Paler, Alexandru

Quantum Fourier addition simplified to Toffoli addition

Published in:
Physical Review A

DOI:
10.1103/PhysRevA.106.042444

Published: 27/10/2022

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Paler, A. (2022). Quantum Fourier addition simplified to Toffoli addition. Physical Review A, 106(4), 1-6. [042444]. https://doi.org/10.1103/PhysRevA.106.042444

This material is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of the repository collections is not permitted, except that material may be duplicated by you for your research use or educational purposes in electronic or print form. You must obtain permission for any other use. Electronic or print copies may not be offered, whether for sale or otherwise to anyone who is not an authorised user.
Quantum Fourier addition simplified to Toffoli addition

Alexandru Paler

Aalto University, Espoo 02150, Finland
and University of Texas at Dallas, Richardson, Texas 75080, USA

(Received 8 May 2022; accepted 29 September 2022; published 27 October 2022)

Quantum addition circuits are considered being of two types: (1) Toffoli-adder circuits which use only classical reversible gates (controlled-NOT and Toffoli), and (2) QFT-adder circuits based on the quantum Fourier transformation. We present a systematic translation of the QFT addition circuit into a Toffoli-based adder. This result shows that QFT addition has fundamentally the same fault-tolerance cost (e.g., T count) as the most cost-efficient Toffoli adder: instead of using approximate decompositions of the gates from the QFT circuit, it is more efficient to merge gates. In order to achieve this, we formulated circuit identities for multicontrolled gates and apply the identities algorithmically. The employed techniques can be used to automate quantum circuit optimization heuristics.

DOI: 10.1103/PhysRevA.106.042444

I. INTRODUCTION

Addition circuits are one of the workhorses of quantum circuit design. The literature on arithmetic circuits includes two types of adders [1,2]: quantum Fourier transform (QFT) adders and Toffoli-based adders. Intuitively, it is the same addition algorithm (one in a Boolean space, the other in a phase space), but there is a gap in the interpretation of one addition circuit in terms of the other. For an excellent introduction to the basics of quantum arithmetic circuits, we refer the reader to Ref. [1]. The challenge we are solving herein is to show the systematic translation between the two types of addition circuits.

Recent applications of QFT adders are quantum walks [3] for NISQ computers (noisy intermediate-scale quantum era). Nevertheless, while QFT adders are considered by some to be NISQ compatible due to their depth and gate counts, there are works on Toffoli-based arithmetic for NISQ [4]. Recently, approximate addition has been proposed in Ref. [5], which can be seen as a mix between QFT and Clifford + T due to the gate set those circuits are using.

A. MOTIVATION

Most of the metrics that influence the fault-tolerant implementation of quantum computations are related to circuit depth, number of wires, and T count. The cost of quantum addition has been investigated from different perspectives, but for practical applications it has almost always boiled down those metrics. Fault-tolerant circuits, even if initially expressed using Toffoli gates, have to be compiled to Clifford + T gates because, practical codes, such as the surface code, can only protect this gate set.

Yoder [6], for example, presented fault-tolerant Toffoli-like gates using Bacon-Shor codes, but such constructions are not compatible with the surface code. For this reason, resource estimations of practical circuits just replaced the QFT addition with the more cost-effective, reversible one (e.g., Ref. [7]).

Our contribution is to show that for arithmetic circuits, the QFT can be avoided by systematically applying circuit identities from [8]. We effectively translate a QFT adder into a Toffoli-based adder. Independent of this work, efforts [9] to connect the ZX calculus (used for Clifford + T circuits) to the ZH calculus (used for Toffoli + H circuits) have highlighted that the connection is mediated by the QFT. The authors of [9] analyzed the cost of addition without looking at explicit addition circuits but used the QFT to derive generalized Toffoli gates. From this perspective, our result is a special case of the result from [9] (it goes back from a single QFT to multiple Toffoli gates), as well the first explicit translation between QFT and Toffoli adders.

B. BACKGROUND

For the purpose of this work, we assume that in a QFT adder (e.g., Fig. 1) the numbers $A$ and $B$ are encoded in two multiqubit registers: the addition is implemented by applying the QFT on register $B$ and then systematically rotating by well-specified angles the relative phase of the individual qubits from the register of $B$ and finally undoing the QFT on register $B$. The rotations are controlled by the $A$ register.

Logical circuits for reversible addition [10] can be expressed exclusively with three-qubit Toffoli and two-qubit controlled-NOT (CNOT) gates. This fact has the advantage that reversible adder constructions can be inspired by classical computer architecture, and some examples are the ripple carry [11] and the carry save adders [12]. Once addition circuits are formulated with reversible gates, there are many exact or empirical methods to optimize the reversible circuits with respect to a given cost function.

One of the disadvantages of the fault-tolerant compilation of QFT adders to Clifford + T is that the controlled rotations in the QFT adders are approximated by CNOTs and sequences of single-qubit gates using algorithms such as [13], which...
incurs a non-negligible T-count and T-depth overhead to the resulting circuit. On the other hand, the fault-tolerant versions of Toffoli adders (such as the ripple carry adder, also known as the Cuccaro adder [11]) have a T-count linear in the number of Toffoli gates whose number is linear in the number of adder wires.

II. RESULTS

Very often it is assumed that a QFT is not related to Toffoli-based circuits. In this work we translate a quantum Fourier adder circuit into a Toffoli-based adder. The construction is iterative and by induction can be applied to adders of arbitrary width. In Sec. III we detail the steps necessary to obtain a reversible adder (Fig. 2) from an initial QFT adder (Fig. 1). To simplify terminology, we consider all $n$-qubit-controlled applications of the $X$ gate as a generalized ($n + 1$)-qubit Toffoli (CCZ) gate. The $CNOT$ (CZ) is a two-qubit Toffoli (CCZ) gate.

Every Toffoli-based adder has a regular structure. This holds also for the adder we derive herein: it performs bitwise addition starting from the highest bits (top wires in each register), after having considered the potential carry bits from all the lower sums. For example, the leftmost gate controlled by $A_2$ in Fig. 2 is computing the XOR sum $A_2 \oplus B_2$, without accounting for carry bits. Afterwards the next two gates (a Toffoli and $CNOT$) are being controlled by $A_1$: the first gate updates the value of $B_2$ to account for the carry arriving from $A_1 \oplus B_1$, and the second gate is effectively computing the XOR sum $A_1 \oplus B_1$. This gate pattern is continued for the entire addition circuit.

Reversible addition circuits have a Toffoli gate count which is linear in the number of addition bits. Thus it is advantageous to compile Toffoli-based adders and then to decompose each generalized Toffoli gate into sequences of three-qubit Toffoli gates [8]. The T count of the decomposed Toffoli-based addition circuits will be linear in the number of qubits of the adder, whereas when the rotations are approximated the T count is a function of approximation and scales logarithmically with the inverse of the approximation error [13]. For small angles in medium-sized QFT addition circuits (e.g., 128 qubits) the T count can easily reach millions.

Systematically transforming a QFT adder into a reversible one uses a sequence of steps which are repeated until the resulting circuit consists entirely of Toffoli gates. The result of our procedure is a circuit that has a regular gate structure (Fig. 2). A second systematic application of gate rewrite rules, based on Toffoli gate commutations, could be applied to obtain the ripple carry adder from [11]. Our reversible adder and the ripple carry adder share a common property: they require no ancillae.

III. METHODS

In this section we will (a) explain the systematic transformation steps (insert QFT and its inverse, and merge/fuse rotation gates) from a QFT- to a Toffoli-based adder, (b) present an example of how rotation gates are merged, and (c) list the transformation algorithm. A step-by-step transformation of a three-qubit QFT adder is illustrated in the Appendix.

The first circuit identity we use [Fig. 3(a)] states that the direction of controlled rotations around the $z$ axis can be changed, in this example, the controlled-S gate. (b) Hadamard gates are merged into $n$-qubit Toffoli gates (in this example $CNOT$).

XOR sum $A_1 \oplus B_1$. This gate pattern is continued for the entire addition circuit.
be flipped. We will also need to remove Hadamard gates [Fig. 3(b)] from the circuits by merging these with the target of multiqubit CCZ gates to obtain Toffoli gates.

A. Inserting QFT and its inverse

The method starts by inserting a reverse (QFT†) and a direct QFT (Fig. 4). The QFTs are inserted before the CZ controlled by the lowest bit from the \( A \) register (\( A_0 \)). The Hadamard gates from the two QFTs transform the CZ into a CX (like in Fig. 3). The next step is to group rotations of the same angle around the CNOT such that the identity from Fig. 5 is applied. Systematic gate cancellations and application of the same identities, as explained in the following section, return the reversible adder from Fig. 2.

B. Merging rotation gates

The QFT and the QFT adder include small angle-controlled rotations which we merge (fuse) into rotations of larger angles. We employ the reverse of a circuit identity, in the following called SQRT, which is the decomposition of arbitrary unitaries into their square roots. For the of example of \( S^2 = Z \), where \( S \) is the square root of the \( Z \) gate, the controlled application of \( Z \) can be expressed using the circuit from Fig. 5 [8].

Novel equivalent formulations of SQRT are presented in Figs. 6 and 7. The correctness of the circuit identities can be shown by computing the exponents of the unitaries that are being applied in a controlled manner (an approach similar to that of Sec. 7 in Ref. [8]).

It is possible to apply SQRT to multiple-controlled operations, as shown in the following. The generalization is enabled by how the CNOTs are applied in Fig. 5. The first step is to double the control wires of the controlled-S gate (Fig. 6). The previous circuit transformation allows us now to transform the CNOTs into simple XORs (see Fig. 7 for the example of \( V = S \) and \( U = Z \)). Finally, it is possible using Figs. 5 and 6 to generalize the SQRT rule to multiqubit controlled operations (Fig. 8).

FIG. 5. Implementing a CZ with controlled-S gates. The circuit identity holds in general for \( V^2 = U \). In this example, \( V = S \) and \( U = Z \).

FIG. 6. Equivalent circuit for a double controlled unitary Z; adding second controls to the first two controlled-S gates does not change the computation.

FIG. 7. Removing the controls from the CNOTs does not change the computation. Two double controlled-S gates and a single controlled-S gate to implement a double controlled-Z.

FIG. 8. Multiqubit controlled gate, where \( U = Z \) using \( V = S \).

FIG. 9. Example of using the SQRT identity as a step during the translation algorithm. The left-hand side is a subcircuit appearing in the QFT adder. The right-hand side is the result of applying the SQRT rule.

FIG. 10. Example illustrating the correctness of the transformation from Fig. 9. (a) The SQRT rule for T and S gates; (b) a CNOT and controlled-T are commuted on the side of the double controlled-S gate; and (c) the second and third wire are swapped.
FIG. 11. (a) An inverse and a direct QFT are inserted before the rightmost CZ gate. (b) The two Hadamards surrounding the CZ gate transform it into a CNOT. (c) The controlled-T and controlled-T† are commuted right next to the CNOT. (d) The direction of the controlled-T gates is changed. (e) The SQRT rule is applied. The result is a double controlled-S gate, a CNOT, and a controlled-T†. (f) The freshly introduced controlled-T† cancels with the leftmost controlled-T. (g) The controlled-S and controlled-S† are commuted right next to the CNOT. (h) The direction of the controlled-S gates is changed. (i) An equivalent circuit to the previous figure. (j) The SQRT rule is applied. The results are a CCZ gate, a CNOT, and a controlled-S†. (k) The direction of the freshly introduced controlled-S† is changed. (l) The freshly introduced controlled-S† cancels with the leftmost controlled-S. (m) The Hadamards surrounding the CCZ transform the gate into a Toffoli. (n) The controlled-S and controlled-S† are commuted right next to the CNOT.

C. Example of merging rotations

The example from Fig. 9 will arise in a three-qubit QFT adder, after inserting a QFT and its inverse, and merging two Hadamard gates with a CZ to form a CNOT. In the following we show step-by-step how to derive the result from Fig. 9. We start from the circuit from Fig. 6, where we replace S with T and Z with S [Fig. 10(a)]. Afterwards, we move the CNOT and controlled-T gate on the side of the double controlled-S gate [Fig. 10(b)]. Finally, we permute the wires and, up to the application of the identity from Fig. 3(a), we obtain a circuit equivalent to the right-hand side of Fig. 9.

D. Algorithm

The idea of the QFT-adder simplification is to use the SQRT identity to combine pairs of m-qubit controlled rotations around the z axis with an angle of $\frac{\pi}{p}$ into single $(m + 1)$-qubit controlled rotation with an angle of $\frac{\pi}{p^2}$. For the circuit from Fig. 1, the controlled-T uses the maximum value $p = 3$.

The first part of the translation algorithm is to insert a pair of QFTs (Sec. III A). The second part of the algorithm has complexity $O(n^4)$, where $n$ is the number of qubits (the QFT has $O(n^2)$ gates, and the algorithm is repeated for each gate to find a matching pair to apply the SQRT rule). The second part of the algorithm is repeating the following steps until the circuit has only Toffoli gates:

1. If possible, eliminate pairs of Hadamard gates surrounding the control of a multiqubit CCZ and transform into a multiqubit Toffoli gate (Fig. 3(b));
2. Commute pairs of opposite angle rotations (e.g., T and T†) next to the new multiqubit Toffoli;
3. Flip the direction of the rotations [Fig. 3(a)];
Fig. 12. (a) The direction of the controlled-S gates is changed. (b) The SQRT rule is applied. The result is a four-qubit controlled-Z gate, a Toffoli and a double controlled-S†. (c) The double controlled-S† cancels with the leftmost double controlled-S. (d) The Hadamards surrounding the CCCZ transform the gate into a four-qubit Toffoli. (e) The Hadamards and the controlled-S gates on the bottom wire cancel. (f) The controlled-T gates on the bottom wire cancel. (g) The two Hadamards are moved next to the CZ. (h) The two Hadamards surrounding the CZ gate transform it into a CNOT. (i) The controlled-S and controlled-S† are commuted right next to the CNOT. (j) The direction of the controlled-S gates is changed. (k) The SQRT rule is applied. The result is a CCZ gate, a CNOT and a controlled-S†. (l) The freshly introduced controlled-S† cancels with the leftmost controlled-S. (m) The Hadamards surrounding the targets of the multiple controlled-Z gates change the gates into Toffolis.

(4) Apply SQRT to the pair of rotations and the CNOT. Obtain a new CNOT and controlled rotation (Fig. 9); and

(5) Find the leftmost controlled rotation that cancels the newly introduced rotation.

IV. DISCUSSION AND CONCLUSION

We showed how to transform a QFT adder into a Toffoli adder by effectively eliminating the QFT from the addition circuit. Instead of decomposing the controlled rotations from the QFT adder, the rotations are merged into ones with larger angles until multiqubit Toffoli gates are obtained.

Eliminating the QFT from computations (e.g., [14]) has been recently of practical interest, because although the circuits have shallow depth in the presence of gate parallelism, the small angles make it difficult for NISQ devices. Small-angle rotations are a significant issue also for the resource efficiency of error-corrected quantum circuits, such that approximate QFT circuits have been proposed and recently optimized [15].

Moreover, it seems that, in some situations, the QFT is not a significant component of quantum circuits (e.g., [16,17]). For example, the Toffoli + H gate set is universal [18], and the ZX and ZH calculus have equivalent computational power [9]. Additionally, eliminating the QFT from circuits might have implications also on quantum circuit simulation methods.

QFT adders are not fundamentally different from the reversible adders. This opens the possibility of optimising QFT-based circuits systematically and also to compile QFT-Toffoli hybrid circuits.

ACKNOWLEDGMENTS

We thank Daniel Herr for correcting a first version of the circuit transformations. A.P. was supported by a Google Faculty Research Award and a Fulbright Senior Researcher Fellowship.

APPENDIX

Figures 11 and 12 illustrate the step-by-step transformation of a three-qubit QFT adder into a Toffoli adder. We include these for completeness. Wider addition circuits can be transformed similarly by applying the algorithm sketched in Sec. III D.
[1] R. Rines and I. Chuang, High performance quantum modular multipliers, arXiv:1801.01081.
[2] L. Ruiz-Perez and J. C. Garcia-Escartin, Quantum arithmetic with the quantum Fourier transform, Quantum Inf. Process. 16, 152 (2017).
[3] A. P. Daniel Koch, Michael Samodurov, and P. M. Alsing, Gate-based circuit designs for quantum adder based quantum random walks on superconducting qubits, arXiv:2012.10268.
[4] H. Thapliyal, E. Muñoz-Coreas, and V. KhaIus, Quantum carry lookahead adders for NISQ and quantum image processing, arXiv:2106.04758.
[5] S. Sajadimanesh, J. P. L. Faye, and E. Atoofian, Practical approximate quantum multipliers for NISQ devices, in Proceedings of the 19th ACM International Conference on Computing Frontiers, CF ’22 (Association for Computing Machinery, New York, 2022), pp. 121–130.
[6] T. J. Yoder, Universal fault-tolerant quantum computation with Bacon-Shor codes, arXiv:1705.01686.
[7] T. Häner, M. Roetteler, and K. M. Svore, Factoring using 2n+ 2 qubits with Toffoli-based modular multiplication, Quantum Inf. Comput. 17, 673 (2017).
[8] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Elementary gates for quantum computation, Phys. Rev. A 52, 3457 (1995).
[9] S. Kuijpers, J. van de Wetering, and A. Kissinger, Graphical Fourier theory and the cost of quantum addition, arXiv:1904.07551.
[10] In the sense of Boolean reversible logic.
[11] S. A. Cuccaro, T. G. Draper, S. A. Kutin, and D. P. Moulton, A new quantum ripple-carry addition circuit, arXiv:quant-ph/0410184.
[12] P. Gossett, Quantum carry-save arithmetic, arXiv:quant-ph/9808061.
[13] P. Selinger, Efficient Clifford+t approximation of single-qubit operators, Quantum Inf. Comput. 15, 159 (2015).
[14] S. Aaronson and P. Rall, Quantum approximate counting, simplified, in Symposium on Simplicity in Algorithms (SIAM, Philadelphia, PA, 2020), pp. 24–32.
[15] Y. Nam, Y. Su, and D. Maslov, Approximate quantum Fourier transform with o (n log (n)) t gates, npj Quantum Inf. 6, 1 (2020).
[16] D. Aharonov, Z. Landau, and J. Makowsky, The quantum FFT can be classically simulated, arXiv:0611156.
[17] M. Van Den Nest, Efficient classical simulations of quantum Fourier transforms and normalizer circuits over Abelian groups, Quantum Inf. Comput. 13, 1007 (2013).
[18] Y. Shi, Both Toffoli and controlled-NOT need little help to do universal quantum computing, Quantum Inf. Comput. 3, 84 (2003).