Complexity Classification of Conjugated Clifford Circuits

Adam Bouland[1]
Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, CA, USA
adam@csail.mit.edu
https://orcid.org/0000-0002-8556-8337

Joseph F. Fitzsimons[2]
Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372
Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543
joe.fitzsimons@nus.edu.sg

Dax Enshan Koh[3]
Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
daxkoh@mit.edu
https://orcid.org/0000-0002-8968-591X

Abstract

Clifford circuits – i.e. circuits composed of only CNOT, Hadamard, and $\pi/4$ phase gates – play a central role in the study of quantum computation. However, their computational power is limited: a well-known result of Gottesman and Knill states that Clifford circuits are efficiently classically simulable. We show that in contrast, “conjugated Clifford circuits” (CCCs) – where one additionally conjugates every qubit by the same one-qubit gate U – can perform hard sampling tasks. In particular, we fully classify the computational power of CCCs by showing that essentially any non-Clifford conjugating unitary U can give rise to sampling tasks which cannot be efficiently classically simulated to constant multiplicative error, unless the polynomial hierarchy collapses. Furthermore, by standard techniques, this hardness result can be extended to allow for the more realistic model of constant additive error, under a plausible complexity-theoretic conjecture. This work can be seen as progress towards classifying the computational power of all restricted quantum gate sets.

2012 ACM Subject Classification Theory of computation → Quantum complexity theory, Theory of computation → Computational complexity and cryptography

Keywords and phrases gate set classification, quantum advantage, sampling problems, polynomial hierarchy

Digital Object Identifier 10.4230/LIPIcs.CCC.2018.21

Related Version A full version of the paper is available at `https://arxiv.org/abs/1709.01805`.

[1] AB was partially supported by the NSF GRFP under Grant No. 1122374, by a Vannevar Bush Fellowship from the US Department of Defense, and by an NSF Waterman award under grant number 1249349.

[2] JFF acknowledges support from the Air Force Office of Scientific Research under AOARD grant no. FA2386-15-1-4082. This material is based on research supported in part by the Singapore National Research Foundation under NRF Award No. NRF-NRFF2013-01.

[3] DEK is supported by the National Science Scholarship from the Agency for Science, Technology and Research (A*STAR).

33rd Computational Complexity Conference (CCC 2018).
Editor: Rocco A. Servedio; Article No. 21; pp. 21:1–21:25
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany
COMPUTATIONAL COMPLEXITY CONFERENCE

Acknowledgements We thank Scott Aaronson, Mick Bremner, Alex Dalzell, Daniel Gottesman, Aram Harrow, Ashley Montanaro, Ted Yoder and Mithuna Yoganathan for helpful discussions.

1 Introduction

Quantum computers hold the promise of efficiently solving certain problems, such as factoring integers [53], which are believed to be intractable for classical computers. However, experimentally implementing many of these quantum algorithms is very difficult. For instance, the largest number factored to date using Shor's algorithm is 21 [40]. These considerations have led to an intense interest in algorithms which can be more easily implemented with near-term quantum devices, as well as a corresponding interest in the difficulty of these computational tasks for classical computers. Some prominent examples of such models are constant-depth quantum circuits [56, 11] and non-adaptive linear optics [3].

In many of these constructions, one can show that these "weak" quantum devices can perform *sampling* tasks which cannot be efficiently simulated classically, even though they may not be known to be capable of performing difficult *decision* tasks. Such arguments were first put forth by Bremner, Jozsa, and Shepherd [14] and Aaronson and Arkhipov [3], who showed that exactly simulating the sampling tasks performed by weak devices is impossible assuming the polynomial hierarchy is infinite. The proofs of these results use the fact that the output probabilities of quantum circuits can be very difficult to compute – in fact they can be GapP-hard and therefore #P-hard to approximate. In contrast the output probabilities of classical samplers can be approximated in $\mathsf{BPP}^{\mathsf{NP}}$ by Stockmeyer's approximate counting theorem [55], and therefore lie in the polynomial hierarchy. Hence a classical simulation of these circuits would collapse the polynomial hierarchy to the third level by Toda's Theorem [57]. Similar hardness results have been shown for many other models of quantum computation [56, 43, 22, 10, 21, 8, 16, 39].

A curious feature of many of these "weak" models of quantum computation is that they can be implemented using non-universal gate sets. That is, despite being able to perform sampling problems which appear to be outside of BPP, these models are not themselves known to be capable of universal quantum computation. In short these models of quantum computation seem to be "quantum-intermediate" between BPP and BQP, analogous to the NP-intermediate problems which are guaranteed to exist by Ladner's theorem [36]. From the standpoint of computational complexity, it is therefore natural to study this intermediate space between BPP and BQP, and to classify its properties.

One natural way to explore the space between BPP and BQP is to classify the power of all possible quantum gate sets over qubits. The Solovay-Kitaev Theorem states that all universal quantum gate sets, i.e. those which densely generate the full unitary group, have equivalent computational power [18]. Therefore the interesting gates sets to classify are those which are non-universal. However just because a gate set is non-universal does not imply it is weaker than BQP – in fact some non-universal gates are known to be capable of universality in an "encoded" sense, and therefore have the same computational power as BQP [32]. Other non-universal gate sets are efficiently classically simulable [25], while others seem to lie "between BPP and BQP" in that they are believed to be neither universal for BQP nor efficiently classically simulable [14]. It is a natural open problem to fully classify all restricted gate sets into these categories according to their computational complexity.

This is a challenging problem, and to date there has only been partial progress towards this classification. One immediate difficulty in approaching this problem is that there is not a known classification of all possible non-universal gate sets. In particular this would require classifying the discrete subgroups of $SU(2^n)$ for all $n \in \mathbb{N}$, which to date has only been solved for $n \leq 2$ [28]. Therefore existing results have characterized the power of modifications of known intermediate gate sets, such as commuting circuits and linear optical elements [9, 10, 47]. Others works have classified the classical subsets of gates [6, 27], or else given sufficient criteria for universality so as to rule out the existence of certain intermediate families [52]. A complete classification of this space "between BPP and BQP" would require a major improvement in our understanding of universality as well as the types of computational hardness possible between BPP and BQP.

One well-known example of a non-universal family of quantum gates is the Clifford group. Clifford circuits – i.e. circuits composed of merely CNOT, Hadamard and Phase gates – are a discrete subgroup of quantum gates which play an important role in quantum error correction [24, 13], measurement-based quantum computing [49, 50, 17], and randomized benchmarking [38]. However a well-known result of Gottesman and Knill states that circuits composed of Clifford elements are efficiently classically simulable [25, 5]. That is, suppose one begins in the state $|0\rangle^{\otimes n}$, applies polynomially many gates from the set $\mathrm{CNOT}, \mathrm{H}, \mathrm{S}$, then measures in the computational basis. Then the Gottesman-Knill theorem states that one can compute the probability a string y is output by such a circuit in classical polynomial time. One can also sample from the same probability distribution on strings as this circuit as well. A key part of the proof of this result is that the quantum state at intermediate stages of the circuit is always a "stabilizer state" – i.e. the state is uniquely described by its set of stabilizers in the Pauli group – and therefore has a compact representation. Therefore the Clifford group is incapable of universal quantum computation (assuming $\mathsf{BPP} \neq \mathsf{BQP}$).

In this work, we will study the power of a related family of non-universal gates, known as *Conjugated Clifford gates*, which we introduce below. These gates are non-universal by construction, but not known to be efficiently classically simulable either. Our main result will be to *fully classify* the computational power of this family of intermediate gate sets.

1.1 Our results

This paper considers a new "weak" model of quantum computation which we call "conjugated Clifford circuits" (CCCs). In this model, we consider the power of quantum circuits which begin in the state $|0\rangle^{\otimes n}$, and then apply gates from the set $(U^\dagger \otimes U^\dagger)(\mathrm{CNOT})(U \otimes U), U^\dagger H U, U^\dagger S U$ where U is a fixed one-qubit gate. In other words, we consider the power of Clifford circuits which are conjugated by an identical one-qubit gate U on each qubit. These gates manifestly perform a discrete subset of unitaries so this gate set is clearly not universal.

Although this transformation preserves the non-universality of the Clifford group, it is unclear if it preserves its computational power. The presence of generic conjugating unitaries (even the same U on each qubit, as in this model) breaks the Gottesman-Knill simulation algorithm [25], as the inputs and outputs of the circuit are not stabilizer states/measurements. Hence the intermediate states of the circuit are no longer efficiently representable by the stabilizer formalism. This, combined with prior results showing hardness for other modified versions of Clifford circuits [33, 34], leads one to suspect that CCCs may not be efficiently classically simulable. However prior to this work no hardness results were known for this model.

In this work, we confirm this intuition and provide two results in this direction. First, we provide a *complete classification* of the power of CCCs according to the choice of U. We do this by showing that *any* U which is not efficiently classically simulable by the

Gottesman-Knill theorem suffices to perform hard sampling problems with CCCs[4]. That is, for generic U, CCCs cannot be efficiently classically simulated to constant multiplicative error by a classical computer unless the polynomial hierarchy collapses. This result can be seen as progress towards classifying the computational complexity of restricted gate sets. Indeed, given a non-universal gate set G, a natural question is to classify the power of G when conjugated by the same one-qubit unitariy U on each qubit, as this transformation preserves non-universality. Our work resolves this question for one of the most prominent examples of non-universal gate sets, namely the Clifford group. As few examples of non-universal gate sets are known[5], this closes one of the major gaps in our understanding of intermediate gate sets. Of course this does not complete the complexity classification of all gate sets, as there is no known classification of all possible non-universal gate sets. However it does make progress towards this goal.

Second, we show that under an additional complexity-theoretic conjecture, classical computers cannot efficiently simulate CCCs to constant error in total variation distance. This is a more experimentally achievable model of error for noisy error-corrected quantum computations. The proof of this result uses standard techniques introduced by Aaronson and Arkhipov [3], which have also been used in other models [22, 15, 8, 16, 42, 39].

This second result is interesting for two reasons. First, it means our results may have relevance to the empirical demonstration of quantum advantage (sometimes referred to as "quantum supremacy") [48, 8, 4], as our results are robust to noise. Second, from the perspective of computational complexity, it gives yet another conjecture upon which one can base the supremacy of noisy quantum devices. As is the case with other quantum supremacy proposals [3, 22, 15, 42, 39], in order to show that simulation of CCCs to additive error still collapses the polynomial hierarchy, we need an additional conjecture stating that the output probabilities of these circuits are hard to approximate on average. Our conjecture essentially states that for most Clifford circuits V and most one-qubit unitaries U, it is #P-hard to approximate a constant fraction of the output probabilities of the CCC $U^{\otimes n}V(U^{\dagger})^{\otimes n}$ to constant multiplicative error. We prove that this conjecture is true in the worst case – in fact, for all non-Clifford U, there exists a V such that some outputs are #P-hard to compute to multiplicative error. However, it remains open to extend this hardness result to the average case, as is the case with other supremacy proposals as well [3, 22, 15, 42, 39]. To the best of our knowledge our conjecture is independent of the conjectures used to establish other quantum advantage results such as boson sampling [3], Fourier sampling [22] or IQP [15, 16]. Therefore our results can be seen as establishing an alternative basis for belief in the advantage of noisy quantum devices over classical computation.

One final motivation for this work is that CCCs might admit a simpler fault-tolerant implementation than universal quantum computing, which we conjecture to be the case. It is well-known that many stabilizer error-correcting codes, such as the 5-qubit and 7-qubit codes [37, 19, 54], admit transversal Clifford operations [24]. That is, performing fault-tolerant Clifford operations on the encoded logical qubits can be done in a very simple manner – by simply performing the corresponding Clifford operation on the physical qubits. This is manifestly fault-tolerant, in that an error on one physical qubit does not "spread" to more than 1 qubit when applying the gate. In contrast, performing non-Clifford operations fault-tolerantly on such codes requires substantially larger (and non-transversal) circuits – and

[4] More precisely, we show that any U that cannot be written as a Clifford times a Z-rotation suffices to perform hard sampling problems with CCCs. See Theorem 7 for the exact statement.

[5] The only examples to our knowledge are matchgates, Clifford gates, diagonal gates, and subsets thereof.

therefore the non-transversal operations are often the most resource intensive. The challenge in fault-tolerantly implementing CCCs therefore lies in performing the initial state preparation and measurement. Initial preparation of non-stabilizer states in these codes is equivalent to the challenge of producing magic states, which are already known to boost Clifford circuits to universality using adaptive Clifford circuits [13, 12] (in contrast our construction would only need non-adaptive Clifford circuits with magic states). Likewise, measuring in a non-Clifford basis would require performing non-Clifford one-qubit gates prior to fault-tolerant measurement in the computational basis. Therefore the state preparation/measurement would be the challenging part of fault-tolerantly implementing CCCs in codes with transversal Cliffords. It remains open if there exists a code with transversal conjugated Cliffords[6] and easy preparation and measurement in the required basis. Such a code would not be ruled out by the Eastin-Knill Theorem [20], which states that the set of transversal gates must be discrete for all codes which correct arbitrary one qubit errors. Of course this is not the main motivation for exploring the power of this model – which is primarily to classify the space between BPP and BQP – but an easier fault-tolerant implementation could be an unexpected bonus of our results.

1.2 Proof Techniques

To prove these results, we use several different techniques.

1.2.1 Proof Techniques: classification of exact sampling hardness

To prove exact (or multiplicative) sampling hardness for CCCs for essentially all non-Clifford U, we use the notion of postselection introduced by Aaronson [2]. Postselection is the (non-physical) ability to discard all runs of the computation which do not achieve some particular outcomes. Our proof works by showing that postselecting such circuits allows them to perform universal quantum computation. Hardness then follows from known techniques [2, 14, 3].

One technical subtlety that we face in this proof, which is not present in other results, is that our postselected gadgets perform operations which are not closed under inversion. This means one cannot use the Solovay-Kitaev theorem to change quantum gate sets [18]. This is a necessary step in the proof that PostBQP = PP [2], which is a key part of the hardness proof (see [10]). Fortunately, it turns out that we can get away without inverses due to a recent inverse-free Solovay-Kitaev theorem of Sardharwalla *et al.* [51], which removes the needs for inverses if the gate set contains the Paulis. Our result would have been much more difficult to obtain without this prior result. To our knowledge this is the first application of their result to structural complexity.

A further difficulty in the classification proof is that the postselection gadgets we derive do not work for all non-Clifford U. In general, most postselection gadgets give rise to non-unitary operations, and for technical reasons we need to work with unitary postselection gadgets to apply the results of [51]. Therefore, we instead use several different gadgets which cover different portions of the parameter space of U's. Our initial proof of this fact used a total

[6] Of course one can always "rotate" a code with transversal Clifford operations to obtain a code with transversal conjugated Cliffords. If the code previously had logical states $|0\rangle_L, |1\rangle_L$, then by setting the states $|0\rangle'_L = U_L^\dagger|0\rangle_L$ and $|1\rangle'_L = U_L^\dagger|1\rangle_L$, one obtains a code in which the conjugated Clifford gates (conjugated by U) are transversal. However having the ability to efficiently fault-tolerantly prepare $|0\rangle_L$ in the old code does not imply the same ability to prepare $|0\rangle'_L$ in the new code.

of seven postselection gadgets found by hand. We later simplified this to two postselection gadgets by conducting a brute-force search for suitable gadgets using Christopher Granade and Ben Criger's QuaEC package [26]. We include this simplified proof in this writeup.

A final difficulty that one often faces with postselected universality proofs is that one must show that the postselection gadgets boost the original gate set to universality. In general this is a nontrivial task; there is no simple test of whether a gate set is universal, though some sufficient (but not necessary) criteria are known [52]. Prior gate set classification theorems have solved this universality problem using representation theory [9, 52] or Lie theory [10, 47]. However, in our work we are able to make use of a powerful fact: namely that the Clifford group plus *any* non-Clifford unitary is universal. This follows from results of Nebe, Rains and Sloane [44, 45, 1] classifying the invariants of the Clifford group[7]. As a result our postselected universality proofs are much simpler than in other gate set classification theorems.

1.2.2 Proof techniques: additive error

To prove hardness of simulation to additive error, we follow the techniques of [3, 15, 22, 42]. In these works, to show hardness of sampling from some probability distribution with additive error, one combines three different ingredients. The first is anti-concentration – showing that for these circuits, the output probabilities in some large set T are somewhat large. Second, one uses Markov's inequality to argue that, since the simulation error sums to ϵ, on some other large set of output probabilities S, the error must be below a constant multiple of the average. If S and T are both large, they must have some intersection – and on this intersection $S \cap T$, the imagined classical simulation is not only a simulation to additive error, but also to multiplicative error as well (since the output probability in question is above some minimum). Therefore a simulation to some amount ϵ of additive error implies a multiplicative simulation to the output probabilities on a constant fraction of the outputs. The impossibility of such a simulation is then obtained by assuming that computing these output probabilities is multiplicatively hard on average. In particular, one assumes that it is a #P-hard task to compute the output probability on $|S \cap T|/2^n$ -fraction of the outputs. This leads to a collapse of the polynomial hierarchy by known techniques [3, 14].

We follow this technique to show hardness of sampling with additive error. In our case, the anticoncentration theorem follows from the fact that the Clifford group is a "2-design" [58, 59] – i.e. a random Clifford circuit behaves equivalently to a random unitary up to its second moment – and therefore must anticoncentrate, as a random unitary does (the fact that unitary designs anticoncentrate was also shown independently by several groups [29, 39, 31]). This is similar to the hardness results for IQP [15] and DQC1 [42], in which the authors also prove their corresponding anticoncentration theorems. In contrast it is open to prove the anticoncentration theorem used for Boson Sampling and Fourier Sampling [3, 22], though these models have other complexity-theoretic advantages[8]. Therefore the only assumption needed is the hardness-on-average assumption. We also show that our hardness assumption is true for worst-case inputs. This result follows from combining known facts about BQP with the classification theorem for exact sampling hardness.

[7] However we note that in our proofs we will only use the fact that the Clifford group plus any non-Clifford element is universal on a qubit. This version of the theorem admits a direct proof using the representation theory of $SU(2)$.

[8] For instance, for these models it is known to be #P-hard to *exactly* compute most output probabilities of their corresponding circuit. This is a necessary but not sufficient condition for the supremacy conjectures to be true, which require it to be #P-hard to *approximately* compute most output probabilities of their corresponding circuit. It remains open to show an exact average-to-worst case reduction for models which exhibit anticoncentration, such as our model, IQP, and DQC1.

1.3 Relation to other works on modified Clifford circuits

While we previously discussed the relation of our results to prior work on gate set classification and sampling problems, here we compare our results to prior work on Clifford circuits. We are not the first to consider the power of modified Clifford circuits. Jozsa and van den Nest [33] and Koh [34], categorized the computational power of a number of modified versions of Clifford circuits. The closest related result is the statement in [33] that if the input state to a Clifford circuit is allowed to be an arbitrary tensor product of one-qubit states, then such circuits cannot be efficiently classically simulated unless the polynomial hierarchy collapses. Their hardness result uses states of the form $|0\rangle^{\otimes n/2}|\alpha\rangle^{\otimes n/2}$, where $|\alpha\rangle = \cos(\pi/8)|0\rangle + i\sin(\pi/8)|1\rangle$ is a magic state. They achieve postselected hardness via the use of magic states to perform T gates, using a well-known construction (see e.g. [13]). So in the [33] construction there are different input states on different qubits. In contrast, our result requires the same input state on every qubit – as well as measurement in that basis at the end of the circuit. This ensures our modified circuit can be interpreted as the action of a discrete gate set, and therefore our result has relevance for the classification of the power of non-universal gate sets.

2 Preliminaries

We denote the single-qubit *Pauli matrices* by $X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The ±1-eigenstates of Z are denoted by $|0\rangle$ and $|1\rangle$ respectively. The *rotation operator* about an axis $t \in \{x, y, z\}$ with an angle $\theta \in [0, 2\pi)$ is

$$R_t(\theta) = e^{-i\theta\sigma_t/2} = \cos(\theta/2)I - i\sin(\theta/2)\sigma_t. \tag{1}$$

We will use the fact that any single-qubit unitary operator U can be written as

$$U = e^{i\alpha} R_z(\phi) R_x(\theta) R_z(\lambda), \tag{2}$$

where $\alpha, \phi, \theta, \lambda \in [0, 2\pi)$ [46].

For linear operators A and B, we write $A \propto B$ to mean that there exists $\alpha \in \mathbb{C}\backslash\{0\}$ such that $A = \alpha B$. For linear operators, vectors or complex numbers a and b, we write $a \sim b$ to mean that a and b differ only by a global phase, i.e. there exists $\theta \in [0, 2\pi)$ such that $a = e^{i\theta} b$. For any subset $S \subseteq \mathbb{R}$ and $k \in \mathbb{R}$, we write kS to refer to the set $\{kn : n \in S\}$. For example, $k\mathbb{Z} = \{kn : n \in \mathbb{Z}\}$. We denote the set of odd integers by $\mathbb{Z}_{odd}$. We denote the complement of a set S by S^c.

2.1 Clifford circuits and conjugated Clifford circuits

The n-qubit *Pauli group* $\mathcal{P}_n$ is the set of all operators of the form $i^k P_1 \otimes \ldots \otimes P_n$, where $k \in \{0, 1, 2, 3\}$ and each P_j is a Pauli matrix. The n-qubit *Clifford group* is the normalizer of $\mathcal{P}_n$ in the n-qubit unitary group $\mathcal{U}_n$, i.e. $\mathcal{C}_n = \{U \in \mathcal{U}_n : U\mathcal{P}_n U^\dagger = \mathcal{P}_n\}$.

The elements of the Clifford group, called *Clifford operations*, have an alternative characterization: an operation is a Clifford operation if and only if it can be written as a circuit comprising the following gates, called *basic Clifford gates*: *Hadamard*, $\pi/4$ *phase*, and *controlled-NOT* gates, whose matrix representations in the computational basis are

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad \text{and} \quad \text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

respectively. An example of a non-Clifford gate is the T gate, whose matrix representation is given by $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$. We denote the group generated by the single-qubit Clifford gates by $\langle S, H \rangle$.

We will make use of the following fact about Clifford operations.

▶ **Fact 1.** *$R_z(\phi)$ is a Clifford operation if and only if $\phi \in \frac{\pi}{2}\mathbb{Z}$.*

A *Clifford circuit* is a circuit that consists of computational basis states being acted on by the basic Clifford gates, before being measured in the computational basis. Without loss of generality, we may assume that the input to the Clifford circuit is the all-zero state $|0\rangle^{\otimes n}$. We define conjugated Clifford circuits (CCCs) similarly to Clifford circuits, except that each basic Clifford gate G is replaced by a conjugated basic Clifford gate $(U^{\otimes k})^\dagger g U^{\otimes k}$, where $k = 1$ when $g = H, S$ and $k = 2$ when $g = \text{CNOT}$. In other words,

▶ **Definition 2.** Let U be a single-qubit unitary gate. A U-conjugated Clifford circuit (U-CCC) on n qubits is defined to be a quantum circuit with the following structure:

1. Start with $|0\rangle^{\otimes n}$.
2. Apply gates from the set $\{U^\dagger H U, U^\dagger S U, (U^\dagger \otimes U^\dagger)\text{CNOT}(U \otimes U)\}$.
3. Measure each qubit in the computational basis.

Because the intermediate U and $U^\dagger$ gates cancel, we may equivalently describe a U-CCC as follows:

1. Start with $|0\rangle^{\otimes n}$.
2. Apply $U^{\otimes n}$.
3. Apply gates from the set $\{H, S, \text{CNOT}\}$.
4. Apply $(U^\dagger)^{\otimes n}$.
5. Measure each qubit in the computational basis.

2.2 Notions of classical simulation of quantum computation

Let $\mathcal{P} = \{p_z\}_z$ and $\mathcal{Q} = \{q_z\}_z$ be (discrete) probability distributions, and let $\epsilon \geq 0$. We say that $\mathcal{Q}$ is a *multiplicative ϵ-approximation* of $\mathcal{P}$ if for all z,

$$|p_z - q_z| \leq \epsilon p_z. \tag{3}$$

We say that $\mathcal{Q}$ is an *additive ϵ-approximation* of $\mathcal{P}$ if

$$\frac{1}{2}\sum_z |p_z - q_z| \leq \epsilon. \tag{4}$$

Note that any multiplicative ϵ-approximation is also an additive $\epsilon/2$-approximation, since summing Eq. (3) over all z produces Eq. (4). Here the factor of 1/2 is present so that ϵ is the total variation distance between the probability distributions.

A *weak simulation with multiplicative (additive) error* $\epsilon > 0$ of a family of quantum circuits is a classical randomized algorithm that samples from a distribution that is a multiplicative (additive) ϵ-approximation of the output distribution of the circuit. Note that from an experimental perspective, additive error is the more appropriate choice, since the fault-tolerance theorem merely guarantees additive closeness between the ideal and realized output distributions [7].

There are of course other notions of simulability of quantum circuits – such as strong simulation where one can compute individual output probabilities. We discuss these further in Section 6.

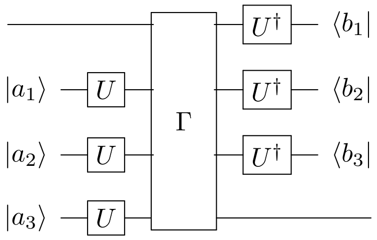
2.3 Postselection gadgets

Our results involve the use of postselection gadgets to simulate unitary operations. In this section, we introduce some terminology to describe these gadgets.

▶ **Definition 3.** Let U be a single-qubit operation. Let $k, l \in \mathbb{Z}^+$ with $k > l$. A *k-to-l U-CCC postselection gadget G* is a postselected circuit fragment that performs the following procedure on an l-qubit system:

1. Introduce a set T of $(k-l)$ ancilla registers in the state $|a_1 \dots a_{k-l}\rangle$, where $a_1 \dots a_{k-l} \in \{0,1\}^{k-l}$.
2. Apply $U^{\otimes(k-l)}$ to the set T of registers.
3. Apply a k-qubit Clifford operation Γ to both the system and ancilla.
4. Choose a subset S of $(k-l)$ registers and apply $(U^\dagger)^{\otimes(k-l)}$ to S.
5. Postselect on the subset S of qubits being in the state $|b_1 \dots b_{k-l}\rangle$, where $b_1 \dots b_{k-l} \in \{0,1\}^{k-l}$.

An example of a 4-to-1 U-CCC postselection gadget is the circuit fragment described by the following diagram:



Let G be a U-CCC postselection gadget as described in Definition 3. The *action* $A(G)$ (also denoted A_G) of G is defined to be the linear operation that it performs, i.e.

$$A(G) = A_G = \langle b_1 \dots b_l|_S \left(\prod_{i\in S} U_i^\dagger\right) \Gamma \left(\prod_{i\in T} U_i\right) |a_1 \dots a_l\rangle_T, \tag{5}$$

and the *normalized action* of G, when it exists, is

$$\tilde{A}_G = \frac{A_G}{(\det A_G)^{2^{-l}}}. \tag{6}$$

Note that the above normalization is chosen so that $\det \tilde{A}_G = 1$.

We say that a U-CCC postselection gadget G is *unitary* if there exists $\alpha \in \mathbb{C}\backslash\{0\}$ and a unitary operator U such that $A_G = \alpha U$. It is straightforward to check that the following are equivalent conditions for gadget unitarity.

▶ **Lemma 4.** *A U-CCC postselection gadget G is unitary if and only if either one of the following holds:*

1. *There exists $\gamma > 0$ such that $A_G^\dagger A_G = \gamma I$,*
2. *$\tilde{A}_G^\dagger \tilde{A}_G = I$, i.e. $\tilde{A}_G$ is unitary.*

Similarly, we say that a U-CCC postselection gadget G is *Clifford* if there exists $\alpha \in \mathbb{C}\backslash\{0\}$ and a Clifford operator U such that $A_G = \alpha U$. The following lemma gives a necessary condition for a gadget to be Clifford.

▶ **Lemma 5.** *If G is a Clifford U-CCC postselection gadget, then*

$$A_G X A_G^\dagger \propto X \text{ or } A_G X A_G^\dagger \propto Y \text{ or } A_G X A_G^\dagger \propto Z, \tag{7}$$

and

$$A_G Z A_G^\dagger \propto X \text{ or } A_G Z A_G^\dagger \propto Y \text{ or } A_G Z A_G^\dagger \propto Z. \tag{8}$$

Proof. If G is a Clifford U-CCC postselection gadget, then there exists $\alpha \in \mathbb{C}\backslash\{0\}$ and a Clifford operation Γ such that $A_G = \alpha\Gamma$. Since Γ is Clifford, $\Gamma X \Gamma^\dagger$ is a Pauli operator. But $\Gamma X \Gamma^\dagger \not\sim I$, otherwise, $X \sim I$, which is a contradiction. Hence, $\Gamma X \Gamma^\dagger \sim X$ or Y or Z, which implies Eq. (7). The proof of Eq. (8) is similar, with X replaced with Z. ◀

3 Weak simulation of CCCs with multiplicative error

3.1 Classification results

In this section, we classify the hardness of weakly simulating U-CCCs as we vary U. As we shall see, it turns out that the classical simulation complexities of the U-CCCs associated with this notion of simulation are all of the following two types: the U-CCCs are either efficiently simulable, or are hard to simulate to constant multiplicative error unless the polynomial hierarchy collapses. To facilitate exposition, we will introduce the following terminology to describe these two cases: Let $\mathcal{C}$ be a class of quantum circuits. Following the terminology in [34], we say that $\mathcal{C}$ is in PWEAK if it is efficiently simulable in the weak sense by a classical computer. We say that $\mathcal{C}$ is PH-*supreme* (or that it exhibits PH-*supremacy*) if it satisfies the property that if $\mathcal{C}$ is efficiently simulable in the weak sense by a classical computer to constant multiplicative error, then the polynomial hierarchy (PH) collapses.

The approach we take to classifying the U-CCCs is to decompose each U into the form given by Eq. (2),

$$U = e^{i\alpha} R_z(\phi) R_x(\theta) R_z(\lambda), \tag{9}$$

and study how the classical simulation complexity changes as we vary α, ϕ, θ and λ. Two simplifications can immediately be made. First, the outcome probabilities of the U-CCC are independent of α, since α appears only in a global phase. Second, the probabilities are also independent of λ. To see this, note that the outcome probabilities are all of the form:

$$|\langle b|R_z(-\lambda)^{\otimes n} V R_z(\lambda)^{\otimes n}|0\rangle|^2 = |\langle b|V|0\rangle|^2, \tag{10}$$

which is independent of λ. In the above expression, $b \in \{0,1\}^n$ and

$$V = R_x(-\theta)^{\otimes n} R_z(-\phi)^{\otimes n} \Gamma R_z(\phi)^{\otimes n} R_x(\theta)^{\otimes n}$$

for some Clifford circuit Γ. The equality follows from the fact that the computational basis states are eigenstates of $R_z(\lambda)^{\otimes n}$ with unit-magnitude eigenvalues.

Table 1 Complete complexity classification of U-CCCs (where $U = R_z(\phi)R_x(\theta)$) with respect to weak simulation, as we vary ϕ and θ. The roman numerals in parentheses indicate the parts of Lemma 6 that are relevant to the corresponding box. All U-CCCs are either in PWEAK (i.e. can be efficiently simulated in the weak sense) or PH-supreme (i.e. cannot be simulated efficiently in the weak sense, unless the polynomial hierarchy collapses.)

ϕ \ θ	$\pi\mathbb{Z}$	$\frac{\pi}{2}\mathbb{Z}_{odd}$	$\left(\frac{\pi}{2}\mathbb{Z}\right)^c$
$\frac{\pi}{2}\mathbb{Z}$	PWEAK (i, ii)	PWEAK (ii)	PH-supreme (iv)
$\left(\frac{\pi}{2}\mathbb{Z}\right)^c$	PWEAK (i)	PH-supreme (iii)	PH-supreme (iv)

Hence, to complete the classification, it suffices to just restrict our attention to the two-parameter family $\{R_z(\phi)R_x(\theta)\}_{\phi,\theta}$ of unitaries. We first prove the following lemma (see Table 1 for a summary):

▶ **Lemma 6.** *Let $U = R_z(\phi)R_x(\theta)$, where $\phi, \theta \in [0, 2\pi)$. Then*

- *U-CCCs are in* PWEAK, *if*
  (i) $\phi \in [0, 2\pi)$ *and* $\theta \in \pi\mathbb{Z}$, *or*

  (ii) $\phi \in \frac{\pi}{2}\mathbb{Z}$ *and* $\theta \in \frac{\pi}{2}\mathbb{Z}$.
- *U-CCCs are* PH-*supreme, if*
  (iii) $\phi \notin \frac{\pi}{2}\mathbb{Z}$ *and* $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$, *or*

  (iv) $\theta \notin \frac{\pi}{2}\mathbb{Z}$.

We defer the proof of Lemma 6 to Sections 3.2 and 3.3. Lemma 6 allows us to prove our main theorem:

▶ **Theorem 7.** *Let U be a single-qubit unitary operator. Consider the following two statements:*

(A) *U-CCC is in* PWEAK.

(B) *There exists a single-qubit Clifford operator $\Gamma \in \langle S, H\rangle$ and $\lambda \in [0, 2\pi)$ such that*[9]

$$U \sim \Gamma R_z(\lambda). \tag{11}$$

Then,

1. *(B) implies (A).*
2. *If the polynomial hierarchy is infinite, then (A) implies (B).*

In other words, if we assume that the polynomial hierarchy is infinite, then U-CCCs are PH-*supreme if and only if they cannot be written in the form $U \sim \Gamma R_z(\lambda)$, where Γ is a Clifford circuit and $R_z(\lambda)$ is a Z-rotation.*

Proof.

1. Since $R_z(\lambda)|0\rangle \sim |0\rangle$, it follows that for any Γ, $\Gamma R_z(\lambda)$-CCCs have the same outcome probabilities as Γ-CCCs. But C-CCCs are efficiently simulable, by the Gottesman-Knill Theorem, since $\Gamma \in \langle S, H\rangle$. Hence, U-CCCs are in PWEAK.

[9] or alternatively, we could restrict the range of λ to be in $[0, \pi]$, since any factor of $R_z(\pi/2) \sim S$ can be absorbed into the Clifford operator Γ.

2. Let U be such that U-CCCs are in PWEAK. Using the decomposition in Eq. (2), write $U = e^{i\alpha} R_z(\phi) R_x(\theta) R_z(\lambda)$. Since we assumed that the polynomial hierarchy is infinite, Lemma 6 implies that

a. $\theta \in \pi\mathbb{Z}$, or

b. $\theta \in \frac{\pi}{2}\mathbb{Z}$ and $\phi \in \frac{\pi}{2}\mathbb{Z}$.

In Case (a), $\theta \in 2\pi\mathbb{Z}$ or $\pi\mathbb{Z}_{odd}$. If $\theta \in 2\pi\mathbb{Z}$, then

$$U \sim R_z(\phi) R_x(2\pi\mathbb{Z}) R_z(\gamma) = I.R_z(\phi + \gamma),$$

which is of the form given by Eq. (11). If $\pi\mathbb{Z}_{odd}$, then

$$U \sim R_z(\phi) R_x(\pi\mathbb{Z}_{odd}) R_z(\gamma) \sim R_z(\phi) X R_z(\gamma) = X R_z(\gamma - \phi),$$

which is again of the form given by Eq. (11).

In Case (b),

$$\begin{aligned} U &\in e^{i\alpha} R_z(\pi\mathbb{Z}/2) R_x(\pi\mathbb{Z}/2) R_z(\gamma) \\ &= e^{i\alpha} R_z(\pi\mathbb{Z}/2) H R_z(\pi\mathbb{Z}/2) H R_z(\gamma). \end{aligned} \tag{12}$$

But the elements of $R_z(\pi\mathbb{Z}/2)$ are of the form S^j, for $j \in \mathbb{Z}$, up to a global phase. Therefore, $R_z(\pi\mathbb{Z}/2) H R_z(\pi\mathbb{Z}/2) H$ is Clifford, and U is of the form Eq. (11). ◀

Hence, Theorem 7 tells us that under the assumption that the polynomial hierarchy is infinite, U-CCCs can be simulated efficiently (in the weak sense) if and only if $U \sim \Gamma R_z(\lambda)$ for some single qubit Clifford operator Γ, i.e. if U is a Clifford operation times a Z-rotation.

3.2 Proofs of efficient classical simulation

In this section, we prove Cases (i) and (ii) of Lemma 6.

3.2.1 Proof of Case (i): $\phi \in [0, 2\pi)$ and $\theta \in \pi\mathbb{Z}$

▶ **Theorem 8.** *Let $U = R_z(\phi) R_x(\theta)$. If $\phi \in [0, 2\pi)$ and $\theta \in \pi\mathbb{Z}$, then U-CCCs are in* PWEAK.

Proof. First, we consider the case where $\theta \in 2\pi\mathbb{Z}$. In this case, $U = R_z(\phi)$, and the amplitudes of the U-CCC can be written as

$$\langle y | R_z(-\phi)^{\otimes n} \Gamma R_z(\phi)^{\otimes n} | x \rangle \sim \langle y | \Gamma | x \rangle \tag{13}$$

for some Clifford operation Γ and computational basis states $|x\rangle$ and $|y\rangle$. By the Gottesman-Knill Theorem, these U-CCCs can be efficiently weakly simulated.

Next, we consider the case where $\theta \in \pi\mathbb{Z}_{odd}$. In this case, $U = R_z(\phi) R_x(\pi) \sim R_z(\phi) X$, and the amplitudes of the U-CCC can be written as

$$\langle y | X^{\otimes n} R_z(-\phi)^{\otimes n} \Gamma R_z(\phi)^{\otimes n} X^{\otimes n} | x \rangle \sim \langle \bar{y} | \Gamma | \bar{x} \rangle \tag{14}$$

for some Clifford operation Γ and computational basis states $|x\rangle$ and $|y\rangle$, where $\bar{z}$ is the bitwise negation of z. By the Gottesman-Knill Theorem, these U-CCCs can be efficiently weakly simulated.

Putting the above results together, we get that U-CCCs are in PWEAK. ◀

3.2.2 Proof of Case (ii): $\phi \in \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}$

▶ **Theorem 9.** *Let $U = R_z(\phi)R_x(\theta)$. If $\phi \in \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}$, then U-CCCs are in* PWEAK*.*

Proof. The elements of $R_z(\frac{\pi}{2}\mathbb{Z})$ are of the form S^j, where $j \in \mathbb{Z}$, up to a global phase. Therefore, $U = R_z(\phi)R_x(\theta) = R_z(\phi)HR_z(\theta)H$ is a Clifford operation, and so, the U-CCCs consist of only Clifford gates. By the Gottesman-Knill Theorem, these U-CCCs can be be efficiently (weakly) simulated. ◀

3.3 Proofs of hardness

In this section, we prove Cases (iii) and (iv) of Lemma 6. Our proof uses postselection gadgets, similar to the techniques used in [14, 10]. One can also prove hardness using techniques from measurement-based-quantum computing, at least for certain U. We give such a proof in the appendix of the full version of our paper for the interested reader; we believe this proof may be more intuitive for those who are familiar with measurement-based quantum computing.

We start by proving a lemma that will be useful for the proofs of hardness.

▶ **Lemma 10.** *(Sufficient condition for* PH*-supremacy) Let U be a single-qubit gate. If there exists a unitary non-Clifford U-CCC postselection gadget G, then U-CCCs are* PH*-supreme.*

Proof. Suppose such a gadget G exists. Then, since the Clifford group plus any non-Clifford gate is universal [44, 45, 1], the Clifford group plus G must be universal on a single qubit. Then, by the inverse-free Solovay-Kitaev Theorem of Sardharwalla *et al.* [51], using polynomially many gates from the set G, H, S one can compile any desired one-qubit unitary V to inverse exponential accuracy (since in particular $\langle H, S \rangle$ contains the Paulis). In particular, since any three-qubit unitary can be expressed as a product of a constant number of CNOTs and one-qubit unitaries, one can compile any gate in the set {CCZ, Controlled-H, all one-qubit gates } to inverse exponential accuracy with polynomial overheard.

In his proof that PostBQP = PP, Aaronson showed that postselected poly-sized circuits of the above gates can compute any language in PP [2]. Furthermore, as his postselection succeeds with inverse exponential probability, compiling these gates to inverse exponential accuracy is sufficient for performing arbitrary PP computations.

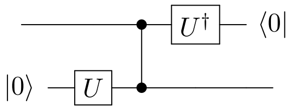
Hence, by using polynomially many gadgets for G, CNOT, H and S, one can compile Aaronson's circuits[10] for computing PP to inverse exponential accuracy, and hence these circuits can compute PP-hard problems. PH-supremacy then follows from the techniques of [14, 3]. Namely, a weak simulation of such circuits with constant multiplicative error would place PP $\subseteq$ BPP$^{\mathsf{NP}}$ $\subseteq \Delta_3$ by Stockmeyer counting, and hence by Toda's theorem this would result in the collapse of PH to the third level. In fact, by the arguments of Fujii *et al.* [23], one can collapse PH to the second level as well, by placing coC$_=$P in SBP, and we refer the interested reader to their work for the complete argument. ◀

[10] More specifically, we compile the circuit given by $(U^\dagger)^{\otimes n}$, then Aaronson's circuit, then $U^{\otimes n}$, as we need to cancel the U's at the beginning and the $U^\dagger$s at the end in order to perform Aaronson's circuit which starts and measures in the computational basis. However as the $U, U^\dagger$ are one-qubit gates, one can cancel them to inverse exponential accuracy using our gates, and hence this construction suffices.

3.3.1 Proof of Case (iii): $\phi \notin \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$

Let $U = R_z(\phi)R_x(\theta)$. Consider the following U-CCC postselection gadget:

$I(\phi, \theta) =$ (15)



We now prove some properties about $I(\phi, \theta)$.

▶ **Theorem 11.**

1. *The action of* $I(\phi, \theta)$ *is*

$$A_{I(\phi,\theta)} = \begin{pmatrix} \cos^2\frac{\theta}{2} & \frac{i}{2}\sin\theta\ e^{-i\phi} \\ -\frac{i}{2}\sin\theta\ e^{i\phi} & -\sin^2\frac{\theta}{2} \end{pmatrix}. \tag{16}$$

2. $I(\phi, \theta)$ *is a unitary gadget if and only if* $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$. *When* $I(\phi, \theta)$ *is unitary,*

$$\tilde{A}_{I(\phi,\theta)} = \frac{i}{\sqrt{2}} \begin{pmatrix} 1 & i(-1)^k e^{-i\phi} \\ -i(-1)^k e^{i\phi} & -1 \end{pmatrix}, \tag{17}$$

where $k = \frac{\theta}{\pi} - \frac{1}{2}$.

3. $I(\phi, \theta)$ *is a Clifford gadget if and only if* $\phi \in \frac{\pi}{2}\mathbb{Z}$ *and* $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$.
4. $I(\phi, \theta)$ *is a unitary non-Clifford gadget if and only if* $\phi \notin \frac{\pi}{2}\mathbb{Z}$ *and* $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$.

Proof.

1. By direct calculation.
2. By Eq. (16),

$$A^\dagger_{I(\phi,\theta)} A_{I(\phi,\theta)} = \begin{pmatrix} \cos^2\frac{\theta}{2} & \frac{i}{4}\sin(2\theta)e^{-i\phi} \\ -\frac{i}{4}\sin(2\theta)e^{i\phi} & \sin^2\frac{\theta}{2} \end{pmatrix}. \tag{18}$$

If $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$, then $A^\dagger_{I(\phi,\theta)} A_{I(\phi,\theta)} = \frac{1}{2}I$, which implies that $I(\phi, \theta)$ is a unitary gadget, by Lemma 4. Conversely, assume that $I(\phi, \theta)$ is a unitary gadget. Suppose that $\theta \notin \frac{\pi}{2}\mathbb{Z}_{odd}$. Then $\sin(2\theta) \neq 0$, which implies that $A^\dagger_{I(\phi,\theta)} A_{I(\phi,\theta)} \not\propto I$, which is a contradiction. Hence, $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$.

Next, $k = \frac{\theta}{\pi} - \frac{1}{2}$ implies that $\theta = \frac{\pi}{2}(2k+1)$. Since $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$, it follows that $k \in \mathbb{Z}$. Then $\sin\theta = (-1)^k$, $\cos^2\frac{\theta}{2} = \frac{1}{2}$ and $\sin^2\frac{\theta}{2} = \frac{1}{2}$. Hence,

$$A_{I(\phi,\theta)} = \begin{pmatrix} \frac{1}{2} & \frac{i}{2}(-1)^k e^{-i\phi} \\ -\frac{i}{2}(-1)^k e^{i\phi} & -\frac{1}{2} \end{pmatrix}. \tag{19}$$

Hence, $\det A_{I(\phi,\theta)} = -\frac{1}{2}$. Plugging this and Eq. (19) into Eq. (6) gives Eq. (17).

3. ($\Leftarrow$) Let $\phi \in \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$. Write $\phi = \frac{\pi}{2}l$ and $\theta = \frac{\pi}{2}(2k+1)$. Then, by Eq. (17),

$$\tilde{A}_{I(\phi,\theta)} = \frac{i}{\sqrt{2}} \begin{pmatrix} 1 & i^{1+2k+3l} \\ i^{3+2k+l} & -1 \end{pmatrix}. \tag{20}$$

Now, it is straightforward to check that for all $k, l \in \mathbb{Z}$, $\tilde{A}_{I(\phi,\theta)} X \tilde{A}^\dagger_{I(\phi,\theta)} \in \{-X, Z, -Z\}$ and $\tilde{A}_{I(\phi,\theta)} Z \tilde{A}^\dagger_{I(\phi,\theta)} \in \{-Y, X, Y, -X\}$. This shows that $\tilde{A}_{I(\phi,\theta)}$ maps the Pauli group to itself, under conjugation, which implies that $\tilde{A}_{I(\phi,\theta)}$ is Clifford.

($\Rightarrow$) Assume that $I(\phi,\theta)$ is a Clifford gadget. Suppose that $\phi \notin \frac{\pi}{2}\mathbb{Z}$ or $\theta \notin \frac{\pi}{2}\mathbb{Z}_{odd}$. But $I(\phi,\theta)$ is unitary, and hence, $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$. So $\phi \notin \frac{\pi}{2}\mathbb{Z}$. By Lemma 5, $\tilde{A}_{I(\phi,\theta)} X \tilde{A}^\dagger_{I(\phi,\theta)} \sim X$ or Y or Z. But, as we compute,

$$\tilde{A}_{I(\phi,\theta)} X \tilde{A}^\dagger_{I(\phi,\theta)} = \begin{pmatrix} (-1)^k \sin\phi & -e^{-i\phi}\cos\phi \\ -e^{i\phi}\cos\phi & -(-1)^k \sin\phi \end{pmatrix}. \tag{21}$$

If $\tilde{A}_{I(\phi,\theta)} X \tilde{A}^\dagger_{I(\phi,\theta)} \sim X$ or Y, then $\sin\phi = 0$, which is a contradiction, since $\phi \notin \frac{\pi}{2}\mathbb{Z}$. Hence, $\tilde{A}_{I(\phi,\theta)} X \tilde{A}^\dagger_{I(\phi,\theta)} \sim Z$, which implies that $\cos\phi = 0$. But this also contradicts $\phi \notin \frac{\pi}{2}\mathbb{Z}$. Hence, $\phi \in \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$.

4. Follows from Parts 2 and 3 of Theorem 11. ◀

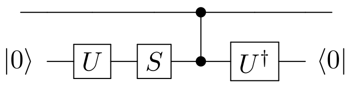
▶ **Theorem 12.** *Let $U = R_z(\phi)R_x(\theta)$. If $\phi \notin \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$, then U-CCCs are* PH*-supreme.*

Proof. By Theorem 11, when $\phi \notin \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$, then $I(\phi,\theta)$ is a unitary non-Clifford U-CCC postselection gadget. Hence, by Lemma 10, U-CCCs are PH-supreme. ◀

3.3.2 Proof of Case (iv): $\theta \notin \frac{\pi}{2}\mathbb{Z}$

Let $U = R_z(\phi)R_x(\theta)$. Consider the following U-CCC postselection gadget:

$J(\phi,\theta) =$ (22)



We now prove some properties about $J(\phi,\theta)$.

▶ **Theorem 13.**

1. *The action of $J(\phi,\theta)$ is*

$$\begin{aligned} A_{J(\phi,\theta)} &= \frac{1}{\sqrt{2}} e^{-i\frac{\pi}{4}} \begin{pmatrix} i+\cos\theta & 0 \\ 0 & 1+i\cos\theta \end{pmatrix} \\ &= \frac{i}{\sqrt{2}} e^{-i\frac{\pi}{4}} \sqrt{1+\cos^2\theta}\; S^\dagger R_z(2\tan^{-1}(\cos\theta)). \end{aligned} \tag{23}$$

2. *$J(\phi,\theta)$ is a unitary gadget for all $\theta,\phi \in [0,2\pi)$. The normalized action is*

$$\tilde{A}_{J(\phi,\theta)} \sim S^\dagger R_z(2\tan^{-1}(\cos\theta)). \tag{24}$$

3. *$J(\phi,\theta)$ is a Clifford gadget if and only if $\theta \in \frac{\pi}{2}\mathbb{Z}$.*
4. *$J(\phi,\theta)$ is a unitary non-Clifford gadget if and only if $\theta \notin \frac{\pi}{2}\mathbb{Z}$.*

Proof.

1. By direct calculation.
2. The determinant of $A_{J(\phi,\theta)}$ is

$$\det A_{J(\phi,\theta)} = \tfrac{1}{2}(1+\cos^2\theta) \neq 0 \tag{25}$$

for all θ and ϕ. Hence, $A_{J(\phi,\theta)} \propto S^\dagger R_z(2\tan^{-1}(\cos\theta))$ for all θ and ϕ, which implies that $J(\phi,\theta)$ is a unitary gadget for all θ and ϕ.

Hence,

$$\tilde{A}_{J(\phi,\theta)} = \frac{A_{J(\phi,\theta)}}{\sqrt{\det A_{J(\phi,\theta)}}} = ie^{-i\frac{\pi}{4}} S^\dagger R_z(2\tan^{-1}(\cos\theta)).$$

3.

$$\begin{aligned} J(\phi,\theta) \text{ is a Clifford gadget} \quad &\Leftrightarrow \quad S^\dagger R_z(2\tan^{-1}(\cos\theta)) \text{ is Clifford} \\ &\Leftrightarrow \quad R_z(2\tan^{-1}(\cos\theta)) \text{ is Clifford} \\ &\Leftrightarrow \quad 2\tan^{-1}(\cos\theta) \in \tfrac{\pi}{2}\mathbb{Z} \qquad \text{by Fact 1} \\ &\Leftrightarrow \quad \cos\theta \in \{0,1,-1\} \\ &\Leftrightarrow \quad \theta \in \tfrac{\pi}{2}\mathbb{Z}. \end{aligned} \tag{26}$$

4. Follows from Parts 2 and 3 of Theorem 13. ◀

▶ **Theorem 14.** *Let $U = R_z(\phi)R_x(\theta)$. If $\theta \notin \frac{\pi}{2}\mathbb{Z}$, then U-CCCs are* PH*-supreme.*

Proof. By Theorem 13, when $\theta \notin \frac{\pi}{2}\mathbb{Z}$, then $I(\phi,\theta)$ is a unitary non-Clifford U-CCC postselection gadget. Hence, by Lemma 10, U-CCCs are PH-supreme. ◀

4 Weak simulation of CCCs with additive error

Here we show how to achieve additive hardness of simulating conjugated Clifford circuits, under additional hardness assumptions. Specifically, we will show that under these assumptions, there is no classical randomized algorithm which given a one-qubit unitary U and a Clifford circuit V, samples the output distribution of V conjugated by U's up to constant ℓ_1 error.

In the following, let V be a Clifford circuit on n qubits, U be a one-qubit unitary which is not a Z-rotation times a Clifford, and $y \in \{0,1\}^n$ be an n-bit string. Define

$$p_{y,U,V} = \left|\langle y|(U^\dagger)^{\otimes n} V U^{\otimes n}|0^n\rangle\right|^2 .$$

In other words $p_{y,U,V}$ is the probability of outputting the string y when applying the circuit V conjugated by U's to the all 0's state, and then measuring in the computational basis. Let the corresponding probability distribution on y's given U and V be denoted $D(U,V)$.

▶ **Theorem 15.** *Assuming that PH is infinite and Conjecture 16, then there is no classical algorithm which given a one-qubit unitary U and an n-qubit Clifford circuit V, outputs a probability distribution which is $1/100$ close to $D(U,V)$ in total variation distance.*

▶ **Conjecture 16.** *For any U which is not equal to a Z-rotation times a Clifford, it is* #P*-hard to approximate a $6/50$ fraction of the $p_{y,U,V}$ over the choice of y, V to within multiplicative error $1/2 + o(1)$.*

In order to prove this we'll actually prove a more general theorem described below; the result will then follow from simply setting $a = c = 1/5$, $\epsilon = 1/100$. One can in general plug in any values they like subject to the constraints; for instance one can strengthen the hardness assumption by assuming computing a smaller fraction of the $p_{y,U,V}$ is still #P-hard to obtain larger allowable error in the simulation. These parameters are similar to those appearing in other hardness conjectures, for example those used for IQP [15].

▶ **Theorem 17.** *Pick constants $0 < \epsilon, a, c < 1$ such that $(1-a)^2/2 - c > 0$ and $\frac{2\epsilon}{ac} < 1$. Then assuming Conjecture 18, given a one-qubit unitary U and an n-qubit Clifford circuit V, one cannot weakly simulate the distribution $D(U,V)$ with a randomized classical algorithm with total variation distance error ϵ, unless the polynomial hierarchy collapses to the third level.*

▶ **Conjecture 18.** *For any U which is not equal to a Z-rotation times a Clifford, it is #P-hard to multiplicatively approximate $(1-a)^2/2 - c$ fraction of the $p_{y,U,V}$ over the choice of (y, V), up to multiplicative error $\frac{2\epsilon}{ac} + o(1)$.*

Proof of Theorem 17. Suppose by way of contradiction that there exists a classical poly-time randomized algorithm which given inputs U, V outputs samples from a distribution $D'(U, V)$ such that $\frac{1}{2}|D(U, V) - D'(U, V)|_1 < \epsilon$. In particular, let $q_{y,U,V}$ be the probability that $D'(U, V)$ outputs y – i.e. the probability that the simulation outputs y under inputs U, V.

By our simulation assumption, for all U, V we have that $\sum_y |q_{y,U,V} - p_{y,U,V}| \leq 2\epsilon$. Therefore by Markov's inequality, given our constant $0 < c < 1$, we have that for all U and V there exists a set $S' \subseteq \{0, 1\}^n$ of output strings y of size $|S'|/2^n > 1 - c$, such that for all $y \in S'$,

$$|q_{y,U,V} - p_{y,U,V}| \leq \frac{2\epsilon}{c2^n}.$$

In particular, by averaging over V's, we see that for any U as above, there exists a set $S \subset \{0, 1\}^n \times \mathcal{C}$ of pairs (y, V) such that for all $(y, V) \in S$, $|q_{y,U,V} - p_{y,U,V}| \leq \frac{2\epsilon}{c2^n}$. Furthermore S has measure at least $(1 - c)$ over a uniformly random choice of (y, V).

We now show the following anticoncentration lemma (similar theorems were shown independently in [29, 39, 31]):

▶ **Lemma 19.** *For any fixed U and y as above, and for any constant $0 < a < 1$, we have that at least $\frac{(1-a)^2}{2}$ fraction of the Clifford circuits V have the property that*

$$p_{y,U,V} \geq \frac{a}{2^n}.$$

We will prove Lemma 19 shortly. First, we will show why this implies Theorem 17. In particular, by averaging Lemma 19 over y's, we see that for any U as above, there exists a set $T \subset \{0, 1\}^n \times \mathcal{C}$ of pairs (y, V) such that for all $(y, V) \in T$, $p_{y,U,V} \geq \frac{a}{2^n}$. Furthermore T has measure at least $\frac{(1-a)^2}{2}$ over a uniformly random choice of (y, V). Since we assumed that $(1 - a)^2/2 + (1 - c) > 1$, then $S \cap T$ must be nonempty, and in particular must contain $(1 - a)^2/2 - c$ fraction of the pairs (y, V). On this set $S \cap T$, we have that

$$q_{y,U,V} \leq p_{y,U,V} + \frac{2\epsilon}{c2^n} = p_{y,U,V} + \frac{2\epsilon}{ac}\frac{a}{2^n} \leq \left(1 + \frac{2\epsilon}{ac}\right) p_{y,U,V},$$

and likewise

$$q_{y,U,V} \geq p_{y,U,V} - \frac{2\epsilon}{c2^n} = p_{y,U,V} - \frac{2\epsilon}{ac}\frac{a}{2^n} \geq \left(1 - \frac{2\epsilon}{ac}\right) p_{y,U,V}.$$

Since $1 - \frac{2\epsilon}{ac} > 0$ (which we guaranteed by assumption), $q_{y,U,V}$ is a multiplicative approximation to $p_{y,U,V}$ with multiplicative error $\frac{2\epsilon}{ac}$ for (y, V) in the set $S \cap T$. The set $S \cap T$ contains at least $(1 - a)^2/2 - c$ fraction of the total pairs (y, V).

On the other hand, by Conjecture 18 we have that computing a $(1 - a)^2/2 - c$ fraction of the $p_{y,U,V}$ to this level of multiplicative error is a #P-hard task. So approximating $p_{y,U,V}$ to this level of multiplicative error for this fraction of outputs is both #P-hard, and achievable by our simulation algorithm. This collapses PH to the third level by known arguments [3, 14]. In particular, by applying Stockmeyer's approximate counting algorithm [55] to $p_{y,U,V}$, one can multiplicatively approximate $q_{y,U,V}$ to multiplicative error $\frac{1}{\mathsf{poly}}$ in $\mathsf{FBPP}^{\mathsf{NP}}$ for those elements in $S \cap T$. But since $q_{y,U,V}$ is a $\frac{2\epsilon}{ac}$-approx to $p_{y,U,V}$, this is a $\frac{2\epsilon}{ac} + o(1)$ multiplicative approximation to $p_{y,U,V}$ in $S \cap T$. Hence a #P-hard quantity is in $\mathsf{FBPP}^{\mathsf{NP}}$. This collapses PH to the third level by Toda's theorem [57].

To complete our proof of Theorem 17, we will prove Lemma 19.

Proof of Lemma 19. To prove this, we will make use of the fact that the Clifford group is an exact 2-design[11] [58, 59]. The fact that the Clifford group is a 2-design means that for any polynomial p over the variables $\{V_{ij}\}$ and their complex conjugates, which is of degree at most 2 in the V_{ij}'s and degree at most 2 in the V_{ij}^*'s, we have that

$$\frac{1}{|C|}\sum_{V \in C} p(V, V^*) = \int p(V, V^*)\mathrm{d}V,$$

where C denotes the Clifford group and the integral $\mathrm{d}V$ is taken over the Haar measure. In other words, the expectation values of low-degree polynomials in the entries of the matrices are exactly identical to the expectation values over the Haar measure.

In particular, note that $p_{y,U,V}$ is a degree-1 polynomial in the entries of V and their complex conjugates, and $p_{y,U,V}^2$ is a degree-2 polynomial in these variables. Therefore, since the Clifford group is an exact 2-design, we have that for any y and U,

$$\frac{1}{|C|}\sum_{V \in \mathcal{C}} p_{y,U,V} = \int p_{y,U,V}\mathrm{d}V = \frac{1}{2^n}$$

and

$$\frac{1}{|C|}\sum_{V \in \mathcal{C}} p_{y,U,V}^2 = \int p_{y,U,V}^2\mathrm{d}V = \frac{2}{2^{2n}-1}\left(1 - \frac{1}{2^n}\right),$$

where the values of these integrals over the Haar measure are well known – see for instance Appendix D of [30].

Following [15], we now invoke the Paley-Zygmund inequality, which states that:

▶ **Fact 20.** *Given a parameter* $0 < a < 1$, *and a non-negative random variable* p *of finite variance, we have*

$$\Pr[p \geq a\mathbb{E}[p]] \geq (1-a)^2\mathbb{E}[p]^2/\mathbb{E}[p^2].$$

Applying this inequality to the random variable $p_{y,U,V}$ over the choice of the Clifford circuit V, we have that

$$\Pr_V\left[p_{y,U,V} \geq \frac{a}{2^n}\right] \geq (1-a)^2\frac{2^{-2n}}{\frac{2-2^{-n+1}}{2^{2n}-1}} = (1-a)^2\frac{1-2^{-2n}}{2-2^{-n+1}} \geq \frac{(1-a)^2}{2}$$

which implies the claim. ◀

This completes the proof of Theorem 17. ◀

[11] The Clifford group is also a 3-design, but we will only need the fact it is a 2-design for our proof.

5 Evidence in favor of hardness conjecture

In Section 4, we saw that by assuming an average case hardness conjecture (namely Conjecture 18), we could show that a weak simulation of CCCs to additive error would collapse the polynomial hierarchy. A natural question is: what evidence do we have that Conjecture 18 is true?

In this section, we show that the worst-case version of Conjecture 18 is true. In fact, we show that for any $U \neq CR_Z(\theta)$ for a Clifford C, there exists a Clifford circuit V and an output y such that computing $p_{y,U,V}$ is #P-hard to constant multiplicative error. Therefore certainly *some* output probabilities of CCCs are #P-hard to compute. Conjecture 18 is merely conjecturing further that computing a large fraction of such output probabilities is just as hard.

▶ **Theorem 21** (Worst-case version of Conjecture 18). *For any U which is not equal to a Z-rotation times a Clifford, there exists a Clifford circuit V and string $y \in \{0,1\}^n$ such that it is #P-hard to multiplicatively approximate a $p_{y,U,V}$ to multiplicative error $1/2 - o(1)$.*

Proof. This follows from combining the ideas from the proof of Lemma 6 with previously known facts about BQP. In particular, we will use the following facts:

1. There exists a uniform family of poly-size BQP[12] circuits C_x where $x \in \{0,1\}^n$ using a gate set with algebraic entries such that computing $|\langle 0^n|C_x|0^n\rangle|^2$ to multiplicative error $1/2$ is #P-hard [15].
2. For any poly-sized quantum circuit C over a gate set with algebraic entries, any non-zero output probability has magnitude at least inverse exponential [35].
3. As shown in the proof of Theorem 7, for any U which is not a Clifford gate times a Z rotation, there is a postselection gadget G which performs a unitary but non-Clifford one-qubit operation. Furthermore all ancilla qubits in G begin in the state $|0\rangle$.

From these facts, we can now prove the theorem. Let $p = |\langle 0^n|C_x|0^n\rangle|^2$. By Fact 2, the circuit C_x from Fact 1 either has $p = 0$ or $p \geq 2^{-O(n^c)}$ for some constant c. Now suppose we compile the circuit C_x from Fact 1 using Clifford gates plus the postselection gadget G – call this new circuit with postselection C_x'. By Sardharwalla *et al.* [51] we can compile this circuit with accuracy $\epsilon = 2^{-O(n^c)-100}$ with only polynomial overhead.

Let $\ell \in \{0,1\}^k$ be the string of postselection bits of the circuit C_x' (which without loss of generality are the last bits of the circuit), and let α is the probability that all postselections succeed. Note α is a known and easily calculated quantity, since each postselection gadget is unitary so succeeds with a known constant probability.

Let $p' = |\langle 0^n \ell|C_x'|0^{n+k}\rangle|^2/\alpha$. Then we have that:

- If $p = 0$ then $p' \leq 2^{-O(n^c)-100}$.
- If $p \neq 0$ then $p - 2^{-O(n^c)-100} \leq p' \leq p + 2^{-O(n^c)-100}$. Since $p \geq 2^{-O(n^c)}$, this is a multiplicative approximation to p with error 2^{-100}.

Now suppose that one can compute $|\langle 0^n \ell|C_x'|0^{n+k}\rangle|^2$ to multiplicative error γ to be chosen shortly. Then immediately one can compute $p' = |\langle 0^n \ell|C_x'|0^{n+k}\rangle|^2/\alpha$ to the same amount of multiplicative error – call this estimate p''. By the above argument, if $p = 0$ then $p'' < 2^{-O(n^c)-100}(1+\gamma)$. On the other hand if $p > 0$ then $p' > 2^{-O(n^c)}$, so $p'' > 2^{-O(n^c)}(1-\gamma)$. So long as γ is chosen such that $2^{-100}(1+\gamma) < (1-\gamma)$ these two cases can be distinguished – which holds in particular if $\gamma \approx 1/2$.

[12] Even IQP suffices here [15].

Therefore, if $p'' < 2^{-O(n^c)}$ then we can infer that $p = 0$. If $p'' > 2^{-O(n^c)}(1-\gamma)$, then $p > 0$ so p'' is a γ approximation to p' and hence a $\gamma + 2^{-100} + \gamma 2^{-100}$ approximation to p. In either case we have computed a $\gamma + 2^{-100} + \gamma 2^{-100}$ approximation to p. Therefore, if $\gamma = 1/2 - 2^{-99}$, then we have computed a $1/2$-multiplicative approximation to p, which is #P-hard by Fact 1. Therefore, computing some the probability that the CCC correspoding to C'_x outputs $|0^n\ell\rangle$ to multiplicative error $1/2 - 2^{-99}$ is #P-hard. One can similarly improve this hardness to $1/2 - o(1)$. ◀

Given that the worst-case version of Conjecture 18 is true, a natural question to ask is how difficult it would be to prove the average-case conjecture. To do so would in particular prove quantum advantage over classical computation with realistic error, and merely assuming the polynomial hierarchy is infinite. In some ways this would be stronger evidence for quantum advantage over classical computation than Shor's factoring algorithm, as there are no known negative complexity-theoretic consequences if factoring is contained in P.

Unfortunately, recent work has shown that proving Conjecture 18 would be a difficult task. Specifically, Aaronson and Chen [4] demonstrated an oracle relative to which PH is infinite, but classical computers can efficiently weakly simulate quantum devices to constant additive error. Therefore, any proof which establishes quantum advantage with additive error under the assumption that PH is infinite must be non-relativizing. In particular this implies any proof of Conjecture 18 would require non-relativizing techniques – in other words it could not remain true if one allows for classical oracle class in the circuit. This same barrier holds for proving the similar average-case hardness conjectures to show advantage for Boson Sampling, IQP, DQC1, or Fourier sampling. Therefore any proof of Conjecture 18 would require facts specific to the Clifford group. We leave this as an open problem. We also note that it remains open to prove the average-case *exact* version of Conjecture 18 - i.e. whether it is hard to exactly compute a large fraction of $p_{y,U,C}$. We believe this may be a more tractable problem to approach than Conjecture 18. However this remains open, as is the analogous average-case exact conjecture corresponding to IQP. We note the corresponding average-case exact conjecture for Boson Sampling and Fourier sampling are known to be true [3, 22], though these models are not known to anticoncentrate.

6 Summary of simulability of CCCs

For completeness, in this section we summarize the simulability of U-CCCs when U is not a Clifford rotation times a Z rotation. There are various notions of classical simulation at play here. The results of this paper so far have focused of notions of approximate *weak* simulation. A *weak* simulation of a family of quantum circuits is a classical randomized algorithm that samples from the same distribution as the output distribution of the circuit. On the other hand, a *strong* simulation of a family of quantum circuits is a classical algorithm that computes not only the joint probabilities, but also any marginal probabilities of the outcomes of the measurements in the circuit. Following [34], we can further refine these definitions according to the number of qubits being measured: a strong(1) simulation computes the marginal output probabilities on individual qubits, and a strong(n) simulation computes the probability of output strings $y \in \{0,1\}^n$. Similarly, a weak(1) simulation samples from the marginal output probabilities on individual qubits, and a weak(n) simulation samples from $p(y_1, \dots, y_n)$. A weak$^+$ simulation samples from the same distribution on all n output qubits up to constant additive error. Our previous results have shown that efficient weak(n) simulations (Theorem 7), weak$^+$ simulations (Theorem 17), and strong(n) simulations (Theorem 21) of CCCs are implausible. However it is natural to ask if it is possible to simulate single output probabilities

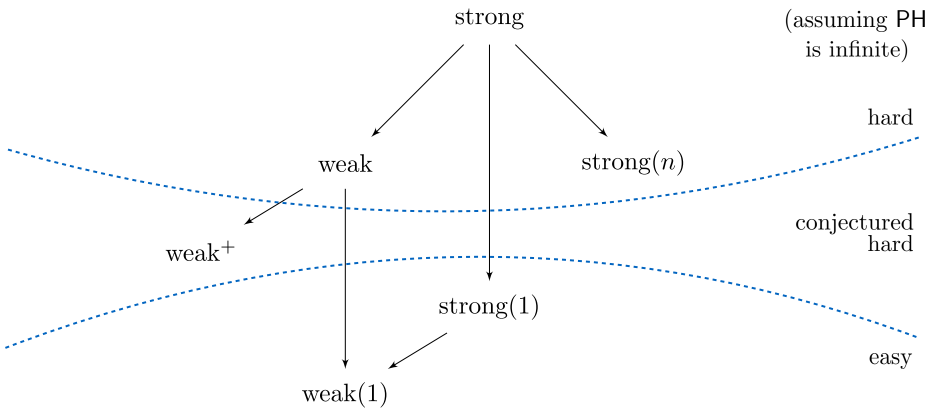


Figure 1 Relationships between different notions of classical simulation and summary of the hardness of simulating CCCs. An arrow from A to B ($A \to B$) means that an efficient A-simulation of a computational task implies that there is an efficient B-simulation for the same task. Note also that an weak(n) simulation exists if and only if a weak simulation exists. For a proof of these relationships, see [34]. The two curves indicate the boundary between efficiencies of simulation of U-CCCs, where U is not a Clifford operation times a Z rotation. "Hard" means that an efficient simulation of U-CCCs is not possible, unless PH collapses. "Conjectured hard" means that an efficient simulation of U-CCCs is not possible, if we assume Conjecture 18. "Easy" means that an efficient simulation of U-CCCs exists. Note that when U is a Clifford operation times a Z rotation, all the above notions become easy.

of CCCs. It turns out the answer to this question is yes. This follows immediately from Theorem 5 of [34], which showed more generally that Clifford circuits with product inputs or measurements have an efficient strong(1) and weak(1) simulation. Therefore this completes the complexity classification of the simulability of such circuits. We note that IQP has identical properties in this regard. This emphasizes that the difficulty in simulating CCCs (or IQP circuits) comes from the difficulty of simulating all of the *marginal* probability distributions contained in the output distribution, where the marginal is taken over a large number of output bits. The probabilities of computing individual output bits of either model are easy for classical computation. This is summarized in Figure 1.

7 Open Problems

Our work leaves open a number of problems.

- What is the computational complexity of commuting CCCs? In other words, can the gate set CZ, S conjugated by a one-qubit gate U ever give rise to quantum advantage? Note that this does not follow from Bremner, Jozsa and Shepherd's results [14], as their hardness proof uses the gate set CZ, T or CCZ, CZ, Z conjugated by one-qubit gates. If this is true, it would say that the "intersection" of CCCs and IQP remains computationally hard. One can also consider the computational power of arbitrary fragments of the Clifford group, which were classified in [27]. Perhaps by studying such fragments of the Clifford group one could achieve hardness with lower depth circuits (see additional question below).

- We showed that Clifford circuits conjugated by tensor-product unitaries are difficult to simulate classically. A natural extension of this question is: suppose your gate set consists of all two-qubit Clifford gates, conjugated by a unitary U which is *not* a tensor product of the same one-qubit gate. Can one show that all such circuits are difficult to simulate classically (say exactly)? Such a theorem could be a useful step towards classifying the power of all two-qubit gate sets.
- Generic Clifford circuits have a depth which is linear in the number of qubits [5]. In particular the lowest-depth decomposition for a generic Clifford circuit over n qubits to date has depth $14n - 4$ [41]. Such depth will be difficult to achieve in near-term quantum devices without error-correction. As a result, others have considered quantum supremacy experiments with lower-depth circuits. For instance, Bremner, Shepherd and Montanaro showed advantage for a restricted version of IQP circuits with depth $O(\log n)$ [16] with long-range gates (which becomes depth $O(n^{1/2} \log n)$ if one uses SWAP gates to simulate long-range gates using local operations on a square lattice). We leave open the problem of determining if quantum advantage can be achieved with CCCs of lower depth (say $O(n^{1/2})$ or $O(n^{1/3})$) with local gates only.
- In order to establish quantum supremacy for CCCs, we conjectured that it is #P-hard to approximate a large fraction of the output probabilities of randomly chosen CCCs (Conjecture 18). Is it also #P-hard to exactly compute that large of a fraction of the output probabilities? This is a necessary but not sufficient condition for Conjecture 18 to be true, and we believe it may be a more approachable problem.

References

1 Universal sets of gates for SU(3)?, 2012. Accessed: 2017-08-01. URL: https://cstheory.stackexchange.com/questions/11308/universal-sets-of-gates-for-su3.

2 Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 461, pages 3473–3482. The Royal Society, 2005.

3 Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the forty-third annual ACM Symposium on Theory of Computing*, pages 333–342. ACM, 2011.

4 Scott Aaronson and Lijie Chen. Complexity-theoretic foundations of quantum supremacy experiments. *Proc. CCC*, 2017.

5 Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70(5):052328, 2004.

6 Scott Aaronson, Daniel Grier, and Luke Schaeffer. The classification of reversible bit operations. In *Proceedings of Innovations in Theoretical Computer Science (ITCS)*, 2017.

7 Dorit Aharonov and Michael Ben-Or. Fault-tolerant quantum computation with constant error. In *Proceedings of the twenty-ninth annual ACM Symposium on Theory of Computing*, pages 176–188. ACM, 1997.

8 Sergio Boixo, Sergei V Isakov, Vadim N Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, John M Martinis, and Hartmut Neven. Characterizing quantum supremacy in near-term devices. *arXiv:1608.00263*, 2016.

9 Adam Bouland and Scott Aaronson. Generation of universal linear optics by any beam splitter. *Physical Review A*, 89(6):062316, 2014.

10 Adam Bouland, Laura Mancinska, and Xue Zhang. Complexity classification of two-qubit commuting hamiltonians. In Ran Raz, editor, *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, volume 50 of *LIPIcs*, pages 28:1–

28:33. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016. doi:10.4230/LIPIcs.CCC.2016.28.

11 Sergey Bravyi, David Gosset, and Robert Koenig. Quantum advantage with shallow circuits. *arXiv:1704.00690*, 2017.

12 Sergey Bravyi and Jeongwan Haah. Magic-state distillation with low overhead. *Physical Review A*, 86(5):052329, 2012.

13 Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Physical Review A*, 71(2):022316, 2005.

14 Michael J Bremner, Richard Jozsa, and Dan J Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, page rspa20100301. The Royal Society, 2010.

15 Michael J Bremner, Ashley Montanaro, and Dan J Shepherd. Average-case complexity versus approximate simulation of commuting quantum computations. *Physical Review Letters*, 117(8):080501, 2016.

16 Michael J Bremner, Ashley Montanaro, and Dan J Shepherd. Achieving quantum supremacy with sparse and noisy commuting quantum computations. *Quantum*, 1, 2017.

17 Hans J Briegel, David E Browne, W Dür, Robert Raussendorf, and Maarten Van den Nest. Measurement-based quantum computation. *Nature Physics*, 5(1):19–26, 2009.

18 Christopher M Dawson and Michael A Nielsen. The Solovay-Kitaev algorithm. *Quantum Information & Computation*, 6(1):81–95, 2006.

19 David P. DiVincenzo and Peter W. Shor. Fault-tolerant error correction with efficient quantum codes. *Phys. Rev. Lett.*, 77:3260–3263, Oct 1996. doi:10.1103/PhysRevLett.77.3260.

20 Bryan Eastin and Emanuel Knill. Restrictions on transversal encoded quantum gate sets. *Physical Review Letters*, 102(11):110502, 2009.

21 Edward Farhi and Aram W Harrow. Quantum supremacy through the quantum approximate optimization algorithm. *arXiv:1602.07674*, 2016.

22 Bill Fefferman and Christopher Umans. On the power of quantum fourier sampling. In Anne Broadbent, editor, *11th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2016, September 27-29, 2016, Berlin, Germany*, volume 61 of *LIPIcs*, pages 1:1–1:19. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016. doi:10.4230/LIPIcs.TQC.2016.1.

23 Keisuke Fujii, Hirotada Kobayashi, Tomoyuki Morimae, Harumichi Nishimura, Shuhei Tamate, and Seiichiro Tani. Impossibility of classically simulating one-clean-qubit computation. *arXiv:1409.6777*, 2014.

24 Daniel Gottesman. Stabilizer codes and quantum error correction. *Ph.D. Thesis, California Institute of Technology, arXiv:quant-ph/9705052*, 1997.

25 Daniel Gottesman. The Heisenberg representation of quantum computers. *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, pages 32–43, 1999.

26 Chris Granade and Ben Criger. QuaEC: Quantum error correction analysis in Python. http://www.cgranade.com/python-quaec/groups.html#, 2012. Accessed: 2017-06-01.

27 Daniel Grier and Luke Schaeffer. The classification of stabilizer operations over qubits. *arXiv:1603.03999*, 2016.

28 Amihay Hanany and Yang-Hui He. A monograph on the classification of the discrete subgroups of SU(4). *Journal of High Energy Physics*, 2001(02):027, 2001.

29 Dominik Hangleiter, Juan Bermejo-Vega, Martin Schwarz, and Jens Eisert. Anticoncentration theorems for schemes showing a quantum computational supremacy. *arXiv:1706.03786*, 2017.

30 Daniel Harlow. Jerusalem lectures on black holes and quantum information. *Reviews of Modern Physics*, 88(1):015002, 2016.

31 Aram Harrow and Saeed Mehraban. Personal communication. 2018.

32 Richard Jozsa and Akimasa Miyake. Matchgates and classical simulation of quantum circuits. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 464, pages 3089–3106. The Royal Society, 2008.

33 Richard Jozsa and Maarten Van den Nest. Classical simulation complexity of extended Clifford circuits. *Quantum Information and Computation*, 14(7/8):633–648, 2014.

34 Dax Enshan Koh. Further extensions of Clifford circuits and their classical simulation complexities. *Quantum Information & Computation*, 17(3&4):0262–0282, 2017.

35 Greg Kuperberg. How hard is it to approximate the Jones polynomial? *Theory of Computing*, 11(6):183–219, 2015.

36 Richard E. Ladner. On the structure of polynomial time reducibility. *J. ACM*, 22(1):155–171, 1975.

37 Raymond Laflamme, Cesar Miquel, Juan Pablo Paz, and Wojciech Hubert Zurek. Perfect quantum error correcting code. *Physical Review Letters*, 77(1):198, 1996.

38 Easwar Magesan, Jay M Gambetta, and Joseph Emerson. Scalable and robust randomized benchmarking of quantum processes. *Physical Review Letters*, 106(18):180504, 2011.

39 Ryan L. Mann and Michael J. Bremner. On the complexity of random quantum computations and the Jones polynomial. *arXiv:1711.00686*, 2017.

40 Enrique Martin-Lopez, Anthony Laing, Thomas Lawson, Roberto Alvarez, Xiao-Qi Zhou, and Jeremy L O'Brien. Experimental realization of shor's quantum factoring algorithm using qubit recycling. *Nature Photonics*, 6(11):773–776, 2012.

41 Dmitri Maslov and Martin Roetteler. Shorter stabilizer circuits via Bruhat decomposition and quantum circuit transformations. *arXiv:1705.09176*, 2017.

42 Tomoyuki Morimae. Hardness of classically sampling one clean qubit model with constant total variation distance error. *arXiv:1704.03640*, 2017.

43 Tomoyuki Morimae, Keisuke Fujii, and Joseph F Fitzsimons. Hardness of classically simulating the one-clean-qubit model. *Physical Review Letters*, 112(13):130502, 2014.

44 Gabriele Nebe, Eric M Rains, and Neil JA Sloane. The invariants of the clifford groups. *Designs, Codes and Cryptography*, 24(1):99–122, 2001.

45 Gabriele Nebe, Eric M Rains, and Neil James Alexander Sloane. *Self-dual codes and invariant theory*, volume 17. Springer, 2006.

46 Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

47 Michał Oszmaniec and Zoltán Zimborás. Universal extensions of restricted classes of quantum operations. *arXiv:1705.11188*, 2017.

48 John Preskill. Quantum computing and the entanglement frontier. *arXiv:1203.5813*, 2012.

49 Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001.

50 Robert Raussendorf, Daniel E Browne, and Hans J Briegel. Measurement-based quantum computation on cluster states. *Physical Review A*, 68(2):022312, 2003.

51 Imdad SB Sardharwalla, Toby S Cubitt, Aram W Harrow, and Noah Linden. Universal refocusing of systematic quantum noise. *arXiv:1602.07963*, 2016.

52 Adam Sawicki and Katarzyna Karnas. Criteria for universality of quantum gates. *Phys. Rev. A*, 95:062303, Jun 2017.

53 Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

54 Andrew Steane. Multiple-particle interference and quantum error correction. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 452, pages 2551–2577. The Royal Society, 1996.

55 Larry Stockmeyer. The complexity of approximate counting. In *Proceedings of the fifteenth annual ACM Symposium on Theory of Computing*, pages 118–126. ACM, 1983.

56 Barbara M Terhal and David P DiVincenzo. Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games. *Quantum Information & Computation*, 4(2):134–145, 2004.

57 Seinosuke Toda. PP is as hard as the polynomial-time hierarchy. *SIAM J. Comput.*, 20(5):865–877, 1991. doi:10.1137/0220053.

58 Zak Webb. The Clifford group forms a unitary 3-design. *Quantum Information and Computation*, 16:1379–1400, 2016.

59 Huangjun Zhu. Multiqubit clifford groups are unitary 3-designs. *Physical Review A*, 96(6):062336, 2017.