Proceedings of the 3rd International Conference on Mathematical Physics and Computational Simulation
DOI: 10.54254/2753-8818/92/2025.22378

Quantum Cellular Automata and Groups

Ruoli Bai

Arcadia High School, Arcadia, USA
rbai1214lm@gmail.com

Abstract: A quantum cellular automaton (QCA) is a unitary discrete-time evolution of a quantum many-body system, which can be described as a dynamics system $\alpha(A) = U^*AU$, where A is any $n \times n$ matrix and U is a unitary operator representing the global evolution of QCA. And QCAs are characterized by locality (or causality). Among them, quantum circuits are the special classes of QCAs, which use unitary operators to control and transform the initial quantum state of qubit into a final quantum state, quantum circuits are special and widely studied in quantum information. A group is a set of elements combined with an operation, which satisfies associativity, identity and invertibility. This article shows that group theory provides the right language for studying the relation between QCAs and quantum circuits among them.

Keywords: quantum cellular automaton, quantum circuit, group.

1. Introduction

Quantum information has garnered tremendous interest from physics and mathematics community [1,2]. Evolution of a quantum lattice system is key to understanding nature. Cellular automaton (CA) has long been studied as mathematical model of computation, where a grid of cells evolves according to local rules over discrete time steps [3]. However, classical CA follows local rules that do not incorporate quantum mechanical principles such as superposition, entanglement, and unitary evolution. Quantum cellular automaton (QCA) extends the classical CA framework into the quantum domain, preserving key features like discrete time steps and locality while introducing quantum properties. Quantum cellular automaton (QCA) provides a mathematical framework [4]. The classification of QCAs is a well-posed and exciting question [5]. QCA generalizes classical cellular automata to quantum mechanics, allowing superposition and entanglement while preserving locality and reversibility [6.7]. The concept of QCA is abstract, and using group theory is a good way to understand it [8]. Group theory is the study of algebraic structures called groups, which is used to analyze symmetries in mathematics and physics, and classify structures in algebra [9,10].

Section 2 provides a brief introduction to quantum information and some basic concepts that are important in quantum information, and starts relating QCA. Section 3 introduces the cellular automaton (CA), quantum cellular automaton (QCA), the property of QCA dynamics and Clifford QCA. Section 4 discusses the relation between QCA and group, showing that using group theory to think about QCA is advantageous. Section 5 discusses the applications of QCA in the future.

2. Brief Note on Quantum Information

In quantum information, the trade-off between acquiring information and creating a disturbance

DOI: 10.54254/2753-8818/92/2025.22378

is related to quantum randomness. It is because the outcome of a measurement has a random element that we are unable to infer the initial state of the system from the measurement outcome. Quantum information differs from classical information due to quantum information cannot be copied with perfect fidelity. If we could make a perfect copy of a quantum state, we could measure an observable of the copy without disturbing the original and we could defeat the principle of disturbance. On the other hand, nothing prevents us from copying classical information perfectly. John Bell showed that the predictions of quantum mechanics cannot be reproduced by any local hidden variable theory, and quantum information can be (in fact, typically is) encoded in nonlocal correlations between the different parts of a physical system, correlations with no classical counterpart.

2.1. Hilbert Space (Hermitian Inner Product) Matrix Algebra

In this section, we talk about the inner product and matrix algebra in Hilbert space. Hilbert space connects with many concepts that we would mention later, qubits are represented as vectors in the Hilbert space, quantum gates are unitary operators that act on the state of a qubit in a Hilbert space.

Definition 1. A Hilbert space $\mathbb{H}$ is a complete complex vector space, that is, $\psi,\ \varphi \in \mathbb{H}$ and $a,\ b \in \mathbb{C}$, then $a\psi + b\varphi \in \mathbb{H}$.

If $a,\ b \in \mathbb{C}$, $a = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ and $b = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$ and $v,\ v_1,\ v_2,\ w,\ w_1,\ w_2 \in \mathbb{H}$. Then, we have totally 4 properties:

Property 1. $\langle av|bw\rangle = \bar{a}\langle v|bw\rangle = b\langle av|w\rangle = \bar{a}b\langle v|w\rangle$

Property 2. $\langle a|b\rangle = \bar{a}^T b = \sum_{i=1}^{n} \bar{a}_i\, b_i = [\bar{a}_1 \quad \cdots \quad \bar{a}_n] \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$

Property 3. $\langle v_1 + v_2|w\rangle = \langle v_1|w\rangle + \langle v_2|w\rangle$

Property 4. $\langle v|w_1 + w_2\rangle = \langle v|w_1\rangle + \langle v|w_2\rangle$

Lemma 2. We define the adjoint of a matrix A to be $A^* = \bar{A}^T$. It can be verified that for any v, w in the Hilbert space, we have

$$\langle v|Aw\rangle = \langle A^* v|w\rangle.$$

In fact, this property uniquely determines the adjoint of A.

Proof. Let $\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$, $A = \begin{bmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \cdots & A_{nn} \end{bmatrix}$ and $w = \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}$. Then,

$$\begin{aligned} \langle v|Aw\rangle &= [\bar{v}_1 \quad \cdots \quad \bar{v}_n] \begin{bmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \cdots & A_{nn} \end{bmatrix} \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} \\ &= \left[A^T \begin{bmatrix} \bar{v}_1 \\ \vdots \\ \bar{v}_n \end{bmatrix} \right]^T \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} \\ &= \overline{\left[\bar{A}^T \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \right]}^T \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} \\ &= \langle A^* v|w\rangle \end{aligned}$$

DOI: 10.54254/2753-8818/92/2025.22378

Lemma 3. In a simiar way as Lemma 2, we define a unitary matrix U, then $U^* = U^{-1}$, we have

$$\langle v|Uw\rangle = \langle U^* v|w\rangle,$$

because $U^* = U^{-1}$, we have

$$\langle v\left|Uw\right\rangle = \langle U^{-1}v\right|w\rangle.$$

2.1.1. Self-Adjoint

Definition 4. The matrix A is called self-adjoint if $A^* = A$, $A^* = (\bar{A})^T$ is called its adjoint.

For example, matrix $A = \begin{bmatrix} 1 & i \\ -i & -1 \end{bmatrix}$ is self-adjoint, because $A^* = \begin{bmatrix} 1 & -i \\ i & -1 \end{bmatrix}^T = \begin{bmatrix} 1 & i \\ -i & -1 \end{bmatrix} = A$.

2.1.2. Unitary Matrix

Definition 5. The matrix U is unitary if $U^* = U^{-1}$ or $UU^* = U^*U = I$.

For example, matrix $U = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ is a unitary matrix, because $U^* = \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix}$, then $UU^* = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$.

2.1.3. Pauli Matrices

Definition 6. The matrices σ_j indexed by either $j \in 1,2,3$ or $j \in x, y, z$ and defined as

$$X := \sigma_x := \sigma_1 := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y := \sigma_y := \sigma_2 := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z := \sigma_z := \sigma_3 := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

are called Pauli matrices. These three Pauli matrices are self-adjoint, and they are unitary matrices.

2.2. Qubit

In this section, we talk about the difference between classical bit and qubit, the general normalized qubit state. The state of a qubit is a vector in the two-dimensional Hilbert space $\mathbb{H}^2$. Let we image a coin, a calssical bit is like a coin lying flat on the table, the state is either heads (0) or tails (1). And a qubit is like spinning that coin in the air, when it's spinning, the state is not just heads (0) or tails (1), it's a mixture of both until we catch it. This "mixture" is the superposition.

A qubit is a quantum mechanical system described by a two-dimensional Hilbert space denoted by $\mathbb{H}$ and called qubit space. A qubit is a fundamental unit of quantum information, analogous to a classical bit in classical computing. However, unlike a classical bit that can only be in one of two states $\{0,1\}$, a qubit can exist in a superposition of states.

This way each classical bit value is mapped to a qubit state. The smallest nontrivial Hilbert space is two-dimensional. We can denote an orthonormal basis for a two-dimensional vector space as $\{|0\rangle, |1\rangle\}$. However, not every qubit state can be mapped to a classical bit value. This is because the most general normalized qubit state is of the form

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{1}$$

with $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$. Qubit state $|0\rangle$ corresponds to the classical bit 0, and qubit state $|1\rangle$ corresponds to the classical bit 1. The superposition case occurs when a qubit exists in a state that is a combination of the basis states $|0\rangle$ and $|1\rangle$, rather than being strictly in one of them, which means $ab \neq 0$ and there is no corresponding classical bit value. The probability of measuring the qubit in

DOI: 10.54254/2753-8818/92/2025.22378

the state $|0\rangle$ is $|a|^2$, the probability of measuring the qubit in the state $|1\rangle$ is $|b|^2$. After the measurement, the state of qubit collapses to either $|0\rangle$ or $|1\rangle$. The total probability must always equal to 1, so this is also the reason why $|a|^2 + |b|^2 = 1$.

Because $|a|^2 + |b|^2 = 1$ we can find $\alpha, \beta, \theta \in \mathbb{R}$ such that $a = e^{i\alpha}\cos\frac{\theta}{2}$ and $b = e^{i\beta}\sin\frac{\theta}{2}$. Thus, a qubit state has the general form

$$\left|\psi\right\rangle = e^{i\alpha}\cos\frac{\theta}{2}\left|0\right\rangle + e^{i\beta}\sin\frac{\theta}{2}|1\rangle. \tag{2}$$

For a 3-dimensional real vector $a = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}$, we can define the 2×2 matrix

$$a \cdot \sigma := \sum_{j=1}^{3} a_j \sigma_j = a_1\sigma_1 + a_2\sigma_2 + a_3\sigma_3 = \begin{bmatrix} a_3 & a_1 - ia_2 \\ a_1 + ia_2 & -a_3 \end{bmatrix}. \tag{3}$$

The matrix $a \cdot \sigma$ is an operation that transform a 3-dimensional real vector $a = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}$ into a 2×2 Hermitian matrix using the Pauli matrices σ_1, σ_2 and σ_3.

2.3. Tensor Product (between vectors as well as matrices)

In this section, we define a new operation that takes two or more Hilbert spaces to produce a new Hilbert space as their product. Tensor product is significant in building higher dimensional space and representing unitary operators in the following sections.

Let $\mathbb{H}^A$ and $\mathbb{H}^B$ be Hilbert spaces, $|\varphi\rangle \in \mathbb{H}^A$ and $|\psi\rangle \in \mathbb{H}^B$, then we define

$$\left|\varphi\right\rangle \otimes \left|\psi\right\rangle \in \mathbb{H}^{\mathrm{A}} \otimes \mathbb{H}^{\mathrm{B}} \tag{4}$$

According to (4), $|\varphi\rangle \otimes |\psi\rangle$ is a vector in the combined Hilbert space $\mathbb{H}^A \otimes \mathbb{H}^B$. If $|\varphi\rangle \in \mathbb{H}^A$ and $|\psi\rangle \in \mathbb{H}^B$ and $a, b \in \mathbb{C}$. Then, we have the following identities.

$$\begin{aligned} (a|\varphi\rangle) \otimes |\psi\rangle &= |\varphi\rangle \otimes (a|\psi\rangle) = a(|\varphi\rangle \otimes |\psi\rangle) \\ a(|\varphi\rangle \otimes |\psi\rangle) + b(|\varphi\rangle \otimes |\psi\rangle) &= (a+b)|\varphi\rangle \otimes |\psi\rangle \\ \left(\left|\varphi_1\right\rangle + \left|\varphi_2\right\rangle\right) \otimes |\psi\rangle &= \left|\varphi_1\right\rangle \otimes \left|\psi\right\rangle + \left|\varphi_2\right\rangle \otimes \left|\psi\right\rangle \\ |\varphi\rangle \otimes \left(\left|\psi_1\right\rangle + \left|\psi_2\right\rangle\right) &= |\varphi\rangle \otimes |\psi_1\rangle + |\varphi\rangle \otimes |\psi_2\rangle. \end{aligned}$$

In order to simplify the notation, we can also write $|\varphi \otimes \psi\rangle := |\varphi\rangle \otimes |\psi\rangle$. For vectors $\left|\varphi_p\right\rangle \otimes \left|\psi_p\right\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$ with $p \in \{1,2\}$ and $|\varphi_p\rangle \in \mathbb{H}^A$, $|\psi_p\rangle \in \mathbb{H}^B$ we define

$$\langle \varphi_1 \otimes \psi_1 \left|\varphi_2 \otimes \psi_2\right\rangle := \langle \varphi_1 \left|\varphi_2\right\rangle^{\mathbb{H}^A} \langle \psi_1 | \psi_2 \rangle^{\mathbb{H}^B}. \tag{5}$$

Lemma 7. Let $\{|a_i\rangle\} \subset \mathbb{H}^A$ be an ONB in $\mathbb{H}^A$ and $\{|b_j\rangle\} \subset \mathbb{H}^B$ be an ONB in $\mathbb{H}^B$. The set $\{\left|a_i \otimes b_j\right\rangle\} = \{\left|a_i\right\rangle \otimes \left|b_j\right\rangle\}$ forms an ONB in $\mathbb{H}^A \otimes \mathbb{H}^B$, and for finite-dimensional $\mathbb{H}^A$ and $\mathbb{H}^B$, we have

$$\dim\left(\mathbb{H}^A \otimes \mathbb{H}^B\right) = \dim\mathbb{H}^A \dim\mathbb{H}^B. \tag{6}$$

If $\dim\mathbb{H}^A = m$, and $\dim\mathbb{H}^B = n$, then let $|\varphi\rangle = \sum_{i=1}^{m} c_i |a_i\rangle$ and $\left|\psi\right\rangle = \sum_{j=1}^{n} d_j \left|b_j\right\rangle$, $|a_i\rangle$ are ONBs in $\mathbb{H}^A$ and $|b_j\rangle$ are ONBs in $\mathbb{H}^B$, c_i and d_j are complex scalars. Thus, the vector in Hilbert space $\mathbb{H}^A \otimes \mathbb{H}^B$ is in the form

DOI: 10.54254/2753-8818/92/2025.22378

$$\begin{aligned} |\varphi\rangle \otimes |\psi\rangle &= \left(\sum_{i=1}^{m} c_i\,|a_i\rangle\right) \otimes \left(\sum_{j=1}^{n} d_j\,|b_j\rangle\right) \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} c_i\,d_j\left(|a_i\rangle \otimes |b_j\rangle\right). \end{aligned} \tag{7}$$

Definition 8. In the Hilbert space $\mathbb{H}^A \otimes \mathbb{H}^B$, the scalar product $\langle\alpha|\beta\rangle = \sum_{a,b} \bar{\alpha}_{ab}\,\beta_{ab}$, $\alpha, \beta \in \mathbb{H}^A \otimes \mathbb{H}^B$ is called the tensor product of the Hilbert spaces $\mathbb{H}^A$ and $\mathbb{H}^B$.

If $\mathbb{H}^A = \mathbb{H}^B \cong \mathbb{C}^2$ with the ONBs $\{|a_i\rangle\} = \{|b_j\rangle\} = \{|0\rangle, |1\rangle\} = \left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right\}$, where the set $\left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right\}$ denotes the standard basis in $\mathbb{C}^2$. For $\mathbb{H}^A \otimes \mathbb{H}^B \cong \mathbb{C}^4$ we have the ONBs $\{|a_i\rangle \otimes |b_j\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} = \left\{\begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\1\end{bmatrix}\right\}$, where the set $\left\{\begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\1\end{bmatrix}\right\}$ also denotes the standard basis in $\mathbb{C}^4$. Besides, for $k \in \{1,2\}$ let $a_k, b_k \in \mathbb{C}$ and qubit states $|\varphi_1\rangle = a_1|0\rangle + b_1\left|1\right\rangle = \begin{bmatrix}a_1\\b_1\end{bmatrix}$, $\left|\varphi_2\right\rangle = a_2|0\rangle + b_2|1\rangle = \begin{bmatrix}a_2\\b_2\end{bmatrix}$. Then, we have

$$\begin{aligned} \left|\varphi_1\right\rangle \otimes \left|\varphi_2\right\rangle &= \left(a_1\left|0\right\rangle + b_1\left|1\right\rangle\right) \otimes \left(a_2\left|0\right\rangle + b_2\left|1\right\rangle\right) \\ &= a_1a_2|0\rangle \otimes |0\rangle + a_1b_2|0\rangle \otimes |1\rangle + b_1a_2|1\rangle \otimes |0\rangle + b_1b_2|1\rangle \otimes |1\rangle \\ &= a_1a_2\left|00\right\rangle + a_1b_2\left|01\right\rangle + b_1a_2\left|10\right\rangle + b_1b_2\left|11\right\rangle \\ &= \begin{bmatrix}a_1a_2\\a_1b_2\\b_1a_2\\b_1b_2\end{bmatrix}, \end{aligned} \tag{8}$$

which represents the state of a two-qubit system.

In a similar way, if $\mathbb{H}^C \cong \mathbb{C}^2$ with the ONB $\{|0\rangle, |1\rangle\}$, then the ONB of $\mathbb{H}^A \otimes \mathbb{H}^B \otimes \mathbb{H}^C \cong \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^8$ is $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$

$$= \left\{\begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\0\\0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\1\\0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\0\\1\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\0\\0\\1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\0\\0\\0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\0\\0\\0\\0\\1\end{bmatrix}\right\}.$$

The first notation that includes "|⟩" is simple, and the second notation is more complicated.

For the tensor product of dual vectors, we have

$$\langle\varphi \otimes \psi| = \langle\varphi| \otimes \langle\psi|. \tag{9}$$

The dual ONBs for $\mathbb{C}^2$ are $\{\langle 0|, \langle 1|\} = \{[1 \quad 0], [0 \quad 1]\}$, this set denotes the standard basis in the dual space $(\mathbb{C}^2)^* \cong \mathbb{C}^2$. For $\mathbb{C}^4$, dual ONBs are $\{\langle 00|, \langle 01|, \langle 10|, \langle 11|\} = \{[1 \quad 0 \quad 0 \quad 0], [0 \quad 1 \quad 0 \quad 0], [0 \quad 0 \quad 1 \quad 0], [0 \quad 0 \quad 0 \quad 1]\}$, this set denotes the standard basis

DOI: 10.54254/2753-8818/92/2025.22378

in the dual space $(\mathbb{C}^4)^* \cong \mathbb{C}^4$. Besides, for $k \in \{1,2\}$, let c_k, $d_k \in \mathbb{C}$, and $\langle\psi_1| = c_1\langle 0| + d_1\langle 1| = [c_1 \quad d_1]$, $\langle\psi_2| = c_2\langle 0| + d_2\langle 1| = [c_2 \quad d_2]$. In the basis $\{|a_i \otimes b_j\rangle\}$, we have

$$\begin{aligned} \langle\psi_1| \otimes \langle\psi_2| &= \left(c_1\langle 0| + d_1\langle 1|\right)\left(c_2\langle 0| + d_2\langle 1|\right) \\ &= c_1c_2\langle 0| \otimes \langle 0| + c_1d_2\langle 0| \otimes \langle 1| + d_1c_2\langle 1| \otimes \langle 0| + d_1d_2\langle 1| \otimes \langle 1| \\ &= c_1c_2\langle 00| + c_1d_2\langle 01| + d_1c_2\langle 10| + d_1d_2\langle 11| \\ &= [c_1c_2 \quad c_1d_2 \quad d_1c_2 \quad d_1d_2]. \end{aligned} \tag{10}$$

For $\mathbb{C}^8$, dual ONBs are $\{\langle 000|, \langle 001|, \langle 010|, \langle 100|, \langle 011|, \langle 101|, \langle 110|, \langle 111|\}$. We can find the pattern, either the n-dimensional space or its dual space has n standard basis.

2.4. Schmidt Decomposition and Entanglement

In this section, we define a powerful way to express bipartite states, which is Schmidt decomposition, in this way, we can easily determine whether the state is separable or entangled. Also, we use W-state to further explain this powerful tool.

Suppose there are two systems A and B, any bipartite state $|\psi\rangle_{AB}$ in the Hilbert space $\mathbb{H}^A \otimes \mathbb{H}^B$ can be expressed as the following by Schmidt decomposition:

$$|\psi\rangle_{AB} = \sum_{k=1}^{r} \lambda_k |u_k\rangle_A \otimes |v_k\rangle_B, \tag{11}$$

where:

- $\{|u_k\rangle_A\}$ and $\{|v_k\rangle_B\}$ are sets of orthonormal basis vectors in subsystems A and B, respectively.
- $\lambda_k \geq 0$ are called Schmidt coefficients, satisfying $\sum_k \lambda_k^2 = 1$.
- r is the Schmidt rank, which is the total number of nonzero Schmidt coefficients.

If the Schmidt rank $r = 1$, then the state is separable and can be expressed as $|\psi\rangle = \lambda_1|u_1\rangle_A \otimes |v_1\rangle_B$, in this case, subsystem A is completely independent of subsystem B, there is no entanglement. If the Schmidt rank $r > 1$, then the state is entangled, the state cannot be written as the tensor product of states in $\mathbb{H}^A$ and $\mathbb{H}^B$.

The W-state for three qubits is

$$|W\rangle = \frac{1}{\sqrt{3}}\left(|001\rangle + |010\rangle + |100\rangle\right), \tag{12}$$

to express this in Schmidt decomposition, we need to divide the system into two subsystems, qubit 1 is one subsystem A and qubits 2 and 3 form another subsystem B. Firstly, we can write W-state in another way:

$$|W\rangle = \sqrt{\frac{1}{3}}\left(|0\rangle_A \otimes |01\rangle_B + |0\rangle_A \otimes |10\rangle_B + |1\rangle_A \otimes |00\rangle_B\right), \tag{13}$$

here, the basis for subsystem A is $\{|0\rangle, |1\rangle\}$, and the basis for subsystem B is $\{|00\rangle, |01\rangle\}, |10\rangle\}, |11\rangle\}$. Then, we have

DOI: 10.54254/2753-8818/92/2025.22378

$$\begin{aligned}|W\rangle &= \sqrt{\frac{1}{3}}\left(|0\rangle_A \otimes (|01\rangle_B + |10\rangle_B) + |1\rangle_A \otimes |00\rangle_B\right) \\ &= \sqrt{\frac{2}{3}}|0\rangle_A \otimes \left(\frac{1}{\sqrt{2}}|01\rangle_B + \frac{1}{\sqrt{2}}|10\rangle_B\right) + \sqrt{\frac{1}{3}}|1\rangle_A \otimes |00\rangle_B \\ &= \sqrt{\frac{2}{3}}|0\rangle_A \otimes \frac{1}{\sqrt{2}}\left(|01\rangle_B + |10\rangle_B\right) + \sqrt{\frac{1}{3}}|1\rangle_A \otimes |00\rangle_B \\ &= \sqrt{\frac{2}{3}}|0\rangle_A \otimes \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)_B + \sqrt{\frac{1}{3}}|1\rangle_A \otimes |00\rangle_B.\end{aligned} \tag{14}$$

The Schmidt rank r is two, because there are two nonzero Schmidt coefficients. Since the Schmidt rank $r > 1$, so the state is entangled between subsystem A and subsystem B. The state of subsystem A is correlated with the state of subsystem B. If we measure one of subsystems:

1. If we find that subsystem A is in state $|0\rangle$, the state of subsystem B collapses to $\frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$.
2. If we find that subsystem A is in state $|1\rangle$, the state of subsystem B collapses to $|00\rangle$.
3. If we find that subsystem B is in state $\frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$, the state of subsystem A collapses to $|0\rangle$.
4. If we find that subsystem B is in state $|00\rangle$, the state of subsystem A collapses to $|1\rangle$.

This dependence shows the quantum correlation between subsystems A and B, this correlation is also what we call entanglement between the two subsystems. Entanglement is a relationship involving two or more distinct subsystems. Measurements on subsystem A can instantaneously affect the outcomes of measurements on subsystem B, no matter how far apart they are. Without this quantum correlation across subsystems, there would be no entanglement. I think writing states in Schmidt decomposition can beneficially analyze the correlation between subsystems, for example, we can use the qubit in subsystem A to check the state of subsystem B is in superposition or not. So I think Schmidt decomposition is a really powerful and helpful tool.

2.5. Finite Depth Quantum Circuit

In this section, we define the quantum gate, the quantum circuit, and the finite depth quantum circuit. A finite depth quantum circuit is like making a multi-layered cake. Each layer of the cake represents a set of quantum gates applied to the qubits, which are like the ingredients on each layer. The total number of layers in the cake corresponds to the finite depth of the circuit, meaning the process stops after a specific number of layers.

In quantum computing, a quantum gate is a fundamental operation that performs a specific transformation on one or more qubits. Unlike many classical logic gates, quantum logic gates are reversible, quantum circuits can perform all operations performed by classical circuits. Quantum gates are unitary operators, and are described as unitary matrices relative to some orthonormal basis. A quantum gate is a unitary operator U that acts on the state of a qubit or multiple qubits in a Hilbert space. This is how a quantum gate works:

$$|\psi_2\rangle = U|\psi_1\rangle, \tag{15}$$

DOI: 10.54254/2753-8818/92/2025.22378

where $|\psi_1\rangle$ is the input quantum state, U is the unitary matrix which represents the quantum gate, $|\psi_2\rangle$ is the resulting quantum state after applying the gate.

Definition 9. A quantum n-gate is a unitary operator $U: \mathbb{H}^{\otimes n} \to \mathbb{H}^{\otimes n}$. For n = 1, a gate U is called a unary quantum gate and for n = 2, a gate U is called a binary quantum gate.

Unary quantum gates are unitary operators $U: \mathbb{H} \to \mathbb{H}$, which can be represented in the standard basis $\{|0\rangle, |1\rangle\}$ by unitary 2×2 matrices. Most common unary quantum gates include Identity, Pauli-X, Pauli-Y and Pauli-Z.

Binary quantum gates are unitary operators $U: \mathbb{H}^{\otimes 2} \to \mathbb{H}^{\otimes 2}$, which can be represented in the standard basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ by unitary 4×4 matrices.

Definition 10. Controlled NOT gate (CNOT) is a quantum gate, CNOT gate operates on a system consisting of 2 qubits. The CNOT gate flips the target qubit if and only if the control qubit is $|1\rangle$.

Control =Qubit 1,Target =Qubit 2		Control=Qubit 2, Target=Qubit 1	
Before	After	Before	After
$\|00\rangle$	$\|00\rangle$	$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$	$\|01\rangle$	$\|11\rangle$
$\|10\rangle$	$\|11\rangle$	$\|10\rangle$	$\|10\rangle$
$\|11\rangle$	$\|10\rangle$	$\|11\rangle$	$\|01\rangle$

The CNOT gate for control qubit and target qubit in a two-qubit system is a 4×4 unitary matrix as the following:

$$\text{Control = Qubit 1, Target = Qubit 2: } CNOT_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$\text{Control = Qubit 2, Target = Qubit 1: } CNOT_{21} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

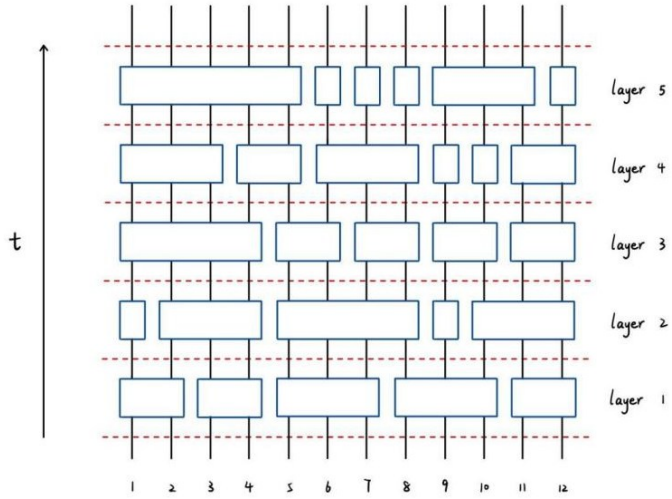

Figure 1: Quantum Circuit Diagram with Twelve Qubits and Five Layers

DOI: 10.54254/2753-8818/92/2025.22378

In a quantum computation, quantum gates are the components of a quantum circuit. A quantum circuit consists of multiple quantum gates applied to qubits. Quantum gates are the tools, while the quantum circuit is the entire mechanism designed to perform a specific quantum computation.

Definition 11. Essentially, a quantum circuit is a framework for using unitary operators (quantum gates) to control and transform the initial quantum state of qubits into a final quantum state, which encodes the result of the quantum computation.

In Figure 1, each vertical line represents a qubit, the blocks represent quantum gates applied to a set of qubits, quantum gates always act on one or more qubits. Each block in a row acts on disjoint sets of qubits, the total number of blocks in the quantum circuit is called its size, and time increases from bottom to top. In the diagram above, there are twelve qubits and five layers.

Definition 12. The depth of a quantum circuit is defined as the number of layers of quantum gates in the quantum circuit diagram.

Definition 13. A finite depth quantum circuit is a quantum circuit with a limited depth required to complete the computation, regardless of the size of quantum circuit or the number of qubits.

Let $\{U_i\}$ be a set of unitary operators that act on disjoint sets of qubits within the same layer, then $U_{layer} = U_1 \otimes U_2 \otimes \cdots \otimes U_k$ represents the unitary operator for a single layer of the quantum circuit, the tensor product is used because quantum gates in the same layer act on non-overlapping sets of qubits.

Lemma 14. The overall unitary operator for the entire quantum circuit is ${U_{\text{circuit}}}^N = {U_l}^{(1)}{U_l}^{(2)} \cdots {U_l}^{(N)}$, N is the depth of the quantum circuit.

Proof. According to Definition 11, we let $|\psi\rangle$ be the initial state of the qubits, then

$$\left|\psi_1\right\rangle = {U_l}^{(1)}\left|\psi\right\rangle \tag{16}$$

represents the quantum state of the qubits after applying the unitary operator of the first layer, in the similar way, the quantum state of the qubits after applying the first two layers is

$$\left|\psi_2\right\rangle = {U_l}^{(2)}\left|\psi_1\right\rangle = {U_l}^{(2)}{U_l}^{(1)}|\psi\rangle. \tag{17}$$

So after applying the N layers in the circuit, the final quantum state of the qubits is

$$\begin{aligned} |\psi_{\text{final}}\rangle &= {U_l}^{(N)}{U_l}^{(N-1)} \cdots {U_l}^{(1)}|\psi\rangle \\ &= {U_l}^{(1)}{U_l}^{(2)} \cdots {U_l}^{(N)}|\psi\rangle. \end{aligned} \tag{18}$$

Thus, the overall unitary operator for the entire quantum circuit is

$${U_{\text{circuit}}}^N = {U_l}^{(1)}{U_l}^{(2)} \cdots {U_l}^{(N)}. \tag{19}$$

3. Clifford Quantum Cellular Automaton

3.1. Quantum Cellular Automaton

A cellular automaton (CA) consists of a regular grid of cells, each in one of a finite number of states. The grid can have any finite number of dimensions (e.g., 1D, 2D, etc.). Every cell has an initial state, and the state of each cell evolves over discrete time steps according to fixed, local rules, all cells in the grid update their states simultaneously at each time step. The new state of each cell depends on its current state and the states of its neighboring cells.

A quantum cellular automaton (QCA) is a lattice-based quantum system where each cell represents a finite-dimensional quantum state. A cell can be in multiple states simultaneously, because of the principle of superposition. The global state of the system evolves in discrete time steps by unitary

DOI: 10.54254/2753-8818/92/2025.22378

operators, which ensures the evolution is reversible. The new state of a cell depends on its current state and the states of its neighboring cells.

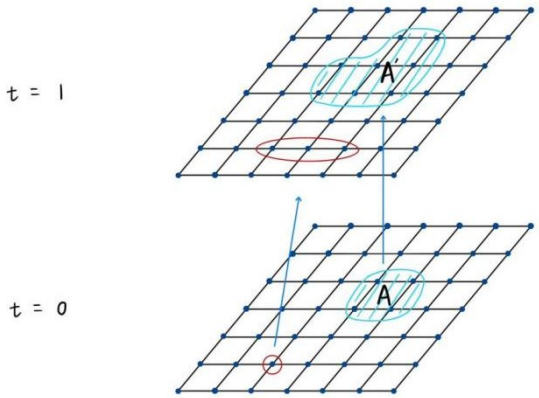

Figure 2: How QCA Works

In Figure 2, the points in the lattice are cells (qubits), A is the region that contains a set of cells in the lattice at the initial time step (t = 0), the quantum state of this region is the combined state of all qubits within A at t = 0. A' is the evolved region of A at t = 1, the quantum state in A' is the result of applying the unitary operator to the quantum state of A. If there is a matrix associated with every cell or group of cells, then the matrix at t = 0 will be transformed into another matrix at t = 1 under the application of the unitary operator of QCA.

Lemma 15. The QCA dynamics, defined as $\alpha(A) = U^*AU$, is a homomorphism, where A is any $n \times n$ matrix and U is a unitary operator representing the global evolution of the QCA.

Proof. We need to show that α satisfies preservation of matrix multiplication: $\alpha(AB) = \alpha(A)\alpha(B)$, where A and B are any $n \times n$ matrices.

Left-Hand Side (LHS):

$$\alpha(AB) = U^*(AB)U, \tag{20}$$

Right-Hand Side (RHS):

$$\begin{aligned} \alpha(A)\alpha(B) &= (U^*AU)(U^*BU) \\ &= U^*A(UU^*)BU \\ &= U^*ABU. \end{aligned} \tag{21}$$

So LHS is equal to RHS, which means that α preserves matrix multiplication. In conclusion, the QCA dynamics $\alpha(A) = U^*AU$ is a homomorphism.

Any 2×2 matrix can be written as $a_1I + a_2X + a_3Y + a_4Z$, $a_1, a_2, a_3, a_4 \in \mathbb{C}$, and I is the identity matrix, X, Y, Z are Pauli matrices as mentioned in Definition 6. We denote the dynamics of a QCA by $\alpha: A \to \alpha(A)$, A is any matrix and α is linear transformation, which maps a matrix $a_1I + a_2X + a_3Y + a_4Z$ to a new matrix $a_1\alpha(I) + a_2\alpha(X) + a_3\alpha(Y) + a_4\alpha(Z)$. We know that $\alpha(I) = I$, if we can figure out where α maps X, Y and Z to, then we can figure out where α maps all the matrices to. Actually, we just need to know $\alpha(X)$ and $\alpha(Z)$, because $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = iXZ$ and because of Lemma 15, then $\alpha(Y) = i\alpha(X)\alpha(Z)$. So if we know $\alpha(X)$ and $\alpha(Z)$, then we know $\alpha(Y)$. Thus, if we know $\alpha(X)$ and $\alpha(Z)$, then we know what the new matrix $a_1\alpha(I) + a_2\alpha(X) + a_3\alpha(Y) + a_4\alpha(Z)$ exactly is. To relate to Section 2.5, quantum circuit is a special class of QCA, but not all QCA comes from quantum circuits. In the QCA dynamics $\alpha(A) = U^*AU$, if U is the overall unitary operator of the quantum circuit, then this QCA comes from quantum circuit.

DOI: 10.54254/2753-8818/92/2025.22378

3.2. Clifford Quantum Cellular Automaton

Definition 16. A Clifford Quantum Cellular Automaton (Clifford QCA) is a specific type of Quantum Cellular Automaton (QCA). This evolution of system is controlled by a global unitary operator U, constructed by local Clifford gates, ensuring locality. And the system is reversible, the state of the system at any previous time step can be uniquely determined from its state at a later time step. Let $\mathcal{P}_n$ be the Pauli group on n-qubits, consisting of all tensor products of Pauli operators $\{I, X, Y, Z\}$ with phase factors ± 1, $\pm i$. For Clifford QCA,

$$\alpha(P) = U^* P U \in \mathcal{P}_n, \ \forall P \in \mathcal{P}_n,$$

where U is the global unitary operator. This means that for any Pauli operator P, its image $\alpha(P)$ is also a Pauli operator.

4. Results

4.1. QCA and Automorphism

Definition 17. An automorphism of a group G is an isomorphism from G to itself. If f is the function such that:

$$1.\ f: G \to G.$$

$$2.\ f(x * y) = f(x) * f(y).$$

$$3.\ f \text{ is bijective.}$$

Theorem 18. The conjugation by an invertible matrix is an automorphism.

Proof. Let $M_n(\mathbb{F})$ be the group that contains $n \times n$ matrices over the field $\mathbb{F}$. And let B be an $n \times n$ invertible matrix, A is any $n \times n$ matrix, then we define the map: $\varphi_B(A) = BAB^{-1}$. If this map satisfy the following, then it is an automorphism:

$$1.\ \varphi_B: M_n(\mathbb{F}) \to M_n(\mathbb{F}).$$

$$2.\ \varphi_B(AC) = \varphi_B(A)\varphi_B(C), \text{ where } C \text{ is any } n \times n \text{ matrix.}$$

$$3.\ \varphi_B \text{ is bijective.}$$

1. To prove $\varphi_B: M_n(\mathbb{F}) \to M_n(\mathbb{F})$: We know that A is an $n \times n$ matrix, B is an $n \times n$ invertible matrix, and B^{-1} is also an $n \times n$ invertible matrix, so the product BAB^{-1} is also an n by n matrix. $A \in M_n(\mathbb{F})$, and $BAB^{-1} \in M_n(\mathbb{F})$, so the map $\varphi_B(A) = BAB^{-1}$ satisfies $\varphi_B: M_n(\mathbb{F}) \to M_n(\mathbb{F})$.
2. To prove $\varphi_B(AC) = \varphi_B(A)\varphi_B(C)$, where C is any $n \times n$ matrix:Left-Hand Side (LHS):

$$\varphi_B(AC) = BACB^{-1}, \tag{22}$$

Right-Hand Side (RHS):

$$\begin{aligned} \varphi_B(A)\varphi_B(C) &= \left(BAB^{-1}\right)\left(BCB^{-1}\right) \\ &= BA\left(B^{-1}B\right)CB^{-1} \\ &= BACB^{-1}. \end{aligned} \tag{23}$$

So LHS is equal to RHS, which means that $\varphi_B(AC) = \varphi_B(A)\varphi_B(C)$.

3. To prove that φ_B is bijective, we need to show

- Injectivity: If $\varphi_B(A) = \varphi_B(C)$, then $A = C$.

DOI: 10.54254/2753-8818/92/2025.22378

Suppose $BAB^{-1} = BCB^{-1}$, then multiplying both sides with B^{-1} on the left and B on the right:

$$\begin{aligned} B^{-1}\left(BAB^{-1}\right)B &= B^{-1}\left(BCB^{-1}\right)B \\ A &= C. \end{aligned} \tag{24}$$

So φ_B is injective.

- Surjectivity: Given any matrix D, we need to find some A such that $\varphi_B(A) = D$, i.e.,

$$\begin{aligned} BAB^{-1} &= D \\ A &= B^{-1}DB. \end{aligned} \tag{25}$$

Since A exists for any D, so φ_B is surjective.

Thus, φ_B is bijective.

In conclusion, the map φ_B is an automorphism, so the conjugation by an invertible matrix is an automorphism.

Lemma 19. Quantum cellular automaton is an automorphism.

Proof. According to Lemma 15, we know that the QCA dynamics $\alpha(A) = U^*AU$ is a homomorphism, where A is any $n \times n$ matrix, and U is an $n \times n$ unitary operator. We only need to prove that $\alpha(A): M_n(\mathbb{F}) \to M_n(\mathbb{F})$ and $\alpha(A)$ is bijective.

1. The mapping preserves the space: A is an $n \times n$ matrix, U is an $n \times n$ unitary matrix, U^* is also an $n \times n$ unitary matrix, so U^*AU is an $n \times n$ matrix. $A \in M_n(\mathbb{F})$ and $U^*AU \in M_n(\mathbb{F})$, so $\alpha(A): M_n(\mathbb{F}) \to M_n(\mathbb{F})$, which means $\alpha(A)$ preserves the space.
2. The mapping is bijective: Since U is unitary, we define the inverse of α as $\alpha^{-1}(A) = UAU^*$. Then, we need to check α^{-1} is indeed the inverse:

$$\begin{aligned} \alpha^{-1}(\alpha(A)) &= U(U^*AU)U^* \\ &= A. \\ \alpha\left(\alpha^{-1}(A)\right) &= U^*(UAU^*)U \\ &= A. \end{aligned} \tag{26}$$

Thus, α is bijective. So QCA is an automorphism.

4.2. Conjugation by a Quantum Circuit

Theorem 20. The conjugation by a (finite depth) quantum circuit is a quantum cellular automaton.

Proof. Let U be a unitary matrix, which represents a quantum circuit, and A be a local operator. So we define the conjugation by a quantum circuit as $\varphi(A): A \to UAU^{-1} = UAU^*$. We suppose that A is supported in region X, which means that A only acts on qubits nontrivially within X, and A acts as the identity outside of X. If Y is disjoint from X, then A commutes with any operator supported in Y. Firstly, we only focus on the case when U is a single-layer circuit. We assume that $U = \prod_\gamma G_\gamma$, where G_γ represents the quantum gate in quantum circuit, there are finite many G_γ intersect with A, and the others don't intersect with A, so all G_γ commute with A except finitely many G_γ that intersect with A. Let the support of G_γ be Z, so we have

$$\begin{aligned} UAU^* &= \textstyle\prod_\gamma G_\gamma \; A \; (\prod_\gamma G_\gamma)^* \\ &= \textstyle\prod_\gamma G_\gamma \; A \; \prod_\gamma G_\gamma^* \\ &= \textstyle\prod_{Z\cap X\neq\emptyset} G_\gamma \, A \; \prod_{Z\cap X\neq\emptyset} G_\gamma^*. \end{aligned} \tag{27}$$

DOI: 10.54254/2753-8818/92/2025.22378

The support of UAU^* is the union of X and the support of all G_γ that intersect with A. And we assume that the support of G_γ has bounded diameter that is less than r, so for G_γ that intersect with A, the farthest distance between the boundary of X and the point on the support of G_γ is less than the bounded diameter of support of G_γ, which is also less than r. So UAU^* is supported within $B_r(X) = \{y \text{ is the point} \mid d(y,X) < r\}$.

Then, in a similar way, when U has multiple layers, then the region where UAU^* is supported expands with each layer, after n layers, the UAU^* is supported within a neighborhood of X that is a ball of radius nr, denoted as $B_{nr}(X) = \{z \text{ is the point} \mid d(z,X) < nr\}$, where r represents the quantity of expansion of region per layer.

All in all, A is supported in region X, then UAU^* is supported in region $B_{nr}(X)$, and $B_{nr}(X)$ always contains X, which means that UAU^* is supported in a neighborhood of X. Thus, the conjugation by (finite depth) quantum circuit is locality-preserving, so the conjugation by a (finite depth) quantum circuit is a quantum cellular automaton.

If the operation of a QCA can be decomposed into the operations of several local quantum circuits, then this QCA can be written as the conjugation by the quantum circuits, so not all QCAs are the conjugation by the quantum circuit.

$SWAP$ is a quantum gate, swap gate swaps two qubits: $|00\rangle \to |00\rangle$, $|01\rangle \to |10\rangle$, $|10\rangle \to |01\rangle$, $|11\rangle \to |11\rangle$. Swap gate can be represented by a unitary matrix $SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$. According to Definition 10, we have $SWAP = CNOT_{12}\, CNOT_{21}\, CNOT_{12}$, $CNOT_{12}$ and $CNOT_{21}$ are unitary matrices, and $CNOT$ is a quantum gate, $SWAP$ can be written as the product of three quantum gates, so $SWAP$ is a quantum circuit.

Lemma 21. $SWAP$ is the conjugation by a quantum circuit.

Proof. By the definition, $SWAP: U \otimes V \to V \otimes U$, where U and V are two operators. If we prove that $SWAP: U \otimes V \to C(U \otimes V)C^*$, where C is a quantum circuit, and $C(U \otimes V)C^* = V \otimes U$, then $SWAP$ is the conjugation by a quantum circuit. We know that $SWAP$ can be represented as a unitary matrix, we find that $SWAP^* = SWAP$. We establish that $C = SWAP$, so $C(U \otimes V)C^* = SWAP(U \otimes V)SWAP^* = SWAP(U \otimes V)SWAP = V \otimes U$, so $SWAP$ is the conjugation by a quantum circuit.

4.3. QC is a Subgroup of QCA

Proposition 22. $QC \subsetneq QCA$, where QC represents the set of conjugations by the quantum circuits, QCA represents the set of QCAs. Besides, QC is a subgroup of QCA, denoted as $QC \leq QCA$.

Proof. According to Lemma 19, the set of QCAs is the set of automorphisms, which forms a group under composition, so the set of QCAs is a group. As we mentioned before, some QCAs can be decomposed by into several local quantum circuits, but some QCAs cannot, so $QC \subsetneq QCA$. And let B be an $n \times n$ unitary matrix, and A is any $n \times n$ matrix, so the conjugation by a quantum circuit is denoted as $\varphi_B(A) = BAB^{-1}$, the inverse of this is $\varphi_B^{-1}(A) = B^{-1}AB$, because B is an $n \times n$ unitary matrix, so the set of conjugations by the quantum circuits is closed under inverse. And let $\varphi_M(A) = MAM^{-1}$, $\varphi_N(A) = NAN^{-1}$ be the elements in the set of conjugations by the quantum circuits, where M and N are $n \times n$ unitary matrices, and A is any $n \times n$ matrix. $\varphi_N(\varphi_M(A)) = NMAM^{-1}N^{-1} = (NM)A(NM)^{-1}$, since the matrix NM is an $n \times n$ unitary matrix, so the set of conjugations by the quantum circuits is closed under multiplication. Thus, the set of conjugations by the quantum circuits is a subgroup of set of QCAs, denoted as $QC \leq QCA$.

DOI: 10.54254/2753-8818/92/2025.22378

4.4. QC is a Normal Subgroup of QCA

Proposition 23. QC is a normal subgroup of QCA, denoted as $QC \trianglelefteq QCA$, where QC represents the set of conjugations by the quantum circuits and QCA represents the set of QCAs.

Proof. Let α be a QCA, β be the conjugation by quantum circuit. We need to prove that $\alpha\beta\alpha^{-1} \in QC$, which means that $\alpha\beta\alpha^{-1}$ is the conjugation by quantum circuit. Suppose $\beta(A) = BAB^{-1}$, where B is an $n \times n$ unitary matrix that represents the quantum circuit, A is any $n \times n$ matrix, O is the matrix on qubits. We have

$$\alpha\beta\alpha^{-1}(O) = \alpha\left(B\alpha^{-1}(O)B^{-1}\right), \tag{28}$$

because of Lemma 19, we have

$$\begin{aligned} \alpha\beta\alpha^{-1}(O) &= \alpha(B)\alpha\left(\alpha^{-1}(O)\right)\alpha\left(B^{-1}\right) \\ &= \alpha(B)O\alpha\left(B^{-1}\right), \end{aligned} \tag{29}$$

because of Lemma 19, so $\alpha(B^{-1}) = \alpha(B)^{-1}$, so

$$\alpha\beta\alpha^{-1}(O) = \alpha(B)O\alpha(B)^{-1}. \tag{30}$$

We know that $n \times n$ unitary matrix B represents the quantum circuit, α operates on a quantum circuit B, meaning that α operates on every quantum gate in circuit, in each layer, quantum gates will act on more qubits, the number of qubits every gate acts on is limited. So $\alpha(B)$ is also a quantum circuit, but the number of qubits that each quantum gate acts on has increased. We find that $\alpha\beta\alpha^{-1}(O) = \alpha(B)O\alpha(B)^{-1}$, where $\alpha(B)$ is a quantum circuit and O is the matrix on qubits, so $\alpha(B)O\alpha(B)^{-1}$ is the conjugation by the quantum circuit, so QC is a normal subgroup of QCA, denoted as $QC \trianglelefteq QCA$, where QC represents the set of conjugations by the quantum circuits and QCA represents the set of QCAs.

4.5. QCA/QC is an Abelian Group

Definition 24. The group G is abelian if $x * y = y * x$ for all $x, y \in G$.

Proposition 25. QCA/QC is an abelian group, where QCA represents the set of QCAs, and QC represents the set of conjugations by the quantum circuits.

Proof. Suppose $\alpha, \beta \in QCA$, according to Proposition 23, we have $QCA/QC = \{\varepsilon QC \mid \varepsilon \in QCA\}$. We suppose that two elements in this group are αQC and βQC, to show that QCA/QC is an abelian group, we need to show that $(\alpha QC)(\beta QC) = (\beta QC)(\alpha QC)$, equivalent to showing that $(\alpha\beta)QC = (\beta\alpha)QC$, which means that we need to show that $\alpha\beta = A\beta B\alpha C \simeq \beta\alpha$, where $A, B, C \in QC$. According to Lemma 21, we have $SWAP \in QC$.

DOI: 10.54254/2753-8818/92/2025.22378

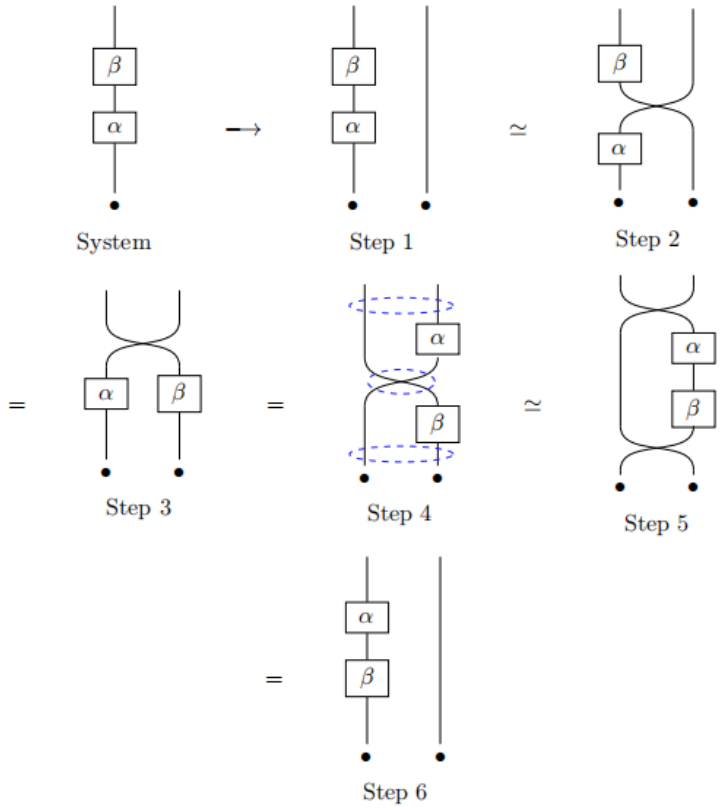

Figure 3: The Operations on a System

In Figure 3, the points represent qubits, and α acts on qubit first and β acts on qubit secondly, then we have a system. Next, we do the stabilization on this system, meaning that the original system does the tensor product with another system that only contains identity operators. Then, though elements in the new whole system have one more dimension, they are essentially unchanged, as shown in Step 1. Subsequently, we insert a $SWAP$ in Step 2, the new system is equal to the system shown in Step 3, which is also equal to the system shown in Step 4. Then, we insert three $SWAP$ in three places circled with dashed line, then we get the system in Step 5, which is equal to the system shown in Step 6. The following is the process we do in Figure 3:

$$\begin{aligned}
\beta \circ \alpha \xrightarrow{Stabilization} & (\beta \otimes I) \circ (\alpha \otimes I) && \cdots\cdots \ Step\ 1 \\
& \cong (\beta \otimes I) \circ SWAP \circ (\alpha \otimes I) && \cdots\cdots \ Step\ 2 \\
& = SWAP \circ (I \otimes \beta) \circ (\alpha \otimes I) && \cdots\cdots \ Step\ 3 \\
& = SWAP \circ (\alpha \otimes I) \circ (I \otimes \beta) && \\
& = (I \otimes \alpha) \circ SWAP \circ (I \otimes \beta) && \cdots\cdots \ Step\ 4 \\
& = SWAP \circ (I \otimes \alpha) \circ (I \otimes \beta) \circ SWAP && \cdots\cdots \ Step\ 5 \\
& = (\alpha \otimes I) \circ (\beta \otimes I) && \cdots\cdots \ Step\ 6
\end{aligned} \tag{31}$$

We can see that the order of α and β is reversed in the first subsystem in step 6 compared to step 1, and only identity operators act on the second subsystem where we do stabilization. Thus, we find that $(\beta \otimes I) \circ (\alpha \otimes I)$ is equivalent to $(\alpha \otimes I) \circ (\beta \otimes I)$ by applying $SWAP$ operations, $A, B, C \in QC$, they are $SWAP$ operations here, so $\alpha\beta = A\beta B\alpha C \simeq \beta\alpha$, then QCA/QC is an abelian group.

DOI: 10.54254/2753-8818/92/2025.22378

5. Discussion

Our study explores QCA through group theory, offering new insights into its mathematical structure. While QCA has primarily been studied in the context of quantum computing and quantum information, its broader applications remain largely unexplored. One intriguing direction is whether QCA can be used as a computational tool to solve hard problems in group theory. Since group-theoretic methods help analyze QCA dynamics, it is natural to ask the reverse — can QCA provide novel solutions for problems like finite simple group classification or infinite group representations? If so, it could introduce new approaches to approach these problems that might be faster or more effective than classical methods. Future research should focus on establishing a formal connection between QCA models and algebraic structures, possibly leading to novel quantum algorithms that extend beyond conventional quantum algorithms.

References

[1] *Gregg Jaeger. Quantum information. Springer, 2007.*
[2] *Wolfgang Scherer. Mathematics of quantum computing. Vol. 11. Springer, 2019.*
[3] *Edgar F Codd. Cellular automata. Academic press, 2014.*
[4] *Terry Farrelly. "A review of quantum cellular automata". In: Quantum 4 (2020), p. 368.*
[5] *Michael Freedman and Matthew B Hastings. "Classification of quantum cellular automata". In: Communications in Mathematical Physics 376 (2020), pp. 1171–1222.*
[6] *Bei Zeng, Xie Chen, Duan-Lu Zhou, Xiao-Gang Wen, et al. Quantum information meets quantum matter. Springer, 2019.*
[7] *Benjamin Schumacher and Reinhard F Werner. "Reversible quantum cellular automata". In: arXiv preprint quant-ph/0405174 (2004).*
[8] *Jeongwan Haah. "Clifford quantum cellular automata: Trivial group in 2D and Witt group in 3D". In: Journal of Mathematical Physics 62.9 (2021).*
[9] *John F Humphreys. A course in group theory. Vol. 6. OUP Oxford, 1996.*
[10] *William Raymond Scott. Group theory. Courier Corporation, 2012.*