Number-Theoretic Characterizations of Some Restricted Clifford+T Circuits (Extended Abstract)

Matthew Amy[1], Andrew N. Glaudell[2] and Neil J. Ross[1]

[1] Department of Mathematics and Statistics, Dalhousie University, Halifax, NS, Canada

[2] Booz Allen Hamilton, Washington, DC, USA

Abstract

Kliuchnikov, Maslov, and Mosca proved in 2012 that a 2×2 unitary matrix V can be exactly represented by a single-qubit Clifford+T circuit if and only if the entries of V belong to the ring $\mathbb{Z}[1/\sqrt{2}, i]$. Later that year, Giles and Selinger showed that the same restriction applies to matrices that can be exactly represented by a multi-qubit Clifford+T circuit. These number-theoretic characterizations shed new light upon the structure of Clifford+T circuits and led to remarkable developments in the field of quantum compiling. In the present paper, we provide number-theoretic characterizations for certain restricted Clifford+T circuits by considering unitary matrices over subrings of $\mathbb{Z}[1/\sqrt{2}, i]$. We focus on the subrings $\mathbb{Z}[1/2]$, $\mathbb{Z}[1/\sqrt{2}]$, $\mathbb{Z}[1/\sqrt{\text{-}2}]$, and $\mathbb{Z}[1/2, i]$, and we prove that unitary matrices with entries in these rings correspond to circuits over well-known universal gate sets. In each case, the desired gate set is obtained by extending the set of classical reversible gates $\{X, CX, CCX\}$ with an analogue of the Hadamard gate and an optional phase gate.

Preprint: The preprint for this extended abstract can be found at `arXiv:1908.06076`.

Introduction: Kliuchnikov, Maslov, and Mosca showed in [20] that a 2-dimensional unitary matrix V can be exactly represented by a single-qubit Clifford+T circuit if and only if the entries of V belong to the ring $\mathbb{Z}[1/\sqrt{2}, i]$. This result gives a number-theoretic characterization of single-qubit Clifford+T circuits. In [12], Giles and Selinger extended the characterization of Kliuchnikov et al. to multi-qubit Clifford+T circuits by proving that a 2^n-dimensional unitary matrix can be exactly represented by an n-qubit Clifford+T circuit if and only if its entries belong to $\mathbb{Z}[1/\sqrt{2}, i]$.

These number-theoretic characterizations provide great insight into the structure of Clifford+T circuits. As a result, single-qubit Clifford+T circuits are now very well understood [9, 13, 21, 22, 24]. In contrast, our understanding of multi-qubit Clifford+T circuits remains more limited, despite interesting results [8, 11, 14, 15, 29]. One of the reasons for this limitation is that large unitary matrices over $\mathbb{Z}[1/\sqrt{2}, i]$ are hard to analyze. In order to circumvent the difficulties associated with multi-qubit Clifford+T circuits, restricted gate sets have been considered in the literature. This led to important developments in the study of multi-qubit Clifford, CNOT+T, and CNOT-dihedral circuits [3, 4, 5, 6, 18, 23, 26]. Unfortunately, the simpler structure of these restricted gate sets comes at a cost: they are not universal for quantum computing.

Contributions: In the present work, our goal is to address both of these limitations by considering restrictions of the Clifford+T gate set which are nevertheless universal for quantum computing. To this end, we study circuits corresponding to unitary matrices over proper subrings of $\mathbb{Z}[1/\sqrt{2}, i]$, focusing on $\mathbb{Z}[1/2]$, $\mathbb{Z}[1/\sqrt{2}]$, $\mathbb{Z}[1/\sqrt{\text{-}2}]$, and $\mathbb{Z}[1/2, i]$. For each subring, we find a set of quantum gates G with the property that circuits over G correspond to unitary matrices over the given ring. Writing $U_{2^n}(R)$ for the group of $2^n \times 2^n$ unitary matrices over a ring R, our main results can then be summarized in the following theorem.

Theorem. *A $2^n \times 2^n$ unitary matrix V can be exactly represented by an n-qubit circuit over*

(i) $\{X, CX, CCX, H \otimes H\}$ *if and only if* $V \in U_{2^n}(\mathbb{Z}[1/2])$,

(ii) $\{X, CX, CCX, H, CH\}$ *if and only if* $V \in U_{2^n}(\mathbb{Z}[1/\sqrt{2}])$,

(iii) $\{X, CX, CCX, F\}$ *if and only if* $V \in U_{2^n}(\mathbb{Z}[1/\sqrt{\text{-}2}])$, *and*

(iv) $\{X, CX, CCX, \omega H, S\}$ *if and only if* $V \in U_{2^n}(\mathbb{Z}[1/2, i])$,

where $\omega = e^{i\pi/4}$ *and* $F \propto \sqrt{H}$. *Moreover, in (i)-(iv), a single ancilla is sufficient.*

The gate sets in items (i)–(iv) of the above theorem are all universal for quantum computing [2, 27], and we sometimes refer to circuits over these gate sets as *integral*, *real*, *imaginary*, and *Gaussian* Clifford+T circuits, respectively.

Restrictions similar to the ones considered here were previously studied in the context of foundations [25], randomized benchmarking [17], and graphical languages for quantum computing [7, 19, 28]. Furthermore, our study fits within a larger program, initiated by Aaronson and others which aims at classifying quantum operations. Such classifications exist for classical reversible operations [1], for stabilizer operations [16], and for beam-splitter interactions [10], but no classification is known for a universal family of quantum operations suited for fault-tolerant quantum computing. In this context, our work can be seen as a partial classification of the universal extensions of the set of classical reversible gates $\{X, CX, CCX\}$. This perspective is illustrated in Figure 1, which depicts a fragment of the lattice of subgroups of $U_n(\mathbb{Z}[1/\sqrt{2}, i])$ where, for conciseness, we wrote $\mathbb{D}$ for the ring $\mathbb{Z}[1/2]$ so that the rings $\mathbb{Z}[1/\sqrt{2}]$, $\mathbb{Z}[1/\sqrt{\text{-}2}]$, $\mathbb{Z}[1/2, i]$ and $\mathbb{Z}[1/\sqrt{2}, i]$ are denoted by $\mathbb{D}\left[\sqrt{2}\right]$, $\mathbb{D}\left[\sqrt{\text{-}2}\right]$, $\mathbb{D}[i]$, and $\mathbb{D}[\omega]$, respectively.

Overview: Unrestricted Clifford+T circuits are generated by

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad CX = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \text{and} \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix}.$$

Since $\omega = (1+i)/\sqrt{2}$, the entries of all the generators belong to the ring $\mathbb{Z}[1/\sqrt{2}, \omega] = \mathbb{Z}[1/\sqrt{2}, i] = \mathbb{D}[\omega]$. Hence, if a matrix V can be represented exactly by an n-qubit Clifford+T circuit, then $V \in U_{2^n}(\mathbb{D}[\omega])$, the group of $2^n \times 2^n$ unitary matrices with entries in $\mathbb{D}[\omega]$. Showing that the ring $\mathbb{D}[\omega]$ characterizes Clifford+T circuits thus amounts to proving the converse implication. An algorithm establishing that every element of $U_{2^n}(\mathbb{D}[\omega])$ can be exactly represented by a Clifford+T circuit is known as an exact synthesis algorithm.

The original insight of Kliuchnikov, Maslov and Mosca in the single-qubit Clifford+T case was to reduce the problem of exact synthesis to the problem of state preparation. The latter problem is to find, given a target vector $v \in \mathbb{D}[\omega]^n$, a sequence $G_1, \ldots, G_\ell$ of Clifford+T gates such that $G_\ell \cdots G_1 e_1 = u$ or, equivalently, such that $G_1^\dagger \cdots G_\ell^\dagger u = e_1$. Kliuchnikov et al. realized that this sequence of gates can be found by first writing v as $v = u/\sqrt{2}^q$ for some $u \in \mathbb{Z}[\omega]$ and then iteratively reducing the exponent q.

This basic premise was extended by Giles and Selinger to the multi-qubit context by adding an outer induction over the columns of an n-qubit unitary. This method amounts to performing a constrained Gaussian elimination where the row operations are restricted to a few basic moves. The Giles-Selinger algorithm proceeds by reducing the leftmost column of an $n \times n$ unitary matrix to the first standard basis vector by applying a sequence of one- and two-level matrices, which act non-trivially on at most two components of a vector, before recursively dealing with the remaining submatrix. If the target unitary is $V = \left[\begin{array}{c|c} v & V' \end{array}\right]$, then the Giles-Selinger algorithm first constructs a sequence of matrices $G_1, \ldots, G_\ell$ such that $G_1 \cdots G_\ell v = e_1$. Left-multiplying V by this sequence of matrices then yields

$$G_1 \cdots G_\ell \left[\begin{array}{c|c} v & V' \end{array}\right] = \left[\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & V'' & \\ 0 & & & \end{array}\right]$$

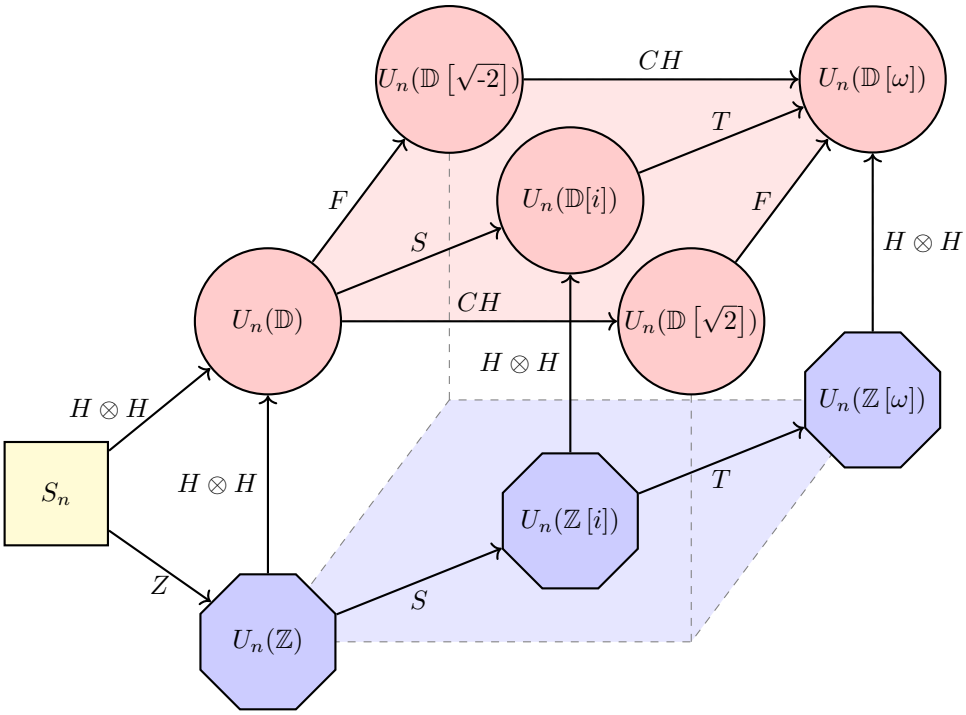

Figure 1: Some subgroups of $U_n(\mathbb{D}[\omega])$. To the left of the cube, in yellow, the symmetric group S_n corresponds to circuits over the gate set $\{X, CX, CCX\}$. On the bottom face of the cube, in blue, are generalized symmetric groups, and on the top face of the cube, in red, are universal subgroups of $U_n(\mathbb{D}[\omega])$. The edges of the lattice denote inclusion. The gates labeling the edges are sufficient to extend the expressive power of a gate set from one subgroup to the next (and no further). For example, the edge labeled Z going from S_n to $U_n(\mathbb{Z})$ indicates that adding the Z gate to $\{X, CX, CCX\}$ produces a gate set expressive enough to represent every matrix in $U_n(\mathbb{Z})$ (but not every matrix in $U_n(\mathbb{Z}[i])$).

where V'' is unitary. The fact that the matrices used in this reduction act non-trivially on no more than two rows of the matrix ensures that when the algorithm recursively reduces the columns of V'' it does so without perturbing the previously fixed columns. The Giles-Selinger algorithm thus relies on the following two facts.

1. A unit vector in $\mathbb{D}[\omega]^n$ can be reduced to a standard basis vector by using one- and two-level matrices and

2. the required one- and two-level matrices can be exactly represented by Clifford+T circuits.

While each of our characterizations presents specificities, our method in characterizing restricted Clifford+T circuits follows this general structure.

Conclusion: In this contribution, we provide number-theoretic characterizations for several classes of restricted but universal Clifford+T circuits, focusing on integral, real, imaginary, and Gaussian circuits. We show that a unitary matrix can be exactly represented by an n-qubit integral Clifford+T circuit if and only if it is an element of the group $U_{2^n}(\mathbb{D})$. We then establish that real, imaginary, and Gaussian circuits similarly correspond to the groups $U_{2^n}(\mathbb{D}[\sqrt{2}])$, $U_{2^n}(\mathbb{D}[\sqrt{-2}])$, and $U_{2^n}(\mathbb{D}[i])$, respectively.

References

[1] S. Aaronson, D. Grier, and L. Schaeffer. The classification of reversible bit operations. In *Proceedings of the 8th Innovations in Theoretical Computer Science Conference*, volume 67 of *LIPIcs*, pages 23:1–23:34, 2017. Also available from `arXiv:1504.05155`.

[2] D. Aharonov. A simple proof that Toffoli and Hadamard are quantum universal. Preprint available from `arXiv:quant-ph/0301040`, Jan. 2003.

[3] M. Amy, J. Chen, and N. J. Ross. A finite presentation of CNOT-dihedral operators. In *Proceedings of the 14th International Conference on Quantum Physics and Logic*, QPL '17, pages 84–97, 2017. Also available from `arXiv:1701.00140`.

[4] M. Amy, D. Maslov, and M. Mosca. Polynomial-time T-depth optimization of Clifford+T circuits via matroid partitioning. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33(10):1476–1489, 2014. Also available from `arXiv:1303.2042`.

[5] M. Amy, D. Maslov, M. Mosca, and M. Roetteler. 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. Also available from `arXiv:1206.0758`.

[6] M. Amy and M. Mosca. T-count optimization and Reed-Muller codes. *IEEE Transactions on Information Theory*, 65(8):4771–4784, 2019. Also available from `arXiv:1601.07363`.

[7] M. Backens and A. Kissinger. ZH: A complete graphical calculus for quantum computations involving classical non-linearity. In *Proceedings of the 15th International Conference on Quantum Physics and Logic*, QPL '18, pages 23–42, 2018. Also available from `arXiv:1805.02175`.

[8] X. Bian and P. Selinger. Relations for the group of 2-qubit Clifford+T operators. Talk given at the Quantum Programming and Circuits Workshop. Slides available from `https://www.mathstat.dal.ca/~xbian/talks/slide_cliffordt2.pdf`, June 2015.

[9] A. Bocharov, M. Roetteler, and K. M. Svore. Efficient synthesis of probabilistic quantum circuits with fallback. *CoRR*, abs/1409.3552, 2014. Also available from `arXiv:1409.3552`.

[10] A. Bouland and S. Aaronson. Generation of universal linear optics by any beam splitter. *Physical Review A*, 89:062316, Jun 2014.

[11] A. De Vos, R. Van Laer, and S. Vandenbrande. The group of dyadic unitary matrices. *Open Systems & Information Dynamics*, 19(1):1250003:1 – 1250003:28, 2012.

[12] B. Giles and P. Selinger. Exact synthesis of multiqubit Clifford+T circuits. *Physical Review A*, 87:032332, 2013. Also available from `arXiv:1212.0506`.

[13] B. Giles and P. Selinger. Remarks on Matsumoto and Amano's normal form for single-qubit Clifford+T operators. Also available from `arXiv:1312.6584`, Dec. 2013.

[14] D. Gosset, V. Kliuchnikov, M. Mosca, and V. Russo. An algorithm for the T-count. *Quantum Information & Computation*, 14(15-16):1261–1276, Nov. 2014. Also available from `arXiv:1308.4134`.

[15] S. Greylyn. Generators and relations for the group $U_4(\mathbb{Z}[1/\sqrt{2}, i])$. Available from `arXiv:1408.6204`, 2014.

[16] D. Grier and L. Schaeffer. The classification of stabilizer operations over qubits. Preprint available from `arXiv:1603.03999`, 2016.

[17] A. K. Hashagen, S. T. Flammia, D. Gross, and J. J. Wallman. Real randomized benchmarking. *Quantum*, 2:85, Aug. 2018. Also available from `arXiv:1801.06121`.

[18] L. E. Heyfron and E. T. Campbell. An efficient quantum compiler that reduces T count. *Quantum Science and Technology*, 4(1):015004, 2018. Also available from `arXiv:1712.01557`.

[19] E. Jeandel, S. Perdrix, and R. Vilmart. Y-calculus: A language for real matrices derived from the ZX-calculus. In *Proceedings of the 14th International Conference on Quantum Physics and Logic*, QPL '17, pages 23–57, 2017. Also available from `arXiv:1702.00934`.

[20] V. Kliuchnikov, D. Maslov, and M. Mosca. Fast and efficient exact synthesis of single-qubit unitaries generated by Clifford and T gates. *Quantum Information & Computation*, 13(7-8):607–630, 2013. Also available from `arXiv:1206.5236`.

[21] V. Kliuchnikov, D. Maslov, and M. Mosca. Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits. *IEEE Transactions on Computers*, 65(1):161–172, Jan 2016. Also available from `arXiv:1212.6964`.

[22] K. Matsumoto and K. Amano. Representation of quantum circuits with Clifford and $\pi/8$ gates. Preprint available from `arXiv:0806.3834`, June 2008.

[23] G. Meuli, M. Soeken, and G. D. Micheli. SAT-based {CNOT, T} quantum circuit synthesis. In *Proceedings of the 10th International Conference on Reversible Computation*, RC '17, pages 175–188, 2018.

[24] N. J. Ross and P. Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. *Quantum Information & Computation*, 16(11-12):901–953, 2016. Also available from `arXiv:1403.2975`.

[25] T. Rudolph and L. Grover. A 2 rebit gate universal for quantum computing. Preprint available from `arXiv:quant-ph/0210187`, nov 2002.

[26] P. Selinger. Generators and relations for n-qubit Clifford operators. *Logical Methods in Computer Science*, 11(10):1–17, Jun 2015. Also available from `arXiv:1310.6813`.

[27] Y. Shi. Both Toffoli and controlled-NOT need little help to do universal quantum computing. *Quantum Information & Computation*, 3(1):84–92, Jan. 2003. Also available from `arXiv:quant-ph/0205115`.

[28] R. Vilmart. A ZX-calculus with triangles for Toffoli-Hadamard, Clifford+T, and beyond. In *Proceedings of the 15th International Conference on Quantum Physics and Logic*, QPL '18, pages 313–344, 2018. Also available from `arXiv:1804.03084`.

[29] J. Welch, A. Bocharov, and K. M. Svore. Efficient approximation of diagonal unitaries over the Clifford+T basis. *Quantum Information & Computation*, 16(1-2):87–104, Jan. 2016. Also available from `arXiv:1412.5608`.