Studying the cost of n-qubit Toffoli gates

Francisco Orts[1 [0000−0002−4312−3671]], Gloria Ortega[1 [0000−0002−6563−2717]], and Ester M. Garzón[1 [0000−0002−0568−5470]]

Supercomputing-Algorithm Research Group, Informatics Department,
University of Almería, Almería, Spain
https://hpca.ual.es/
{francisco.orts,gloriaortega,gmartin}@ual.es

Abstract. There are several Toffoli gate designs for quantum computers in the literature. Each of these designs is focused on a specific technology or on optimising one or several metrics (T-count, number of qubits, etc.), and therefore has its advantages and disadvantages. While there is some consensus in the state of the art on the best implementations for the Toffoli gate, scaling this gate for use with three or more control qubits is not trivial. In this paper, we analyse the known techniques for constructing an n-qubit Toffoli gate, as well as the existing state-of-the-art designs for the 2-qubit version, which is an indispensable building block for the larger gates. In particular, we are interested in a construction of the temporary logical-AND gate with more than two control qubits. This gate is widely used in the literature due to the T-count and qubit reduction it provides. However, its use with more than two control qubits has not been analysed in detail in any work. The resulting information is offered in the form of comparative tables that will facilitate its consultation for researchers and people interested in the subject, so that they can easily choose the design that best suits their interests. As part of this work, the studied implementations have been reproduced and tested on both quantum simulators and real quantum devices.

Keywords: Quantum circuits · Toffoli gate · n-qubit Toffoli gate.

1 Introduction

The circuit paradigm is the most widely used paradigm for programming a quantum computer [11]. This paradigm consists of using quantum gates (unitary operations) to manipulate the information contained in qubits. In the classical world, it is possible to limit the number of existing logic gates. For example, there are only two classical gates that act on a bit: the NOT gate and the identity. However, in the quantum case, there are infinitely many gates that can act on 1 qubit, given their special nature [4]. Although it is impossible to have a universal set of gates that generate the rest of the infinite quantum gates (although there is a set that allows us to approximate them), there are certain gates that are well known in the community and widely used due to the operation they perform. This is the case of the Toffoli gate, which, given three values c_1, c_2,

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_10

and t, performs the operation $t \oplus c_1 c_2$. Using the correct notation, the operation can be expressed as $Toffoli(|c_1\rangle |c_2\rangle |t\rangle) = |c_1\rangle |c_2\rangle |t \oplus c_1 c_2\rangle$. By convention, c_1 and c_2 are usually called control qubits, and t target qubit. A simple example of the usefulness of this operation is to operate on $t = 0$ and considering only the standard bases as possible values for c_1 and c_2. In such a case, the result $c_1 c_2$ coincides with the classical AND operation. The Toffoli gate is useful in operations as varied as adders [12], cryptography [17], image processing [13], etc.

When designing a quantum circuit, one should try to make it as small as possible in order to optimise the use of resources. In fact, a small circuit is a very valuable resource even if it has no quantum properties, since it can be used as part of major circuits [15]. However, it is not always easy to measure the cost of a circuit in order to determine if it is "smaller" than other. Two metrics are particularly important in today's NISQ devices: the number of ancilla qubits, and the so-called T-count. Regarding the ancilla qubits, it is necessary to minimise them as current quantum devices have a low number of qubits, [10]. The second metric, the T-count, is the number of T-gates used by a circuit. NISQ devices are very sensitive to external and internal noise. The use of T-gates allows the use of error detection and correction codes to reduce the effects of noise. However, the cost of the T-gate is much higher than the cost of other gates (in the order of 100 times more), so it is important and necessary to keep the number of T-gates small [14].

In this paper, we focus on studying the use of the Toffoli gate using more than two control qubits, formally labeled as n-qubit Toffoli gates for the general n case (being n the number of involved qubits). As will be demonstrated later, implementing Toffoli gates with n control qubits will require the use of Toffoli gates with two control qubits (that is, the normal Toffoli gate). Therefore, it is necessary to study the implementations of the Toffoli gate available in the state of the art. It is worth mentioning that some implementations are focused on a particular technology. For example, there are Toffoli gate designs focused exclusively on reducing the number of controlled gates required for its implementation [8]. These gates have this objective as in linear optics is only possible to implement controlled quantum gates probabilistically. In this work we will not consider gates dependent on the physical technologies of the quantum computer, but we will consider those focused on reducing the T-count and the number of ancilla qubits.

2 Decomposition of n-qubit controlled gates

Controlled operations are operations that are only executed when all control qubits are set to one. Let be U a unitary operation that acts on a single qubit. For every unitary operation U there exist unitary operators A, B and C such that $ABC = I, U = e^{i\alpha} A \times B \times C$, being α some overall phase factor [1]. Note that, in case the qubit control is $|0\rangle$, only the operations $ABC = I$ will be performed. In case it is $|1\rangle$, the operation $e^{i\alpha} A \times B \times C = U$ will be computed [11]. If we now focus on the case of a 2-qubit controlled operation U, the approach is different.

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_10

It is necessary to find an operator V such that $U = V^2$. For instance, in the case of the Toffoli gate the operation U would be X. Then, if V is defined as $(1-i)(I+iX)/2$, we see how the equality $X = ((1-i)(I+iX)/2)^2$ is satisfied.

Note that for the construction of a gate with n control qubits, gates with $n-1$ control qubits are used. Therefore, methodologies are proposed to design gates controlled by n qubits using iterative processes based on gates controlled by 1 or 2 qubits, using auxiliary qubits to store intermediate results. Nielsen and Chuag [11] presented a procedure to implement $C^n(U)$ gates consisting of computing the product $c_1c_2...c_n$ using Toffoli gates. The idea is to first compute c_1c_2 on an auxiliary qubit, then to compute the product of this value with c_3 on another auxiliary qubit, and so on. The operation will therefore require $n-1$ auxiliary qubits. Finally, to avoid rubbish outputs the circuit must be reversed.

Since order does not matter in a product, He et al. proposed to parallelise the computation $c_1c_2...c_n$ so that the result can be obtained more quickly [6]. This product is computed as follows:

1. Step 1: $p_1 = c_1c_2$ is computed and stored in the first ancilla qubit. At the same time, $p_2 = c_3c_4$ is also computed and stored in the second ancilla qubit. Since both operations does not share any qubit, they can be computed in parallel.
2. Step 2: $p_3 = p_1p_2$ is computed.
3. Step 3: $p_4 = p_3c_5$ is computed.
4. Step 4: p_4 is "copied" into the target qubit.
5. Step 5−7: The circuit is reverted using Bennett's garbage removal scheme [3].

Barenco et al. proposed another scheme to build a multiple control Toffoli gate [2]. This work takes into account factors such as the possibility of working directly with negated controls and error correction. The main advantage obtained is that it manages to implement the gate using one less qubit. On the downside, the cost is much higher than previous schemes, going from needing $n-1$ Toffoli gates with two control qubits to needing $4n-8$.

Although we have found other schemes in the literature, they contain one or more gates that are theoretically defined but whose implementation is not addressed. This is why we do not include them in this paper. As a summary of this section, the information on the analysed schemes is compiled in Table 1.

Design	Number of Toffoli gates	Delay	Ancilla qubits
Nielsen and Chuang [11]	$n-1$	$O(n)$	$n-1$
He et al. [6]	$n-1$	$O(Log(n))$	$n-1$
Barenco et al [9]	$4n-8$	$O(n)$	$n-2$

Table 1. Existing schemes to build a n-qubit Toffoli gates. The number of ancilla qubits may be increased due to the implementation of the 2-qubit Toffoli gates.

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_10

3 Implementations of the Toffoli gate

In the previous subsection, has been demonstrated the need to use 2-qubit Toffoli gates in order to build the n-qubit versions. It is therefore essential to consider existing versions of the 2-qubit Toffoli gate. There are designs in the literature that allow an approximation of the result. That is, they do not guarantee the correct result even in a noise-free device. This kind of gates has not been included in this work.

A Toffoli gate design has already been presented in the previous section. To make this design effective, it is necessary to specify an implementation for the controlled-V gate, such that $V^2 = X$ is satisfied. Amy et al. proposed a design for this gate, consisting of two CNOT gates, two Hadamard gates, two T gates, and one T' gate [1]. The T-count of this version of the V gate (as well as the V' gate) is 3. Since the Toffoli gate contains three V gates, its T-count is 9. It also requires 3 qubits for its implementation. Although this may seem obvious, some later implementations use extra qubits for their implementation. This is why it is important to keep this count.

From the previous Toffoli gate, some operations can be reorganised and simplified, as explained in Amy et al [1]. This new version reduces the T-count by 2 with respect to the previous design, keeping the same number of qubits. Likewise, the number of CNOT and Hadamard gates is also reduced.

Jones proposed a new implementation [7] which allows the T-count to be reduced to 4. At the cost, however, of using an ancilla qubit to hold the intermediate result before being transferred to the target qubit. This Toffoli gate is based on an implementation of the iX gate proposed by Selinger [16], which has a T-count of 4. Jones' Toffoli gate has no T gates beyond those contained in Selinger's iX gate, so its quantum cost is also 4. Jones' contribution is not only limited to this reduction of the T-count, as explained below.

In quantum computing, reversing qubits after use to make them available for future operations is considered a good practice. In fact, in NISQ devices, it is a necessity due to the limited number of available qubits. After applying a Toffoli gate, two possibilities can occur:

- The value contained in the target qubit must be retained, since it will be one of the values measured and used at the end of the circuit.
- The value contained in the target qubit is only used temporarily or as an auxiliary operation and, once used, is no longer needed.

In the latter case, the operation performed by the Toffoli gate must be reversed. For this, it is necessary to apply a second Toffoli gate, which will then be focused only on returning the qubits involved to the value they had prior to the application of the first Toffoli gate [3]. Note that this operation will increase the total T-count (but not the number of qubits).

Returning to Jones' circuit, the c_1c_2 operation is computed using the iX gate and a S' gate. Subsequently, the operation $t \oplus c_1c_2$ is performed on the target qubit, and the c_1c_2 operation contained in the ancilla qubit is uncomputed.

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_10

However, instead of applying the inverse circuit to reverse the operation, Jones resorts to a measure-and-fixup approach. Specifically, a Hadamard gate is applied to then measure and classically control the obtained value to correct the phase (which will be 1 if the measurement is 0, and $(-1)^{q_0 q_1}$ if it is 1). The cost of applying the inverse circuit would be, in terms of T-count, 4 (and the global T-count 8). Using this approximation, the T-count is 0 (and the global T-count 4).

Despite the obvious improvements it offers, the Toffoli gate proposed by Jones has two points to bear in mind. First, it uses an auxiliary qubit, i.e., one more qubit than the other implementations. Second, although the c_1c_2 operation is reversed, the same is not true for the $t \oplus c_1c_2$ operation. Aware of these points, Gidney [5] separated Jones' Toffoli gate into two parts. A first gate, called temporary logical-AND gate, computes the c_1c_2 operation on an ancilla qubit prepared in state $\frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{i\pi}{4}}|1\rangle)$. And a second gate whose function is to reverse the operation carried out by the previous one using the described measure-and-fixup approach. By this simple idea of delaying the uncomputation of the AND operation until such time as it is no longer needed, Gidney saves the extra qubit used by the previous circuit, and reverses the gate operations altogether.

As a summary, the information on the possible implementations of the Toffoli gate is compiled in Table 2.

Design	T-count	T-count with uncomputation	Ancilla inputs
Amy et al (1). [1]	9	18	0
Amy et al (2). [1]	7	14	0
Jones [7]	4	4	1
Gidney [5]	4	4	0

Table 2. Comparison in terms of T-count in terms of computation, T-count in terms of computation and uncomputation, and number of ancilla inputs between our proposal and the best designs in the literature.

4 Analysis and Comparison

To test the correct operation of the circuits and to reinforce the metrics used, all the gates have been tested and measured using the IBM Q Experience platform, with the circuits being written in Python and tested on real devices and, when not possible due to circuit size, on a simulator. The measurement methodology described in Orts et al. [12].

The possible implementations of m-qubit Toffoli gates arise from the combination of the schemes listed in Table 1 with the Toffoli gate implementations studied in Table2. Table 3 shows the obtained metrics for each scheme-design

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_10

combination, in terms of ancilla inputs and T-count. Since this information is trivial, the delay is not indicated in the table. For the sake of clarity, we again clarify that the fastest scheme is the He et al. one (logarithmic order) [7], followed by the Nielsen and Chuang scheme (linear order) [11], and finally the Barenco scheme (linear order, but slower than the Nielsen scheme because it performs a higher number of operations, as discussed in Section 2) [2].

Design	Nielsen and Chuang [11]		He et al. [6]		Barenco [2]	
	T-count	Ancilla inputs	T-count	Ancilla inputs	T-count	Ancilla inputs
Amy et al. (1) [1]	$18n-18$	$n-1$	$18n-18$	$n-1$	$64n-144$	$n-2$
Amy et al. (2) [1]	$14n-14$	$n-1$	$14n-14$	$n-1$	$56n-112$	$n-2$
Jones [7]	$4n-4$	$2n-2$	$4n-4$	$2n-2$	$16n-32$	$2n-3$
Gidney [5]	$4n-4$	$n-1$	$4n-4$	$n-1$	$16n-32$	$n-2$

Table 3. Comparison in terms of T-count (including uncomputation) and ancilla inputs of m-qubit Toffoli gates created according to existing schemes using the most efficient Toffoli gates (of 2 control qubits) available in the literature. It is important to note that, although the Nielsen and Chuang and He et al. schemes share the same values, the Nielsen scheme has a linear delay and the He et al. scheme has a logarithmic delay. Regardless of the chosen scheme, the most appropriate uncomputation technique is adopted for each gate.

In terms of T-count, the best implementations are given by the Nielsen and Chuan [11] and He et al. [7] schemes using the Jones gates or the Gidney temporary, with a final value of $4n-4$. Since the logical-AND temporary gate allows to reduce the number of ancilla inputs (it needs $n-1$ versus $2n-2$ using the Jones gate), it becomes the best option in these terms. Note also that the number of $n-1$ ancilla qubits is the best possible for these two schemes, and is also achieved by the designs of Amy et al. However, using Barenco's scheme, the number of ancilla inputs needed can be reduced by one. At the cost, however, of a large increase in the T-count. The best value obtained in this scheme is again obtained using the temporary, achieving a T-count of $16n-32$ with $n-2$ ancilla inputs. That is, a $12n-28$ increase in the T-count to save a single qubit.

5 Conclusions

In this paper we provide a review of the existing techniques for constructing n-qubit Toffoli gates. These gates has been analized (and reproduced) in terms of noise tolerance and ancilla qubits. Their design is provided using only Clifford+T gates. Moreover, a revision on the state-of-the-art reversible Toffoli gates has been carried out. Appropriate metrics have been considered for the measurement and comparison of quantum gates and circuits. The analysis has been carried out with two essential goals in mind: first, to find all the procedures to build a

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_10

n-qubit Toffoli gate, and second to dispose of the best implementations of the Toffoli gates to, in combination with the mentioned procedures, to build the most optimized n-qubit Toffoli gate possible in terms of T-count and number of ancilla qubits. Special attention has been paid to the temporary logical-AND gate, whose design to act with more than two control qubits had not yet been analyzed in the literature. Finally, the possibilities has been compared in such terms, highlighting the advantages and the drawbacks of each candidate.

References

1. Amy, M., Maslov, D., Mosca, M., Roetteler, M.: A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **32**(6), 818–830 (2013)
2. Barenco, A., Bennett, C., Cleve, R., DiVincenzo, D., Margolus, N., Shor, P., Sleator, T., Smolin, J., Weinfurter, H.: Elementary gates for quantum computation. Physical review A **52**(5), 3457 (1995)
3. Bennett, C.: Logical reversibility of computation. IBM journal of Research and Development **17**(6), 525–532 (1973)
4. Bernhardt, C.: Quantum computing for everyone. Mit Press (2019)
5. Gidney, C.: Halving the cost of quantum addition. Quantum **2**, 74 (Jun 2018)
6. He, Y., Luo, M., Zhang, E., Wang, H., Wang, X.: Decompositions of n-qubit toffoli gates with linear circuit complexity. International Journal of Theoretical Physics **56**(7), 2350–2361 (2017)
7. Jones, C.: Low-overhead constructions for the fault-tolerant toffoli gate. Physical Review A **87**(2), 022328 (2013)
8. Lanyon, B., Barbieri, M., Almeida, M., Jennewein, T., Ralph, T., Resch, K., Pryde, G., O'brien, J., Gilchrist, A., White, A.: Simplifying quantum logic using higher-dimensional hilbert spaces. Nature Physics **5**(2), 134–140 (2009)
9. Maslov, D., Dueck, G., Miller, D., Negrevergne, C.: Quantum circuit simplification and level compaction. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **27**(3), 436–444 (2008)
10. Mohammadi, M., Eshghi, M.: On figures of merit in reversible and quantum logic designs. Quantum Information Processing **8**(4), 297–318 (2009)
11. Nielsen, M., Chuang, I.: Quantum computation and quantum information (2002)
12. Orts, F., Ortega, G., Combarro, E.F., Garzón, E.M.: A review on reversible quantum adders. Journal of Network and Computer Applications p. 102810 (2020)
13. Orts, F., Ortega, G., Cucura, A., Filatovas, E., Garzón, E.: Optimal fault-tolerant quantum comparators for image binarization. The Journal of Supercomputing pp. 1–12 (2021)
14. Orts, F., Ortega, G., Garzon, E.M.: Efficient reversible quantum design of sign-magnitude to two's complement converters. Quantum Information & Computation **20**(9-10), 747–765 (2020)
15. Pérez-Salinas, A., Cervera-Lierta, A., Gil-Fuster, E., Latorre, J.: Data re-uploading for a universal quantum classifier. Quantum **4**, 226 (2020)
16. Selinger, P.: Quantum circuits of t-depth one. Physical Review A **87**(4), 042302 (2013)
17. Zhou, R., Wu, Q., Zhang, M., Shen, C.: Quantum image encryption and decryption algorithms based on quantum image geometric transformations. International Journal of Theoretical Physics **52**(6), 1802–1817 (2013)

ICCS Camera Ready Version 2022
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-08760-8_10