# 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

Presented Physically at the 2nd International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols

November 21, 2023 - Brisbane, Australia

# Contents

# Contents

# Introduction

- 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 imposed on the targeted device.
- Consequently, the quantum circuit and its compiled counterpart are significantly different. Therefore, it is crucial to verify the equivalence of two quantum circuits constructed from quantum gates based on their functionality.

# Equivalence Checking Problem for Quantum Circuits

## Definition 1 (Equivalence checking problem)

Given two quantum circuits constructed from by quantum gates, $U = U_m \dots U_0$ 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 $\theta \in [0, 2\pi)$.

- L. Burgholzer et al.[1] have proposed an advanced method for equivalence checking of quantum circuits based on two key observations:
  - Quantum circuits are inherently reversible
  - Even small differences in quantum circuits may impact the overall behavior of quantum circuits
- In this study, we present a theoretical foundation for checking the equivalence of quantum circuits, where it suffices to compare each column vector of two matrices modulo the same global phase.

[1] Lukas Burgholzer and Robert Wille. "Advanced Equivalence Checking for Quantum Circuits". In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (2021).

# Contents

# Hilbert Spaces

- A Hilbert space $\mathcal{H}$ usually serves as the state space of a quantum system that is a complex vector space equipped with an inner product such that each Cauchy sequence of vectors has a limit.
- An $n$-qubit system is the complex $2^n$-space $\mathbb{C}^{2^n}$, where $\mathbb{C}$ stands for the complex plane.
- Pure states in the $n$-qubit systems $\mathbb{C}^{2^n}$ are unit vectors in $2^n$-space $\mathbb{C}^{2^n}$.
- The orthogonal basis called computational basis in the one-qubit system $\mathbb{C}^2$ is the set $\{|0\rangle, |1\rangle\}$ that consists of the column vectors $|0\rangle = (1,0)^T$ and $|1\rangle = (0,1)^T$, where $^T$ denotes the transpose operator.
- In the two-qubit system $\mathbb{C}^4$, there are pure states that cannot be represented in the form $|\psi_1\rangle \otimes |\psi_2\rangle$ and called entangled states, where $\otimes$ denotes the tensor product (more precisely, the Kronecker product).
- For example, the EPR state (Einstein-Podolsky-Rosen state) $|EPR\rangle = (|00\rangle + |11\rangle)/\sqrt{(2)}$ is an entangled state, where $|00\rangle = |0\rangle \otimes |0\rangle$ and $|11\rangle = |1\rangle \otimes |1\rangle$.

# Unitary Operators

- Quantum computation is represented by unitary operators (also called quantum gates).
- For example, the Hadamard gate $H$ and Pauli gates $X$, $Y$, and $Z$ are quantum gates on the one-qubit system $\mathbb{C}^2$ and are defined as follows:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- Two typical quantum gates on the two-qubit systems $\mathbb{C}^4$ are the controlled-X gate (also called the controlled-NOT gate) $CX$ and the swap gate $SWAP$ are defined by

$$CX = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X,$$
$$SWAP = CX(I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|)CX,$$

where $I$ denotes the identity matrix of size $2 \times 2$.

# Contents

# Contents

**Definition 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 whether $|\psi\rangle \approx |\psi'\rangle$, we can check the equality of their density matrices $|\psi\rangle\langle\psi|$ and $|\psi'\rangle\langle\psi'|$. This result is derived from the following lemma.

**Lemma 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 $\Rightarrow$ direction), it is straightforward.

## Proof (Cont.)

- We now consider the '*if*' part (the $\Leftarrow$ direction). Let $\{|\phi_0\rangle, \ldots, |\phi_i\rangle, \ldots |\phi_{2^n-1}\rangle\}$ be an orthonormal basis of $\mathcal{H}$ with $n$ dimension. $|\psi\rangle = c_0 |\phi_0\rangle + \cdots + c_i |\phi_i\rangle + \cdots + c_{2^n-1} |\phi_{2^n-1}\rangle$ and $|\psi'\rangle = c'_0 |\phi_0\rangle + \cdots + c'_i |\phi_i\rangle + \cdots + c'_{2^n-1} |\phi_{2^n-1}\rangle$.
- 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 $a_{ij} = \langle\phi_i| A |\phi_j\rangle = \langle\phi_i|\psi\rangle \langle\psi|\phi_j\rangle = c_i c_j^*$ and similarly for $a'_{ij} = c'_i c'^*_j$.
- We have $a_{ij} = a'_{ij}$ for any $i, j \in [0 \ldots 2^n - 1]$ because of A = A' from the assumption. Let us consider $a_{ii} = a'_{ii}$ as follows:

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

## Proof (Cont.)

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 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 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.**

Straightforward. □

☞ In Lemma 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 to check whether $U = e^{i\theta}U'$.

**Lemma 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.**

Straightforward. □

**Remark (Important)**

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 same phase $\theta$.

☞ To check $U|\phi_i\rangle \approx_\theta U'|\phi_i\rangle$ for each basis vector $|\phi_i\rangle$ in an orthonormal basis of $\mathcal{H}$.

**Lemma 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, $U|\phi_i\rangle (U|\phi_j\rangle)^\dagger = e^{i\theta}U'|\phi_i\rangle (e^{i\theta}U'|\phi_j\rangle)^\dagger = U'|\phi_i\rangle (U'|\phi_j\rangle)^\dagger$

## Proof (Cont.)

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.
Using the second condition in the assumption, we have as follows:

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

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 $|\phi_i\rangle$. □

# Our Main Theorem

☞ From Lemma 1, Lemma 3 and Lemma 4, we have the main theorem to check whether $U = e^{i\theta}U'$ for some $\theta \in [0, 2\pi)$.

## Theorem 1

*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 $\phi_i$ 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 1, Lemma 3 and Lemma 4. □

# An Efficient Way to Calculate for Our Main Theorem

- 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 multiple with each $|\phi_i\rangle$ and $|\phi_j\rangle$ in Theorem 1.
- We can perform a series of matrix-vector multiplications between unitary matrices and vectors in sequence as follows:

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

  where 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 $U'$.
- For the first condition in Theorem 1, we check whether $|u_i\rangle\langle u_i|$ is equal to $|u'_i\rangle\langle u'_i|$.
- For the second condition in Theorem 1, 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 $j \neq i$.

# Contents

# An Algorithm

**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

# Contents

# Conclusions and Future Work

- We have presented a theoretical foundation for checking the equivalence of quantum circuits based on which an algorithm is also 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.
- As one piece of future work, we would develop a support tool based on symbolic reasoning in[2][3] for our approach and conduct case studies to demonstrate the effectiveness of our approach for equivalence checking of quantum circuits.

[2] Canh Minh Do and Kazuhiro Ogata. "Symbolic Model Checking Quantum Circuits in Maude". In: *The 35th International Conference on Software Engineering and Knowledge Engineering, SEKE 2023*. 2023.

[3] Tsubasa Takagi, Canh Minh Do, and Kazuhiro Ogata. "Automated Quantum Program Verification in Dynamic Quantum Logic". In: *DaLí: Dynamic Logic – New trends and applications*. 2023.

# Thank You!