九州大学学術情報リポジトリ
Kyushu University Institutional Repository

Generalized Partitioned Quantum Cellular Automata and Quantization of Classical CA

Inokuchi, Shuichi
Faculty of Mathematics, Kyushu University

Mizoguchi, Yoshihiro
Faculty of Mathematics, Kyushu University

https://hdl.handle.net/2324/11845

出版情報：International journal of unconventional computing. 1 (2), pp.149-160, 2005. Old City Publishing
バージョン：
権利関係：

MHF Preprint Series

Kyushu University
21st Century COE Program
Development of Dynamic Mathematics with High Functionality

Generalized partitioned quantum cellular automata and quantization of classical CA

S. Inokuchi & Y. Mizoguchi

MHF 2004-30

(Received November 1, 2004)

Faculty of Mathematics
Kyushu University
Fukuoka, JAPAN

Generalized Partitioned Quantum Cellular Automata and Quantization of Classical CA

Shuichi INOKUCHI* Yoshihiro MIZOGUCHI†

Abstract

In this paper, in order to investigate natural transformations from discrete CA to QCA, we introduce a formulation of finite cyclic QCA and generalized notion of partitioned QCA. According to the formulations, we demonstrate the condition of local transition functions, which induce a global transition of well-formed QCA. Following the results, extending a natural correspondence of classical cells and quantum cells to the correspondence of classical CA and QCA, we have the condition of classical CA such that CA generated by quantization of its cells is well-formed QCA. Finally we report some results of computer simulations of quantization of classical CA.

1 Introduction

J. Watrous introduced the notion of quantum cellular automata(QCA) and showed that any quantum Turing machine can be efficiently simulated by a QCA with constant slowdown in 1995. C. Dürr and M. Santha [4] considered the properties between local function of quantum cellular automata and the unitarity of the global time evolution operator and proposed an algorithm to decide if a linear quantum cellular automaton is unitary. W. van Dam [14, 15] focused on a quantum cellular automata with circular bounded configurations. He also introduced an periodic quantum gate cellular automata and prove that the universality of it.

CA with quantum cells is well-formed QCA if and only if its global transition function is unitary. Generally quantization of cells of a classical CA dose not always induce a QCA, because usually classical CA dose not have reversibility. Morita and Harao show that we can get reversible CA by partition a cell into three part and partitioned CA can simulate non-partitioned CA[11]. But there is not a trivial inclusion relation between partitioned CA and non-partitioned CA.

*Faculty of Mathematics, Kyushu University, E-mail:inokuchi@math.kyushu-u.ac.jp
†Faculty of Mathematics, Kyushu University, E-mail:ym@math.kyushu-u.ac.jp

In this paper, we introduce another systematic formulation of finite cyclic QCA and generalized notion of partitioned QCA in order to investigate natural transformation from discrete classical CA to QCA.

According to the formulations, we demonstrate a condition of a local transition function, which induce a well-formed QCA. A natural correspondence of classical cells and quantum cells can be extended to the correspondence of classical CA and QCA. If a classical CA satisfies our conditions then the extended QCA is well-formed. Finally we report some results of computer simulations of quantization of classical CA.

2 Preliminaries

Let Q be a set of states of cells and $|Q| = s$. We consider Q^n is the set of configurations of CA where n is the size of CA.q_i denotes the ith element of the configuration $q \in Q^n$, and assume that $q_0 = q_n$ and $q_{n+1} = q_1$.

Before considering computing process of quantum states, we recall that of deterministic states. We use the set of all subset of Q, that is, the set 2^Q of all functions from Q to $2 = \{0, 1\}$ to represent nondeterministic states.

A element q of Q is normally considered as an element $\{q\}$ of 2^Q. Let Σ be the finite set of input characters, then a transition function of input characters of deterministic finite automata is provided as $\delta : Q \times \Sigma \to Q$, and expanded naturally into the transition function $\delta_* : Q \times \Sigma^* \to Q$ of input strings. Let $[\delta] : Q \times \Sigma \to 2^Q$ be a function defined by $[\delta](q, \alpha) = [\delta(q, \alpha)]$.

The function $[\delta]$ is a state transition function of nondeterministic finite automata and we can expand $[\delta]$ into $[\delta]_* : Q \times \Sigma^* \to 2^Q$. Recall $[\delta_*] : Q \times \Sigma^* \to 2^Q$ be a function defined by $[\delta_*](q, \alpha) = [\delta_*(q, \alpha)]$, and we can show that $[\delta_*] = [\delta]_*$ easily. This shows that the set of all deterministic finite automata are included in the set of all nondeterministic finite automata naturally.

We can consider quantum states as generalized states of classical state and extend to a quantum formulation of computer system. But a classical computer system is not always a quantum computer system generally, because a quantum computing process should be a unitary operator and every classical computing process is not so.

A quantum state denotes a function from a finite set Q to a set of complex numbers $\mathbf{C}$ and $\mathbf{C}^Q$ is denoted by the set of all functions from Q to $\mathbf{C}$. For $q \in Q$ we define $[q] \in \mathbf{C}^Q$ as follows;

$$[q](x) = \begin{cases} 1 & (x = q) \\ 0 & (x \neq q) \end{cases}$$

$\mathbf{C}^Q$ is a linear space on $\mathbf{C}$ such that its bases is Q. An inner product in $\mathbf{C}^Q$ is defined by $\langle p, q \rangle = \sum_{x \in Q} (p(x) \cdot q(x))$ where $p, q \in \mathbf{C}^Q$.

A linear space $\mathbf{C}^{(Q^n)}$ on $\mathbf{C}$ is considered as a tensor product $\underbrace{\mathbf{C}^Q \otimes \mathbf{C}^Q \otimes \cdots \otimes \mathbf{C}^Q}_{n}$, that is, for $p \in Q^n$ $[p] = [p_1] \otimes [p_2] \otimes \cdots \otimes [p_n]$. For $p, q \in Q^n$ the inner product

$\langle [p],[q]\rangle$ on $\mathbf{C}^{(Q^n)}$ is as follows;

$$
\begin{aligned}
& \langle [p],[q]\rangle \\
= & \sum_{x\in Q^n}([p](x)\cdot[q](x)) \\
= & \sum_{(x_1,x_2,\ldots,x_n)\in Q^n}(([p_1](x_1)[p_2](x_2)\cdots[p_n](x_n)) \\
& \qquad\qquad \cdot([q_1](x_1)[q_2](x_2)\cdots[q_n](x_n))) \\
= & \sum_{x_1\in Q}([p_1](x_1)[q_2](x_1))\cdot\sum_{x_2\in Q}([p_2](x_2)[q_2](x_2)) \\
& \quad \cdots\sum_{x_n\in Q}([p_n](x_n)[q_n](x_n)) \\
= & \langle [p_1],[q_1]\rangle\langle [p_2],[q_2]\rangle\cdots\langle [p_n],[q_n]\rangle.
\end{aligned}
$$

For a function $F : Q^n \to \mathbf{C}^{(Q^n)}$, we define functions $\alpha_F : Q^n \times Q^n \to \mathbf{C}$ and $\overline{F} : \mathbf{C}^{(Q^n)} \to \mathbf{C}^{(Q^n)}$ by $\alpha_F(p,q) = F(p)(q)$ and $\overline{F}(X) = \sum_{q\in Q^n}(X(q)(F(q)))$. We call $\overline{F}$ is *unitary* if $||\overline{F}(X)|| = 1$ for any $X \in \mathbf{C}^{(Q^n)}$ such that $||X|| = 1$.

Since Q is finite, we can label elements of Q numbers from 1 to s and also elements of Q^n numbers from 1 to s^n by lexicographical ordering. We define a $s^n \times s^n$ matrix (α_{ij}) by $\alpha_{ij} = \alpha_F(p,q)$ where numbers of elements p and q are i and j.

Proposition 1 *If the matrix $(\alpha_{i,j})$ is unitary then $\overline{F}$ is unitary.*

Proof. Assume that (α_{ij}) is a unitary matrix and $\langle X,X\rangle = 1$.

$$
\begin{aligned}
& \langle \overline{F}(X),\overline{F}(X)\rangle \\
= & \langle \sum_{p\in Q^n}X(p)\overline{F}(p),\sum_{q\in Q^n}X(q)\overline{F}(q)\rangle \\
= & \sum_{p\in Q^n}\sum_{q\in Q^n}\langle X(p)\overline{F}(p),X(q)\overline{F}(q)\rangle \\
= & \sum_{p\in Q^n}(X(p)\sum_{q\in Q^n}(X(q)\sum_{r\in Q^n}(\overline{F}(p)(r)\cdot\overline{F}(q)(r)))) \\
= & \sum_{p\in Q^n}(X(p)\sum_{q\in Q^n}(X(q)\sum_{r\in Q^n}(\alpha(p,r)\cdot\alpha(q,r)))) \\
= & \sum_{p\in Q^n}(X(p)\sum_{q\in Q^n}(X(q)\sum_{r\in Q^n}(\alpha(p,r)\cdot\overline{\alpha(r,q)}))) \\
= & \sum_{p\in Q^n}(X(p)\cdot X(p)) \\
= & 1
\end{aligned}
$$

So $\overline{F}$ is unitary. □

Proposition 2 *Let $\hat{\sigma} : \mathbf{C}^{Q^n} \to \mathbf{C}^{Q^n}$ be defined by $\hat{\sigma}(X) = \sum_{p \in Q^n}(X(p)[\sigma(p)])$ where $\sigma : Q^n \to Q^n$. Then $\hat{\sigma}$ are unitary if and only if σ is a bijection.*

Proof. (If) Assume that σ is bijection and $\langle X, X \rangle = 1$.

$$\begin{aligned}
& \langle \hat{\sigma}(X), \hat{\sigma}(X) \rangle \\
= & \sum_{p \in Q^n} (\hat{\sigma}(X)(p), \hat{\sigma}(X)(p)) \\
= & \sum_{p \in Q^n} (\sum_{q \in Q^n} (X(q)[\sigma(q)](p)), \sum_{q \in Q^n} (X(q)[\sigma(q)](p))) \\
= & \sum_{p \in Q^n} (X(\sigma^{-1}(p)), X(\sigma^{-1}(p))) \\
= & \sum_{p \in Q^n} (X(p), X(p)) \\
= & 1
\end{aligned}$$

So $\hat{\sigma}$ is unitary.
(Only if) Assume that $\hat{\sigma}$ is unitary and σ is not bijection. Now we let

$$\begin{aligned}
Q_0 &= \{q_0 \in Q^n | \sigma(p) \neq q_0 \ \ for \ \ \forall p \in Q^n\}, \\
Q_1 &= \{q_1 \in Q^n | \exists ! p \in Q^n \ \ such \ \ that \ \ \sigma(p) = q_1\}, \\
Q_2 &= \{q_2 \in Q^n | \exists p_1, p_2 \in Q^n \ \ such \ \ that \ \ q_2 = \sigma(p_1) = \sigma(p_2) \ \ and \ \ p_1 \neq p_2\},
\end{aligned}$$

$|Q_2| = s (\neq 0)$ and

$$X(q) = \begin{cases} \frac{1}{\sqrt{s}} & (q \in Q_2) \\ 0 & otherwise. \end{cases}$$

Then $\langle X, X \rangle = 1$ and

$$\begin{aligned}
& \langle \hat{\sigma}(X), \hat{\sigma}(X) \rangle \\
= & \sum_{q \in Q^n} (\hat{\sigma}(X)(q) \cdot \hat{\sigma}(X)(q)) \\
= & \sum_{q \in Q^n} (\sum_{p \in Q^n} (X(p)[\sigma(p)])(q) \cdot \sum_{p \in Q^n} (X(p)[\sigma(p)])(q)) \\
= & \sum_{q \in Q^n} (\sum_{\sigma(p)=q} X(p) \cdot \sum_{\sigma(p)=q} X(p)) \\
= & \sum_{q \in Q_2} (\sum_{\sigma(p)=q} X(p) \cdot \sum_{\sigma(p)=q} X(p)) \\
\neq & 1
\end{aligned}$$

This is contradiction. So we get that σ is bijection. □

A classical CA[17] is a transition system in Q defined by a global transition function $F : Q^n \to Q^n$ where $F(q)_i = f(q_{i-1}, q_i, q_{i+1})$ and $f : Q \times Q \times Q \to Q$ is a local transition function.

When $Q = \{0,1\}$, a local transition function is defined by the eight values $f(0,0,0) = r_0,\ f(0,0,1) = r_1,\ f(0,1,0) = r_2,\ f(0,1,1) = r_3,\ f(1,0,0) = r_4,$ $f(1,0,1) = r_5,\ f(1,1,0) = r_6$ and $f(1,1,1) = r_7$ $(r_i = 0,1)$. The rule number R of a local transition function f is defined by

$$R = 2^7 r_7 + 2^6 r_6 + 2^5 r_5 + 2^4 r_4 + 2^3 r_3 + 2^2 r_2 + 2^1 r_1 + r_0.$$

The local transition function of rule number R is denoted by f_R. The local transition rules with rule number 204,240 and 170 are illustrated as follows;

	111	110	101	100	011	010	001	000
204	1	1	0	0	1	1	0	0
	111	110	101	100	011	010	001	000
240	1	1	1	1	0	0	0	0
	111	110	101	100	011	010	001	000
170	1	0	1	0	1	0	1	0

f_{204}, f_{240} and f_{170} are identity, shift-right and shift-left functions respectively.

3 Quantum Cellular Automata

The global transition function $F : Q^n \to \mathbf{C}^{(Q^n)}$ is defined by $F_h(q)(x) = h(q_0,q_1,q_2)(x_1) \cdot h(q_1,q_2,q_3)(x_2) \cdots h(q_{n-1},q_n,q_{n+1})(x_n)$ for a local transition function $h : Q \times Q \times Q \to \mathbf{C}^Q$, A transition system in $\mathbf{C}^{(Q^n)}$ is defined by $\overline{F_h} : \mathbf{C}^{(Q^n)} \to \mathbf{C}^{(Q^n)}$. The local transition function h is called 'forming a quantum cellular automaton' if $\overline{F_h}$ is unitary.

Let $F_f : Q^n \to Q^n$ be a global transition function of a local transition function $f : Q^3 \to Q$, and $[F_f] : Q^n \to \mathbf{C}^{Q^n}$ a function such that $[F_f](x) = [F_f(x)]$ for $x \in Q^n$. And we let $[f] : Q^3 \to \mathbf{C}^Q$ be a local transition function of QCA such that $[f](x) = [f(x)]$ for $x \in Q^3$, and $F_{[f]} : Q^n \to \mathbf{C}^{(Q^n)}$ its global transition function. Then we can show that $[F_f] = F_{[f]}$ by easy computation. But a local transition functions $[f] : Q^3 \to \mathbf{C}^Q$ does not always form a QCA, that is, a $\overline{[F_f]}$ is not always unitary. W. van Dam[14, 15] introduced a formulation of cyclic quantum cellular automata and investigate their properties of well-formedness. We focused on reinvestigating similar results related with the extension of classical CA and their local functions.

Proposition 3 *$[f]$ is forming a quantum cellular automata if and only if $F_f : Q^n \to Q^n$ is a bijection.*

Proof. For $X \in \mathbf{C}^{(Q^n)}$

$$\begin{aligned} \overline{F_{[f]}}(X) &= \overline{[F_f]}(X) \\ &= \sum_{q \in Q^n} (X(q)([F_f](q))) \\ &= \sum_{q \in Q^n} (X(q)([F_f(q)])) \\ &= \hat{F}_f(X). \end{aligned}$$

So this is derived from proposition 2. $\square$

4 Partitioned Quantum Cellular Automata

We define functions $G : Q^n \to \mathbf{C}^{(Q^n)}$ and $\lambda : Q \times Q \to \mathbf{C}$ by $G(q)(x) = g(q_1)(x_1) \cdot g(q_2)(x_2) \cdots g(q_n)(x_n)$ and $\lambda(p, q) = g(p)(q)$ for a function $g : Q \to C^Q$.

We label the elements of Q^n numbers from 1 to s^n and define a $s^n \times s^n$ matrix (α_{ij}) from $\alpha_G : Q^n \times Q^n \to \mathbf{C}$. And we label the elements of Q numbers from 1 to s and define a $s \times s$ matrix (λ_{ij}) from the function λ.

Proposition 4 *(λ_{ij}) is a unitary matrix if and only if (α_{ij}) is a unitary matrix.*

Proof. (Only if) Assume that $(\lambda_{i,j})$ is unitary.

$$\begin{aligned} & \sum_{q \in Q^n} (\alpha(p,q) \cdot \alpha(r,q)) \\ = \ & \sum_{q \in Q^n} (G(p)(q) \cdot G(r)(q)) \\ = \ & \sum_{q_1 \in Q} \cdots \sum_{q_n \in Q} g(p_1)(q_1) \cdots g(p_n)(q_n) \cdot g(r_1)(q_1) \cdots g(r_n)(q_n) \\ = \ & \lambda(p_1, r_1) \cdot \lambda(p_2, r_2) \cdots \lambda(p_n, r_n) \\ = \ & \langle [p_1], [r_1] \rangle \cdot \langle [p_2], [r_2] \rangle \cdots \langle [p_n], [r_n] \rangle \\ = \ & \langle [p], [r] \rangle \end{aligned}$$

So $\alpha_{i,j}$ is unitary.
(If) Assume that $\alpha_{i,j}$ is unitary and $\lambda_{i,j}$ is not so, that is, $\lambda(p_i, q_i) \neq \langle [p_i], [q_i] \rangle$. Then

$$\begin{aligned} \sum_{q \in Q^n} (\alpha(p,q) \cdot \alpha(r,q)) &= \lambda(p_1, r_1) \cdot \lambda(p_2, r_2) \cdots \lambda(p_n, r_n) \\ &\neq \langle [p_1], [r_1] \rangle \cdot \langle [p_2], [r_2] \rangle \cdots \langle [p_n], [r_n] \rangle \\ &= \langle [p], [r] \rangle \end{aligned}$$

This is contradiction. So $\lambda_{i,j}$ is unitary. $\square$

Proposition 5 *If $\sigma : Q^n \to Q^n$ is a bijection, then the followings hold;*

(i) $\overline{G \circ \sigma} = \overline{G} \circ \hat{\sigma}$.

(ii) *$\overline{G \circ \sigma}$ is unitary if and only if $\overline{G}$ is unitary.*

$$\begin{array}{ccccc} Q^n & \xrightarrow{\sigma} & Q^n & \xrightarrow{G} & \mathbf{C}^{(Q^n)} \\ \downarrow & & \downarrow & & \Updownarrow \\ \mathbf{C}^{(Q^n)} & \xrightarrow[\hat{\sigma}]{} & \mathbf{C}^{(Q^n)} & \xrightarrow[\overline{G}]{} & \mathbf{C}^{(Q^n)} \end{array}$$

Proof.

(i)

$$\begin{aligned}
\overline{G \circ \sigma}(X) &= \sum_{q \in Q^n} (X(q)((G \circ \sigma)(q))) \\
&= \sum_{q \in Q^n} (X(q)(G(\sigma(q))) \\
&= \sum_{p \in Q^n} (X(\sigma^{-1}(p))(G(q))) \\
&= \sum_{p \in Q^n} ((\sum_{r \in Q^n} (X(r)[\sigma(r)]))(q)(G(q)))) \\
&= \sum_{p \in Q^n} (\hat{\sigma}(X)(q)(G(q)))) \\
&= \overline{G} \circ \hat{\sigma}(X)
\end{aligned}$$

(ii) (If) It is trivial from (i) and proposition 2.
(Only if) Assume that $\overline{G \circ \sigma} = \overline{G} \circ \hat{\sigma}$ is unitary and $\overline{G}$ is not so, that is, $\langle \overline{G \circ \sigma}(X), \overline{G \circ \sigma}(X) \rangle = 1$ and $\langle \hat{\sigma}(X), \hat{\sigma}(X) \rangle = 1$ for any $X \in \mathbf{C}^{(Q^n)}$ such that $\langle X, X \rangle = 1$, and there exists $Y \in \mathbf{C}^{(Q^n)}$ such that $\langle Y, Y \rangle = 1$ and $\langle \overline{G}(Y), \overline{G}(Y) \rangle \neq 1$. Then

$$\begin{aligned}
1 &= \langle \overline{G \circ \sigma}(\hat{\sigma}^{-1}(Y)), \overline{G \circ \sigma}(\hat{\sigma}^{-1}(Y)) \rangle \\
&= \langle \overline{G} \circ \hat{\sigma}(\hat{\sigma}^{-1}(Y)), \overline{G} \circ \hat{\sigma}(\hat{\sigma}^{-1}(Y)) \rangle \\
&= \langle \overline{G}(\hat{\sigma}(\hat{\sigma}^{-1}(Y))), \overline{G}(\hat{\sigma}(\hat{\sigma}^{-1}(Y))) \rangle \\
&= \langle \overline{G}(Y), \overline{G}(Y) \rangle \\
&\neq 1
\end{aligned}$$

□

Theorem 6 *The composition function $f = g \circ e : Q^3 \to \mathbf{C}^Q$ of functions $e : Q^3 \to Q$ and $g : Q \to \mathbf{C}^Q$ is forming a quantum cellular automaton if both of the following two conditions hold:*

(i) *$F_e : Q^n \to Q^n$ is a bijection.*

(ii) *The matrix (λ_{ij}) defined from $g : Q \to \mathbf{C}^Q$ is unitary.*

Proof. At First we show that $\overline{F_f} = \overline{G \circ F_e}$.

$$\begin{aligned}
& G \circ F_e(q)(x) \\
= \;& g(e(q_0, q_1, q_2))(x_1) \cdot g(e(q_1, q_2, q_3))(x_2) \cdots g(e(q_{n-1}, q_n, q_{n+1}))(x_n) \\
= \;& (g \circ e)(q_0, q_1, q_2)(x_1) \cdot (g \circ e)(q_1, q_2, q_3)(x_2) \cdots (g \circ e)(q_{n-1}, q_n, q_{n+1})(x_n) \\
= \;& F_{g \circ e}(q)(x).
\end{aligned}$$

Therefore

$$\begin{aligned}\overline{F_f}(X) &= \overline{F_{g\circ e}}(X)\\ &= \sum_{q\in Q^n}(X(q)(F_{g\circ e}(q)))\\ &= \sum_{q\in Q^n}(X(q)(G\circ F_e)(q))\\ &= \overline{G\circ F_e}(X).\end{aligned}$$

So we can prove this by proposition 4 and 5. □

Example 7 *Let $Q = L\times M\times R$ for finite sets L, M and R. We define $e : Q^3 \to Q$ and $g : Q \to \mathbf{C}^Q$ by $e(((l_1, m_1, r_1), (l_2, m_2, r_2), (l_3, m_3, r_3))) = (l_3, m_2, r_1)$ and $g(q) = [q]$. Then the composition function $f = g\circ e$ is forming a quantum cellular automaton. Because $F_e : Q^n \to Q^n$ is a bijection, $F_e(((l_i, m_i, r_i)))_j = (l_{j+1}, m_j, r_{j-1})$, and (λ_{ij}) defined from g is an identity matrix.*

In example 7, we can replace g to another function $g : Q \to \mathbf{C}^Q$ where the matrix (λ_{ij}) defined from g is unitary. On that occasion $f : (L\times M\times R)^3 \to (L\times M\times R)$ is also forming a quantum cellular automaton. Consequently a partitioned quantum cellular automaton introduced in [16] is demonstrated as a special case of our general formulation.

Example 8 *Let $Q = \{0, 1\}$, $e : Q^3 \to Q$ be a function such that $F_e : Q^n \to Q^n$ is a bijection, and $\Lambda = (\lambda_{ij})$ defined from $g : Q \to \mathbf{C}^Q$ be as follows;*

$$\Lambda = \begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}.$$

Then the local transition function defined from $f = g\circ e$ forms a quantum cellular automaton. This shows a quantum cellular automaton formed by a synthesised function of a local transition function e and its reverse function. That is, if $\theta = 0$ then $f = e$ and if $\theta = \frac{\pi}{2}$ then f is the reversed function of e, so we can consider f for $0 < \theta < \frac{\pi}{2}$ as a synthesised function of two classical local functions.

Example 9 *Let $Q = \{0, 1\}\times\{0, 1\}$,
$e((a_1, b_1), (a_2, b_2), (a_3, b_3)) = (a_1, b_3)$, and $\Lambda = (\lambda_{ij})$ defined by $g : Q \to \mathbf{C}^Q$ be as follows;*

$$\Lambda = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}.$$

Then $f = g\circ e$ forms a QCA and $f((a_1, b_1), (a_2, b_2), (a_3, b_3)) = (a_1, a_1 \oplus b_3)$.

5 Computer Analysis

The following is a table of the size n of CA and rule number R where the local transition function $f_R : Q^3 \to Q$ forms QCA ($Q = \{0, 1\}$, $3 \leq n \leq 22$ and $128 \leq R \leq 255$). We note that if f_R forms QCA then f_{255-R} also forms QCA.

Size n	Rule number R
3	142, 154, 156, 166, 170, 172, 178, 180, 184 198, 202, 204, 210, 212, 216, 226, 228, 240
4, 8, 10, 14 16, 20, 22	150, 170, 204, 240
5, 7, 11, 13, 19	150, 154, 166, 170, 180, 204, 210, 240
9, 15, 21	154, 166, 170, 180, 204, 210, 240
6, 12, 18	170, 204, 240

In the case of size 6, 12 and 18, trivial transitions, that is, identity, right shift and left shift functions only form QCA. In other case, there is a nontrivial transition function forming QCA.

From the above table, we can guess the following table of sizes of CA and rule numbers of local transition functions forming QCA, but we have not proved it yet.

Size ($k \geq 1$)	Rule number
$6k \pm 2$	150, 170, 204, 240
$6k \pm 1$	150, 154, 166, 170, 180, 204, 210, 240
$6k + 3$	154, 166, 170, 180, 204, 210, 240
$6k$	170, 204, 240

Example 10 *When the size of CA is* 4 *or* 5*, the local transition function* $f_{150}(x, y, z) = x + y + z(\mathbf{mod} 2)$ *forms a quantum CA.*
Let F_f *be the global transition function, then the following hold;*

$$\begin{aligned}
F_f(x)_i &= x_{i-1} + x_i + x_{i+1} \\
F_f^2(x)_i &= x_{i-2} + x_{i-1} + x_i \\
&\quad + x_{i-1} + x_i + x_{i+1} \\
&\quad + x_i + x_{i+1} + x_{i+2} \\
&= x_{i-2} + x_i + x_{i+2} \\
F_f^3(x)_i &= x_{i-3} + x_{i-2} + x_{i-1} \\
&\quad + x_{i-1} + x_i + x_{i+1} \\
&\quad + x_{i+1} + x_{i+2} + x_{i+3} \\
&= x_{i-3} + x_{i-2} + x_i + x_{i+2} + x_{i+3}
\end{aligned}$$

In the case that the size of CA is 4*,* $F_f^2(x)_i = x_{i+2} + x_i + x_{i+2} = x_i$*. So* $F_f^2(x) = x$*. In the case that the size of CA is* 5*,* $F_f^3(x)_i = x_{i+2} + x_{i+3} + x_i + x_{i+2} + x_{i+3} = x_i$*. So* $F_f^3(x) = x$*. Namely there exists* y *such that* $F_f(y) = x$ *for any* $x \in Q^n$ $(n = 4, 5)$*, and* F_f *is a bijection. So* f *forms a QCA.*

6 Related Works and Conclusion

Cellular automata dealt in this paper is finite cyclic CA and different from CA without boundary, that is, infinite CA dealt by Watrous[16], Morita and Harao[11]. Because the size of CA is finite it does not have the universal computability[12, 1, 2]. But the conditions of local transition functions forming QCA is formulated clearly in our framework.

Injectivity of global maps of classical CA is an essential property for extending to a QCA. The injectivity are considered in [8, 9, 10, 12] for classical CA without boundary and in [6, 3, 7] for classical finite cyclic CA.

A further direction of this study will be to consider properties on construction and synthesis of general quantum computer system by examining construction and synthesis of local transition function of realizable QCA.

References

[1] A. Birthiaume and G. Brassard: The Quantum Challenge to Structural Complexity Theory, *Proc. 7th IEEE Conf. Struct. Comp. Theo.*, 1992.

[2] D. Deutsch: Quantum Theory, The Church Turing Principle and The Universal Quantum Computer, *Proc. the Royal Society of London A400*, pp. 97–117, 1985.

[3] R.A. Dow: Additive Cellular Automata and Global Injectivity, *Physica D*, 110, pp. 67–91, 1997.

[4] C. Dürr and M. Santha: A Decision Procedure for unitary linear quantum cellular automata, *SIAM J. Comput.*, 31(4), pp. 1076–1089, 2002

[5] J. Gruska: *Quantum Computing*, McGraw-Hill, 1999.

[6] M. Harao and S. Noguchi: On the Algebraic Properties of the Iterative Automaton, *Trans. IEICE*, J55-D, pp.767–774, 1972. [Japanese]

[7] K. Ichikawa, H. Aso, Y. Inagaki and N. Honda: Dynamical Chracteristics of Linear Circular Cellular Automata, *Trans. IEICE*, J65-D, pp.1129–1136, 1982. [Japanese]

[8] M. Ito, N. Osato and M. Nasu: Linear Cellular Automata over Z_m, *J. Computer and System Sciences*, 27, pp.125–140, 1983.

[9] A. Maruoka and M. Kimura: Condition for Injectivity of Global Maps for Tesselation Automata, *Information and Control*, 32, pp.158–162, 1976.

[10] A. Maruoka and M. Kimura: Injectivity and Surjectivity of Parallel Maps for Cellular Automata, *J. Computer and System Sciences*, 18, pp.47–64, 1979.

[11] K. Morita and M. Harao: Computation Universality of One-Dimensional Reversible (Injective) Cellular Automata, *Trans. IEICE*, E72, pp. 758–762, 1989.

[12] T. Toffoli: Computation and Construction Universality of Reversible Cellular Automata, *J. Comput. System Sci.*, 15, pp. 213–231, 1977.

[13] T. Toffoli and H. Margolus: Invertible Cellular Automata: A Review, *Physica D*, 45, pp.229–253, 1990.

[14] W. van Dam: Quantum Cellular Automata, Master's thesis, University of Nijmegen, The Netherlands

[15] W. van Dam: A Universal Quantum Cellular Automaton, *Proceedings of the Fourth Workshop on Physics and Computation*, pp. 323–331, 1996

[16] J. Watrous: On One-Dimensional Quantum Cellular Automata, *Proceedings of the 36th Annual Symposium on Foundations of Computer Science*, pp. 528–537, 1995.

[17] S. Wolfram:*Cellular Automata and Complexity: Collected Papers*, Addison-Wesley Publishing Company, 1994

List of MHF Preprint Series, Kyushu University

21st Century COE Program
Development of Dynamic Mathematics with High Functionality

MHF2003-1 Mitsuhiro T. NAKAO, Kouji HASHIMOTO & Yoshitaka WATANABE
A numerical method to verify the invertibility of linear elliptic operators with applications to nonlinear problems

MHF2003-2 Masahisa TABATA & Daisuke TAGAMI
Error estimates of finite element methods for nonstationary thermal convection problems with temperature-dependent coefficients

MHF2003-3 Tomohiro ANDO, Sadanori KONISHI & Seiya IMOTO
Adaptive learning machines for nonlinear classification and Bayesian information criteria

MHF2003-4 Kazuhiro YOKOYAMA
On systems of algebraic equations with parametric exponents

MHF2003-5 Masao ISHIKAWA & Masato WAKAYAMA
Applications of Minor Summation Formulas III, Plücker relations, Lattice paths and Pfaffian identities

MHF2003-6 Atsushi SUZUKI & Masahisa TABATA
Finite element matrices in congruent subdomains and their effective use for large-scale computations

MHF2003-7 Setsuo TANIGUCHI
Stochastic oscillatory integrals - asymptotic and exact expressions for quadratic phase functions -

MHF2003-8 Shoki MIYAMOTO & Atsushi YOSHIKAWA
Computable sequences in the Sobolev spaces

MHF2003-9 Toru FUJII & Takashi YANAGAWA
Wavelet based estimate for non-linear and non-stationary auto-regressive model

MHF2003-10 Atsushi YOSHIKAWA
Maple and wave-front tracking — an experiment

MHF2003-11 Masanobu KANEKO
On the local factor of the zeta function of quadratic orders

MHF2003-12 Hidefumi KAWASAKI
Conjugate-set game for a nonlinear programming problem

MHF2004-1 Koji YONEMOTO & Takashi YANAGAWA
Estimating the Lyapunov exponent from chaotic time series with dynamic noise

MHF2004-2 Rui YAMAGUCHI, Eiko TSUCHIYA & Tomoyuki HIGUCHI
State space modeling approach to decompose daily sales of a restaurant into time-dependent multi-factors

MHF2004-3 Kenji KAJIWARA, Tetsu MASUDA, Masatoshi NOUMI, Yasuhiro OHTA & Yasuhiko YAMADA
Cubic pencils and Painlevé Hamiltonians

MHF2004-4 Atsushi KAWAGUCHI, Koji YONEMOTO & Takashi YANAGAWA
Estimating the correlation dimension from a chaotic system with dynamic noise

MHF2004-5 Atsushi KAWAGUCHI, Kentarou KITAMURA, Koji YONEMOTO, Takashi YANAGAWA & Kiyofumi YUMOTO
Detection of auroral breakups using the correlation dimension

MHF2004-6 Ryo IKOTA, Masayasu MIMURA & Tatsuyuki NAKAKI
A methodology for numerical simulations to a singular limit

MHF2004-7 Ryo IKOTA & Eiji YANAGIDA
Stability of stationary interfaces of binary-tree type

MHF2004-8 Yuko ARAKI, Sadanori KONISHI & Seiya IMOTO
Functional discriminant analysis for gene expression data via radial basis expansion

MHF2004-9 Kenji KAJIWARA, Tetsu MASUDA, Masatoshi NOUMI, Yasuhiro OHTA & Yasuhiko YAMADA
Hypergeometric solutions to the q - Painlevé equations

MHF2004-10 Raimundas VIDŪNAS
Expressions for values of the gamma function

MHF2004-11 Raimundas VIDŪNAS
Transformations of Gauss hypergeometric functions

MHF2004-12 Koji NAKAGAWA & Masakazu SUZUKI
Mathematical knowledge browser

MHF2004-13 Ken-ichi MARUNO, Wen-Xiu MA & Masayuki OIKAWA
Generalized Casorati determinant and Positon-Negaton-Type solutions of the Toda lattice equation

MHF2004-14 Nalini JOSHI, Kenji KAJIWARA & Marta MAZZOCCO
Generating function associated with the determinant formula for the solutions of the Painlevé II equation

MHF2004-15 Kouji HASHIMOTO, Ryohei ABE, Mitsuhiro T. NAKAO & Yoshitaka WATANABE
Numerical verification methods of solutions for nonlinear singularly perturbed problem

MHF2004-16 Ken-ichi MARUNO & Gino BIONDINI
Resonance and web structure in discrete soliton systems: the two-dimensional Toda lattice and its fully discrete and ultra-discrete versions

MHF2004-17 Ryuei NISHII & Shinto EGUCHI
Supervised image classification in Markov random field models with Jeffreys divergence

MHF2004-18 Kouji HASHIMOTO, Kenta KOBAYASHI & Mitsuhiro T. NAKAO
Numerical verification methods of solutions for the free boundary problem

MHF2004-19 Hiroki MASUDA
Ergodicity and exponential β-mixing bounds for a strong solution of Lévy-driven stochastic differential equations

MHF2004-20 Setsuo TANIGUCHI
The Brownian sheet and the reflectionless potentials

MHF2004-21 Ryuei NISHII & Shinto EGUCHI
Supervised image classification based on AdaBoost with contextual weak classifiers

MHF2004-22 Hideki KOSAKI
On intersections of domains of unbounded positive operators

MHF2004-23 Masahisa TABATA & Shoichi FUJIMA
Robustness of a characteristic finite element scheme of second order in time increment

MHF2004-24 Ken-ichi MARUNO, Adrian ANKIEWICZ & Nail AKHMEDIEV
Dissipative solitons of the discrete complex cubic-quintic Ginzburg-Landau equation

MHF2004-25 Raimundas VIDŪNAS
Degenerate Gauss hypergeometric functions

MHF2004-26 Ryo IKOTA
The boundedness of propagation speeds of disturbances for reaction-diffusion systems

MHF2004-27 Ryusuke KON
Convex dominates concave: an exclusion principle in discrete-time Kolmogorov systems

MHF2004-28 Ryusuke KON
Multiple attractors in host-parasitoid interactions: coexistence and extinction

MHF2004-29 Kentaro IHARA, Masanobu KANEKO & Don ZAGIER
Derivation and double shuffle relations for multiple zeta values

MHF2004-30 Shuichi INOKUCHI & Yoshihiro MIZOGUCHI
Generalized partitioned quantum cellular automata and quantization of classical CA