Universality verification for a set of quantum gates

Adam Sawicki,[1] Lorenzo Mattioli,[1] and Zoltán Zimborás[2,3]

[1]*Center for Theoretical Physics PAS, Aleja Lotników 32/46, PL-02-668 Warszawa, Poland*
[2]*Wigner Research Centre for Physics, P.O. Box 49, H-1525 Budapest, Hungary*
[3]*BME-MTA Lendület Quantum Information Theory Research Group, 1111 Budapest, Hungary*

(Received 28 November 2021; revised 29 March 2022; accepted 25 April 2022; published 12 May 2022)

We establish a relationship between the notion of universal quantum gates and the notion of unitary t-designs. We show that a set of qudit gates $\mathcal{S} \subset U(d)$ is universal if and only if $\mathcal{S}$ forms a δ-approximate $t(d)$-design, where $\delta < 1$, $t(2) = 6$, and $t(d) = 4$ for $d \geqslant 3$. Moreover, we argue that from the application point of view sets $\mathcal{S}$ with the δ close to 1 should be regarded as nonuniversal. We also provide a second, more algebraic, criterion for the universality verification. It says that $\mathcal{S} \subset U(d)$ is universal if and only if the matrices that commute with $\{U^{\otimes t(d)} \otimes \bar{U}^{\otimes t(d)} | U \in \mathcal{S}\}$ commute also with $\{U^{\otimes t(d)} \otimes \bar{U}^{\otimes t(d)} | U \in U(d)\}$, where $t(2) = 3$, and $t(d) = 2$ for $d \geqslant 3$. Finally, we show that the complexity of checking this algebraic criterion scales polynomially with the dimension d.

DOI: 10.1103/PhysRevA.105.052602

I. INTRODUCTION

Universal and efficient quantum gates play a central role in quantum computing [1–14]. It is well known that in order to construct a universal set of gates for many qudits it is enough to take a universal set for one qudit and extend it by a two-qudit entangling gate [15,16] (see Ref. [17] for fermionic systems). On the other hand, it is a great challenge to find a time-efficient procedure that enables deciding if a given set of gates $\mathcal{S} \subset G_d := U(d)$ is universal. Any unitary matrix U can, up to a global phase factor, be written as the exponent of a non-Hermitain traceless matrix X, i.e., $U = e^X$. Therefore, in a search for a universality checking algorithm for quantum gates it is natural to consider first an analogous universality problem for Hamiltonians, i.e., given a set of anti-Hermitian traceless matrices, $\mathcal{X} \subset \mathfrak{su}(d)$, we want to check if by taking nested commutators and linear combinations of elements form $\mathcal{X}$ we can obtain any anti-Hermitian traceless matrix. The answer turns out to be relatively simple and can be phrased in terms of the *centralizer* of the tensor squares of the elements belonging to $\mathcal{X}$ [18–20] (cf. Refs. [21–23]). It turns out that the approach through tensor powers can be extended from Hamiltonians to quantum gates. To this end one considers the centralizers of $\mathcal{S}^{t,t} = \{U^{\otimes t} \otimes \bar{U}^{\otimes t} | U \in \mathcal{S}\}$ and $G_d^{t,t} = \{U^{\otimes t} \otimes \bar{U}^{\otimes t} | U \in G_d\}$ for any t, i.e., the sets of matrices that commute with $\mathcal{S}^{t,t}$ and $G_d^{t,t}$. In Refs. [24,25] it was shown that the equality of the centralizers of $\mathcal{S}^{1,1}$ and $G_d^{1,1}$ implies that $\mathcal{S}$ is universal provided $\mathcal{S}$ generates an infinite subgroup of G_d. We will call the equality of the centralizers of $\mathcal{S}^{1,1}$ and $G_d^{1,1}$ the necessary universality condition. For $\mathcal{S}$ satisfying the necessary universality condition, in order to verify if the group generated by $\mathcal{S}$ is infinite, it is enough to check if it forms an ϵ-net with $\epsilon = \frac{1}{2\sqrt{2}}$ in the Hilbert-Schmidt distance [24–27]. To move further the notion of unitary t-designs turns out to be crucial. A t-design is an ensemble of unitaries with associated probabilities that mimics the Haar measure, i.e., the natural group theoretic notion of randomness, in a sense that it acts exactly as the Haar measure up to tth order in the statistical moments. A δ-approximate t-design possesses this property only approximately, where δ is the approximation quality parameter that takes values between zero (perfect approximation) and one (no approximation). The main interest in t-designs comes from the fact that sampling from the Haar measure requires exponential resources [28], but sampling from t-designs can be done efficiently (see, for example, Ref. [29]). The connection between t-designs and ϵ-nets has been recently established [30]. Using this connection, the authors of Ref. [30] rephrased the above-mentioned requirement of $\frac{1}{2\sqrt{2}}$ net in terms of δ-approximate t-designs and showed that $\mathcal{S}$ is universal if and only if (1) $\mathcal{S} \subset G_d$ satisfies the necessary universality condition, and (2) gates belonging to $\mathcal{S}$ form a δ-approximate $t(d)$-design, with $\delta < 1$ and $t(d) = O(d^{5/2})$.

In this paper, we show that actually the required $t(d)$ does not grow with d. Utilizing the recent results regarding the so-called unitary t-groups [31], i.e., t-designs that are also finite groups, we formulate our first universality criterion (Theorem 1). It states that $\mathcal{S} \subset G_d$ is universal if and only if $\mathcal{S}$ forms a δ-approximate $t(d)$-design, where $\delta < 1$, $t(2) = 6$, and $t(d) = 4$ for $d \geqslant 3$. Moreover, we argue that from the application point of view sets $\mathcal{S}$ with the δ close to 1 should be regarded as nonuniversal. This is because, as we show, the length of a circuit needed to approximate any unitary with a given precision ϵ for such $\mathcal{S}$ grows to infinity when δ approaches 1. Next, using further properties of t-designs, we formulate our second universality criterion (Theorem 2) which says that $\mathcal{S} \subset G_d$ is universal if and only if the centralizer of $\mathcal{S}^{t(d),t(d)}$ is equal to the centralizer $G_d^{t(d),t(d)}$, where $t(2) = 3$, and $t(d) = 2$ for $d \geqslant 3$. The equality of the centralizers can be verified by checking their dimensions. We calculate the dimensions of the centralizers of $G_d^{t(d),t(d)}$ using representation theory methods, for all $t(d)$ listed above and use them in our final criterion for universality, i.e., Theorem 3. Thus the problem reduces to finding the dimension of the centralizer of $\mathcal{S}^{t(d),t(d)}$ which is a standard linear algebra task.

II. UNIVERSALITY AND δ-APPROXIMATE t-DESIGNS

Let $\{\mathcal{S}, \nu_{\mathcal{S}}\}$ be an ensemble of quantum gates, where $\mathcal{S}$ is a finite subset of $G_d := U(d)$ and $\nu_{\mathcal{S}}$ is the uniform measure on $\mathcal{S}$. Throughout the paper we assume that $\mathcal{S}$ contains identity, which of course does not influence the universality of $\mathcal{S}$. An ensemble $\{\mathcal{S}, \nu_{\mathcal{S}}\}$ is called $\delta(t, \nu_{\mathcal{S}})$-approximate t-design if and only if

$$\delta(t, \nu_{\mathcal{S}}) := \|T_{\nu_{\mathcal{S}},t} - T_{\mu,t}\|_{\infty} < 1, \tag{1}$$

where $\|\cdot\|$ is the operator norm and for any measure ν (in particular for the Haar measure μ) we define a *moment operator*

$$T_{\nu,t} := \int_{G_d} d\nu(U) U^{\otimes t} \otimes \bar{U}^{\otimes t}. \tag{2}$$

One can easily show that $0 \leqslant \delta(t, \nu_{\mathcal{S}}) \leqslant 1$ [30]. When $\delta(t, \nu_{\mathcal{S}}) = 0$ we say that $\mathcal{S}$ is *an exact t-design* and when $\delta(t, \nu_{\mathcal{S}}) = 1$ we say that $\mathcal{S}$ is *not a t-design*. In order to give an equivalent definition of an exact t-design [32,33], we recall the definition of an S^t-twirl of an operator A:

$$\int_{G_d} d\nu_{\mathcal{S}}(U) U^{\otimes t} A (U^{\dagger})^{\otimes t}. \tag{3}$$

$\mathcal{S}$ is an exact t-design if and only if for any operator A the S^t-twirl and the G_d^t-twirl coincide, i.e.,

$$\int_{G_d} d\nu_{\mathcal{S}}(U) U^{\otimes t} A (U^{\dagger})^{\otimes t} = \int_{G_d} d\mu(U) U^{\otimes t} A (U^{\dagger})^{\otimes t}. \tag{4}$$

To proceed, we note that a map $U \mapsto U^{\otimes t} \otimes \bar{U}^{\otimes t}$ is a representation of the unitary group G_d. This representation turns out to be reducible and as such it decomposes into some irreducible representations π of G_d,

$$U^{\otimes t} \otimes \bar{U}^{\otimes t} \simeq \bigoplus_{\pi} \pi(U)^{\oplus m_{\pi}} \simeq (U \otimes \bar{U})^{\otimes t}, \tag{5}$$

where m_{π} is the multiplicity of π. The representations occurring in this decomposition are in fact irreducible representation of the projective unitary group, $PG_d = G_d/\sim$, where $U \sim V$ if and only if $U = e^{i\phi} V$. One can show that every irreducible representation of PG_d arises this way for some, possibly large, t [34]. For $t = 1$ the decomposition (5) is particularly simple and reads $U \otimes \bar{U} = \mathrm{Ad}_U \oplus 1$, where 1 stands for the trivial representation and Ad_U is the adjoint representation of G_d and $PG_d \simeq \mathrm{Ad}_{G_d}$. Next, we define the notion of a group generated by a gate set.

Definition 1. Let $\mathcal{S} \subset G_d$ be a set of quantum gates. The group $G_{\mathcal{S}}$ generated by $\mathcal{S}$ is

$$G_{\mathcal{S}} := \mathrm{cl}(\langle \mathcal{S} \rangle), \tag{6}$$

$$\langle \mathcal{S} \rangle := \bigcup_{l \in \mathbb{N}} \mathcal{S}_l, \quad \mathcal{S}_l := \{g_1 g_2 \cdots g_l | g_i \in \mathcal{S}\}. \tag{7}$$

The closure in (6) corresponds to adding all the limiting points of the sequences of words from $\mathcal{S}_l$ when l goes to infinity. We next introduce the notion of a universal gate set.

Definition 2. A set $\mathcal{S} \subset G_d$ is universal if and only if $PG_d \simeq G_{\mathcal{S}}/\sim$, where $U \sim V$ if and only if $U = e^{i\phi} V$.

In other words, a set $\mathcal{S}$ is universal if, up to a phase factor, any unitary can be approximated to any precision by a finite product of elements from $\mathcal{S}$. Having a representation π of G_d we can consider its restriction to $G_{\mathcal{S}}$, which we denote by $\mathrm{Res}^{G_d}_{G_{\mathcal{S}}} \pi$. For any $U \in G_{\mathcal{S}}$ we simply have

$$\mathrm{Res}^{G_d}_{G_{\mathcal{S}}} \pi(U) = \pi(U). \tag{8}$$

A crucial observation here is that $\mathrm{Res}^{G_d}_{G_{\mathcal{S}}} \pi$ can be a reducible representation of $G_{\mathcal{S}}$ even though π is an irreducible representation of G_d. This observation plays a central role in representation theory (cf. branching rules) and turns out to be central in our context. For any irreducible representations occurring in the decomposition (5) we can consider the restriction of $T_{\nu_{\mathcal{S}},t}$ to π which is given by

$$T_{\nu_{\mathcal{S}},t,\pi} = \int_{G_d} d\nu_{\mathcal{S}}(U) \pi(U). \tag{9}$$

It follows directly from the definitions and discussion above that

$$T_{\nu_{\mathcal{S}},t} \simeq \bigoplus_{\pi} (T_{\nu_{\mathcal{S}},t,\pi})^{\oplus m_{\pi}}, \tag{10}$$

where π goes over irreducible representations occurring in the decomposition (5). Moreover,

$$\delta(t, \nu_{\mathcal{S}}) = \sup_{\pi} \|T_{\nu_{\mathcal{S}},t,\pi}\|_{\infty}, \tag{11}$$

where this time π goes over nontrivial irreducible representations occurring in the decomposition (5).

Lemma 1. Let $\mathcal{S} \subset G_d$ be an arbitrary set of quantum gates. Then $\delta(t, \nu_{\mathcal{S}}) = 1$ if and only if for some nontrivial irreducible representation π appearing in the decomposition (5) representation $\mathrm{Res}^{G_d}_{G_{\mathcal{S}}} \pi$ is reducible and contains a copy of the trivial representation.

Proof. The implication "$\Leftarrow$" is obvious. For "$\Rightarrow$" assume that $\delta(t, \nu_{\mathcal{S}}) = 1$. Then for some irreducible nontrivial representation π appearing in the decomposition (5) we have $\|T_{\nu_{\mathcal{S}},t,\pi}\| = 1$. There exists a vector of norm one, $v \in V_{\pi}$, such that $\sum_{g,h \in \mathcal{S}} \pi(gh^{\dagger}) v = |\mathcal{S}|^2 v$. Hence, $\sum_{g,h \in \mathcal{S}} \langle v | \pi(gh^{\dagger}) v \rangle = |\mathcal{S}|^2$. By the unitarity of $\pi(gh^{\dagger})$ we have $|\langle v | \pi(gh^{\dagger}) v \rangle| \leqslant 1$, for any $v \in V_{\pi}$ of norm one. Thus $\forall g, h \in \mathcal{S}\, \pi(g) v = \pi(h) v$. Note, however, that under the assumption that $I \in \mathcal{S}$, this implies $\forall g \in \mathcal{S}\, \pi(g) v = v$ which means v is a common eigenvector of all operators $\pi(g)$, $g \in \mathcal{S}$. This in turn means that $\mathrm{Res}^{G_d}_{G_{\mathcal{S}}} \pi$ is reducible and contains a copy of the trivial representation. This ends the proof. ■

Remark 1. The following is an equivalent way of formulating Lemma 1 using Eq. (4): $\{\mathcal{S}, \nu_{\mathcal{S}}\}$ is not a t-design if and only if there exists an operator A such that $A = \int_{G_d} d\nu_{\mathcal{S}}(U) U^{\otimes t} A (U^{\dagger})^{\otimes t} \neq \int_{G_d} d\mu(U) U^{\otimes t} A (U^{\dagger})^{\otimes t}$.

Corollary 1. Assume $\mathcal{S}$ is universal. Then $\delta(t, \nu_{\mathcal{S}}) < 1$ for any finite t.

Proof. When $\mathcal{S}$ is a universal set, $PG_d = G_{\mathcal{S}}/\sim$ and hence the restriction of any irreducible representation π of PG_d to $G_{\mathcal{S}}$ remains irreducible. ■

Let us next define

$$\mathcal{S}^{t_1,t_2} = \{U^{\otimes t_1} \otimes \bar{U}^{\otimes t_2} | U \in \mathcal{S}\},$$

$$G_d^{t_1,t_2} = \{U^{\otimes t_1} \otimes \bar{U}^{\otimes t_2} | U \in G_d\}.$$

We will denote $\mathcal{S}^{t,0}$ by $\mathcal{S}^t$ and $G_d^{t,0}$ by G_d^t. For any set of matrices $B \subset \mathcal{B}(\mathbb{C}^n)$ let

$$\mathcal{C}(B) = \{X \in \mathcal{B}(\mathbb{C}^n) | [X, Y] = 0, \ \forall Y \in B\}. \tag{12}$$

Using $U \otimes \bar{U} = \mathrm{Ad}_U \oplus 1$ we can rewrite Lemma 3.4 from Ref. [24] as follows:

Lemma 2. Assume $\mathcal{S}$ is such that

$$\mathcal{C}(\mathcal{S}^{1,1}) = \mathcal{C}(G_d^{1,1}). \tag{13}$$

Then $\mathcal{S}$ is universal if and only if $G_{\mathcal{S}}$ is infinite.

In other words, whenever the condition (13) is satisfied, $\mathcal{S}$ is either universal or $G_{\mathcal{S}}$ is a finite subgroup of G_d. In what follows we will call the condition (13) the necessary universality condition. We note also that we always have $\mathcal{C}(\mathcal{S}^{t,t}) = \mathcal{C}(G_{\mathcal{S}}^{t,t})$. Lemma 2 implies that finite groups satisfying the necessary universality condition play a central role in deciding whether $\mathcal{S}$ is universal.

Definition 3. A finite subgroup $G \subset G_d$ is a unitary t-group if and only if $\delta(t, \nu_G) = 0$, where ν_G is the uniform measure on G.

The concept of unitary t-groups will play a central role in what follows.

Lemma 3. Assume that $\mathcal{S}$ is a generating set of a finite subgroup of G_d. Then for any t, either $\delta(t, \nu_{G_{\mathcal{S}}}) = 0$ or $\delta(t, \nu_{G_{\mathcal{S}}}) = 1$. Moreover, for any t (1) either $\delta(t, \nu_{\mathcal{S}}) < 1$ if and only if $\delta(t, \nu_{G_{\mathcal{S}}}) = 0$ or (2) $\delta(t, \nu_{\mathcal{S}}) = 1$ if and only if $\delta(t, \nu_{G_{\mathcal{S}}}) = 1$.

Proof. One can easily verify that for any measure ν, $\delta(t, \nu^{*l}) = \delta(t, \nu)^l$, where ν^{*l} is the l-fold convolution of measure ν. Under the assumption that $G_{\mathcal{S}}$ is finite there is l_0 such that $\mathcal{S}_{l_0} = G_{\mathcal{S}}$. On the other hand, it is known [35] that for $l \to \infty$ the measure $\nu_{\mathcal{S}}^{*l}$ converges to $\nu_{G_{\mathcal{S}}}$. Thus we have $\delta(t, \nu_{\mathcal{S}})^l \to \delta(t, \nu_{G_{\mathcal{S}}})$. Note, however, that $\nu_{G_{\mathcal{S}}} = \nu_{G_{\mathcal{S}}}^{*2}$. Thus $\delta(t, \nu_{G_{\mathcal{S}}}) = 0$ or $\delta(t, \nu_{G_{\mathcal{S}}}) = 1$. The result follows. ■

Recently there has been some development in the theory of unitary t-groups. The main result of Ref. [31] states the following:

Fact 1. There are no finite unitary t-groups in G_d for $t \geqslant 6$ and $d \geqslant 2$. Moreover:

(1) When $d = 2$ there is unitary 5-group but no unitary t-group with $t \geqslant 6$.

(2) When $d \geqslant 3$ there is no unitary t-group with $t \geqslant 4$.

This leads to our first main result.

Theorem 1. Let $\mathcal{S}$ be a set of gates in G_d such that $\mathcal{C}(\mathcal{S}^{1,1}) = \mathcal{C}(G_d^{1,1})$. Then $\mathcal{S}$ is universal if and only if

(1) $\{\mathcal{S}, \nu_{\mathcal{S}}\}$ is a δ-approximate 6-design with $\delta < 1$, when $d = 2$,

(2) $\{\mathcal{S}, \nu_{\mathcal{S}}\}$ is a δ-approximate 4-design with $\delta < 1$, when $d \geqslant 3$.

Proof. By Lemma 2 the set $\mathcal{S}$ can be either universal or $G_{\mathcal{S}}$ is a finite group. If $\mathcal{S}$ is universal, then by Corollary 1 we have that $\delta(t, \nu_{\mathcal{S}}) < 1$ for any $t \geqslant 1$. On the other hand, if $G_{\mathcal{S}}$ is a finite group, then by Lemma 3 and Fact 1 we can only have (1) $\delta(t, \nu_{\mathcal{S}}) = 1$ for $t = 6$ and $d = 2$, and (2) $\delta(t, \nu_{\mathcal{S}}) = 1$ for $t = 4$ and $d > 2$. This finishes the proof. ■

III. UNIVERSALITY AND CENTRALIZERS

In order to state our second universality criterion we will need the following lemma.

Lemma 4. Assume that for some $t \geqslant 2$,

$$\mathcal{C}(\mathcal{S}^{t,t}) = \mathcal{C}\big(G_d^{t,t}\big). \tag{14}$$

Then any irreducible representation occurring in the decomposition (5) remains irreducible when restricted to $G_{\mathcal{S}}$. Moreover, $\mathcal{C}(\mathcal{S}^{1,1}) = \mathcal{C}(G_d^{1,1})$.

Proof. The fact that any irreducible representation occurring in the decomposition (5) remains irreducible when restricted to $G_{\mathcal{S}}$ is obvious. For the second part of the statement note that

$$\begin{aligned} U^{\otimes t} \otimes \bar{U}^{\otimes t} &\simeq (U^{\otimes t-1} \otimes \bar{U}^{\otimes t-1}) \otimes (\mathrm{Ad}_U \oplus 1) \\ &= [(U^{\otimes t-1} \otimes \bar{U}^{\otimes t-1}) \otimes \mathrm{Ad}_U] \\ &\quad \times \oplus (U^{\otimes t-1} \otimes \bar{U}^{\otimes t-1}). \end{aligned} \tag{15}$$

Repeating this decomposition we get that $U \otimes \bar{U}$ is one of the summands in the decomposition of $U^{\otimes t} \otimes \bar{U}^{\otimes t}$. Hence, under condition (14) we have $\mathrm{Res}^{G_d}_{G_{\mathcal{S}}} \mathrm{Ad}$ is irreducible. Thus $\mathcal{C}(\mathcal{S}^{1,1}) = \mathcal{C}(G_d^{1,1})$. ■

We can now formulate a sufficient condition for universality in terms of centralizers.

Corollary 2. Let $\mathcal{S}$ be a set of gates in G_d. Then $\mathcal{S}$ is universal if and only if for $t(2) = 6$ and $t(d) = 4$ for $d > 2$ we have

$$\mathcal{C}(\mathcal{S}^{t(d),t(d)}) = \mathcal{C}\big(G_d^{t(d),t(d)}\big). \tag{16}$$

Proof. The condition (16) combined with Lemma 4 implies that the necessary condition for universality is satisfied and that all irreducible representations occurring in the decomposition (5) remain irreducible when restricted to $G_{\mathcal{S}}$, where $t(d)$ is as in the statement of the theorem. Hence by Lemma 1 we have $\delta(6, \nu_{\mathcal{S}}) \neq 1$ for $d = 2$ and $\delta(4, \nu_{\mathcal{S}}) \neq 1$ for $d > 2$. Assume $G_{\mathcal{S}}$ is a finite group. Then by Lemma 3 and Fact 1 we have $\delta(6, \nu_{\mathcal{S}}) = 1$ for $d = 2$ and $\delta(4, \nu_{\mathcal{S}}) = 1$ for $d > 2$. Thus we get a contradiction and $\mathcal{S}$ is universal. ■

Corollary 2 can be further improved. For this, we will use a technique connecting $\mathcal{C}(\mathcal{S}^{t_1,t_2})$ with $\mathcal{C}(\mathcal{S}^{t_1-n,t_2+n})$ through a partial transpose map. To be more concrete, we will use the following lemma:

Lemma 5. Let $\mathcal{S}$ be a set of gates in G_d, and let θ denote the transposition operator on $\mathcal{B}(\mathbb{C}^d)$. Then for any non-negative integer number $n \leqslant t$, we have that

$$\mathrm{id}^{\otimes(t-n)} \otimes \theta^{\otimes n}[\mathcal{C}(\mathcal{S}^t)] = \mathcal{C}(\mathcal{S}^{t-n,n}). \tag{17}$$

In particular, the dimensions of $\mathcal{C}(\mathcal{S}^t)$ and $\mathcal{C}(\mathcal{S}^{t-n,n})$ are equal.

Proof. Let $X = \sum_i X_i^1 \otimes X_i^2 \cdots \otimes X_i^t$ be an element of $\mathcal{C}(\mathcal{S}^t)$ (note that the upper index is indeed an index, not an exponent). Using the notations $m = t - n$ and $B^T = \theta(B)$ (and noting that $U^T = \bar{U}^\dagger$ for any unitary), we calculate the adjoint action of an arbitrary $U^{\otimes m} \otimes \bar{U}^{\otimes n} \in \mathcal{S}^{m,n}$ (with $U \in \mathcal{S}$) on $\mathrm{id}^{\otimes m} \otimes \theta^{\otimes n}(X)$,

$$\begin{aligned} U^{\otimes m} \otimes \bar{U}^{\otimes n}[\mathrm{id}^{\otimes m} \otimes \theta^{\otimes n}(X)](U^{\otimes m} \otimes \bar{U}^{\otimes n})^{\dagger} &= \sum_i UX_i^1U^{\dagger} \otimes \cdots UX_i^mU^{\dagger} \otimes \bar{U}\left(X_i^{m+1}\right)^T \bar{U}^{\dagger} \otimes \cdots \bar{U}\left(X_i^t\right)^T \bar{U}^{\dagger} \\ &= \sum_i UX_i^1U^{\dagger} \otimes \cdots \otimes (U^{\dagger})^T \left(X_i^{m+1}\right)^T U^T \otimes \cdots (U^{\dagger})^T \left(X_i^t\right)^T U^T \\ &= \sum_i UX_i^1U^{\dagger} \otimes \cdots UX_i^mU^{\dagger} \otimes \left(UX_i^{m+1}U^{\dagger}\right)^T \otimes \cdots \left(UX_i^tU^{\dagger}\right)^T \\ &= \sum_i \mathrm{id}^{\otimes m} \otimes \theta^{\otimes n}\left(UX_i^1U^{\dagger} \otimes \cdots \otimes UX_i^tU^{\dagger}\right) \\ &= \mathrm{id}^{\otimes m} \otimes \theta^{\otimes n}[U^{\otimes t}X(U^{\dagger})^{\otimes t}] = \mathrm{id}^{\otimes m} \otimes \theta^{\otimes n}(X), \end{aligned} \tag{18}$$

where the last equality followed from the fact that X commutes with $U^{\otimes t}$. This means that for any $X \in \mathcal{C}(\mathcal{S}^t)$ we have $\mathrm{id}^{\otimes m} \otimes \theta^{\otimes n}(X) \in \mathcal{C}(\mathcal{S}^{t-n,n})$. To prove that all the elements of $\mathcal{C}(\mathcal{S}^{t-n,n})$ can be obtained this way, one can note that $(\mathrm{id}^{\otimes m} \otimes \theta^{\otimes n}) \circ (\mathrm{id}^{\otimes m} \otimes \theta^{\otimes n}) = \mathrm{id}^{\otimes t}$ and then repeat a completely analogous proof for showing that $Y \in \mathcal{C}(\mathcal{S}^{t-n,n})$ implies $(\mathrm{id}^{\otimes m} \otimes \theta^{\otimes n})(Y) \in \mathcal{C}(\mathcal{S}^t)$. ■

Theorem 2. Let $\mathcal{S}$ be a set of gates in G_d. Then $\mathcal{S}$ is universal if and only if

$$\mathcal{C}\left(\mathcal{S}^{t(d),t(d)}\right) = \mathcal{C}\left(G_d^{t(d),t(d)}\right), \tag{19}$$

where $t(2) = 3$, and $t(d) = 2$ for $d \geqslant 3$.

Proof. Suppose that the set of gates $\mathcal{S} \subset G_d$ is nonuniversal, and denote by $G_{\mathcal{S}}$ the group generated by $\mathcal{S}$. If $G_{\mathcal{S}}$ is infinite, then Lemma 2 guarantees that $\mathcal{C}(\mathcal{S}^{1,1}) \neq \mathcal{C}(G_d^{1,1})$, hence also $\mathcal{C}(\mathcal{S}^{n,n}) \neq \mathcal{C}(G_d^{n,n})$ for any positive integer n. If $G_{\mathcal{S}}$ is finite, then we know that it cannot form a $k(d)$-design with $k(2) = 6$ and $k(d) = 4$ for $d \geqslant 3$. From Remark 1 it follows that there exists an operator A such that $A = \int_{G_d} d\nu_{G_{\mathcal{S}}}(U)U^{\otimes k(d)}A(U^{\dagger})^{\otimes k(d)} \neq \int_{G_d} d\mu(U)U^{\otimes k(d)}A(U^{\dagger})^{\otimes k(d)}$. On the one hand, $A \in \mathcal{C}(\mathcal{S}^{k(d)})$, since every $G_{\mathcal{S}}^k$-twirled element commutes with the elements of $G_{\mathcal{S}}^k$ [36]. On the other hand, $A \notin \mathcal{C}(G_d^{k(d)})$ since A is not equal to its $G_d^{k(d)}$-twirl. Thus, $\mathcal{C}(\mathcal{S}^{k(d)}) \neq \mathcal{C}(G_d^{k(d)})$. Now using the last sentence of Lemma 5, we get that $\mathcal{C}(\mathcal{S}^{t(d),t(d)}) \neq \mathcal{C}(G_d^{t(d),t(d)})$, where $t(d) = k(d)/2$. Therefore, if $\mathcal{C}(\mathcal{S}^{t(d),t(d)}) = \mathcal{C}(G_d^{t(d),t(d)})$, then $\mathcal{S}$ has to be a universal gate set. This concludes the proof. ■

One can calculate explicitly the dimension of the centralizer $\mathcal{C}(G_d^{t,t})$ from the following formula [37],

$$\dim \mathcal{C}\left(G_d^{t,t}\right) = \sum_{\pi} (m_{\pi})^2, \tag{20}$$

where π are irreducible representations occurring in the decomposition (5). Following Corollary 5.4 of Ref. [37] we know that

$$\dim \mathcal{C}\left(G_d^{t,t}\right) = (2t)!, \quad d \geqslant 2t. \tag{21}$$

We can reformulate Theorem 2 to a more computationally friendly form:

Theorem 3. Let $\mathcal{S}$ be a set of gates in G_d. Then $\mathcal{S}$ is universal if and only if (1) $\dim \mathcal{C}(\mathcal{S}^{3,3}) = 132$ for $d = 2$, (2) $\dim \mathcal{C}(\mathcal{S}^{2,2}) = 23$ for $d = 3$, and (3) $\dim \mathcal{C}(\mathcal{S}^{2,2}) = 4! = 24$ for $d \geqslant 4$.

Proof. Obviously, for any $\mathcal{S} \subset G_d$ we have $\dim \mathcal{C}(\mathcal{S}^{t,t}) \geqslant \dim \mathcal{C}(G_d^{t,t})$. The equality of these dimensions is possible if and only if the restrictions to $G_{\mathcal{S}}$ of all irreducible representations occurring in the decomposition (5) are irreducible. Thus $\dim \mathcal{C}(\mathcal{S}^{t,t}) = \dim \mathcal{C}(G_d^{t,t})$ if and only if $\mathcal{C}(\mathcal{S}^{t,t}) = \mathcal{C}(G_d^{t,t})$. We are left with finding dimensions of $\mathcal{C}(G_d^{t(d),t(d)})$, where $t(d)$ is as in the statement of Theorem 2. For $d \geqslant 4$ we use identity (21). For $d = 2$ we have

$$U^{\otimes t} \otimes \bar{U}^{\otimes t} = \bigoplus_{0 \leqslant \nu \leqslant 2t,\ \nu-\text{even}} m_{\pi_{\nu}} \pi_{\nu}(U), \tag{22}$$

where $\dim \pi_{\nu} = \nu + 1$ and $m_{\pi_{\nu}} \neq 0$ for every even ν satisfying $0 \leqslant \nu \leqslant 2t$. Moreover, $\mathrm{Ad}_U = \pi_2(U)$ and

$$U^{\otimes t} \otimes \bar{U}^{\otimes t} \simeq [\pi_2(U) \oplus 1]^{\otimes t}. \tag{23}$$

In addition we known that $\pi_l(U) \otimes \pi_k(U) \simeq \pi_{l+k} \oplus \pi_{l+k-2} \oplus \cdots \oplus \pi_{|l-k|}$. Using these identities we find that

$$U^{\otimes 3} \otimes \bar{U}^{\otimes 3} \simeq \pi_6(U) \oplus 5\pi_4(U) + 9\pi_2(U) \oplus 5. \tag{24}$$

Thus using formula (20) we get $\dim \mathcal{C}(G_2^{3,3}) = 132$. A decomposition similar to (22) can be found for PG_3 [37,38]. We know that irreducible representations of PG_3 are indexed by pairs of non-negative integers $\lambda = (\lambda_1, \lambda_2)$, where $\lambda_1 \geqslant \lambda_2 \geqslant 0$. The adjoint representation of G_3 has $\lambda = (2, 1)$. Using the rules for decomposing a tensor product of $\pi_{(\lambda_1,\lambda_2)} \otimes \pi_{(\lambda_1',\lambda_2')}$ into irreducible representations [37,38] we found that for $d = 3$,

$$U^{\otimes 2} \otimes \bar{U}^{\otimes 2} \simeq \pi_{(4,2)} \oplus \pi_{(3,0)} \oplus \pi_{(3,3)} \oplus 4\pi_{(2,1)} \oplus 2, \tag{25}$$

Thus using (20) we get $\dim \mathcal{C}(G_3^{2,2}) = 23$. ■

IV. CONCLUSIONS

We have presented two ways to verify the universality of a gate set. They are given by Theorems 1 and 3. We now discuss the advantages and disadvantages of both methods.

The approach through Theorem 3 is clearly computationally simple. Calculation of $\dim \mathcal{C}(\mathcal{S}^{t(d),t(d)})$ boils down to finding the dimension of the kernel of the $|\mathcal{S}|d^{4t(d)} \times d^{4t(d)}$ matrix, where $t(d)$ is as in Theorem 3. Finding the dimension of the kernel of the $n \times m$ matrix is the same as finding the number of nonzero singular values. The complexity of singular value decomposition of an $n \times m$ matrix is well known to be at most $O(mn^2 + nm^2 + n^3)$. So the complexity we obtain is $O(d^{12t(d)})$. This means that our direct universality check is much more efficient and more feasible than the previously developed methods [24,25,30] with $O(d^{d^{5/2}})$ scaling. We note, however, that in a numerical implementation of this method, a small numerical perturbation of gate entries can actually lead to a step change of the centralizer dimension. It is known that universal sets form an open set [24]. Therefore in order to be sure that a gate set $\mathcal{S}$ identified by this method as universal is actually universal, one should confirm that in an infinitesimal neighborhood of $\mathcal{S}$ all sets are identified as universal as well.

The approach given in Theorem 1 is computationally more involved as it requires calculation of the norms given by (11). On the other hand, the information contained in calculated $\delta(t(d), \nu_{\mathcal{S}})$ can be used to assess the efficiency of a gate set $\mathcal{S}$. The efficiency of a universal set $\mathcal{S}$ is measured by the length of a circuit needed to approximate any unitary with a given precision ϵ. The Solovay-Kitaev theorem [16] states that all universal sets are roughly the same efficient. More precisely, the length of a circuit that ϵ-approximates any $U \in SU(d)$ is bounded by $A(\mathcal{S}) \ln^c(1/\epsilon)$ [16], where $c \geqslant 1$. To estimate the value of $A(\mathcal{S})$ one uses the concept of δ-approximate t-designs [39]. The results of [30,35] ensure that for a given precision ϵ the constant $A(\mathcal{S})$ is inversely proportional to $1 - \delta(t(\epsilon), \nu_{\mathcal{S}})$, where $t(\epsilon) = O(\epsilon^{-1})$, and the constant $c = 1$. The bigger is $A(\mathcal{S})$ the less efficient is a gate set $\mathcal{S}$. Moreover, $\delta(t, \nu_{\mathcal{S}})$ is a nondecreasing function of t. Therefore, for $d \geqslant 3$, a gate set $\mathcal{S} \subset U(d)$ that is a $\delta(4, \nu_{\mathcal{S}})$-approximate 4-design with $\delta(4, \nu_{\mathcal{S}})$ very close to one is also very inefficient in terms of approximating unitaries. Thus from the point of view of applications, gate sets that are δ-approximate 4-designs with δ very close to one can be regarded as nonuniversal. In this respect, Theorem 1 is much more powerful than Theorem 3 and other methods of universality verification (cf. Ref. [40]).

Last but not least, we also expect that our simple algebraic criterion for universality will allow general proofs about the universal extension of different gate-set families going well beyond the earlier results [15,17,41]. We leave this as future work.

ACKNOWLEDGMENTS

A.S. would like to thank M. Oszmaniec for ingenious discussions regarding Lemma 3. This work was supported by National Science Centre, Poland under Grant No. SONATA BIS:2015/18/E/ST1/00200, and by the Hungarian National Research, Development and Innovation Office through the Quantum Information National Laboratory program and Grants No. FK135220, No. KH129601, and No. K124351.

[1] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[2] D. Deutsch, Proc. R. Soc. London, Ser. A **425**, 73 (1989).

[3] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).

[4] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).

[5] Y. Bromberg, Y. Lahini, R. Morandotti, and Y. Silberberg, Phys. Rev. Lett. **102**, 253904 (2009).

[6] A. Politi *et al.*, Science **320**, 646 (2008).

[7] A. W. Harrow, B. Recht, and I. L. Chuang, J. Math. Phys. **43**, 4445 (2002).

[8] A. Sawicki, Quantum Inf. Comput. **16**, 291 (2016).

[9] K. Karnas and A. Sawicki, J. Phys. A: Math. Theor. **51**, 075305 (2018).

[10] A. Bouland and S. Aaronson, Phys. Rev. A **89**, 062316 (2014).

[11] P. Selinger, Quantum Inf. Comput. **15**, 159 (2015).

[12] V. Kliuchnikov, D. Maslov, and M. Mosca, IEEE Trans. Comput. **65**, 161 (2016).

[13] A. Bocharov, Y. Gurevich, and K. M. Svore, Phys. Rev. A **88**, 012313 (2013).

[14] P. Sarnak, Letter to Scott Aaronson and Andy Pollington on the Solovay-Kitaev theorem, 2015, http://publications.ias.edu/sarnak/paper/2637 (to be published).

[15] J. L. Brylinski and R. Brylinski, in *Mathematics of Quantum Computation* (Chapman and Hall/CRC Press, London/Boca Raton, FL, 2011), pp. 117–134.

[16] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).

[17] M. Oszmaniec and Z. Zimborás, Phys. Rev. Lett. **119**, 220502 (2017).

[18] Z. Zimborás, R. Zeier, T. Schulte-Herbrüggen, and D. Burgarth, Phys. Rev. A **92**, 042309 (2015).

[19] R. Zeier and T. Schulte-Herbrüggen, J. Math. Phys. **52**, 113510 (2011).

[20] R. Zeier and Z. Zimborás, J. Math. Phys. **56**, 081702 (2015).

[21] A. M. Childs, D. Leung, L. Mančinska, and M. Ozols, Quantum Inf. Comput. **11**, 19 (2011).

[22] C. Altafini, J. Math. Phys. **43**, 2051 (2002).

[23] F. Albertini and D. D'Alessandro, IEEE Trans. Autom. Control **48**, 1399 (2003).

[24] A. Sawicki and K. Karnas, Ann. Henri Poincaré **18**, 3515 (2017).

[25] A. Sawicki and K. Karnas, Phys. Rev. A **95**, 062303 (2017).

[26] L. Mattioli and A. Sawicki, arXiv:2110.04210.

[27] M. H. Freedman, A. Kitaev, and J. Lurie, Math. Res. Lett. **10**, 11 (2003).

[28] E. Knill, arXiv:quant-ph/9508006.

[29] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Phys. Rev. A **80**, 012304 (2009).

[30] M. Oszmaniec, A. Sawicki, and M. Horodecki, IEEE Trans. Inf. Theory **68**, 989 (2022).

[31] E. Bannai, G. Navarro, N. Rizo, and P. H. Tiep, J. Math. Soc. Jpn. **72**, 909 (2020).

[32] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement* (Cambridge University Press, Cambridge, UK, 2017).

[33] D. Gross, K. Audenaert, and J. Eisert, J. Math. Phys. **48**, 052104 (2007).

[34] T. Bröcker and T. Dieck, *Representations of Compact Lie Groups*, (Springer, New York, 1985).

[35] P. P. Varjú, Doc. Math. **18**, 1137 (2013).

[36] P. Diaconis, *Group Representations in Probability and Statistics*, Lecture Notes–Monograph Series Vol. 11 (Institute of Mathematical Statistics, London, 1988).

[37] G. Benkart, M. Chakrabarti, T. Halverson, R. Leduc, C. Y. Lee, and J. Stroomer, J. Algebra **166**, 529 (1994).

[38] A. Roy and A. J. Scott, Des. Codes Cryptogr. **53**, 13 (2009).

[39] O. Słowik and A. Sawicki, arXiv:2201.11774.

[40] L. Babai, R. Beals, and D. N. Rockmore, in *Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC 93* (ACM, New York, 1993), pp. 117–126.

[41] M. J. Bremner, J. L. Dodd, M. A. Nielsen, and D. Bacon, Phys. Rev. A **69**, 012313 (2004).