A Mathematical Exploration to Equivalence Checking of Quantum Circuits

You-Cheng Lin[1], Yi-Ting Li[2], Wuqian Tang[2], Yung-Chih Chen[1,3], Chia-Chieh Chu[2], and Chun-Yao Wang[1,2]

[1]ARCULUS SYSTEM CO., LTD., US
[2]National Tsing Hua University, Taiwan, ROC
[3]National Taiwan University of Science and Technology, Taiwan, ROC

***Abstract*—Simulation-based approaches to detecting the non-equivalence of quantum circuits are efficient since they usually conclude the result of non-equivalence faster than traditional methods. However, proving the equivalence of two quantum circuits remains challenging. As a result, this paper aims at analyzing simulation-based approaches and uncovering their potential and limitations in equivalence checking.**

I. Introduction

Quantum computing has demonstrated remarkable efficiency in tackling specific problems, such as Grover's algorithm for unstructured search [6] or Shor's algorithm for integer factorization [16]. Notably, major players in the industry, such as Google, IBM, Intel, and Microsoft, alongside various startups, are increasingly investing in this technology. However, the current generation of quantum devices, operating in the Noisy-Intermediate-Scale-Quantum (NISQ) era, face significant challenges due to noise and decoherence effects, emphasizing the imperative for quantum circuit optimizations. These optimizations, including gate fusion and cancellation, aim to reduce the overall gate count and to counter the impact of noise. Moreover, mapping techniques are evolving to achieve noise-adaptive mappings by considering the device's calibration and error data.

The surge in quantum computing research, driven by its potential, spans both academia and industry. The design procedures of quantum circuits, including preprocessing [17][18], compilation [10][14], optimization [5][12], and verification [1][20], have gotten significant attention. In light of the current limited accessibility of quantum circuits, simulation methods using classical computers have been proposed. Open-source toolkits like IBM's Qiskit [15] and Microsoft's QDK [11] further support this drive towards making quantum computing more accessible and understandable.

Various methods for equivalence checking of two quantum circuits were proposed recently [1][3][4][7][8][9][19][20].

This work was supported in part by the National Science and Technology Council (Taiwan) under Grant MOST 111-2221-E-007-121, Grant MOST 111-2221-E-011-137-MY3, Grant NSTC 112-2218-E-007-014, Grant NSTC 112-2221-E-007-106-MY2, Grant NSTC 112-2221-E-007-108, Grant NSTC 112-2425-H-007-002, and Grant NSTC 113-2425-H-007-004, Grant NSTC 113-2640-E-011-003, Grant NSTC 113-2221-E-007-082-MY3, Grant NSTC 114-2221-E-007-125-MY3, Grant NSTC 114-2218-E-007-002, Grant NSTC 114-2221-E-007-126-MY3, Grant NSTC 114-2425-H-007-002, and National Tsing Hua University under NTHU 113A0257EX and 114A0078EX.

In this paper, we focus on analyzing the potential and limitations of simulation-based equivalence checking. In general, simulation-based approaches often involve combining two quantum circuits U and V: one (U) is inverse, and the other (V) is kept unchanged, to verify whether the resultant combined circuit ($U^{-1} \cdot V$) is an identity matrix (I) or not. Consequently, this problem can be viewed as the Non-Identity Check problem, which asks whether a given quantum circuit is far away from the identity or not. When the combined circuit $U^{-1} \cdot V$ is equivalent to an identity matrix, the output of the circuit will precisely match the input stimulus.

In general, there usually appear minor differences between U and V, resulting in a simplified structure of the combined quantum circuit $U^{-1} \cdot V$. Inspired by this observation, we present a constrained situation to characterize the structure of $U^{-1} \cdot V$. The constrained situation involves restricting the elements of the matrix of $U^{-1} \cdot V$. This constrained situation proves the equivalence of two quantum circuits using significantly fewer stimuli than exhaustive simulation.

II. Preliminaries

The objective of equivalence checking for two quantum circuits is checking whether they are functionally equivalent, or functionally non-equivalent with a counterexample. Here, a counterexample is a stimulus that displays difference of these two quantum circuits.

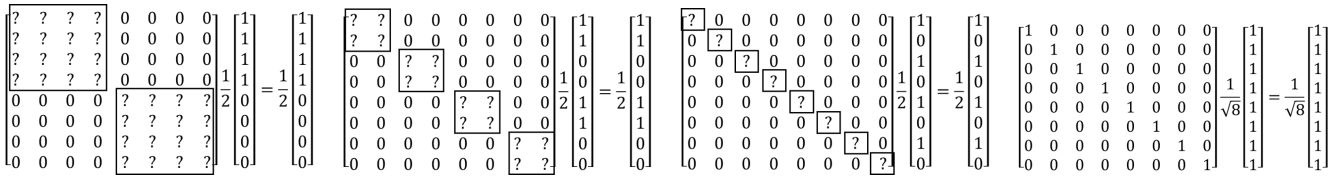
Let the matrix representation of two quantum circuits be U and V. We would like to verify whether $U = V$. More precisely, U and V are said to be functionally equivalent up to a global phase factor $e^{i\phi}$ with satisfying the condition $U = e^{i\phi}V$, where $\phi \in [0, 2\pi)$, which is not observable in essence [13]. Hence, in our work, we ignore the global phase factor $e^{i\phi}$ for simplicity.

A common method to verifying $U = V$ is to combine the two quantum circuits $U = U_k \dots U_1$ and $V = V_m \dots V_1$ as EQ(1).

$$\begin{aligned} U^{-1} \cdot V = U^{\dagger} \cdot V &= (U_k \dots U_1)^{\dagger} \cdot (V_m \dots V_1) \\ &= (U_1^{\dagger} \dots U_k^{\dagger}) \cdot (V_m \dots V_1) \end{aligned} \tag{1}$$

In EQ(1), k and m are the numbers of quantum gates in U and V, respectively. Moreover, the notation $U^{\dagger} \cdot V$ is called a *miter* in quantum computing. Therefore, U and V are equivalent if and only if the miter $U^{\dagger} \cdot V$ is equal to I.

978-3-9826741-1-7/DATE26/© 2026 EDAA



(a) A miter passing $|\psi_1\rangle$. (b) A miter passing $|\psi_2\rangle$. (c) A miter passing $|\psi_3\rangle$. (d) A miter passing $|\psi_0\rangle$.

Figure 1: The illustration of the binary checking method.

For a simulation-based approach to quantum circuit equivalence checking, it is usually to prove non-equivalence of two circuits with a counterexample, which can be modeled as follows. Given a set of stimuli $\mathcal{S} = \{|\psi_1\rangle, \ldots, |\psi_p\rangle\}$ and an n-qubit miter $U^\dagger \cdot V$. For the simulation in EQ(2),

$$U^\dagger \cdot V |\psi_i\rangle, \forall i \in [1, p] \tag{2}$$

there are two possible outcomes:

1) $\exists i \in [1, p]$ s.t. $U^\dagger \cdot V |\psi_i\rangle \neq |\psi_i\rangle$
2) $\forall i \in [1, p]$ s.t. $U^\dagger \cdot V |\psi_i\rangle = |\psi_i\rangle$

For the first outcome, we can conclude $U \neq V$ immediately because $|\psi_i\rangle$ is exactly a counterexample for the non-equivalence. For the second outcome, we can just say U is equivalent to V with a higher probability, but not confirmed. However, U and V are still indistinguishable under the vector space, span($\mathcal{S}$), where span($\mathcal{S}$) $= \{c_1 |\psi_1\rangle + \cdots + c_p |\psi_p\rangle \mid c_1, \ldots, c_p \in \mathbb{C}\}$ is the vector space spanned by $\mathcal{S}$. In the span($\mathcal{S}$), the functionalities of $U^\dagger \cdot V$ and I are the same, i.e., they both map $|\psi_i\rangle$ to $|\psi_i\rangle$, $\forall i \in [1, p]$.

III. Proposed Methods

In an n-qubit system, the set $\mathcal{S}$ of specially-designed stimuli in [9] can be formulated as EQ(3),

$$\left\{ |\psi_0\rangle = \sqrt{\frac{1}{2^n}} \left(\sum_{j=0}^{2^n-1} |j\rangle \right) \right\} \cup \left\{ |\psi_i\rangle = \sqrt{\frac{1}{2^{n-1}}} \left(\sum_{k=0}^{2^{i-1}-1} \sum_{j=0}^{2^{n-i}-1} |j + k \cdot 2^{n-i+1}\rangle \right) \right\}_{i=1}^{n} \tag{3}$$

which consists of $n + 1$ stimuli only in total.

Unit-Norm Quantum Circuits: In the state-of-the-art [9], the authors proposed a set of specially-designed stimuli for detecting non-equivalence of two distinct quantum circuits efficiently. For two equivalent quantum circuits, however, they suggest to use other methods [1][2]. Here, we propose Theorem 1 to show that this set of specially-designed stimuli is capable of proving equivalence of two **constrained** quantum circuits, i.e., determining the miter is an identity matrix.

Theorem 1: *When a miter is restricted to containing elements with norms of either 0 or 1, the miter can be proven to be or to be not an identity matrix by simulating the set of specially-designed stimuli in EQ(3).*

Proof: Suppose $U^\dagger \cdot V$ is the unitary matrix representing the miter in an n-qubit system, and the matrix is restricted to containing elements with norms of either 0 or 1.

When we simulate specially-designed stimulus $|\psi_0\rangle$ to $|\psi_n\rangle$ in EQ(3) on $U^\dagger \cdot V$, we will obtain one of two possible outcomes in EQ(2). If the first outcome occurs, we deduce $U^\dagger \cdot V \neq I_{2^n}$. If the second outcome occurs, we can gradually limit the locations of the elements in $U^\dagger \cdot V$ with their norms being 1 in the diagonal of $U^\dagger \cdot V$. Because $U^\dagger \cdot V$ is a unitary matrix, for each element u_{ij} in $U^\dagger \cdot V$, it satisfies EQ(4).

$$\begin{aligned} \text{Column vector } j: \sum_{i=0}^{2^n-1} |u_{ij}|^2 = 1, \forall j \in [0, 2^n - 1] \\ \text{Row vector } i: \sum_{j=0}^{2^n-1} |u_{ij}|^2 = 1, \forall i \in [0, 2^n - 1] \end{aligned} \tag{4}$$

When $|u_{ij}| = 1$, the elements in the i^{th} row vector and in the j^{th} column vector are all zeros except for u_{ij} itself. Thus, there is only one element with norm of 1, and the other elements are all zeros in each row vector or column vector of $U^\dagger \cdot V$.

Figure 1 illustrates that we can gradually determine the structure of the miter with a 3-qubit system. Figure 1(a) determines the nonzero elements located in the region of two black squares; otherwise the miter will not pass $|\psi_1\rangle$. Next, Figure 1(b) and Figure 1(c) determine the rest of the unknown elements of the miter. Finally, Figure 1(d) concludes that all the diagonal elements of the miter are exactly 1. As a result, we conclude that $U^\dagger \cdot V$ is an identity matrix when it passes the set of specially-designed stimuli in EQ(3). ■

Whenever quantum circuits only consist of gates with the elements of their matrix representations have norms of either 0 or 1 (Pauli gates, Phase shifting gates, CNOT gates and so on), called *Unit-Norm* quantum circuits, they can be proven equivalent passing **only** the set of specially-designed stimuli in EQ(3). The number of stimuli in this set is only $(n+1)$ instead of 2^n. In fact, most of the benchmarks in [21] are contained in the range of *Unit-Norm* quantum circuits. This implies that our approach is not only **theoretically sound** but also **practically valuable** for real-world quantum circuit equivalence checking.

IV. Conclusion

In this work, we prove that **non-exhaustive simulation** can still be used in proving equivalence more efficiently under a certain constraint. This work sheds light on the limitations and potentials of simulation-based equivalence checking in quantum circuit, offering valuable insights for future investigations.

References

[1] L. Burgholzer and R. Wille, "Advanced equivalence checking for quantum circuits," *IEEE TCAD*, vol. 40, no. 9, pp. 1810–1824, 2020.

[2] ——, "Improved dd-based equivalence checking of quantum circuits," in *Proc. of ASP-DAC*, 2020, pp. 127–132.

[3] ——, "The power of simulation for equivalence checking in quantum computing," in *Proc. of DAC*, 2020, pp. 1–6.

[4] Y.-F. Chen, K.-M. Chung, O. Lengál, J.-A. Lin, W.-L. Tsai, and D.-D. Yen, "An automata-based framework for verification and bug hunting in quantum circuits," *ACM PLDI*, vol. 7, pp. 1218–1243, 2023.

[5] A. Gilyén, S. Arunachalam, and N. Wiebe, "Optimizing quantum optimization algorithms via faster quantum gradient computation," in *Proc. of ACM-SIAM Symp. Discrete Algorithms*, 2019, pp. 1425–1444.

[6] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. of ACM STOC*, 1996, pp. 212–219.

[7] X. Hong, M. Ying *et al.*, "Approximate equivalence checking of noisy quantum circuits," in *Proc. of DAC*, 2021, pp. 637–642.

[8] X. Hong, X. Zhou, S. Li, Y. Feng, and M. Ying, "A tensor network based decision diagram for representation of quantum circuits," *ACM TODAES*, vol. 27, no. 6, pp. 1–30, 2022.

[9] H.-L. Liu, Y.-T. Li, Y.-C. Chen, and C.-Y. Wang, "A robust approach to detecting non-equivalent quantum circuits using specially designed stimuli," in *Proc. of ASP-DAC*, 2023, pp. 696–701.

[10] G. Meuli, M. Soeken, E. Campbell, M. Roetteler, and G. De Micheli, "The role of multiplicative complexity in compiling low T-count oracle circuits," in *Proc. of ICCAD*, 2019, pp. 1–8.

[11] Microsoft, "QDK," https://github.com/microsoft/, [Online].

[12] N. Moll, P. Barkoutsos *et al.*, "Quantum optimization using variational algorithms on near-term quantum devices," *Quantum Science and Technology*, vol. 3, no. 3, 2018, art. no. 030503.

[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge university press, 2010.

[14] A. Paler, I. Polian, K. Nemoto, and S. J. Devitt, "Fault-tolerant, high-level quantum circuits: form, compilation and description," *Quantum Science and Technology*, vol. 2, no. 2, 2017, art. no. 025003.

[15] Qiskit Development Team, "Qiskit," https://qiskit.org/, [Online].

[16] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. of IEEE FOCS*, 1994, pp. 124–134.

[17] E. Testa, M. Soeken, L. Amarù, and G. De Micheli, "Reducing the multiplicative complexity in logic networks for cryptography and security applications," in *Proc. of DAC*, 2019, pp. 1–6.

[18] E. Testa, M. Soeken, H. Riener, L. Amaru, and G. De Micheli, "A logic synthesis toolbox for reducing the multiplicative complexity in logic networks," in *Proc. of DATE*, 2020, pp. 568–573.

[19] Y.-H. Tsai, J.-H. R. Jiang, and C.-S. Jhang, "Bit-slicing the hilbert space: Scaling up accurate quantum circuit simulation," in *Proc. of DAC*, 2021, pp. 439–444.

[20] C.-Y. Wei, Y.-H. Tsai, C.-S. Jhang, and J.-H. R. Jiang, "Accurate bdd-based unitary operator manipulation for scalable and robust quantum circuit verification," in *Proc. of DAC*, 2022, pp. 523–528.

[21] R. Wille, D. Große, L. Teuber, G. W. Dueck, and R. Drechsler, "Revlib: An online resource for reversible functions and reversible circuits," in *38th International Symposium on Multiple Valued Logic (ismvl 2008)*. IEEE, 2008, pp. 220–225.