# A CRITERION FOR QUANTUM ADVANTAGE

CHAITANYA KARAMCHEDU[†], MATTHEW FOX[†], AND DANIEL GOTTESMAN

Abstract. Assuming the polynomial hierarchy is infinite, we prove a sufficient condition for determining if uniform and polynomial size quantum circuits over a non-universal gate set are not efficiently classically simulable in the weak multiplicative sense. Our criterion exploits the fact that subgroups of $\mathrm{SL}(2;\mathbb{C})$ are essentially either discrete or dense in $\mathrm{SL}(2;\mathbb{C})$. Using our criterion, we give a new proof that both instantaneous quantum polynomial (IQP) circuits and conjugated Clifford circuits (CCCs) afford a quantum advantage. We also prove that both commuting CCCs and CCCs over various fragments of the Clifford group afford a quantum advantage, which settles two questions of Bouland, Fitzsimons, and Koh. Our results imply that circuits over just $(U^\dagger \otimes U^\dagger)\mathrm{CZ}(U \otimes U)$ afford a quantum advantage for almost all $U \in \mathrm{U}(2)$.

## 1. Introduction

Quantum computers promise to outperform classical computers in certain computational tasks, such as simulating quantum systems [Fey81] or solving abelian hidden subgroup problems like factoring integers [CvD10, Sho99]. In computational complexity, this promise is largely encapsulated in the difficult conjecture that $\mathsf{BPP} \neq \mathsf{BQP}$ [AB09, NC11]. However, experimentally implementing most quantum algorithms, especially those that decide suspected $\mathsf{BQP}\backslash\mathsf{BPP}$ languages, is very difficult. For example, the largest number ever factored using Shor's algorithm is 21, and this occurred over a decade ago [MLLL$^+$12].

Given both the theoretical challenges in formally proving a quantum advantage, as well as the experimental challenges in practically realizing fault-tolerant universal quantum computation, there is considerable interest in "restricted models" of quantum computation. These are models of quantum computation that are non-universal by design, but which are nevertheless able to perform computational tasks that no efficient classical computer can, at least under standard complexity assumptions.

Notable examples of restricted models include: non-adaptive linear optics [AA11], constant-depth quantum circuits [TD04, BGK18], instantaneous quantum polynomial (IQP) circuits [BJS11], conjugated Clifford circuits (CCCs) [BFK18], and quantum circuits with one clean qubit [KL98, FKM$^+$18]. Interestingly, under the standard complexity assumption that the polynomial hierarchy is infinite [AB09], all of these restricted models can perform *sampling* tasks that no efficient classical computer can, and this is despite the fact, but in no way in contradiction to it, that some of these restricted models can probably not solve *decision* tasks outside of $\mathsf{BPP}$.

From a theoretical perspective, restricted models are interesting because they seem to straddle the purported boundary between $\mathsf{BPP}$ and $\mathsf{BQP}$, analogous to how $\mathsf{NP}$-intermediate problems straddle the purported boundary between $\mathsf{P}$ and $\mathsf{NP}$ [Lad75]. A deeper understanding of the computational complexity of restricted models, therefore, might inform the relationship between $\mathsf{BPP}$ and $\mathsf{BQP}$.

From an experimental perspective, restricted models are particularly useful because they make the task of demonstrating a quantum advantage distinct from realizing a universal quantum computer. This follows because many restricted models that can perform "hard" sampling

[†] These authors contributed equally.

tasks are substantially easier to implement fault-tolerantly than a full-blown universal quantum computer [AA11].

There are many ways to formulate a restricted model, but arguably the most straightforward is to consider quantum circuits over a *non*-universal gate set $\mathcal{S}$, such as

$$\mathcal{S}_{\text{IQP}} := \big\{HTH, (H \otimes H)\text{CZ}(H \otimes H)\big\},$$

which underlies a subset of IQP circuits, and, for any single-qubit unitary $U$,

$$\mathcal{S}_{\text{CCC}}(U) := \big\{U^\dagger HU, U^\dagger SU, (U^\dagger \otimes U^\dagger)\text{CNOT}(U \otimes U)\big\},$$

which underlies all $U$-CCCs.

Non-universal gate sets are interesting for a number of reasons. On one hand, they are "rare" in the measure-theoretic sense that almost every set of qudit gates is universal [Llo95]. On the other hand, non-universal gate sets are somewhat easy to contrive (particularly in the context of $U$-CCCs where the conjugating $U$ can be any single-qubit unitary) and while it is possible to decide if a gate set is universal [Iva06], doing so is generally difficult [SK17]. What is especially interesting, though, is that for many non-universal gate sets $\mathcal{S}$, there is a *post-selected* circuit over $\mathcal{S}$ that can decide a $\mathsf{PP}$-complete language. By a standard complexity argument that is detailed in our Proposition 3.1, this implies that the original, *non*-post-selected circuit over $\mathcal{S}$ can perform a sampling task that no efficient classical computer can, unless the polynomial hierarchy collapses. Given this, we ask: under standard complexity assumptions, is there a simple "catch all" (or at the very least a "catch many") criterion for understanding when post-selected circuits over a non-universal gate set can decide a $\mathsf{PP}$-complete language?

In this paper, we answer this question in the affirmative by exhibiting an elementary algorithm that does just this. Our techniques exploit the fact that the subgroups of $\text{SL}(2;\mathbb{C})$ are stringently constrained. In particular, we show that for any non-universal gate set $\mathcal{S}$, if a finite collection $\Gamma$ of invertible, single-qubit, post-selection gadgets over $\mathcal{S}$ generates a group $\langle\Gamma\rangle$, then $\langle\Gamma\rangle$ is essentially either discrete or dense in a closed subgroup of $\text{SL}(2;\mathbb{C})$. Thus, roughly speaking, if $\langle\Gamma\rangle$ is *non*-discrete, then when augmented with post-selection, circuits over $\mathcal{S}$ can simulate a universal gate set and therefore simulate any *universal* quantum computer. Consequently, to determine if post-selected circuits over $\mathcal{S}$ can decide a $\mathsf{PP}$-complete language, it more or less suffices to determine if $\langle\Gamma\rangle$ is discrete or not. Modulo several group-theoretic details, this is all that our algorithm does.

Using our criterion, we answer two questions raised by Bouland et al. in [BFK18] by proving that efficient classical computers can neither simulate *commuting* conjugated Clifford circuits, which are in some sense the "intersection" of CCCs and IQP circuits, nor can they simulate CCCs when the interstitial Clifford circuit is restricted to one of several "fragments" of the Clifford group (as classified in [GS22]), such as Clifford circuits made entirely of $Z$ and CZ gates, or even just CZ gates. We remark that the topological idea of finding sufficient conditions for $\Gamma$ to generate a dense subgroup of $\text{SL}(2;\mathbb{C})$ (as opposed to, say, $\text{SU}(2)$) was inspired by the techniques in [AAEL07] and [BMZ16].

This paper is structured as follows. In Section 2, we review several standard notions such as efficient classical and quantum computers, as well as their post-selected counterparts. There, we also introduce most of our notation and central definitions. In Section 3, we state and prove our criterion for quantum advantage. In Section 4, we introduce several results to do with the group theory of $\text{SL}(2;\mathbb{C})$, which together afford a practical algorithm that implements our criterion. In Section 5, we demonstrate the utility of our criterion by proving that IQP circuits, CCCs, commuting CCCs, and CCCs over several fragments of the Clifford group can all perform a sampling task that no efficient classical computer can, unless the polynomial hierarchy collapses. Finally, in Section 6, we discuss several open questions, some of which serve as a means of improving our criterion.

## 2. Preliminaries

In this paper, $\{0,1\}^n$ is the set of all (binary) strings with length $n$, $\{0,1\}^*$ is the set of all strings with finite length, $x_i$ is the $i$th bit of the string $x$, $x.y$ is the concatenation of the strings $x$ and $y$, $x_{[k\,:\,\ell]}$ is the substring $x_k \dots x_\ell$ of the string $x$, $[k]$ is the set $\{1, 2, \dots, k\}$, $\mathbb{N}$ is the set of positive integers, $\mathbb{Z}$ is the set of integers, $\mathbb{R}$ is the set of real numbers, $(a, b)$ is the open interval $\{x \in \mathbb{R} \mid a < x < b\}$, $[a, b]$ is the closed interval $\{x \in \mathbb{R} \mid a \leq x \leq b\}$, $\mathbb{C}$ is the set of complex numbers, $\langle \Gamma \rangle$ is the group generated by a set $\Gamma$ (where it is implicitly assumed that $\Gamma$ is closed under inverses), $I_k$ is the $2^k \times 2^k$ identity matrix, and $\Sigma_k\mathsf{P}$ is the $k$th level of the polynomial hierarchy, $\mathsf{PH}$. All other notation is defined along the way, except for standard complexity classes like $\mathsf{P}$ and $\mathsf{PP}$ and standard Lie groups like $\mathrm{SO}(n)$ and $\mathrm{SL}(n; \mathbb{C})$. Finally, every topological statement like "such-and-such is dense in $\mathrm{SL}(2; \mathbb{C})$" is meant with respect to the operator norm topology on $\mathrm{SL}(2; \mathbb{C})$.

### 2.1. Notions of Simulation.

Let $\mathbf{A}$ and $\mathbf{B}$ be classical or quantum algorithms that, for all $n \in \mathbb{N}$, output $y \in \{0,1\}^{f(n)}$ on input $x \in \{0,1\}^n$ with probabilities $\Pr[\mathbf{A}(x) = y]$ and $\Pr[\mathbf{B}(x) = y]$, respectively. Here, $f : \mathbb{N} \to \mathbb{N}$ characterizes the length of the strings that $\mathbf{A}$ and $\mathbf{B}$ output on a given input size.

We begin by defining a particular type of simulation, known as a *weak multiplicative simulation*, where the word "weak" refers to the fact that the simulation of $\mathbf{B}$ by $\mathbf{A}$ is only required to simulate the output distribution of $\mathbf{B}$ on a given input, as opposed to a much stronger notion where $\mathbf{A}$ is required to output the probability that $\mathbf{B}$ outputs a particular string on a given input.

**Definition 2.1.** We say $\mathbf{A}$ *simulates* $\mathbf{B}$ *to within multiplicative error* $\epsilon \geq 0$ if and only if (iff) for all $n \in \mathbb{N}$, all $x \in \{0,1\}^n$, and all $y \in \{0,1\}^{f(n)}$,

$$\frac{1}{1+\epsilon}\Pr[\mathbf{B}(x) = y] \leq \Pr[\mathbf{A}(x) = y] \leq (1+\epsilon)\Pr[\mathbf{B}(x) = y].$$

In other words, $\mathbf{A}$ simulates $\mathbf{B}$ to within multiplicative error $\epsilon$ iff on every valuation (and hence in the worst case), $\mathbf{A}$ samples the output distribution of $\mathbf{B}$ to within $\epsilon$. While this is the notion of simulation we employ in this paper, we admit that it is rather restrictive. For example, if $\mathbf{B}$ has two likely events with probability $1/2 - 1/2^n$ and two unlikely events with probability $1/2^n$, insisting that $\mathbf{A}$ simulates $\mathbf{B}$ to within small multiplicative error means $\mathbf{A}$ must approximate the two unlikely events essentially just as well as it approximates the two likely events. However, it should be difficult to actually differentiate between the correct distribution underlying $\mathbf{B}$ and the distribution where the two likely events have probability $1/2$ each.

Incidentally, from an experimental perspective, a better notion of simulation is that of a *weak additive simulation.* In this case, it is merely required that *on the average* (as opposed to on every valuation) $\mathbf{A}$ samples the output distribution of $\mathbf{B}$ to within some error $\epsilon$. This notion is better experimentally because the threshold theorem for quantum fault tolerance only guarantees the robustness of quantum computation up to *additive* error between the target and actualized output distributions [AB97].

Evidently, if $\mathbf{A}$ simulates $\mathbf{B}$ to within multiplicative error $\epsilon$, then $\mathbf{A}$ simulates $\mathbf{B}$ to within additive error $\epsilon$ as well. However, the converse is not generally true because $\mathbf{A}$ can sample the output distribution of $\mathbf{B}$ to within error $\epsilon$ *on the average* but not on every valuation [NLD$^+$22]. Nevertheless, if $\epsilon = 0$, then $\Pr[\mathbf{A}(x) = y] = \Pr[\mathbf{B}(x) = y]$ for all $n \in \mathbb{N}$, all $x \in \{0,1\}^n$, and all $y \in \{0,1\}^{f(n)}$. In this case, the weak additive and multiplicative senses entail the same thing, so we say that $\mathbf{A}$ *exactly simulates* $\mathbf{B}$

We now discuss a variety of algorithmic models, starting with efficient classical computers.

2.2. **Classical Computers.** On account of the extended Church-Turing thesis [AB09], an *efficient classical computer* $\mathbf{C}$ is a probabilistic and polynomial time Turing machine. For every $\mathbf{C}$, there is a polynomial $f_{\mathbf{C}} : \mathbb{N} \to \mathbb{N}$ that specifies the *output size of* $\mathbf{C}$, i.e., the length of the output strings of $\mathbf{C}$ on a given input size. For all $n \in \mathbb{N}$, the probability $\mathbf{C}$ outputs $y \in \{0,1\}^{f_{\mathbf{C}}(n)}$ on input $x \in \{0,1\}^n$ is $\Pr[\mathbf{C}(x) = y]$, where the probability is over the internal randomness of $\mathbf{C}$.

2.3. **Post-Selected Classical Computers.** We now define the notion of an "efficient post-selected classical computer".

**Definition 2.2.** An *efficient post-selected classical computer* $\mathbf{C}_{\text{post}}$ is a tuple $(\mathbf{C}, \text{post})$, where $\mathbf{C}$ is an efficient classical computer and $\text{post} : \mathbb{N} \to \{0,1\}^*$ is a total and polynomial time computable function that specifies a post-selection string on a given input size. For all $n \in \mathbb{N}$ and all $x \in \{0,1\}^n$, $\mathbf{C}$ and post satisfy $f_{\mathbf{C}_{\text{post}}}(n) \coloneqq f_{\mathbf{C}}(n) - |\text{post}(n)| > 0$ and

$$\Pr\big[\mathbf{C}(x)_{[f_{\mathbf{C}_{\text{post}}}(n)+1\,:\,f_{\mathbf{C}}(n)]} = \text{post}(n)\big] = \sum_{z \in \{0,1\}^{f_{\mathbf{C}_{\text{post}}}(n)}} \Pr\left[\mathbf{C}(x) = z.\text{post}(n)\right] \neq 0.$$

The former condition ensures that the *output size of* $\mathbf{C}_{\text{post}}$*,* $f_{\mathbf{C}_{\text{post}}}$*,* is always positive, and the latter condition ensures that the probability that $\mathbf{C}$ outputs a string whose last $|\text{post}(n)|$ bits equal $\text{post}(n)$ is nonzero. This way, for all $n \in \mathbb{N}$, the probability $\mathbf{C}_{\text{post}}$ outputs $y \in \{0,1\}^{f_{\mathbf{C}_{\text{post}}}(n)}$ on input $x \in \{0,1\}^n$ is well-defined:

$$\begin{aligned}\Pr\left[\mathbf{C}_{\text{post}}(x) = y\right] &\coloneqq \Pr\big[\mathbf{C}(x)_{[1\,:\,f_{\mathbf{C}_{\text{post}}}(n)]} = y \mid \mathbf{C}(x)_{[f_{\mathbf{C}_{\text{post}}}(n)+1\,:\,f_{\mathbf{C}}(n)]} = \text{post}(n)\big] \\ &= \frac{\Pr\left[\mathbf{C}(x) = y.\text{post}(n)\right]}{\Pr\big[\mathbf{C}(x)_{[f_{\mathbf{C}_{\text{post}}}(n)+1\,:\,f_{\mathbf{C}}(n)]} = \text{post}(n)\big]}.\end{aligned}$$

Notice, this is the conditional probability that the first $f_{\mathbf{C}_{\text{post}}}(n)$ bits of $\mathbf{C}(x)$ equal $y$, given that the last $|\text{post}(n)|$ bits of $\mathbf{C}(x)$ equal $\text{post}(n)$.

The set of languages that efficient post-selected classical computers can decide is often called $\mathsf{PostBPP}$ [BJS11], but this class is also known as $\mathsf{BPP}_{\text{path}}$ [HHT97].

**Definition 2.3.** The class $\mathsf{PostBPP}$ consists of all languages $L$ for which there is an efficient post-selected classical computer $\mathbf{C}_{\text{post}}$ and $\delta \in (0, 1/2)$ such that for all $x \in \{0,1\}^*$, $\Pr[\mathbf{C}_{\text{post}}(x)_1 = L(x)] \geq 1/2 + \delta$, where $L(\cdot)$ is the indicator function of $L$.

Crucially, $\mathsf{PostBPP}$ is actually independent of $\delta$ because efficient post-selected classical computers can compute the majority function, and hence they can amplify the acceptance probabilities [BJS11]. This implies that if $L \in \mathsf{PostBPP}$, then *for all* $\delta \in (0, 1/2)$, there is an efficient post-selected classical computer $\mathbf{C}_{\text{post}}$ that decides $L$ to within bounded error $1/2 + \delta$.

2.4. **Quantum Computers.** We now recall several notions to do with the quantum circuit model.

**Definition 2.4.** A *gate set* $\mathcal{S}$ is a finite subset of $\bigcup_{\ell \in [k]} \mathrm{U}(2^\ell)$ for some fixed $k > 1$ that contains at least one entangling gate.[1] We say $\mathcal{S}$ is *universal* iff there exists $\ell \in [k]$ for which $\langle \mathcal{S} \cap \mathrm{U}(2^\ell) \rangle$ is dense in $\mathrm{U}(2^\ell)$.[2] Otherwise, $\mathcal{S}$ is *non-universal.*

[1] If $\mathcal{S}$ does not contain an entangling gate, then uniform and polynomial size circuits over $\mathcal{S}$ with pure state inputs are efficiently classically simulable, so there is no hope for a quantum advantage [JL03].

[2] Interestingly, for a gate set $\mathcal{S}$ to be universal, it need not be closed under inverses due to the *inverse free* Solovay-Kitaev theorem [BG21].

Note, whenever we say “gate set” in this paper, we implicitly mean a “not necessarily universal gate set”.

Given a gate set, one can build circuits over it.

**Definition 2.5.** An *$n$-qubit quantum circuit $Q_n$ over a gate set $\mathcal{S}$* is an operator in $\mathrm{U}(2^n)$ that admits the product decomposition

$$Q_n = U_{d_n} \dots U_1.$$

Here, each $U_1, \dots, U_{d_n} \in \mathrm{U}(2^n)$ is a tensor product of operators in $\mathcal{S} \cup \{I_1\}$. The total number of operators in $\mathcal{S}$ that make up $Q_n$ is the *size of* $Q_n$ and $d_n$ is the *depth of* $Q_n$.

We now define what we mean by an “efficient quantum computer”.

**Definition 2.6.** An *efficient quantum computer* $\mathbf{Q}$ *over a gate set* $\mathcal{S}$ is a triple $(Q, \mathcal{S}, \mathrm{anc})$, where $\mathrm{anc} : \mathbb{N} \to \{0,1\}^*$ is a total and polynomial time computable function whose purpose is to specify an ancilla string on a given input size and $Q = (Q_n)_{n\in\mathbb{N}}$ is a uniform family of polynomial size, $(n + |\mathrm{anc}(n)|)$-qubit quantum circuits $Q_n$ over $\mathcal{S}$. For all $n \in \mathbb{N}$, the *output size of* $\mathbf{Q}$ is the polynomial $f_{\mathbf{Q}}(n) \coloneqq n + |\mathrm{anc}(n)|$ and the probability that $\mathbf{Q}$ outputs $y \in \{0,1\}^{f_{\mathbf{Q}}(n)}$ on input $x \in \{0,1\}^n$ is $\Pr[\mathbf{Q}(x) = y] \coloneqq |\langle y| Q_n |x\rangle \otimes |\mathrm{anc}(n)\rangle|^2$.

2.5. **Post-Selected Quantum Computers.** We now introduce the notion of an “efficient post-selected quantum computer”.

**Definition 2.7.** An *efficient post-selected quantum computer* $\mathbf{Q}_{\mathrm{post}}$ *over a gate set* $\mathcal{S}$ is a 4-tuple $(Q, \mathcal{S}, \mathrm{anc}, \mathrm{post})$, where $\mathbf{Q} = (Q, \mathcal{S}, \mathrm{anc})$ is an efficient quantum computer and $\mathrm{post} : \mathbb{N} \to \{0,1\}^*$ is a total and polynomial time computable function whose purpose is to specify a post-selection string on a given input size. For all $n \in \mathbb{N}$ and all $x \in \{0,1\}^n$, $\mathbf{Q}$ and post satisfy $f_{\mathbf{Q}_{\mathrm{post}}}(n) \coloneqq f_{\mathbf{Q}}(n) - |\mathrm{post}(n)| > 0$ and

$$\Pr\big[\mathbf{Q}(x)_{[f_{\mathbf{Q}_{\mathrm{post}}}(n)+1 \,:\, f_{\mathbf{Q}}(n)]} = \mathrm{post}(n)\big] = \sum_{z\in\{0,1\}^{f_{\mathbf{Q}_{\mathrm{post}}}(n)}} \Pr[\mathbf{Q}(x) = z.\mathrm{post}(n)] \neq 0.$$

The former condition ensures that the *output size of* $\mathbf{Q}_{\mathrm{post}}$, $f_{\mathbf{Q}_{\mathrm{post}}}$, is always positive, and the latter condition ensures that the probability that $\mathbf{Q}$ outputs a string whose last $|\mathrm{post}(n)|$ bits equal $\mathrm{post}(n)$ is nonzero. This way, the probability the last $|\mathrm{post}(n)|$ registers of $\mathbf{Q}(x)$ have $|\mathrm{post}(n)\rangle$ as the state is non-zero, which is necessary for the probability that $\mathbf{Q}_{\mathrm{post}}$ outputs $y \in \{0,1\}^{f_{\mathbf{Q}_{\mathrm{post}}}(n)}$ on input $x \in \{0,1\}^n$ to be well-defined:

$$\begin{aligned}\Pr[\mathbf{Q}_{\mathrm{post}}(x) = y] &\coloneqq \Pr\big[\mathbf{Q}(x)_{[1 \,:\, f_{\mathbf{Q}_{\mathrm{post}}}(n)]} = y \mid \mathbf{Q}(x)_{[f_{\mathbf{Q}_{\mathrm{post}}}(n)+1 \,:\, f_{\mathbf{Q}}(n)]} = \mathrm{post}(n)\big] \\ &= \frac{\Pr[\mathbf{Q}(x) = y.\mathrm{post}(n)]}{\Pr\big[\mathbf{Q}(x)_{[f_{\mathbf{Q}_{\mathrm{post}}}(n)+1 \,:\, f_{\mathbf{Q}}(n)]} = \mathrm{post}(n)\big]}.\end{aligned}$$

Notice, this is the conditional probability that the upper $f_{\mathbf{Q}_{\mathrm{post}}}(n)$ registers of $\mathbf{Q}(x)$ have $|y\rangle$ as the state, given that the lower $|\mathrm{post}(n)|$ registers of $\mathbf{Q}(x)$ have $|\mathrm{post}(n)\rangle$ as the state.

The set of languages that efficient post-selected quantum computers over a universal gate set $\mathcal{S}$ can decide is usually called $\mathsf{PostBQP}$ [Aar05]. We extend this definition as follows, which allows for non-universal $\mathcal{S}$.

**Definition 2.8.** Let $\mathcal{S}$ be a gate set. The class $\mathsf{PostBQP}(\mathcal{S})$ consists of all languages $L$ for which there is an efficient post-selected quantum computer $\mathbf{Q}_{\mathrm{post}}$ over $\mathcal{S}$ and $\delta \in (0, 1/2)$ such that for all $x \in \{0,1\}^*$, $\Pr[\mathbf{Q}_{\mathrm{post}}(x)_1 = L(x)] \geq 1/2 + \delta$.

As already remarked, if $\mathcal{S}$ is universal, then $\mathsf{PostBQP}(\mathcal{S}) = \mathsf{PostBQP}$. In this case, $\mathsf{PostBQP}$ is independent of $\delta$ because efficient post-selected quantum computers over a universal gate set can compute the majority function [Aar05]. Therefore, if $L \in \mathsf{PostBQP}$, then *for all* $\delta \in (0, 1/2)$, there is an efficient post-selected quantum computer $\mathbf{Q}_{\text{post}}$ that decides $L$ to within bounded error $1/2 + \delta$. However, for non-universal $\mathcal{S}$, $\mathsf{PostBQP}(\mathcal{S})$ is not necessarily independent of $\delta$ in this sense, because $\mathcal{S}$ may be sufficiently constrained that no circuit over $\mathcal{S}$ can approximate the majority function in any useful sense. Therefore, a priori, if $L \in \mathsf{PostBQP}(\mathcal{S})$ for some non-universal $\mathcal{S}$, then there merely *exists* $\delta \in (0, 1/2)$ and an efficient post-selected quantum computer $\mathbf{Q}_{\text{post}}$ that decides $L$ to within bounded error $1/2 + \delta$.

2.6. **Postselection Gadgets and Gadget Quantum Computers.** We now define "post-selection gadgets", which give rise to particular post-selected quantum computers.

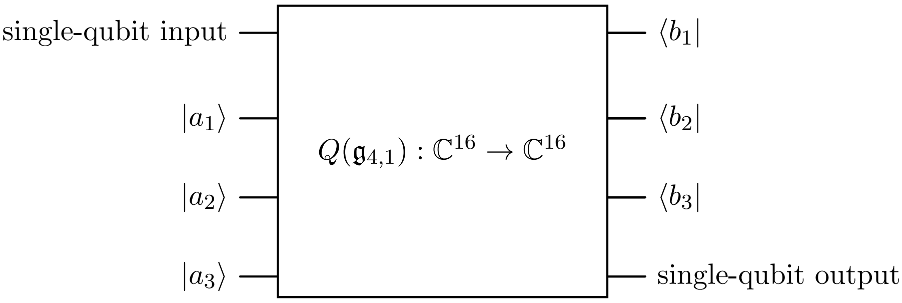
**Definition 2.9.** Let $\mathcal{S}$ be a gate set. A *$j$-to-$k$ post-selection gadget over $\mathcal{S}$* (or, if $\mathcal{S}$ is contextually clear, a *$j$-to-$k$ post-selection gadget*, or just a *$j$-to-$k$ gadget*) is a map $\mathfrak{g}_{j,k} : \mathbb{C}^{2^j} \to \mathbb{C}^{2^j}$ that acts on a $k$-qubit system as follows:

(i) Introduce a set $A$ of $j - k$ ancillae in the state $|a_1 \dots a_{j-k}\rangle_A$, where each $a_i \in \{0, 1\}$.

(ii) Apply a $j$-qubit circuit $Q(\mathfrak{g}_{j,k}) : \mathbb{C}^{2^j} \to \mathbb{C}^{2^j}$ over $\mathcal{S}$ to both the system and ancillae.

(iii) Post-select on a set $B$ of $j - k$ qubits being in the state $|b_1 \dots b_{j-k}\rangle_B$, where each $b_i \in \{0, 1\}$.

For example, the following circuit fragment is a 4-to-1 post-selection gadget $\mathfrak{g}_{4,1}$ over $\mathcal{S}$:



Given a $j$-to-$k$ post-selection gadget $\mathfrak{g}_{j,k}$, we define its *action* $\mathscr{A}(\mathfrak{g}_{j,k})$ as the $2^k \times 2^k$ matrix

$$\mathscr{A}(\mathfrak{g}_{j,k}) := {}_B\langle b_1 \dots b_{j-k}| \, Q(\mathfrak{g}_{j,k}) \, |a_1 \dots a_{j-k}\rangle_A .$$

If $\det \mathscr{A}(\mathfrak{g}_{j,k}) \neq 0$, then the *normalized action* of $\mathfrak{g}_{j,k}$ is the unit-determinant $2^k \times 2^k$ matrix

$$\tilde{\mathscr{A}}(\mathfrak{g}_{j,k}) := \frac{\mathscr{A}(\mathfrak{g}_{j,k})}{(\det \mathscr{A}(\mathfrak{g}_{j,k}))^{2^{-k}}}.$$

Finally, the set $\mathrm{gad}_k(\mathcal{S})$ consists of the normalized actions of all $j$-to-$k$ post-selection gadgets over $\mathcal{S}$ with non-zero determinant, i.e.,

$$\mathrm{gad}_k(\mathcal{S}) := \bigcup_{j \in \mathbb{N}} \left\{ \tilde{\mathscr{A}}(\mathfrak{g}_{j,k}) \mid \mathfrak{g}_{j,k} \text{ is a } j\text{-to-}k \text{ post-selection gadget with } \det \mathscr{A}(\mathfrak{g}_{j,k}) \neq 0 \right\}.$$

**Observation 2.1.** *For every $k \in \mathbb{N}$ and every gate set $\mathcal{S}$, $I_k \in \mathrm{gad}_k(\mathcal{S})$ and $\mathrm{gad}_k(\mathcal{S}) \subset \mathrm{SL}(2^k; \mathbb{C})$. Therefore, if $\Gamma \subset \mathrm{gad}_k(\mathcal{S})$ and $\langle \Gamma \rangle$ is closed under inverses, then $\langle \Gamma \rangle$ is a subgroup of $\mathrm{SL}(2^k; \mathbb{C})$.*

In practice, proving that $\langle \Gamma \rangle$ is closed under inverses is difficult. This is because while it is easy to contrive gadgets, it is not always easy to contrive their "inverse".

**Definition 2.10.** Let $\mathfrak{g} = \mathfrak{g}_{j,k}$ be a $j$-to-$k$ gadget over a gate set $\mathcal{S}$ such that $\det \mathscr{A}(\mathfrak{g}) \neq 0$. We call a $j'$-to-$k$ gadget $\mathfrak{g}^{-1} = \mathfrak{g}_{j',k}$ over $\mathcal{S}$ an *inverse gadget of* $\mathfrak{g}$ iff $\mathscr{A}(\mathfrak{g})^{-1} \in \langle \mathscr{A}(\mathfrak{g}), \mathscr{A}(\mathfrak{g}^{-1}) \rangle$.

A means of improving our results is to show that for any $j$-to-$k$ post-selection gadget $\mathfrak{g} = \mathfrak{g}_{j,k}$ over a gate set $\mathcal{S}$ such that $\det \mathscr{A}(\mathfrak{g}) \neq 0$, there exists an inverse gadget of $\mathfrak{g}$ over $\mathcal{S}$. If this is true, then for any finite set $\Gamma \subset \operatorname{gad}_k(\mathcal{S})$, there exists another finite set $\Gamma' \subset \operatorname{gad}_k(\mathcal{S})$ such that $\Gamma \subseteq \Gamma'$ and $\langle \Gamma' \rangle$ is a subgroup of $\mathrm{SL}(2;\mathbb{C})$. We leave this as an open question (see Conjecture 6.1).

We now define "gadget quantum circuits", which are essentially quantum circuits defined over $\mathcal{S} \cup \Gamma$ for some gate set $\mathcal{S}$ and some finite collection of gadgets $\Gamma \subset \bigcup_{k\in\mathbb{N}} \operatorname{gad}_k(\mathcal{S})$.

**Definition 2.11.** Let $\Gamma \subset \bigcup_{\ell\in[k]} \mathrm{SL}(2^\ell;\mathbb{C})$ be a finite subset for some fixed $k > 1$. An *$n$-qubit gadget quantum circuit $Q_n$ over* $\Gamma$ is an operator in $\mathrm{SL}(2^n;\mathbb{C})$ that admits the product decomposition

$$Q_n = \omega_{d_n} \dots \omega_1,$$

where each $\omega_1, \dots, \omega_{d_n} \in \mathrm{SL}(2^n;\mathbb{C})$ is a tensor product of operators in $\Gamma \cup \{I_1\}$. The total number of operators in $\Gamma$ that make up $Q_n$ is the *size of* $Q_n$ and $d_n$ is the *depth of* $Q_n$.

Gadget quantum circuits naturally define a "gadget quantum computer".

**Definition 2.12.** An *efficient gadget quantum computer* $\mathbf{G}$ *over a gate set* $\mathcal{S}$ is a 4-tuple $(G, \mathcal{S}, \Gamma, \mathrm{anc})$, where $\Gamma \subset \bigcup_{k\in\mathbb{N}} \operatorname{gad}_k(\mathcal{S})$ is a finite set, $\mathrm{anc} : \mathbb{N} \to \{0,1\}^*$ is a total and polynomial time computable function, and $Q = (Q_n)_{n\in\mathbb{N}}$ is a uniform family of polynomial size $(n + |\mathrm{anc}(n)|)$-qubit gadget quantum circuits $Q_n$ over $\mathcal{S} \cup \Gamma$. For all $n \in \mathbb{N}$, the *output size of* $\mathbf{Q}_{\mathrm{gad}}$ is the polynomial $f_{\mathbf{Q}_{\mathrm{gad}}}(n) := n + |\mathrm{anc}(n)|$ and the probability that $\mathbf{Q}_{\mathrm{gad}}$ outputs $y \in \{0,1\}^{f_{\mathbf{Q}_{\mathrm{gad}}}(n)}$ on input $x \in \{0,1\}^n$ is $\Pr[\mathbf{Q}_{\mathrm{gad}}(x) = y] := |\langle y| Q_n |x\rangle \otimes |\mathrm{anc}(n)\rangle|^2$.

2.7. **Post-Selected Gadget Quantum Computers.** Finally, we introduce the notion of a "post-selected gadget quantum computer", which is to a gadget quantum computer what a post-selected quantum computer is to a quantum computer.

**Definition 2.13.** An *efficient post-selected gadget quantum computer* $\mathbf{G}_{\mathrm{post}}$ *over a gate set* $\mathcal{S}$ is a 5-tuple $(G, \mathcal{S}, \Gamma, \mathrm{anc}, \mathrm{post})$, where $\mathbf{G} = (G, \mathcal{S}, \Gamma, \mathrm{anc})$ is an efficient gadget quantum computer and $\mathrm{post} : \mathbb{N} \to \{0,1\}^*$ is a total and polynomial time computable function whose purpose is to specify a post-selection string on a given input size. For all $n \in \mathbb{N}$ and all $x \in \{0,1\}^n$, $\mathbf{G}$ and post satisfy $f_{\mathbf{G}_{\mathrm{post}}}(n) := f_{\mathbf{G}}(n) - |\mathrm{post}(n)| > 0$ and

$$\Pr\big[\mathbf{G}(x)_{[f_{\mathbf{G}_{\mathrm{post}}}(n)+1\,:\,f_{\mathbf{G}}(n)]} = \mathrm{post}(n)\big] = \sum_{z\in\{0,1\}^{f_{\mathbf{G}_{\mathrm{post}}}(n)}} \Pr[\mathbf{G}(x) = z.\mathrm{post}(n)] \neq 0.$$

The former condition ensures that the *output size of* $\mathbf{G}_{\mathrm{post}}$, $f_{\mathbf{G}_{\mathrm{post}}}$, is always positive, and the latter condition ensures that the probability that $\mathbf{G}$ outputs a string whose last $|\mathrm{post}(n)|$ bits equal $\mathrm{post}(n)$ is nonzero. This way, the probability the last $|\mathrm{post}(n)|$ registers of $\mathbf{G}(x)$ have $|\mathrm{post}(n)\rangle$ as the state is non-zero, which is necessary for the probability that $\mathbf{G}_{\mathrm{post}}$ outputs $y \in \{0,1\}^{f_{\mathbf{G}_{\mathrm{post}}}(n)}$ on input $x \in \{0,1\}^n$ to be well-defined:

$$\begin{aligned}\Pr[\mathbf{G}_{\mathrm{post}}(x) = y] &:= \Pr\big[\mathbf{G}(x)_{[1\,:\,f_{\mathbf{G}_{\mathrm{post}}}(n)]} = y \mid \mathbf{G}(x)_{[f_{\mathbf{G}_{\mathrm{post}}}(n)+1\,:\,f_{\mathbf{G}}(n)]} = \mathrm{post}(n)\big] \\ &= \frac{\Pr[\mathbf{G}(x) = y.\mathrm{post}(n)]}{\Pr\big[\mathbf{G}(x)_{[f_{\mathbf{G}_{\mathrm{post}}}(n)+1\,:\,f_{\mathbf{G}}(n)]} = \mathrm{post}(n)\big]}.\end{aligned}$$

Notice, this is the conditional probability that the upper $f_{\mathbf{G}_{\mathrm{post}}}(n)$ registers of $\mathbf{G}(x)$ have $|y\rangle$ as the state, given that the lower $|\mathrm{post}(n)|$ registers of $\mathbf{G}(x)$ have $|\mathrm{post}(n)\rangle$ as the state.

We now introduce the complexity class $\mathsf{GadBQP}(\mathcal{S})$, which characterizes the languages decidable by efficient post-selected gadget quantum computers over the gate set $\mathcal{S}$.

**Definition 2.14.** Let $\mathcal{S}$ be a gate set. The class $\mathsf{GadBQP}(\mathcal{S})$ consists of all languages $L$ for which there is an efficient post-selected gadget quantum computer $\mathbf{G}_{\text{post}}$ over $\mathcal{S}$ and $\delta \in (0, 1/2)$ such that for all $x \in \{0,1\}^*$, $\Pr[\mathbf{G}_{\text{post}}(x)_1 = L(x)] \geq 1/2 + \delta$.

It is plain that for every gate set $\mathcal{S}$, $\mathsf{PostBQP}(\mathcal{S}) \subseteq \mathsf{GadBQP}(\mathcal{S}) \subseteq \mathsf{PostBQP}$. Thus, if $\mathcal{S}$ is universal, then $\mathsf{PostBQP}(\mathcal{S}) = \mathsf{GadBQP}(\mathcal{S}) = \mathsf{PostBQP}$. In this case, $\mathsf{GadBQP}(\mathcal{S})$ is independent of $\delta$ for the same reason that $\mathsf{PostBQP}$ is. However, for non-universal $\mathcal{S}$, $\mathsf{GadBQP}(\mathcal{S})$ is not necessarily independent of $\delta$, because $\mathcal{S}$ may be sufficiently constrained that no gadget quantum computer over $\mathcal{S}$ can approximate the majority function in any useful sense. Therefore, a priori, if $L \in \mathsf{GadBQP}(\mathcal{S})$ for some non-universal $\mathcal{S}$, then there merely *exists* $\delta \in (0, 1/2)$ and an efficient post-selected gadget quantum computer $\mathbf{G}_{\text{post}}$ that decides $L$ to within bounded error $1/2 + \delta$.

To better understand the relationship between $\mathsf{PostBQP}(\mathcal{S})$ and $\mathsf{GadBQP}(\mathcal{S})$, observe that every efficient gadget quantum computer is an efficient post-selected quantum computer over the same gate set (simply substitute every gadget for its corresponding element of $\Gamma$). Therefore, every efficient *post-selected* gadget quantum computer is an efficient post-selected quantum computer. This observation implies the following proposition.

**Proposition 2.2.** *For every gate set $\mathcal{S}$, $\mathsf{PostBQP}(\mathcal{S}) = \mathsf{GadBQP}(\mathcal{S}) \subseteq \mathsf{PostBQP}$.*

Ultimately, we are interested in those *non*-universal gate sets $\mathcal{S}$ for which $\mathsf{GadBQP}(\mathcal{S}) = \mathsf{PostBQP}$. In this case, $\mathsf{GadBQP}(\mathcal{S})$ becomes independent of $\delta$, so that if $L \in \mathsf{PostBQP}(\mathcal{S}) = \mathsf{GadBQP}(\mathcal{S})$, then *for all* $\delta \in (0, 1/2)$, there exists an efficient gadget quantum computer that decides $L$ to within bounded error $1/2 + \delta$. This fact is paramount to Proposition 3.1 below.

## 3. Statement and Proof of Main Result

Our main result affords a sufficient condition for $\mathsf{GadBQP}(\mathcal{S}) = \mathsf{PostBQP}$ for a non-universal gate set $\mathcal{S}$. Together with the following proposition and the reasonable assumption that the polynomial hierarchy does not collapse, we obtain a sufficient condition for determining if efficient classical computers cannot simulate efficient quantum computers over a non-universal gate set $\mathcal{S}$ in the weak multiplicative sense.

**Proposition 3.1.** *Let $\mathcal{S}$ be a gate set. If $\mathsf{GadBQP}(\mathcal{S}) = \mathsf{PostBQP}$ and for every efficient quantum computer $\mathbf{Q}$ over $\mathcal{S}$ there exists an efficient classical computer $\mathbf{C}$ that simulates $\mathbf{Q}$ to within multiplicative error $\epsilon < \sqrt{2} - 1$, then $\mathsf{PH} \subseteq \Sigma_3\mathsf{P}$. Therefore, if the polynomial hierarchy is infinite and $\mathsf{GadBQP}(\mathcal{S}) = \mathsf{PostBQP}$, then efficient classical computers cannot simulate efficient quantum computers over $\mathcal{S}$ to within multiplicative error $\epsilon < \sqrt{2} - 1$.*

*Proof.* Aaronson proved that $\mathsf{PostBQP} = \mathsf{PP}$ [Aar05], Toda proved that $\mathsf{PH} \subseteq \mathsf{P}^{\mathsf{PP}}$ [Tod91], and Han, Hemaspaandra, and Thierauf proved that $\mathsf{PostBPP} \subseteq \mathsf{P}^{\Sigma_2\mathsf{P}}$ [HHT97]. Therefore, if $\mathsf{PostBPP} = \mathsf{PostBQP}$, then $\mathsf{PH} \subseteq \mathsf{P}^{\mathsf{PostBPP}} \subseteq \mathsf{P}^{\mathsf{P}^{\Sigma_2\mathsf{P}}} \subseteq \Sigma_3\mathsf{P}$. Since $\mathsf{PostBPP} \subseteq \mathsf{PostBQP}$ unconditionally, it suffices to show that our additional assumptions imply $\mathsf{PostBQP} \subseteq \mathsf{PostBPP}$.

To this end, consider any $L \in \mathsf{PostBQP}$. By the assumption $\mathsf{GadBQP}(\mathcal{S}) = \mathsf{PostBQP}$ and Proposition 2.2, it holds that $\mathsf{PostBQP}(\mathcal{S}) = \mathsf{PostBQP}$. Thus, $L \in \mathsf{PostBQP}(\mathcal{S})$, so there exists an efficient post-selected quantum computer $\mathbf{Q}_{\text{post}} = (\mathbf{Q}, \text{post}) = (Q, \mathcal{S}, \text{anc}, \text{post})$ that decides $L$ to within bounded error $\delta \in (0, 1/2)$. Since $L \in \mathsf{PostBQP}$, we can choose any $\delta$ in this range.

By assumption, there is an efficient classical computer $\mathbf{C}$ that simulates $\mathbf{Q}$ to within multiplicative error $\epsilon < \sqrt{2} - 1$. Therefore, for all $n \in \mathbb{N}$, all $x \in \{0,1\}^n$, and all $y \in \{0,1\}^{f_{\mathbf{Q}_{\text{post}}}(n)}$,

$$\frac{1}{1+\epsilon}\Pr[\mathbf{C}(x) = y.\text{post}(n)] \leq \Pr[\mathbf{Q}(x) = y.\text{post}(n)] \leq (1+\epsilon)\Pr[\mathbf{C}(x) = y.\text{post}(n)].$$

Consequently,

$$\begin{aligned}\Pr[\mathbf{Q}_{\text{post}}(x) = y] &= \frac{\Pr\left[\mathbf{Q}(x) = y.\text{post}(n)\right]}{\Pr\left[\mathbf{Q}(x)_{[f_{\mathbf{Q}_{\text{post}}}(n)+1\,:\,f_{\mathbf{Q}}(n)]} = \text{post}(n)\right]}\\ &\le \frac{(1+\epsilon)\Pr\left[\mathbf{C}(x) = y.\text{post}(n)\right]}{\Pr\left[\mathbf{C}(x)_{[f_{\mathbf{C}_{\text{post}}}(n)+1\,:\,f_{\mathbf{C}}(n)]} = \text{post}(n)\right]/(1+\epsilon)}\\ &= (1+\epsilon)^2\Pr[\mathbf{C}_{\text{post}}(x) = y],\end{aligned}$$

where $\mathbf{C}_{\text{post}}$ is the efficient post-selected classical computer $(\mathbf{C}, \text{post})$. Thus, for every $x \in \{0,1\}^*$,

$$\Pr[\mathbf{C}_{\text{post}}(x)_1 = L(x)] \ge \frac{1}{(1+\epsilon)^2}\left(\frac{1}{2} + \delta\right) = \frac{1}{2} \cdot \frac{1+2\delta}{(1+\epsilon)^2}.$$

Consequently, $\mathbf{C}_{\text{post}}$ decides $L$ in the sense of $\mathsf{PostBPP}$ provided $(1+\epsilon)^2 < 1 + 2\delta$. Since $\delta$ can be any value satisfying $0 < \delta < 1/2$, it suffices for $0 \le \epsilon < \sqrt{2} - 1$ to ensure $L \in \mathsf{PostBPP}$. ■

We now state and prove our main technical result, which gives a sufficient condition for a gate set $\mathcal{S}$ to satisfy $\mathsf{GadBQP}(\mathcal{S}) = \mathsf{PostBQP}$.

**Theorem 3.2.** *Let $\mathcal{S}$ be a gate set. If there exists a finite subset $\Gamma \subset \text{gad}_1(\mathcal{S})$ such that $\langle \Gamma \rangle$ is a dense subgroup of* $\text{SL}(2;\mathbb{C})$*, then* $\mathsf{GadBQP}(\mathcal{S}) = \mathsf{PostBQP}$.

To prove this, we rely on a result due to Aharanov, Arad, Eban, and Landau [AAEL07], which establishes a non-unitary analogue of the Solovay-Kitaev theorem. In the following, $\|\cdot\|_{\text{op}}$ is the operator norm and $B_r$ is the identity-centered open ball $\{\omega \in \text{SL}(2;\mathbb{C}) \mid \|\omega - I_1\|_{\text{op}} < r\}$ for $r > 0$.

**Theorem 3.3** (Theorem 7.6 in [AAEL07])**.** *Let $\Gamma'$ be a finite subset of* $\text{SL}(2;\mathbb{C})$*. For all $r > 0$, there exists a constant $\epsilon_0 > 0$ such that if $\Gamma'$ is an $\epsilon_0$-net for $B_r$, then there exists a constant $c > 0$ such that for all $\delta > 0$ and all $\omega \in B_r$, there is a sequence $\sigma_\omega$ of operators from $\Gamma'$ of length $O(\log^c 1/\delta)$ such that $\|\omega - \sigma_\omega\|_{\text{op}} < \delta$. Moreover, there is an algorithm that constructs $\sigma_\omega$ in polylogarithmic time in the parameter $1/\delta$.*

This implies Theorem 3.2.

*Proof of Theorem 3.2.* By Proposition 2.2, $\mathsf{GadBQP}(\mathcal{S}) \subseteq \mathsf{PostBQP}$, so it remains to show the reverse containment. To this end, let $E$ be an entangling gate in $\mathcal{S}$, which exists by our definition of "gate set" (see Definition 2.4). Then, $\mathcal{S}' = \{E, \tilde{H}, \tilde{T}\}$ is a universal gate set, where

$$\tilde{H} = \frac{i}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad \tilde{T} = \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$$

are the SU(2) versions of the usual Hadamard and $\pi/8$ gates, respectively. Consequently, $\mathsf{PostBQP}(\mathcal{S}') = \mathsf{PostBQP}$, so $\mathsf{PostBQP} \subseteq \mathsf{GadBQP}(\mathcal{S})$ iff $\mathsf{PostBQP}(\mathcal{S}') \subseteq \mathsf{GadBQP}(\mathcal{S})$.

To prove the latter containment, let $L \in \mathsf{PostBQP}(\mathcal{S}')$. Then, there is an efficient post-selected quantum computer $(Q' = (Q'_n)_{n\in\mathbb{N}}, \mathcal{S}', \text{anc}', \text{post}')$ that decides $L$. By assumption, there exists a finite subset $\Gamma \subset \text{gad}_1(\mathcal{S})$ such that $\langle\Gamma\rangle$ is dense in $\text{SL}(2;\mathbb{C})$. Put $r = 2.1$ so that $\text{SU}(2) \subset B_r$. Since $\langle\Gamma\rangle$ is dense in $\text{SL}(2;\mathbb{C})$, for all $\epsilon > 0$, there exists a finite set $\Gamma' \subset \langle\Gamma\rangle$ that is an $\epsilon$-net for $B_r$. The set $\Gamma'$ can be found in finite time by a naïve search. Choose $\epsilon \le \epsilon_0$ so that the conditions of Theorem 3.3 are satisfied. Then, there exists $c > 0$ such that for all $n \in \mathbb{N}$, there are sequences $\sigma_{\tilde{H}}(n)$ and $\sigma_{\tilde{T}}(n)$ of gates from $\Gamma'$ with lengths $O(\log^c 1/\epsilon)$ such that $\|\tilde{H} - \sigma_{\tilde{H}}(n)\|_{\text{op}} < 2^{-n}/s'(n)$ and $\|\tilde{T} - \sigma_{\tilde{T}}(n)\|_{\text{op}} < 2^{-n}/s'(n)$, where $s'(n)$ is the (polynomial) size of the circuit $Q'_n$. By Theorem 3.3, both $\sigma_{\tilde{H}}(n)$ and $\sigma_{\tilde{T}}(n)$ can be constructed from $\Gamma$ in polylogarithmic time $s'(n)2^n$. Therefore, both $\sigma_{\tilde{H}}(n)$ and $\sigma_{\tilde{T}}(n)$ can be constructed from $\Gamma$ in polynomial time with respect to the parameter $n$. Consequently, for each $n \in \mathbb{N}$, replacing every $\tilde{H}$ and $\tilde{T}$ gate in the $(n + |\mathrm{anc}'(n)|)$-qubit quantum circuit $Q'_n$ with $\sigma_{\tilde{H}}(n)$ and $\sigma_{\tilde{T}}(n)$, respectively, yields an $(n + |\mathrm{anc}'(n)|)$-qubit gadget quantum circuit $Q_n$ over $\mathcal{S} \cup \Gamma$ such that $\|Q'_n - Q_n\|_{\mathrm{op}} < 2^{-n}$. Thus, $Q := (Q_n)_{n\in\mathbb{N}}$ is a uniform and polynomial size family of $(n + |\mathrm{anc}'(n)|)$-qubit gadget quantum circuits over $\mathcal{S} \cup \Gamma$ that approximates $Q'$ to exponential accuracy. It holds, therefore, that $(Q, \mathcal{S}, \Gamma, \mathrm{anc}', \mathrm{post}')$ is an efficient post-selected gadget quantum computer over $\mathcal{S}$ that decides $L$, so $L \in \mathsf{GadBQP}(\mathcal{S})$. ■

Consequently, if a finite number of single-qubit post-selection gadgets $\Gamma$ over a gate set $\mathcal{S}$ generate a dense subgroup of $\mathrm{SL}(2;\mathbb{C})$, then efficient quantum computers over $\mathcal{S}$ can perform a sampling task that no efficient classical computer can. The problem, then, is to understand when $\Gamma$ generates a dense subgroup of $\mathrm{SL}(2;\mathbb{C})$. Interestingly, unlike $\mathrm{SU}(2)$, this is rather simple thanks to a result of Sullivan [Sul85] (our Theorem 4.9), which proves that the so-called "non-elementary" subgroups of $\mathrm{SL}(2;\mathbb{C})$ are essentially either discrete or dense in $\mathrm{SL}(2;\mathbb{C})$. Note that the theorem below is actually a simplified version of Sullivan's theorem, which we explain in more detail in Section 4.3. Note also that while Sullivan's theorem is couched in several hitherto undefined terms, the point to keep in mind is that each premise is algorithmically easy to check.

**Theorem 3.4** (Simplified version of Theorem 4.9)**.** *Let $\Gamma$ be a finite subset of $\mathrm{SL}(2;\mathbb{C})$. If $\langle\Gamma\rangle$ is a non-elementary, non-discrete, and strictly loxodromic subgroup of $\mathrm{SL}(2;\mathbb{C})$, then $\langle\Gamma\rangle$ is dense in $\mathrm{SL}(2;\mathbb{C})$.*

Together, Proposition 3.1, Theorem 3.2, and Theorem 3.4 entail our criterion for concluding if no efficient classical computer can simulate an efficient quantum computer over a non-universal gate set to within small multiplicative error:

**Theorem 3.5** (Criterion for Quantum Advantage)**.** *Let $\mathcal{S}$ be a gate set and suppose the polynomial hierarchy is infinite. If there exists a finite subset $\Gamma \subset \mathrm{gad}_1(\mathcal{S})$ such that $\langle\Gamma\rangle$ is a non-elementary, non-discrete, and strictly loxodromic subgroup of $\mathrm{SL}(2;\mathbb{C})$, then efficient classical computers cannot simulate efficient quantum computers over $\mathcal{S}$ to within multiplicative error $\epsilon < \sqrt{2} - 1$.*

Of course, since we have yet to define what the terms "non-elementary" and "strictly loxodromic" mean, it is not apparent if our criterion is actually of any use. However, as we detail in the next section, these terms are not complicated, and there is in fact a simple algorithm that checks if a finitely generated subgroup $\langle\Gamma\rangle$ of $\mathrm{SL}(2;\mathbb{C})$ is non-elementary, non-discrete, and strictly loxodromic (and hence dense in $\mathrm{SL}(2;\mathbb{C})$ à la Theorem 3.4). Consequently, on account of Theorem 3.5, there is a simple algorithm that checks if efficient classical computers cannot simulate efficient quantum computers over a non-universal gate set $\mathcal{S}$ in the weak multiplicative sense. In Section 5, we illustrate the power of our criterion by proving several new quantum advantage results in addition to some well-known old ones.

We emphasize that this approach provides a *sufficient* criterion to infer the classical intractability of a quantum gate set, but not a strictly necessary one. In other words, it could happen that a non-universal gate set does not satisfy the premises of Theorem 3.5, but nevertheless engenders circuits that no efficient classical computer can simulate.[3] There are also a few ways we think our criterion Theorem 3.5 can be improved; see Conjectures 6.1 and 6.2.

## 4. Some Properties of Subgroups of $\mathrm{SL}(2;\mathbb{C})$

There are several important properties that a subgroup of $\mathrm{SL}(2;\mathbb{C})$ can possess. The first property is *elementarity.*

[3] This could happen, for example, if $\Gamma$ generates a dense subgroup of $\mathrm{SU}(2)$ as opposed to $\mathrm{SL}(2;\mathbb{C})$.

4.1. **Elementary Subgroups of** $\mathrm{SL}(2;\mathbb{C})$**.** Given an element $x$ of a set $X$ and a group $H$ that acts on $X$ from the left via the operation $\alpha : H \times X \to X$, recall that the *$H$-orbit of $x$* is the set $\{\alpha(h,x) \mid h \in H\}$. We say there exists a *finite $H$-orbit in $X$* iff there is $x \in X$ such that the $H$-orbit of $x$ is a finite set.

**Definition 4.1.** A subgroup $H \leq \mathrm{SL}(2;\mathbb{C})$ is *elementary* iff there exists a finite $H$-orbit in $\mathbb{R}^3$.

For example, $\mathrm{SU}(2) \leq \mathrm{SL}(2;\mathbb{C})$ is elementary. To see this, consider the representation $\rho := R \circ \pi$, where $\pi : \mathrm{SU}(2) \to \mathrm{SO}(3) \cong \mathrm{SU}(2)/\mathbb{Z}_2$ is the covering homomorphism and $R : \mathrm{SO}(3) \to \mathrm{GL}(3;\mathbb{R})$ is the defining (i.e. vector) representation of $\mathrm{SO}(3)$. Since every rotation in $\mathbb{R}^3$ fixes the origin $(0,0,0)^T \in \mathbb{R}^3$, $\{\rho(U)(0,0,0)^T \mid U \in \mathrm{SU}(2)\}$ is a finite $\mathrm{SU}(2)$-orbit in $\mathbb{R}^3$.

Elementary subgroups are important in the theory of Möbius transformations, for which a standard introduction is a textbook by Bearden [Bea83]. Rather than digressing into this theory, however, we shall simply quote a series of useful results for determining when a subgroup of $\mathrm{SL}(2;\mathbb{C})$ is elementary. The first of these is an exercise in Bearden's textbook.

**Proposition 4.1** (Exercise 5.1, Problem 2 in [Bea83])**.** *A subgroup $H \leq \mathrm{SL}(2;\mathbb{C})$ is elementary iff for all $g,h \in H$, the two-generated subgroup $\langle g,h\rangle$ is elementary.*

Therefore, the elementarity of a group depends solely on the information contained in all of its rank-two subgroups. Unfortunately, if $H \leq \mathrm{SL}(2;\mathbb{C})$ is finitely generated, then it is not necessarily the case that $H$ is elementary if every two-generated subgroup of generators is elementary.[4] Nevertheless, the logical inverse of this statement is true by Proposition 4.1, so there is a sufficient, purely generator-based condition for a finitely generated subgroup of $\mathrm{SL}(2;\mathbb{C})$ to be *non*-elementary:

**Corollary 4.2.** *Let $H = \langle\Gamma\rangle \leq \mathrm{SL}(2;\mathbb{C})$ be finitely generated by $\Gamma \subset \mathrm{SL}(2;\mathbb{C})$. If there exist $g,h \in \Gamma$ such that $\langle g,h\rangle$ is non-elementary, then $H$ is non-elementary.*

The next proposition by Baribeau and Ransford [BR00] entails a very useful necessary and sufficient condition for a two-generated subgroup of $\mathrm{SL}(2;\mathbb{C})$ to be elementary.

**Proposition 4.3** (Proposition 2.1 in [BR00])**.** *For all $g,h \in \mathrm{SL}(2;\mathbb{C})$, define $\beta(g) := \mathrm{tr}^2(g) - 4$ and $\gamma(g,h) := \mathrm{tr}(ghg^{-1}h^{-1}) - 2$. Then, $\langle g,h\rangle$ is an elementary subgroup of $\mathrm{SL}(2;\mathbb{C})$ iff one of the following three conditions hold:*

*(i)* $\beta(g), \beta(h) \in [-4,0]$, *and* $\gamma(g,h) \in [-\beta(g)\beta(h)/4, 0]$,
*(ii)* $\gamma(g,h) = 0$,
*(iii)* $\beta(g) = \gamma(g,h)$ *and* $\beta(h) = -4$, *or* $\beta(g) = -4$ *and* $\beta(h) = \gamma(g,h)$, *or* $\beta(g) = -4$ *and* $\beta(h) = -4$.

Altogether, one gets Algorithm 1, `IsElementary`, for determining if a finitely generated subgroup of $\mathrm{SL}(2;\mathbb{C})$ is non-elementary. This algorithm combines Corollary 4.2 with the contrapositive of Proposition 4.3.

4.2. **Discrete Subgroups of** $\mathrm{SL}(2;\mathbb{C})$**.** Another important property that a subgroup of $\mathrm{SL}(2;\mathbb{C})$ can possess is *discreteness*. This property is the familiar topological one, so we do not define it here. Instead, we cite several famous results that help determine when a non-elementary subgroup of $\mathrm{SL}(2;\mathbb{C})$ is discrete.

Like elementarity, the first result proves that the discreteness of a non-elementary subgroup of $\mathrm{SL}(2;\mathbb{C})$ depends solely on the information contained in all of its rank-two subgroups.

**Proposition 4.4** (Theorem 5.4.2 in [Bea83])**.** *A non-elementary subgroup $H \leq \mathrm{SL}(2;\mathbb{C})$ is discrete iff for all $g,h \in H$, the two-generated subgroup $\langle g,h\rangle$ is discrete.*

[4] A counterexample follows from the fact that any two involutions generate an elementary subgroup [Koh24].

**Algorithm 1** IsElementary

```
Input: Finite set $\Gamma \subset \mathrm{SL}(2;\mathbb{C})$ such that $\langle \Gamma \rangle \leq \mathrm{SL}(2;\mathbb{C})$
Output: NO if $\langle \Gamma \rangle$ is non-elementary, IDK ("I don't know") otherwise
for $g, h \in \Gamma$ do
    if $\beta(g) \notin [-4, 0]$ or $\beta(h) \notin [-4, 0]$ or $\gamma(g, h) \notin [-\beta(g)\beta(h)/4, 0]$ then
        if $\gamma(g, h) \neq 0$ then
            if $\beta(g) \neq \gamma(g, h)$ or $\beta(h) \neq -4$ then
                if $\beta(g) \neq -4$ or $\beta(h) \neq \gamma(g, h)$ then
                    if $\beta(g) \neq -4$ or $\beta(h) \neq -4$ then
                        return NO
return IDK
```

Unfortunately, if $H \leq \mathrm{SL}(2;\mathbb{C})$ is finitely generated and non-elementary, then it is not necessarily the case that $H$ is discrete if every two-generated subgroup of generators is discrete.[5] Nevertheless, the logical inverse of this statement is true by Proposition 4.4, so there is a sufficient, purely generator-based condition for a finitely generated and non-elementary subgroup of $\mathrm{SL}(2;\mathbb{C})$ to be *non*-discrete:

**Corollary 4.5.** *Let $H = \langle \Gamma \rangle \leq \mathrm{SL}(2;\mathbb{C})$ be non-elementary and finitely generated by $\Gamma \subset \mathrm{SL}(2;\mathbb{C})$. If there exist $g, h \in \Gamma$ such that $\langle g, h \rangle$ is non-discrete, then $H$ is non-discrete.*

Consequently, to determine if a finitely generated and non-elementary subgroup $H \leq \mathrm{SL}(2;\mathbb{C})$ is non-discrete, it suffices to interrogate the rank-two subgroups of $H$ that are generated by the generators. The most natural way to do this is to employ a famous result of Jørgensen [Jør76], which concerns every discrete and non-elementary two-generated subgroup of $\mathrm{SL}(2;\mathbb{C})$.

**Proposition 4.6** (Jørgensen's Inequality [Jør76])**.** *Suppose $\langle g, h \rangle$ generates a discrete and non-elementary subgroup of $\mathrm{SL}(2;\mathbb{C})$. Then*

$$\left|\mathrm{tr}^2(g) - 4\right| + \left|\mathrm{tr}(ghg^{-1}h^{-1}) - 2\right| \geq 1. \tag{1}$$

*Therefore, if $\langle g, h \rangle$ is a non-elementary subgroup of $\mathrm{SL}(2;\mathbb{C})$ and $g$ and $h$ violate Eq. (1), then $\langle g, h \rangle$ is non-discrete.*

In fact, there are many interesting generalizations of Jørgensen's inequality, such as the following few. For more, see [BM81, CT09, AGM21].

**Proposition 4.7** (Theorems 1 – 3 in [Tan89])**.** *Suppose $\langle g, h \rangle$ generates a discrete subgroup of $\mathrm{SL}(2;\mathbb{C})$.*

*(i) If $\mathrm{tr}(ghg^{-1}h^{-1}) \neq 1$, then*

$$\left|\mathrm{tr}^2(g) - 2\right| + \left|\mathrm{tr}(ghg^{-1}h^{-1}) - 1\right| \geq 1.$$

*(ii) If $\mathrm{tr}(ghg^{-1}h^{-1}) = 1$ and $\mathrm{tr}^2(g) \neq 2$, then*

$$\left|\mathrm{tr}^2(g) - 2\right| > \frac{1}{2}.$$

*(iii) If $\mathrm{tr}^2(g) \neq 1$, then*

$$\left|\mathrm{tr}^2(g) - 1\right| + \left|\mathrm{tr}(ghg^{-1}h^{-1})\right| \geq 1.$$

[5] A counterexample follows from the following three facts [Koh24]: (1) there are arbitrary small triangles $T$ in the hyperbolic plane $\mathbb{H}^2$ with angles that are rational multiples of $\pi$, (2) the hyperbolic isometry group $G$ generated by reflections in the edges of $T$ is non-discrete if $T$ is small enough, and (3) any two generators of $G$ generate a finite group of isometries.

*(iv) If* $\mathrm{tr}^2(g) = 1$*, then*

$$\left|\mathrm{tr}(ghg^{-1}h^{-1})\right| > \frac{1}{2} \quad \textit{or} \quad \mathrm{tr}(ghg^{-1}h^{-1}) = 0$$

*and*

$$\left|\mathrm{tr}(ghg^{-1}h^{-1}) - 1\right| > \frac{1}{2} \quad \textit{or} \quad \mathrm{tr}(ghg^{-1}h^{-1}) = 1.$$

*(v) If* $\mathrm{tr}(ghg^{-1}h^{-1}) \neq 1$*, then*

$$\left|\mathrm{tr}^2(g) - \mathrm{tr}(ghg^{-1}h^{-1})\right| + \left|\mathrm{tr}(ghg^{-1}h^{-1}) - 1\right| \geq 1.$$

*(vi) If* $\mathrm{tr}(ghg^{-1}h^{-1}) = 1$ *and* $\mathrm{tr}^2(g) \neq 1$*, then*

$$\left|\mathrm{tr}^2(g) - 1\right| > \frac{1}{2}.$$

Altogether, one gets Algorithm 2, `IsDiscrete`, for determining if a finitely generated and non-elementary subgroup of $\mathrm{SL}(2;\mathbb{C})$ is non-discrete. This algorithm combines Corollary 4.5 with the contrapositive of Jørgensen's inequality (Proposition 4.6) and the contrapositive of Proposition 4.7.

**Algorithm 2** `IsDiscrete`

```
Input: Finite set $\Gamma \subset \mathrm{SL}(2;\mathbb{C})$ such that $\langle\Gamma\rangle \leq \mathrm{SL}(2;\mathbb{C})$
Output: NO if $\langle\Gamma\rangle$ is non-discrete, IDK otherwise
for $g, h \in \Gamma$ do
  if IsElementary($\{g,h\}$) = NO and $|\mathrm{tr}^2(g) - 4| + |\mathrm{tr}(ghg^{-1}h^{-1}) - 2| < 1$ then
    return NO
  if $\mathrm{tr}(ghg^{-1}h^{-1}) \neq 1$ and $|\mathrm{tr}^2(g) - 2| + |\mathrm{tr}(ghg^{-1}h^{-1}) - 1| < 1$ then
    return NO
  if $\mathrm{tr}(ghg^{-1}h^{-1}) = 1$ and $\mathrm{tr}^2(g) \neq 2$ and $|\mathrm{tr}^2(g) - 2| \leq 1/2$ then
    return NO
  if $\mathrm{tr}^2(g) \neq 1$ and $|\mathrm{tr}^2(g) - 1| + |\mathrm{tr}(ghg^{-1}h^{-1})| < 1$ then
    return NO
  if $\mathrm{tr}^2(g) = 1$ and $|\mathrm{tr}(ghg^{-1}h^{-1})| \leq 1/2$ and $\mathrm{tr}(ghg^{-1}h^{-1}) \neq 0$ then
    return NO
  if $\mathrm{tr}^2(g) = 1$ and $|\mathrm{tr}(ghg^{-1}h^{-1}) - 1| \leq 1/2$ and $\mathrm{tr}(ghg^{-1}h^{-1}) \neq 1$ then
    return NO
  if $\mathrm{tr}(ghg^{-1}h^{-1}) \neq 1$ and $|\mathrm{tr}^2(g) - \mathrm{tr}(ghg^{-1}h^{-1})| + |\mathrm{tr}(ghg^{-1}h^{-1}) - 1| < 1$ then
    return NO
  if $\mathrm{tr}(ghg^{-1}h^{-1}) = 1$ and $\mathrm{tr}^2(g) \neq 1$ and $|\mathrm{tr}^2(g) - 1| \leq 1/2$ then
    return NO
return IDK
```

4.3. **Strictly Loxodromic Subgroups of** $\mathrm{SL}(2;\mathbb{C})$**.** Another important property that a subgroup of $\mathrm{SL}(2;\mathbb{C})$ can possess is *strict loxodromy.* As no subgroup of $\mathrm{SL}(2;\mathbb{R})$ is strictly loxodromic, this property is a purely complex phenomenon.

**Definition 4.2.** A subgroup $H \leq \mathrm{SL}(2;\mathbb{C})$ is *loxodromic* iff there exists $g \in H$ such that $\mathrm{tr}^2(g) \in \mathbb{C}\backslash[0,4]$. We say $H \leq \mathrm{SL}(2;\mathbb{C})$ is *strictly loxodromic* iff there exists $g \in H$ such that $\mathrm{tr}(g) \in \mathbb{C}\backslash\mathbb{R}$. In this latter case, $g$ is called a *strictly loxodromic element* of $\mathrm{SL}(2;\mathbb{C})$.

Unfortunately, like discreteness and elementarity, if $H \leq \mathrm{SL}(2;\mathbb{C})$ is finitely generated, then it is not necessarily the case that $H$ is strictly loxodromic only if there is a strictly loxodromic generator.[6] Nevertheless, the converse of this statement is true definitionally:

**Lemma 4.8.** *Let $H = \langle \Gamma \rangle \leq \mathrm{SL}(2;\mathbb{C})$ be finitely generated by $\Gamma \subset \mathrm{SL}(2;\mathbb{C})$. If $\Gamma$ contains a strictly loxodromic element, then $H$ is strictly loxodromic.*

Altogether, Lemma 4.8 entails the very simple Algorithm 3, `IsLoxodromic`, for determining if a finitely generated subgroup of $\mathrm{SL}(2;\mathbb{C})$ is strictly loxodromic.

**Algorithm 3** `IsLoxodromic`

```
Input: Finite set $\Gamma \subset \mathrm{SL}(2;\mathbb{C})$ such that $\langle\Gamma\rangle \leq \mathrm{SL}(2;\mathbb{C})$
Output: YES if $\langle\Gamma\rangle$ is strictly loxodromic, IDK otherwise
for $g \in \Gamma$ do
    if $\mathrm{tr}(g) \in \mathbb{C}\backslash\mathbb{R}$ then
        return YES
return IDK
```

## 4.4. Dense Subgroups of $\mathrm{SL}(2;\mathbb{C})$.

If $H \leq \mathrm{SL}(2;\mathbb{C})$ is non-discrete, then it may be topologically dense in $\mathrm{SL}(2;\mathbb{C})$. Surprisingly, at least for non-elementary $H$, this is essentially always the case, according to a result of Sullivan [Sul85] (c.f. Theorem 9.3 in [AAEL07]).

**Theorem 4.9** (First proposition in [Sul85])**.** *If $H \leq \mathrm{SL}(2;\mathbb{C})$ is non-elementary and non-discrete, then $H$ is either dense in $\mathrm{SL}(2;\mathbb{C})$ or conjugate to a dense subgroup of $\mathrm{SL}(2;\mathbb{R})$.*

If $H$ is conjugate to a dense subgroup of $\mathrm{SL}(2;\mathbb{R})$, then there exists $\omega \in \mathrm{SL}(2;\mathbb{C})$ such that $\bar{H}$, the topological closure of $H$, equals $\omega^{-1}\mathrm{SL}(2;\mathbb{R})\omega$. While we conjecture that density in this sense should yield a statement similar to Theorem 3.2 (see Conjecture 6.2), we were not able to prove this. Instead, we use strict loxodromy to restrict $H$ enough so that it is necessarily dense in $\mathrm{SL}(2;\mathbb{C})$. This was the content of Theorem 3.4, which we restate and prove below.

**Theorem 3.4** (Simplified version of Theorem 4.9)**.** *Let $\Gamma$ be a finite subset of $\mathrm{SL}(2;\mathbb{C})$. If $\langle\Gamma\rangle$ is a non-elementary, non-discrete, and strictly loxodromic subgroup of $\mathrm{SL}(2;\mathbb{C})$, then $\langle\Gamma\rangle$ is dense in $\mathrm{SL}(2;\mathbb{C})$.*

*Proof.* For all $\omega \in \mathrm{SL}(2;\mathbb{C})$ and all $g \in \omega^{-1}\mathrm{SL}(2;\mathbb{R})\omega$, $\mathrm{tr}(g) \in \mathbb{R}$. Thus, $\omega^{-1}\mathrm{SL}(2;\mathbb{R})\omega$ contains no strictly loxodromic elements, so $\langle\Gamma\rangle$ must be dense in $\mathrm{SL}(2;\mathbb{C})$ by Theorem 4.9. ■

By composing the algorithms `IsElementary`, `IsDiscrete`, and `IsLoxodromic`, we obtain an algorithm for checking if a finitely generated subgroup of $\mathrm{SL}(2;\mathbb{C})$ is dense in $\mathrm{SL}(2;\mathbb{C})$. The exact composition is illustrated on the left side of Figure 1. Put in the context of our criterion Theorem 3.5, we get an algorithm for checking if efficient classical computers cannot simulate efficient quantum computers over a non-universal gate set to within small multiplicative error (assuming the polynomial hierarchy is infinite). This is depicted on the right side of Figure 1.

[6] A counterexample is the group $H = \langle\{\omega_1, \omega_2, \omega_1^{-1}, \omega_2^{-1}\}\rangle$, where

$$\omega_1 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{and} \quad \omega_2 = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}.$$

Evidently, $H$ is strictly loxodromic because $\mathrm{tr}(\omega_1\omega_2) \in \mathbb{C}\backslash\mathbb{R}$, however no generator of $H$ is strictly loxodromic.

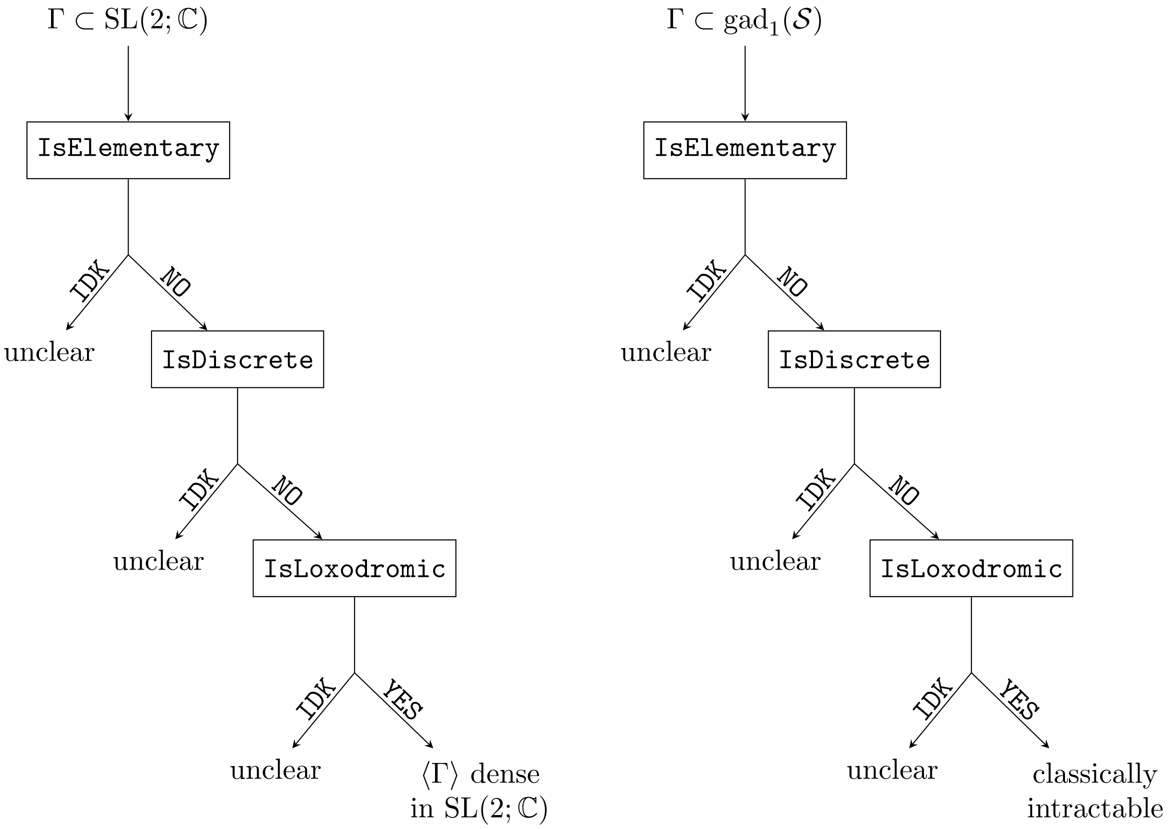


Figure 1. (Left) A flowchart illustrating our algorithm for checking if a finite subset $\Gamma \subset \mathrm{SL}(2;\mathbb{C})$ generates a dense subgroup of $\mathrm{SL}(2;\mathbb{C})$. (Right) An identical flowchart, but placed in the context of our criterion, Theorem 3.5. In this case, $\Gamma$ is a finite subset of $\mathrm{gad}_1(\mathcal{S})$ for some gate set $\mathcal{S}$ and "$\langle\Gamma\rangle$ dense in $\mathrm{SL}(2;\mathbb{C})$" is replaced by "classically intractable" in the sense of Theorem 3.5.

## 5. Applications

In this section, we demonstrate the utility of our criterion by proving quantum advantage results for several types of restricted quantum computational models, including: instantaneous quantum polynomial (IQP) circuits, conjugated Clifford circuits (CCCs), *commuting* CCCs, CCCs over various fragments of the Clifford group, and CCCs where the interstitial Clifford circuit is composed exclusively of CZ gates. Using our criterion, we re-derive the quantum advantage of IQP circuits and CCCs, which were originally found in [BJS11] and [BFK18], respectively. The quantum advantage of commuting CCCs, CCCs over the Clifford fragments, and CCCs over just CZ gates are (as far as we know) new, and this speaks to the utility of our intractability criterion in settings where other standard approaches do not directly apply.

In addition to these quantum advantage results (which are all statements of the form "there exists a circuit in this restricted quantum model that no efficient classical computer can simulate unless the polynomial hierarchy collapses"), we also prove the full complexity classification of CCCs, commuting CCCs, and CCCs over some of the fragments of the Clifford group (which are all statements of the form "if the polynomial hierarchy is infinite, then efficient classical computers can simulate circuits in this restricted quantum model if and only if the circuit takes such-and-such form"). These classification results make extensive use of Wolfram Mathematica 14.1. Our notebook is available online for anyone trying to reproduce our calculations [KFG24].

In what follows, we make extensive use of the following gates in the computational basis:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad \text{and} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We also use the rotation matrices

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \quad \text{and} \quad R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

as well as the entangling gates

$$\mathrm{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad \text{and} \quad \mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Finally, to help the reader navigate the structure of all of our quantum advantage and classification results, we have provided two dependency diagrams. One, Figure 2, indicates the statements that each quantum advantage result depends on, and the other, Figure 3, indicates the statements that each classification result depends on.

### 5.1. **Instantaneous Quantum Polynomial Circuits.**

At a high level, the IQP model describes quantum computations that only use commuting operations. Physically, this means that there is no temporal order to the computation, save the output measurement of the qubits, which happens last.

**Definition 5.1.** An *IQP circuit* is an efficient quantum computer over a gate set $\mathcal{S}$ for which every $U \in \mathcal{S}$ is diagonal in the basis $\{|0\rangle \pm |1\rangle\}$. In other words, if $U \in \mathcal{S}$ is a $2^k \times 2^k$ matrix, then there exists $D \in \mathrm{U}(2^k)$ such that $D$ is diagonal in the computational basis and $U = H^{\otimes k} D H^{\otimes k}$.

In [BJS11], Bremner, Jozsa, and Shepherd prove that when augmented with post-selection, IQP circuits can decide PP-complete languages. Therefore, by an argument that is nearly identical to our Proposition 3.1, one gets the following theorem.

**Theorem 5.1** (Corollary 1 in [BJS11]). *If the polynomial hierarchy is infinite, then efficient classical computers cannot simulate IQP circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$.*

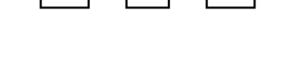
Bremner et al. prove Theorem 5.1 by first restricting to the gate set

$$\mathcal{S}_{\mathrm{IQP}} \coloneqq \{HTH, (H \otimes H)\mathrm{CZ}(H \otimes H)\}.$$

Since $T$ and CZ are diagonal in the computational basis, circuits over $\mathcal{S}_{\mathrm{IQP}}$ are indeed IQP circuits. They then show that there exists a post-selection gadget over $\mathcal{S}_{\mathrm{IQP}}$ that can be used to "inject" a Hadamard gate anywhere in the circuit. Together with the fact that $\{H, T, \mathrm{CZ}\}$ is a universal gate set, it follows that post-selected IQP circuits can decide PP-complete languages.

Here, we reproduce Theorem 5.1 using our criterion, Theorem 3.5, together with the same gate set $\mathcal{S}_{\mathrm{IQP}}$ that Bremner et al. used.

*Proof of Theorem 5.1.* By Theorem 3.5, it suffices to find a finite number of post-selection gadgets over $\mathcal{S}_{\mathrm{IQP}}$ whose normalized actions generate a non-elementary, non-discrete, and strictly loxodromic subgroup of $\mathrm{SL}(2;\mathbb{C})$. To this end, consider the 1-to-1 post-selection gadget

$\mathfrak{a} =$ 

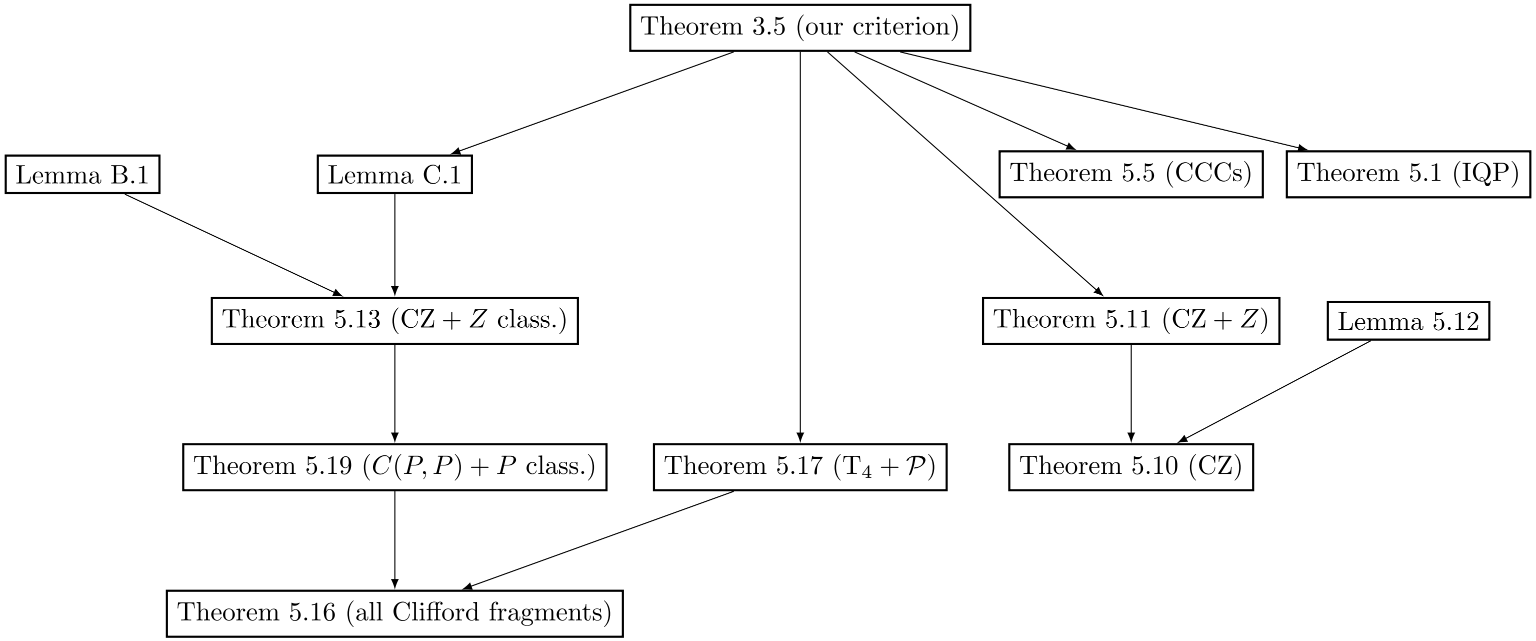

Theorem 3.5 (our criterion)
Lemma B.1
Lemma C.1
Theorem 5.5 (CCCs)
Theorem 5.1 (IQP)
Theorem 5.13 (CZ + $Z$ class.)
Theorem 5.11 (CZ + $Z$)
Lemma 5.12
Theorem 5.19 ($C(P, P) + P$ class.)
Theorem 5.17 ($\mathrm{T}_4 + \mathcal{P}$)
Theorem 5.10 (CZ)
Theorem 5.16 (all Clifford fragments)

Figure 2. A dependency diagram for our hardness results, where an arrow from A to B means "A is used in the proof of B" and "class." means the associated theorem is a classification result.

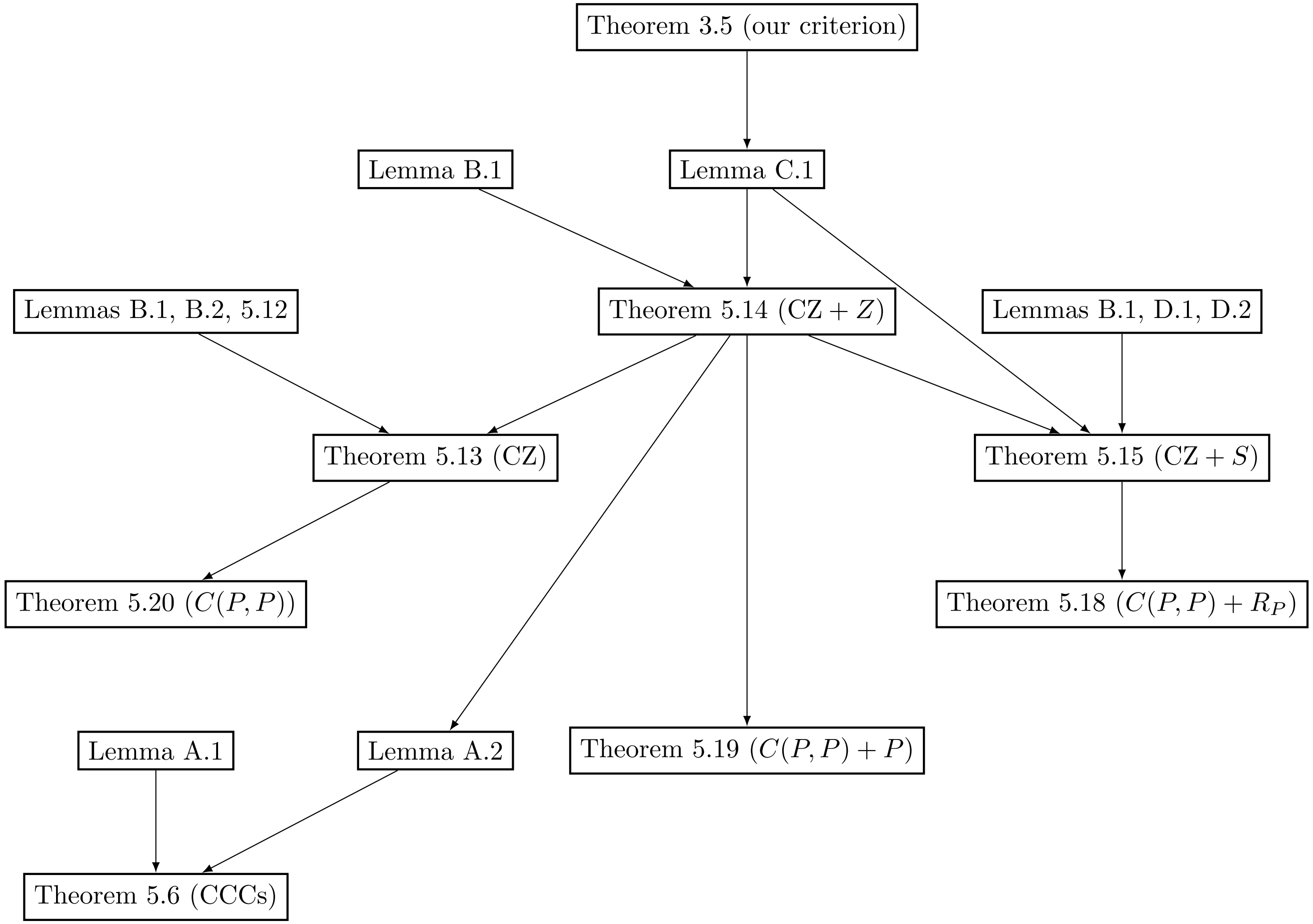
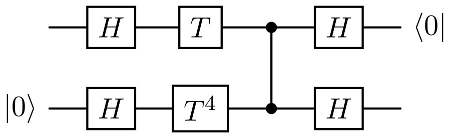


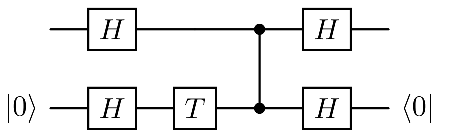
FIGURE 3. A dependency diagram for our classification results, where an arrow from A to B means "A is used in the proof of B".

as well as the two 2-to-1 post-selection gadgets

$\mathfrak{b} =$



and $\mathfrak{c} =$



It is easy to prove that the normalized actions of $\mathfrak{a}$ and $\mathfrak{b}$ are the unitary $\mathrm{SL}(2;\mathbb{C})$ matrices

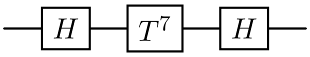
$$A := \tilde{\mathscr{A}}(\mathfrak{a}) = \frac{1}{2e^{i\pi/8}}\begin{pmatrix}1+e^{i\pi/4} & 1-e^{i\pi/4}\\ 1-e^{i\pi/4} & 1+e^{i\pi/4}\end{pmatrix} \quad \text{and} \quad B := \tilde{\mathscr{A}}(\mathfrak{b}) = \frac{1}{\sqrt{2}}\begin{pmatrix}e^{i\pi/8} & -e^{i\pi/8}\\ e^{-i\pi/8} & e^{-i\pi/8}\end{pmatrix},$$

while the normalized action of $\mathfrak{c}$ is the *non*-unitary $\mathrm{SL}(2;\mathbb{C})$ matrix

$$C := \tilde{\mathscr{A}}(\mathfrak{c}) = \frac{1}{\sqrt{1-i}}\begin{pmatrix}1 & e^{i\pi/4}\\ e^{i\pi/4} & 1\end{pmatrix}.$$

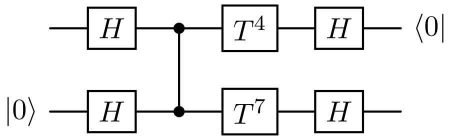
Crucially, inverse gadgets of $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$ are also realizable over $\mathcal{S}_{\mathrm{IQP}}$. For $\mathfrak{a}$, the inverse is the 1-to-1 post-selection gadget

$\mathfrak{a}^{-1} =$

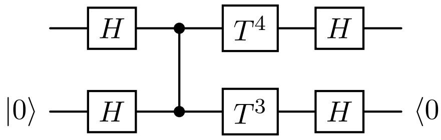


while for $\mathfrak{b}$ and $\mathfrak{c}$, the inverses are the 2-to-1 post-selection gadgets

$\mathfrak{b}^{-1} =$



and $\mathfrak{c}^{-1} =$



These are inverses of $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$ in the sense of Definition 2.10 because $\tilde{\mathscr{A}}(\mathfrak{a}^{-1}) = \tilde{\mathscr{A}}(\mathfrak{a})^{-1} = A^{-1}$, $\tilde{\mathscr{A}}(\mathfrak{b}^{-1}) = \tilde{\mathscr{A}}(\mathfrak{b})^{-1} = B^{-1}$, and $\tilde{\mathscr{A}}(\mathfrak{c}^{-1}) = -\tilde{\mathscr{A}}(\mathfrak{c})^{-1} = -C^{-1}$.

Now let $\Gamma_{\mathrm{IQP}} := \{A, A^{-1}, B, B^{-1}, C, -C^{-1}\}$. Evidently, $\langle\Gamma_{\mathrm{IQP}}\rangle$ is closed under inverses, so $\langle\Gamma_{\mathrm{IQP}}\rangle$ is a subgroup of $\mathrm{SL}(2;\mathbb{C})$. In fact, $\langle\Gamma_{\mathrm{IQP}}\rangle$ is a non-elementary, non-discrete, and strictly loxodromic subgroup of $\mathrm{SL}(2;\mathbb{C})$.

**Claim 5.2.** *$\langle\Gamma_{\mathrm{IQP}}\rangle$ is a non-elementary subgroup of* $\mathrm{SL}(2;\mathbb{C})$.

*Proof.* Since $\beta(B) = -3 - \frac{1}{\sqrt{2}}$, $\beta(C) = -2 + 2i$, and $\gamma(B, C) = -1 + i$, `IsElementary`$(\Gamma_{\mathrm{IQP}}) =$ `NO`. ■

**Claim 5.3.** *$\langle\Gamma_{\mathrm{IQP}}\rangle$ is a non-discrete subgroup of* $\mathrm{SL}(2;\mathbb{C})$.

*Proof.* Since $\mathrm{tr}(BAB^{-1}A^{-1}) = 1 + \frac{1}{\sqrt{2}} \neq 1$ and

$$\left|\mathrm{tr}^2(B) - \mathrm{tr}(BAB^{-1}A^{-1})\right| + \left|\mathrm{tr}(BAB^{-1}A^{-1}) - 1\right| = \frac{1}{\sqrt{2}} < 1,$$

is follows from line 16 in Algorithm 2 that `IsDiscrete`$(\Gamma_{\mathrm{IQP}}) =$ `NO`. ■

**Claim 5.4.** *$\langle\Gamma_{\mathrm{IQP}}\rangle$ is a strictly loxodromic subgroup of* $\mathrm{SL}(2;\mathbb{C})$.

*Proof.* Since $\mathrm{tr}(C) = \frac{2}{\sqrt{1-i}} = \sqrt{2+2i} \in \mathbb{C}\backslash\mathbb{R}$, `IsLoxodromic`$(\Gamma_{\mathrm{IQP}}) =$ `YES`. ■

Thus, the quantum advantage of IQP circuits follows from our criterion Theorem 3.5. ■

5.2. **Conjugated Clifford Circuits.** The Gottesman-Knill theorem proves that efficient classical computers can simulate uniform and polynomial size Clifford circuits *exactly* [Got98, AG04]. However, this result sensitively depends on an efficient state representation that is afforded by the Clifford group. It is therefore natural to wonder if by "perturbing" the Clifford group in some way, the perturbed circuits become hard to simulate classically.

CCCs are a type of perturbed Clifford circuit in which every $k$-qubit Clifford operation is conjugated by $U^{\otimes k}$ for some fixed single-qubit unitary $U$.

**Definition 5.2.** Fix $U \in \mathrm{U}(2)$. A *$U$-conjugated Clifford circuit* (or *$U$-CCC* for short) is an efficient quantum computer over the gate set[7]

$$\mathcal{S}_{\mathrm{CCC}}(U) \coloneqq \big\{U^\dagger H U, U^\dagger S U, (U^\dagger \otimes U^\dagger)\mathrm{CZ}(U \otimes U)\big\}.$$

A *conjugated Clifford circuit* is a $U$-CCC for some $U \in \mathrm{U}(2)$.

In [BFK18], Bouland, Fitzsimons, and Koh prove that when augmented with post-selection, CCCs can decide $\mathsf{PP}$-complete languages. Therefore, by an argument that is nearly identical to our Proposition 3.1, one gets the following theorem.

**Theorem 5.5** (Corollary of Theorem 3.2 in [BFK18]). *If the polynomial hierarchy is infinite, then efficient classical computers cannot simulate CCCs to within multiplicative error $\epsilon < \sqrt{2}-1$.*

Bouland et al. prove Theorem 5.5 by employing the well-known result that if $V$ is any non-Clifford single-qubit gate, then $\{V, H, S, \mathrm{CZ}\}$ is a universal gate set [NRS01]. They then show that if $U \neq e^{i\alpha} C R_z(\lambda)$ for all $C \in \langle H, S\rangle$ and all $\alpha, \lambda \in [0, 2\pi)$, then there exists a post-selection gadget over $\mathcal{S}_{\mathrm{CCC}}(U)$ that realizes a unitary non-Clifford gate $V$. Together, these facts imply that post-selected $U$-CCCs can decide $\mathsf{PP}$-complete languages. When combined with the Gottesman-Knill theorem, their techniques complete the complexity classification of $U$-CCCs:

**Theorem 5.6** (Theorem 3.2 in [BFK18]). *If the polynomial hierarchy is infinite, then efficient classical computers can simulate $U$-CCCs to within multiplicative error $\epsilon < \sqrt{2}-1$ iff there exists $C \in \langle H, S\rangle$ and $\alpha, \lambda \in [0, 2\pi)$ such that $U = e^{i\alpha} C R_z(\lambda)$.*

Here, we reproduce Theorem 5.5 using our criterion. In Appendix A, we reproduce the full complexity classification of CCC's (Theorem 5.6), again using our criterion.

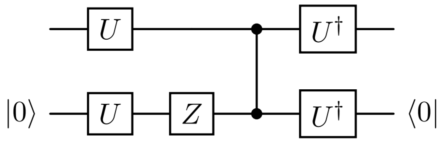
*Proof of Theorem 5.5.* It suffices to exhibit a single-qubit unitary $U$ such that a finite number of post-selection gadgets over $\mathcal{S}_{\mathrm{CCC}}(U)$ have normalized actions that generate a non-elementary, non-discrete, and strictly loxodromic subgroup of $\mathrm{SL}(2; \mathbb{C})$. To this end, let

$$U = R_x\left(\frac{2\pi}{3}\right) = \begin{pmatrix} \cos\frac{\pi}{3} & -i\sin\frac{\pi}{3} \\ -i\sin\frac{\pi}{3} & \cos\frac{\pi}{3} \end{pmatrix}$$

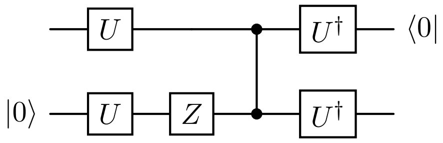
[7] In the original CCC paper [BFK18], the authors use the gate set $\{U^\dagger H U, U^\dagger S U, (U^\dagger \otimes U^\dagger)\mathrm{CNOT}(U \otimes U)\}$. However, since $\mathrm{CNOT} = (I_1 \otimes H)\mathrm{CZ}(I_1 \otimes H)$, our gate set $\mathcal{S}_{\mathrm{CCC}}(U)$ is equivalent to theirs.

and consider the following three 2-to-1 post-selection gadgets over $\mathcal{S}_{\mathrm{CCC}}(U)$:

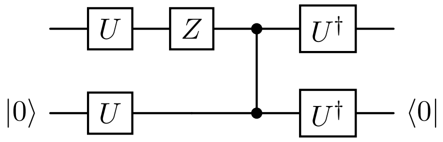
$\mathfrak{d} =$



$\mathfrak{e} =$



$\mathfrak{f} =$



It is easy to prove that the normalized actions of $\mathfrak{d}$, $\mathfrak{e}$, and $\mathfrak{f}$ are, respectively, the non-unitary $\mathrm{SL}(2;\mathbb{C})$ matrices

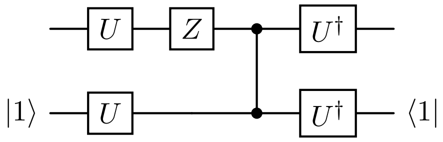
$$D := \widetilde{\mathscr{A}}(\mathfrak{d}) = \frac{1}{4\sqrt{2}}\begin{pmatrix} -5i & 3\sqrt{3} \\ -3\sqrt{3} & i \end{pmatrix}$$

$$E := \widetilde{\mathscr{A}}(\mathfrak{e}) = \frac{1}{2\sqrt{6}}\begin{pmatrix} 5 & 3i\sqrt{3} \\ i\sqrt{3} & 3 \end{pmatrix}$$

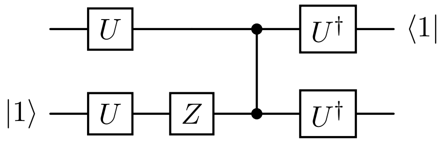
$$F := \widetilde{\mathscr{A}}(\mathfrak{f}) = \frac{1}{4\sqrt{2}}\begin{pmatrix} 5 & -i\sqrt{3} \\ i\sqrt{3} & 7 \end{pmatrix}.$$

Crucially, inverse gadgets of $\mathfrak{d}$, $\mathfrak{e}$, and $\mathfrak{f}$ are also realizable over $\mathcal{S}_{\mathrm{CCC}}(U)$:

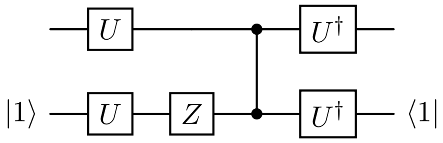
$\mathfrak{d}^{-1} =$



$\mathfrak{e}^{-1} =$



$\mathfrak{f}^{-1} =$



Indeed, these are inverses of $\mathfrak{d}$, $\mathfrak{e}$, and $\mathfrak{f}$ because $\widetilde{\mathscr{A}}(\mathfrak{d}^{-1}) = \widetilde{\mathscr{A}}(\mathfrak{d})^{-1} = D^{-1}$, $\widetilde{\mathscr{A}}(\mathfrak{e}^{-1}) = \widetilde{\mathscr{A}}(\mathfrak{e})^{-1} = E^{-1}$, and $\widetilde{\mathscr{A}}(\mathfrak{f}^{-1}) = \widetilde{\mathscr{A}}(\mathfrak{f})^{-1} = F^{-1}$.

Now let $\Gamma_{\mathrm{CCC}}(U) := \{D, D^{-1}, E, E^{-1}, F, F^{-1}\}$. Evidently, $\langle\Gamma_{\mathrm{CCC}}(U)\rangle$ is closed under inverses, so $\langle\Gamma_{\mathrm{CCC}}(U)\rangle$ is a subgroup of $\mathrm{SL}(2;\mathbb{C})$. In fact, $\langle\Gamma_{\mathrm{CCC}}(U)\rangle$ is a non-elementary, non-discrete, and strictly loxodromic subgroup of $\mathrm{SL}(2;\mathbb{C})$.

**Claim 5.7.** *$\langle\Gamma_{\mathrm{CCC}}(U)\rangle$ is a non-elementary subgroup of* $\mathrm{SL}(2;\mathbb{C})$.

*Proof.* Since $\beta(E) = -\frac{4}{3}$, $\beta(F) = \frac{1}{2}$, and $\gamma(E,F) = \frac{1}{4}$, $\texttt{IsElementary}(\Gamma_{\mathrm{CCC}}(U)) = \texttt{NO}$. ■

**Claim 5.8.** *$\langle \Gamma_{\text{CCC}}(U)\rangle$ is a non-discrete subgroup of* $\mathrm{SL}(2;\mathbb{C})$.

*Proof.* Since $\texttt{IsElementary}(\{E,F\}) = \texttt{NO}$ and

$$\left|\mathrm{tr}^2(F) - 4\right| + \left|\mathrm{tr}(FEF^{-1}E^{-1}) - 2\right| = \frac{3}{4} < 1,$$

it follows from line 4 in Algorithm 2 that $\texttt{IsDiscrete}(\Gamma_{\text{CCC}}(U)) = \texttt{NO}$. ■

**Claim 5.9.** *$\langle \Gamma_{\text{CCC}}(U)\rangle$ is a strictly loxodromic subgroup of* $\mathrm{SL}(2;\mathbb{C})$.

*Proof.* Since $\mathrm{tr}(D) = -\frac{i}{\sqrt{2}} \in \mathbb{C}\backslash\mathbb{R}$, $\texttt{IsLoxodromic}(\Gamma_{\text{CCC}}(U)) = \texttt{YES}$. ■

Thus, the quantum advantage of CCCs follows from our criterion Theorem 3.5. ■

5.3. **Conjugated** CZ **Circuits.** In this section, we prove a quantum advantage result for a special subclass of CCCs that we call *conjugated* CZ *circuits*. As the name suggests, conjugated CZ circuits are CCCs where the interstitial Clifford circuit is made entirely of CZ gates.

**Definition 5.3.** Fix $U \in \mathrm{U}(2)$. A *$U$-conjugated* CZ *circuit* is an efficient quantum computer over the gate set

$$\mathcal{S}_{\text{CZ}}(U) := \{(U^\dagger \otimes U^\dagger)\text{CZ}(U \otimes U)\}.$$

A *conjugated* CZ *circuit* is a $U$-conjugated CZ circuit for some $U \in \mathrm{U}(2)$.

Conjugated CZ circuits are incredibly simple. Nevertheless, it is very unlikely that efficient classical computers can simulate them in the weak multiplicative sense.

**Theorem 5.10.** *If the polynomial hierarchy is infinite, then efficient classical computers cannot simulate conjugated* CZ *circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$.*

To prove this, we employ an ostensibly less restrictive model of quantum computation.

**Definition 5.4.** Fix $U \in \mathrm{U}(2)$. A *$U$-conjugated* CZ$+Z$ *circuit* is an efficient quantum computer over the gate set

$$\mathcal{S}_{\text{CZ}+Z}(U) := \{U^\dagger Z U, (U^\dagger \otimes U^\dagger)\text{CZ}(U \otimes U)\}.$$

A *conjugated* CZ $+ Z$ *circuit* is a $U$-conjugated CZ $+ Z$ circuit for some $U \in \mathrm{U}(2)$.

Conjugated CZ circuits are a type of conjugated CZ$+Z$ circuit, so indeed conjugated CZ$+Z$ circuits are less restrictive. In fact, we have already proven that efficient classical computers can most likely not simulate conjugated CZ $+ Z$ circuits in the weak multiplicative sense.

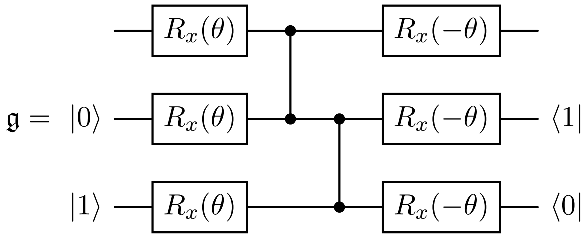
**Theorem 5.11.** *If the polynomial hierarchy is infinite, then efficient classical computers cannot simulate conjugated* CZ $+ Z$ *circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$.*

*Proof.* Put $U = R_x(\frac{2\pi}{3})$ as in Section 5.2. Since the gadgets $\mathfrak{d}, \mathfrak{e}, \mathfrak{f}, \mathfrak{d}^{-1}, \mathfrak{e}^{-1}$, and $\mathfrak{f}^{-1}$ are all realizable over $\mathcal{S}_{\text{CZ}+Z}(U)$, the result follows from our criterion. ■

We now prove a lemma which together with Theorem 5.11 implies Theorem 5.10.

**Lemma 5.12.** *If the polynomial hierarchy is infinite, then for all $\theta \notin \frac{\pi}{2}\mathbb{Z}$, efficient classical computers can simulate $R_x(\theta)$-conjugated* CZ *circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$ iff they can simulate $R_x(\theta)$-conjugated* CZ $+ Z$ *circuits to within the same multiplicative error.*

*Proof.* By Proposition 3.1, it suffices to prove that for all $\theta \notin \frac{\pi}{2}\mathbb{Z}$, $\mathsf{GadBQP}(\mathcal{S}_{\mathrm{CZ}}(R_x(\theta))) = \mathsf{GadBQP}(\mathcal{S}_{\mathrm{CZ}+Z}(R_x(\theta)))$. It is plain that $\mathsf{GadBQP}(\mathcal{S}_{\mathrm{CZ}}(R_x(\theta))) \subseteq \mathsf{GadBQP}(\mathcal{S}_{\mathrm{CZ}+Z}(R_x(\theta)))$ because every $R_x(\theta)$-conjugated CZ circuit is an $R_x(\theta)$-conjugated $\mathrm{CZ}+Z$ circuit. For the other direction, consider the following gadget over $\mathcal{S}_{\mathrm{CZ}}(R_x(\theta))$:



It is straightforward to show that $\det \mathscr{A}(\mathfrak{g}) = -\frac{1}{4}\sin^4(\theta)$. Therefore, the normalized action $\tilde{\mathscr{A}}(\mathfrak{g})$ exists if $\theta \notin \frac{\pi}{2}\mathbb{Z}$. In this case,

$$\tilde{\mathscr{A}}(\mathfrak{g}) = \begin{pmatrix} i\cos(\theta) & \sin(\theta) \\ -\sin(\theta) & -i\cos(\theta) \end{pmatrix} = iR_x(\theta)ZR_x(-\theta).$$

Consequently, if $\theta \notin \frac{\pi}{2}\mathbb{Z}$, then there exists a gadget over $\mathcal{S}_{\mathrm{CZ}}(R_x(\theta))$ that exactly implements an $R_x(\theta)$-conjugated $Z$ gate (up to the immaterial phase $i$), so every efficient gadget quantum computer over $S_{\mathrm{CZ}+Z}(R_x(\theta))$ can be exactly simulated by an efficient gadget quantum computer over $S_{\mathrm{CZ}}(R_x(\theta))$. This implies $\mathsf{GadBQP}(\mathcal{S}_{\mathrm{CZ}+Z}(R_x(\theta))) \subseteq \mathsf{GadBQP}(\mathcal{S}_{\mathrm{CZ}}(R_x(\theta)))$, as desired. ■

We now prove Theorem 5.10.

*Proof of Theorem 5.10.* Put $U = R_x(\frac{2\pi}{3})$ and suppose that the polynomial hierarchy is infinite. Then, by the proof of Theorem 5.11, no efficient classical computer can simulate $U$-conjugated $\mathrm{CZ}+Z$ circuits to within multiplicative error $\epsilon < \sqrt{2}-1$. Therefore, by Lemma 5.12 and the fact that $\frac{2\pi}{3} \notin \frac{\pi}{2}\mathbb{Z}$, no efficient classical computer can simulate $U$-conjugated CZ circuits to within the same multiplicative error. ■

In Appendix B, we prove the full complexity classification of $U$-conjugated CZ circuits.

**Theorem 5.13.** *If the polynomial hierarchy is infinite, then efficient classical computers can simulate $U$-conjugated* CZ *circuits to within multiplicative error $\epsilon < \sqrt{2}-1$ iff there exists $C \in \langle H, S\rangle$ and $\alpha, \phi, \lambda \in [0, 2\pi)$ such that $U = e^{i\alpha}R_z(\phi)CR_z(\lambda)$.*

Interestingly, in Appendices C and D, respectively, we are also able to prove that this same classification applies to conjugated $\mathrm{CZ}+Z$ circuits and so-called *conjugated* $\mathrm{CZ}+S$ *circuits*, which are defined exactly like conjugated $\mathrm{CZ}+Z$ circuits but with $Z$ replaced by $S$.

**Theorem 5.14.** *If the polynomial hierarchy is infinite, then efficient classical computers can simulate $U$-conjugated* $\mathrm{CZ}+Z$ *circuits to within multiplicative error $\epsilon < \sqrt{2}-1$ iff there exists $C \in \langle H, S\rangle$ and $\alpha, \phi, \lambda \in [0, 2\pi)$ such that $U = e^{i\alpha}R_z(\phi)CR_z(\lambda)$.*

**Theorem 5.15.** *If the polynomial hierarchy is infinite, then efficient classical computers can simulate $U$-conjugated* $\mathrm{CZ}+S$ *circuits to within multiplicative error $\epsilon < \sqrt{2}-1$ iff there exists $C \in \langle H, S\rangle$ and $\alpha, \phi, \lambda \in [0, 2\pi)$ such that $U = e^{i\alpha}R_z(\phi)CR_z(\lambda)$.*

We remark that conjugated $\mathrm{CZ}+S$ circuits are also known as *commuting conjugated Clifford circuits*. Commuting CCCs are a sort of intersection of IQP circuits and CCCs. Given the quantum advantage of both IQP circuits and CCCs, Bouland et al. ask in [BFK18] if commuting

CCCs afford a quantum advantage. Indeed, our Theorem 5.15 not only resolves this question, but it also gives the full complexity classification of commuting CCCs.

In the next section, we study the complexity of CCCs over other subsets of the Clifford group.

5.4. **Conjugated Clifford Fragment Circuits.** In 1941, Emil Post published a complete classification of all the ways in which sets of Boolean logic gates can fail to be universal [Pos41]. In [AGS17], Aaronson, Grier, and Schaeffer describe the ambitious program of doing the same but for all quantum gates. In [GS22], Grier and Schaeffer completed this classification for all Clifford gates assuming an "ancilla rule". They found that any subset of Clifford gates generate one of 57 distinct classes or "fragments" of Clifford operations.

A natural question is if efficient classical computers can simulate CCCs when the interstitial Clifford circuit is restricted to one of these fragments. We call these *conjugated Clifford fragment circuits*, or CCFCs for short. This question was posed by Bouland et al. in their CCC paper [BFK18]. Of the 57 Clifford fragments, there are 30 that are generated by single-qubit gates alone. These are obviously insufficient to afford any sort of quantum advantage because they contain no entangling gates [JL03]. This leaves $57 - 30 = 27$ fragments. The inclusion lattice for the generators of these 27 fragments is shown in Figure 4, which is from [GS22].

In this section, we use our criterion to prove that if the polynomial hierarchy is infinite, then no efficient classical computer can simulate CCFCs to within small multiplicative error for all 27 of the remaining fragments. This resolves the question raised by Bouland et al.

We now define the generators of some of the fragments in Figure 4.

The set $\mathcal{P}$ is the single-qubit Pauli group, i.e., the group generated by the three single-qubit Pauli gates:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \text{and} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Given $P, Q \in \{X, Y, Z\}$, we define a generalized CNOT gate by

$$C(P,Q) \coloneqq \frac{I_1 \otimes I_1 + P \otimes I_1 + I_1 \otimes Q - P \otimes Q}{2},$$

where if the first qubit is in the $+1$ eigenspace of $P$, then $C(P,Q)$ does nothing, but if it is in the $-1$ eigenspace of $P$, then $C(P,Q)$ applies $Q$ to the second qubit. Therefore, $C(Z,Z)$ is CZ. The $R_Z$ gate is the $S$ gate (i.e., a $\pi/2$ rotation about the $\hat{z}$-axis of the Bloch sphere); the $R_X$ and $R_Y$ gates are the same rotation but about the $\hat{x}$- and $\hat{y}$-axes, respectively:

$$R_X = \frac{I_1 - iX}{\sqrt{2}} \quad \text{and} \quad R_Y = \frac{I_1 - iY}{\sqrt{2}}.$$

The $\theta_{X+Z}$ gate is the Hadamard gate (i.e., a $\pi$ rotation about the $(\hat{x} + \hat{z})/\sqrt{2}$ axis of the Bloch sphere); the $\theta_{Y+Z}$ and $\theta_{X+Y}$ gates are the same rotation but about the $(\hat{y} + \hat{z})/\sqrt{2}$- and $(\hat{x} + \hat{y})/\sqrt{2}$-axes, respectively:

$$\theta_{Y+Z} = \frac{Y + Z}{\sqrt{2}} \quad \text{and} \quad \theta_{X+Y} = \frac{X + Y}{\sqrt{2}}.$$

For $P, Q \in \{X, Y, Z\}$, one can analogously define a $\theta_{P-Q}$ gate. In Figure 4, fragments with $\theta_{PQ}$ are fragments that contain both $\theta_{P+Q}$ and $\theta_{P-Q}$.

Finally, for all $k \in \mathbb{N}$, the $\mathrm{T}_{2k}$ gate is such that for every $x = (x_1, x_2, \ldots, x_{2k}) \in \{0,1\}^{2k}$,

$$\mathrm{T}_{2k} \left| x_1, x_2, \ldots, x_{2k} \right\rangle = \left| x_1 \oplus b_x, x_2 \oplus b_x, \ldots, x_{2k} \oplus b_x \right\rangle,$$

where $\oplus$ is addition modulo 2 and $b_x = x_1 \oplus x_2 \oplus \cdots \oplus x_{2k}$. In other words, for computational basis inputs, $\mathrm{T}_{2k}$ outputs the complement of the input when the parity of the input is odd and does nothing when the parity of the input is even. Therefore, $\mathrm{T}_2$ is the SWAP gate, and $\mathrm{T}_4$ maps $|1011\rangle \mapsto |0100\rangle$ and $|1100\rangle \mapsto |1100\rangle$.

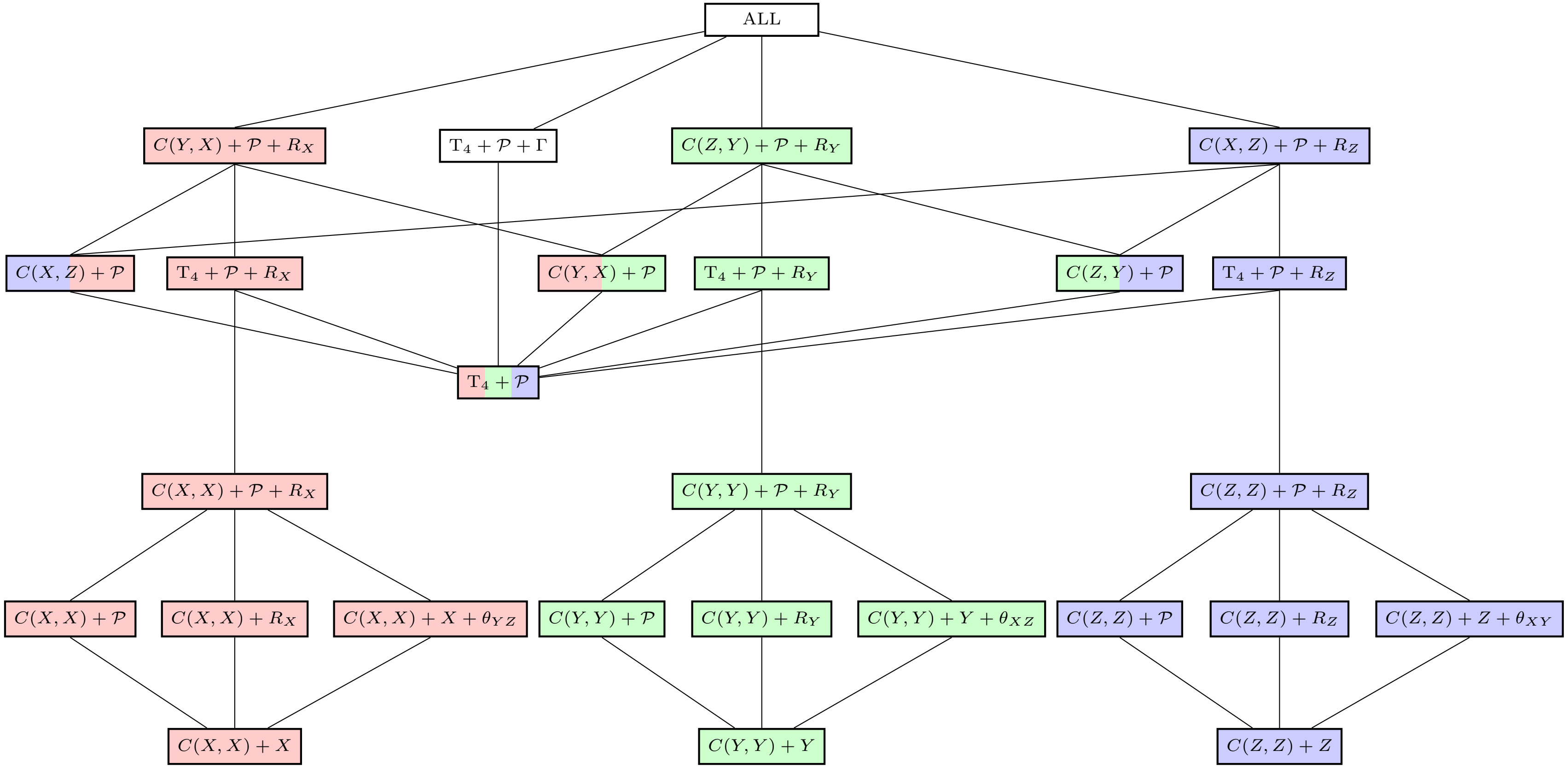


Figure 4. The inclusion lattice of the 27 fragments of the multi-qubit Clifford operations. Here, "ALL" denotes every such Clifford operation, $\Gamma$ is the "vertex rotation" $(I-iX-iY-iZ)/2$, and all other generators are defined in the main text. Red, green, and blue denote $X$-, $Y$-, and $Z$-preserving, respectively. See [GS22] for complete details.

We now formally define the CCFC model. In the following, $\deg(P) = k$ iff $P \in \mathrm{U}(2^k)$.

**Definition 5.5.** Fix $U \in \mathrm{U}(2)$ and let $\mathcal{F}$ be the generators of one of the 27 fragments depicted in Figure 4. A *$U$-conjugated $\mathcal{F}$ circuit* is an efficient quantum computer over the gate set

$$\mathcal{S}_{\mathcal{F}}(U) := \big\{(U^\dagger)^{\otimes \deg(P)} P U^{\otimes \deg(P)} \mid P \in \mathcal{F}\big\}.$$

A *conjugated $\mathcal{F}$ circuit* is a $U$-conjugated $\mathcal{F}$ circuit for some $U \in \mathrm{U}(2)$.

In this section, we prove the following quantum advantage result using our criterion.

**Theorem 5.16.** *If the polynomial hierarchy is infinite, then for all fragments $\mathcal{F}$ in Figure 4, efficient classical computers cannot simulate conjugated $\mathcal{F}$ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$.*

A main ingredient of the proof of Theorem 5.16 is the following hardness result for CCFCs over the $\mathrm{T}_4 + \mathcal{P}$ fragment, which is a special case of Theorem 5.16.

**Theorem 5.17.** *If the polynomial hierarchy is infinite, then efficient classical computers cannot simulate conjugated $\mathrm{T}_4 + \mathcal{P}$ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$.*

We also establish the full complexity classification for the $C(P, P) + R_P$ and $C(P, P) + P$ fragments:

**Theorem 5.18.** *If the polynomial hierarchy is infinite, then for all $P \in \{X, Y, Z\}$, efficient classical computers can simulate $U$-conjugated $C(P, P) + R_P$ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$ iff there exists $C \in \langle H, S\rangle$ and $\alpha, \phi, \lambda \in [0, 2\pi)$ such that:*

*(i) if $P = X$, then $U = e^{i\alpha} H R_z(\phi) C R_z(\lambda)$,*
*(ii) if $P = Y$, then $U = e^{i\alpha} \theta_{Y+Z} R_z(\phi) C R_z(\lambda)$,*
*(iii) if $P = Z$, then $U = e^{i\alpha} R_z(\phi) C R_z(\lambda)$.*

**Theorem 5.19.** *If the polynomial hierarchy is infinite, then for all $P \in \{X, Y, Z\}$, efficient classical computers can simulate $U$-conjugated $C(P, P) + P$ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$ iff there exists $C \in \langle H, S\rangle$ and $\alpha, \phi, \lambda \in [0, 2\pi)$ such that:*

*(i) if $P = X$, then $U = e^{i\alpha} H R_z(\phi) C R_z(\lambda)$,*
*(ii) if $P = Y$, then $U = e^{i\alpha} \theta_{Y+Z} R_z(\phi) C R_z(\lambda)$,*
*(iii) if $P = Z$, then $U = e^{i\alpha} R_z(\phi) C R_z(\lambda)$.*

In fact, in consequence to our complexity classification for conjugated CZ circuits (Theorem 5.13), we can easily obtain a complexity classification for all conjugated $C(P, P)$ circuits, for any $P \in \{X, Y, Z\}$.

**Theorem 5.20.** *If the polynomial hierarchy is infinite, then for all $P \in \{X, Y, Z\}$, efficient classical computers can simulate $U$-conjugated $C(P, P)$ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$ iff there exists $C \in \langle H, S\rangle$ and $\alpha, \phi, \lambda \in [0, 2\pi)$ such that:*

*(i) if $P = X$, then $U = e^{i\alpha} H R_z(\phi) C R_z(\lambda)$,*
*(ii) if $P = Y$, then $U = e^{i\alpha} \theta_{Y+Z} R_z(\phi) C R_z(\lambda)$,*
*(iii) if $P = Z$, then $U = e^{i\alpha} R_z(\phi) C R_z(\lambda)$.*

Since they are simpler, we begin by proving Theorems 5.18 – 5.20.

*Proof of Theorem 5.18.* Conjugated $C(Z, Z) + R_Z$ circuits are exactly the commuting CCC (i.e. conjugated CZ$+S$ circuit) model. Thus, this case follows from Theorem 5.15. For the remaining two fragments $C(X, X) + R_X$ and $C(Y, Y) + R_Y$, simply note that for all $U \in \mathrm{U}(2)$,

$$\mathcal{S}_{C(X,X)+R_X}(HU) = \mathcal{S}_{C(Z,Z)+R_Z}(U) \quad \text{and} \quad \mathcal{S}_{C(Y,Y)+R_Y}(\theta_{Y+Z}U) = \mathcal{S}_{C(Z,Z)+R_Z}(U).$$

Thus, the remaining two cases also follow from Theorem 5.15. ■

The proofs of Theorems 5.19 and 5.20 are analogous to the proof of Theorem 5.18, but instead rely on Theorems 5.14 and 5.13, respectively.

We now prove that it is very likely that CCFCs over any fragment of the Clifford group afford a quantum advantage.

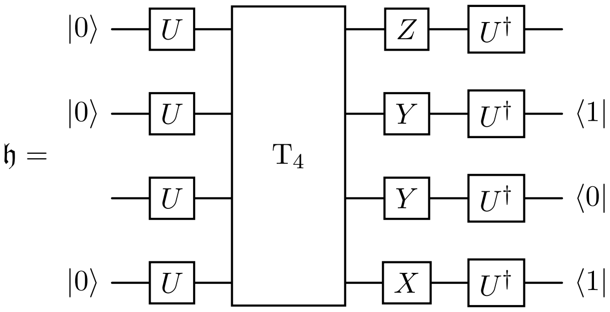
*Proof of Theorem 5.16.* Assuming the polynomial hierarchy is infinite, it suffices to prove that efficient classical computers can neither simulate conjugated $\mathrm{T}_4+\mathcal{P}$ circuits to within multiplicative error $\epsilon < \sqrt{2}-1$ nor can they simulate conjugated $C(P,P)+P$ circuits for any $P \in \{X, Y, Z\}$ to within the same multiplicative error. This suffices, because every fragment in Figure 4 contains either the $\mathrm{T}_4+\mathcal{P}$ fragment or one of the $C(P,P)+P$ fragments. The quantum advantage of the three $C(P,P)+P$ fragments follows from the classification result Theorem 5.19, and the quantum advantage of the $\mathrm{T}_4+\mathcal{P}$ fragment follows from Theorem 5.17. ■

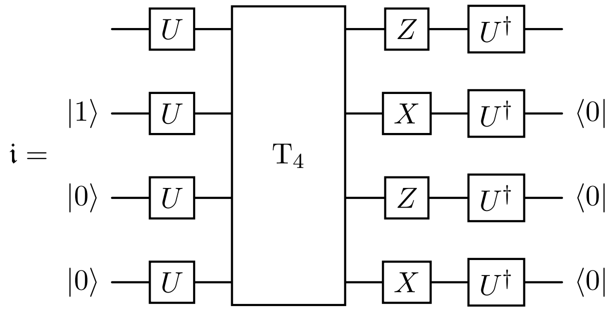
Thus it remains to prove Theorem 5.17.

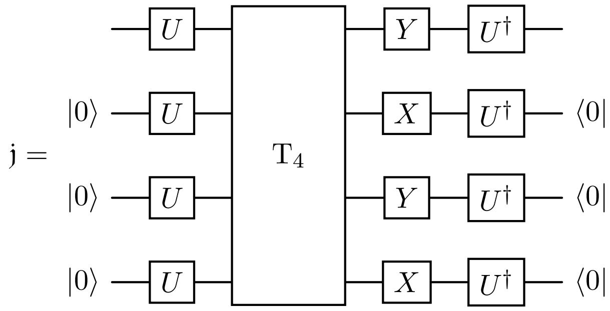
*Proof of Theorem 5.17.* It suffices to exhibit a single-qubit unitary $U$ such that a finite number of post-selection gadgets over $\mathcal{S}_{\mathrm{T}_4+\mathcal{P}}(U)$ have normalized actions that generate a non-elementary, non-discrete, and strictly loxodromic subgroup of $\mathrm{SL}(2;\mathbb{C})$. To this end, let

$$U = TR_x\left(\frac{2\pi}{3}\right) = \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3}i \\ \sqrt{\frac{3}{2}}(1-i) & e^{i\pi/4} \end{pmatrix}$$

and consider the following three 4-to-1 post-selection gadgets:







The normalized action of $\mathfrak{h}$ is the unitary $\mathrm{SL}(2;\mathbb{C})$ matrix

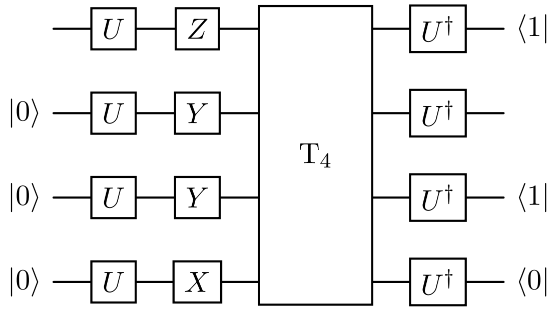
$$H := \tilde{\mathscr{A}}(\mathfrak{h}) = \frac{1}{2\sqrt{2}}\begin{pmatrix} 2-i & \sqrt{3} \\ -\sqrt{3} & 2+i \end{pmatrix},$$

while the normalized actions of $\mathfrak{i}$ and $\mathfrak{j}$ are the *non*-unitary $\mathrm{SL}(2;\mathbb{C})$ matrices

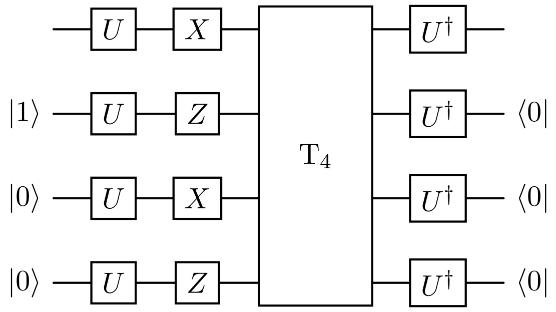
$$I := \tilde{\mathscr{A}}(\mathfrak{i}) = \frac{1}{5}\begin{pmatrix} \sqrt{5}(2-i) & 0 \\ -2-4i & \sqrt{3}(2+i) \end{pmatrix} \quad \text{and} \quad J := \tilde{\mathscr{A}}(\mathfrak{j}) = \frac{1}{10}\begin{pmatrix} -3\sqrt{3}i & -11 \\ 11 & -\frac{7i}{\sqrt{3}} \end{pmatrix}.$$

Inverse gadgets of $\mathfrak{h}$, $\mathfrak{i}$, and $\mathfrak{j}$ are also realizable over $\mathcal{S}_{\mathrm{T}_4+\mathcal{P}}(U)$:

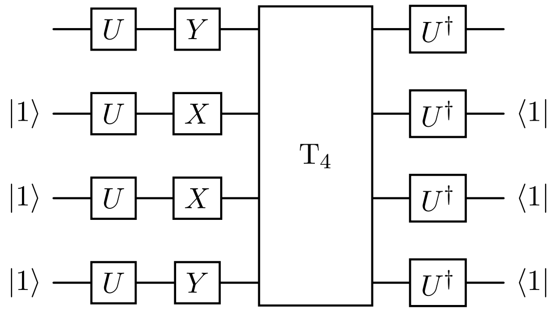
$\mathfrak{h}^{-1} =$



$\mathfrak{i}^{-1} =$



$\mathfrak{j}^{-1} =$



These are inverses of $\mathfrak{h}$, $\mathfrak{i}$, and $\mathfrak{j}$ in the sense of Definition 2.10 because $\tilde{\mathscr{A}}(\mathfrak{h}^{-1}) = -\tilde{\mathscr{A}}(\mathfrak{h})^{-1} = -H^{-1}$, $\tilde{\mathscr{A}}(\mathfrak{i}^{-1}) = \tilde{\mathscr{A}}(\mathfrak{i})^{-1} = I^{-1}$, and $\tilde{\mathscr{A}}(\mathfrak{j}^{-1}) = \tilde{\mathscr{A}}(\mathfrak{j})^{-1} = J^{-1}$.

Now let $\Gamma_{\mathrm{T}_4+\mathcal{P}}(U) \coloneqq \{H, -H^{-1}, I, I^{-1}, J, J^{-1}\}$. Evidently, $\langle\Gamma_{\mathrm{T}_4+\mathcal{P}}(U)\rangle$ is closed under inverses, so $\langle\Gamma_{\mathrm{T}_4+\mathcal{P}}(U)\rangle$ is a subgroup of $\mathrm{SL}(2;\mathbb{C})$. In fact, $\langle\Gamma_{\mathrm{T}_4+\mathcal{P}}(U)\rangle$ is a non-elementary, non-discrete, and strictly loxodromic subgroup of $\mathrm{SL}(2;\mathbb{C})$.

**Claim 5.21.** $\langle\Gamma_{\mathrm{T}_4+\mathcal{P}}(U)\rangle$ *is a non-elementary subgroup of* $\mathrm{SL}(2;\mathbb{C})$.

*Proof.* Since $\beta(H) = -2$, $\beta(I) = -\frac{4}{5}$, and $\gamma(H, I) = -\frac{36}{125} + \frac{48i}{125}$, $\texttt{IsElementary}(\Gamma_{\mathrm{T}_4+\mathcal{P}}(U)) = \texttt{NO}$. ∎

**Claim 5.22.** $\langle\Gamma_{\mathrm{T}_4+\mathcal{P}}(U)\rangle$ *is a non-discrete subgroup of* $\mathrm{SL}(2;\mathbb{C})$.

*Proof.* Since $\mathrm{tr}(HIH^{-1}I^{-1}) = \frac{214}{125} + \frac{48i}{125} \neq 1$ and

$$\left|\mathrm{tr}^2(H) - 2\right| + \left|\mathrm{tr}(HIH^{-1}I^{-1}) - 1\right| = \frac{\sqrt{409}}{25} \approx 0.809 < 1,$$

it follows from line 6 in Algorithm 2 that $\texttt{IsDiscrete}(\Gamma_{\mathrm{T}_4+\mathcal{P}}(U)) = \texttt{NO}$. ∎

**Claim 5.23.** $\langle\Gamma_{\mathrm{T}_4+\mathcal{P}}(U)\rangle$ *is a strictly loxodromic subgroup of* $\mathrm{SL}(2;\mathbb{C})$.

*Proof.* Since $\mathrm{tr}(J) = -\frac{8i}{5\sqrt{3}} \in \mathbb{C}\backslash\mathbb{R}$, $\texttt{IsLoxodromic}(\Gamma_{\mathrm{T}_4+\mathcal{P}}(U)) = \texttt{YES}$. ■

Thus, the quantum advantage of conjugated $\mathrm{T}_4 + \mathcal{P}$ circuits follows from our criterion Theorem 3.5. ■

A natural problem is to complete the complexity classification of CCFS for every fragment, such as conjugated $\mathrm{T}_4 + \mathcal{P}$ circuits.

## 6. Discussion

In this work, we have established a criterion (Theorem 3.5) for testing if an efficient quantum computer over a non-universal gate set $\mathcal{S}$ can perform a sampling task that no efficient classical computer can, assuming standard complexity assumptions. In particular, we showed that if there exist a finite number of post-selection gadgets over $\mathcal{S}$ whose normalized actions generate a non-elementary, non-discrete, and strictly loxodromic subgroup of $\mathrm{SL}(2;\mathbb{C})$, then efficient classical computers cannot simulate efficient quantum computers over $\mathcal{S}$, assuming the polynomial hierarchy is infinite. We also demonstrated that this criterion is "simple" in the sense that there is a straightforward algorithm for checking if the normalized gadget actions generate a non-elementary, non-discrete, and strictly loxodromic subgroup of $\mathrm{SL}(2;\mathbb{C})$. That said, we acknowledge that there is no obvious, systematic way to find the gadgets to use in our criterion. On the other hand, our approach is simple enough that for "small" $j$, one can conceivably automate the search for the $j$-to-1 post-selection gadgets to use in our criterion.

Using our criterion, we reproduced the well-known quantum advantage results that IQP circuits and CCCs can perform a sampling task that no efficient classical computer can, assuming the polynomial hierarchy is infinite [BJS11, BFK18]. We also proved that commuting CCCs and CCCs over every multi-qubit fragment of the Cliffford group (as classified in [GS22]) can similarly perform a sampling task that no efficient classical computer can, again assuming the polynomial hierarchy is infinite. For CCCs, CCCs over $C(P,P)$, and CCCs over the $C(P,P)+P$ and $C(P,P)+R_P$ fragments, we proved the full complexity classification (Appendices A, B, C, and D, respectively).

Our results for commuting CCCs and CCCs over the various fragments of the Clifford group resolve two open questions that were raised by Bouland et al. in [BFK18]. We attribute our ability to address these questions to the historical fact that the "standard" approach for showing classical intractability in the weak multiplicative sense is via *unitary* gadget injection. On the other hand, the quantum advantage of commuting CCCs and CCCs over the various Clifford fragments follow from the group theory of $\mathrm{SL}(2;\mathbb{C})$, and hence via *non*-unitary gadget injection. Incidentally, non-unitary gadget injection was also used to prove a quantum advantage result for two-qubit commuting Hamiltonians [BMZ16].

Our results lead to many natural open questions. First, throughout this paper we have assumed that the set of normalized gadget actions $\Gamma$ contains only the actions of normalizable $j$-to-1 gadgets for any $j$. The reason, of course, is because such gadgets have actions in $\mathrm{SL}(2;\mathbb{C})$. Consequently, the group theory of $\mathrm{SL}(2;\mathbb{C})$ can be used to infer their effect on quantum computation. However, at least on the surface, we see no substantive reason why more general $j$-to-$k$ gadgets cannot be used, save the epistemological fact that the group theory of $\mathrm{SL}(2^k;\mathbb{C})$ is not nearly as understood as the group theory of $\mathrm{SL}(2;\mathbb{C})$. In this regard, we wonder if there are statements similar to our criterion, but for more general $j$-to-$k$ post-selection gadgets.

A separate question has to do with the existence of inverse gadgets. As it stands, our criterion only works if there is an inverse of every gadget used. Of course, this is necessary for $\langle\Gamma\rangle$ to be a subgroup of $\mathrm{SL}(2;\mathbb{C})$. In Section 5, we guarantee this by explicitly finding an inverse of each gadget. However, this approach does not easily scale. A means of improving our results, therefore, is to show that every $j$-to-$k$ post-selection gadget has an inverse. This way, any finite subset $\Gamma \subset \mathrm{gad}_k(\mathcal{S})$ implies another finite subset $\Gamma' \subset \mathrm{gad}_k(\mathcal{S})$ such that $\Gamma \subseteq \Gamma'$ and $\langle \Gamma' \rangle$ is a subgroup of $\mathrm{SL}(2;\mathbb{C})$. If this is right, then one could assume without loss of generality that $\langle \Gamma \rangle$ is always closed under inverses and hence that $\langle \Gamma \rangle$ is always a subgroup of $\mathrm{SL}(2;\mathbb{C})$. Indeed, we conjecture this to be true:

**Conjecture 6.1** (Existence of inverse gadgets)**.** *Let $\mathcal{S}$ be a gate set. For all $j$-to-$k$ post-selection gadgets $\mathfrak{g} = \mathfrak{g}_{j,k}$ over $\mathcal{S}$ for which $\det \mathscr{A}(\mathfrak{g}) \neq 0$, there exists a $j'$-to-$k$ post-selection gadget $\mathfrak{g}^{-1} = \mathfrak{g}_{j',k}$ over $\mathcal{S}$ such that $\mathscr{A}(\mathfrak{g})^{-1} \in \langle \mathscr{A}(\mathfrak{g}), \mathscr{A}(\mathfrak{g}^{-1}) \rangle$.*[8]

Another question concerns the need for strict loxodromy in Theorem 3.5. Recall that demanding that $\Gamma \subset \mathrm{gad}_1(\mathcal{S})$ generate a strictly loxodromic subgroup $H = \langle \Gamma \rangle$ of $\mathrm{SL}(2;\mathbb{C})$ forced $H$ to be dense in $\mathrm{SL}(2;\mathbb{C})$ by Sullivan's Theorem 4.9. This, in turn, implies $\mathsf{GadBQP}(\mathcal{S}) = \mathsf{PostBQP}$. Technically, however, $H$ need not be dense in $\mathrm{SL}(2;\mathbb{C})$ for $\mathsf{GadBQP}(\mathcal{S}) = \mathsf{PostBQP}$. This holds, for example, if $H$ is dense in $\mathrm{SU}(2)$ or if $H$ is dense in $\mathrm{SL}(2;\mathbb{R})$ and the entangling gate in $\mathcal{S}$ is a real matrix [BV93, McK13] (in which case one must also appeal to an $\mathrm{SL}(2;\mathbb{R})$ analogue of the Solovay-Kitaev theorem [AAEL07]). With this intuition, we suspect that as long as $H$ is conjugate to a dense subgroup of $\mathrm{SL}(2;\mathbb{R})$, then $\mathsf{GadBQP}(\mathcal{S}) = \mathsf{PostBQP}$.

**Conjecture 6.2** (Irrelevance of strict loxodromy)**.** *Let $\mathcal{S}$ be a gate set. If there exists a finite subset $\Gamma \subset \mathrm{gad}_1(\mathcal{S})$ such that $\langle \Gamma \rangle$ is conjugate to a dense subgroup of $\mathrm{SL}(2;\mathbb{R})$, then $\mathsf{GadBQP}(\mathcal{S}) = \mathsf{PostBQP}$.*

If this conjecture is right, then we extirpate the need for strict loxodromy in Theorem 3.5 and thereby obtain a stronger criterion for quantum advantage:

**Theorem 6.3.** *Let $\mathcal{S}$ be a gate set and suppose Conjecture 6.2 and that the polynomial hierarchy is infinite. If there exists a finite subset $\Gamma \subset \mathrm{gad}_1(\mathcal{S})$ such that $\langle \Gamma \rangle$ is a non-elementary and non-discrete subgroup of $\mathrm{SL}(2;\mathbb{C})$, then efficient classical computers cannot simulate efficient quantum computers over $\mathcal{S}$ to within multiplicative error $\epsilon < \sqrt{2} - 1$.*

We close with a series of unrelated questions that we think are interesting:

- Are there any non-trivial *necessary* conditions, perhaps in the form of alternative algorithms for `IsElementary` and `IsDiscrete`, for a gate set $\mathcal{S}$ to satisfy $\mathsf{GadBQP}(\mathcal{S}) = \mathsf{PostBQP}$?
- Assuming $\mathsf{PostBPP} \neq \mathsf{PostBQP}$, is there a non-universal gate set $\mathcal{S}$ for which $\mathsf{PostBPP} \subsetneq \mathsf{PostBQP}(\mathcal{S}) \subsetneq \mathsf{PostBQP}$?
- For which $U \in \mathrm{U}(2)$ are $U$-CCCs over the $\mathrm{T}_4{+}\mathcal{P}$ fragment of the Clifford group efficiently classically simulable (assuming the polynomial hierarchy is infinite)? What about for the other unclassified Clifford fragments?

We hope our work inspires more research in these directions.

**Acknowledgements.** C.K. and M.F. thank the organizers and participants of the 2024 "Foundations of Quantum Advantage" conference at the Perimeter Institute, which is where work on this paper began. The authors thank Adam Bouland for substantive comments on an earlier draft of this paper and Luke Schaeffer for helpful discussions

Research at Perimeter Institute is supported in part by the Government of Canada through the Department of Innovation, Science and Economic Development Canada and by the Province of Ontario through the Ministry of Colleges and Universities.

[8] Perhaps this is only true when $\mathcal{S}$ itself is closed under inverses.

## Appendix A. Proof of Theorem 5.6

In this section, we reproduce the complexity classification of $U$-CCCs, which was originally done in [BFK18]. Formally, this is our Theorem 5.6, which we restate below for convenience.

**Theorem 5.6** (Theorem 3.2 in [BFK18])**.** *If the polynomial hierarchy is infinite, then efficient classical computers can simulate $U$-CCCs to within multiplicative error $\epsilon < \sqrt{2}-1$ iff there exists $C \in \langle H, S\rangle$ and $\alpha, \lambda \in [0, 2\pi)$ such that $U = e^{i\alpha} C R_z(\lambda)$.*

The proof follows from two lemmas, the second of which depends on Theorem 5.14, the complexity classification of conjugated $\mathrm{CZ} + Z$ circuits.

**Lemma A.1.** *Let $U$ and $V$ be single-qubit unitaries such that $U = e^{i\alpha} CVR_z(\lambda)$ for $C \in \langle H, S\rangle$ and $\alpha, \lambda \in [0, 2\pi)$. Then, $U$-CCCs are efficiently classically simulable to within multiplicative error $\epsilon < \sqrt{2}-1$ iff $V$-CCCs are.*

**Lemma A.2.** *If the polynomial hierarchy is infinite, then efficient classical computers can simulate $R_z(\phi)R_x(\theta)$-CCCs to within multiplicative error $\epsilon < \sqrt{2}-1$ iff either $\phi \in \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}$, or $\theta \in \pi\mathbb{Z}$.*

*Proof of Theorem 5.6.* Suppose $U = e^{i\alpha} C R_z(\lambda)$ for $C \in \langle H, S\rangle$ and $\alpha, \lambda \in [0, 2\pi)$. Then, by Lemma A.1, $U$-CCCs are efficiently classically simulable to within mulpitlicative error $\epsilon$ iff $I_1$-CCCs are. But $I_1$-CCCs are Clifford circuits, which are exactly simulable by the Gottesman-Knill theorem.

Now suppose that $U$-CCCs are efficiently classically simulable to within multiplicative error $\epsilon < \sqrt{2}-1$, and let $U = e^{i\alpha} R_z(\phi)R_x(\theta)R_z(\lambda)$ be the Euler decomposition of $U$. By Lemmas A.1 and A.2, $U$-CCCs are efficiently classically simulable to within multiplicative error $\epsilon$ iff $R_z(\phi)R_x(\theta)$-CCCs are iff either $\phi \in \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}$, or $\theta \in \pi\mathbb{Z}$. In both cases, it is easy to verify that $R_z(\phi)R_x(\theta) = e^{i\alpha'} C R_z(\lambda')$ for some $C \in \langle H, S\rangle$ and $\alpha', \lambda' \in [0, 2\pi)$. Therefore, $U = e^{i\alpha+\alpha'} C R_z(\lambda + \lambda')$, which is the desired form. ■

Thus, it remains to prove Lemmas A.1 and A.2. While the proof of Lemma A.1 is straightforward, the proof of Lemma A.2 is rather involved. Note that in this and the next section, we often write $U \sim V$ for any $U, V \in \mathrm{U}(2)$ that are related by $U = e^{i\alpha} V$ for some $\alpha \in [0, 2\pi)$.

*Proof of Lemma A.1.* Let $Q$ be an $n$-qubit circuit over $\mathcal{S}_{\mathrm{CCC}}(U)$ where, by assumption, $U = e^{i\alpha} CVR_z(\lambda)$ for some $V \in \mathrm{U}(2)$, $C \in \langle H, S\rangle$, and $\alpha, \lambda \in [0, 2\pi)$. Then, $Q = (U^\dagger)^{\otimes n} E U^{\otimes n}$ for some $n$-qubit Clifford circuit $E$. Since $C \in \langle H, S\rangle$, $E' = (C^\dagger)^{\otimes n} E C^{\otimes n}$ is an $n$-qubit Clifford circuit. Therefore, $e^{i\alpha} CVR_z(\lambda)$-CCCs are efficiently classically simulable to within multiplicative error $\epsilon$ iff $e^{i\alpha} VR_z(\lambda)$-CCCs are. Finally, since for all $x, y \in \{0,1\}^n$,

$$\left|\langle y| \left(e^{-i\alpha} R_z(-\lambda) V^\dagger\right)^{\otimes n} E' \left(e^{i\alpha} V R_z(\lambda)\right)^{\otimes n} |x\rangle\right|^2 = \left|\langle y| (V^\dagger)^{\otimes n} E' V^{\otimes n} |x\rangle\right|^2,$$

it holds that $e^{i\alpha} VR_z(\lambda)$-CCCs are efficiently classically simulable to within multiplicative error $\epsilon$ iff $V$-CCCs are. ■

*Proof of Lemma A.2.* We break the proof up into three claims:

**Claim A.3.** *If either $\phi \in \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}$, or $\theta \in \pi\mathbb{Z}$, then efficient classical computers can simulate $R_z(\phi)R_x(\theta)$-CCCs to within multiplicative error $\epsilon < \sqrt{2}-1$.*

**Claim A.4.** *Suppose the polynomial hierarchy is infinite. If $\theta \notin \frac{\pi}{2}\mathbb{Z}$, then efficient classical computers cannot simulate $R_z(\phi)R_x(\theta)$-CCCs to within multiplicative error $\epsilon < \sqrt{2}-1$.*

**Claim A.5.** *Suppose the polynomial hierarchy is infinite. If $\phi \notin \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}_{\text{odd}}$, then efficient classical computers cannot simulate $R_z(\phi)R_x(\theta)$-CCCs to within multiplicative error $\epsilon < \sqrt{2}-1$.*

Indeed, together these claims imply the lemma, because Claim A.3 implies the forward direction, while the contrapositive of Claims A.4 and A.5 imply the latter direction (namely, supposing that the polynomial hierarchy is infinite, if efficient classical computers can simulate $R_z(\phi)R_x(\theta)$-CCCs to within multiplicative error $\epsilon < \sqrt{2}-1$, then either $\phi \in \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}_{\text{odd}} \subset \frac{\pi}{2}\mathbb{Z}$, or $\theta \in \frac{\pi}{2}\mathbb{Z}_{\text{even}} = \pi\mathbb{Z}$).

*Proof of Claim A.3.* If $\phi \in \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}$, then $R_z(\phi)R_x(\theta)$ is a Clifford gate. Therefore, $R_z(\phi)R_x(\theta)$-CCCs are exactly simulable by the Gottesman-Knill theorem. If $\theta \in \pi\mathbb{Z}$, then either $\theta \in 2\pi\mathbb{Z}$ or $\theta \in \pi\mathbb{Z}_{\text{odd}}$. If $\theta \in 2\pi\mathbb{Z}$, then $R_x(\theta) \sim I_1$, so $R_z(\phi)R_x(\theta)$-CCCs are exactly simulable by combining Lemma A.1 and the Gottesman-Knill theorem. If $\theta \in \pi\mathbb{Z}_{\text{odd}}$, then $R_x(\phi) \sim X$, so $R_z(\phi)R_x(\theta) \sim R_z(\phi)X = XR_z(-\phi)$. By Lemma A.1, $XR_z(-\phi)$-CCCs are efficiently classically simulable to within multiplicative error $\epsilon$ iff $X$-CCCs are. But $X$ is a Clifford gate, so $X$-CCCs are exactly simulable by the Gottesman-Knill theorem. ■

*Proof of Claim A.4.* For all $\phi \in [0, 2\pi)$, if $\theta \notin \frac{\pi}{2}\mathbb{Z}$, then by Theorem 5.14 (whose proof is in Appendix C), efficient classical computers cannot simulate $R_z(\phi)R_x(\theta)$-conjugated CZ + $Z$ circuits to within multiplicative error $\epsilon < \sqrt{2}-1$. Therefore, efficient classical computers cannot simulate $R_z(\phi)R_x(\theta)$-CCCs to within the same multiplicative error. ■

*Proof of Claim A.5.* If $\theta \in \frac{\pi}{2}\mathbb{Z}_{\text{odd}}$, then, up to a global phase, $R_x(\theta)$ is either $HSH$ or $HS^\dagger H$. In this proof we suppose $R_x(\theta) \sim HSH$, but an analogous argument works for the other case. Since $S \sim R_z(\frac{\pi}{2})$ and, more generally, $R_z(\phi) \sim R_z(\phi - \frac{\pi}{2})S$, it follows from Lemma A.1 that $R_z(\phi)R_x(\theta)$-CCCs are efficiently classically simulable to within multiplicative error $\epsilon < \sqrt{2}-1$ iff $R_z(\phi - \frac{\pi}{2})SR_x(\theta)S$-CCCs are. Because $R_x(\theta) \sim HSH$ and $SHSHS \sim H$, we have that $R_z(\phi - \frac{\pi}{2})SR_x(\theta)S$-CCCs are efficiently classically simulable to within multiplicative error $\epsilon$ iff $R_z(\phi - \frac{\pi}{2})H$-CCCs are. Finally, by Lemma A.1, $R_z(\phi - \frac{\pi}{2})H$-CCCs are efficiently classically simulable to within multiplicative error $\epsilon$ iff $HR_z(\phi - \frac{\pi}{2})H$-CCCs are. But $HR_z(\phi - \frac{\pi}{2})H = R_x(\phi - \frac{\pi}{2})$, so $R_z(\phi - \frac{\pi}{2})H$-CCCs are efficiently classically simulable to within multiplicative error $\epsilon$ iff $R_x(\phi - \frac{\pi}{2})$-CCCs are. Since $\phi \notin \frac{\pi}{2}\mathbb{Z}$, $\phi - \frac{\pi}{2} \notin \frac{\pi}{2}\mathbb{Z}$. Therefore, by Theorem 5.14, efficient classical computers cannot simulate $R_x(\phi - \frac{\pi}{2})$-conjugated CZ+$Z$ circuits to within multiplicative error $\epsilon < \sqrt{2}-1$. Therefore, efficient classical computers cannot simulate $R_x(\phi - \frac{\pi}{2})$-CCCs to within the same multiplicative error. ■

Altogether, Claims A.3 – A.5 complete the proof. ■

## Appendix B. Proof of Theorem 5.13

In this section, we classify the complexity of $U$-conjugated CZ circuits. Formally, this is our Theorem 5.13, which we restate below for convenience.

**Theorem 5.13.** *If the polynomial hierarchy is infinite, then efficient classical computers can simulate $U$-conjugated* CZ *circuits to within multiplicative error $\epsilon < \sqrt{2}-1$ iff there exists $C \in \langle H, S\rangle$ and $\alpha, \phi, \lambda \in [0, 2\pi)$ such that $U = e^{i\alpha}R_z(\phi)CR_z(\lambda)$.*

Our method of proof is to show that for all $U \in \mathrm{U}(2)$, $U$-conjugated CZ circuits are efficiently classically simuilable iff $U$-conjugated CZ + $Z$ circuits are, thereby reducing the problem to finding the complexity classification of $U$-conjugated CZ+$Z$ circuits, which we do in Appendix C. To show this reduction, we rely on Lemma 5.12 and the following lemma.

**Lemma B.1.** *Let $U$ and $V$ be single-qubit unitaries such that $U = e^{i\alpha} R_z(\phi) V R_z(\lambda)$ for $\alpha, \phi, \lambda \in [0, 2\pi)$. Then, $U$-conjugated $\mathrm{CZ} + Z$ circuits are efficiently classically simulable to within multiplicative error $\epsilon < \sqrt{2} - 1$ iff $V$-conjugated $\mathrm{CZ} + Z$ circuits are.*

*Proof.* Let $Q$ be an $n$-qubit circuit over $\mathcal{S}_{\mathrm{CZ}+Z}(U)$ where, by assumption, $U = e^{i\alpha} R_z(\phi) V R_z(\lambda)$ for some $V \in \mathrm{U}(2)$. Then, $Q = (U^\dagger)^{\otimes n} D U^{\otimes n}$ for some $n$-qubit circuit $D$ that is diagonal in the computational basis. Consequently, $R_z(-\phi)^{\otimes n} D R_z(\phi)^{\otimes n} = D$, so $e^{i\alpha} R_z(\phi) V R_z(\lambda)$-conjugated $\mathrm{CZ} + Z$ circuits are efficiently classically simulable to within multiplicative error $\epsilon$ iff $e^{i\alpha} V R_z(\lambda)$-conjugated $\mathrm{CZ} + Z$ circuits are. Finally, since for all $x, y \in \{0,1\}^n$,

$$\left| \langle y| \, (e^{-i\alpha} R_z(-\lambda) V^\dagger)^{\otimes n} D (e^{i\alpha} V R_z(\lambda))^{\otimes n} \, |x\rangle \right|^2 = \left| \langle y| \, (V^\dagger)^{\otimes n} D V^{\otimes n} \, |x\rangle \right|^2,$$

it holds that $e^{i\alpha} V R_z(\lambda)$-conjugated $\mathrm{CZ} + Z$ circuits are efficiently classically simulable to within multiplicative error $\epsilon$ iff $V$-conjugated $\mathrm{CZ} + Z$ circuits are. ■

We now prove that the complexity classifications of conjugated CZ circuits and conjugated $\mathrm{CZ} + Z$ circuits are the same. Consequently, Theorem 5.13 follows from Theorem 5.14, which is proved in Appendix C.

**Lemma B.2.** *If the polynomial hierarchy is infinite, then for all $U \in \mathrm{U}(2)$, efficient classical computers can simulate $U$-conjugated $\mathrm{CZ} + Z$ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$ iff efficient classical computers can simulate $U$-conjugated CZ circuits to within the same multiplicative error.*

*Proof.* The forward direction is trivial, because every $U$-conjugated CZ circuit is a $U$-conjugated $\mathrm{CZ} + Z$ circuit. Now suppose efficient classical computers can simulate $U$-conjugated CZ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$, and let $U = e^{i\alpha} R_z(\phi) R_x(\theta) R_z(\lambda)$ be the Euler decomposition of $U$. Then, by Lemma B.1, efficient classical computers can simulate $U$-conjugated $\mathrm{CZ} + Z$ circuits to within multiplicative error $\epsilon$ iff they can simulate $R_x(\theta)$-conjugated $\mathrm{CZ} + Z$ circuits. If $\theta \in \frac{\pi}{2}\mathbb{Z}$, then $R_x(\theta) \in \langle H, S \rangle$, so every $R_x(\theta)$-conjugated $\mathrm{CZ} + Z$ circuit and every $R_x(\theta)$-conjugated CZ circuit is a Clifford circuit, so both types are exactly simulable by the Gottesman-Knill theorem. If $\theta \notin \frac{\pi}{2}\mathbb{Z}$, then by Lemma 5.12, efficient classical computers can simulate $R_x(\theta)$-conjugated $\mathrm{CZ} + Z$ circuits to within multiplicative error $\epsilon$ iff they can simulate $R_x(\theta)$-conjugated CZ circuits to within the same multiplicative error. ■

## Appendix C. Proof of Theorem 5.14

In this section, we classify the complexity of $U$-conjugated $\mathrm{CZ} + Z$ circuits. Formally, this is our Theorem 5.14, which we restate below for convenience.

**Theorem 5.14.** *If the polynomial hierarchy is infinite, then efficient classical computers can simulate $U$-conjugated $\mathrm{CZ} + Z$ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$ iff there exists $C \in \langle H, S \rangle$ and $\alpha, \phi, \lambda \in [0, 2\pi)$ such that $U = e^{i\alpha} R_z(\phi) C R_z(\lambda)$.*

The proof follows from Lemma B.1 and the following lemma.

**Lemma C.1.** *If the polynomial hierarchy is infinite, then efficient classical computers can simulate $R_x(\theta)$-conjugated $\mathrm{CZ} + Z$ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$ iff $\theta \in \frac{\pi}{2}\mathbb{Z}$.*

*Proof of Theorem 5.14.* Suppose $U = e^{i\alpha} R_z(\phi) C R_z(\lambda)$ for $C \in \langle H, S \rangle$ and $\alpha, \phi, \lambda \in [0, 2\pi)$. Then, by Lemma B.1, $U$-conjugated $\mathrm{CZ} + Z$ circuits are efficiently classically simulable to within multiplicative error $\epsilon$ iff $C$-conjugated $\mathrm{CZ} + Z$ circuits are. But $C$ is a Clifford operation, so $C$-conjugated $\mathrm{CZ} + Z$ circuits are exactly simulable by the Gottesman-Knill theorem.

Now suppose that $U$-conjugated $\mathrm{CZ}+Z$ circuits are efficiently classically simulable to within multiplicative error $\epsilon < \sqrt{2}-1$, and let $U = e^{i\alpha}R_z(\phi)R_x(\theta)R_z(\lambda)$ be the Euler decomposition of $U$. By Lemmas B.1 and C.1, $U$-conjugated $\mathrm{CZ}+Z$ circuits are efficiently classically simulable to within multiplicative error $\epsilon$ iff $R_x(\theta)$-conjugated $\mathrm{CZ}+Z$ circuits are iff $\theta \in \frac{\pi}{2}\mathbb{Z}$. Therefore, $R_x(\theta) \in \langle H, S\rangle$, so $U = e^{i\alpha}R_z(\phi)CR_z(\lambda)$ for $C = R_x(\theta) \in \langle H, S\rangle$, as desired. ■

Thus, it remains to prove Lemma C.1. While the proof uses our criterion, it is rather involved because it is arithmetically tedious. Because of this, we made extensive use of Wolfram Mathematica 14.1. Our notebook is available online [KFG24].

*Proof of Lemma C.1.* Suppose $\theta \in \frac{\pi}{2}\mathbb{Z}$. Then, $R_x(\theta) \in \langle H, S\rangle$, so the $R_x(\theta)$-conjugated $\mathrm{CZ}+Z$ circuit is a Clifford circuit and is therefore exactly simulable by the Gottesman-Knill theorem.

Now suppose $\theta \notin \frac{\pi}{2}\mathbb{Z}$. We will show that efficient classical computers cannot simulate $R_x(\theta)$-conjugated $\mathrm{CZ}+Z$ circuits to within multiplicative error $\epsilon < \sqrt{2}-1$ unless the polynomial hierarchy collapses. To this end, it suffices to exhibit a finite number of post-selection gadgets over $\mathcal{S}_{\mathrm{CZ}+Z}(R_x(\theta))$ such that their normalized actions generate a non-elementary, non-discrete, and strictly loxodromic subgroup of $\mathrm{SL}(2;\mathbb{C})$. The gadgets and their inverses are presented in Table 1. The determinants of the actions of these gadgets are:

$$\begin{aligned}
\det \mathscr{A}(\mathfrak{c}_0) &= \det \mathscr{A}(\mathfrak{c}_0^{-1}) = \frac{\sin^4(\theta)}{4}\\
\det \mathscr{A}(\mathfrak{c}_1) &= \det \mathscr{A}(\mathfrak{c}_1^{-1}) = \frac{1}{32}\left(5 - 28\cos(\theta) - 4\cos(2\theta) - 4\cos(3\theta) - \cos(4\theta)\right)\\
\det \mathscr{A}(\mathfrak{c}_2) &= \det \mathscr{A}(\mathfrak{c}_2^{-1}) = \frac{1}{32}\left(5 + 28\cos(\theta) - 4\cos(2\theta) + 4\cos(3\theta) - \cos(4\theta)\right)\\
\det \mathscr{A}(\mathfrak{c}_3) &= \det \mathscr{A}(\mathfrak{c}_3^{-1}) = \cos(\theta)\\
\det \mathscr{A}(\mathfrak{c}_4) &= \det \mathscr{A}(\mathfrak{c}_4^{-1}) = -\cos(\theta).
\end{aligned}$$

Evidently, if $\theta \notin \frac{\pi}{2}\mathbb{Z}$, then $\det \mathscr{A}(\mathfrak{c}_i) \neq 0$ for $i \in \{0,3,4\}$, so the *normalized* actions of $\mathfrak{c}_0$, $\mathfrak{c}_3$, and $\mathfrak{c}_4$ exist for such $\theta$. They are:

$$\begin{aligned}
C_0 &:= \tilde{\mathscr{A}}(\mathfrak{c}_0) = \frac{1}{4}\begin{pmatrix} (-\cos(\theta) + 2\cos(2\theta) + \cos(3\theta) + 6)\csc^2(\theta) & \frac{4i\sin(\theta)\cos(\theta)}{\cos(\theta)-1} \\ 2i\sin(\theta)\cos(\theta)\csc^2\left(\frac{\theta}{2}\right) & 4(\cos(\theta)+1) \end{pmatrix}\\
C_3 &:= \tilde{\mathscr{A}}(\mathfrak{c}_3) = \frac{1}{\sqrt{\cos(\theta)}}\begin{pmatrix} \frac{1}{4}(\cos(2\theta)+3) & i\sin^2\left(\frac{\theta}{2}\right)\sin(\theta) \\ -i\sin^2\left(\frac{\theta}{2}\right)\sin(\theta) & \frac{1}{2}\left(\sin^2(\theta) + 2\cos(\theta)\right) \end{pmatrix}\\
C_4 &:= \tilde{\mathscr{A}}(\mathfrak{c}_4) = \frac{\sqrt{-\cos(\theta)}}{2}\begin{pmatrix} -\frac{1}{2}(\cos(2\theta)+3)\sec(\theta) & i(\sin(\theta)+\tan(\theta)) \\ -i(\sin(\theta)+\tan(\theta)) & \frac{1}{2}(4\cos(\theta)+\cos(2\theta)-1)\sec(\theta) \end{pmatrix}.
\end{aligned}$$

However, since $\det \mathscr{A}(\mathfrak{c}_1) = 0$ iff $\theta \in 2\pi\mathbb{Z} \pm 2\tan^{-1}\left(\sqrt{\sqrt{2}-1}\right)$ and $\det \mathscr{A}(\mathfrak{c}_2) = 0$ iff $\theta \in 2\pi\mathbb{Z} \pm 2\tan^{-1}\left(\sqrt{\sqrt{2}+1}\right)$, we will proceed on a case-by-case basis. To do this, we partition $[0, 2\pi)$ into the two disjoint intervals $A := (\frac{\pi}{2}, \frac{3\pi}{2})$ and $B := [0, \frac{\pi}{2}] \cup [\frac{3\pi}{2}, 2\pi)$ and prove the lemma in each interval.

If $\theta \in A$, then $\det \mathscr{A}(\mathfrak{c}_1) \neq 0$, so the normalized of action of $\mathfrak{c}_1$ exists for such $\theta$. It is:

$$C_1 := \tilde{\mathscr{A}}(\mathfrak{c}_1) = \frac{\mathscr{A}(\mathfrak{c}_1)}{\sqrt{\det \mathscr{A}(\mathfrak{c}_1)}},$$

where

$$\mathscr{A}(\mathfrak{c}_1) = \frac{1}{8}\begin{pmatrix} -\cos(\theta) + 2\cos(2\theta) + \cos(3\theta) + 6 & -i(\sin(\theta) + 2\sin(2\theta) + \sin(3\theta)) \\ i(\sin(\theta) + 2\sin(2\theta) + \sin(3\theta)) & -7\cos(\theta) - 2\cos(2\theta) - \cos(3\theta) + 2 \end{pmatrix}.$$

Similarly, if $\theta \in B$, then $\det \mathscr{A}(\mathfrak{c}_2) \neq 0$, so the normalized action of $\mathfrak{c}_2$ exists for such $\theta$. It is:

$$C_2 := \tilde{\mathscr{A}}(\mathfrak{c}_2) = \frac{\mathscr{A}(\mathfrak{c}_2)}{\sqrt{\det \mathscr{A}(\mathfrak{c}_2)}},$$

where

$$\mathscr{A}(\mathfrak{c}_2) = \frac{1}{8}\begin{pmatrix} 7\cos(\theta) - 2\cos(2\theta) + \cos(3\theta) + 2 & -i(\sin(\theta) - 2\sin(2\theta) + \sin(3\theta)) \\ -8i\sin^2\left(\frac{\theta}{2}\right)\sin(\theta)\cos(\theta) & \cos(\theta) + 2\cos(2\theta) - \cos(3\theta) + 6 \end{pmatrix}.$$

We underscore that for all values of $\theta$ where the normalized action of $\mathfrak{c}_i$ is defined, the gadget $\mathfrak{c}_i^{-1}$ given in Table 1 is also defined and an inverse of $\mathfrak{c}_i$:

$$\begin{aligned}
\tilde{\mathscr{A}}(\mathfrak{c}_0^{-1}) &= \tilde{\mathscr{A}}(\mathfrak{c}_0)^{-1} = C_0^{-1} \\
\tilde{\mathscr{A}}(\mathfrak{c}_1^{-1}) &= \tilde{\mathscr{A}}(\mathfrak{c}_1)^{-1} = C_1^{-1} \\
-\tilde{\mathscr{A}}(\mathfrak{c}_2^{-1}) &= \tilde{\mathscr{A}}(\mathfrak{c}_2)^{-1} = C_2^{-1} \\
\tilde{\mathscr{A}}(\mathfrak{c}_3^{-1}) &= \tilde{\mathscr{A}}(\mathfrak{c}_3)^{-1} = C_3^{-1} \\
\tilde{\mathscr{A}}(\mathfrak{c}_4^{-1}) &= \tilde{\mathscr{A}}(\mathfrak{c}_4)^{-1} = C_4^{-1}
\end{aligned}$$

Now let

$$\Gamma^A_{\mathrm{CZ}+Z}(R_x(\theta)) := \left\{C_0, C_0^{-1}, C_1, C_1^{-1}, C_3, C_3^{-1}, C_4, C_4^{-1}\right\}$$

and

$$\Gamma^B_{\mathrm{CZ}+Z}(R_x(\theta)) := \left\{C_0, C_0^{-1}, C_2, -C_2^{-1}, C_3, C_3^{-1}, C_4, C_4^{-1}\right\}.$$

Evidently, if $\theta \in A \backslash \frac{\pi}{2}\mathbb{Z}$, then $\Gamma^A_{\mathrm{CZ}+Z}(R_x(\theta))$ is closed under inverses, so $\langle \Gamma^A_{\mathrm{CZ}+Z}(R_x(\theta))\rangle$ is a subgroup of $\mathrm{SL}(2;\mathbb{C})$. Likewise, if $\theta \in B \backslash \frac{\pi}{2}\mathbb{Z}$, then $\langle \Gamma^B_{\mathrm{CZ}+Z}(R_x(\theta))\rangle$ is a subgroup of $\mathrm{SL}(2;\mathbb{C})$. In fact, for the appropriate choice of $\theta$, both $\langle \Gamma^A_{\mathrm{CZ}+Z}(R_x(\theta))\rangle$ and $\langle \Gamma^B_{\mathrm{CZ}+Z}(R_x(\theta))\rangle$ are non-elementary, non-discrete, and strictly loxodromic subgroups of $\mathrm{SL}(2;\mathbb{C})$.

**Claim C.2.** *If $\theta \in A \backslash \frac{\pi}{2}\mathbb{Z}$, then $\langle \Gamma^A_{\mathrm{CZ}+Z}(R_x(\theta))\rangle$ is a non-elementary subgroup of* $\mathrm{SL}(2;\mathbb{C})$.

*Proof.* We find

$$\begin{aligned}
\beta(C_0) &= 4(\csc^4(\theta) - 1) \\
\beta(C_1) &= \frac{4}{\sec^2(\theta)\tan^4\left(\frac{\theta}{2}\right)} \\
\gamma(C_0, C_1) &= \frac{32\cos^4(\theta)\cot^2\left(\frac{\theta}{2}\right)}{-5 + 28\cos(\theta) + 4\cos(2\theta) + 4\cos(3\theta) + \cos(4\theta)}.
\end{aligned}$$

It is an elementary exercise to verify that if $\theta \in A \backslash \frac{\pi}{2}\mathbb{Z}$, then `IsElementary`$(\Gamma^A_{\mathrm{CZ}+Z}(R_x(\theta))) =$ `NO`. ■

**Claim C.3.** *If $\theta \in B \backslash \frac{\pi}{2}\mathbb{Z}$, then $\langle \Gamma^B_{\mathrm{CZ}+Z}(R_x(\theta))\rangle$ is a non-elementary subgroup of* $\mathrm{SL}(2;\mathbb{C})$.

*Proof.* We find

$$\begin{aligned}
\beta(C_0) &= 4(\csc^4(\theta) - 1) \\
\beta(C_2) &= \frac{128\cos^2(\theta)\sin^4\left(\frac{\theta}{2}\right)}{-5 - 28\cos(\theta) + 4\cos(2\theta) - 4\cos(3\theta) + \cos(4\theta)} \\
\gamma(C_0, C_2) &= \frac{32\cos^4(\theta)\cot^2\left(\frac{\theta}{2}\right)}{-5 - 28\cos(\theta) + 4\cos(2\theta) - 4\cos(3\theta) + \cos(4\theta)}.
\end{aligned}$$

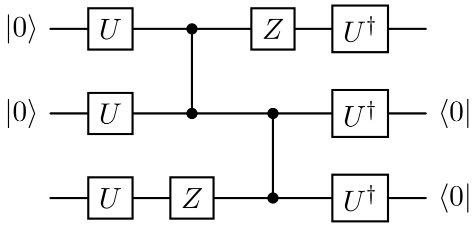
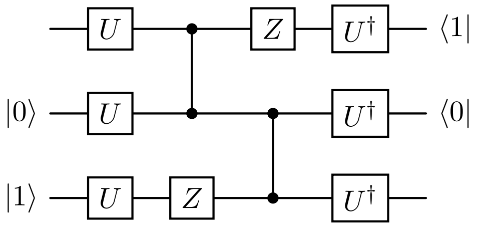
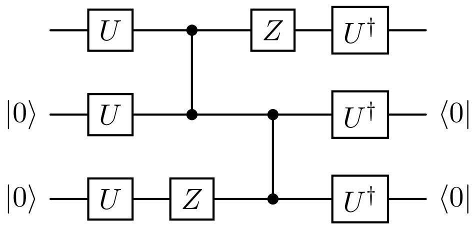
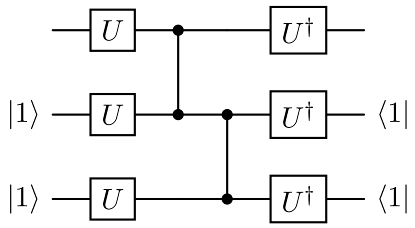
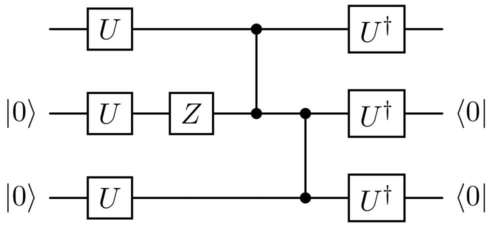
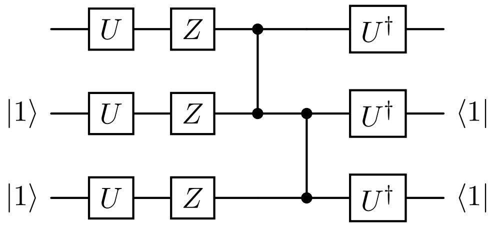
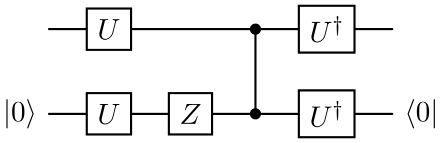
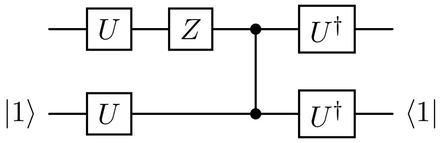
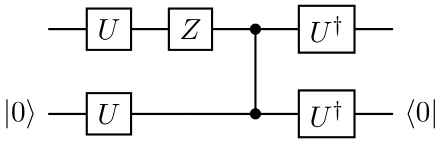
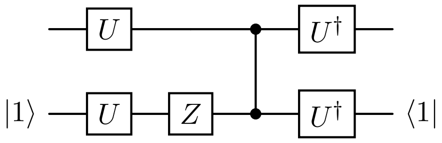
| $\mathfrak{c}_i$ | Gadget in $\mathcal{S}_{\mathrm{CZ}+Z}(U)$ | $\mathfrak{c}_i^{-1}$ | Inverse gadget in $\mathcal{S}_{\mathrm{CZ}+Z}(U)$ |
|---|---|---|---|
| $\mathfrak{c}_0$ |  | $\mathfrak{c}_0^{-1}$ |  |
| $\mathfrak{c}_1$ |  | $\mathfrak{c}_1^{-1}$ |  |
| $\mathfrak{c}_2$ |  | $\mathfrak{c}_2^{-1}$ |  |
| $\mathfrak{c}_3$ |  | $\mathfrak{c}_3^{-1}$ |  |
| $\mathfrak{c}_4$ |  | $\mathfrak{c}_4^{-1}$ |  |

Table 1. Post-selection gadgets for $U$-conjugated $\mathrm{CZ} + Z$ Clifford circuits with $U = R_x(\theta)$ and $\theta \notin \frac{\pi}{2}\mathbb{Z}$.

It is an elementary exercise to verify that if $\theta \in B\backslash\frac{\pi}{2}\mathbb{Z}$, then $\texttt{IsElementary}(\Gamma^B_{\text{CZ}+Z}(R_x(\theta))) = \texttt{NO}$. ■

**Claim C.4.** *If $\theta \in A\backslash\frac{\pi}{2}\mathbb{Z}$, then $\langle\Gamma^A_{\text{CZ}+Z}(R_x(\theta))\rangle$ is a non-discrete subgroup of* $\mathrm{SL}(2;\mathbb{C})$*.*

*Proof.* From the proof of Claim C.2, we know that if $\theta \in A\backslash\frac{\pi}{2}\mathbb{Z}$, then $C_0$ and $C_1$ (together with their inverses) generate a non-elementary subgroup of $\mathrm{SL}(2;\mathbb{C})$. Therefore, we may use Jørgensen's inequality (line 4 in Algorithm 2) to test discreteness. We find that if $\theta \in A\backslash\frac{\pi}{2}\mathbb{Z}$, then indeed

$$\left|\mathrm{tr}^2(C_1) - 4\right| + \left|\mathrm{tr}(C_1C_0C_1^{-1}C_0^{-1}) - 2\right| = \frac{32\left(\cos^4(\theta)\left|\cot\left(\frac{\theta}{2}\right)\right|^2 + 4\cos^2(\theta)\cos^4\left(\frac{\theta}{2}\right)\right)}{|28\cos(\theta) + 4\cos(2\theta) + 4\cos(3\theta) + \cos(4\theta) - 5|} < 1.$$

Therefore, if $\theta \in A\backslash\frac{\pi}{2}\mathbb{Z}$, then $\texttt{IsDiscrete}(\Gamma^A_{\text{CZ}+Z}(R_x(\theta))) = \texttt{NO}$. ■

**Claim C.5.** *If $\theta \in B\backslash\frac{\pi}{2}\mathbb{Z}$, then $\langle\Gamma^B_{\text{CZ}+Z}(R_x(\theta))\rangle$ is a non-discrete subgroup of* $\mathrm{SL}(2;\mathbb{C})$*.*

*Proof.* From the proof of Claim C.3, we know that if $\theta \in B\backslash\frac{\pi}{2}\mathbb{Z}$, then $C_0$ and $C_2$ (together with their inverses) generate a non-elementary subgroup of $\mathrm{SL}(2;\mathbb{C})$. Therefore, we may use Jørgensen's inequality (line 4 in Algorithm 2) to test discreteness. We find that if $\theta \in B\backslash\frac{\pi}{2}\mathbb{Z}$, then indeed

$$\left|\mathrm{tr}^2(C_2) - 4\right| + \left|\mathrm{tr}(C_2C_0C_2^{-1}C_0^{-1}) - 2\right| = \frac{32\left(\cos^4(\theta)\left|\tan\left(\frac{\theta}{2}\right)\right|^2 + 4\sin^4\left(\frac{\theta}{2}\right)\cos^2(\theta)\right)}{|-28\cos(\theta) + 4\cos(2\theta) - 4\cos(3\theta) + \cos(4\theta) - 5|} < 1.$$

Therefore, if $\theta \in B\backslash\frac{\pi}{2}\mathbb{Z}$, then $\texttt{IsDiscrete}(\Gamma^B_{\text{CZ}+Z}(R_x(\theta))) = \texttt{NO}$. ■

**Claim C.6.** *If $\theta \in A\backslash\frac{\pi}{2}\mathbb{Z}$, then $\langle\Gamma^A_{\text{CZ}+Z}(R_x(\theta))\rangle$ is a strictly loxodromic subgroup of* $\mathrm{SL}(2;\mathbb{C})$*.*

*Proof.* Since

$$\mathrm{tr}(C_3) = \frac{1+\cos(\theta)}{\sqrt{\cos(\theta)}} \quad \text{and} \quad \mathrm{tr}(C_4) = (\cos(\theta) - 1)\sqrt{-\cos(\theta)}\sec(\theta),$$

if $\theta \in A\backslash\frac{\pi}{2}\mathbb{Z}$, then either $\sqrt{\cos(\theta)} \in \mathbb{C}\backslash\mathbb{R}$ or $\sqrt{-\cos(\theta)} \in \mathbb{C}\backslash\mathbb{R}$. Consequently, if $\theta \in A\backslash\frac{\pi}{2}\mathbb{Z}$, then $\texttt{IsLoxodromic}(\Gamma^A_{\text{CZ}+Z}(R_x(\theta))) = \texttt{YES}$. ■

**Claim C.7.** *If $\theta \in B\backslash\frac{\pi}{2}\mathbb{Z}$, then $\langle\Gamma^B_{\text{CZ}+Z}(R_x(\theta))\rangle$ is a strictly loxodromic subgroup of* $\mathrm{SL}(2;\mathbb{C})$*.*

*Proof.* The proof is identical to the proof of Claim C.6. ■

Altogether, Claims C.2 – C.7 and our criterion Theorem 3.5 imply that if $\theta \notin \frac{\pi}{2}\mathbb{Z}$, then no efficient classical computer can simulate $R_x(\theta)$-conjugated $\text{CZ}+Z$ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$. ■

## Appendix D. Proof of Theorem 5.15

In this section, we classify the complexity of $U$-conjugated $\mathrm{CZ} + S$ circuits (also known as commuting conjugated Clifford circuits). Formally, this is our Theorem 5.15, which we restate below for convenience.

**Theorem 5.15.** *If the polynomial hierarchy is infinite, then efficient classical computers can simulate $U$-conjugated $\mathrm{CZ} + S$ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$ iff there exists $C \in \langle H, S \rangle$ and $\alpha, \phi, \lambda \in [0, 2\pi)$ such that $U = e^{i\alpha} R_z(\phi) C R_z(\lambda)$.*

Our method of proof is to show that for all $U \in \mathrm{U}(2)$, $U$-conjugated $\mathrm{CZ} + S$ circuits are efficiently classically simuilable iff $U$-conjugated $\mathrm{CZ} + Z$ circuits are, thereby showing that the complexity classification of $U$-conjugated $\mathrm{CZ} + S$ circuits is the same as the complexity classification of $U$-conjugated $\mathrm{CZ} + Z$ circuits, which we proved in Appendix C. To do this, we require the following lemma.

**Lemma D.1.** *Let $U$ and $V$ be single-qubit unitaries such that $U = e^{i\alpha} R_z(\phi) V R_z(\lambda)$ for $\alpha, \phi, \lambda \in [0, 2\pi)$. Then, $U$-conjugated $\mathrm{CZ} + S$ circuits are efficiently classically simulable to within multiplicative error $\epsilon < \sqrt{2} - 1$ iff $V$-conjugated $\mathrm{CZ} + S$ circuits are.*

*Proof.* The proof is identical to the proof of Lemma B.1. ■

**Lemma D.2.** *If the polynomial hierarchy is infinite, then for all $U \in \mathrm{U}(2)$, efficient classical computers can simulate $U$-conjugated $\mathrm{CZ} + S$ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$ iff they can simulate $U$-conjugated $\mathrm{CZ} + Z$ circuits to within the same multiplicative error.*

*Proof.* The forward direction is trivial, because every $U$-conjugated $\mathrm{CZ} + Z$ circuit is a $U$-conjugated $\mathrm{CZ} + S$ circuit. For the other direction, suppose efficient classical computers can simulate $U$-conjugated $\mathrm{CZ} + Z$ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$ and let $U = e^{i\alpha} R_z(\phi) R_x(\theta) R_z(\lambda)$ be the Euler decomposition of $U$. By Lemma B.1, $U$-conjugated $\mathrm{CZ} + Z$ circuits are efficiently classically simulable to within multiplicative error $\epsilon$ iff $R_x(\theta)$-conjugated $\mathrm{CZ} + Z$ circuits are. But, by Lemma C.1, efficient classical computers can simulate $R_x(\theta)$-conjugated $\mathrm{CZ} + Z$ circuits to within multiplicative error $\epsilon < \sqrt{2} - 1$ iff $\theta \in \frac{\pi}{2}\mathbb{Z}$. Therefore, $\theta \in \frac{\pi}{2}\mathbb{Z}$, so $R_x(\theta) \in \langle H, S \rangle$. Consequently, every $R_x(\theta)$-conjugated $\mathrm{CZ} + S$ circuit is a Clifford circuit and hence is efficiently classically simulable. Thus, by Lemma D.1, $U$-conjugated $\mathrm{CZ} + S$ circuits are also efficiently classically simulable. ■

## References

[AA11] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing*, STOC '11, pages 333–342, New York, NY, USA, 2011. Association for Computing Machinery.

[AAEL07] Dorit Aharonov, Itai Arad, Elad Eban, and Zeph Landau. Polynomial quantum algorithms for additive approximations of the potts model and other points of the tutte plane, 2007.

[Aar05] Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2063):3473–3482, 2005.

[AB97] Dorit Aharonov and Michael Ben-Or. Fault-tolerant quantum computation with constant error. *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, page 176–188, 1997.

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach.* Cambridge University Press, 1st edition, 2009.

[AG04] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70:052328, Nov 2004.

[AGM21] Hala Alaqad, Jianhua Gong, and Gaven Martin. Chebyshev polynomials and inequalities for Kleinian groups. *Communications in Contemporary Mathematics*, 25(02), December 2021.

[AGS17] Scott Aaronson, Daniel Grier, and Luke Schaeffer. The Classification of Reversible Bit Operations. In Christos H. Papadimitriou, editor, *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*, volume 67 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 23:1–23:34, Dagstuhl, Germany, 2017. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[Bea83] Alan F. Beardon. *The geometry of discrete groups.* Springer-Verlag, Berlin, 1983.

[BFK18] Adam Bouland, Joseph F. Fitzsimons, and Dax Enshan Koh. Complexity classification of conjugated clifford circuits. In *Proceedings of the 33rd Computational Complexity Conference*, CCC '18, Dagstuhl, DEU, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[BG21] Adam Bouland and Tudor Giurgica-Tiron. Efficient universal quantum compilation: An inverse-free Solovay-Kitaev algorithm, 2021.

[BGK18] Sergey Bravyi, David Gosset, and Robert König. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, 2018.

[BJS11] Michael J. Bremner, Richard Jozsa, and Dan J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 467(2126):459–472, 2011.

[BM81] Robert Brooks and Peter J. Matelski. The dynamics of 2-generator subgroups of PSL$(2;\mathbb{C})$. *Riemann Surfaces and Related Topics (AM-97)*, 97:65–72, 1981.

[BMZ16] 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)*, volume 50 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 28:1–28:33, Dagstuhl, Germany, 2016. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[BR00] Line Baribeau and Thomas Ransford. On the set of discrete two-generator groups. *Mathematical Proceedings of the Cambridge Philosophical Society*, 128:245–255, 2000.

[BV93] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '93, page 11–20, New York, NY, USA, 1993. Association for Computing Machinery.

[CT09] Wensheng Cao and Haiou Tan. Jørgensen's inequality for quternionic hyperbolic space with elliptic elements. *Bulletin of the Australian Mathematical Society*, 81:121 – 131, 2009.

[CvD10] Andrew M. Childs and Wim van Dam. Quantum algorithms for algebraic problems. *Rev. Mod. Phys.*, 82:1–52, Jan 2010.

[Fey81] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 1981.

[FKM$^+$18] Keisuke Fujii, Hirotada Kobayashi, Tomoyuki Morimae, Harumichi Nishimura, Shuhei Tamate, and Seiichiro Tani. Impossibility of classically simulating one-clean-qubit model with multiplicative error. *Phys. Rev. Lett.*, 120:200502, May 2018.

[Got98] Daniel Gottesman. The heisenberg representation of quantum computers, 1998.

[GS22] Daniel Grier and Luke Schaeffer. The classification of clifford gates over qubits. *Quantum*, 6:734, 2022.

[HHT97] Yenjo Han, Lane A. Hemaspaandra, and Thomas Thierauf. Threshold computation and cryptographic security. *SIAM Journal on Computing*, 26(1):59–78, 1997.

[Iva06] Gabor Ivanyos. Deciding universality of quantum gates, 2006.

[JL03] Richard Jozsa and Noah Linden. On the role of entanglement in quantum-computational speed-up. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 459(2036):2011–2032, 2003.

[Jør76] Troels Jørgensen. On discrete groups of mobius transformations. *American Journal of Mathematics*, 98(3):739–749, 1976.

[KFG24] Chaitanya Karamchedu, Matthew Fox, and Daniel Gottesman. A criterion for quantum advantage. `https://github.com/psi-is-the-world/a-criterion-for-quantum-advantage`, 2024.

[KL98] Emanuel Knill and Raymond Laflamme. Power of one bit of quantum information. *Phys. Rev. Lett.*, 81:5672–5675, Dec 1998.

[Koh24] Moishe Kohan. If every pair of generators generates an elementary group, is the group generated by all the generators necessarily elementary? Mathematics Stack Exchange, 2024. URL:`https://math.stackexchange.com/q/4911481` (version: 2024-05-05).

[Lad75] Richard E. Ladner. On the structure of polynomial time reducibility. *J. ACM*, 22(1):155–171, 1975.

[Llo95] Seth Lloyd. Almost any quantum logic gate is universal. *Phys. Rev. Lett.*, 75:346–349, Jul 1995.

[McK13] Matthew McKague. On the power quantum computation over real hilbert spaces. *International Journal of Quantum Information*, 11(01):1350001, 2013.

[MLLL+12] 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.

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, anniversary edition, 2011.

[NLD+22] John C. Napp, Rolando L. La Placa, Alexander M. Dalzell, Fernando G. S. L. Brandão, and Aram W. Harrow. Efficient classical simulation of random shallow 2d quantum circuits. *Phys. Rev. X*, 12:021021, Apr 2022.

[NRS01] G. Nebe, E.M. Rains, and N.J.A. Sloane. The invariants of the clifford groups. *Designs, Codes and Cryptography*, 24:99–122, 2001.

[Pos41] Emil L. Post. *The Two-Valued Iterative Systems of Mathematical Logic. (AM-5)*. Princeton University Press, 1941.

[Sho99] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41:303–332, 1999.

[SK17] Adam Sawicki and Katarzyna Karnas. Criteria for universality of quantum gates. *Phys. Rev. A*, 95:062303, Jun 2017.

[Sul85] Dennis Sullivan. Quasiconformal homeomorphisms and dynamics II: Structural stability implies hyperbolicity for Kleinian groups. *Acta Mathematica*, 155:243 – 260, 1985.

[Tan89] Delin Tan. On two-generator discrete groups of möbius transformations. *Proceedings of the American Mathematical Society*, 106(3):763–770, 1989.

[TD04] 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.

[Tod91] Seinosuke Toda. PP is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991.

Department of Computer Science, University of Maryland
*Email address*: cdkaram@umd.edu

Department of Physics, University of Colorado Boulder
*Email address*: matthew.fox@colorado.edu

Department of Computer Science, University of Maryland
*Email address*: dgottesm@umd.edu