Accelerating Formal Methods for Quantum Circuit Compilation

Dimitrios Thanos and Alfons Laarman

Leiden Institute of Advanced Computer Science (LIACS), Leiden University, Leiden
2333 CA, The Netherlands

Towards Quantum Supremacy

Quantum computing holds the promise of revolutionizing the field of computation by surpassing classical computers in terms of efficiency, particularly in tackling tasks that are deemed classically intractable [26,25]. Quantum supremacy leverages quantum phenomena like superposition and entanglement to handle exponentially more states than a classical computer. That way many practical problems, for example period finding, have been shown to exhibit algorithms that are exponentially faster than their best known classical versions [26]. One of the most prevalent forms of quantum computing involves the utilization of a limited set of quantum gates, specifically reversible operators designed to manipulate qubits. These operators form quantum circuits, which are not necessarily unique, meaning that different circuits that implement the same computation can exist. As we enter the era of Noisy Intermediate-Scale Quantum computing [29], there are many challenges which we need to overcome while compiling quantum circuits into real world devices. Such challenges are the high noise levels, the shallow-depth of the circuits that can be practically implemented and the various constraints (connectivity, topology, native gate sets, etc.) [14,10]. Therefore circuit compilation problems are closely tied to the goal of achieving quantum supremacy.

Challenges of quantum circuit compilation

Given the multitude of constraints, there exists an extensive range of parameters that needs to be optimized to get quantum advantage as early as possible. A number of significant questions arise when considering a textbook description of a quantum circuit:

- *Is the presented circuit the "optimal" one (e.g. with the least depth) for the aimed computation?*

  Or a more basic question:
- *Is the optimized circuit still equivalent to the original one?*
- *Can the circuit be simulated by a classical computation?*

  Or in the case that we are presented with an arbitrary many-qubit operator:
- *Can we synthesize a quantum circuit that implements the same operation as the given unitary?*

These are some of the basic questions of circuit compilation. They cover circuit optimization, equivalence checking, circuit simulation, and circuit synthesis. They address crucial aspects of quantum circuit design and analysis, enabling us to verify and validate the performance of our devices and algorithms.

Formal methods

A promising range of techniques for addressing these questions exists within the field of Formal Methods. Formal methods play a crucial role in ensuring the accuracy and dependability of computing systems by employing rigorous techniques to analyze and verify system behavior. In the realm of classical computing, these methods have been extensively studied and effectively applied to ensure the accuracy of digital circuits [13,30,11,17,16,22,21]. Through rigorous analysis, these methods ensure that circuits meet their intended specifications and operate accurately across all potential inputs and scenarios. However, the direct transfer of all these methods to the realm of quantum computing is not always feasible. The state of n quantum bits is generally represented as 2^n complex values [26] and poses a challenge for numerous classical techniques, rendering them inefficient for quantum computing tasks.

However, diverse methodologies have been employed in the analysis of quantum circuits, drawing upon a range of techniques. For instance, existing approaches involve encoding circuits as Boolean satisfiability instances [5] (and also [39,40] for restricted circuits), utilizing satisfiability modulo theories [4], path-sums [1,2], rewrite rules [28] [12][38]. Additionally, diverse variants of decision diagrams are utilized, such as QMDD [8,33,27,7], LIMDD [35], Tensor-DD [20], BDD [37,9] and others [36,41]. Furthermore, probabilistic methods have been investigated within this domain as well [6,23].

First contribution

The correctness verification of quantum circuits assumes a critical role in the design and optimization of quantum circuits, ensuring compliance with rigorous specifications. It encompasses the crucial task of formally establishing whether two quantum circuits, represented through a classical description, indeed implement identical quantum operations. Our work represents a notable advancement in this domain, surpassing previously established techniques for the case of Clifford circuits [32].

Clifford gates hold significant importance in the realm of quantum computing as they are widely utilized in quantum error correction [18,31] and quantum networking applications [19]. Previous work by [5] introduced the QuSAT tool, which reduced the problem of equivalence checking for Clifford circuits to satisfiability. Approximate equivalence checking has been also introduced, one such work is [3] where a polynomial-time algorithm for approximate non-identity check is presented, with the runtime dependenting on the desired accuracy of the approximation. Our approach for equivalence check of Clifford circuits entails a deterministic algorithm, based on a folklore mathematical result (10.5.2 in [26]) which translates into an efficient equivalence checking algorithm of complexity $O(n^2 + nm)$ where n the number of qubits and m the number of gates. This can become linear for $m \gg n$.

In our empirical evaluation, we assessed the algorithm's performance using the efficient Clifford-circuit simulator Stim [15]. Our evaluation demonstrated that the algorithm successfully handled circuit depths of up to 1000 qubits and 10,000 elementary Clifford gates within a minute. Moreover, for depth-10 circuits with 100,000 qubits, the evaluation took approximately 15 minutes. These results showcased a significant improvement over the SAT-based approach, surpassing it by an order of magnitude.

This is accomplished through the utilization of the stabilizers formalism [26]. The stabilizers formalism is an efficient approach for representing quantum states by leveraging the underlying symmetries of stabilizer states (i.e., states generated by Clifford circuits) and associating a subgroup of the "Pauli group" with each state. Interestingly, it suffices to track the generators of the group, which entails storing only a small subset of it, thereby enabling efficient simulation of Clifford circuits. The elements of the underlying group consist of tensor-product strings composed of a set of 2×2 linear operators known as the Pauli operators giving rise to what are known as "Pauli strings". The length of the Pauli strings depends on the number of qubits. The four Pauli operators are commonly denoted by the letters I, X, Z, and Y. For a detailed treatment of the stabilizers formalism see [26]. Below, we provide a formal statement of the theorem that serves as the foundation for the algorithm:

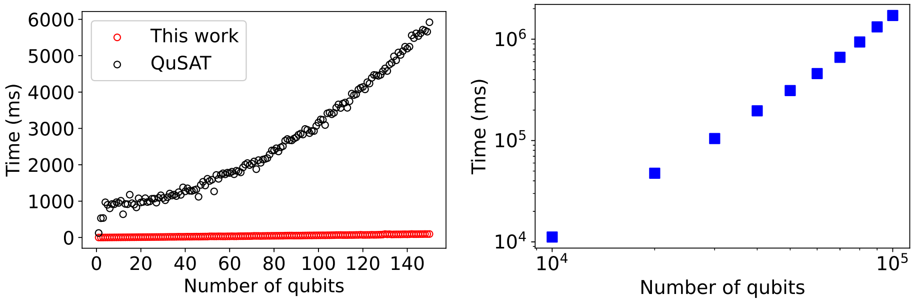
Theorem. *Let U, V be two Clifford unitaries on $n \geq 1$ qubits. Then U is equivalent to V if and only if the following conditions hold:*

1. *for all $j \in \{1, 2, \ldots, n\}$, we have $UZ_jU^\dagger = VZ_jV^\dagger$; and*
2. *for all $j \in \{1, 2, \ldots, n\}$, we have $UX_jU^\dagger = VX_jV^\dagger$.*

Here, $G_j = \mathbb{1}_2 \otimes \mathbb{1}_2 \cdots \otimes \mathbb{1}_2 \otimes G \otimes \mathbb{1}_2 \ldots \mathbb{1}_2$, with G the j-th factor of the length-n tensor product and single-qubit identity operators $\mathbb{1}_2$ everywhere else, is the single-qubit gate G applied to the j-th qubit of an n-qubit register.

Based on the above theorem, our algorithm for comparing two circuits U,V consists of simulating both circuits, gate-by-gate, and then comparing the resulting generators. This must be done for two different initial state generators, one where the initial Pauli strings consist of only Z operators and another one for the case where the initial Pauli strings consist of only X operators. If both simulations result into the same set of generators then we deduce that the circuits are indeed equivalent. A more elementary treatment of our algorithm can be found in [32].

The figure below, demonstrates the efficiency of our algorithm compared to the implementation of the previously-leading-method, QuSAT. Specifically, the left panel (Figure 1a) superposes the running time of our method with the running time of QuSAT, while the right panel (Figure 1b) demonstrates that our algorithm can reach number of qubits much higher than what was ever reached for the task of circuit equivalence.



(a) Runtime comparison for fixed circuit depth of 1000.

(b) Reaching beyond what was previously feasible: Fixed depth 10 and number of qubits up to 100.000. Both axes in logarithmic scale.

Projecting to the future

Thus far, our analysis has focused on Clifford circuits. These circuits represent Stabilizer states. How can we broaden our approach to enable circuit compilation for more general types of circuits? The solution could lie into combining our methods with existing data structures. There are two dimensions of possible extension for our methods: 1) Extending beyond Stabilizer states and 2) extending beyond circuit equivalence, e.g. to quantum circuit optimization or synthesis, where a variant could serve as a subroutine for a more comprehensive approach.

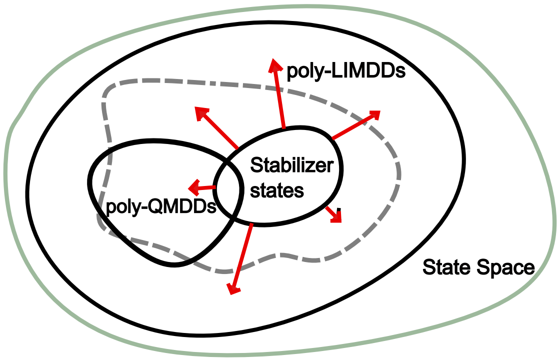


Fig. 2: How much further, from the Stabilizer states, can the limits of quantum-circuit compilation be pushed? Poly-sized QMDDs and LIMDDs here are examples of state classes that can be efficiently represented by different classical data structures [34,24].

References

1. Amy, M.: Towards large-scale functional verification of universal quantum circuits. arXiv:1805.06908 (2018)
2. Amy, M.: Formal methods in quantum circuit design (PhD thesis) (2019)
3. Arunachalam, S., Bravyi, S., Nirkhe, C., O'Gorman, B.: The parameterized complexity of quantum verification. arXiv:2202.08119 (2022)
4. Bauer-Marquart, F., Leue, S., Schilling, C.: symQV: Automated symbolic verification of quantum programs. In: Formal Methods: 25th International Symposium, FM 2023, Lübeck, Germany, March 6–10, 2023, Proceedings. pp. 181–198. Springer (2023)
5. Berent, L., Burgholzer, L., Wille, R.: Towards a SAT encoding for quantum circuits: A journey from classical circuits to Clifford circuits and beyond. arXiv:2203.00698 (2022)
6. Burgholzer, L., Kueng, R., Wille, R.: Random stimuli generation for the verification of quantum circuits. In: Proceedings of the 26th Asia and South Pacific Design Automation Conference. pp. 767–772 (2021)
7. Burgholzer, L., Wille, R.: Advanced equivalence checking for quantum circuits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 40(9), 1810–1824 (2020)
8. Burgholzer, L., Wille, R.: Improved DD-based equivalence checking of quantum circuits. In: 2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC). pp. 127–132 (2020)
9. Chen, T.F., Jiang, J.H.R., Hsieh, M.H.: Partial equivalence checking of quantum circuits. In: 2022 IEEE International Conference on Quantum Computing and Engineering (QCE). pp. 594–604. IEEE (2022)
10. Córcoles, A.D., Kandala, A., Javadi-Abhari, A., McClure, D.T., Cross, A.W., Temme, K., Nation, P.D., Steffen, M., Gambetta, J.M.: Challenges and opportunities of near-term quantum computing systems. arXiv:1910.02894 (2019)
11. Darwiche, A., Marquis, P.: A knowledge compilation map (10 2002)
12. Duncan, R., Kissinger, A., Perdrix, S., van de Wetering, J.: Graph-theoretic Simplification of Quantum Circuits with the ZX-calculus. Quantum 4, 279 (Jun 2020), `https://doi.org/10.22331/q-2020-06-04-279`
13. Fargier, H., Marquis, P., Schmidt, N.: Semiring labelled decision diagrams, revisited: Canonicity and spatial efficiency issues. In: International Joint Conference on Artificial Intelligence - IJCAI 2013. pp. 884–890. AAAI Press, Beijing, CN (2013), thanks to ACM
14. Finigan, W., Cubeddu, M., Lively, T., Flick, J., Narang, P.: Qubit allocation for noisy intermediate-scale quantum computers. arXiv:1810.08291 (2018)
15. Gidney, C.: Stim: a fast stabilizer circuit simulator. Quantum 5, 497 (Jul 2021), `https://doi.org/10.22331/q-2021-07-06-497`
16. Goldberg, E., Novikov, Y.: How good can a resolution based SAT-solver be? In: Giunchiglia, E., Tacchella, A. (eds.) Theory and Applications of Satisfiability Testing. pp. 37–52. Springer Berlin Heidelberg, Berlin, Heidelberg (2004)
17. Golia, P., Roy, S., Meel, K.S.: Manthan: A data-driven approach for boolean function synthesis. In: Lahiri, S.K., Wang, C. (eds.) Computer Aided Verification. pp. 611–633. Springer International Publishing, Cham (2020)
18. Gottesman, D.: Stabilizer codes and quantum error correction. arXiv:quant-ph/9705052 (1997)

19. Hein, M., Dür, W., Eisert, J., Raussendorf, R., Nest, M., Briegel, H.J.: Entanglement in graph states and its applications. arXiv:0602096 (2006)
20. Hong, X., Ying, M., Feng, Y., Zhou, X., Li, S.: Approximate equivalence checking of noisy quantum circuits. In: 2021 58th ACM/IEEE Design Automation Conference (DAC). pp. 637–642 (2021)
21. Kuehlmann, A.: Dynamic transition relation simplification for bounded property checking. In: IEEE/ACM International Conference on Computer Aided Design, 2004. ICCAD-2004. pp. 50–57 (2004)
22. Kuehlmann, A., Paruthi, V., Krohm, F., Ganai, M.: Robust boolean reasoning for equivalence checking and functional property verification. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 21(12), 1377–1394 (2002)
23. Linden, N., de Wolf, R.: Lightweight detection of a small number of large errors in a quantum circuit. Quantum 5, 436 (2021)
24. Miller, D.M., Thornton, M.A.: Qmdd: A decision diagram structure for reversible and quantum circuits. 36th International Symposium on Multiple-Valued Logic (ISMVL'06) pp. 30–30 (2006)
25. Montanaro, A.: Quantum algorithms: an overview. npj Quantum Information 2(1), 15023 (Jan 2016), https://doi.org/10.1038/npjqi.2015.23
26. Nielsen, M.A., Chuang, I.L.: Quantum information and quantum computation. Cambridge: Cambridge University Press 2(8), 23 (2000)
27. Niemann, P., Wille, R., Drechsler, R.: Equivalence checking in multi-level quantum systems. In: Reversible Computation: 6th International Conference, RC 2014, Kyoto, Japan, July 10-11, 2014. Proceedings 6. pp. 201–215. Springer (2014)
28. Peham, T., Burgholzer, L., Wille, R.: Equivalence checking of quantum circuits with the ZX-calculus. IEEE Journal on Emerging and Selected Topics in Circuits and Systems 12(3), 662–675 (2022)
29. Preskill, J.: Quantum Computing in the NISQ era and beyond. Quantum 2, 79 (Aug 2018), https://doi.org/10.22331/q-2018-08-06-79
30. Sanner, S., Mcallester, D.: Affine algebraic decision diagrams (AADDs) and their application to structured probabilistic inference. pp. 1384–1390 (01 2005)
31. Terhal, B.M.: Quantum error correction for quantum memories. Rev. Mod. Phys. 87, 307–346 (Apr 2015), https://link.aps.org/doi/10.1103/RevModPhys.87.307
32. Thanos, D., Coopmans, T., Laarman, A.: Fast equivalence checking of quantum circuits of clifford gates. In: (To appear in ATVA 2023)
33. Viamontes, G.F., Markov, I.L., Hayes, J.P.: Checking equivalence of quantum circuits and states. In: 2007 IEEE/ACM International Conference on Computer-Aided Design. pp. 69–74 (2007)
34. Vinkhuijzen, L., Coopmans, T., Elkouss, D., Dunjko, V., Laarman, A.: LIMDD A Decision Diagram for Simulation of Quantum Computing Including Stabilizer States (8 2021)
35. Vinkhuijzen, L., Grurl, T., Hillmich, S., Brand, S., Wille, R., Laarman, A.: Efficient implementation of LIMDDs for quantum circuit simulation. In: International Symposium on Model Checking of Software (SPIN) (2023)
36. Wang, S.A., Lu, C.Y., Tsai, I.M., Kuo, S.Y.: An XQDD-based verification method for quantum circuits. IEICE transactions on fundamentals of electronics, communications and computer sciences 91(2), 584–594 (2008)
37. Wei, C.Y., Tsai, Y.H., Jhang, C.S., Jiang, J.H.R.: Accurate BDD-based unitary operator manipulation for scalable and robust quantum circuit verification. In:

Proceedings of the 59th ACM/IEEE Design Automation Conference. pp. 523–528 (2022)

38. van de Wetering, J.: ZX-calculus for the working quantum computer scientist (2020)
39. Wille, R., Przigoda, N., Drechsler, R.: A compact and efficient sat encoding for quantum circuits. In: 2013 Africon. pp. 1–6. IEEE (2013)
40. Yamashita, S., Markov, I.L.: Fast equivalence-checking for quantum circuits. In: 2010 IEEE/ACM International Symposium on Nanoscale Architectures. pp. 23–28. IEEE (2010)
41. Yamashita, S., Minato, S.i., Miller, D.M.: DDMF: An efficient decision diagram structure for design verification of quantum circuits under a practical restriction. IEICE transactions on fundamentals of electronics, communications and computer sciences 91(12), 3793–3802 (2008)