

BOUNDS ON EVENTUALLY UNIVERSAL QUANTUM GATE SETS

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

ABSTRACT. Say a collection of n -qudit gates Γ is *eventually universal* if and only if there exists $N_0 \geq n$ such that for all $N \geq N_0$, one can approximate any N -qudit unitary to arbitrary precision by a circuit over Γ . In this work, we improve the best known upper bound on the smallest N_0 with the above property. Our new bound is roughly $d^4 n$, where d is the local dimension (the ‘ d ’ in qudit), whereas the previous bound was roughly $d^8 n$. For qubits ($d = 2$), our result implies that if an n -qubit gate set is eventually universal, then it will exhibit universality when acting on a $16n$ qubit system, as opposed to the previous bound of a $256n$ qubit system. In other words, if adding just $15n$ ancillary qubits to a quantum system (as opposed to the previous bound of $255n$ ancillary qubits) does not boost a gate set to universality, then no number of ancillary qubits ever will. Our proof relies on the invariants of finite linear groups as well as a classification result for all finite groups that are unitary 2-designs.

1. INTRODUCTION

Let Γ be a finite subset of the special unitary group $\mathbf{SU}(d^n)$, where $d, n \geq 2$. We adopt a quantum computing perspective and think of Γ as an n -qudit gate set so that each element of Γ acts on an n -qudit system whose Hilbert space is $(\mathbb{C}^d)^{\otimes n} \cong \mathbb{C}^{d^n}$. We say Γ is *universal* if and only if Γ generates a dense subset of $\mathbf{SU}(d^n)$ with respect to the operator norm topology. In the circuit model of quantum computation, universal gate sets play the role of the AND, OR, and NOT gates (or any other functionally complete set of Boolean logic gates) in the circuit model of classical computation.

Interestingly, in the quantum setting a gate set Γ need not be universal in the above sense to perform universal quantum computation (possibly in an encoded subspace [15]). For example, $\{H, \text{TOFFOLI}\}$ is not universal, but circuits over these gates can nevertheless simulate any quantum computation [23]. On the other hand, there exist non-universal gate sets that are classically simulable (e.g., Clifford [9]) as well as other gate sets whose computational power is expected to lie somewhere “in between” the complexity classes BPP and BQP [3, 24, 16]. Ultimately, there are many different types of non-universal gate sets, and, as stressed in [2], it is both a natural and theoretically important goal to understand all the ways in which a gate set can fail to be universal. Incidentally, this goal is similar to Post’s classification of all the ways in which a set of Boolean logic gates can fail to be universal [21].

One reason why this goal is so challenging is because a gate set can be non-universal, despite the fact that a higher-dimensional version of it *is* universal. For example, Jeandel identified a simple 6-qubit ($d = 2$) gate set that does not densely generate $\mathbf{SU}(2^6)$, but which does densely generate $\mathbf{SU}(2^9)$ when allowed to act on a 9-qubit system [14]. In fact, Jeandel’s construction generalizes to n -qubit gate sets, and it establishes the existence of gate sets that are non-universal on fewer than $2n - 5$ qubits, but are universal on $2n - 3$ qubits. We review his construction in Appendix C.

In this work, we are interested in this Jeandel-type of universality—hereafter called *eventual universality*—in which an n -qudit gate set is non-universal on an n -qudit system, but is universal on an N -qudit system for some $N \geq n$. In particular, our work builds on a paper by Ivanyos

[†] These authors contributed equally.

who considered the question of whether eventual universality is decidable [13]. Indeed, a priori, one does not know how many additional qudits are needed before a given gate set might exhibit universality, so it is not clear if eventual universality is even decidable. Remarkably, however, Ivanyos proved that eventual universality is decidable. To achieve this, he bounded the number of ancillary qudits one would need to add to a system before a given gate set acting on that system would exhibit universality. Specifically, he showed that an n -qudit gate set is eventually universal if and only if it is universal on a larger, N qudit system, where $N \leq d^8(n-1) + 1$.

Our main result is a significant improvement to this bound, thus improving Ivanyos' algorithm for deciding eventual universality. Our new bound is essentially a quadratic improvement and is roughly d^4n . For qubits, our result implies that if an n -qubit gate set is eventually universal, then it will exhibit universality when acting on a $16n$ qubit system, as opposed to the previous bound of a $256n$ qubit system. In other words, if adding just $15n$ ancillary qubits to a quantum system (as opposed to the previous bound of $255n$ ancillary qubits) does not boost a gate set to universality, then no number of ancillary qubits ever will.

Our method of proof is similar to Ivanyos' and hinges significantly on the invariants of finite linear groups as well as a classification result for all finite groups that are unitary 2-designs. However, in an effort to make this article comprehensible to the quantum computing community, we have deferred most of the technical details to the appendices.

2. PRELIMINARIES

Let Γ be an n -qudit gate set, where $d, n \geq 2$. As mentioned in the introduction, Γ is *universal* if and only if Γ generates a dense subset of $\mathbf{SU}(d^n)$ with respect to the operator norm topology. In general, Γ is not closed under inverses, so the set it generates is merely a *semigroup* in $\mathbf{SU}(d^n)$. However, since $\mathbf{SU}(d^n)$ is compact, the semigroup generated by Γ is dense in $\mathbf{SU}(d^n)$ if and only if the group generated by Γ and its inverse elements is dense in $\mathbf{SU}(d^n)$. For this reason, we will always assume that Γ is closed under inverses so that Γ generates a *subgroup* of $\mathbf{SU}(d^n)$.

Here, we are interested in a weaker notion of universality that we call *eventual universality*. Informally, this is the idea that, while Γ itself may not be universal, a higher-dimensional variant of Γ is. To be more precise, let $N \geq n$, let I be the identity on $(\mathbb{C}^d)^{\otimes N-n}$, and let

$$\Gamma^N := \{ \pi(\gamma \otimes I) \pi^{-1} : \gamma \in \Gamma, \pi \in S_N \},$$

where S_N is the symmetric group of degree N . In words, Γ^N is the set of all N -qudit unitaries that can be made from a single element of Γ acting on any subset of n qudits (in any order), with the identity acting on the remaining $N - n$ qudits. As shown in [13], Γ^N is equivalently the set of all N -qudit unitaries that can be made from a single element of Γ and any number of SWAP gates. Given this, we say Γ is *eventually universal* if and only if there exists $N \geq n$ such that Γ^N is universal, and we write $\mathcal{K}(\Gamma)$ for the smallest $N \geq n$ such that Γ^N is universal. In case Γ^N is not universal for all $N \geq n$, we set $\mathcal{K}(\Gamma) = \infty$. Thus, Γ is eventually universal if and only if $\mathcal{K}(\Gamma) < \infty$.

Evidently, if Γ is universal, then it is eventually universal. Moreover, it is known that if Γ^N is universal, then Γ^M is universal for all $M \geq N$ [6, 13]. However, if Γ is eventually universal, then it is not necessarily universal. In other words, there exist n -qudit gate sets Γ which *are* eventually universal, but for which $\mathcal{K}(\Gamma) > n$. Examples of such gate sets include Jeandel's construction in [14], which we review in Appendix C.

In this paper, we are interested in upper bounding $\mathcal{K}(\Gamma)$. Such a bound gives the maximum number of ancillary qudits one would need to add to a quantum system before an eventually universal gate set Γ exhibits universality. The first and only upper bound (as far as we know) is due to Ivanyos [13], who proved that an n -qudit gate set Γ is eventually universal if and only

if $\mathcal{K}(\Gamma) \leq d^8(n-1) + 1$. Here, we improve this result to roughly d^4n . Formally, our main result is as follows.

Theorem 1. *Let Γ be an n -qudit gate set, where $d, n \geq 2$. Then, Γ is eventually universal if and only if $\mathcal{K}(\Gamma) \leq d^4(n-1) + 1$.*

The remainder of this paper is dedicated to proving this result.

3. MAIN RESULTS

Fix $d, n \geq 2$, $N \geq n$, and let G be a compact subgroup of the general linear group $\mathbf{GL}(d^N, \mathbb{C})$. A key notion in this work is the $2k$ th moment of G ,

$$\mathcal{M}_{2k}(G) = \int_{g \in G} |\mathrm{tr}(g)|^{2k} \mu_{\mathrm{Haar}}(G),$$

where $\mu_{\mathrm{Haar}}(G)$ is the Haar measure on G . Importantly, if G is a compact unitary group, then $\mathcal{M}_{2k}(G)$ is the *frame potential* of the Haar measure on G [12, 17, 18].

A priori, the various moments of G are arbitrary real numbers. However, these moments actually carry a tremendous amount of information about the “size” of G . Specifically, Larsen established the remarkable fact that if the 4th moment of a compact and unitary group G is a particular value, then there are few alternatives for what G can be.

Theorem 2 (Larsen’s Alternative for Unitary Groups [18]). *If $G \leq \mathbf{SU}(d^N)$ is compact and $\mathcal{M}_4(G) = \mathcal{M}_4(\mathbf{SU}(d^N))$, then G is finite or $G = \mathbf{SU}(d^N)$.*

Larsen’s alternative is useful because it implies a very simple criterion for eventual universality. To improve the readability of what follows, we slightly abuse our notation and write $\mathcal{M}_k(\Gamma^N)$ for $\mathcal{M}_k(\mathrm{cl}(\langle \Gamma^N \rangle))$, where Γ is a gate set, $\langle \Gamma^N \rangle$ is the group generated by Γ^N , and $\mathrm{cl}(\langle \Gamma^N \rangle)$ is the closure of $\langle \Gamma^N \rangle$ in $\mathbf{SU}(d^N)$. Note also that $\mathrm{cl}(\langle \Gamma^N \rangle)$ is compact because it is a closed subgroup of the compact group $\mathbf{SU}(d^N)$.

Corollary 3 (Criterion for Eventual Universality). *Let $\Gamma \subset \mathbf{SU}(d^n)$ be an n -qudit gate set. Then, Γ is eventually universal if and only if there is $N \geq n$ such that $\mathcal{M}_4(\Gamma^N) = \mathcal{M}_4(\mathbf{SU}(d^N))$ and $|\langle \Gamma^N \rangle| = \infty$. Moreover, $\mathcal{K}(\Gamma) \leq N$.*

In [13], Ivanyos uses Corollary 3 to obtain his upper bound on $\mathcal{K}(\Gamma)$, and this is also our approach to improve his bound. In Ivanyos’ case, however, he leverages the fact that for all compact $G \leq \mathbf{SU}(d^N)$, $\mathcal{M}_8(G) = \mathcal{M}_8(\mathbf{SU}(d^N))$ implies $\mathcal{M}_4(G) = \mathcal{M}_4(\mathbf{SU}(d^N))$ [11, 12]. (In the language of unitary t -designs, this is simply the statement that a unitary 4-design is a unitary 2-design.) Therefore, it suffices to look at the 8th moment of G , as opposed to the 4th. This is a major simplification, for a result of Bannai et al. [7], which builds on the work of Guralnick and Tiep [11], proves that if $d^N \geq 5$, then there are no finite groups $G \leq \mathbf{SU}(d^N)$ for which $\mathcal{M}_8(G) = \mathcal{M}_8(\mathbf{SU}(d^N))$. Therefore, to upper-bound N such that $\mathcal{M}_8(\Gamma^N) = \mathcal{M}_8(\mathbf{SU}(d^N))$ is to upper-bound N such that $\mathcal{M}_8(\Gamma^N) = \mathcal{M}_8(\mathbf{SU}(d^N))$ and $|\langle \Gamma^N \rangle| = \infty$. In [13], Ivanyos does just this and proves the following result.

Theorem 4 (Ivanyos [13]). *Let Γ be an n -qudit gate set for which there exists $N \geq n$ such that $\mathcal{M}_8(\Gamma^N) = \mathcal{M}_8(\mathbf{SU}(d^N))$. Then, the smallest such N satisfies $N \leq d^8(n-1) + 1$. Consequently, $\mathcal{K}(\Gamma) \leq d^8(n-1) + 1$.*

However, Larsen’s alternative and Corollary 3 only call for the 4th moments to be equal, not the 8th. Thus, a better bound on the least N for which $\mathcal{M}_4(\Gamma^N) = \mathcal{M}_4(\mathbf{SU}(d^N))$ seems plausible. Indeed, in Appendix A, we prove as much using similar techniques to Ivanyos.

Theorem 5. *Let Γ be an n -qudit gate set for which there exists $N \geq n$ such that $\mathcal{M}_4(\Gamma^N) = \mathcal{M}_4(\mathbf{SU}(d^N))$. Then, the smallest such N satisfies $N \leq d^4(n-1) + 1$.*

However, unlike Ivanyos' Theorem 4, we cannot conclude from Theorem 5 and Corollary 3 alone that $\mathcal{K}(\Gamma) \leq d^4(n-1) + 1$ because there exist *finite* $G \leq \mathbf{SU}(d^N)$ for which $\mathcal{M}_4(G) = \mathcal{M}_4(\mathbf{SU}(d^N))$, e.g., the N -qudit Clifford group $\mathbf{Cl}_d(N)$ [5, 12]. For that, we need to better understand the *finite* subgroups $G < \mathbf{SU}(d^N)$ for which $\mathcal{M}_4(G) = \mathcal{M}_4(\mathbf{SU}(d^N))$.

As defined in [11], a *finite* group $G \leq \mathbf{SU}(d^N)$ satisfying $\mathcal{M}_4(G) = \mathcal{M}_4(\mathbf{SU}(d^N))$ is called a *unitary 2-group*, which is an instance of a *unitary k -group*. Fortunately, the properties of unitary k -groups are well-understood, and there is a complete classification of all unitary 2-groups due to Bannai et al. [7, 11]. That said, the complete classification is rather involved and includes certain irreducible representations of particular unitary and symplectic groups, as well as a finite list of exceptions. Here, we give an abridged version of this classification so to not distract from the details of the classification that matter to us. In what follows, $\overline{G}$ is the projective group $G/\mathbf{Z}(G)$, where $\mathbf{Z}(G)$ is the center of G , and $\mathbf{Cl}_d(N)$ is the N -qudit Clifford group.

Theorem 6 (Bannai et al. [7], Guralnick and Tiep [11], Heinrich [12], Abridged). *Let $d, N \geq 2$ such that $d^N \geq 5$ and let $G < \mathbf{SU}(d^N)$ be a unitary 2-group (i.e., a finite unitary group such that $\mathcal{M}_4(G) = \mathcal{M}_4(\mathbf{SU}(d^N))$). Then, one of the following cases applies.*

- (i) *(Lie-Type Case) d^N equals $(3^k \pm 1)/2$ or $(2^k + (-1)^k)/3$ for some positive integer k , and G is a particular group that is not isomorphic to $\mathbf{Cl}_d(N)$.*
- (ii) *(Extraspecial Case) d is a prime power and $\overline{G}$ is isomorphic to $\overline{\mathbf{Cl}_d(N)}$.*
- (iii) *(Exceptional Case) $d = 2$, $N = 3$, and G is a particular 3-qubit group that is not isomorphic to $\mathbf{Cl}_2(3)$.¹*

This classification details all the ways in which a unitary group G can satisfy $\mathcal{M}_4(G) = \mathcal{M}_4(\mathbf{SU}(d^N))$ and $|G| < \infty$. In the context of the criterion for eventual universality (Corollary 3), it details all the ways in which an n -qudit gate set Γ can satisfy $\mathcal{M}_4(\Gamma^N) = \mathcal{M}_4(\mathbf{SU}(d^N))$ and $|\langle \Gamma^N \rangle| < \infty$ for any given $N \geq n$. In what follows, we will use this classification to show that unless Γ is the Clifford gate set, if $\mathcal{M}_4(\Gamma^N) = \mathcal{M}_4(\mathbf{SU}(d^N))$ and $N > 3$, then $\mathcal{M}_4(\Gamma^{N+1}) = \mathcal{M}_4(\mathbf{SU}(d^{N+1}))$ and $|\langle \Gamma^{N+1} \rangle| = \infty$.

First, consider the extraspecial case in Theorem 6. A result by Heinrich [12] essentially “singles out” the Clifford gate set as the unique gate set that always generates a finite group, no matter how many ancillary qudits are added.

Proposition 7 (Proposition 13.1(i) in [12]). *Let Γ be an n -qudit gate set, where $d, n \geq 2$. If for all $N \geq n$, $\mathcal{M}_4(\Gamma^N) = \mathcal{M}_4(\mathbf{SU}(d^N))$ and $|\langle \Gamma^N \rangle| < \infty$, then d is a prime power and $\overline{\langle \Gamma^N \rangle}$ is isomorphic to the N -qudit Clifford group $\overline{\mathbf{Cl}_d(N)}$. In particular, Γ is not eventually universal.*

This proposition proves that the extraspecial case in Theorem 6 is the unique instance for which Γ satisfies $\mathcal{M}_4(\Gamma^N) = \mathcal{M}_4(\mathbf{SU}(d^N))$ for all $N \geq n$, and yet still fail to be eventually universal. Of course, it is not surprising that the Clifford group behaves this way. What is surprising, though, is that the Clifford group is the *only* group that behaves this way.

On the other hand, if Γ is such that $\langle \Gamma \rangle$ is either Lie-type or exceptional, then the question remains *how large* must N be for $|\langle \Gamma^N \rangle| = \infty$. Below, we will prove that in both cases, if $N > 4$, then $|\langle \Gamma^N \rangle| = \infty$. We start with the Lie-type case.

Proposition 8. *Let Γ be an n -qudit gate set, where $d, n \geq 2$. If there exists $N \geq n$ such that $\mathcal{M}_4(\Gamma^N) = \mathcal{M}_4(\mathbf{SU}(d^N))$, $|\langle \Gamma^N \rangle| < \infty$, and $\langle \Gamma^N \rangle$ is either Lie-type or exceptional, then $N \leq 3$ and $\mathcal{K}(\Gamma) \leq d^4(n-1) + 1$.*

¹That this is the only exceptional case in this abridged classification follows from the full classification in [7, 11] together with our assumption that the dimension d^N is a perfect power.

The proof idea is to exploit the dimensional requirements in the exceptional and Lie-type cases of Theorem 6 to obtain a restriction on N and n that bounds $\mathcal{K}(\Gamma)$. Of course, the exceptional case is “maximally restrictive” in the sense that it only applies when $N = 3$. Interestingly, the Lie-type case is similar, as the next result implies.

Lemma 9. *Let $d, N \geq 2$. Then, there exists a positive integer k such that $d^N \in \{(3^k \pm 1)/2, (2^k + (-1)^k)/3\}$ if and only if $N = 2$ and $d \in \{2, 11\}$.*

We prove this in Appendix B. Using it, we can easily prove Proposition 8.

Proof of Proposition 8. On one hand, it follows from Lemma 9 that $\langle \Gamma^N \rangle$ is Lie-type only if $N = 2$. On the other hand, it follows from Theorem 6 that $\langle \Gamma^N \rangle$ is exceptional only if $N = 3$. In either case, $N \leq 3$. Since $\mathcal{M}_4(\langle \Gamma^N \rangle) = \mathcal{M}_4(\mathbf{SU}(d^N))$, it holds that $\mathcal{M}_4(\langle \Gamma^4 \rangle) = \mathcal{M}_4(\mathbf{SU}(d^4))$. Moreover, $\langle \Gamma^4 \rangle$ is neither exceptional nor Lie-type, because $4 > 3$, and $\langle \Gamma^4 \rangle$ is also not extraspecial, because $\langle \Gamma^N \rangle$, and hence $\langle \Gamma^4 \rangle$, is not isomorphic to a subgroup of the Clifford group. These options exhaust the possibilities of $\langle \Gamma^4 \rangle$ being finite, so $|\langle \Gamma^4 \rangle| = \infty$. Consequently, $\mathcal{K}(\Gamma) \leq 4$. Since $2 \leq n \leq N \leq 3$ and $d \geq 2$, $d^4(n-1) + 1 \geq 4$. Therefore, $\mathcal{K}(\Gamma) \leq d^4(n-1) + 1$, as desired. ■

As a consequence of Proposition 8, we obtain the following corollary.

Corollary 10. *Let Γ be an n -qudit gate set, where $d, n \geq 2$. If there exists $N \geq n$ such that $N \geq 4$, $\mathcal{M}_4(\langle \Gamma^N \rangle) = \mathcal{M}_4(\mathbf{SU}(d^N))$, and $\langle \Gamma^N \rangle$ is not extraspecial, then Γ is eventually universal and $\mathcal{K}(\Gamma) \leq d^4(n-1) + 1$.*

Altogether, these results prove Theorem 1.

Proof of Theorem 1. If $\mathcal{K}(\Gamma) \leq d^4(n-1) + 1$, then Γ is eventually universal because $\mathcal{K}(\Gamma) < \infty$. For the other direction, suppose that Γ is eventually universal. Then, by Corollary 3, there exists $N \geq n$ such that $\mathcal{M}_4(\Gamma^N) = \mathcal{M}_4(\mathbf{SU}(d^N))$. By Theorem 5, the smallest such N satisfies $N \leq d^4(n-1) + 1$. For this N , it follows from Proposition 7 that $\langle \Gamma^N \rangle$ is not extraspecial, because Γ is eventually universal. Consequently, by Proposition 8 and Corollary 10, $\mathcal{K}(\Gamma) \leq d^4(n-1) + 1$, as desired. ■

4. DISCUSSION

In this work, we have improved the previously best known upper bound on the number of ancillary qudits needed for an eventually universal n -qudit gate set to exhibit universality. Our methods are similar to Ivanyos’ [13], who gave the first non-trivial upper bound of roughly $d^8 n$. By contrast, our upper bound is essentially a quadratic improvement and is roughly $d^4 n$.

Our work leaves several questions open. First, it is unclear whether our new bound is optimal. While we have, in a sense, maximally exploited Larsen’s alternative in the sense that our methods use the 4th moment function (as opposed to the 8th moment function, like in [13]), it is conceivable that a more nuanced criterion for eventual universality could exist, and that this new criterion could support better upper bounds.

Second, there is the related question of *lower* bounds on eventual universality. These are known for some gate sets (e.g., those studied in [14]), however they are unknown for more general gate sets. We discuss this in more detail in Appendix C.

Finally, the basic techniques used in this paper are applicable to non-unitary groups as well. Since post-selected quantum circuits are essentially just general linear transformations [1], it could be interesting to mimic this study but for “eventual post-selected universality”.

We hope our work inspires more research in these directions.

APPENDIX A. PROOF OF THEOREM 5

In this section, we will prove Theorem 5, which we restate below for convenience.

Theorem 5. *Let Γ be an n -qudit gate set for which there exists $N \geq n$ such that $\mathcal{M}_4(\Gamma^N) = \mathcal{M}_4(\mathbf{SU}(d^N))$. Then, the smallest such N satisfies $N \leq d^4(n-1) + 1$.*

Our proof of this uses techniques that are largely inspired by the methods used in [13].

Recall that, conceptually, Γ^N is the set of all N -qudit gates formed by applying elements of Γ to any subset of n qudits, and then leaving the remaining $N - n$ qudits unchanged. Formally,

$$\Gamma^N := \{ \pi(\gamma \otimes I) \pi^{-1} : \gamma \in \Gamma, \pi \in S_N \},$$

where S_N is the symmetric group of order N . Observe that as N grows, the only aspect of Γ^N that changes is the set of available permutations. In particular, the underlying “fundamental” gates $\gamma \in \Gamma$ are independent of N . This suggests that there is a way to separate the behavior of Γ^N as given by the elements of Γ from the behavior of Γ^N as given by the permutations S_N . Indeed, this is the essential idea underlying the following result.

Lemma 11. (Lemma 4 in [13]) *Let $d, n \geq 2$ and $N \geq n$, let Γ be an n -qudit gate set, and let Σ_N be a generating set of S_N . Then, $\langle \Gamma^N \rangle$ is dense in $\mathbf{SU}(d^N)$ if and only if $\langle (\Gamma \otimes I_{N-n}) \cup \Sigma_N \rangle$ is dense in $\mathbf{SU}(d^N)$.*

Consequently, we can think of Γ^N as simply a gate set consisting of the elements of Γ together with a generating set of all permutations over the N qudits (e.g., the set of all pairwise qudit SWAP gates). We adopt this interpretation of Γ^N for the remainder of this section.

Ultimately, this interpretation of Γ^N will allow us to relate Γ to a particular *polynomial ideal* $J(\langle \Gamma \rangle)$ whose degree N part $J_N(\langle \Gamma \rangle)$ will “correspond” to Γ^N . The essential idea for this comes from *invariant theory*.

To be more precise, let m be a positive integer, and consider the $\mathbb{C}$ -vector space $\mathbb{C}^m$ with dual space $(\mathbb{C}^m)^* := \text{Hom}_{\mathbb{C}}(\mathbb{C}^m, \mathbb{C})$. It is an elementary fact that if G is a subgroup of the general linear group $\mathbf{GL}(m, \mathbb{C})$, then $\mathbb{C}^m$ is a left $\mathbb{C}[G]$ -module and $(\mathbb{C}^m)^*$ is a right $\mathbb{C}[G]$ -module. This means that $\mathbb{C}^m ((\mathbb{C}^m)^*)$ is also an abelian group that admits left (right) scalar multiplication by elements of $\mathbb{C}[G]$, the ring of polynomials with coefficients from $\mathbb{C}$ and variables from G .

Now suppose $G \leq \mathbf{GL}(m, \mathbb{C})$ acts on $\mathbb{C}^m$, and let $R = \mathbb{C}[x_1, \dots, x_m]$ be the (commutative) polynomial ring on the variables $\{x_1, \dots, x_m\}$. Then, a polynomial $f(\mathbf{x}) \in R$ is said to be *invariant* under G if and only if $f(\mathbf{x}) = f(g\mathbf{x})$ for all $g \in G$. The *invariant subring* of G , denoted R^G , is the subring of R consisting of all the polynomials that are invariant under G .

Interestingly, as the next theorem shows, for almost all positive integers N , the dimension of the invariant homomorphism space of G , i.e., $\dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}[G]}((\mathbb{C}^m)^{\otimes N}, \mathbb{C})$, equals the size of the “slice” of degree N elements of the invariant subring R^G .

Theorem 12 (Section 3.1 in [13]). *Let m and n be positive integers, let $W = \mathbb{C}^m$, let Γ be a finite generating set of $G \leq \mathbf{GL}(m, \mathbb{C})$, and let $R = \mathbb{C}[x_1, \dots, x_m]$. Then, there exists a polynomial ideal $J(G) \subseteq R$, generated by homogeneous polynomials of degree n , such that for every $N \geq n$,*

$$\dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}[\Gamma^N]}(W^{\otimes N}, \mathbb{C}) = \dim(R_N / J_N(G)),$$

where R_N and $J_N(G)$ denote the degree N “slice” of R and $J(G)$, respectively, i.e., the homogeneous polynomials in R and $J(G)$, respectively, with total degree N , including the zero polynomial.²

²Ivanyos gives this result in terms of the dimension of the quotient ring $\dim(R_N / J_N(G))$, but this is equivalent to the dimension of the invariant subring $\dim R_N^G$ due to duality, see [10].

This equivalence is the key to understanding how $\mathcal{M}_4(\Gamma^N)$ behaves as a function of N , where, recall, $\mathcal{M}_4(\Gamma^N)$ is our notational shorthand for $\mathcal{M}_4(\text{cl}(\langle \Gamma^N \rangle))$. To see how this works, we start by revisiting the definition of the $2k$ th moment of G , $\mathcal{M}_{2k}(G)$, which we originally defined in terms of a particular integral over the Haar measure on a compact group $G \leq \mathbf{GL}(m, \mathbb{C})$,

$$\mathcal{M}_{2k}(G) = \int_{g \in G} |\text{tr}(g)|^{2k} \mu_{\text{Haar}}(G).$$

However, as explained in detail in [18], and as discussed in [17, 22], there is in fact a natural generalization of these moment functions to non-compact G . In particular, $\mathcal{M}_{2k}(G)$ has a more general interpretation as the dimension of a particular invariant space, namely, the space of $\mathbb{C}[G]$ -module homomorphisms from $(\mathbb{C}^m \otimes (\mathbb{C}^m)^*)^{\otimes k}$ to $\mathbb{C}$,

$$\mathcal{M}_{2k}(G) := \dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}[G]} \left((\mathbb{C}^m \otimes (\mathbb{C}^m)^*)^{\otimes k}, \mathbb{C} \right).$$

We note that this abstract form of the moment function is precisely how Larsen's Alternative generalizes to non-compact groups.

Combining this more general definition of the moment function with Theorem 12, if $G = \langle \Gamma^N \rangle \leq \mathbf{GL}(d, \mathbb{C})$ and $W = \mathbb{C}^d \otimes (\mathbb{C}^d)^*$ so that $W^{\otimes 2} \cong \mathbb{C}^{d^4}$, then for all $N \geq n$,

$$\begin{aligned} \mathcal{M}_4(\Gamma^N) &= \dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}[\langle \Gamma^N \rangle]} (W^{\otimes 2}, \mathbb{C}) \\ &= \dim (R_N / J_N(\langle \Gamma \rangle)), \end{aligned}$$

where $R = \mathbb{C}[x_1, \dots, x_{d^4}]$. Since $\mathcal{M}_4(\mathbf{SU}(d^N)) = 2$ for all $N \geq 2$ [12], we get that $\mathcal{M}_4(\Gamma^N) = \mathcal{M}_4(\mathbf{SU}(d^N))$ if and only if $\dim (R_N / J_N(\langle \Gamma \rangle)) = 2$. Therefore, to prove Theorem 5, it suffices to determine the smallest N_0 such that for all $N \geq N_0$, $\dim (R_N / J_N(\langle \Gamma \rangle)) = 2$ (assuming, of course, that such an N_0 even exists).

We have now recast the proof of Theorem 5 into a question about the quotient of particular polynomial ideal. Therefore, we can use some tools from algebraic geometry for assistance. For a homogeneous ideal J , the map $N \mapsto \dim(\mathbb{C}[x_1, \dots, x_m]_N / J_N)$ is called the *Hilbert function of J* , and it is typically denoted as $HF_J(N)$. Importantly, the Hilbert function is always “eventually” polynomial. In other words, for all homogeneous ideals J , there exists a polynomial HP_J (called the *Hilbert polynomial of J*) and an integer N_0 such that for all $N \geq N_0$, $HF_J(N) = HP_J(N)$. The smallest N_0 with this property is called the *index of regularity of J* .

In this language, then, if there exists $N \geq n$ such that $\mathcal{M}_4(\Gamma^N) = \mathcal{M}_4(\mathbf{SU}(d^N)) = 2$, then the Hilbert polynomial of the ideal $J(\langle \Gamma \rangle)$ is simply the degree-0 polynomial $HP_{J(\langle \Gamma \rangle)}(N) = 2$.

Finally, in the particular case that the Hilbert polynomial of an ideal $J \subseteq \mathbb{C}[x_1, \dots, x_m]$ is *constant*, Lazard proved that if J is generated by homogeneous polynomials of degree n , then the index of regularity is bounded above by $m(n-1) + 1$ [19, 20]. In our case, $J(\langle \Gamma \rangle)$ is a polynomial ideal in $R = \mathbb{C}[x_1, \dots, x_{d^4}]$, and is indeed generated by homogeneous polynomials of degree n . Therefore, Lazard's bound shows that if there exists an N such that $\mathcal{M}_4(\Gamma^N) = \mathcal{M}_4(\mathbf{SU}(d^N)) = 2$, then $N \leq d^4(n-1) + 1$. This completes the proof of Theorem 5.

APPENDIX B. PROOF OF LEMMA 9

In this section, we will prove Lemma 9, which we restate below for convenience.

Lemma 9. *Let $d, N \geq 2$. Then, there exists a positive integer k such that $d^N \in \{(3^k \pm 1)/2, (2^k + (-1)^k)/3\}$ if and only if $N = 2$ and $d \in \{2, 11\}$.*

Our proof relies on three lemmas to do with the theory of Diophantine equations.

Lemma 13 (Theorem 3 in [25]). *The equation*

$$y^q = \frac{x^n - 1}{x - 1}$$

has only three solutions in integers with $2 \leq x \leq 10^6$, $y > 1$, $n > 2$, and $q \geq 2$, namely, (x, y, n, q) is either $(3, 11, 5, 2)$, $(7, 20, 4, 2)$, or $(18, 7, 3, 3)$.

Lemma 14 (Theorem 2 in [25]). *The equation*

$$y^q = \frac{x^n + 1}{x + 1}$$

has no solution in integers with $2 \leq x \leq 10^4$, $n \geq 5$ odd, $y > 1$, and $q \geq 2$.

Lemma 15 (Lemma in [4]). *The equation $y^2 - 2z^k = -1$ has only two solutions in integers with $k > 2$, namely, (y, z, k) is either $(239, 13, 4)$ or $(1, 1, k)$.*

We now prove Lemma 9.

Proof of Lemma 9. We will show that $N = 2$ and $d \in \{2, 11\}$ are the only possibilities via a case-by-case study.

Case 1: Suppose $d^N = (3^k - 1)/2$. Then,

$$d^N = \frac{3^k - 1}{3 - 1}.$$

By Lemma 13, the only solution in integers to this equation with $k \geq 2$ is $(d, N, k) = (11, 2, 5)$. If $k = 2$, then the only solution is $(d, N, k) = (2, 2, 2)$. By Lemma 13, these are the only solutions.

Case 2: Suppose $d^N = (3^k + 1)/2$. Then,

$$2d^N = 3^k + 1.$$

We will show that there are no integer solutions in d, N , and k with $d, N \geq 2$. If d is even, then $2d^N = 0 \pmod{8}$, however $3^k + 1 \in \{2, 4\} \pmod{8}$. Therefore, d is odd. Since $3^k + 1 = 1 \pmod{3}$, $2d^N = 1 \pmod{3}$ as well, so $d^N \equiv 2 \pmod{3}$. Consequently, $d \not\equiv \{0, 1\} \pmod{3}$, which is to say that $d \equiv 2 \pmod{3}$. Therefore, $d^N = 2^N \equiv 2 \pmod{3}$, which implies that N is odd. Since d is also odd, $d^N \in \{1, 3, 5, 7\} \pmod{8}$, so $2d^N \in \{2, 6\} \pmod{8}$. However, $3^k + 1 = 2 \pmod{8}$ if k is even, and $3^k + 1 = 4 \pmod{8}$ if k is odd. Thus, k is even, so $k = 2\ell$ for some integer ℓ . Rearranging the equation in Case 2, we get that $2d^N - 3^{2\ell} = 1$, or equivalently,

$$2d^N - (3^\ell)^2 = 1.$$

By Lemma 15, there are no integer solutions to this expression with $d \geq 2$ and $N \geq 3$. Finally since we know from above that N must be odd, $N = 2$ can also not yield a valid solution, so there are no integer solutions to the equation $d^N = (3^k + 1)/2$ with $d \geq 2$ and $N \geq 2$.

Case 3: Suppose $d^N = (2^k - (-1)^k)/3$. We will show that there are no integer solutions in d, N , and k with $d, N \geq 2$. On one hand, if k is even, then $k = 2\ell$ for some integer ℓ . Thus,

$$d^N = \frac{2^k - 1}{3} = \frac{2^{2\ell} - 1}{3} = \frac{4^\ell - 1}{4 - 1}.$$

By Lemma 13, there are no integer solutions to this equation with $\ell \geq 3$. It is straightforward to check that $\ell \in \{1, 2\}$ do not yield valid solutions either. On the other hand, if k is odd, then

$$d^N = \frac{2^k + 1}{3} = \frac{2^k + 1}{2 + 1}.$$

By Lemma 14, there are no integer solutions to this equation with $k \geq 5$. Since $d, N \geq 2$, it is straightforward to check that $k = 3$ does not yield a valid solution either.

Altogether, the only valid solution to the premise of Lemma 9 derives from Case 1, where $N = 2$ and $d \in \{2, 11\}$. This is the desired result. $\blacksquare$

APPENDIX C. JEANDEL'S CONSTRUCTION

Here, we review the main idea in Jeandel's paper [14], which not only establishes the existence of eventually universal n -qudit gate sets Γ with $\mathcal{K}(\Gamma) > n$, but which also gives a general method to construct n -qubit ($d = 2$) gate sets Γ for which $2n - 5 \leq \mathcal{K}(\Gamma) \leq 2n - 3$.

Let Ω be a universal 2-qubit gate set with elements $A_1, A_2, \dots, A_{|\Omega|}$, and suppose that for all i , $A_i^2 = I$, where I is the identity operation. For any positive integer $k \geq 2$, we define a $(k + 2)$ -qubit gate set Γ implicitly as follows: $B_{k,i} \in \Gamma$ if and only if for all $|t\rangle \in \mathbb{C}^4$ and all $|c\rangle \in \mathbb{C}^{2^k}$,

$$B_{k,i}(|t\rangle \otimes |c\rangle) = \begin{cases} (A_i |t\rangle) \otimes |c\rangle & \text{if } |c\rangle \in \{|0\rangle^{\otimes k}, |1\rangle^{\otimes k}\}, \\ |t\rangle \otimes |c\rangle & \text{otherwise.} \end{cases}$$

Conceptually, $B_{k,i} \in \Gamma$ provided it applies $A_i \in \Omega$ to the first two qubits if and only if the latter k qubits are either all $|0\rangle$ or all $|1\rangle$.

We claim that Γ is not universal on fewer than $2k - 2$ qubits. To see this, consider the action of Γ on the subspace spanned by $|0\rangle^{k-1} \otimes |1\rangle^{k-1}$ up to permutations of the qubits (i.e., any computational basis state with $k - 1$ $|0\rangle$'s and $k - 1$ $|1\rangle$'s). By construction, no subset of k qubits satisfies the control conditions of the individual gates $B_{k,i}$, so every such gate leaves this subspace invariant. As such, Γ is not universal on $2k - 2$ qubits.

On the other hand, at least for some specific values of k , $B_{k,i}$ is universal on $2k + 1$ qubits. To see this, consider a set of $2k + 1$ qubits, and suppose that we want to apply A_i to the first two qubits. To do this, we need to act $B_{k,i}$ on a $k + 2$ qubit subsystem that includes the first two qubits, as well as k control qubits. These control qubits are selected as a subset of the remaining $2k - 1$ qubits. However, we do not know the state of those $2k - 1$ qubits, and so a priori we do not know which subset of k qubits to select as the controls. So, instead of selecting any particular subset, we will simply try every subset, and apply the $B_{k,i}$ gate $\binom{2k-1}{k}$ times. The question, then, is how many times is the gate A_i applied to the first 2 qubits? We will show that for an appropriate choice of k , no matter the state over the $2k - 1$ qubits, A_i will be applied exactly once on the first two qubits.

Let $|\psi\rangle$ be any computational basis state on $2k - 1$ qubits. Then $|\psi\rangle$ contains at least k tensor factors of either $|0\rangle$ or $|1\rangle$. Without loss of generality, suppose that there are $k + q$ tensor factors of $|0\rangle$, where $0 \leq q \leq k - 1$. Then, the number of times that the gate A_i is applied on the first two qubits is $\binom{k+q}{k}$. The key observation is that if $k = 2^j$ and $q \leq k - 1$, then $\binom{k+q}{k}$ is odd. (This follows from inducting on j .)

Thus, by the reasoning above, for any computational basis state $|\psi\rangle$ on $2k - 1$ qubits, applying $B_{k,i}$ $\binom{2k-1}{k}$ times, once for every subset of the k control qubits, results in A_i being applied exactly once to the first two qubits, provided k is a power of two. Since this will be true for any computational basis state over the $2k - 1$ qubits, this construction will hold for any superposition state over them as well.

If we now want to apply the gate A_i on a different set of two qubits, we just separate those two qubits as "the first two" and repeat the exact same process as described above. As such, the gates in Ω can be applied on *any* of the $2k + 1$ qubits, which proves that Γ is universal on $2k + 1$ qubits.

Altogether, then, we have shown that there exists a $(k+2)$ -qubit gate set Γ for which $2k-1 \leq \mathcal{K}(\Gamma) \leq 2k+1$. With $n = k+2$, we have equivalently shown the existence of an n -qubit gate set Γ for which $2n-5 \leq \mathcal{K}(\Gamma) \leq 2n-3$.

We note that by basically the same argument above, one can establish the existence of an n -qudit gate Γ for which $\mathcal{K}(\Gamma) \geq dn - 2d - 1$. Therefore, there exist n -qudit gate sets that are not universal on n -qudits. However, it remains to show that such gates sets are also eventually universal. Unfortunately, the upper bound argument above does not obviously generalize to qudit systems. This is because the proof for the upper bound uses the fact that when $d = 2$, one can count the number of times a gate $B_{k,i}$ is “activated” via a single binomial coefficient. When $d > 2$, however, this count is a complicated sum of binomial coefficients whose parity is not easily deducible. Thus, the argument does not go through, at least not obviously. Still, we conjecture that for all $d > 2$, there exists an *eventually universal* n -qudit gate set Γ for which $dn - 2d - 1 \leq \mathcal{K}(\Gamma)$, or something morally equivalent. We leave this as an open question.

ACKNOWLEDGMENTS

The authors thank Gabor Ivanyos, Jonathan Rosenberg, Luke Schaeffer, Amin Gholampour, Ian Teixeira, and Adam Bouland for several useful discussions.

REFERENCES

1. Scott Aaronson, *Is quantum mechanics an island in theoryspace?*, (2004).
2. Scott Aaronson, Daniel Grier, and Luke Schaeffer, *The Classification of Reversible Bit Operations*, 8th Innovations in Theoretical Computer Science Conference (ITCS 2017) (Dagstuhl, Germany) (Christos H. Papadimitriou, ed.), Leibniz International Proceedings in Informatics (LIPIcs), vol. 67, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2017, pp. 23:1–23:34.
3. 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** (2011), no. 2126, 459–472.
4. John Cohn, *Perfect Pell powers*, Glasgow Mathematical Journal **38** (1996), no. 1, 19–20.
5. K.M.R. Audenaert D. Gross and J. Eisert, *Evenly distributed unitaries: On the structure of unitary designs*, Journal of Mathematical Physics **48** (2007), no. 5, 052104.
6. David P. Divincenzo, *Two-bit gates are universal for quantum computation*, Phys. Rev. A **51** (1995), 1015.
7. N. Rizo E. Banai, G. Navarro and P.H. Tiep, *Unitary t-groups*, (2018).
8. The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.14.0*, 2024.
9. Daniel Gottesman, *The heisenberg representation of quantum computers*, 1998.
10. Werner Greub, *Multilinear algebra*, 2 ed., Springer-Verlag, New York, 1978.
11. R.M. Guralnick and P.H. Tiep, *Decompositions of small tensor powers and Larsen’s conjecture*, (2005).
12. M. Heinrich, *On stabiliser techniques and their application to simulation and certification of quantum devices*, (2021), PhD thesis, University of Cologne.
13. Gabor Ivanyos, *Deciding universality of quantum gates*, 2006.
14. E Jeandel, *Universality in quantum computation*, Proc. 31st ICALP (2004), 793–804.
15. R. Jozsa and A. Miyake, *Matchgates and classical simulation of quantum circuits*, Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences **464** (2008), no. 2100, 3089–3106.
16. Chaitanya Karamchedu, Matthew Fox, and Daniel Gottesman, *A criterion for quantum advantage*, (2024), v1, submitted 4 Nov 2024.
17. Nicholas Katz, *Larsen’s alternative, moments, and the monodromy of Lefschetz pencils*, (2004).
18. E. Kowalski, *An introduction to the representation theory of groups*, American Mathematical Society, 2014.
19. D. Lazard, *Résolution des systèmes d’équations algébriques*, Theoretical Computer Science **15** (1981), no. 1, 77–110 (French). MR 619687
20. Daniel Lazard, *Solving systems of algebraic equations*, ACM SIGSAM Bulletin **35** (2001), no. 3, 11–37, English translation by Michael Abramson of “Résolution des Systèmes d’Équations Algébriques”, Theoretical Computer Science 15 (1981), 77–110.
21. Emil L. Post, *The two-valued iterative systems of mathematical logic. (am-5)*, Princeton University Press, 1941.
22. Cheng Qin, *Fourth moments and Larsen’s alternatives*, (2021).

- 23. Y. Shi, *Both Toffoli and Controlled-NOT need little help to do universal quantum computation*, (2002), v2, revised 26 May 2002.
- 24. Barbara M. Terhal and David P. DiVincenzo, *Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games.*, Quantum Information & Computation **4** (2004), no. 2, 134–145.
- 25. Y.Bugeaud and M. Mignotte, *On the Diophantine equation $\frac{x^n-1}{x-1} = y^q$ with negative x* , Number Theory for the Millenium I (2002), 145–151.

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`