Application of a resource theory for magic states to fault-tolerant quantum computing

Mark Howard and Earl Campbell
University of Sheffield.
arXiv:1609.07488

Overview

Motivated by their necessity for most fault-tolerant quantum computation schemes, we formulate a resource theory for magic states. We first show that robustness of magic is a well-behaved magic monotone that operationally quantifies the classical simulation overhead for a Gottesman-Knill type scheme using ancillary magic states. Our framework subsequently finds immediate application in the task of synthesizing non-Clifford gates using magic states. When magic states are interspersed with Clifford gates, Pauli measurements and stabilizer ancillas—the most general synthesis scenario—then the class of synthesizable unitaries is hard to characterize. Our techniques can place non-trivial lower bounds on the number of magic states required for implementing a given target unitary. Guided by these results we have found new and optimal examples of such synthesis.

Background

Quantum resource theories attempt to capture what is quintessentially quantum in a piece of technology. For example, entanglement is the relevant resource for quantum cryptography and communication. An abundance of other resource theories have been related to various aspects of quantum theory [1–8]. Once a quantum computer is made fault-tolerant, some computational operations become relatively easy, and some more difficult, leading to a natural resource picture called the magic state model [9;10]. Preparation of stabilizer states and implementation of Clifford unitaries and Pauli measurements constitute free resources. Difficult operations include preparation of magic states, a supply of which is necessary in order to promote the easier operations to a universal gate set. With only free resources, the computation can be efficiently classically simulated, whereas with a liberal supply of pure magic states, universal quantum computation is unlocked. For qudit (d-level) quantum computers with odd d, a resource theory of magic (or equivalently contextuality with respect to stabilizer measurements [11]) has been developed [7;12]. This relies on a well-behaved discrete Wigner function [13], which in turn relies on quirks of odd dimensional Hilbert space. Here we address the most practically important case by quantifying the magic for multiqubit systems, relating this resource measure to simulation complexity and applying the resource theory to the practical problem of gate synthesis.

The canonical magic state is $|H\rangle = (|0\rangle + e^{i\pi/4}|1\rangle)/\sqrt{2}$, which enables application of a single-qubit unitary $T = \text{diag}(1, e^{i\pi/4})$ [9;10]. A circuit composed of elements from the Clifford+T gate set acting on the standard computational basis input suffices for universal quantum computation. Such a circuit can be classically simulated, but in a time that scales exponentially in the number of T gates [14]. Faster simulation algorithms were recently discovered that relate the simulation complexity to the stabilizer rank [15–17], a measure of magic for pure states. Such techniques do not naturally adapt to mixed magic states, and stabilizer rank is qualitatively very different to the magic measure we establish here. For quantum computations using qudits with odd dimension, the discrete Wigner function provides a quasiprobabilitiy distribution and Pashayan et al. [18] showed that the negativity quantifies the simulation complexity. Here we provide a general simulation scheme, which can be naturally applied to mixed-state qubit quantum computations using any kind of ancillary magic state (e.g., a multi-qubit magic state enabling a Toffoli gate). Furthermore, for many problems our approach is more efficient than the most directly comparable scheme [16].

Due to the high price assigned to $|H\rangle$ states and hence T gates, it behooves us to find Clifford+T circuit implementations of quantum algorithms that are parsimonious in their use of T gates. Recently, there has been significant progress [19–27] over previous Solovay-Kitaev type constructions. Developments include identifying special algebraic forms for all gates that can be unitarily synthesized over the Clifford+T gate set [21] or over the smaller CNOT+T gate set [19;20]. However, circuit synthesis need not be a purely unitary process, and more generally may be aided by ancillary stabilizer states, measurements and classical feed-forward. There are hints that general synthesis can be significantly more powerful [23;24;27;28], though the paradigm is not well understood. Our resource framework helps with this problem by establishing non-trivial lower bounds on the number of $|H\rangle$ states, or equivalently T gates, required for the general synthesis scenario. This allows us to identify several circuits as optimal. Such resource-theoretic tools work for any kind of state, not just $|H\rangle$, but they are particularly well-motivated for magic states from the third level of the Clifford hierarchy e.g., Toffoli resource states. We note how general synthesis has a curious relationship to Clifford equivalence of magic states. From this vantage point, we discover several new examples of general synthesis protocols with resource savings over previous unitary synthesis methods.

Methodology & Tools

• Robustness of Magic

Vidal and Tarrach[8] established robustness of entanglement as an entanglement monotone. We adapt their definition so that the free states are stabilizer states. Denoting $\mathcal{S}_n = \{\sigma_i\}$ as the set of pure n-qubit stabilizer states, we define the robustness of magic as

$$\text{(RoM)} \qquad \mathcal{R}(\rho) = \min_x \left\{ \sum_i |x_i|; \rho = \sum_i x_i \sigma_i \right\} . \tag{1}$$

Decompositions of the form $\sum_i x_i \sigma_i$ are called stabilizer pseudomixtures. We have $\sum_i x_i = 1$, but x_i may be negative and so they provide a quasiprobability distribution.

• Calculating Robustness of Magic is a Linear Program

The optimization in (1) can be rewritten in terms of a linear system as

$$\mathcal{R}(\rho) = \min ||x||_1 \text{ subject to } Ax = b \, , \tag{2}$$

where $||x||_1 = \sum_i |x_i|$, $b_i = \text{Tr}(P_i \rho)$ and $A_{j,i} = \text{Tr}(P_j \sigma_i)$ where P_j is the jth Pauli operator. From our formulation of the problem it is clear that $\min_{Ax=b} ||x||_1$ is feasible and bounded. Consequently, strong duality holds i.e.,

$$\min_{Ax=b} ||x||_1 = \max_{||A^T y||_\infty \leq 1} -b^T y \, , \tag{3}$$

and LP solvers can provide a certificate y of optimality *.

• Third level of Clifford Hierarchy

The third level of the Clifford hierarchy consists of the set of gates that map Pauli operators to Clifford gates under conjugation. Famous examples of third-level gates include $T = \text{diag}(1, e^{i\pi/4})$, control-control-Z (CCZ)—which is Clifford equivalent to the Toffoli—and control-S (CS) where $S = T^2$. For any quantum circuit we can find an equivalent gadgetized version[9;15;16] over the Clifford plus U gate set using third-level U; all uses of k-qubit U are replaced with the standard state injection circuit whereby a $|U\rangle = U|+\rangle^{\otimes k}$ state is entangled with a data qubit(s). Fig. 1 shows two different ways to gadgetise a CS gate. These gadgets work because access to the state $|U\rangle$ deterministically allows for implementation of the gate U[29;30], as depicted in Fig. 1. We remark that diagonal, third-level gates are exactly synthesizable from CNOT and T gates[19;20;31;32].

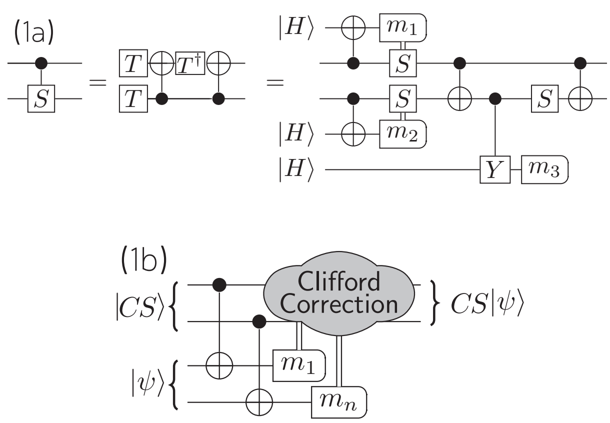

Figure 1: Implementing a non-Clifford CS gate: (1a) decomposing CS into the CNOT+T basis and implementing each T using $|H\rangle$-type state injection (1b) using a single $|CS\rangle = CS|+\rangle^{\otimes 2}$ state.

*This certificate of optimality can be used to obtain a magic witness—an operator whose expectation value with respect to stabilizer states is in the interval $[-1, 1]$ and whose expectation with respect to ρ is $\mathcal{R}(\rho)$. These witnesses can be used to derive exact expressions for robustness as we have done in our full paper

Main results

• Robustness is a well-behaved magic monotone

RoM (1) is faithful and non-increasing under stabilizer operations. Furthermore it is submultiplicative i.e, $\mathscr{R}(\rho_1 \otimes \rho_2) \leq \mathscr{R}(\rho_1)\mathscr{R}(\rho_2)$. Therefore $\log(\mathscr{R}(\rho))$ is a subadditive magic monotone.

• Lower Bound on Robustness of Magic

We establish a lower bound $\mathscr{D}(\rho) \leq \mathscr{R}(\rho)$, where the quantity $\mathscr{D}$ is multiplicative; $\mathscr{D}(\rho^{\otimes n}) = [\mathscr{D}(\rho)]^n$.

• Simulation scheme for a Universal Quantum Computer

1. We establish a Gottesman-Knill type simulation scheme [14] with sample complexity given by

$$N = \frac{2}{\delta}(\sum_i |x_i|)^2 \ln\left(\frac{2}{\epsilon}\right) \geq \frac{2}{\delta}\mathscr{R}(\rho)^2 \ln\left(\frac{2}{\epsilon}\right), \quad (4)$$

   i.e., quadratic in the robustness of the ancillary magic state ρ used to enable non-Clifford gates. This follows from reinterpreting the quasiprobability distribution x_i over stabilizer states as a probability distribution $p_i = |x_i|/\sum_i |x_i|$ and applying Hoeffding inequalities.
   The most obvious application for Eq. (4) is to simulate a circuit, acting on a standard computational basis input, consisting of Clifford gates interspersed with n T gates. Our simulation scales as 1.685^n (as compared with 1.9185^n in [16]). Alternatively, we could use n Toffoli ancilla states, which scales as 6.531^n.

2. We find bounds on the regularized robustness of $|H\rangle$ type magic states,

$$\lim_{n\to\infty} \mathscr{R}(|H^{\otimes n}\rangle)^{\frac{1}{n}} \in [1.207, 1.298] . \quad (5)$$

   This is achieved by using the quantity $\mathscr{D}$ (described above) and numerical calculation of $\mathscr{R}(|H^{\otimes 5}\rangle)^{\frac{1}{5}}$.

• Numerics up to five qubits

We performed substantial numerical investigations up to 5 qubit systems, for which there are over two million stabilizer states and over one thousand Pauli operators. A sparse representation of the five qubit A matrix (see Eq. (2)) is over 30MB. Doing so we obtain a complete classification of the robustness of all gates from the CNOT+T gate set on 5 qubits.

• Synthesis of non-Clifford gates

1. Lower Bounds on number of T gates required to implement a target unitary:
   Consider the circuit synthesis depicted in Figure 1, where a control-S gate is implemented by using up three $|H\rangle$ magic states. Since each magic state is expensive to obtain (via magic state distillation), how can we be sure we are not wasting any? Our resource framework provides an answer since for any diagonal U, the state $|U\rangle$ cannot be be created by a stabilizer circuit using n $|H\rangle$ states if $\mathscr{R}(|U\rangle) > \mathscr{R}(|H^{\otimes n}\rangle)$. Our calculations enable us to show that e.g.,

$$\mathscr{R}(|H^{\otimes 2}\rangle) < \mathscr{R}(|CS\rangle) < \mathscr{R}(|H^{\otimes 3}\rangle), \quad (6)$$

$$\mathscr{R}(|H^{\otimes 3}\rangle) < \mathscr{R}(|CCZ\rangle) < \mathscr{R}(|H^{\otimes 4}\rangle). \quad (7)$$

   so that the decomposition of CS into 3 T gates is provably optimal. Similarly, the second expression shows that the ancilla-assisted synthesis of CCZ using four T gates [28] is optimal.

2. Enable T savings by identifying Clifford-equivalence of magic states:
   We identify a surprising feature—Clifford equivalence of magic states—that can lead to improved synthesis. Recall that, for a third-level unitary U, access to the state $|U\rangle$ deterministically allows for implementation of the gate U. By using robustness we have found examples where $C|U\rangle = |V\rangle$, for a Clifford gate C, and yet unitary synthesis of U uses fewer T-gates than V. Practically, this gives a recipe for implementing V using fewer T gates.

References

[1] F. Brandão and G. Gour, Phys. Rev. Lett. **115**, 070503 (2015).
[2] B. Coecke, T. Fritz, and R. W. Spekkens, Information and Computation (2016), 10.1016/j.ic.2016.02.008.
[3] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, P. Joshi, W. Kłobus, and A. Wójcik, Phys. Rev. Lett. **112**, 120401 (2014).
[4] M. Horodecki and J. Oppenheim, Int. J. Mod. Phys. B **27**, 1345019 (2013).
[5] C. Napoli, T. R. Bromley, M. Cianciaruso, M. Piani, N. Johnston, and G. Adesso, Phys. Rev. Lett. **116**, 150502 (2016).
[6] D. Stahlke, Phys. Rev. A **90**, 022302 (2014).
[7] V. Veitch, S. A. H. Mousavian, D. Gottesman, and J. Emerson, New J. Phys. **16**, 013009 (2014).
[8] G. Vidal and R. Tarrach, Phys. Rev. A **59**, 141 (1999).
[9] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).
[10] E. Knill, Nature **434**, 39 (2005).
[11] M. Howard, J. Wallman, V. Veitch, and J. Emerson, Nature **510**, 351 (2014).
[12] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, New J. Phys. **14**, 113011 (2012).
[13] D. Gross, Journal of Mathematical Physics **47**, 122107 (2006).
[14] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).
[15] S. Bravyi and D. Gosset, Phys. Rev. Lett. **116**, 250501 (2016).
[16] S. Bravyi, G. Smith, and J. A. Smolin, Phys. Rev. X **6**, 021043 (2016).
[17] H. J. García, I. L. Markov, and A. W. Cross, Quantum Information & Computation **14**, 683 (2014).
[18] H. Pashayan, J. J. Wallman, and S. D. Bartlett, Phys. Rev. Lett. **115**, 070501 (2015).
[19] M. Amy, D. Maslov, and M. Mosca, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **33**, 1476 (2014).
[20] M. Amy and M. Mosca, arXiv:1601.07363 [quant-ph] (2016), arXiv:1601.07363 [quant-ph] .
[21] D. Gosset, V. Kliuchnikov, M. Mosca, and V. Russo, Quantum Information & Computation **14**, 1261 (2014).
[22] A. Bocharov, Y. Gurevich, and K. M. Svore, Phys. Rev. A **88**, 012313 (2013).
[23] G. Duclos-Cianci and K. M. Svore, Phys. Rev. A **88**, 042325 (2013).
[24] A. Paetznick and K. M. Svore, Quantum Information & Computation **14**, 1277 (2014).
[25] N. J. Ross and P. Selinger, arXiv:1403.2975 [quant-ph] (2014), arXiv:1403.2975 [quant-ph] .
[26] P. Selinger, Phys. Rev. A **87**, 042302 (2013).
[27] N. Wiebe and M. Roetteler, Quantum Information and Communication **16**, 134 (2016).
[28] C. Jones, Phys. Rev. A **87**, 022328 (2013).
[29] D. Gottesman and I. L. Chuang, Nature **402**, 390 (1999).
[30] X. Zhou, D. W. Leung, and I. L. Chuang, Phys. Rev. A **62**, 052316 (2000).
[31] E. T. Campbell and M. Howard, arXiv:1606.01904 [quant-ph] (2016), arXiv:1606.01904 [quant-ph] .
[32] E. T. Campbell and M. Howard, arXiv:1606.01906 [quant-ph] (2016), arXiv:1606.01906 [quant-ph] .