On the advantages of relative phase Toffoli gates

Unathi Skosana[1] and Mark Tame

Department of Physics, SU, Matieland 7602, South Africa

E-mail: [1]`unathiskosana@protonmail.com`

Abstract. Many of the quantum algorithms that make theoretical guarantees on computational speedups are well beyond the capabilities of currently existing noisy intermediate-scale quantum (NISQ) hardware. The requisite resource demands of these algorithms (*e.g.* qubits, quantum gates, circuit repetitions etc) make their implementation impractical on such hardware. For some algorithms, various approaches exist to reduce these demands. We consider one such approach here. This approach uses relative phase Toffoli gates, advantageous over regular Toffoli gates due to their smaller circuit size. As a proof-of-concept demonstration of the utility of relative phase Toffoli gates, we have used a configuration of these gates in constructing the compiled quantum phase estimation routine to achieve a complete factoring of $N = 21$.

1. Introduction

In classical computation the reversible Toffoli gate is a universal logic gate, *i.e.* any logic circuit L which computes a Boolean function of the form $f : \{0,1\}^n \to \{0,1\}$ can be decomposed into a reversible logic circuit L', equivalent in operation, made up of only Toffoli gates. The truth table and circuit diagram for a Toffoli gate are shown in figure 1.

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

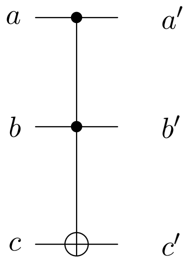

Figure 1. Truth table and circuit for a Toffoli gate.

The reversibility of a Toffoli gate implies that its operation can be realized as a unitary quantum logic gate ($U^{-1} = U^{\dagger}$), making reversible Boolean arithmetic reproducible on a quantum computer. The Toffoli gate, which is a doubly-controlled NOT (CCX) gate, is described by the following map on a quantum state,

$$\mathrm{CCX}_{abc} : |a, b, c\rangle \mapsto |a, b, c \oplus a \cdot b\rangle \,, \tag{1}$$

where $\oplus$ is modulo 2 addition, $\cdot$ is the bitwise inner product and qubit Hilbert spaces are separated by commas. Notwithstanding their apparent importance, current quantum hardware do not natively support Toffoli gates but rather physically implement a universal gate-set made up of single-qubit gates (*e.g.* $\sqrt{\mathrm{X}}, \mathrm{X}, \mathrm{RZ}$) and a single two-qubit entangling gate (*e.g.* $\mathrm{CX}, \mathrm{CZ}, \sqrt{\mathrm{iSWAP}}$) with high fidelity ($\gtrsim 99\%$ for superconducting qubits, see Ref. [1]). A Toffoli gate is then decomposed into single and two-qubit gates from this native gate-set [2]. Due to the effects of decoherence, there is an upper limit on the number of two-qubit gates over a set of qubits that can be in a circuit, this makes the study of Toffoli gates a subject of interest for practical quantum computing. It has been shown that a three-qubit Toffoli gate (CCX) cannot be implemented with less than five two-qubit gates [3, 4], the traditional three-qubit decomposition into six controlled-NOT (CX) and seven $T/T^\dagger$ gates is shown below

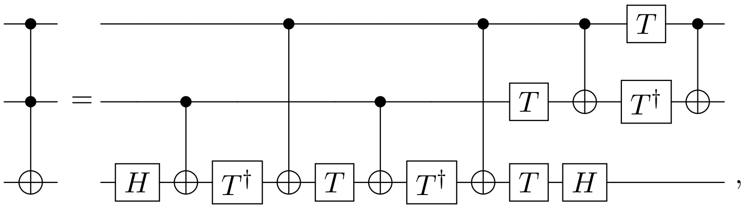

Figure 2. Circuit diagram showing the decomposition of a Toffoli gate in terms of elementary gates; six controlled-NOT (CX) and seven $T/T^\dagger$ gates.

where H is a Hadamard gate and $T = \mathrm{diag}(1, e^{i\frac{\pi}{4}})$. However, there exists variants of the Toffoli gate, smaller in circuit size, collectively called 'relative phase' Toffoli gates due to their operation being equivalent to that of a Toffoli modulo a relative phase shift. Maslov [5] showed that the utility and application of these relative phase variants extends beyond specific and commonly conceived scenarios, leading to a reduction in gate count of known configurations of multiply-controlled Toffolis while preserving functional correctness. Our recently published scheme [6] represents such a specific application of relative phase Toffoli gates, where we employed them for carrying out a demonstration of Shor's quantum algorithm [7] for factoring $N = 21$ on IBM Q's quantum processors. Hence, we introduce the relative phase Toffoli gate and characterize its performance.

2. Generation of entanglement with relative phase Toffoli gates

The relative phase variant which implements a three-qubit Toffoli gate up to a relative shift ($|101\rangle \mapsto -|101\rangle$) is the one considered. The decomposition of such a gate by Margolus [8] , as shown in figure 3, optimally uses three CX gates and four single-qubit gates [9]. We label this gate as RCCX. If in the use of a Toffoli gate such a relative phase shift is permitted, the CX count is significantly reduced in comparison to the full Toffoli shown in figure 2. Consider such an example scenario where we seek to generate entanglement from a state prepared in a three-qubit register:

$$|\psi\rangle = X_0 H_1 |0\rangle_0 |0\rangle_1 |0\rangle_2 = |1\rangle_0 |+\rangle_1 |0\rangle_2 \,, \tag{2}$$

where X is a bit-flip ($|0\rangle \mapsto |1\rangle$,$|1\rangle \mapsto |0\rangle$) and H is a Hadamard gate ($|0\rangle \mapsto |+\rangle$,$|1\rangle \mapsto |-\rangle$).

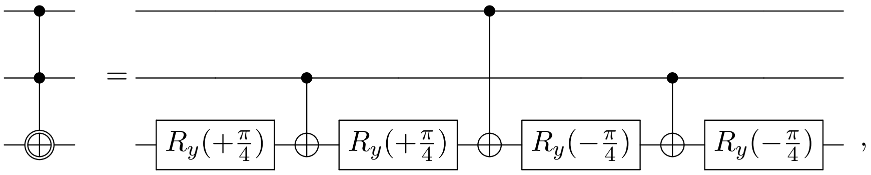

Figure 3. Circuit diagram showing the decomposition of a Margolus gate in terms of elementary gates; three controlled-NOT (CX) and four $R_y(\pi/4)$ single qubit gates, where $R_y(\pi/4) = e^{-i\pi/8} SHTHSZ$,$S = \mathrm{diag}(1, i)$ and $Z = \mathrm{diag}(1, -1)$.

Applying a CCX_{012} to the above state controlled by qubits $0, 1$ and targeted on qubit 2, we produce the state

$$\begin{aligned}\mathrm{CCX}_{012}\,|\psi\rangle = \mathrm{RCCX}_{012}\,|\psi\rangle &= \frac{1}{\sqrt{2}}\,|1\rangle_0\,(|0\rangle_1\,|0\rangle_2 + |1\rangle_1\,|1\rangle_2),\\ &= |1\rangle_0\,|\Phi^+\rangle_{12}\,,\end{aligned} \tag{3}$$

$|\Phi^+\rangle = 1/\sqrt{2}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle)$ is one of the maximally entangled two-qubit Bell states. In such a scenario, one observes that the state $|101\rangle_{012}$ never arises in the register and thus the operation of CCX and RCCX gates are equivalent. We characterize the performance of these two gates by performing state tomography of qubits 1 and 2 on the state in (3), experimentally prepared on IBM Q's seven-qubit quantum processor *ibmq_casablanca* [10] through the software development kit Qiskit [11]. A typical measured density matrix from the ensemble of measured density matrices is shown in figure 4. To quantitatively evaluate the performance of the two gates in generating the Bell state in (3), we measure the fidelity for two quantum states ρ and σ, defined as $F(\rho, \sigma) = \mathrm{tr}\Big(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}^{\,2}\Big)$ [12]. We measured (within 95% confidence intervals) the fidelities to be $F(|\Phi^+\rangle\!\langle\Phi^+|\,, \sigma_{\mathrm{CCX}}) = 0.929 \pm 0.003$ and $F(|\Phi^+\rangle\!\langle\Phi^+|\,, \sigma_{\mathrm{RCCX}}) = 0.972 \pm 0.008$ for measured density matrices with a CCX and a RCCX gate, respectively. Each measurement performs 8192 circuit repetitions and all other subsequent measurements. The fidelity ranges between 0 and 1, a fidelity equal to 1 means the measured state is equal to the ideal state $\rho = |\Phi^+\rangle\,\langle\Phi^+|$ and fidelity less than 1 indicates how "far away" the state is from ideal. In a larger circuit where more than one Toffoli gate is replaced in such a manner the overall functionality of the circuit would be unaltered, and the difference between the performance of the two gates would be much more discernible.

As further characterization of the two gates concerned, we perform quantum process tomography and reconstruct the χ matrix representation of a quantum channel $\mathcal{E}$ that describes the operation of a circuit. We do this for circuits on the aforesaid quantum processor; *ibmq_casablanca*, which prepared the states shown in figure 4. How closely a quantum channel $\mathcal{E}$ approximates U (the ideal circuit) is described by the average gate fidelity given by:

$$\bar{F}(\mathcal{E}, U) = \int d\psi\,\langle\psi|U^\dagger\mathcal{E}(|\psi\rangle\!\langle\psi|)U|\psi\rangle\,, \tag{4}$$

where the integration is over the uniform Haar measure on the state space, and $\mathcal{E}(\cdot)$ is an evolution with respect to the quantum channel $\mathcal{E}$. The χ-matrix representation of $\mathcal{E}$ is a matrix χ such that a density matrix ρ under the action of quantum channel $\mathcal{E}$ evolves as such:

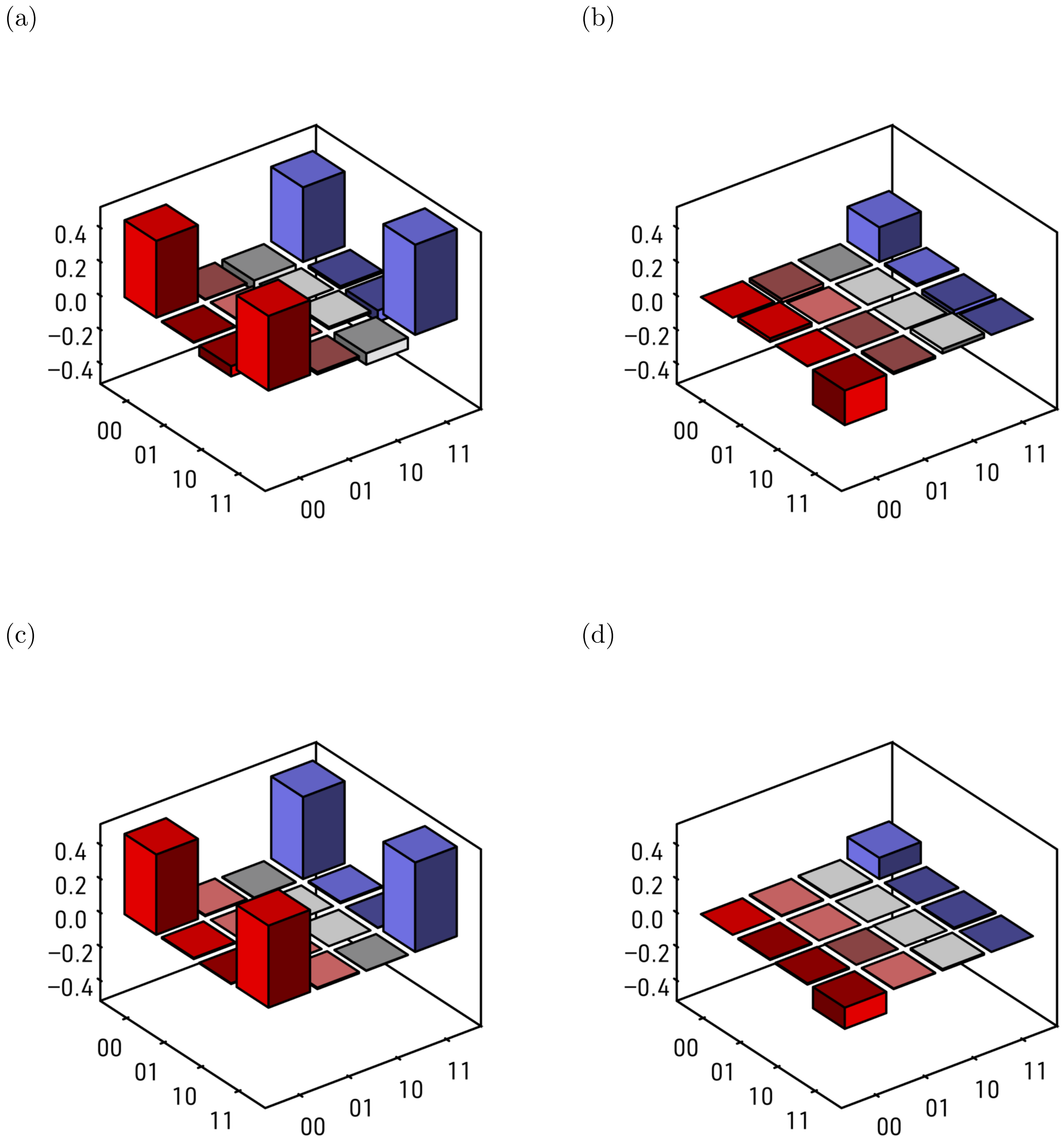

Figure 4. (a) Real and (b) imaginary parts of the measured density matrix of the state of qubits 1 and 2 in (3) prepared with a CCX gate on IBM Q's *ibmq_casablanca*. Similarly, (c) and (d) are real and imaginary parts, respectively, of the same state prepared with a RCCX gate.

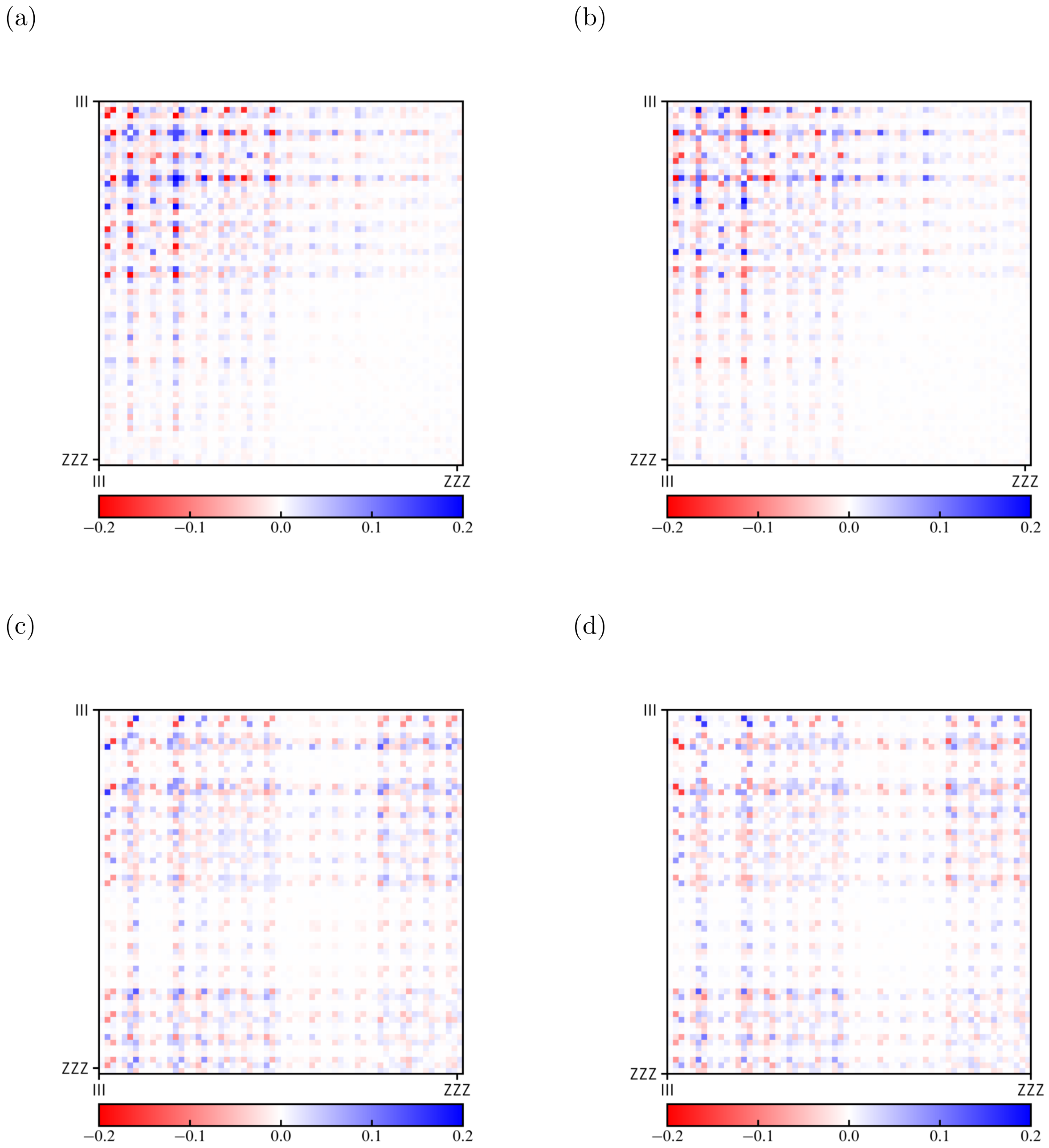

Figure 5. (a) Real and (b) imaginary part of the difference between experimentally measured and the ideal χ-matrix matrix presentation of the quantum channel prepared with a CCX gate on IBM Q's *ibmq_casablanca*, $\mathcal{E}_{\text{ideal}} - \mathcal{E}_{\text{CCX}}$; The largest element differences are 0.254 and 0.322, respectively. Similarly, (c) and (d) are real and imaginary parts, respectively, of the difference the measured and the ideal χ-matrix matrix presentation of the quantum channel prepared with a RCCX gate on IBM Q's *ibmq_casablanca*, $\mathcal{E}_{\text{ideal}} - \mathcal{E}_{\text{RCCX}}$. The largest element differences are 0.163 and 0.163, respectively. In all figures the color bar is rescaled to a range between -0.2 and 0.2 for visual clarity.

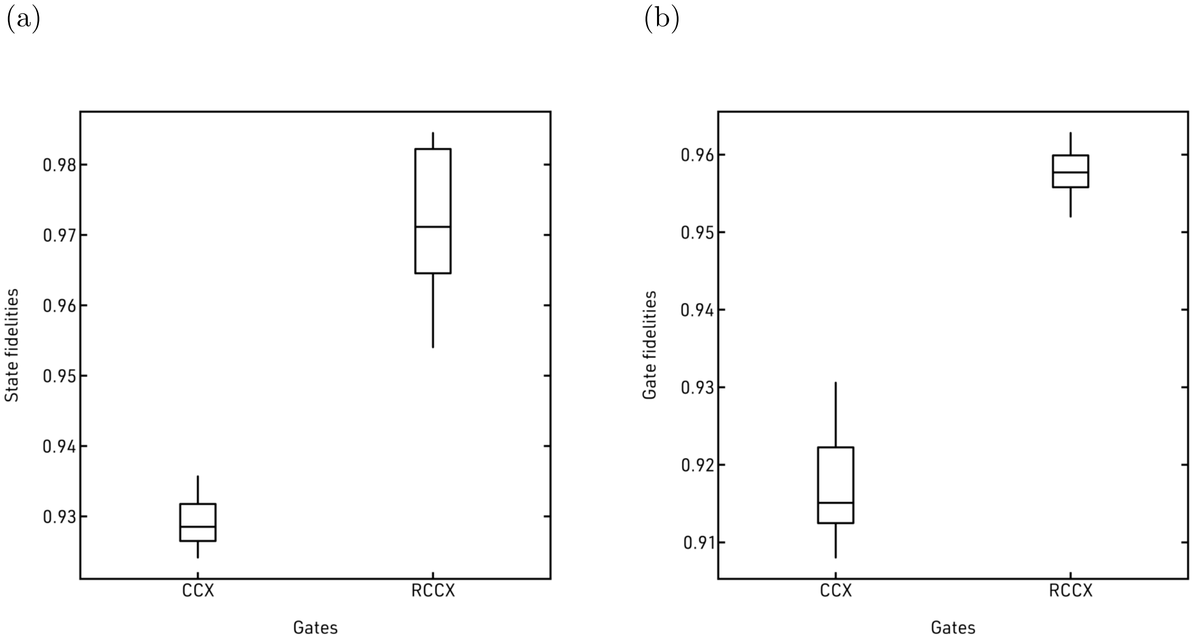

Figure 6. (a) State fidelities between the ideal Bell state $|\Phi^+\rangle\langle\Phi^+|$ and the members of the measured ensemble of density matrices σ_{CCX} and σ_{RCCX} respectively, and (b) average gate fidelities of the quantum channels that prepare the state in (3) with a CCX and RCCX gate respectively.

$$\mathcal{E}(\rho) = \sum_{i,j} \chi_{ij} E_i \rho E_j^\dagger, \tag{5}$$

here the E_i's are n-fold tensor products of all 3^n combinations of Pauli matrices X, Y, Z plus the 2×2 identity matrix I (*e.g.* $E_0 = I \otimes I \otimes I$). See references [13, 14] for closed-form expressions of (4). We measured the average gate fidelities to be $\bar{F}_{\text{CCX}}(\mathcal{E}, U) = 0.917 \pm 0.005$ and $\bar{F}_{\text{RCCX}}(\mathcal{E}, U) = 0.958 \pm 0.002$ respectively, and show differences between the respective measured and ideal χ-matrices in figure 5. In the case of using a RCCX gate, the target unitary preparing the state in (3) is better reconstructed than a CCX gate on the respective processor; the measured χ-matrix for the quantum channel $\mathcal{E}_{\text{RCCX}}$ shows a smaller maximum element-wise difference from its respective ideal χ-matrix than the measured χ-matrix for the quantum channel $\mathcal{E}_{\text{CCX}}$. This is also corroborated by Figure 6, which shows boxplots of state fidelities and average gate fidelities, respectively. We see that comparatively the RCCX gate prepares a Bell state with a higher state fidelity than a CCX gate. Similarly, due to the RCCX gate being comparatively smaller than the CCX gate in terms of its circuit size, it has an overall better average gate fidelity on the IBM Q's *ibmq_casablanca* processor.

3. Relative phase Toffoli gates for quantum factoring

In 2012, the integer $N = 21$ was factored using a small-scale quantum processor, setting the record for the largest integer factored with Shor's quantum factoring algorithm [15]; Similarly in 2019, the integer $N = 21$ was factored again [16]. These two schemes adopt an iterative version of Shor's algorithm which employs a single qubit in the control register that is recycled through feed forward operations to reduce the qubit overhead of the algorithm. However, at the time of writing, real-time conditional feed forwards operations are not widely supported among current quantum hardware, which the latter implementation [16] circumvented by splitting up the iterations of the algorithm into separate circuits. Moreover, upon further scrutiny, the former implementation [15] fell one iteration short of achieving full factoring.

Building upon the implementation of [15], we identified that Toffoli gates in the algorithm's construction could be replaced with the relative phase Toffoli gate studied here while leaving the operation of the circuit unaltered. As we have seen the latter gate decomposes into fewer elementary gates than the former, and hence improving the fidelity of the output state. As a result, we were able to add a further iteration to the algorithm while maintaining a clear resolution in algorithmic output, from which we were able to successfully extracted the factors of $N = 21$. Our scheme is based on the non-iterative version of Shor's algorithm which uses three qubits for the control register. Notwithstanding the increase in number of qubits in comparison to the aforesaid implementation [15], we were able to successfully factor the integer $N = 21$, and additionally verify the presence of entanglement across the quantum registers in the circuit, See Ref. [6] for details.

4. Summary

Through the use of relative phase Toffoli gates studied in this paper, we were able to go beyond the demonstration of Ref. [15] in fully factoring $N = 21$. In the aforementioned reference, they implemented a compiled and iterative version of Shor's quantum algorithm to factor $N = 21$, and their scheme uses full Toffoli gates to realize Shor's quantum algorithm. Due to this, they were only able to implement two iterations of the algorithm, which falls one iteration short of the minimum number of iterations to be able to extract the factors $N = 21$ from the algorithmic output. Our scheme [6] replaces the full Toffoli gates with relative phase Toffoli gates, while remaining functionally correct (relative phase shifts introduced by gate do not affect the circuit's correctness). This replacement significantly reduces the number of elementary gates in the circuit, allowing our scheme to implement the minimum number of iterations of the algorithm for the full factorization of $N = 21$. We implemented the algorithm on IBM quantum processors using only 5 qubits, successfully verifying the presence of entanglement between the control and work register qubits, which is a necessary condition for the algorithm's speedup in general. Future work in this direction would explore whether the use of relative phase Toffoli gates may be viable in carrying out Shor's algorithm for larger integers, or other algorithms in systems with a limited number of noisy qubits.

Acknowledgments

We acknowledge the use of IBM Quantum services for this work. The views expressed are those of the authors, and do not reflect the official policy or position of IBM or the IBM Quantum team. We thank Taariq Surtee and Barry Dwolatzky at the University of the Witwatersrand and Ismail Akhalwaya at IBM Research Africa for access to the IBM processors through the Q Network and African Research Universities Alliance. This research was supported by the South African National Research Foundation, the South African Council for Scientific and Industrial Research, and the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.

References

[1] Kjaergaard M, Schwartz M E, Braumüller J, Krantz P, Wang J I J, Gustavsson S and Oliver W D 2020 *Annu. Rev. Condens. Matter Phys.* **11** 369–395

[2] Barenco A, Bennett C H, Cleve R, DiVincenzo D P, Margolus N, Shor P, Sleator T, Smolin J A and Weinfurter H 1995 *Phys. Rev. A* **52** 3457–3467

[3] Yu N, Duan R and Ying M 2013 *Phys. Rev. A* **88** 010304

[4] Shende V V and Markov I L 2009 *Quantum Inf. Comput.* **9** 461–486

[5] Maslov D 2016 *Phys. Rev. A* **93** 022311

[6] Skosana U and Tame M 2021 *Sci. Rep.* **11** 16599

[7] Shor P W 1997 *SIAM J. Comput.* **26** 1484–1509

[8] Margolus N 1994 *Unpublished manuscript (circa 1994)*

[9] Song G and Klappenecker A 2003 *Quantum Inf. Comput.* **3** 139–156

[10] IBM Quantum 2021 https://quantum-computing.ibm.com

[11] Abraham H *et al.* 2019 Qiskit: An open-source framework for quantum computing

[12] Nielsen M A and Chuang I L 2011 *Quantum Computation and Quantum Information: 10th Anniversary Edition* 10th ed (USA: Cambridge University Press)

[13] Nielsen M A 2002 *Phys. Lett. A* **303** 249–252

[14] Magesan E, Blume-Kohout R and Emerson J 2011 *Phys. Rev. A* **84**

[15] Martín-López E, Laing A, Lawson T, Alvarez R, Zhou X Q and O'Brien J L 2012 *Nature Photonics* **6** 773–776

[16] Amico M, Saleem Z H and Kumph M 2019 *Phys. Rev. A* **100** 012305