PhysComp96: vand
Extended abstract
Draft, 21 May 1996
vandam: wimvdam@cs.kun.nl

A universal quantum cellular automaton

Wim van Dam
wimvdam@cs.kun.nl
Computing Science Institute, University of Nijmegen
Toernooiveld 1, NL – 6525 ED Nijmegen, The Netherlands

We will prove the existence of a universal quantum cellular automaton. Such QCA are defined as the quantum-mechanical pendant of classical one-dimensional cellular automata. As is the case with quantum Turing machines, the well-formedness restriction plays an important role. It will be shown that every proper QCA obeys a local constraint which is comparable with the 'inverse neighborhood' of classical reversible cellular automata. This allows us to describe every QCA as a periodic quantum gate array, which can be simulated (with a bounded error) by a universal automaton $\mathcal{U}$. The time complexity of this simulation does not depend on the size of the QCA to be simulated.

1 Introduction

Over the past few years there has been a growing interest in the theory of *quantum computation.* This was aroused in the 80's by Benioff[5], Deutsch[9, 10] and Feynman[15, 16] who replaced the implicit classical assumptions of computational models by the laws of quantum physics. By doing so, computer scientists and physicists enter the joint field of quantum Turing machines[7, 9, 22], quantum gates[3, 4, 11], quantum networks[4, 8, 10, 22], etc.

This article applies the 'quantum paradigm shift' to the computational model of *cellular automata*, which will lead us to a definition of one-dimensional *quantum* CA. These automata have been described before in a similar way by Watrous[21] and Dürr et al.[13, 14]. Along with this definition we have to take a closer look at the well-formedness restriction which tells us that only a fraction of the possible QCA has a valid physical meaning. (This is the main interest of the two articles by Dürr et al.) Coherent quantum mechanical processes are only possible in combination with a unitary and therefore reversible time operator. For this reason the 'classical results' on invertible computation have a great significance to the theory of quantum computation[6]. The QCA-model makes no exception to this 'rule of thumb'.

Watrous uses the earlier results on reversible, one-dimensional CA which are computational universal[19, 20] to create a QCA that can simulate quantum Turing machines. By this result it is affirmed that quantum cellular automata are 'computational universal', although other related questions remain unanswered. A problem mentioned by both Dürr and Watrous, concerns the simulation of QCA by quantum Turing machines. In this article we will show that every proper QCA can be simulated by a periodic quantum gate array (Theorem 2) with only linear slowdown (both space and time complexity). Because quantum circuits and quantum TMs are equivalent[22], this result solves the above problem positively.

In combination with the construction of a universal QTM [7] and the article by Watrous, this also shows that there exists a well-formed QCA that can simulate any other well-formed QCA. Still, this will *not* be considered a *universal* QCA because the time complexity of the simulation depends on the size of the QCA to be simulated. In other words: the parallel computations of the QCA are repeated in a sequential manner. With an 'intrinsically' universal CA [18] the simulation coincides with the parallel structure of the CA-model. The construction of such 'self-referring' universal automata has been shown possible in the classical case by Albert and Culik[1], and Martin[18]. In this paper we will do the same for the quantum mechanical model. This is done by constructing a QCA $\mathcal{U}$ that can mimic the behavior of any periodic quantum gate array.

2 Preliminaries

2.1 State spaces

The state space of a quantum mechanical system is embedded in a complex valued vector space $\mathbb{C}_Q$, with Q the set of canonical or 'classical' configurations. Every state $x \in \mathbb{C}_Q$ corresponds to a linear combination of those basis states and can therefore be described by:

$$x = \sum_{\xi \in Q} \alpha_\xi \, |\xi\rangle$$

with $\alpha_\xi \in \mathbb{C}$ and $|\xi\rangle$ a representation of the basis state as a member of $\mathbb{C}_Q$ for every $\xi \in Q$. The complex values α_ξ are called the *probability amplitudes* of x.

If Q is a finite set then $\mathbb{C}_Q$ can be viewed as a finite dimensional Hilbert space with its associated *inner product* $\langle\cdot,\cdot\rangle : \mathbb{C}_Q \times \mathbb{C}_Q \to \mathbb{C}$. Given two vectors x and $y \in \mathbb{C}_Q$ with amplitudes α_ξ and β_ξ, this inner product is defined by:

$$\langle x, y\rangle = \sum_{\xi \in Q} \alpha_\xi \cdot \beta^*_\xi$$

If $\langle x, y\rangle = 0$, the vectors x and y are *orthogonal*: $x \perp y$.

Another attribute of $\mathbb{C}_Q$ is the *norm* of a vector $\|\cdot\| : \mathbb{C}_Q \to \mathbb{R}$, which is defined by:

$$\|x\| = \sqrt{\langle x, x\rangle}$$

for every $x \in \mathbb{C}_Q$. A vector which represents a *valid* quantum mechanical state has norm 1. This is called the *normalization condition* on the amplitudes of x. If we apply this restriction to all the vectors of $\mathbb{C}_Q$ we get the *proper* state space:

$$\mathcal{H}_Q = \{x \mid x \in \mathbb{C}_Q \text{ and } \|x\| = 1\}$$

If the norm of a vector does not equal 1, then it is called *not proper* or *not well-formed*. From now on, only finite dimensional state spaces are considered.

2.2 Well-formed transformations

Every linear transformation U of the space $\mathbb{C}_Q$ is identified with a complex valued matrix $U \in \mathbb{C}_{|Q|\times|Q|}$. A well-formed transformation is function U which respects the normalization condition for every $x \in \mathcal{H}_Q$. This is only the case if it corresponds to a matrix with the property $U \cdot U^\dagger = U^\dagger \cdot U = I$, with I the identity matrix In other words: U has to be a *unitary* matrix. Conversely, every unitary matrix describes a proper transformation. Such finite dimensional transformations are both norm and angle preserving (and therefore bijective).

2.3 Notational conventions

In this paper we will use the well-known bracket notation supplemented with the following conventions:

repeated tensor products: Because the tensor product does not commute, we define explicitly:

$$\bigotimes_{i\in\mathbb{Z}_r} |X_i\rangle = |X_0\rangle \otimes |X_1\rangle \otimes \cdots \otimes |X_{r-1}\rangle$$

in combination with:

$$\bigotimes_{i\in\mathbb{Z}_r} |X_i\rangle = |X_0, X_1, \ldots, X_{r-1}\rangle$$

If and only if a vector can be expressed as a tensor product, we can 'access' the initial factors by:

$$\left[\bigotimes_{i\in\mathbb{Z}_r} |X_i\rangle\right]_{a:b} = |X_a\rangle \otimes \cdots \otimes |X_b\rangle$$

(Note: if $|Y\rangle$ is *not* a tensor product, the expression $[|Y\rangle]_t$ is meaningless.)

ket abbreviation: By $|x\rangle$ with $x \in Q^n$ a canonical state, we refer to the corresponding state vector as an element of $\mathcal{H}_{Q^n}$. Long ket expressions are abbreviated to:

$$|x_0, x_1, \ldots, x_n\rangle = |[x_i]_{i=0}^n\rangle$$

time evolution: For every time operator F, by

$$|X\rangle \xrightarrow{*}_F |Y\rangle$$

it is meant that there exists a $t \in \mathbb{N}$ such that $F^t|X\rangle = |Y\rangle$ (if $t = 1$ the "$*$" will be omitted).

3 Quantum CA

In this article we will only deal with one-dimensional cellular automata. The characteristic component of such automata is the local function which determines the time evolution of the configurations. If we replace the classical local function of conventional CA by its quantum mechanical equivalent, we have a definition of *quantum cellular automata*.

Definition 1 (QCA) *A quantum cellular automaton F is defined by the tuple $\langle Q, r, N, f\rangle$, where Q is the finite set of states and $N \subset \mathbb{Z}$ defines the neighborhood-scheme. The neighborhood-size is indicated by $r \in \mathbb{N}^+$, such that the neighborhood-set equals $N = \{n_1, n_2, \ldots, n_r\}$. The local function is defined by $f : Q^r \to \mathcal{H}_Q$.*

In order to avoid the pitfalls of uncountable infinite dimensional transformations, we will only define the behavior on circular bounded configurations.

For every $k \in \mathbb{N}^+$ the QCA F defines a global function F_k on the set $\mathbb{C}_{Q^k}$. By superposition we have for every $X \in \mathbb{C}_{Q^k}$:

$$F_k(X) = F_k\left(\sum_{\xi\in Q^k} \alpha_\xi \cdot |\xi\rangle\right) = \sum_{\xi\in Q^k} \alpha_\xi \cdot F_k|\xi\rangle$$

with $\alpha_\xi \in \mathbb{C}$ and $\sum_\xi$ the summation on the set of basis states. The global function on the set of canonical states is determined by the the local function and is expressed by (note that the addition "$j + n$" is in $\mathbb{Z}_k$):

$$F_k|\xi\rangle = \bigotimes_{j\in\mathbb{Z}_k} f(\xi_{j+n_1}, \xi_{j+n_2}, \ldots, \xi_{j+n_r})$$

This shows that $F_k|\xi\rangle$ is a tensor product and therefore:

$$\langle F_k|X\rangle, F_k|Y\rangle\rangle = \prod_{i\in\mathbb{Z}_k} \langle [F_k|X\rangle]_i, [F_k|Y\rangle]_i\rangle$$

for every $X, Y \in Q^k$. This is an important property if we want to decide if $F_k|X\rangle$ and $F_k|Y\rangle$ are mutually orthogonal, because this amounts to the question: $\langle F_k(X), F_k(Y)\rangle = 0$?

3.1 Well-formed QCA

If we want our QCA to make sense in a physical way, we have to investigate the 'well-formedness issue'. The laws of physics teach us that the global functions described above, have to be both norm and angle preserving. This is equivalent with the constraint on the functions F_k to be unitary.

Definition 2 (well-formed QCA) *A* QCA *F is* well-formed *if and only if for every $k \in \mathbb{N}^+$ the corresponding F_k is a unitary transformation.*

Because there is an infinite number of k to be considered this leads us to the question whether well-formedness is a decidable property or not. This is answered affirmatively by the following theorem which will be the backbone of this paper.

Theorem 1 *For every well-formed* QCA *$F = \langle Q, r, N, f\rangle$ there exist $p, q \in \mathbb{Z}$ such that for every $k \in \mathbb{N}^+$ and $X, Y \in Q^k$ with $X_0 \neq Y_0$ it holds that*

$$\prod_{i=p}^{q} \langle [F_k\,|X\rangle]_i, [F_k\,|Y\rangle]_i\rangle = 0$$

where the values p and q are bounded by

$$-|Q|^{2R} - n_1 \leq p \leq q \leq |Q|^{2R} - n_1 - 1$$

with $R = n_r - n_1 + 1$.
PROOF *See the Appendix A.1.* ∎

This local constraint on well-formed QCA resembles the so called 'inverse neighborhood' of classical reversible CA [2, 17]. As a direct result, this theorem provides us with an algorithm which determines the well-formedness of a given QCA.

Lemma 1 *The well-formedness property of a* QCA *F is decidable.*
PROOF *The proof in Appendix A.1 shows that if F is* not *well-formed there exists a $k \leq 2|Q|^{2R}$ (with $R = n_r - n_1 + 1$) such that the finite dimensional transformation F_k is not unitary. Conversely, if such a k exists then F is not well-formed. This is decidable in finite time.* ∎

The above definition of well-formedness is not equivalent with the one used by Watrous and Dürr. This is because we have used circular bounded structures instead of finite configurations. Secondly, Definition 2 also holds for QCA with no quiescent state, which are not considered by the former authors. It can been shown that our well-formedness constraint is stronger than the one used by Watrous and Dürr. To summarize:

1. Every well-formed QCA with a quiescent state is also proper according to Dürr et al.
2. Not every unitary QCA as described by Dürr et al.[14] is well-formed by our definition.

Obviously this discrepancy asks for further investigation, although it may seem more alarming than it actual is: the same differences also hold for classical injective CA [12].

3.2 QCA simulating QCA

What do we mean if make the statement: "QCA $F = \langle Q, r, N, f\rangle$ *simulates* QCA $G = \langle P, s, M, g\rangle$ *with only linear slowdown*"?

Without giving a formal definition in this article, this will mean that there exist two 'simple' injective transformations:

$$\begin{aligned} \Phi_k : Q^{ak} &\rightarrow P^{bk} \\ \Psi_k : P^{ck} &\rightarrow Q^{dk} \end{aligned}$$

with $a, b, c, d, \lambda \in \mathbb{N}^+$ such that for every $k, t \in \mathbb{N}^+$:

$$\Phi_{dk} \circ F^t_{adk} \equiv G^{\lambda t}_{bdk} \circ \Psi_{bk}$$

with "$\equiv$" denoting a shift, or translation-equivalence. The λ-parameter indicates the time complexity of the simulation, which does not depend on the size k. Conversely, the time parameter t does not influence the amount (bdk) of space required by G. Because both λ (time) and bd (space) are constants, it is said that the simulation has *linear slowdown.*

This prescription is perhaps better illustrated by the following lemma.

Lemma 2 *Every* QCA *$F = \langle Q, r, N, f\rangle$ can be simulated by a* QCA *$G = \langle Q^{\Delta}, 2, \{0, 1\}, g\rangle$ and $\Delta = n_r - n_1$.*
PROOF *First we will transform the* QCA *F to the continuous* QCA

$$F' = \langle Q, d = n_r - n_1 + 1, \{n_1, \ldots, n_r\}, f'\rangle$$

with the same behavior. This is done by defining the local function:

$$f'(q_{n_1}, q_{n_1+1}, \ldots, q_{n_r}) = f(q_{n_1}, q_{n_2}, \ldots, q_{n_r})$$

for every $q_n \in Q$. The QCA *F' is shift-equivalent with the* QCA *$G' = \langle Q, d, \{0, \ldots, d-1\}, f'\rangle$ which will be simulated by G and its local function:*

$$g(q_{1:\Delta}, q_{(\Delta+1):2\Delta}) = \big|[f'(q_{1+i}, \ldots, q_{d+i})]_{i \in \mathbb{Z}_\Delta}\big\rangle$$

for every $q_{1:\Delta}$ and $q_{(\Delta+1):2\Delta} \in Q^{\Delta}$. This completes the proof of the simulation of F by G. ∎

4 Quantum-gate CA

The well-formedness restriction on QCA resembles the reversibility constraint for classical CA. In general well-formed QCA with non-trivial behavior are rare and hard to find. In order to by-pass this problem, a sub-class of QCA is defined: *quantum gate cellular automata*. This is an extension of the partitioned quantum cellular automata, which were introduced by John Watrous.

If we replace the local functions $f : Q^r \to \mathcal{H}_Q$ by proper quantum gates $M : \mathcal{H}_{Q^n} \to \mathcal{H}_{Q^n}$, the well-formedness property holds by definition. A visualization of this idea is given in Fig. 1. Each cell is divided into n-subparts which correspond to the fan-in and fan-out of the quantum gate M.

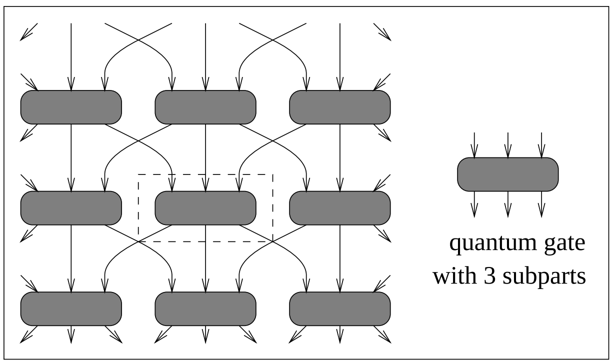

Figure 1: Example of a QGCA with fan $n = 3$.

The 'communication' between the different gates is defined by a *neighborhood-scheme* $P = \langle n, \sigma, \phi \rangle$. With this definition the subpart i of a cell j receives its information from the subpart $\sigma(i)$ of the cell $j + \phi(i)$. Formally:

Definition 3 (neighborhood-scheme) *A* neighborhood-scheme *is defined by the tuple $P = \langle n, \sigma, \phi \rangle$, with $\sigma : \mathbb{Z}_n \to \mathbb{Z}_n$ and $\phi : \mathbb{Z}_n \to \mathbb{Z}$. The function σ is bijective.*

The neighborhood-scheme of Fig. 1 is therefore described by:

$$\begin{array}{rclcrcr} \sigma(0) & = & 2 & & \phi(0) & = & -1 \\ \sigma(1) & = & 1 & \text{and} & \phi(1) & = & 0 \\ \sigma(2) & = & 0 & & \phi(2) & = & 1 \end{array}$$

We are now ssufficiently equipped for the definition of *quantum gate cellular automata:*

Definition 4 (QGCA) *A* QGCA *F is defined by the tuple $\langle Q, n, M, P \rangle$, with Q a state-set, M a proper quantum-gate with fan n which operates on $\mathcal{H}_{Q^n}$ and the neighborhood-scheme $P = \langle n, \sigma, \phi \rangle$.*

If x_j^i denotes the i-th subpart of cell x_j, the behavior F_k of such a QGCA is described by:

$$\begin{aligned} F_k(X) &= M^{[k]} \cdot P\left(\bigotimes_{j\in\mathbb{Z}_k}\left(\bigotimes_{i\in\mathbb{Z}_n} x_j^i\right)\right) \\ &= \bigotimes_{j\in\mathbb{Z}_k} M\left(\bigotimes_{i\in\mathbb{Z}_n} x_{j+\phi(i)}^{\sigma(i)}\right) \end{aligned}$$

for every $k \in \mathbb{N}^+$. The following lemma shows us that every QGCA can be identified with a well-formed QCA.

Lemma 3 *Every* QGCA *$G = \langle Q, n, M, P \rangle$ is equivalent with a well-formed* QCA *$F = \langle Q^n, r, N, f \rangle$.*

PROOF *The 'mapping' of the values between G and F is done by: $x_j = x_j^0 \otimes \cdots \otimes x_j^{n-1}$. The neighborhood-scheme $P = \langle n, \sigma, \phi \rangle$ gives us the neighborhood-set of F according to: $N = \{\phi(i) \mid i \in \mathbb{Z}_n\}$ and consequently $r = |N|$. The definition of F is completed with the local function $f : (Q^n)^r \to \mathcal{H}_{Q^n}$ which obeys*

$$f(x_{n_0}, \ldots, x_{n_{r-1}}) = M\left(\bigotimes_{i\in\mathbb{Z}_n} x_{\phi(i)}^{\sigma(i)}\right)$$

for every $x \in (Q^n)^r$. By this construction it holds for every $k \in \mathbb{N}^+$ that:

$$\begin{aligned} G_k\left(\bigotimes_{j\in\mathbb{Z}_k}\left(\bigotimes_{i\in\mathbb{Z}_n} x_j^i\right)\right) &= \bigotimes_{j\in\mathbb{Z}_k}\left(M\left(\bigotimes_{i\in\mathbb{Z}_n} x_{j+\phi(i)}^{\sigma(i)}\right)\right) \\ &= \bigotimes_{j\in\mathbb{Z}_k} f(x_{j+n_0}, \ldots, x_{j+n_{r-1}}) \\ &= F_k\left(\bigotimes_{j\in\mathbb{Z}_k} x_j\right) \end{aligned}$$

∎

The *Shift neighborhood-scheme* plays an important part in the following sections and will always be denoted by S. Its behavior is defined for every $k, n \in \mathbb{N}^+$ by:

$$S\left|x_0^0, x_0^1, \ldots, x_{k-1}^{n-1}\right\rangle = \left|x_0^1, \ldots, x_{k-1}^{n-1}, x_0^0\right\rangle$$

The neighborhood-schemes S^2, S^{-1} et cetera are defined in a similar way..

4.1 Periodic-QGCA

If we replace the identical layers of a QGCA by a periodic pattern of layers, we get a more flexible model which will be called *periodic*-QGCA.

Definition 5 (periodic-QGCA) *A periodic*-QGCA *F is defined by the tuple*

$$\langle Q, n, \mu, M_0, \ldots, M_{\mu-1}, P_0, \ldots, P_{\mu-1} \rangle$$

with M_i proper quantum gates and P_i proper neighborhood- schemes for every $0 \le i < \mu \in \mathbb{N}^+$.

The unitary operator of the first μ layers of this automaton is described by:

$$F_k \quad = \quad \prod_{i=\mu-1}^{0} \left(M_i^{[k]} \cdot P_i \right)$$

(Notice the order of the index i and the fact that F_k is defined as the operator of *several* layers.)

Lemma 4 *Every periodic* QGCA G *can be simulated by a periodic* QGCA $\langle \{0,1\}, n, \lambda, M_0, \ldots, M_{\lambda-1}, S, \ldots, S \rangle$ *which only uses the Shift neighborhood-scheme. The 'extra costs' of this simulation are linear both in space and time complexity.*

PROOF *After converting the periodic-*QGCA G *to a periodic-*QGCA *with state set* $\{0,1\}$*, we will have to simulate the various neighborhood-schemes. This can be done by 'inserting' layers that will have the same behavior (except for a horizontal shift). An explicit proof of this lemma is omitted in this extended abstract.* ∎

We are now able to return to the class of plain QGCA by applying the following lemma.

Lemma 5 *Every periodic-*QGCA

$$F = \langle \{0,1\}, n, \lambda, M_0, \ldots, M_{\lambda-1}, S, \ldots, S \rangle$$

can be simulated by a QGCA $G = \langle \{0,1\}, n+\Delta, M', S \rangle$ *with* $\Delta = \lceil \log_2(\lambda) \rceil$.

PROOF *The additional* Δ *bits are used by the* M' *gates to calculate the index* i *of the different* M_i *gates. With* $\phi : \mathbb{Z}_\lambda \rightarrow \{0,1\}^\Delta$ *an injective function, the behavior of* M' *is described by:*

$$\begin{aligned} &M' \left| x_0, \ldots, x_{n-2}, \phi(t), x_{n-1} \right\rangle \\ &\qquad = M_t \left| x_0, \ldots, x_{n-1} \right\rangle \otimes \left| \phi(t+1) \right\rangle \end{aligned}$$

for every $t \in \mathbb{Z}_\lambda$ *and* $x_i \in \{0,1\}$.

As a result, if the behavior of F_k *is characterized by*

$$F_k \left| \left[X_j^0, \ldots, X_j^{n-1} \right]_{j \in \mathbb{Z}_k} \right\rangle \quad = \quad \left| \left[Y_j^0, \ldots, Y_j^{n-1} \right]_{j \in \mathbb{Z}_k} \right\rangle$$

with $X_j^i \in \{0,1\}$*, then also:*

$$\begin{aligned} &G_k^\lambda \left| \left[X_j^0, \ldots, X_j^{n-1}, \phi(0) \right]_{j \in \mathbb{Z}_k} \right\rangle \\ &\qquad = \left| \left[Y_j^0, \ldots, Y_j^{n-1}, \phi(0) \right]_{j \in \mathbb{Z}_k} \right\rangle \end{aligned}$$

which certifies the simulation of F *by* G. ∎

The 'value' of periodic-QGCA is shown by the following lemma which uses the local constraint of well-formed QCA in combination with the more flexible characteristics (in comparison with plain QGCA) of periodic-QGCA.

Lemma 6 *Every well-formed* QCA F *can be simulated by a periodic-*QGCA G.

PROOF *This proof will be restricted to the* QCA $F = \langle Q, 2, \{0,1\}, f \rangle$ *(see Lemma 2). The behavior of the* QCA F *is therefore described by the equalities*

$$X_i \in Q \quad \text{and} \quad Y_i = f(X_i, X_{i+1})$$

for every i*. By Theorem 1 there exists an 'inverse neighborhood' of* F *bounded by* $p \leq 0 < q$*. These values determine the fan* $2r$ *of the three gates involved, with* $r = q - p + 1$*. The first two we will use are described by:*

$$A \left| \left[x_j, x_j \right]_{j \in \mathbb{Z}_r} \right\rangle \quad = \quad \left| \left[x_j, y_j \right]_{j \in \mathbb{Z}_{r-1}} ; x_{r-1}, x_{r-1} \right\rangle$$

$$\begin{aligned} &\text{and } B \left| \left[x_j, y_j \right]_{j \in \mathbb{Z}_{r-2}} ; x_{r-2}, x_{r-2}, x_{r-1}, y_{r-1} \right\rangle \\ &\qquad = \left| \left[x_j, y_j \right]_{j \in \mathbb{Z}_r} \right\rangle \end{aligned}$$

for every $x_i \in Q$ *and* $y_i = f(x_i, x_{i+1})$*. Because no information (regarding the* x*-values) is lost, these gates are reversible and therefore proper.*

The behavior of the C*-gate is more complex and defined by:*

$$\begin{aligned} &C \left| \left[z_j, y_j \right]_{j \in \mathbb{Z}_{-p}} ; x_{-p}, y_{-p} ; \left[z_j, y_j \right]_{j=-p+1}^{r-1} \right\rangle \\ &\qquad = \left| \left[z_j, y_j \right]_{j \in \mathbb{Z}_{-p}} ; y_{-p}, y_{-p} ; \left[z_j, y_j \right]_{j=-p+1}^{r-1} \right\rangle \end{aligned}$$

for every $x_i \in Q, y_i = f(x_i, x_{i+1})$ *and* $z_j \in \{x_j, y_j\}$*. The proper reversibility of this gate is assured by the values of* p *and* q *in combination with Theorem 1. Note that we do not 'clone' the* y *qubit. If* $|y\rangle = \alpha|0\rangle + \beta|1\rangle$*, the* $|y,y\rangle$ *expression stands for:* $|y,y\rangle = \alpha|0,0\rangle + \beta|1,1\rangle$.

*We are now ready to define the periodic-*QGCA G *by the tuple (with* I *the 'identity neighborhood-scheme'):*

$$\langle Q, 2r, r+2, A, B, C, \ldots, C, I, S^2, S^{2(r-2)}, S^2, \ldots, S^2 \rangle$$

For every $k \in \mathbb{N}^+$*, the function* F_{kr} *will be simulated by* G_{2kr}*. This is confirmed by the evolution of the* G_{2kr} *operator, which starts with the initial configuration:*

$$\left| \left[X_j, X_j \right]_{j \in \mathbb{Z}_{kr}} \right\rangle$$

First the two A *and* B *layers calculate the* Y *values, without removing the old information ...*

$$\longrightarrow_{S_k^{2(r-3)} \cdot B^{[k]} \cdot S_k^2 \cdot A^{[k]} \cdot I_k} \quad \left| \left[X_{r-2+j}, Y_{r-2+j} \right]_{j \in \mathbb{Z}_{kr}} \right\rangle$$

after which the sequence (size r*) of* C *layers replaces every* X *by the new* Y *values:*

$$\stackrel{*}{\longrightarrow}_{C^{[k]} \cdot S_k^2} \quad \left| \left[Y_j, Y_j \right]_{j \in \mathbb{Z}_{kr}} \right\rangle$$

This completes the simulation of F_{kr}. ∎

With the preceding lemmas we can reduce the QCA-model to the theory of QGCA.

Theorem 2 *Every well-formed* QCA *can be simulated by a* QGCA $\langle\{0,1\},n,M,S\rangle$ *with linear slowdown (time and space-complexity).*
PROOF *Combine the results of Lemma 6, Lemma 4 and Lemma 5.* ∎

Because the QGCA G in the above proof uses a binary state set, we have made a connection between QCA and quantum gate arrays. This is analogous to the result which states that every proper quantum Turing machine can be simulated by quantum gate arrays and vice-versa[22]. We therefore can answer the following question posed by Dürr et al. and Watrous (although we have to keep in mind the discrepancy mentioned in §3.1).

Lemma 7 *Every well-formed* QCA F *can be simulated by a quantum Turing machine* T.
PROOF *Construct a* QTM T *which simulates the corresponding* QGCA G *(see Theorem 2) of the initial* QCA F. ∎

By the existence of a QCA which simulates a universal QTM [21], this lemma shows us that there is a QCA which is able of simulating any other well-formed QCA. Nevertheless this will *not* be considered a universal QCA because the time complexity of the simulation depends on the size k of the QCA to be simulated. If we want a genuine universal automaton, we have to pay justice to the parallel structure of cellular automata.

In the next section it will be shown that this possible by using some well-known theorems about quantum-gate arrays.

5 A universal QCA

5.1 Universal gates

In a sequence of articles[3, 4, 10, 11] it has been shown that there exists a universal two bit quantum gate U. By 'universal' is meant that any finite-dimensional unitary operator M can be simulated (with a bounded error ε) by an array which uses a finite number of U-gates and no other. This 'not perfect'-simulation is inevitable because there is an uncountable number of possible unitary transformations. The bounded error method assures us that -although perfection is not possible- for any $\varepsilon > 0$ we can design a unitary transformation M' with $\|M - M'\| \leq \varepsilon$.

The same considerations hold for a potential universal quantum cellular automaton. Because every QCA can be simulated by a QGCA with state set $\{0,1\}$, it suffices to construct a QCA $\mathcal{U}$ which can simulate every QGCA with a bounded error. It will be of no surprise that this simulation makes extensive use of the universal gate U.

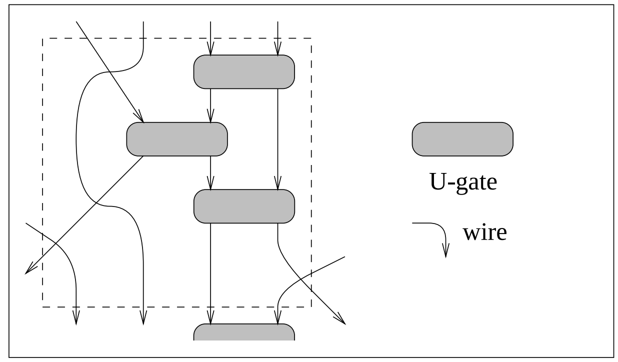

Figure 2: Part of a U-gate array which simulates a QGCA.

5.2 Periodic U-gate arrays

For every QGCA G with gate M, there exists a U-gate array which approximates the behavior of G with a bounded error. Because of the isomorphic structure of QGCA, this U-gate array will also be periodic in both dimensions, therefore the term *periodic U-gate arrays* will be used. Fig. 2 shows us a possible simulation of the QGCA of Fig. 1 (note the additional work bit in the gate-array). In order to translate the 'wiring' of this array, another model will be introduced.

5.3 Uniform U-gate arrays

We proceed by defining two gates I and X that will mimic the wiring of a gate-array. The gate I corresponds with the two-qubit identity gate, whereas X describes a cross-over:

$$I\,|x,y\rangle \;=\; |x,y\rangle \quad\text{and}\quad X\,|x,y\rangle \;=\; |y,x\rangle$$

for every $x, y \in \{0,1\}$. By combining the I, X and U-gates in a wall-like, periodic structure, we can mimic any periodic U-gate array. An example of this is shown in Fig. 3.

To describe these structures we use the following definition:

Definition 6 (uniform U-gate array) *A uniform U-gate array F is defined by the tuple $\langle m,n,A^i_j,B^i_j\rangle$ with $A^i_j, B^i_j \in \{I,X,U\}$ for every $j \in \mathbb{Z}_m$ and $i \in \mathbb{Z}_n$.*

For every $k \in \mathbb{N}^+$ the transformation F_{2mk} (after $2n$ layers) is described by the function

$$\prod_{i=n-1}^{0}\left[S^\dagger \cdot \left(\bigotimes_{j\in\mathbb{Z}_{mk}} B^i_{j \bmod m}\right)\cdot S\cdot\left(\bigotimes_{j\in\mathbb{Z}_{mk}} A^i_{j \bmod m}\right)\right]$$

Without going into full detail we can safely state the following lemma

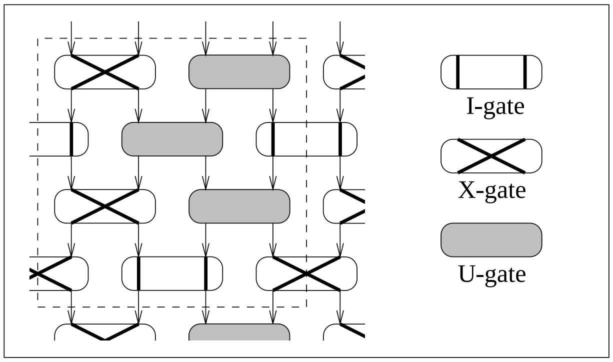

Figure 3: Example of a uniform U-gate array. The indicated area mimics the U-gate array of Fig. 2.

Lemma 8 *For every* QGCA $G = \langle\{0,1\}, n, M, S\rangle$ *there exists a uniform U-gate array $G = \langle n, m, A^i_j, B^i_j\rangle$ (with* $\gcd(m,n) = 1$*) which simulates G. This simulation is within an arbitrary small error.*

PROOF *Use the above described transformation from* QGCA *to periodic U-gate arrays to uniform U-gate arrays. The* $\gcd(m,n) = 1$ *constraint is satisfied by adding a sufficient number of identity-layers which only consist of I-gates, thereby increasing the value of n until the desired number is reached.* ∎

If we express the cell values of the uniform U-gate array at time t by $\left|x^t_0, y^t_0, \ldots, x^t_{km-1}, y^t_{km-1}\right\rangle$, the behavior of the U-gate array is expressed by the equations:

$$\begin{aligned} A^{i \bmod n}_{j \bmod m} \left|x^{2i}_j, y^{2i}_j\right\rangle &= \left|x^{2i+1}_j, y^{2i+1}_j\right\rangle \\ B^{i \bmod n}_{j \bmod m} \left|y^{2i+1}_j, x^{2i+1}_{j+1}\right\rangle &= \left|y^{2i+2}_j, x^{2i+2}_{j+1}\right\rangle \end{aligned} \quad (1)$$

for every $i \in \mathbb{N}$ and $j \in \mathbb{Z}_{km}$. We will use this 'calibration' to prove that the universal automaton $\mathcal{U}$ embeds the same behavior.

5.4 The $\mathcal{U}$ automaton

The universal quantum cellular automaton $\mathcal{U}$ is described by the following definition (an explanation of its semantics will be given below):

Definition 7 ($\mathcal{U}$ automaton) *The $\mathcal{U}$ automaton is a* QGCA $\langle Q, n, M, P\rangle$ *with:*

state set $Q = \{0, 1, \lhd, \_, \ulcorner I \urcorner, \ulcorner X \urcorner, \ulcorner U \urcorner\}$ *and* $n = 4$

quantum gate $M : \mathcal{H}_{Q^4} \to \mathcal{H}_{Q^4}$ *that obeys:*

$$\begin{aligned} M\left|\_, \_, \ulcorner A \urcorner, \_\right\rangle &= \left|\_, \_, \ulcorner A \urcorner, \_\right\rangle \\ M\left|\_, x, \ulcorner A \urcorner, \_\right\rangle &= \left|\_, x, \ulcorner A \urcorner, \_\right\rangle \\ M\left|\_, \_, \ulcorner A \urcorner, x\right\rangle &= \left|x, \_, \ulcorner A \urcorner, \_\right\rangle \\ M\left|\_, \_, \ulcorner A \urcorner, \lhd\right\rangle &= \left|\lhd, \_, \ulcorner A \urcorner, \_\right\rangle \\ M\left|x, \_, \ulcorner A \urcorner, \lhd\right\rangle &= \left|\lhd, x, \ulcorner A \urcorner, \_\right\rangle \\ M\left|\_, x, \ulcorner A \urcorner, y\right\rangle &= \left|x', \_, \ulcorner A \urcorner, y'\right\rangle \end{aligned}$$

for every $x, y \in \{0,1\}$, $A \in \{I, X, U\}$ and

$$A\left|x, y\right\rangle = \left|x', y'\right\rangle$$

neighborhood-scheme $P = \langle n, \sigma, \phi\rangle$ *defined by*

$$\begin{aligned} \sigma(0) &= 3 & \phi(0) &= -1 \\ \sigma(1) &= 1 & \phi(1) &= 0 \\ \sigma(2) &= 2 & \phi(2) &= 0 \\ \sigma(3) &= 0 & \phi(3) &= 1 \end{aligned}$$

(End of definition.)

If we supply this automaton with the appropriate input, it will simulate a uniform U-gate array. More specifically:

For every $N, K \in \mathbb{N}^+$ the input:

$$\left|\left[\_x^0_J\pi^0_J\_, y^0_J\_\pi^1_J\_, \_\_\pi^2_J\_, \lhd\ \_\pi^3_J\_, \left[\_\_\pi^i_J\_\right]^{2N-1}_{i=4}\right]_{J\in\mathbb{Z}_K}\right\rangle$$

with $\pi \in \{\ulcorner I \urcorner, \ulcorner X \urcorner, \ulcorner U \urcorner\}$ and $x, y \in \{0,1\}$, will evolve after two layers of $\mathcal{U}_{2NK}$ to the configuration:

$$\left|\left[\_\_\pi^0_J\_, \lhd\ y^1_J\pi^1_J\_, \left[\_\_\pi^i_J\_\right]^{2N-2}_{i=2}, x^1_{J+1}\_\pi^{2N-1}_J\_\right]_{J\in\mathbb{Z}_K}\right\rangle$$

with $\Pi^0_J \left|x^0_J, y^0_J\right\rangle = \left|x^1_J, x^1_J\right\rangle$ (the gate Π is determined by $\pi^0_J = \ulcorner \Pi^0_J \urcorner$). At this point the x-values will travel step-by-step to the left, while the y-values have moved one place to the right and are now stationary (this is established by the "$\lhd$"-symbol).

The next important situation occurs (after $\Theta(N)$ layers) when the x and y values 'meet again' at the π^1_J gates, which are then to be simulated. This will result in the configuration:

$$\left|\left[y^2_J\_\pi^0_J\_, \_\_\pi^1_J\_, \lhd\ x^2_{J+1}\pi^2_J\_, \left[\_\_\pi^i_J\_\right]^{2N-1}_{i=2}\right]_{J\in\mathbb{Z}_K}\right\rangle$$

with $\Pi^1_J \left|y^1_J, x^1_{J+1}\right\rangle = \left|y^2_J, x^2_{J+1}\right\rangle$ and $\pi^1_J = \ulcorner \Pi^1_J \urcorner$.

By now the y-values go left in order to collide at the π^2_J gates with the x-variables. This process will be repeated in the obvious way.

A careful examination of the behavior of $\mathcal{U}_{2NK}$ on this input reveals that the overall time evolution is calibrated by the equations:

$$\begin{aligned} \Pi^{2i \bmod 2N}_{J+\lfloor\frac{2i}{2N}\rfloor \bmod K} \left|x^{2i}_{J+i}, y^{2i}_{J+i}\right\rangle &= \left|x^{2i+1}_{J+i}, y^{2i+1}_{J+i}\right\rangle \\ \Pi^{2i+1 \bmod 2N}_{J+\lfloor\frac{2i+1}{2N}\rfloor \bmod K} \left|y^{2i+1}_{J+i}, x^{2i+1}_{J+i+1}\right\rangle &= \left|y^{2i+2}_{J+i}, y^{2i+2}_{J+i+1}\right\rangle \end{aligned} \quad (2)$$

for every $i \in \mathbb{N}$, $J \in \mathbb{Z}_K$, and $\pi^{\cdot}_{\cdot} = \ulcorner \Pi^{\cdot}_{\cdot} \urcorner$.

By using the calibrations (1) and (2) we can prove the following lemma.

Lemma 9 *Every uniform U-gate array $F = \langle m, n, A^i_j, B^i_j \rangle$ with $\gcd(m,n) = 1$ can be simulated by the* QGCA $\mathcal{U}$. *The time complexity of the simulation is linear and does not depend on the size k of the U-gate array F_{2mk}.*

PROOF *If a 'mapping' between the two calibrations is possible, it follows that the two automata have the same evolution. Because $\gcd(m,n) = 1$, there exists a positive integer α such that $\alpha n \bmod m = 1$. With $N = \alpha n$ and $K = km$ every F_{2mk} can be simulated by $\mathcal{U}_{2NK}$. This is shown by the existence of a mapping which satisfies (assuming $J = j - i$):*

$$\begin{aligned} A^{i \bmod n}_{j \bmod m} &= \Pi^{2i \bmod 2N}_{j-i+\lfloor \frac{2i}{2N} \rfloor \bmod K} \\ B^{i \bmod n}_{j \bmod m} &= \Pi^{2i+1 \bmod 2N}_{j-i+\lfloor \frac{2i+1}{2N} \rfloor \bmod K} \end{aligned}$$

for every $i \in \mathbb{N}$ and $j \in \mathbb{Z}$. Appendix A.2 proves the possibility of such a mapping. Because α does not depend on k, the time complexity is bounded by $\Theta(Ni) = \Theta(i)$ for the simulation of $2i$ layers of F. ∎

With this lemma we have removed the last obstacle between Theorem 1 and the final conclusion of this article.

Theorem 3 *There exists a proper universal quantum cellular automaton $\mathcal{U}$ which can simulate any well-formed* QCA *F with a bounded error. The extra costs of the simulation of F^t_k has time complexity $\Theta(t)$ and space-complexity $\Theta(k)$.*

PROOF *This follows from the results of Theorem 2, Lemma 8 and Lemma 9.* ∎

Because the classical reversible cellular automata (RCA) are a subset of QCA, we also know that every RCA can be simulated by the *non-classical* $\mathcal{U}$-automaton. If we want a universal RCA, we have to adapt Definition 7 in such a way that it uses a universal *three-bit* gate (the Toffoli-gate for example). This is because there does not exist a classical two-bit gate U that is universal in its computational power[3, 4, 10, 11]. The author is unknown of an earlier construction of such an automaton.

5.5 Conclusions

We have defined a class of well-formed quantum cellular automata which are one-dimensional and circular bounded. It has been shown that every proper QCA resembles a periodic quantum gate array. There exists a QCA $\mathcal{U}$ which can simulate any such array (by using a universal two-qubit gate U). The time complexity of this simulation does not depend on the size k of the initial QCA. This proves that $\mathcal{U}$ is a *universal quantum cellular automaton.*

Acknowledgements

Among the people I wish to thank are Paul Vitányi for his experienced guidance and interest, Andre Berthiaume for giving me a 'first-hand' introduction to the area of quantum computing and Kees Koster for his critical remarks on some earlier versions of this paper. Adriano Barenco pointed out an indistinctness in a former lemma.

Also the hospitality of Christophe Dürr and Huong Lê Thanh should be mentioned, it made an inspiring visit to Paris possible in the summer of '95.

A Appendices

A.1 Proving Theorem 1

This theorem will be proven by contradiction. Without loss of generality we assume the existence of leqa QCA $F = \langle Q, r, \{0, 1, \ldots, r-1\}, f \rangle$ in combination with a value $K \in \mathbb{N}^+$ and $X, Y \in Q^K$ with $X_0 \neq Y_0$, such that for every $-|Q|^{2r} \leq i \leq |Q|^{2r} - 1$ we have

$$\langle [F_K \, |X\rangle]_i, [F_K \, |Y\rangle]_i \rangle \neq 0 \tag{3}$$

We will now prove that, given these X and Y, we are able to construct a $k \in \mathbb{N}^+$ and a $X', Y' \in Q^k$, with $|X'\rangle \perp |Y'\rangle$ but yet $F_k \, |X'\rangle \not\perp F_k \, |Y'\rangle$.

Take a, b, c and d (with $a < b \leq 0 \leq c < d$), such that:

$$\begin{aligned} X_{a:(a+r-1)} &= X_{b:(b+r-1)} & \quad Y_{a:(a+r-1)} &= Y_{b:(b+r-1)} \\ X_{c:(c+r-1)} &= X_{d:(d+r-1)} & \quad Y_{c:(c+r-1)} &= Y_{d:(d+r-1)} \end{aligned}$$

Because there are 'only' $|Q|^{2r}$ different combinations of $[X_{i:(i+r-1)}; Y_{i:(i+r-1)}]$, this is always possible for

$$-|Q|^{2r} \; a < b \leq 0 \leq c < d \leq |Q|^{2r}$$

With these values we define:

$$\begin{aligned} X_L &= X_{a:(b-1)} & \quad X_R &= X_{c:(d-1)} \\ Y_L &= Y_{a:(b-1)} & \quad Y_R &= Y_{c:(d-1)} \end{aligned}$$

Now we can distinguish the following three possibilities:

1. $X_L \neq Y_L$: Take $X' = X_L$, $Y' = Y_L$ both elements of Q^k with $k = b - a$ (thus $|X'\rangle \perp |Y'\rangle$). We now have

$$X'_{k:(k+r-1)} = X_{(a+k):(a+k+r-1)}$$

and therefore

$$\begin{aligned} F_k \, |X'\rangle &= \bigotimes_{j \in \mathbb{Z}_k} f\left(\bigotimes_{i \in \mathbb{Z}_r} X'_{j+i} \right) \\ &= \bigotimes_{j \in \mathbb{Z}_k} f\left(\bigotimes_{i \in \mathbb{Z}_r} X_{a+j+i} \right) \\ &= [F_K \, |X\rangle]_{a:(b-1)} \end{aligned}$$

For the same reasons also

$$F_k\left|Y'\right\rangle \quad = \quad [F_K\left|Y\right\rangle]_{a:(b-1)}$$

which leads to:

$$\langle F_k\left|X'\right\rangle, F_k\left|Y'\right\rangle\rangle \quad = \quad \prod_{i=a}^{b-1}\langle[F_K\left|X\right\rangle]_i, [F\left|Y\right\rangle]_i\rangle$$

By equation (3) we now know that $F_k\left|X'\right\rangle \not\perp F_k\left|Y'\right\rangle$, which proves that F_k is not a unitary transformation. This contradicts the assumed well-formedness of F.

2. $X_R \neq Y_R$: With $X' = X_R$, $Y' = Y_R$ and $k = d - c$, the same reasoning as with $X_L \neq Y_L$ holds.

3. $X_L = Y_L$ and $X_R = Y_R$: First we will prove $X_{a:(b+r-1)} = Y_{a:(b+r-1)}$. We already know $X_{a:(b-1)} = Y_{a:(b-1)}$. With induction (given $0 \leq i \leq r-1$ and $X_{a:(b+i-1)} = Y_{a:(b+i-1)}$) it follows that $X_{b+i} = X_{a+i} = Y_{a+i} = Y_{b+i}$ holds. Likewise we can prove: $X_{c:(d+r-1)} = Y_{c:(d+r-1)}$.

   Now we take $X' = X_{b:(c+r-1)}$ and $Y' = Y_{b:(c+r-1)} \in Q^k$, with $k = c + r - b$. Because $b \leq 0 \leq c + r - 1$ and $X_0 \neq Y_0$, we have $X' \perp Y'$. In addition we also know that:

$$\begin{aligned} & X'_{(c-b):(k-1)} = Y_{c:(k+b-1)} \\ \text{and} \quad & X'_{k:(k+r-2)} = Y_{b:(b+r-2)} \end{aligned}$$

   This can be summarized by:

$$X'_{(c-b):(k+r-2)} = Y'_{(c-b):(k+r-2)}$$

   which gives us:

$$\begin{aligned} F_k\left|X'\right\rangle &= [F_k\left|X'\right\rangle]_{0:(c-b-1)} \otimes [F_k\left|X'\right\rangle]_{(c-b):(k-1)} \\ &= [F_K\left|X\right\rangle]_{b:(c-1)} \otimes [F_K\left|Y'\right\rangle]_{(c-b):(k-1)} \end{aligned}$$

   If we combine this 'tail equality' with:

$$F_k\left|Y'\right\rangle \quad = \quad [F_K\left|Y\right\rangle]_{b:(c-1)} \otimes [F_K\left|Y'\right\rangle]_{(c-b):(k-1)}$$

   it follows that the inner-product of $F_k\left|X'\right\rangle$ and $F_k\left|Y'\right\rangle$ equals:

$$\langle F_k\left|X'\right\rangle, F_k\left|Y'\right\rangle\rangle \quad = \quad \prod_{i=b}^{c-1}\langle[F_K\left|X\right\rangle]_i, [F_K\left|Y\right\rangle]_i\rangle$$

   Again, equation (3) shows us that $F_k\left|X'\right\rangle \not\perp F_k\left|Y'\right\rangle$, which proves F not to be a well-formed QCA.

Because 1, 2 and 3 cover all possibilities, we have proven that the QCA F is not a well-formed. This contradicts the initial assumptions.

A.2 Mapping the calibrations

In order to ensure a correct mapping between the A^i_j gates and the π-indices of the $\mathcal{U}_{2NK}$ automaton, we have to prove that if:

$$\begin{aligned} 2i \bmod 2N &\equiv 2p \bmod 2N \\ j - i + \left\lfloor \frac{2i}{2N} \right\rfloor \bmod K &\equiv q - p + \left\lfloor \frac{2p}{2N} \right\rfloor \bmod K \end{aligned}$$

then:

$$\begin{aligned} i \bmod n &\equiv p \bmod n \\ j \bmod m &\equiv q \bmod m \end{aligned}$$

for every $i, p \in \mathbb{N}$ and $j, q \in \mathbb{Z}$.

By defining $K = km$ and $N = \alpha n \equiv 1 \bmod m$, the initial conditions can be restated to:

$$\begin{aligned} 2(i-p) \bmod 2\alpha n &\equiv 0 \\ (j-q) - (i-p) + \left\lfloor \frac{2i}{2\alpha n} \right\rfloor - \left\lfloor \frac{2p}{2\alpha n} \right\rfloor \bmod km &\equiv 0 \end{aligned}$$

The first restriction leads to $p = i + \lambda\alpha n$ (with $\lambda \in \mathbb{Z}$). As a result the second restriction becomes:

$$(j-q) + \lambda(\alpha n - 1) \bmod km \quad \equiv \quad 0$$

which proves the

$$j \bmod m \quad \equiv \quad q \bmod m$$

equation.

The same reasoning holds if we want to prove the existence of a consistent mapping between the B^i_j gates and the π-indices. This completes the proof of Lemma 9.

References

[1] Albert, Jürgen, and Karel Culik II, *A Simple Universal Cellular Automaton and its One-Way and Totalistic Version,* Complex Systems **1** (1987), 1–16.

[2] Amoroso, Serafino, and Yale N. Patt, *Decision Procedures for Surjectivity and Injectivity of Parallel Maps for Tessellation Structures,* Journal of Computer and System Sciences **6** (1972), 448–464.

[3] Barenco, Adriano, *A Universal Two-Bit Gate for Quantum Computation,* Proceedings of the Royal Society of London A **449** (1995), 679–683.

[4] Barenco, Adriano, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John Smolin, and Harald Weinfurter, *Elementary gates for quantum computation,* Physical Review A **52(5)** (1995) 3457–3467.

[5] Benioff, Paul, *Quantum mechanical Hamiltonian models of Turing machines,* Journal of Statistical Physics **29** (1982), 515–546.

[6] Bennett, Charles H., *Logical reversibility of computation*, IBM Journal of Research and Development **17** (1973), 525–532.

[7] Bernstein, Ethan, and Umesh Vazirani, *Quantum Complexity Theory*, Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing (1993), 11–20.

[8] Berthiaume, Andre, *Quantum Computation*, to appear in Complexity Theory Retrospective II, Springer–Verlag (1996).

[9] Deutsch, David, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proceedings of the Royal Society of London A **400** (1985), 97–117.

[10] Deutsch, David, *Quantum computational networks*, Proceedings of the Royal Society of London A **425** (1989), 73–90.

[11] DiVincenzo, David P., *Two-bit gates are universal for quantum computation*, Physical Review A **51(2)** (1995), 1015–1022.

[12] Durand, Bruno, *Automates cellulaires: réversibilité et complexité*, thesis l'Ecole Normale Supérieure de Lyon (1984), or `http://alife.santafe.edu/alife/topics/cas/ca-faq/durand/durand.html`.

[13] Dürr, Christoph, Huong Lê Thanh, and Miklos Santha, *A decision procedure for well-formed quantum linear cellular automata*, Proceedings of the 13th Annual Symposium on Theoretical Aspects of Computer Science (1996), 281–292.

[14] Dürr, Christoph, and Miklos Santha, *A decision procedure for unitary linear quantum cellular automata*, `http://xxx.lanl.gov/abs/quant-ph/9604007`, to appear.

[15] Feynman, Richard, *Simulating Physics with Computers*, International Journal of Theoretical Physics **21** (1982), 467–488.

[16] Feynman, Richard, *Quantum Mechanical Computers*, Optic News **11** (1985), 11–29.

[17] Kari, Jarkko, On the Inverse Neighborhoods of Reversible Cellular Automata, *Lindenmayer Systems: Impacts on theoretical Computer Graphics, and Developmental Biology* (Grzegorz Rozenberg, and Arto Salomaa ed.), Springer-Verlag (1992), 477–495.

[18] Martin, Bruno, *A universal cellular automaton in quasi-linear time and its S–m–n form*, Theoretical Computer Science **123** (1994), 199–237.

[19] Morita, Kenichi, and Masateru Harao, *Computation Universality of One-Dimensional Reversible (Injective) Cellular Automata*, Transactions IEICE Japan **E72** (1989), 758–762.

[20] Morita, Kenichi, *Computation-universality of one-dimensional one-way reversible cellular automata*, Information Processing Letters **42** (1992), 325–329.

[21] Watrous, John, *On One-Dimensional Quantum Cellular Automata*, Proceedings of the 36th Annual Symposium on Foundations of Computer Science (1995), 528–537.

[22] Yao, Andrew Chi–Chih, *Quantum Circuit Complexity*, Proceedings of the 34th Annual Symposium on Foundations of Computer Science (1993), 352–361.