On the advantages of relative phase Toffoli gates

Unathi K. Skosana Supervisor: Prof. Mark Tame

Department of Physics, Stellenbosch University

Boolean arithmetic, universality and Toffoli gates

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.

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

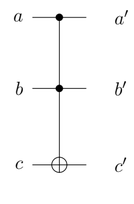


Figure 1. Truth table and circuit for a Toffoli gate

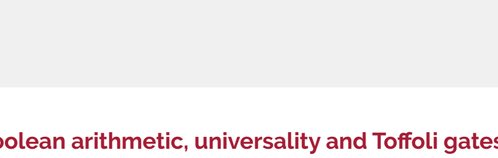
Decomposition of Toffoli gates

The classical Toffoli logic gate admits a realization as a unitary quantum logic gate on the merit of being reversible. As a quantum logic gate (CCX), though not universal, the Toffoli gate is a substratum for Boolean arithmetic across quantum logical registers and ensures that any classical computation is reproducible on a quantum computer

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

However, Toffoli gates are not easy to implement on current quantum hardware:

- **Not natively supported.** Current quantum hardware instead decomposes Toffoli gates onto a physically implemented (native) universal gate made up of several single qubit gates and one two-qubit gate [1], *i.e.*, no less than $2n$ two-qubit gates (CX, CZ, etc) for a n-controlled Toffoli gate [2] and the traditional three-qubit Toffoli decomposes into six CX and seven $T/T^\dagger$ gates:



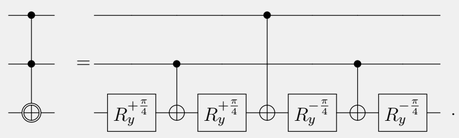
(2)

- **Decoherence.** Despite high fidelity implementations ($\gtrsim 99\%$ for superconducting qubits, see Reference [3]), the effects of decoherence are considerable and set a limit on the number of two-qubit gates over a set of qubits in a computation lest it fail.

Relative phase Toffoli gates

Variants of Toffoli gates, collectively called relative phase Toffoli gates, due to their operation being equivalent to that of a Toffoli gate up to some undesirable phase:

- **Smaller in circuit size.** Margolus gate (RCCX) is an optimal three-qubit relative phase Toffoli gate up to a relative shift ($|101\rangle \mapsto -|101\rangle$), that uses three CX gates and four single-qubit gates [4, 5]:



(3)

- **Use beyond commonly conceived scenarios.** Optimization of multiply-controlled full Toffolis via relative phase Toffoli replacements [6].

Gate characterization

We characterize and compare the performances of a three-qubit Toffoli gate (CCX) and Margolus gate (RCCX) in two ways on IBM's superconducting quantum processors through the Qiskit SDK [7].

Via quantum state tomography

We prepare an example state with a CCX in comparison to one prepared with a RCCX gate.

$$\begin{aligned} |\psi\rangle &= \mathrm{CCX}_{012}\,|1\rangle_0\,|+\rangle_1\,|0\rangle_2 = \mathrm{RCCX}_{012}\,|1\rangle_0\,|+\rangle_1\,|0\rangle_2\,, \\ &= \frac{1}{\sqrt{2}}\,|1\rangle_0\,(|0\rangle_1\,|0\rangle_2 + |1\rangle_1\,|1\rangle_2), \\ &= |1\rangle_0\,|\Phi^+\rangle_{12}\,, \end{aligned} \tag{4}$$

then perform state tomography on qubits $1, 2$ (maximally entangled Bell state), experimentally prepared on IBM Q's seven-qubit quantum processor **ibmq_casablanca**.

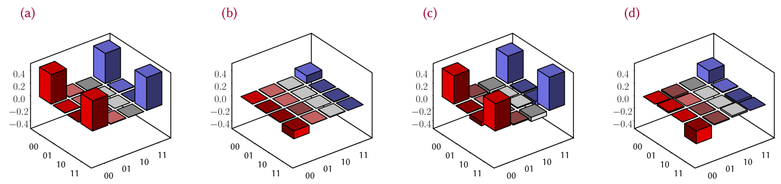


Figure 2. (a) Real and (b) imaginary part of the measured density matrix of the state in equation [4] prepared with a CCX gate on IBM Q's *ibmq_casablanca*. Similarly, (c) and (d) are real and imaginary parts, respectively, of the same state prepared with a RCCX gate.

To quantitatively evaluate the performance of the two gates in generating the Bell state in equation [4], we measure the fidelity for two quantum states ρ and σ, defined as $F(\rho, \sigma) = \mathrm{Tr}(\sqrt{\rho^{1/2}\sigma\rho^{1/2}})$ [8]. For this particular instance they were measured (within 95% confidence intervals) to be $F(|\Phi^+\rangle\langle\Phi^+|\,, \sigma_{\mathrm{CCX}}) = 0.929 \pm 0.003$ and $F(|\Phi^+\rangle\langle\Phi^+|\,, \sigma_{\mathrm{RCCX}}) = 0.972 \pm 0.008$ respectively.

Via quantum process tomography

For each a circuit, we perform process tomography and reconstruct a description of the quantum channel $\mathcal{E}$ that describes the circuit's operation on the aforesaid processor.

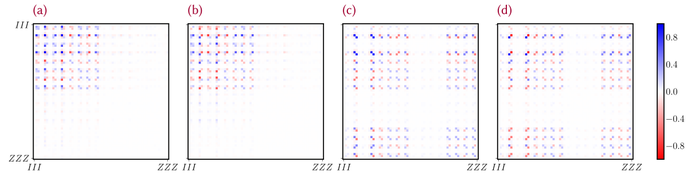


Figure 3. (a) Real and (b) imaginary part of the measured χ-matrix representation of the quantum channel $\mathcal{E}_{\mathrm{CCX}}$ prepared with a CCX gate on IBM Q's *ibmq_casablanca*. Similarly, (c) and (d) are real and imaginary parts, respectively, of the quantum channel $\mathcal{E}_{\mathrm{RCCX}}$ prepared with a RCCX gate.

The average gate fidelity of a quantum channel $\mathcal{E}$ with respect to a target unitary U measures how close $\mathcal{E}$ approximates U, is given by

$$\bar{F}(\mathcal{E}, U) = \int d\psi\, \langle\psi|U^\dagger\mathcal{E}(|\psi\rangle\langle\psi|)U|\psi\rangle\,, \tag{5}$$

$$\mathcal{E}(\rho) = \sum_{i,j} \chi_{i,j}\sigma_i\rho\sigma_j \quad \text{Evolution of a density matrix } \rho \text{ w.r.t the } \chi\text{-presentation of } \mathcal{E}. \tag{6}$$

where the integration is over the uniform Haar measure and $\mathcal{E}(\cdot)$ is an evolution with respect to the quantum channel $\mathcal{E}$ (See references [9, 10] for closed forms of equation 5). We measured the average gate fidelities to be $\bar{F}_{\mathrm{CCX}}(\mathcal{E}, U) = 0.917 \pm 0.005$ and $\bar{F}_{\mathrm{RCCX}}(\mathcal{E}, U) = 0.958 \pm 0.002$ respectively.

Case studies: Quantum factoring of $N = 21$

In 2012 [11], and recently in 2019 [12], the integer $N = 21$ was factored, setting the record for the largest integer factored with Shor's quantum factoring algorithm [13].

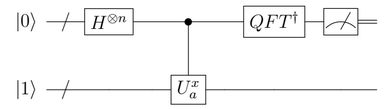


Figure 4. Schematic of the order-finding routine for Shor's algorithm for n qubits. The number of qubits in the control register determines the bit-accuracy of the value of the extracted order. The bottom (work) register has the m qubits required to encode N. First, the control and work registers are initialized, then conditional modular exponentiation is performed, indicated by the controlled unitary and an inverse quantum Fourier transform is applied to the control register followed by a standard computational basis measurement.

- First scheme (Martín-López et al. [11]):
  - **Iterative** via real-time conditionals operations and feed forward operations, recycling a single-qubit in the control register on each iteration.
  - **Uses full Toffolis** to implement the modular exponentiation operation.
  - **Full factoring not achieved,** falls one iteration short of full factorization of $N = 21$.
- Second scheme (Amico et al. [12]):
  - **Pseudo-iterative** via splitting the iterations into separate circuits and reseting the computation on each iteration, using a single-qubit in the work-register.
  - **Without the use of the continued fractions algorithm,** the order is extracted via a statistical test instead.
  - **Also uses full Toffolis,** in a similar fashion to the first scheme.
- Our scheme (Skosana and Tame. [14]):
  - **Non-iterative** uses three qubits in the control register.
  - **Uses relative phase Toffolis** while preserving the functional correctness of the modular exponentiation operation.
  - **Fully factors** $N = 21$ by giving the correct order via the continued fractions algorithm.
  - **Entanglement across the registers in the circuit** is verified, which is a requisite for the speed-up of the algorithm.

References

[1] 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

[2] Shende V V and Markov I L 2008 On the cnot-cost of toffoli gates (*Preprint* `0803.2316`)

[3] Kjaergaard M, Schwartz M E, Braumüller J, Krantz P, Wang J I J, Gustavsson S and Oliver W D 2020 *Annual Review of Condensed Matter Physics* **11** 369–395

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

[5] Song G and Klappenecker A 2003 (*Preprint* `quant-ph/0312225`)

[6] Maslov D 2016 *Phys. Rev. A* **93**(2) 022311

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

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

[9] Nielsen M A 2002 *Physics Letters A* **303** 249–252

[10] Magesan E, Blume-Kohout R and Emerson J 2011 *Physical Review A* **84**

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

[12] Amico M, Saleem Z H and Kumph M 2019 *Phys. Rev. A* **100**(1) 012305

[13] Shor P W 1997 *SIAM Journal on Computing* **26** 1484–1509

[14] Skosana U and Tame M 2021 Demonstration of shor's factoring algorithm for n=21 on ibm quantum processors (*Preprint* `2103.13855`)