Theoretical Foundation for Equivalence Checking of Quantum Circuits

Canh Minh Do*, Kazuhiro Ogata

Japan Advanced Institute of Science and Technology, 1-8 Asahidai, Nomi, Japan

Abstract

Quantum circuits are typically used to design quantum algorithms at a high abstraction level without considering specific hardware restrictions. To execute quantum circuits on an actual quantum device, they must undergo a compilation process, transforming the high abstraction level into a low abstraction level that conforms to all restrictions imposed on the target device. As a result, the original quantum circuits and their compiled counterparts differ significantly. Therefore, it is crucial to verify the equivalence of two quantum circuits constructed from quantum gates based on their functionality. This paper presents a theoretical foundation for checking the equivalence of quantum circuits based on which an algorithm is constructed. The equivalence of quantum circuits can be reduced to matrix equivalence modulo a global phase. To achieve this, we compare each column vector of two matrices modulo the same global phase, making it significantly faster than the actual matrix equivalence check, especially in cases of non-equivalent quantum circuits.

Keywords

Observable Equivalence, Density Matrices, Equivalence Checking, Quantum Circuits

1. Introduction

Quantum computing is a rapidly emerging technology that uses the principles of quantum mechanics to solve complex problems beyond the capabilities of current classical computing. Several quantum algorithms have been proposed, showing significant improvements over classical algorithms, such as Shor's fast algorithms for discrete logarithms and factoring in 1994 [1]. Although practical quantum computers capable of running such algorithms effectively are not yet available, recent exponential investments from big companies like IBM, Google, Microsoft, and Intel bring the future of the quantum era within closer reach.

Quantum circuits are a natural model of quantum computation, comprising qubits and quantum operations (e.g., quantum gates), that can be used to design and implement quantum algorithms. However, quantum circuits are typically used to design quantum algorithms at a high abstraction level without considering specific hardware restrictions. To execute the quantum circuits on an actual quantum device, they have to undergo a *compilation* process, transforming the high abstraction level to a low abstraction level that conforms to all restrictions

The 2nd International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols, November 11, 2023, Brisbane, Australia

*Corresponding author.

canhdo@jaist.ac.jp (C. M. Do); ogata@jaist.ac.jp (K. Ogata)

0000-0002-1601-4584 (C. M. Do); 0000-0002-4441-3259 (K. Ogata)

imposed on the targeted device. More precisely, this compilation process has several key aspects as follows. Firstly, quantum devices natively support only a limited set of quantum operations. Consequently, quantum circuits intended for the target device must be expressed using only these native quantum operations. This requires a *decomposition* (or *translation*) step of non-native quantum operations into sequences of native ones [2, 3, 4]. Secondly, logical qubits used in quantum circuits have to be mapped to physical qubits on the target device. However, this mapping cannot be arbitrary because the target device imposes restrictions on which physical qubits can interact with each other. To achieve this, a *mapping* (or *routing*) step is required, which involves adding SWAP and Hadmard gates to quantum circuits [5, 6, 7]. Lastly, after the decomposition and mapping steps, the size of quantum circuits tends to increase, posing challenges for their execution on quantum devices due to noise and decoherence effects. Therefore, an *optimization* step is required to reduce the size of quantum circuits in terms of the number of quantum gates [8, 9, 10]. As a result of these processes, the quantum circuit defined at a high abstraction level and its compiled counterpart defined at a low abstraction level are significantly different. Therefore, it is crucial to verify the equivalence of two quantum circuits based on their functionality.

The functionality of quantum circuits can be described by a sequence of quantum gates, which are represented by unitary matrices. Given two quantum circuits constructed from quantum gates in the form of $U = U_m \ldots U_0$ and $U' = U'_{m'} \ldots U'_0$, the two quantum circuits are considered equivalent if U is equal to U' modulo a global phase, which is physically unobservable [11]. Directly comparing U and U' is inefficient because it requires costly matrix-matrix multiplications $U_m \ldots U_0$ and $U'_{m'} \ldots U'_0$ to obtain U and U' for comparison. Moreover, if U is significantly different from U', constructing the entire elements of both matrices is unnecessary. Instead, we can compare each column of two matrices modulo a global phase. Concretely, for each basis vector $|\phi_i\rangle$ in an orthonormal basis of a Hilbert space, if $U|\phi_i\rangle$ is equal to $U'|\phi_i\rangle$ modulo the same global phase, then the two quantum circuits are equivalent. It is important to note that we may need a few iterations to check that some quantum circuits are not equivalent in cases of non-equivalent quantum circuits, making it significantly faster than the actual matrix equivalence check. We present a theoretical foundation for checking the equivalence of quantum circuits with a theorem to guarantee the correctness of our approach. An algorithm is also constructed based on our theorem.

The rest of the paper is organized as follows: Sect. 2 provides the basics of quantum mechanics related mostly to linear algebra, Sect. 3 proposes a theoretical foundation of equivalence checking of quantum circuits in this work based on which an algorithm is constructed, Sect. 4 presents some existing work, and Sect. 5 concludes the paper with some pieces of future work.

2. Basic Quantum Mechanics

In classical computing, the fundamental unit of information is a bit whose value is either 0 or 1. In quantum computing, the counterpart is a *quantum bit* or *qubit*, which has two basis states, conventionally written in Dirac notation [12] as $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$, which denote two column vectors $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}0\\1\end{pmatrix}$, respectively. In quantum theory, a general state of a quantum system is a superposition or linear combination of basis states. A quantum state is a unit vector in a Hilbert space $\mathcal{H}$, which is a vector space equipped with an inner product such that each Cauchy sequence has a limit. The state of a single qubit is $|\psi\rangle = \alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle$, where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. States can be represented by column complex vectors as follows: $|\psi\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix} = \alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle$, where $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$ forms an orthonormal basis of the two-dimensional complex vector space.

The basis $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$ is called as the *standard* basis. Besides, there are some other orthonormal bases studied in the literature, such as *diagonal* (or *dual*, or *Hadamard*) basis consisting of the following vectors:

$$|+\rangle = \tfrac{1}{\sqrt{2}}(|\mathbf{0}\rangle + |\mathbf{1}\rangle) \text{ and } |-\rangle = \tfrac{1}{\sqrt{2}}(|\mathbf{0}\rangle - |\mathbf{1}\rangle)$$

The evolution of a closed quantum system can be performed by a unitary transformation. If the state of a qubit is represented by a column vector, then a unitary transformation $\boldsymbol{U}$ can be represented by a complex-value matrix such that $\boldsymbol{U}\boldsymbol{U}^\dagger = \boldsymbol{U}^\dagger\boldsymbol{U} = \boldsymbol{I}$ or $\boldsymbol{U}^\dagger = \boldsymbol{U}^{-1}$, where $\boldsymbol{U}^\dagger$ is the conjugate transpose of $\boldsymbol{U}$. $\boldsymbol{U}$ acts on the Hilbert space $\mathcal{H}$ transforming a state $|\psi\rangle$ to a state $|\psi'\rangle$ by a matrix multiplication such that $|\psi'\rangle = \boldsymbol{U}|\psi\rangle$. There are some frequently used quantum gates in applications: the Hadamard gate $\boldsymbol{H}$, the identity gate $\boldsymbol{I}$, the Pauli gates $\boldsymbol{X}$, $\boldsymbol{Y}$, and $\boldsymbol{Z}$, and the controlled-NOT gate $\boldsymbol{CX}$. Note that the $\boldsymbol{CX}$ gate performs on two qubits, while the remaining gates perform on a single qubit. Their matrix representations are as follows:

$$\boldsymbol{I}_2 = \begin{pmatrix}1 & 0 \\ 0 & 1\end{pmatrix}, \qquad \boldsymbol{X} = \begin{pmatrix}0 & 1 \\ 1 & 0\end{pmatrix}, \qquad \boldsymbol{Y} = \begin{pmatrix}0 & -i \\ i & 0\end{pmatrix},$$

$$\boldsymbol{Z} = \begin{pmatrix}1 & 0 \\ 0 & -1\end{pmatrix}, \qquad \boldsymbol{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 \\ 1 & -1\end{pmatrix}, \qquad \boldsymbol{CX} = \begin{pmatrix}1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0\end{pmatrix}.$$

where i is the imaginary unit. For example, the Hadamard gate on a single qubit performs the mapping $|\mathbf{0}\rangle \mapsto \frac{1}{\sqrt{2}}(|\mathbf{0}\rangle + |\mathbf{1}\rangle)$ and $|\mathbf{1}\rangle \mapsto \frac{1}{\sqrt{2}}(|\mathbf{0}\rangle - |\mathbf{1}\rangle)$. The controlled-NOT gate on pairs of qubits performs the mapping $|\mathbf{00}\rangle \mapsto |\mathbf{00}\rangle, |\mathbf{01}\rangle \mapsto |\mathbf{01}\rangle, |\mathbf{10}\rangle \mapsto |\mathbf{11}\rangle, |\mathbf{11}\rangle \mapsto |\mathbf{10}\rangle$, which can be understood as inverting the second qubit (referred to as the *target*) if and only if the first qubit (referred to as the *control*) is one.

For multiple qubits, we use the tensor product of Hilbert spaces. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces. Their tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$ is defined as a vector space consisting of linear combinations of the vectors $|\psi_1\psi_2\rangle = |\psi_1\rangle|\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, where $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$. Systems of two or more qubits may be in *entangled* states, meaning that states of qubits are correlated and inseparable. Entanglement shows that an entangled state of two qubits cannot be expressed as a tensor product of single-qubit states. We can use $\boldsymbol{H}$ and $\boldsymbol{CX}$ gates to create entangled states as follows: $\boldsymbol{CX}((\boldsymbol{H} \otimes \boldsymbol{I})|\mathbf{00}\rangle) = \frac{1}{\sqrt{2}}(|\mathbf{00}\rangle + |\mathbf{11}\rangle)$.

Let $|\psi\rangle$ be a quantum state and $\theta \in [0, 2\pi)$. In quantum mechanics, the state $e^{i\theta} |\psi\rangle$ is considered to be physically equal to $|\psi\rangle$ with respect to the global phase factor $e^{i\theta}$. From an observable perspective, two states are undistinguishable if they differ only by a global phase. We can use density matrices $|\psi\rangle\langle\psi|$ to present quantum states $|\psi\rangle$ from which we can eliminate the global phase factor as follows: $e^{i\theta} |\psi\rangle (e^{i\theta} |\psi\rangle)^\dagger = e^{i\theta} |\psi\rangle e^{-i\theta} \langle\psi| = |\psi\rangle\langle\psi|$.

3. Equivalence Checking of Quantum Circuits

This section presents the theoretical foundation of equivalence checking of quantum circuits by introducing a theorem based on which an algorithm is constructed.

3.1. Theoretical Foundation

We propose a method for checking the equivalence of quantum circuits constructed from quantum gates based on their functionality. We suppose that quantum circuits operate on quantum states in a Hilbert space $\mathcal{H}$ with n qubits. The unitary evolution of quantum systems is described by unitary matrices whose size is $2^n \times 2^n$. We first define the equivalence checking problem of quantum circuits.

Definition 3.1 (Equivalence checking problem). Given two quantum circuits represented by unitary matrices, $U = U_m \dots U_0$ and $U' = U'_{m'} \dots U'_0$, the equivalence checking problem of U and U' is asked to check whether $U = e^{i\theta} U'$ for some $\theta \in [0, 2\pi)$.

We call $e^{i\theta}$ a global phase that is physically unobservable [11]. In quantum mechanics, quantum states that differ only by a global phase are physically indistinguishable and equivalent under observation [11]. Hence, we define observable equivalence for quantum states as follows:

Definition 3.2 (Observable equivalence for quantum states). $|\psi\rangle \approx |\psi'\rangle$ (or $|\psi\rangle \approx_\theta |\psi'\rangle$ to make it clear from the context) is defined as $|\psi\rangle = e^{i\theta} |\psi'\rangle$ for some $\theta \in [0, 2\pi)$.

To check $|\psi\rangle \approx |\psi'\rangle$, we can check the equality of their density matrices $|\psi\rangle\langle\psi|$ and $|\psi'\rangle\langle\psi'|$. Because using density matrices to represent quantum states can eliminate the global phase, it is a handy trick to check the observable equivalence of two quantum states by comparing their density matrices. This result is derived from the following lemma.

Lemma 3.1. $|\psi\rangle \approx |\psi'\rangle$ if and only if $|\psi\rangle\langle\psi| = |\psi'\rangle\langle\psi'|$.

Proof. For the '*only if*' part (the ⇒ direction), it is straightforward.

We now consider the '*if*' part (the ⇐ direction). Let $\{|\phi_0\rangle, \dots, |\phi_i\rangle, \dots |\phi_{2^n-1}\rangle\}$ be an orthonormal basis of $\mathcal{H}$ with n dimension. There exists $c_0, \dots, c_i, \dots, c_{2^n-1}$ such that $|\psi\rangle = c_0 |\phi_0\rangle + \dots + c_i |\phi_i\rangle + \dots + c_{2^n-1} |\phi_{2^n-1}\rangle$ and $|c_0|^2 + \dots + |c_i|^2 + \dots + |c_{2^n-1}|^2 = 1$. Similarly, we have $|\psi'\rangle = c'_0 |\phi_0\rangle + \dots + c'_i |\phi_i\rangle + \dots + c'_{2^n-1} |\phi_{2^n-1}\rangle$. Let A and A' be $2^n \times 2^n$ matrices denoting $|\psi\rangle\langle\psi|$ and $|\psi'\rangle\langle\psi'|$, respectively. The elements of matrix A are calculated as follows:

$$\begin{aligned} a_{ij} &= \langle\phi_i| A |\phi_j\rangle \\ &= \langle\phi_i|\psi\rangle \langle\psi|\phi_j\rangle \end{aligned}$$

$$= c_i c_j^*$$

Similarly, the elements of matrix A' are calculated as follows: $a'_{ij} = c'_i c'^*_j$.

We have $a_{ij} = a'_{ij}$ for any $i, j \in [0 \dots 2^n - 1]$ because of A = A' from the assumption. Let us consider $a_{ii} = a'_{ii}$ as follows:

$$\begin{aligned}
& a_{ii} = a'_{ii} \\
\Leftrightarrow\ & c_i c_i^* = c'_i c'^*_i \\
\Leftrightarrow\ & re^{i\alpha}(r.e^{i\alpha})^* = r'e^{i\alpha'}(r'e^{i\alpha'})^* && \text{(by the exponential form of complex numbers)} \\
\Leftrightarrow\ & r = r' && \text{(because r and r' are non-negative numbers)}
\end{aligned}$$

We have $c_i = re^{i\alpha}$, $c'_i = r'e^{i\alpha'}$, and $r = r'$, where $i \in [0 \dots 2^n - 1]$. Let us consider two cases:

- If $r = r' = 0$, then it is immediate that $c_i = e^{i\theta_i} c'_i$ for some $\theta_i \in [0, 2\pi)$.
- If $r = r' \neq 0$, then we have $\frac{c_i}{c'_i} = \frac{re^{i\alpha}}{r'e^{i\alpha'}} = e^{i(\alpha - \alpha')} = e^{i\theta_i}$, where $\theta_i = \alpha - \alpha'$. Then, we have $c_i = e^{i\theta_i} c'_i$ for some $\theta_i \in [0, 2\pi)$.

Therefore, for all $i \in [0 \dots 2^n - 1]$, there exists $\theta_i \in [0, 2\pi)$ such that $c_i = e^{i\theta_i} c'_i$. Now let us consider $a_{ij} = a'_{ij}$ as follows:

$$\begin{aligned}
& a_{ij} = a'_{ij} \\
\Leftrightarrow\ & c_i c_j^* = c'_i c'^*_j \\
\Leftrightarrow\ & e^{i\theta_i} c'_i (e^{i\theta_j} c'_j)^* = c'_i c'^*_j && \text{(by the result above)} \\
\Leftrightarrow\ & e^{i(\theta_i - \theta_j)} c'_i c'^*_j = c'_i c'^*_j
\end{aligned}$$

Therefore, we have $\theta_i = \theta_j$ for any $c_i, c_j \neq 0$. It indicates that $|\psi\rangle = e^{i\theta} |\psi'\rangle$ for some $\theta \in [0, 2\pi)$. From Definition 3.2, we have $|\psi\rangle \approx |\psi'\rangle$. □

Recall to check the equivalence of quantum circuits U and U', we need to check whether $U = e^{i\theta} U'$ for some $\theta \in [0, 2\pi)$. We can use the following lemma to solve this problem.

Lemma 3.2. Let U and U' be $2^n \times 2^n$ unitary matrices, then $U = e^{i\theta} U'$ for some $\theta \in [0, 2\pi)$ if and only if $U |\psi\rangle \approx_\theta U' |\psi\rangle$ for any vector $|\psi\rangle \in \mathcal{H}$.

Proof. For the '*only if*' part (the ⇒ direction), for any $|\psi\rangle$, we have $U |\psi\rangle = e^{i\theta} U' |\psi\rangle$ for some $\theta \in [0, 2\pi)$ using the assumption. From Definition 3.2, we have $e^{i\theta} U' |\psi\rangle \approx U' |\psi\rangle$. Therefore, $U |\psi\rangle \approx_\theta U' |\psi\rangle$.

For the '*if*' part (the ⇐ direction), because $U |\psi\rangle \approx_\theta U' |\psi\rangle$ for any $|\psi\rangle$ from the assumption, we have $U |\psi\rangle = e^{i\theta} U' |\psi\rangle$ for some $\theta \in [0, 2\pi)$. Therefore, $U = e^{i\theta} U'$ for some $\theta \in [0, 2\pi)$. □

In Lemma 3.2, it is unfeasible to consider any vector $|\psi\rangle \in \mathcal{H}$ because there are infinite vectors in $\mathcal{H}$. Therefore, we introduce the following lemma to help us check whether $U = e^{i\theta}U'$ by considering only basis vectors in an orthonormal basis of $\mathcal{H}$. If the dimension of $\mathcal{H}$ is n, we need to consider at most 2^n basis vectors with respect to the same global phase.

Lemma 3.3. Let U and U' be $2^n \times 2^n$ matrices, then $U = e^{i\theta}U'$ for some $\theta \in [0, 2\pi)$ if and only if $U|\phi_i\rangle \approx_\theta U'|\phi_i\rangle$ for each basis vector $|\phi_i\rangle$ in an orthonormal basis of $\mathcal{H}$.

Proof. The '*only if*' part (the $\Rightarrow$ direction) is immediate from Lemma 3.2.

For the '*if*' part (the $\Leftarrow$ direction), let $\{|\phi_0\rangle, \dots, |\phi_i\rangle, \dots |\phi_{2^n-1}\rangle\}$ be an orthonormal basis of $\mathcal{H}$ with n dimension. For each basis vector ϕ_i, we have $U|\phi_i\rangle \approx_\theta U'|\phi_i\rangle$ from the assumption. From Definition 3.2, we have $U|\phi_i\rangle = e^{i\theta}U'|\phi_i\rangle$ for some $\theta \in [0, 2\pi)$. Therefore, for any complex number c_i, we have $Uc_i|\phi_i\rangle = e^{i\theta}U'c_i|\phi_i\rangle$ (1).

For arbitrary $|\psi\rangle \in \mathcal{H}$, there exists $c_0, \dots, c_i, \dots, c_{2^n-1}$ such that $|\psi\rangle = c_0|\phi_0\rangle + \dots + c_i|\phi_i\rangle + \dots + c_{2^n-1}|\phi_{2^n-1}\rangle$ and $|c_0|^2 + \dots + |c_i|^2 + \dots + |c_{2^n-1}|^2 = 1$. Because of (1), we have the following:

$$\begin{aligned} U|\psi\rangle &= Uc_0|\phi_0\rangle + \dots + Uc_i|\phi_i\rangle + \dots + Uc_{2^n-1}|\phi_{2^n-1}\rangle \\ &= e^{i\theta}U'c_0|\phi_0\rangle + \dots + e^{i\theta}U'c_i|\phi_i\rangle + \dots + e^{i\theta}U'c_{2^n-1}|\phi_{2^n-1}\rangle \\ &= e^{i\theta}U'(c_0|\phi_0\rangle + \dots + c_i|\phi_i\rangle + \dots + c_{2^n-1}|\phi_{2^n-1}\rangle) \\ &= e^{i\theta}U'|\psi\rangle \end{aligned}$$

for any $|\psi\rangle$ and θ. It means that $U|\psi\rangle \approx_\theta U'|\psi\rangle$ for any vector $|\psi\rangle$. Therefore, $U = e^{i\theta}U'$ by Lemma 3.2. □

Remark 3.1. Checking $U|\psi_i\rangle \approx_\theta U'|\psi_i\rangle$ is actually checking the observable equivalence of the i-th column vector of U and the i-th column vector of U' with respect to the phase θ.

Lemma 3.4. $U|\phi_i\rangle \approx_\theta U'|\phi_i\rangle$ for each basis vector $|\phi_i\rangle$ in an orthonormal basis of $\mathcal{H}$ if and only if $U|\phi_i\rangle \approx U'|\phi_i\rangle$ for each $|\phi_i\rangle$ and $U|\phi_i\rangle(U|\phi_j\rangle)^\dagger = U'|\phi_i\rangle(U'|\phi_j\rangle)^\dagger$ for each $|\phi_i\rangle$ and $|\phi_j\rangle$.

Proof. For the '*only if*' part (the $\Rightarrow$ direction), we have $U|\phi_i\rangle \approx U'|\phi_i\rangle$ for each basis vector $|\phi_i\rangle$ using the assumption. Moreover, we have $U|\phi_i\rangle = e^{i\theta}U'|\phi_i\rangle$ and $U|\phi_j\rangle = e^{i\theta}U'|\phi_j\rangle$ for each $|\phi_i\rangle$ and $|\phi_j\rangle$. Therefore, $U|\phi_i\rangle(U|\phi_j\rangle)^\dagger = e^{i\theta}U'|\phi_i\rangle(e^{i\theta}U'|\phi_j\rangle)^\dagger = U'|\phi_i\rangle(U'|\phi_j\rangle)^\dagger$

For the '*if*' part (the $\Leftarrow$ direction), we have $U|\phi_i\rangle = e^{i\theta_i}U'|\phi_i\rangle$ and $U|\phi_j\rangle = e^{i\theta_j}U'|\phi_j\rangle$ for each $|\phi_i\rangle$ and $|\phi_j\rangle$ using the first condition in the assumption. For the second condition in the assumption, we have as follows:

$$\begin{aligned} &U|\phi_i\rangle(U|\phi_j\rangle)^\dagger = U'|\phi_i\rangle(U'|\phi_j\rangle)^\dagger \\ \Leftrightarrow\ &e^{i\theta_i}U'|\phi_i\rangle(e^{i\theta_j}U'|\phi_j\rangle)^\dagger = U'|\phi_i\rangle(U'|\phi_j\rangle)^\dagger \\ \Leftrightarrow\ &e^{i(\theta_i-\theta_j)}U'|\phi_i\rangle(U'|\phi_j\rangle)^\dagger = U'|\phi_i\rangle(U'|\phi_j\rangle)^\dagger \end{aligned}$$

Therefore, we have $\theta_i = \theta_j$ for each $|\phi_i\rangle$ and $|\phi_j\rangle$. It indicates that $U|\phi_i\rangle \approx_\theta U'|\phi_i\rangle$ for each basis vector $|\phi_i\rangle$. □

Algorithm 1: Equivalence Checking of Quantum Circuits

```
input : $n$ – the dimension of a Hilbert space
        $U = U_m \dots U_0$ and $U' = U'_{m'} \dots U'_0$ – two quantum circuits
        $\{|\phi_0\rangle, \dots, |\phi_{2^n-1}\rangle\}$ – an orthonormal basis of a Hilbert space $\mathcal{H}$
        $\theta \in [0, 2\pi)$ – the phase
output: True ($U = e^{i\theta}U'$) or False ($U \neq e^{i\theta}U'$)
1 forall $|\phi_i\rangle \in \{|\phi_0\rangle, \dots, |\phi_{2^n-1}\rangle\}$ do
2     $|u_i\rangle = U_m \cdot (\dots(U_0 \cdot |\phi_i\rangle)\dots)$
3     $|u'_i\rangle = U'_{m'} \cdot (\dots(U'_0 \cdot |\phi_i\rangle)\dots)$
4     if $|u_i\rangle\langle u_i| \neq |u'_i\rangle\langle u'_i|$ then
5         return False
6     if $i \neq 0 \wedge |u_0\rangle\langle u_i| \neq |u'_0\rangle\langle u'_i|$ then
7         return False
8 return True
```

Based on Lemma 3.1, Lemma 3.3 and Lemma 3.4, we introduce the following theorem to check whether $U = e^{i\theta}U'$ for some $\theta \in [0, 2\pi)$.

Theorem 3.5. Let U and U' be $2^n \times 2^n$ matrices, then $U = e^{i\theta}U'$ for some $\theta \in [0, 2\pi)$ if and only if $U|\phi_i\rangle (U|\phi_i\rangle)^\dagger = U'|\phi_i\rangle (U'|\phi_i\rangle)^\dagger$ for each basis vector ϕ_i and $U|\phi_i\rangle (U|\phi_j\rangle)^\dagger = U'|\phi_i\rangle (U'|\phi_j\rangle)^\dagger$ for each $|\phi_i\rangle$ and $|\phi_j\rangle$ in an orthonormal basis of $\mathcal{H}$.

Proof. It is immediate from Lemma 3.1, Lemma 3.3 and Lemma 3.4. □

It is extremely expensive to calculate matrix-matrix multiplications $U_m \dots U_0$ and $U'_{m'} \dots U'_0$ to obtain U and U' and subsequently multiple with each $|\phi_i\rangle$ and $|\phi_j\rangle$ in Theorem 3.5 because of the exponential size of unitary matrices. Instead, we can perform a series of matrix-vector multiplications between unitary matrices and vectors in sequence as follows:

$$\left|u_i^0\right\rangle = U_0 |\phi_i\rangle, \left|u_i^1\right\rangle = U_1 \left|u_i^0\right\rangle, \dots, |u_i^m\rangle = U_m \cdot u_i^{m-1}$$

The i-th column vector of matrix U is $|u_i\rangle$ (i.e., $|u_i^m\rangle$) and similarly for the i-th column vector $|u'_i\rangle$ of matrix U'. We are now ready to check whether $|u_i\rangle\langle u_i|$ is equal to $|u'_i\rangle\langle u'_i|$ for the first condition in Theorem 3.5. Moreover, for the second condition in Theorem 3.5, it suffices to fix $|u_i\rangle$ and $|u'_i\rangle$, and check whether $|u_i\rangle\langle u_j| = \left|u'_i\right\rangle\left\langle u'_j\right|$ for all $j \neq i$. This is an efficient way to handle the calculation in Theorem 3.5.

3.2. Algorithm for Equivalence Checking of Quantum Circuits

An algorithm for equivalence checking of quantum circuits can be constructed based on Theorem 3.5, which is shown as Algorithm 1. Given two quantum circuits in the form of $U = U_m \dots U_0$ and $U' = U'_{m'} \dots U'_0$, and an orthonormal basis $\{|\phi_0\rangle, \dots, |\phi_{2^n-1}\rangle\}$, for each basis vector ϕ_i, we first construct the series of matrix-vector multiplications between unitary matrices and vectors to obtain $|u_i\rangle$ and $|u'_i\rangle$ in the code fragment at lines 2–3. We then check whether their corresponding density matrices $|u_i\rangle\langle u_i|$ and $|u'_i\rangle\langle u'_i|$ are equal for the first condition in Theorem 3.5 in the code fragment at lines 4–5. If this is not the case, False is returned. Otherwise, we keep on checking for the second condition in Theorem 3.5 except for the case of the basis vector $|\phi_0\rangle$ in the code fragment at lines 6–7. If $|u_0\rangle\langle u_i|$ is not equal to $|u'_0\rangle\langle u'_i|$, False is returned. Otherwise, we move to check for other basis vectors. True is returned at the end once all basis vectors have been checked.

4. Related Work

L. Burgholzer et al. [13] have proposed an advanced method for equivalence checking of quantum circuits based on a decision diagram. Their approach involves two quantum circuits $U = U_m \ldots U_0$ and $U'_{m'} \ldots U'_0$ as inputs and they check whether the two quantum circuits are equivalent. They leverage two key observations: (1) quantum circuits are inherently reversible, and (2) even small differences in quantum circuits may impact the overall behavior of quantum circuits. Their strategy is as follows. For (2), they first randomly prepare some basis vectors ϕ_i and calculate the i-th column of each matrix U and U' to obtain $|u_i\rangle$ and $|u'_i\rangle$ as we do. They then compare $|u_i\rangle$ and $|u'_i\rangle$ modulo the global phase by using the fidelity, denoted $\mathcal{F} = |\langle u_i|u'_i\rangle|^2$, to measure the overlap between the two states. The two states are considered equivalent if the fidelity between them is 1 up to a given tolerance ε. This is an approximate estimation, while we use their density matrices for the comparison, which provides an exact estimation. After several runs, if they find $|u_i\rangle$ and $|u'_i\rangle$ that are not equivalent, the process is stopped. Otherwise, they attempt to resolve $U \Rightarrow I \Leftarrow U'$ into the identity matrix I based on (1) to solve the equivalence checking problem. However, calculating $U_i(U'_{i'})^\dagger$ involves an expensive matrix-matrix multiplication. Moreover, they seem not to consider the global phase in this step. We have proven a theorem that it suffices to consider all basis vectors in an orthonormal basis with the same global phase to conclude the equivalence checking problem. Our approach considers the global phase and can be adopted by other approaches/tools for checking the equivalence of quantum circuits.

5. Conclusion

We have presented a theoretical foundation for checking the equivalence of quantum circuits based on which an algorithm is constructed. The equivalence checking process is simplified to comparing each column vector of two unitary matrices, representing two quantum circuits, modulo the same global phase. To eliminate the global phase during the comparison, we compare their corresponding density matrices instead of their column vectors. To guarantee the same global phase is used, we compare the outer products of two columns from each unitary matrix, with one column fixed. We have proven a theorem to guarantee the correctness of our approach. As one piece of future work, we would develop a support tool based on symbolic reasoning in [14, 15] for our approach and conduct case studies to demonstrate the effectiveness of our approach for equivalence checking of quantum circuits.

Acknowledgments

The research was supported by JAIST Research Grant for Fundamental Research, by JST SICORP Grant Number JPMJSC20C2, and by JSPS KAKENHI Grant Number JP23K19959.

References

[1] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134. doi:10.1109/SFCS.1994.365700.

[2] B. Giles, P. Selinger, Exact synthesis of multiqubit clifford+t circuits, Phys. Rev. A 87 (2013) 032332. doi:10.1103/PhysRevA.87.032332.

[3] M. Amy, D. Maslov, M. Mosca, M. Roetteler, A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits, Trans. Comp.-Aided Des. Integ. Cir. Sys. 32 (2013) 818–830. doi:10.1109/TCAD.2013.2244643.

[4] D. Maslov, Advantages of using relative-phase toffoli gates with an application to multiple control toffoli optimization, Physical Review A 93 (2016). doi:10.1103/physreva.93.022311.

[5] M. Y. Siraichi, V. F. d. Santos, C. Collange, F. M. Q. Pereira, Qubit allocation, in: Proceedings of the 2018 International Symposium on Code Generation and Optimization, CGO 2018, Association for Computing Machinery, New York, NY, USA, 2018, p. 113–125. doi:10.1145/3168822.

[6] A. Zulehner, A. Paler, R. Wille, Efficient mapping of quantum circuits to the ibm qx architectures, in: 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2018, pp. 1135–1138. doi:10.23919/DATE.2018.8342181.

[7] A. Cowtan, S. Dilkes, R. Duncan, A. Krajenbrink, W. Simmons, S. Sivarajah, On the qubit routing problem (2019). doi:10.4230/LIPICS.TQC.2019.5.

[8] D. Maslov, G. W. Dueck, D. M. Miller, C. Negrevergne, Quantum circuit simplification and level compaction, Trans. Comp.-Aided Des. Integ. Cir. Sys. 27 (2008) 436–444. doi:10.1109/TCAD.2007.911334.

[9] Z. Sasanian, D. M. Miller, Reversible and quantum circuit optimization: A functional approach, in: R. Glück, T. Yokoyama (Eds.), Reversible Computation, Springer Berlin Heidelberg, 2013, pp. 112–124. doi:10.1007/978-3-642-36315-3_9.

[10] Y. Nam, N. J. Ross, Y. Su, A. M. Childs, D. Maslov, Automated optimization of large quantum circuits with continuous parameters, npj Quantum Information 4 (2018) 23. doi:10.1038/s41534-018-0072-4.

[11] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information: 10th Anniversary Edition, Cambridge University Press, 2010. doi:10.1017/CBO9780511976667.

[12] P. A. M. Dirac, A new notation for quantum mechanics, Mathematical Proceedings of the Cambridge Philosophical Society 35 (1939) 416–418. doi:10.1017/S0305004100021162.

[13] L. Burgholzer, R. Wille, Advanced equivalence checking for quantum circuits, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 40 (2021) 1810–1824. doi:10.1109/TCAD.2020.3032630.

[14] C. M. Do, K. Ogata, Symbolic model checking quantum circuits in maude, in: The 35th International Conference on Software Engineering and Knowledge Engineering, SEKE 2023, 2023, pp. 103–108. doi:10.18293/SEKE2023-014.

[15] T. Takagi, C. M. Do, K. Ogata, Automated quantum program verification in dynamic quantum logic (to appear), in: DaLí: Dynamic Logic – New trends and applications, 2023.