Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 310 (2007) 49–56
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Deciding universality of quantum gates ☆

Gábor Ivanyos

Computer and Automation Research Institute of the Hungarian Academy of Sciences, Kende u. 13-17, H-1111 Budapest, Hungary

Received 22 June 2006

Available online 23 October 2006

Communicated by Harm Derksen

Abstract

We say that collection of n-qudit gates is universal if there exists $N_0 \geqslant n$ such that for every $N \geqslant N_0$ every N-qudit unitary operation can be approximated with arbitrary precision by a circuit built from gates of the collection. Our main result is an upper bound on the smallest N_0 with the above property. The bound is roughly $d^8 n$, where d is the number of levels of the base system (the 'd' in the term qu$d$it). The proof is based on a recent result on invariants of (finite) linear groups.

Keywords: Quantum computing; Group representations

1. Introduction

A qu$d$it is a vector of norm 1 from the Hilbert space $\mathbb{C}^d$, an n-qu$d$it state is an element of norm 1 of $(\mathbb{C}^d)^{\otimes n} \cong \mathbb{C}^{d^n}$. In quantum computation it is usual to fix an orthonormal basis $|0\rangle, \ldots, |d-1\rangle$ of $\mathbb{C}^d$. An orthonormal basis of $\mathbb{C}^{d^n}$ naturally corresponding to this basis consists of vectors of the form $|i_1\rangle \otimes \cdots \otimes |i_n\rangle$. This basis is called the computational basis. The space $(\mathbb{C}^d)^{\otimes n}$ is called an n-qu$d$it quantum system and the factors of the n-fold tensor product $(\mathbb{C}^d)^{\otimes n}$ are referred as the qu$d$its of the system.

An n-qu$d$it quantum operation (or gate) is a unitary transformation acting on the n-qu$d$it states, i.e., an element of the unitary group U_{d^n}. As in quantum computation, states which are scalar multiples of each other are considered equivalent, quantum operations are also understood

☆ Research partially supported by the project RESQ IST-2001-37559 of the IST-FET program of the EC, and by the Hungarian Scientific Research Fund (OTKA) under grants T42706 and T42481.

E-mail address: gabor.ivanyos@sztaki.hu.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2006.09.013

projectively. In particular, for every $u \in U_{d^n}$, the normalized operation $\alpha^{-1}u$ represents the same gate as u where α is any d^nth root of $\det u$.

Let $\Gamma \subset U_{d^n}$ be a (finite) collection of n-qu$d$it quantum gates. We say that Γ is a *complete* set of n-qu$d$it gates if a scalar multiple of every n-qu$d$it operation from U_{d^n}, can be approximated with an arbitrary precision by a product of operations from Γ. In other words, Γ is complete if the semigroup of U_{d^n} generated by Γ and the unitary scalar matrices is dense in U_{d^n}. The latter condition, because of compactness, is equivalent to saying that the *group* generated by Γ and the unitary scalar matrices is dense in U_{d^n}, see [9].

Note that in the quantum computation literature complete sets of gates are frequently called universal. In this paper, partly following the terminology of [5], we reserve the term *universal* for expressing a weaker version discussed below.

For $N \geqslant n$ we can view $(\mathbb{C}^d)^{\otimes N}$ as a bipartite system $(\mathbb{C}^d)^{\otimes n} \otimes (\mathbb{C}^d)^{\otimes N-n}$ and let an n-qu$d$it gate u act on the first part only. Formally, the N-qu$d$it extension u_N of u is the operation $u \otimes I$ where I stands for the identity of $(\mathbb{C}^d)^{\otimes N-n}$. For an n-qu$d$it gate set Γ the gate set Γ_N is the collection of the extensions of gates from Γ obtained this way: $\Gamma_N = \{u_N \mid u \in \Gamma\}$.

More generally, we can extend an n-qu$d$it gate u to N qu$d$its by selecting an embedding μ of $\{1, \ldots, n\}$ into $\{1, \ldots, N\}$ and let act u on the components indexed by $\mu(1), \ldots, \mu(n)$ (in this order) and leave the rest "unchanged." It will be convenient to formalize this in terms of permutations of the qu$d$its of the larger system as follows. Each permutation from the symmetric group S_N acts on $(\mathbb{C}^d)^{\otimes N}$ by permuting the tensor components. For an N-qu$d$it gate v and $\sigma \in S_N$ the operation $v^\sigma = \sigma v \sigma^{-1}$ is also a quantum gate which can be considered as the gate v with "fans" permuted by σ. We denote by Γ^N the collection of gates obtained from gates in Γ_N this way: $\Gamma^N = \{u_N^\sigma \mid u \in \Gamma,\ \sigma \in S_N\}$.

We say that for $N \geqslant n$ the n-qu$d$it gate set Γ is *N-universal* if Γ^N is complete. The collection Γ is called ∞-universal or just universal, for short, if there exists $N_0 \geqslant n$ such that Γ is N-universal for every $N \geqslant N_0$. It turns out that for $n \geqslant 2$, every complete n-qu$d$it gate is N-universal for every $N \geqslant n$. This claim follows from the fact that the Lie algebra su_{d^N} is generated by $su_{d^2}^N = \{(u \otimes I)^\sigma \mid u \in su_{d^2},\ \sigma \in S_N\}$. This is shown in [2] for $d = 2$ but essentially the same proof works for $d > 2$ as well.

Hence an n-qu$d$it gate set Γ is universal if and only if there exists an integer $N \geqslant n$ such that Γ is N-universal. On the other hand, no 1-qu$d$it gate set can be universal as the resulting group preserves the natural tensor decomposition.

Completeness of a gate set can be decided by computing the (real) Zariski closure of the group generated by the gates using the method in [1]. A polynomial time algorithm for gates defined over a number field is given in [5,6]. Reducing the problem of universality to completeness requires a bound for the smallest N such that a universal set of gates is N-universal. In [5,6] Jeandel gives a 6-qubit gate set which is 9-universal but not 6-universal and it is explained how to extend this example to a gate set over $2^k + 2$ qubits which is $2^{k+1} + 1$-universal but not $2^{k+1} - 2$-universal where k is an integer greater than 1. (A qubit is a qu$d$it with $d = 2$.) Our main result is the following.

Theorem 1. *Let Γ be an n-qu$d$it gate set where $n, d \geqslant 2$. Then Γ is universal if and only if it is N-universal for some integer $N \leqslant d^8(n-1)+1$.*

Our main technical tool, a criterion for completeness based on invariants of groups, is given in Section 2. It can be considered as a "more algebraic" variant of Jeandel's criterion given in [5,6]. Correctness is a consequence of a recent result of Guralnick and Tiep stating that certain

low degree invariants distinguish the special linear group from its closed (in particular, finite) subgroups. Needless to say, the proof of the applied result heavily uses the classification of finite simple groups and their representations.

We prove Theorem 1 in Section 3. The outline of the proof is the following. We relate polynomial ideals to gate sets. The completeness criterion gives that the Hilbert polynomial of the ideal corresponding to a universal gate set must be the constant polynomial 24. Our result is then a consequence of Lazard's bound on the regularity of Hilbert functions of zero-dimensional ideals.

2. Completeness

In Jeandel's work [5,6], testing gate sets for completeness is based on the following observation.

Fact 1. *Let $d \geqslant 2$ and let G be subgroup of SU_{d^N}. Assume further the real vector space su_{d^N} (the Lie algebra of SU_{d^N}) consisting of the traceless skew Hermitian $d^N \times d^N$ matrices is an irreducible $\mathbb{R}G$-module under the conjugation action by elements of G. Then G is either finite or dense in SU_{d^N}.*

(To see this let G_0 stand for the connected component of the identity in the closure of G. Then G_0 is a connected compact Lie group. If G is infinite then so is G_0 and hence the (real) Lie algebra L of G_0 is a non-zero submodule of su_{d^N} under the conjugation action of G. Because of irreducibility we have $L = su_{d^N}$ and hence $G_0 = SU_{d^N}$.)

By Fact 1 if Γ is a finite collection of normalized gates then testing Γ for completeness amounts to testing irreducibility of su_{d^N} under conjugation of elements of Γ and to testing if the linear group generated by Γ is finite. Informally, we are going to replace the latter test with a test similar to the first one.

Set $V = \mathbb{C}^{d^N}$, the complex column vectors of length d^N. The vector space V is a left $\mathbb{C}G$-module for every linear group $G \leqslant GL_{d^N}(\mathbb{C})$. The dual space $V^* = \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$ is a right $\mathbb{C}G$-module. It can be made a left $\mathbb{C}G$ module by letting u^{-1} act in place of u. This module (denoted also by V^*) is called the module contragradient to V. In terms of matrices, the contragradient matrix representation can be obtained by taking the inverse of the transpose of the original matrix representation. Note that for $u \in U_{d^N}$ the matrix of u in the contragradient representation will be simply the complex conjugate of the matrix of u.

We adopt notation from [7] and [4]. For a pair k, k' of positive integers and a subgroup $G \leqslant GL_{d^N}(\mathbb{C})$ the quantity $\mathcal{M}_{k,k'}(G)$ is defined as the dimension of the space of G-invariant tensors from $V^{\otimes k} \otimes (V^*)^{\otimes k'}$ and $\mathcal{M}_{2k}(G)$ as $\mathcal{M}_{k,k}(G)$. For the purposes of this paper it will be convenient working with the definition

$$\mathcal{M}_{2k}(G) = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}G}\big(\big(V \otimes V^*\big)^{\otimes k}, \mathbb{C}\big). \tag{1}$$

Recall that for a left $\mathbb{C}G$-module W

$$\mathrm{Hom}_{\mathbb{C}G}(W, \mathbb{C}) = \big\{ f \in W^* \;\big|\; f(gw) = f(w) \text{ for every } g \in G,\ w \in W \big\}.$$

Formula (1) is equivalent to the original definition because of self-duality of $(V \otimes V^*)^{\otimes k}$. Note that if a finite set Γ generates a dense subgroup of G and B is a basis of W then

$$\mathrm{Hom}_{\mathbb{C}G}(W, \mathbb{C}) = \big\{ f \in W^* \;\big|\; f(gw) = f(w) \text{ for every } g \in \Gamma,\ w \in B \big\}, \tag{2}$$

and hence (a basis of) the space $\mathrm{Hom}_G(W,\mathbb{C})$ can be computed by solving a system of linear equations.

Also note that $V\otimes V^*\cong \mathrm{End}_{\mathbb{C}}(V)$ and $\mathcal{M}_2(G)$ is the dimension of the centralizer of G (in $\mathrm{End}_{\mathbb{C}}(V)$). In particular, $\mathcal{M}_2(G)=1$ if and only if V is an irreducible $\mathbb{C}G$-module. Similarly, $\mathcal{M}_4(G)$ is the dimension of the centralizer of the conjugation action of G on $d^N\times d^N$ complex matrices.

M. Larsen observed that if $\mathcal{G}$ is the entire complex linear group $GL_{d^N}(\mathbb{C})$, or the complex orthogonal group or the complex symplectic group and G is a Zariski closed subgroup of $\mathcal{G}$ such that the connected component of the identity in G is reductive (including the case when this component is trivial) and $\mathcal{M}_4(G)=\mathcal{M}_4(\mathcal{G})$ then either G is finite or $G\geqslant[\mathcal{G},\mathcal{G}]$. (Notice that Fact 1 can be viewed as the unitary analogue of Larsen's alternative.) Larsen also conjectured that for a finite subgroup $G<\mathcal{G}$ we have $\mathcal{M}_{2k}(G)>\mathcal{M}_{2k}(\mathcal{G})$ with some $k\leqslant 4$. For an introduction to Larsen's alternative and Larsen's conjecture the reader is referred to the article of N.M. Katz [7].

Recently R.M. Guralnick and P.H. Tiep [4], using the classification of finite simple groups and their irreducible representations, settled Larsen's conjecture. The conjecture holds basically true, there are only two exceptions. In any case, $\mathcal{M}_{2k}(G)>\mathcal{M}_{2k}(\mathcal{G})$ with some $k\leqslant 6$. For $\mathcal{G}=GL_{d^N}(\mathbb{C})$, the group relevant to the present paper, the following can be extracted from Theorems 1.4 and 2.12 in [4].

Theorem 2. (Guralnick and Tiep [4]) *Let G be a Zariski closed subgroup of $GL_{d^N}(\mathbb{C})$ such that the connected component of the identity in G is reductive or trivial. If $\mathcal{M}_{2k}(G)=\mathcal{M}_{2k}(GL_{d^N}(\mathbb{C}))$ for $k=1,2,3,4$ then either $G\geqslant SL_{d^N}(\mathbb{C})$ or $G=SL_2(5)$ and $d^N=2$. In the latter case $\mathcal{M}_{12}(G)>\mathcal{M}_{12}(GL_{d^N}(\mathbb{C}))$.*

The following statement is an easy consequence of the results from [4]. In order to shorten notation, for a collection $\Gamma\subseteq U_{d^N}$ we define $\mathcal{M}_{2k}(\Gamma)$ as $\mathcal{M}_{2k}(G)$ where G is the smallest closed subgroup of U_{d^N} containing Γ (in the norm topology). Also, in view (2) and the comment following it, computing $\mathcal{M}_{2k}(\Gamma)$ can be accomplished by computing the rank of a d^{N2k} by $|\Gamma|d^{N2k}$ matrix if Γ is finite.

Proposition 3. *Assume that $d^N>2$ and let $\Gamma\subset U_{d^N}$. Then Γ is complete if and only if $\mathcal{M}_8(\Gamma)=\mathcal{M}_8(GL_{d^N}(\mathbb{C}))$. If $d^N=2$ then the necessary and sufficient condition for completeness is $\mathcal{M}_{12}(\Gamma)=\mathcal{M}_{12}(GL_{d^N}(\mathbb{C}))$.*

Proof. We only prove the first statement, the second assertion can be verified with a slight modification of the arguments. Let G be the smallest closed subgroup of U_{d^N} containing Γ (in the norm topology). We replace each $u\in G$ with its normalized version $\alpha^{-1}u$ where α is any d^Nth root of $\det u$. In this way we achieve that G is a closed subgroup of SU_{d^N}. As the action of $\alpha^{-1}u\cdot u$ is the same as that of u on $V^{\otimes k}\otimes V^{*\otimes k}$, this change does not affect the quantities $\mathcal{M}_{2k}(G)$. If Γ is complete then $G=SU_{d^N}$. Therefore the Zariski closure of G in $GL_{d^N}(\mathbb{C})$ (over the complex numbers) is $SL_{d^N}(\mathbb{C})$ and hence $\mathcal{M}_{2k}(G)=\mathcal{M}_{2k}(SL_{d^N}(\mathbb{C}))=\mathcal{M}_{2k}(GL_{d^N}(\mathbb{C}))$ for every k. This shows the "only if" part.

To prove the reverse implication, assume that $\mathcal{M}_8(G)=\mathcal{M}_8(GL_{d^N}(\mathbb{C}))$. By Lemma 3.1 of [4], $\mathcal{M}_{2k}(G)=\mathcal{M}_{2k}(GL_{d^N}(\mathbb{C}))$ for $k=1,2,3$ as well. In particular, $\mathcal{M}_4(G)=\mathcal{M}_4(GL_{d^N}(\mathbb{C}))=2$. Notice that G is a compact Lie group therefore every finite-dimensional representation of G is completely reducible. Hence the conjugation action of G on $d^N\times d^N$ matrices has two irreducible components: one consists of the scalar matrices the other one is

the Lie algebra $sl_{d^N}(\mathbb{C})$ of traceless matrices. As a real vector space, $sl_{d^N}(\mathbb{C})$ is the direct sum of su_{d^N} and $i \cdot su_{d^N}$ (here $i = \sqrt{-1}$). Both subspaces are invariant under the action of U_{d^N}, therefore they are $\mathbb{R}G$-submodules and multiplication by i gives an $\mathbb{R}G$-module isomorphism between them. It follows that su_{d^N} must be an irreducible $\mathbb{R}G$-module. Hence by Fact 1, either $G = SU_{d^N}$ or G is finite. In the first case Γ is complete. In the second case, by Theorem 2, G must be $SL_2(5)$ and $d^N = 2$. This contradicts the assumption $d^N > 2$. □

3. Universality

We begin with a lemma which establishes a condition for N-universality which suits better our purposes than the original definition.

Lemma 4. *Let $d > 1$ and Γ be an n-qudit gate set, let $N \geqslant n$ and let Σ be an arbitrary generating set for S_N. Then Γ is N-universal if and only if $\Gamma_N \cup \Sigma$ is complete.*

Proof. Let H respectively G denote the closure of the subgroup of SU_{d^N} generated by the normalized gates from Γ^N and $\Gamma_N \cup \Sigma$, respectively. As Γ^N is in the subgroup generated by $\Gamma_N \cup \Sigma$, the group H is a subgroup of G and hence the "only if" part of the statement is obvious. To see the reverse implication, observe that H is closed under conjugation by the elements of $\Gamma_N \cup S_N$, whence H is a closed normal subgroup of G. Furthermore, H has finite index in G because $HS_N = G$. Also notice that (say, because of simplicity of PSU_{d^N}) the only normal subgroup of finite index in SU_{d^N} is the whole group. This implies that if $\Gamma_N \cup \Sigma$ is complete, i.e., $G = SU_{d^N}$, then $H = G$, which means that Γ^N is complete as well. □

By Lemma 4, we can consider gate sets on N qu$d$its which consist of two parts. The gates in the first part act on the first n qu$d$its while the rest consists of permutations. We exploit this property in Subsection 3.1, where we relate polynomial ideals to such a sequence of gate sets where N varies. We finish the proof of Theorem 1 in Subsection 3.2 by observing that the sequence $\mathcal{M}_8$ for letting an n-qu$d$it gate set together with the symmetric group S_N act on $(C^d)^{\otimes N}$ $(N = n, n+1, \ldots)$ take the same values as the Hilbert function of the corresponding ideal.

3.1. The ideal of a gate set

In this subsection $W = \mathbb{C}^m$ for some integer $m > 0$ and G is a subgroup of $GL(W^{\otimes n})$. For every $N \geqslant n$ we establish a relation between $\mathrm{Hom}_{\langle G, S_n\rangle}(W^{\otimes n}, \mathbb{C})$ and $\mathrm{Hom}_{\langle G\otimes I, S_N\rangle}(W^{\otimes N}, \mathbb{C})$. Here S_N denotes the subgroup of $GL(W^{\otimes N})$ consisting of the permutations of tensor components and I stands for the identity on $W^{\otimes(N-n)}$.

We work with the tensor algebra $T = \bigoplus_{j=0}^{\infty} W^{\otimes j}$ of W. We use some elementary properties of T and its substructures. Most of the proofs can be found in Section 9 of [3]. We say that an element w of T is homogeneous of degree j if $w \in W^{\otimes j}$. If we fix a basis $w_1, \ldots, w_m$ of W, then a basis of T consists of the non-commutative monomials of the form $w_{i_1} \otimes \cdots \otimes w_{i_j}$ and T can be interpreted as the ring of non-commutative polynomials in $w_1, \ldots, w_m$ over $\mathbb{C}$. In this interpretation, for every $j \geqslant 0$ the elements of $W^{\otimes j}$ are identified with the homogeneous non-commutative polynomials of degree j. A right (or two sided) ideal J of T is called graded if J equals the sum $\bigoplus_{j=0}^{\infty} J^j$ where $J^j = W^{\otimes j} \cap J$. The component J^j is called the degree j part of J. It turns out that a right (respectively two-sided) ideal J of T is graded if and only if there is a set of homogeneous elements of J which generate J as a right (respectively two-sided) ideal.

Let M be the two-sided ideal of T generated by $w_i \otimes w_j - w_j \otimes w_i$ ($i, j \in \{1, \ldots, m\}$), and let $\phi : T \to R = T/M$ be the natural map. Then M is a graded ideal with degree j parts M^j which are spanned by $w_{i_1} \otimes \cdots \otimes w_{i_j} - w_{i_{\sigma(1)}} \otimes \cdots \otimes w_{i_{\sigma(j)}}$ where $(i_1, \ldots, i_j) \in \{1, \ldots, m\}^j$ and $\sigma \in S_j$. The factor algebra R is called the symmetric algebra of W. Set $x_i = \phi(w_i)$ for $i = 1, \ldots, m$. Then R is identified with the (commutative) polynomial ring $\mathbb{C}[x_1, \ldots, x_m]$. The image of R^j of $W^{\otimes j}$ under ϕ is the jth symmetric power of W. In interpretation of R as polynomial ring, R^j consists of the homogeneous polynomials of degree j.

For a subspace L of $(W^{\otimes N})^*$ we denote by $L^\perp$ the subspace of $W^{\otimes N}$ annihilated by L: $L^\perp = \{w \in W^{\otimes N} \mid l(w) = 0 \text{ for every } l \in L\}$. Because of duality, $\dim L = \dim(W^{\otimes N}/L^\perp)$ and $(L_1 \cap L_2)^\perp = L_1^\perp + L_2^\perp$. In particular, $\mathrm{Hom}_{\langle G \otimes I \cup S_N \rangle}(W^{\otimes N}, \mathbb{C})^\perp = \mathrm{Hom}_{G \otimes I}(W^{\otimes N}, \mathbb{C})^\perp + \mathrm{Hom}_{S_N}(W^{\otimes N}, \mathbb{C})^\perp$.

From the equality $\mathrm{Hom}_{G \otimes I}(W^{\otimes N}, \mathbb{C}) = \mathrm{Hom}_G(W^{\otimes n}, \mathbb{C}) \otimes (W^{\otimes (N-n)})^*$ we obtain that $\mathrm{Hom}_{G \otimes I}(W^{\otimes N}, \mathbb{C})^\perp = \mathrm{Hom}_G(W^{\otimes n}, \mathbb{C})^\perp \otimes W^{\otimes (N-n)}$, in other words, the space $\mathrm{Hom}_{G \otimes I}(W^{\otimes N}, \mathbb{C})^\perp$ is the degree N part of the right ideal $H(G)$ in T generated by $\mathrm{Hom}_G(W^{\otimes n}, \mathbb{C})^\perp$.

The space $\mathrm{Hom}_{S_N}(W^{\otimes N}, \mathbb{C})$ corresponds the symmetric N-linear functions, i.e., it consists of the linear functions $W^{\otimes N} \to \mathbb{C}$ which take identical values on $w_{i_1} \otimes \cdots \otimes w_{i_N}$ and $w_{i_{\sigma(1)}} \otimes \cdots \otimes w_{i_{\sigma(N)}}$ for every permutation $\sigma \in S_N$. Therefore $\mathrm{Hom}_{S_N}(W^{\otimes N}, \mathbb{C})^\perp$ coincides with the degree N part M^N of the ideal M.

We obtain that $\mathrm{Hom}_{\langle G \otimes I \cup S_N \rangle}(W^{\otimes N}, \mathbb{C})^\perp$ is the degree N part of $H(G) + M$. As $H(G)$ is a right ideal and M is an ideal in T with $R = T/M$ commutative, $H(G) + M$ is an ideal in T containing M. Setting $J(G) = \phi(H(G) + M)$ we conclude that for every $N \geqslant n$, $J^N(G) = \phi(\mathrm{Hom}_{\langle G \otimes I \cup S_N \rangle}(W^{\otimes N}, \mathbb{C})^\perp)$ is the degree N part of $J(G)$. Furthermore, $J(G)$ is the ideal of the commutative polynomial ring R generated by $J^n(G)$ and

$$\dim \mathrm{Hom}_{\langle G \otimes I \cup S_N \rangle}\big(W^{\otimes N}, \mathbb{C}\big) = \dim\big(R^N / J^N(G)\big).$$

3.2. The proof of Theorem 1

Let $n, d \geqslant 2$, let $\Gamma \subseteq GL((\mathbb{C}^d)^{\otimes n})$ and let G be the subgroup of $GL(\mathbb{C}^d)$ generated by Γ. For every integer $N \geqslant n$, we consider the G-module $V = (\mathbb{C}^d)^{\otimes N}$ where the action of G is given by $G \otimes I$ (here I is the identity on $(\mathbb{C}^d)^{\otimes (N-n)}$). We set $W = (\mathbb{C}^d)^{\otimes 4} \otimes ((\mathbb{C}^d)^*)^{\otimes 4}$ and consider the action of G on W. For every $N \geqslant n$ we have the G-module isomorphism $V^{\otimes 4} \otimes (V^*)^{\otimes 4} \cong W^{\otimes N}$ where the action of G on the right-hand side is $G \otimes I$ (this time I is the identity on $W^{\otimes (N-n)}$). Applying the notation and observations of the preceding subsection in this context, we obtain that

$$\mathcal{M}_8\big(\langle G \otimes I \cup S_N \rangle\big) = \dim\big(R^N / J^N(G)\big)$$

for every $N \geqslant n$.

First we consider the full linear group $GL_{d^n}(\mathbb{C})$. The n-universality of U_{d^n} for $n \geqslant 2$ gives $\dim(R^N / J^N(GL_{d^n}(\mathbb{C}))) = \mathcal{M}_8(GL_{d^N}(\mathbb{C}))$. From the first fundamental theorem in invariant theory of the general linear group (see [10]) we obtain $\mathcal{M}_8(GL_{d^N}(\mathbb{C})) = 4! = 24$.

Now consider an arbitrary gate set $\Gamma \subseteq U_{d^n}$ and let $G \leqslant GL_{d^n}(\mathbb{C})$ the group generated by Γ. The preceding discussion and Proposition 3 give that Γ is universal if and only if $\dim(R^N / J^N(G)) = 24$ for sufficiently large degree N.

The ideal $J(G)$ is an ideal of $R = \mathbb{C}[x_1, \ldots, x_m]$ generated by homogeneous polynomials of degree n. In the context of polynomial rings, graded ideals are called homogeneous. That is, an ideal J of the polynomial ring R is called homogeneous if J is the direct sum its homogeneous components $J^j = R^j \cap J$; and an ideal generated by homogeneous polynomials is homogeneous. The *Hilbert function* of the homogeneous ideal J is given as $j \mapsto h_J(j) = \dim R^j/J^j$. It turns out that the Hilbert function is ultimately a polynomial: there is a polynomial p_J (in one variable) and an integer N such that $h_J(j) = p_J(j)$ for $j \geqslant N$. The smallest N with this property is called the regularity of the Hilbert function of J. The degree of the Hilbert polynomial is the *dimension* of J. (Actually, it is the dimension of the projective variety consisting of the common projective zeros of the polynomials in J.)

The discussion above shows that the Hilbert polynomial of the ideal $J(G)$ corresponding to a universal gate set is the constant 24. In particular, the zero set of $J(G)$ inside the projective space is zero dimensional. In [8], D. Lazard proved that the regularity of the Hilbert function of a zero-dimensional ideal in $\mathbb{C}[x_1, \ldots, x_m]$ generated by homogeneous polynomials of degree n is bounded by $mn - m + 1$. From this, the proof of Theorem 1 is finished by observing that the smallest N for which Γ is N-universal coincides with the regularity of the Hilbert function of $J(G)$.

4. Concluding remarks

Very probably the bound proved in Theorem 1 is not tight. However, for fixed d it is linear in n and Jeandel's construction discussed in the introduction shows that in fact the smallest N such that a universal n-qubit gate set is N-universal can be at least $2n - 6$.

Proving better upper bounds would require deeper knowledge of subspaces of $V^{*\otimes 4} \otimes V^{\otimes 4}$ which occur as $\mathrm{Hom}_G(V^{\otimes 4} \otimes V^{*\otimes 4}, \mathbb{C})$ for $G \leqslant GL(V)$. Using the isomorphism $\mathrm{Hom}_G(V^{\otimes 4} \otimes V^{*\otimes 4}, \mathbb{C}) \cong \mathrm{End}_G(V^{\otimes 4})$, a natural restriction is that these subspaces must be subalgebras of $\mathrm{End}_{\mathbb{C}}(V^{\otimes 4})$. However, it is not obvious how to exploit this fact.

Effectiveness and complexity of algorithms for testing completeness and universality based on Proposition 3, Theorem 1 and Lemma 4 depend on the computational model and on the way how the input gate set is represented. In the Blum–Shub–Smale model, if the input gates are given as arrays of $n \times n$ complex numbers, the completeness test can be accomplished in polynomial time. With the same assumption on the input, for constant d (e.g., for qubits or qutrits) even universality can be tested in polynomial time. Similar results can be stated for Boolean complexity if the entries of the matrices representing the input gates are from an algebraic number field. Even it is decidable if there is a non-universal gate set which is ϵ-close to a given collection of gates in the Hadamard norm of matrices. Indeed, existence is equivalent to solvability of a (huge) system of polynomial equations and inequalities over the real numbers. Of course, this straightforward method is far from practical.

Acknowledgments

The author is grateful to Emmanuel Jeandel, Lajos Rónyai, Csaba Schneider and to an anonymous referee for their useful remarks and suggestions.

References

[1] H. Derksen, E. Jeandel, P. Koiran, Quantum automata and algebraic groups, J. Symbolic Comput. 39 (3–4) (2005) 357–371.

[2] D.B. DiVincenzo, Two-bit gates are universal for quantum computation, Phys. Rev. A 51 (1995) 1015–1022.
[3] W. Greub, Multilinear Algebra, second ed., Springer-Verlag, New York, 1978.
[4] R.M. Guralnick, P.H. Tiep, Decompositions of small tensor powers and Larsen's conjecture, Represent. Theory 9 (2005) 138–208.
[5] E. Jeandel, Universality in quantum computation, in: Proc. 31st ICALP, in: Lecture Notes in Comput. Sci., vol. 3142, 2004, pp. 793–804.
[6] E. Jeandel, Techniques algébriques en calcul quantique, PhD thesis, ENS Lyon, 2005.
[7] N.M. Katz, Larsen's alternative, moments, and the monodromy of Lefschetz pencils, in: Contributions to Automorphic Forms, Geometry, and Number Theory, Johns Hopkins Univ. Press, 2004, pp. 521–560.
[8] D. Lazard, Résolution des systèmes d'équations algébriques, Theoret. Comput. Sci. 15 (1) (1981) 77–110.
[9] L. Pontryagin, Topological Groups, Princeton Univ. Press, Princeton, 1946.
[10] H. Weyl, The Classical Groups, Princeton Univ. Press, Princeton, 1946.