indeed this is the feature that makes examples like the XOR-CA possible, and makes the problem whether or not an automaton is reversible undecidable in ≥ 2 dimensions. In contrast, computing the quantum inverse is literally as easy as transposing and conjugating a unitary matrix.

If we apply (1) to f^{-1} we get

$$\mathcal{N}(f^{-1}) \subseteq \mathcal{N}(Q_{f^{-1}}) \subseteq \mathcal{N}(f^{-1})\mathcal{N}^T(f^{-1})\mathcal{N}^T(f) \,. \tag{2}$$

The quantization $Q_{f^{-1}}$ of the inverse of f is equal to Q_f^{-1}, the inverse operation of the quantization of f. We can therefore write

$$\mathcal{N}(f^{-1}) \subseteq \mathcal{N}(Q_f^{-1}) \subseteq \mathcal{N}(f^{-1})\mathcal{N}^T(f^{-1})\mathcal{N}^T(f)\ . \tag{3}$$

We now take the transpose of these terms; keeping in mind that this operation reverses the order of composition, we get

$$\mathcal{N}^T(f^{-1}) \subseteq \mathcal{N}^T(Q_f^{-1}) \subseteq \mathcal{N}(f)\mathcal{N}(f^{-1})\mathcal{N}^T(f^{-1})\ . \tag{4}$$

Lastly, since $\mathcal{N}(Q^{-1}) = \mathcal{N}^T(Q)$, we have

$$\mathcal{N}^T(f^{-1}) \subseteq \mathcal{N}(Q_f) \subseteq \mathcal{N}(f)\mathcal{N}(f^{-1})\mathcal{N}^T(f^{-1})\ . \tag{5}$$

Corollary 1. $\mathcal{N}(f)\cup\mathcal{N}^T(f^{-1}) \subseteq \mathcal{N}(Q_f) \subseteq \big(\mathcal{N}(f)\mathcal{N}^T(f)\mathcal{N}^T(f^{-1})\big)\cap\big(\mathcal{N}(f)\mathcal{N}(f^{-1})\mathcal{N}^T(f^{-1})\big)$.

These are the best general bounds on $\mathcal{N}(Q_f)$ known to us. The dependencies in the classical neighborhoods which must be satisfied for a dependence $(x, y) \in \mathcal{N}(Q_f)$ to occur are shown in Fig. 4.

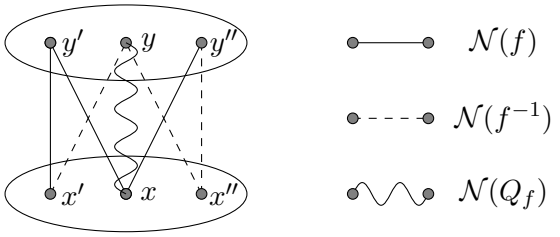

FIG. 4. Illustration of the combined upper bounds (1) and (5). In order to be able to send a signal from x to y in the quantum regime, it is necessary that there exist x', x'', y' and y'' forming such a pattern (points on each side need not be distinct).

IV. TOFFOLI-CA: AN EXAMPLE WITH LARGE QUANTUM STEP SIZE

Examples using the ideas of the XOR-CA, i.e., examples with $\mathcal{N}(f^{-1})$ much larger than $\mathcal{N}(f)$ show that $\mathcal{N}(Q_f)$ can be much larger than $\mathcal{N}(f)$. But can the upper bounds (1) and (5) also be exhausted? That is, even if we accept for a fact that the inverse neighborhood of f enters $\mathcal{N}(Q_f)$, can we get a speedup? An example, the Toffoli-CA[4], is illustrated in Figure 5. It is based on the TOFFOLI gate, a double conditioned CNOT. In the diagrams the conditioning is represented as a horizontal line, and the qubits by slanted lines. Since neighboring TOFFOLI gates commute, their

ordering is irrelevant. Each single cell now contains two qubits. The alphabet is $\{00, 01, 01, 11\}$, with 00 taken as the quiescent symbol. The classical transition function acting for updating a cell with content cd, with left neighbor containing ab is $\delta(abcd) = b(c \oplus b \cdot d)$, where the product $b \cdot d$ is just the AND of bits.

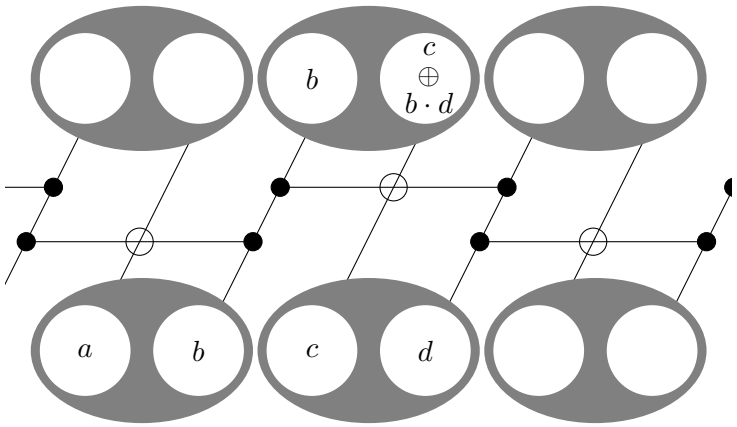

FIG. 5. The Toffoli-CA.

Each cell is made of two bits. The leftmost bit at the next time step is just the rightmost bit of the left neighbor at the previous time step (b). The rightmost bit at the next time step is the leftmost bit at the previous time step (c), inverted if both b and the rightmost bit (d) were set to one, i.e. $c \oplus b \cdot d$.

Whenever a transition rule commutes with translations, the neighborhoods have the property that $(x, y) \in \mathcal{N} \Leftrightarrow (x + z, y + z) \in \mathcal{N}$, and are hence completely characterized by the set $\mathcal{N}' = \{y - x | (x, y) \in \mathcal{N}\}$. This is the case for the Toffoli-CA for which we have $\mathcal{N}'(f) = \{-1, 0\}$. Its inverse neighborhood is also quite small: $\mathcal{N}'(f^{-1}) = \{0, 1\}$. Indeed, each TOFFOLI gate is its own inverse, so f^{-1} can be represented simply by turning Figure 5 upside-down. So the discrepancy between forward and a possibly much larger inverse neighborhood is irrelevant here. Yet, the quantum neighborhood is strictly larger than its classical neighborhood. For instance, using the fact that $\mathrm{CNot}|+-\rangle = |--\rangle$, Figure 6 shows how to transmit information from cell 0 to cell 2. This does saturates the upper bounds (1) and (5) in the sense that the speed in $\mathcal{N}(Q_f)$ is least twice that of both $\mathcal{N}(f)$ and $\mathcal{N}(f^{-1})$. If we look at things more closely, however, the upper bounds (1) and (5) would both give $\{-2, -1, 0, 1\}$, whereas we actually have $\mathcal{N}'(Q_f) = \{-2, -1, 0\}$. However it is clear that a symmetrized version of the Toffoli-CA (two symmetrical versions of it, running in parallel) would saturate the bounds $\{-2 \ldots 2\}$ on both sides.

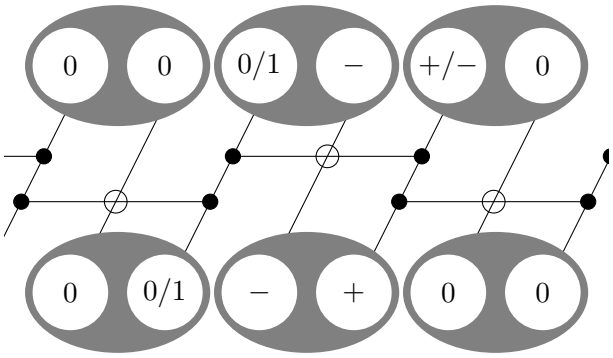

FIG. 6. For the Toffoli-CA, the quantum neighborhood $\mathcal{N}(Q_f)$ contains -2. Indeed, focus on the middle TOFFOLI gate, and forget about its left wire for a second. We are left with a CNot gate, apparently controlled by its right wire. But it is a well-known (albeit curious) fact that switching to the $|\pm\rangle$ basis flips who controls whom. So, this CNot gate, if activated, will effectively toggle the right wire. Now, recalling that this CNot gate is in fact part of a TOFFOLI gate and thus activated by the left wire, we see that changing the left, toggles the right.

V. ASYMPTOTICS

A. Toffoli-CA: no asymptotic quantum speedup

It would thus appear that quantum information can travel twice as fast as classical information under the Toffoli-CA. But in order to realize this gain, we must iterate the automaton. Figure 7 shows the result. The iterated quantum neighborhood is again larger than its classical counterpart, but not by much: it is $\mathcal{N}(Q_{f^n}) = \{-(n+1), -n, \ldots, 0\}$, which differs from $\mathcal{N}(f^n)$ by the single cell $-(n+1)$. Indeed, we have seen how in one step the right component of cell -2 reaches the left component of cell 0. But then, as the TOFFOLI gates commute, the left component of cell 0 can only reach the left component of cell 1, and so on.

The Toffoli-CA supports a large first step, but from then on no further speedup—is this a special, or a general property? The following corollary settles this question. It comes from and Proposition 1 and proposition 2.3 in [1], its proof is to be found in [1], and is too tedious to be reproduced here.

Corollary 2. $\mathcal{N}(Q_{f_n \cdots f_1}) \subseteq \bigcup_{k=1}^{n} \mathcal{N}^T\left((f_n \cdots f_{k+1})^{-1}\right) \mathcal{N}(Q_{f_k}) \mathcal{N}(f_{k-1} \cdots f_1)$.

If we apply this result to the case where $f_1 = f_2 = \ldots = f_n = f$, we get

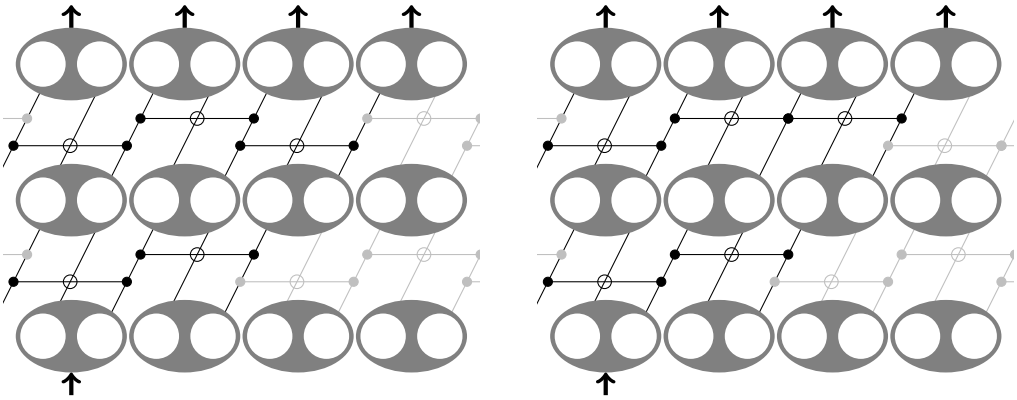

FIG. 7. The quantum neighborhood of the iterated Toffoli-CA does not grow very fast. The bottom-left cell can spread its influence only through the black gates (*left*). In the first step, because it touches the left wire of a TOFFOLI gate, it can signal at speed two. But it only reaches the rightmost bit of the third cell, so that in the second step, because the top-left TOFFOLI gates commute (*right*), there is no way it can signal at speed two again.

$$\mathcal{N}(Q_{f^n}) \subseteq \bigcup_{k=1}^{n} \mathcal{N}^T(f^{k-n})\mathcal{N}(Q_f)\mathcal{N}(f^{k-1}) \tag{6}$$

When f is the Toffoli-CA, we have $\mathcal{N}(f^n) = \mathcal{N}^T(f^{-n})$, which implies that all the quantum speedup of $\mathcal{N}(Q_{f^n})$ just comes from the single-step speedup: The ratio between the sizes of $\mathcal{N}(Q_{f^n})$ and $\mathcal{N}(f^n)$ asymptotically goes to 1, as n goes to infinity.

In the general case the result involves a composition of arbitrary f_i-s, and is illustrated in Figure 8 for arbitrary f_i-s and $n = 3$. Although it is difficult to give an intuitive explanation as to *why* this corollary is true, it is not too hard to grasp what it *means*: The messages that can be transmitted from one location to another in a quantum universe ruled by the dynamics $f_n \cdots f_1$ must follow a particular protocol. First, they are transmitted trough $k-1$ steps under a purely classical form — this is denoted in Figure 8 with a plain line. Then, on the k-th step, similarly to the trick we used for the Toffoli-CA, something quantum happens — this is denoted with a wavy line. Afterwards, through the remaining $n-k$ steps, this message is transmitted in a way that can be described as dual to a classical channel — this is denoted with a dotted line.

Figure 9, on the other hand, illustrates it when all of the f_i-s are equal, for an arbitrary number of steps of a one-dimensional CA. Notice that the dotted lines in this Figure 9 suggest that, in the specific case when $\mathcal{N}_{f^{-1}} \supset \mathcal{N}(f)$, the corresponding QCA Q_f could, in principle, take that

one benefit to signal asymptotically faster than f. Since this is not the case of the Toffoli-CA we now need an example showing that when $\mathcal{N}(f^{-n})$ is larger than $\mathcal{N}(f^n)$, you can actually transmit information at a long distance, thereby saturating Corollary 2.

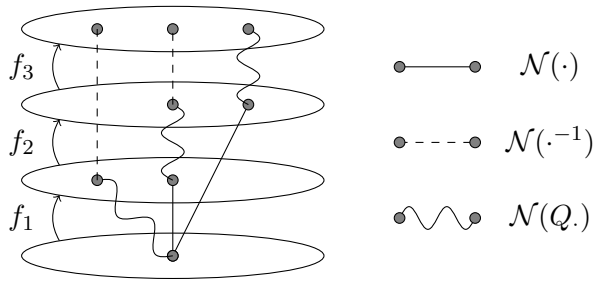

FIG. 8. Illustration of Corollary 2 when $n = 3$.

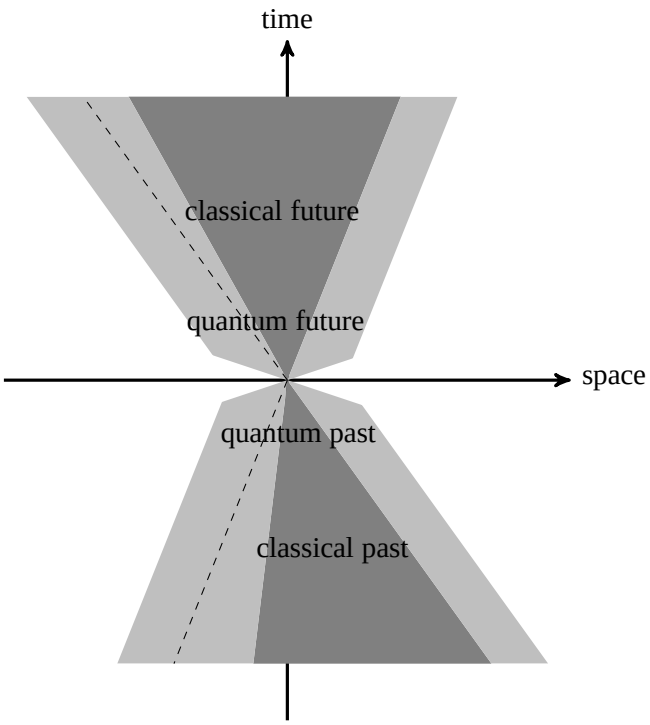

FIG. 9. Typical asymptotics for iterated dynamics.

B. J-CA: achieving the maximal quantum speed

Let $\Sigma = (\mathbb{Z}/2\mathbb{Z})^d$. For $x \in \Sigma$, x^i denotes its i-th component. We define a CA J_d on this cell structure in the following way:

$$J_d(v)_0^i = \begin{cases} v_0^i + v_1^{i+1} & \text{if } i < d \\ v_1^1 & \text{if } i = d \end{cases}. \tag{7}$$

Its inverse is given by

$$J_d^{-1}(v)_0^i = v_{-i}^d + \sum_{j=1}^{i-1} v_{j-i}^j. \tag{8}$$

We thus have $\mathcal{N}(J_d) = \{0, 1\}$ and $\mathcal{N}(J_d^{-1}) = \{-d, \dots, -1\}$. Let us now illustrate the left inclusion of (5) by showing that the quantum neighborhood of J_d does indeed contain d.

Let b be the zero configuration defined by $b_k = (0, \dots, 0)$ for all $n \in \mathbb{Z}$, and c defined by $c_k^i = \delta_{in}$. It is easily checked that $f(b)$ is also the zero word, whereas $f(c)_k^i = \delta_{k0}$. The point is that $f(b)$ and $f(c)$ coincide on $\mathbb{Z} \setminus \{0\}$, whereas $b_d \neq c_d$. Now, imagine Alice and Bob respectively live in cell d and 0, and that the dynamics of their universe is described by $Q(J_d)$. Assuming they share prior entanglement, Alice can transmit a message to Bob in a single step. Indeed, say the initial state is $|\psi_+\rangle = \frac{1}{\sqrt{2}}(|b\rangle + |c\rangle)$. Since Alice is at a place where she can distinguish b from c, she can, by applying a local controlled phase gate, switch at will from $|\psi_+\rangle$ to $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|b\rangle - |c\rangle)$. One time step later, their world is in the pure state $|\phi_\pm\rangle = \frac{1}{\sqrt{2}}(|J_d(b)\rangle \pm |J_d(c)\rangle)$. Since $J_d(b)$ and $J_d(c)$ coincide outside Bob's place, where they are equal to zero, one can write $|\phi_\pm\rangle = |\underline{0}\rangle \otimes |\varphi_\pm\rangle$, where $|\varphi_\pm\rangle$ is totally accessible to Bob, and so that he can easily observe, with local measurement, whether Alice switched from $|\psi_+\rangle$ to $|\psi_-\rangle$. Alice was thus able to transmit one bit of information to Bob in just one time step, proving $d \in \mathcal{N}(Q_{J_d})$.

As for the asymptotic bound, $\mathcal{N}(J_d^n)$ must be included in $\mathcal{N}(J_d)^n = \{0, \dots, n\}$, but one can notice, for instance, that $J_d^{-n}(v)_0^d$ contains the term v_{-dn}^d also exactly once; Therefore $dn \in \mathcal{N}^T(J_d^{-n})$. Hence this example saturates the asymptotic upper bound. It is a pure example where the sound cone of the quantized automaton is just the union of the classical sound cone ($\mathcal{N}(f^n)$) and its dual ($\mathcal{N}^T(f^{-n})$). As n increases, the ratio of the widths of the classical cone and the quantum one remains a constant d. This example can also be easily symmetrized, by taking $\Sigma = (\mathbb{Z}/2\mathbb{Z})^{2d}$, applying J_d on the first d entries, and the symmetrized of J_d on the others.

CONCLUSION

Let us summarize the main points of interest.

- For a single step of a dynamics f, quantum information can jump unboundedly further than

classical information, as propagated by f. This typically requires prior entanglement shared between parties.

- Quantum information can also jump further than classical information, as propagated by both f and f^{-1}, but only in a bounded way. We give optimal bounds on this quantum neighborhood, as a function of the neighborhoods of f and f^{-1}.

- Therefore, even though the neighborhood of f^{-1} cannot be bounded by a computable function in terms of the neighborhood of f [14–16], it is still the case that if we are given both the neighborhoods of f and f^{-1}, then we can bound the quantum neighborhood.

- When iterating the dynamics f, quantum information can again flow asymptotically unboundedly faster than classical information, as propagated by f. But it cannot flow asymptotically faster than classical information as propagated by both f and f^{-1}.

- Therefore in the case of an evolution with a proper time symmetry, quantum information cannot flow asymptotically faster than classical information.

Future works include of course a better understanding and physical interpretation of this channel, which should make full use of the duality.

ACKNOWLEDGEMENTS

This work has been funded by the ANR-12-BS02-007-01 TARMAC grant, the ANR-10-JCJC-0208 CausaQ grant, and the Deutsche Forschungsgemeinschaft (Forschergruppe 635). This work has been partially done at IXXI.

---

[1] ARRIGHI, P., AND NESME, V. The Block Neighborhood. In *Proceedings of JAC 2010* (Turku, Finlande, Dec. 2010), TUCS, Ed., pp. 43–53.

[2] ARRIGHI, P., NESME, V., AND WERNER, R. Unitarity plus causality implies localizability. *J. of Computer and Systems Sciences 77* (2010), 372–378. QIP 2010 (long talk).

[3] ARRIGHI, P., NESME, V., AND WERNER, R. Unitarity plus causality implies localizability (full version). *Journal of Computer and System Sciences 77*, 2 (2011), 372–378.

[4] ARRIGHI, P., NESME, V., AND WERNER, R. F. One-dimensional quantum cellular automata over finite, unbounded configurations. In *Language and Automata Theory and Applications: Second International Conference, LATA 2008, Tarragona, Spain, March 13-19, 2008. Revised Papers* (Berlin, Heidelberg, 2008), Springer-Verlag, pp. 64–75.

[5] ARRIGHI, P., NESME, V., AND WERNER, R. F. Unitarity plus causality implies localizability. *J. Comput. Syst. Sci. 77*, 2 (2011), 372–378.

[6] BIALYNICKI-BIRULA, I. Weyl, Dirac, and Maxwell equations on a lattice as unitary cellular automata. *Phys. Rev. D. 49*, 12 (1994), 6920–6927.

[7] BOGHOSIAN, B. M., AND TAYLOR, W. Quantum lattice-gas model for the many-particle Schrödinger equation in d-dimensions. *Phys. Rev. E. 57*, 1 (1998), 54–66.

[8] BRATTELI, O., AND ROBINSON, D. W. *Operators algebras and quantum statistical mechanics*, vol. 1. Springer, 1987.

[9] BRENNEN, G. K., AND WILLIAMS, J. E. Entanglement dynamics in one-dimensional quantum cellular automata. *Phys. Rev. A. 68*, 4 (Oct 2003), 042311.

[10] EGGELING, T., SCHLINGEMANN, D., AND WERNER, R. F. Semilocal operations are semilocalizable. *Europhysics Letters 57*, 6 (2002), 782–788.

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

[12] GÜTSCHOW, J., UPHOFF, S., WERNER, R. F., AND ZIMBORÁS, Z. Time asymptotics and entanglement generation of Clifford quantum cellular automata. *Journal of Mathematical Physics 51*, 1 (2010), 015203.

[13] HEDLUND, G. A. Endomorphisms and automorphisms of the shift dynamical system. *Mathematical systems theory 3*, 4 (December 1969), 320–375.

[14] KARI, J. Reversibility of 2d cellular automata is undecidable. *Physica D 45*, 1-3 (1990), 386–395.

[15] KARI, J. Reversibility of 2D cellular automata is undecidable. In *Cellular Automata: Theory and Experiment*, vol. 45. MIT Press, 1991, pp. 379–385.

[16] KARI, J. Representation of reversible cellular automata with block permutations. *Mathematical Systems Theory 29*, 1 (1996), 47–61.

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

[18] LLOYD, S. A theory of quantum gravity based on quantum computation. ArXiv preprint: quant-ph/0501135, 2005.

[19] LOVE, P., AND BOGHOSIAN, B. From Dirac to Diffusion: decoherence in Quantum Lattice gases. *Quantum Information Processing 4*, 4 (2005), 335–354.

[20] MARGOLUS, N. Physics-like models of computation. *Physica D: Nonlinear Phenomena 10*, 1-2 (1984), 81–95.

[21] MARGOLUS, N. 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, May-June 1989, in Santa Fe, New Mexico* (1990), Perseus Books, pp. 273–293.

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

[23] NAGAJ, D., AND WOCJAN, P. Hamiltonian quantum cellular automata in one dimension. *Phy. Rev. A. 78*, 3 (2008), 032311.

[24] SCHUMACHER, B., AND WERNER, R. F. Reversible quantum cellular automata. `arXiv:quant-ph/0405174`, May 2004.

[25] 'T HOOFT, G. Entangled quantum states in a local deterministic theory. `arXiv:0908.3408`, August 2009.

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

[27] VOLLBRECHT, K. G. H., AND CIRAC, J. I. Reversible universal quantum computation within translation-invariant systems. *Phys. Rev. A. 73*, 1 (2006).

[28] VON NEUMANN, J. *Theory of Self-Reproducing Automata*. University of Illinois Press, Champaign, IL, USA, 1966.

Appendix: The quantum neighborhood contains the block neighborhood

Proposition 2. $\mathcal{BN}(f) \subseteq \mathcal{N}(Q_f)$.

Let $x, y \in X$ such that $(x, y) \notin \mathcal{N}(Q_f)$, i.e. such that $Q_f(\mathcal{A}_y) \subseteq \mathcal{A}_{X\setminus\{x\}}$. We have to prove that $(x, y) \notin \mathcal{BN}(f)$, i.e. that f can be semilocalized as in Figure 2 with $Z = X \setminus \{x\}$. We will proceed in two steps. In the first step, we prove four combinatorial properties that we will tap into in the second and final step, where we explicitly construct the bijections g and h as seen in Figure 2.

Four properties

We will prove that these hold:

(1) $(x, y) \notin \mathcal{N}(f)$;

(2) $(y, x) \notin \mathcal{N}(f^{-1})$;

(3) When $v, w \in \mathcal{C}$ are such that $v_x = w_x$, it is enough to know $v_{X\setminus\{x\}}$ and $w_{X\setminus\{x\}}$ in order to determine whether $f(v)_{X\setminus\{y\}} = f(w)_{X\setminus\{y\}}$;

(4) When $v, w \in \mathcal{C}$ are such that $f(v)_y = f(w)_y$, it is enough to know $f(v)_{X\setminus\{y\}}$ and $f(w)_{X\setminus\{y\}}$ in order to determine whether $v_{X\setminus\{x\}} = w_{X\setminus\{x\}}$.

In order to do so, let us introduce some notations. For $v, w \in \mathcal{C}$ and $a, b \in \Sigma_y$, let $q(v, w, a, b)$ be $\langle v|Q_f\left(|a\rangle\langle b|\right)|w\rangle$. Since $q(v, w, a, b) = \sum_{u\in\Sigma_{X\setminus\{y\}}} \langle f(v)|(|a\rangle\langle b| \otimes |u\rangle\langle u|)|f(w)\rangle$, we have

$$q(v, w, a, b) = \begin{cases} 1 \text{ if } f(v)_y = a,\ f(w)_y = b \text{ and } f(v)_{X\setminus\{y\}} = f(w)_{X\setminus\{y\}} \\ 0 \text{ otherwise} \end{cases} \tag{A.1}$$

Since $Q_f\left(\mathcal{A}_y\right) \subseteq \mathcal{A}_{X\setminus\{x\}}$, we have $Q_f\left(\mathcal{A}_y\right) = M \otimes \mathbb{I}_{\mathcal{A}_x}$ for some $M \in \mathcal{A}_{X\setminus\{x\}}$, from which we deduce that q has the following properties :

(i) if $v_x \neq w_x$, then $q(v, w, a, b) = 0$;

(ii) if $v_x = w_x$, then $q(v, w, a, b)$ depends only on $v_{X\setminus\{x\}}$ and $w_{X\setminus\{x\}}$, a and b.

Let us now prove points (1), (2), (3) and (4).

(1) In order to prove that x is not in the classical neighborhood of y for f, we have to show that, for any configurations v and w that coincide on $X \setminus \{x\}$, $f(v)_y = f(w)_y$. Let then $v, w \in \mathcal{C}$ such that $v_{X\setminus\{x\}} = w_{X\setminus\{x\}}$. First, $q\left(v, v, f(v)_y, f(v)_y\right)) = 1$. But, by (ii), since $w_{X\setminus\{x\}} = v_{X\setminus\{x\}}$, we get $q\left(w, w, f(v)_y, f(v)_y\right) = 1$, which means $f(v)_y = f(w)_y$.

(2) Similarly, in order to prove that y is not in the classical neighborhood of x for f^{-1}, we have to show that, for any configurations v and w such that $f(v)$ and $f(w)$ coincide on $X \setminus \{y\}$, $v_x = w_x$. Let then $v, w \in \mathcal{C}$ such that $f(v)_{X\setminus\{y\}} = f(w)_{X\setminus\{y\}}$. We then have $q\left(v, w, f(v)_y, f(w)_y\right) = 1$, which implies, by (i), that $v_x = w_x$.

(3) Let $v, w \in \mathcal{C}$ be configurations such that $v_x = w_x$. Then $q(v, w, f(v)_y, f(w)_y) = 1$ if and only if $f(v)_{X\setminus\{y\}} = f(w)_{X\setminus\{y\}}$. Can this quantity be determined knowing only $v_{X\setminus\{x\}}$ and $w_{X\setminus\{x\}}$? Yes: We have already proven in (1) that $f(v)_y$ and $f(w)_y$ are determined by $v_{X\setminus\{x\}}$ and $w_{X\setminus\{x\}}$; and by hypothesis, for any fixed $a, b \in \Sigma_y$, $q(v, w, a, b)$ depends only on $v_{X\setminus\{x\}}$ and $w_{X\setminus\{x\}}$.

(4) We want to prove that, for any $v, w \in \mathcal{C}$ such that $f(v)_y = f(w)_y$, it is enough to know $f(v)_{X\setminus\{y\}}$ and $f(w)_{X\setminus\{y\}}$ to determine whether $v_{X\setminus\{x\}} = w_{X\setminus\{x\}}$.

In order to do so, let $v, w, v', w' \in \mathcal{C}$ be such that $f(v)_y = f(w)_y$, $f(v')_y = f(w')_y$, $f(v)_{X\setminus\{y\}} = f(v')_{X\setminus\{y\}}$, $f(w)_{X\setminus\{y\}} = f(w')_{X\setminus\{y\}}$ and $v_{X\setminus\{x\}} = w_{X\setminus\{x\}}$. We have to prove that $v'_{X\setminus\{x\}} = w'_{X\setminus\{x\}}$.

First, from (2) and $f(v)_{X\setminus\{y\}} = f(v')_{X\setminus\{y\}}$, we get $v_x = v'_x$; therefore, according to (3), not only do we have $f(v_{X\setminus\{x\}}.v_x)_{X\setminus\{y\}} = f(v'_{X\setminus\{x\}}.v_x)_{X\setminus\{y\}}$, but for any $a \in \Sigma_x$, $f(v_{X\setminus\{x\}}.a)_{X\setminus\{y\}} = f(v'_{X\setminus\{x\}}.a)_{X\setminus\{y\}}$. Likewise, for any $a \in \Sigma_x$, $f(w_{X\setminus\{x\}}.a)_{X\setminus\{y\}} = f(w'_{X\setminus\{x\}}.a)_{X\setminus\{y\}}$.

Let a be an arbitrary element of Σ_x. Since, by assumption, $v_{X\setminus\{x\}} = w_{X\setminus\{x\}}$, we can therefore deduce the following :

$$f(v'_{X\setminus\{x\}}.a)_{X\setminus\{y\}} = f(v_{X\setminus\{x\}}.a)_{X\setminus\{y\}} = f(w_{X\setminus\{x\}}.a)_{X\setminus\{y\}} = f(w'_{X\setminus\{x\}}.a)_{X\setminus\{y\}}.$$

Moreover, from (1) we get $f(v'_{X\setminus\{x\}}.a)_y = f(w'_{X\setminus\{x\}}.a)_y$. Therefore $f(v'_{X\setminus\{x\}}.a) = f(w'_{X\setminus\{x\}}.a)$; since f is one-to-one, we conclude that $v'_{X\setminus\{x\}} = w'_{X\setminus\{x\}}$.

Block construction

Let $\sim_x$ be the binary relation on $\Sigma_{X\setminus\{x\}}$ defined by

$$v \sim_x v' \quad \text{iff} \quad \forall a \in \Sigma_x \; f(v.a)_{X\setminus\{y\}} = f(v'.a)_{X\setminus\{y\}}.$$

Note that, because of (3), this is actually equivalent to $\exists a \in \Sigma_x \; f(v.a)_{X\setminus\{y\}} = f(v'.a)_{X\setminus\{y\}}$, from which we deduce

$$\forall b, b' \in \Sigma_y \; \forall w \in \Sigma_{X\setminus\{y\}} \quad f^{-1}(w.b)_{X\setminus\{x\}} \sim_x f^{-1}(w.b')_{X\setminus\{x\}} \tag{A.2}$$

Indeed, given any $b, b' \in \Sigma_y$ and $w \in \Sigma_{X\setminus\{y\}}$, we can set $v = f^{-1}(w.b)_{X\setminus\{x\}}$, $v' = f^{-1}(w.b')_{X\setminus\{x\}}$ and $a = f^{-1}(w.b)_x$. Because of (2), we also have $a = f^{-1}(w.b')$, so that $f(v.a)_{X\setminus\{y\}} = f(v'.a)_{X\setminus\{y\}}$.

$\sim_x$ is clearly an equivalence relation, so using (1) we can define

$$\lambda : \begin{pmatrix} \Sigma_{X\setminus\{x\}} & \to & \Sigma_y \times (\Sigma_{X\setminus\{x\}}/\sim_x) \\ v & \mapsto & (f(v.a)_y, [v]) \end{pmatrix}$$

where a is an arbitrary element of Σ_x and $[v]$ is the class of v in $\Sigma_{X\setminus\{x\}}/\sim_x$. Thanks to (2) and (4), one can likewise define $\sim_y$ on $\Sigma_{X\setminus\{y\}}$; we have the corresponding property

$$\forall a, a' \in \Sigma_x \; \forall v \in \Sigma_{X\setminus\{x\}} \quad f(v.a)_{X\setminus\{y\}} \sim_y f(v.a')_{X\setminus\{y\}} \tag{A.3}$$

and we can define

$$\mu : \begin{pmatrix} \Sigma_{X\setminus\{y\}} & \to & \Sigma_x \times (\Sigma_{X\setminus\{y\}}/\sim_y) \\ w & \mapsto & (f^{-1}(w.b)_x, [w]) \end{pmatrix}$$

where b is an arbitrary element of Σ_y.

We now introduce

$$\alpha : \begin{pmatrix} \Sigma_{X\setminus\{x\}}/\sim_x & \to & \Sigma_{X\setminus\{y\}}/\sim_y \\ [v] & \mapsto & \left[f(v.a)_{X\setminus\{y\}}\right] \end{pmatrix}$$

where a is again an arbitrary element of Σ_x. Let us prove that α is a well-defined bijection. In order to prove that it is well-defined, we need to show that for every $v, v' \in X \setminus \{x\}$ such that $v \sim_x v'$ and every $a, a' \in \Sigma_x$, $f(v.a)_{X\setminus\{y\}} \sim_y f(v'.a')_{X\setminus\{y\}}$, which is easily done in two small steps. First, by definition of $\sim_x$, $f(v.a)_{X\setminus\{y\}} = f(v'.a)_{X\setminus\{y\}}$. Then, by (A.3), $f(v'.a)_{X\setminus\{y\}} \sim_y f(v'.a')$. We now prove that α is bijection by constructing its inverse β. We define β as follows:

$$\beta : \begin{pmatrix} \Sigma_{X\setminus\{y\}}/\sim_y & \to & \Sigma_{X\setminus\{x\}}/\sim_x \\ [w] & \mapsto & \left[f^{-1}(w.b)_{X\setminus\{x\}}\right] \end{pmatrix}$$

We then have $\beta\alpha([v]) = [f^{-1}(f(v.a)_{X\setminus\{y\}}.b)_{X\setminus\{x\}}]$. Since this value is independent of b, we can try in particular with $b = f(v.a)_y$, where it is clear that we get $[v]$.

We near the end of our construction, which consists in finding a block decomposition according to Figure 2, where $Z = X \setminus \{x\}$. We define $g = (\mathrm{id}_{\Sigma_y} \times \alpha)\lambda : \Sigma_{X\setminus\{x\}} \to \Sigma_y \times (\Sigma_{X\setminus\{y\}}/\sim_y)$. It is a bijection because we can define its inverse g^{-1} by $g^{-1}(b, [w]) = f^{-1}(w.b)_{X\setminus\{x\}}$, which is well-defined by definition of $\sim_y$.

Since α and g are bijections, so is λ, and so is μ symmetrically. We can therefore define $h = \mu^{-1}$ and thus complete our proof.