Universality in Quantum Computation

Emmanuel Jeandel*

LIP (UMR CNRS, ENS Lyon, INRIA, Univ. Claude Bernard Lyon 1),
École Normale Supérieure de Lyon,
46 allée d'Italie 69364 LYON cedex 07 FRANCE

Abstract. We introduce several new definitions of universality for sets of quantum gates, and prove separation results for these definitions. In particular, we prove that realisability with ancillas is different from the classical notion of completeness. We give a polynomial time algorithm of independent interest which decides if a subgroup of a classical group ($\mathbf{SO}_n, \mathbf{SU}_n, \mathbf{SL}_n \ldots$) is Zariski dense, thus solving the decision problem for the completeness. We also present partial methods for the realisability with ancillas.

Quantum circuits are the quantum analogous of boolean circuits. It is well known that all boolean functions can be obtained from circuits using only the two gates `OR` and `NOT`. The problem of finding which gates have this property was solved when Post gave in [1] a complete classification of all classes of boolean functions closed under arbitrary composition. Such a set of gates was also found [2] for reversible computation: There exists a set of reversible gates that can generate any reversible boolean operator.

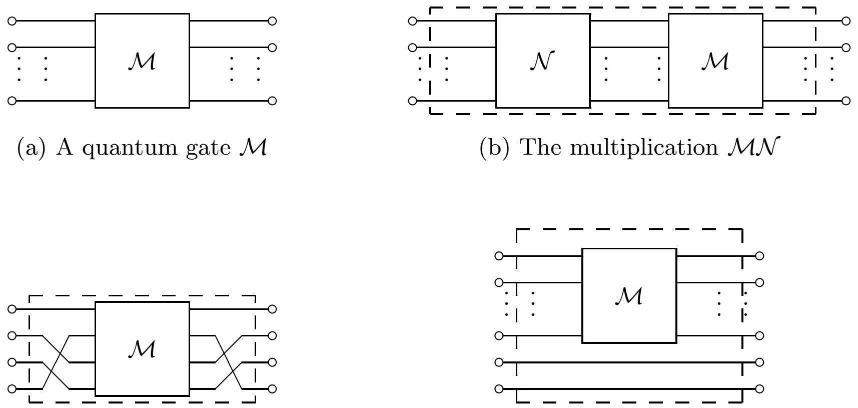
The existence of such sets for quantum computation was answered positively, and many sets of gates have been found [3,4,5,6,7,8]. However, a finite set of gates cannot produce all quantum gates and a notion of approximation is needed. Different notions of universality were then introduced and we define in this paper a wider notion of universality that extends many previous definitions while trying to clarify them. We give some separation results to show that all these notions are distinct, thus answering an open question in [9] about the use of ancillas. We then give an algorithm of independent interest that decides for many linear algebraic groups G whether a subgroup of G is dense, thereby providing a procedure to decide whether a set of quantum gates is complete.

1 Universality

1.1 Quantum Gates

A n-qubit $|\phi\rangle$ is a vector of norm 1 in the Hilbert space $(\mathbb{C}^2)^{\otimes n}$. We will note $\|\cdot\|$ the norm corresponding to the usual scalar product. The canonical (orthonormal) basis of $(\mathbb{C}^2)^{\otimes n}$ is given by the n-qubits $|\omega\rangle$ where ω ranges over all words of

* `Emmanuel.Jeandel@ens-lyon.fr`



(a) A quantum gate $\mathcal{M}$

(b) The multiplication $\mathcal{M}\mathcal{N}$

(c) $\mathcal{M}[\sigma]$

(d) The operation $\mathcal{M} \otimes \mathcal{I}$

Fig. 1. Operations on quantum gates

length n over $\{\mathbf{0}, \mathbf{1}\}$. We will index the matrices by words of length n rather than integers from 1 to 2^n. With these notations, for any matrix $\mathcal{M}$, we have $\mathcal{M} |\omega\rangle = \sum_\nu \mathcal{M}_{\nu,\omega} |\nu\rangle$.

A quantum gate $\mathcal{M}$ over n qubits is an element of $\mathbf{U}_{2^n}$, that is an unitary matrix of dimension 2^n. It therefore maps n-qubits to n-qubits. We will represent it as a black box between two n-qubits (See figure 1(a)). The identity matrix will be written $\mathcal{I}_{2^n}$ or $\mathcal{I}$ when there is no ambiguity about the dimension.

There are three natural operations on quantum gates:

- The multiplication $\mathcal{M}\mathcal{N}$ of two quantum gates over n-qubits represents the composition of the gates, as $(\mathcal{M}\mathcal{N}) |\phi\rangle = \mathcal{M}(\mathcal{N} |\phi\rangle)$ (see fig. 1(b)).
- If σ is a permutation of $\{1, n\}$, $\mathcal{M}[\sigma]$ represents the action of $\mathcal{M}$ over n-qubits where the qubits are swapped: $\mathcal{M}[\sigma]_{\omega,\nu} = \mathcal{M}_{\sigma(\omega),\sigma(\nu)}$ where $\sigma(\omega) = \omega_{\sigma(1)} \ldots \omega_{\sigma(n)}$ (see fig. 1(c))
- The tensor product $\mathcal{M} \otimes \mathcal{I}_{2^{m-n}}$ represents the action of the matrix $\mathcal{M}$ over m qubits: As $(\mathcal{M} \otimes \mathcal{I})(|\phi\rangle \otimes |\psi\rangle) = \mathcal{M} |\phi\rangle \otimes |\psi\rangle$, this means intuitively that $\mathcal{M}$ acts over the n first qubits and leaves the others qubits unchanged (see fig 1(d)). (Note that not all m-qubits can be decomposed into the form $|\phi\rangle \otimes |\psi\rangle$; qubits that cannot be decomposed into smaller qubits are called entangled qubits.)

All these operations are natural when viewed as circuit manipulation, and pretty natural compared to the physical model. However, the phase shift is unimportant from the physical point of view: The qubit $|\phi\rangle$ has the same property than the qubit $\lambda |\phi\rangle$ for λ a scalar of norm 1, that is $\lambda \in \mathbf{U}_1$. All the quantum gates must then be seen as elements of $\mathbf{U}_{2^n}/\mathbf{U}_1$ rather than elements of $\mathbf{U}_{2^n}$.

1.2 Quantum circuits and universality

If $\mathcal{S}$ is a set of quantum gates, a quantum circuit over $\mathcal{S}$ is any gate obtained starting from gates in $\mathcal{S}$ and using the previous constructions. We will note $G_p(\mathcal{S})$ the set of quantum circuits over p qubits with gates in $\mathcal{S}$. It is easy to see that $G_p(\mathcal{S})$ is the semigroup generated by $2^p \times 2^p$ matrices of the form $(\mathcal{M} \times \mathcal{I})[\sigma]$ for $\mathcal{M} \in \mathcal{S}$; $G_p(\mathcal{S})$ is then a finitely generated semigroup. If $\mathcal{S}$ is closed under inversion ($\mathcal{M}^{-1} \in \mathcal{S}$ for $\mathcal{M} \in \mathcal{S}$), which we will implicitly assume from now on, $G_p(\mathcal{S})$ is a finitely generated group.

If we can find an easy way to represent a set $\mathcal{S}$ of gates which, in some sense, achieve to produce any quantum circuit, then we can represent in a compact fashion the quantum circuit, by explaining how it is obtained from the gates in $\mathcal{S}$. However, any finite set of gates $\mathcal{S}$ cannot produce all quantum circuits (as we may obtain in this way only countable quantum circuits), and some notion of approximation is needed.

The easiest notion of universality is the following: $\mathcal{S}$ is universal if for every gate $\mathcal{M}$, for every ϵ, we can approach $\mathcal{M}$ by a circuit $\mathcal{N}$ in $\mathcal{S}$ in the sense that $\|\mathcal{M} - \mathcal{N}\|_m < \epsilon$, with $\|\cdot\|_m$ some chosen norm over $\mathbf{M}_{2^n}(\mathbb{C})$. This notion is also called completeness. Many sets of complete gates have been discovered [4,5,6,7,8], and it was shown that, in some sense, almost all sets of gates over 2 qubits is complete [3,10].

However, we can define many other notions of universality. One may help the gate $\mathcal{N}$ to approach $\mathcal{M}$ by giving it some auxiliary qubits initialised to $\mathbf{0}$: We can ask that $\mathcal{N}(|\psi\rangle \otimes |\mathbf{0}\rangle)$ is near $\mathcal{M}(|\psi\rangle) \otimes |\mathbf{0}\rangle$ for all $|\psi\rangle$. This is called universality using ancillas.

We now give a general definition of universality

Definition 1 (Universality). *Let $\mathcal{S}$ be a set of quantum gates over n qubits.*

$\mathcal{S}$ is said to be (k,p)-universal if for every ϵ, for every gate $\mathcal{M}$ over $k+n$ qubits, there exists a quantum circuit $\mathcal{N}$ with gates in $\mathcal{S}$ over $k+n+l$ qubits, $l \leq p$ such that for all $k+n$-qubit $|\phi\rangle$, $\|(\mathcal{M}\,|\phi\rangle) \otimes |\mathbf{0}\cdots\mathbf{0}\rangle - \mathcal{N}\,|\phi\rangle\,|\mathbf{0}\cdots\mathbf{0}\rangle\,\| \leq \epsilon$.

The notion of (k,∞)-universality is the most general: The number of auxiliary qubits to be used strongly depends on the precision we want to achieve. The notion of completeness coincides in this context with the $(0,0)$-universality.

We will now state the condition in a topological way. We will note $P_{i,p}$ the function that associates to any $2^p \times 2^p$ matrix the $2^i \times 2^i$ matrix in its upper left corner.

Definition 2 (Universality). *Let $\mathcal{S}$ be a set of quantum gates over n qubits.*

- *$\mathcal{S}$ is (k,p)-universal if $P_{n+k,n+k+p}(G_{k+n+p}(\mathcal{S}))$ is dense over $\mathbf{U}_{2^{n+k}}/\mathbf{U}_1$.*
- *$\mathcal{S}$ is (k,∞)-universal if $\bigcup_p P_{n+k,n+k+p}(G_{k+n+p}(\mathcal{S}))$ is dense over $\mathbf{U}_{2^{n+k}}/\mathbf{U}_1$.*

We now give some basic properties of these classes.

Proposition 1 *If $k \leq k'$, a (k,p)-universal set is also (k',p)-universal.*

If $p \leq p'$, a (k,p)-universal set is also (k,p')-universal.

A (k,p)-universal set is also $(k-i,p+i)$-universal.

The first two properties are elementary. The third one says that if we can find a circuit that works for any qubit, then in particular it will work for qubits of the form $|\psi\mathbf{0}\cdots\mathbf{0}\rangle$.

It is not clear at this point whether all these notions of universality are in fact distinct. It was in particular asked in [9] whether the use of ancillas can help the computation.

We will prove in the following section the following separation results:

Theorem 2. *There exists a set of gates over $n+3$ qubits that is $(0,n)$-universal but not (k,p)-universal for $p < n$.*

There exists a set of gates over 6 qubits that is $(3,0)$-universal but not $(0,0)$-universal.

The second result is somewhat surprising: There exists a set of gates over 6 qubits that cannot approximate all quantum gates over 6 qubits but that can approximate any quantum gate over 9 qubits. The proofs rely on the existence of a complete set of gates over 2 qubits, and some combinatorial properties of permutations.

We will then establish some decision procedures for universality. We gave in [11] a general purpose algorithm that computes the closure of every finitely generated matrix group. This entailed the decidability of (k,p)-universality.

However, as the (k,p)-universality is an easier problem, an algorithm with a better complexity can be found. We will prove

Theorem 3. *There exists an algorithm that works in polynomial time and that decides, given generators $\mathcal{X}_1 \dots \mathcal{X}_k$, whether the group generated by $\mathcal{X}_1 \dots \mathcal{X}_k$ is dense over $\mathbf{U}_n$.*

Note that the algorithm will be polynomial over its entry, hence exponential over n when dealing with $2^n \times 2^n$ matrices (that is quantum gates over n qubits). However, it is likely to be used for a fixed value of n ($n = 2$ or 3). This gives a decision procedure for $(k,0)$-universality. We will give only a partial result for (k,p)-universality. The decidability of (k,∞)-universality is open. We conjecture that a set of quantum gates over n qubits is (k,∞)-universal if and only if it is (k,p)-universal for a p that depends only on n.

2 Separation Results for Universality

2.1 On the Contribution of Ancillas

We prove here the first part of the theorem

Theorem 4. *There exists a set of gates over $n+2$ qubits that is $(0,n)$-universal but not (k,p)-universal for $p < n$.*

We will note $\mathcal{A}_1 \dots \mathcal{A}_l$ a set of quantum gates over 2 qubits that is $(0,0)$-universal (that is complete). Many such sets can be found in the literature, see for example [8]. It is important to note that as quantum circuits over $\mathcal{A}_1 \dots \mathcal{A}_l$

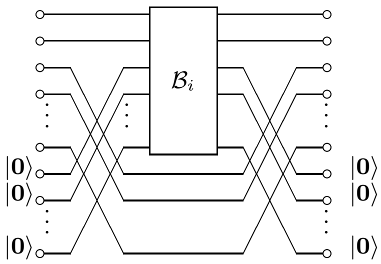


Fig. 2. The gate $\mathcal{M}_i$

can approach any quantum gate over 2 qubits, it is also the case for quantum gates over p qubits for $p \geq 2$.

We now construct the gates $\mathcal{B}_i$ over $2+n$ qubits in the following way: $\mathcal{B}_i$ acts as $\mathcal{A}_i$ only if the n last qubits are all $\mathbf{0}$. $\mathcal{B}_i$ is then defined over the canonical basis by $\mathcal{B}_i\,|\nu\rangle\,|\mathbf{0}\ldots\mathbf{0}\rangle = (\mathcal{A}_i\,|\nu\rangle) \otimes |\mathbf{0}\ldots\mathbf{0}\rangle$ and $\mathcal{B}_i\,|\nu\rangle\,|\omega\rangle = |\nu\rangle\,|\omega\rangle$ for all other words ω.

If we have n qubits with the value $|\mathbf{0}\rangle$, then we can apply $\mathcal{A}_i$. As $\{\mathcal{A}_i\}$ was chosen to be a complete set, we obtain:

Lemma 1. *The set $\{\mathcal{B}_i\}$ is $(0, n)$-universal.*

Proof. It suffices to show that we can obtain quantum circuits over $2n+2$-qubits representing the gates $\mathcal{A}_i \otimes \mathcal{I}$.

Let σ denote any permutation that permutes the sets $\{3 \ldots n+2\}$ and $\{n+3 \ldots 2n+2\}$, that is σ permutes the wires numbered from 3 to n with the last n wires. (see figure 2). Define $\mathcal{M}_i = (\mathcal{B}_i \otimes \mathcal{I}_{2^n})[\sigma]$. Then it is easy to see that $\mathcal{M}_i(|\omega\rangle\,|\nu\rangle\,|\mathbf{0}\ldots\mathbf{0}\rangle) = \mathcal{A}_i\,|\omega\rangle \otimes (|\nu\rangle\,|\mathbf{0}\ldots\mathbf{0}\rangle) = (\mathcal{A}_i \otimes \mathcal{I})(|\omega\rangle\,|\nu\rangle)\,|\mathbf{0}\ldots\mathbf{0}\rangle$.

The previous formula is valid for the whole basis of $(\mathbb{C}^2)^{\otimes n+2}$, hence is true for all $|\phi\rangle$, that is $\mathcal{M}_i(|\phi\rangle\,|\mathbf{0}\ldots\mathbf{0}\rangle) = (\mathcal{A}_i \otimes \mathcal{I})(|\phi\rangle) \otimes |\mathbf{0}\ldots\mathbf{0}\rangle$. This completes the proof. $\square$

The other statement follows easily. We use the fact that, for some entries, we can have less than n qubits set to $\mathbf{0}$, which prevents from applying $\mathcal{A}_i$

Lemma 2. *The set $\{\mathcal{B}_i\}$ is not (k, p)-universal for $p < n$.*

Proof. Let E denote the set of $k+p+(n+2)$ qubits generated by all qubits $|\omega\rangle$ where the word ω has less than n bits to $\mathbf{0}$. It is easy to see that every gate of the form $(\mathcal{B}_i \otimes \mathcal{I})[\sigma]$ preserves E (as this is true for the generating set). Hence any quantum circuit over $\{\mathcal{B}_i\}$ preserves E.

However, there exists a quantum gate over $(n+2)+k$ qubits $\mathcal{X}$ such that $\mathcal{X}\,|\mathbf{1}\ldots\mathbf{1}\rangle = |\mathbf{0}\ldots\mathbf{0}\rangle$. $\mathcal{X}\,|\mathbf{1}\ldots\mathbf{1}\rangle \otimes |\mathbf{0}\ldots\mathbf{0}\rangle = |\mathbf{0}\ldots\mathbf{0}\rangle \in E^{\perp}$. But every quantum circuit $\mathcal{N}$ over $\{\mathcal{B}_i\}$ satisfies $\mathcal{N}(|\mathbf{1}\ldots\mathbf{1}\rangle \otimes |\mathbf{0}\ldots\mathbf{0}\rangle) \in E$. Hence the distance between these two qubits is $\|\mathcal{N}(|\mathbf{1}\ldots\mathbf{1}\rangle \otimes |\mathbf{0}\ldots\mathbf{0}\rangle) - \mathcal{X}\,|\mathbf{1}\ldots\mathbf{1}\rangle \otimes |\mathbf{0}\ldots\mathbf{0}\rangle\,\| = \sqrt{2}$.

No circuit in $\{\mathcal{B}_i\}$ can therefore approach $\mathcal{X}$ from less than $\sqrt{2}$ and $\{\mathcal{B}_i\}$ is therefore not (k, p)-universal. $\square$

This proof strategy is essential and will be used in the next paragraph.

2.2 Contribution of the number of qubits

We will prove here the last part of the theorem, which is the most intriguing part.

Again, we start from $\mathcal{A}_1 \dots \mathcal{A}_p$ a set of quantum gates over 2 qubits that is $(0,0)$-universal and such that $\mathcal{A}_i^2 = \mathcal{I}$. This is not a strong restriction as it is easy to write any matrix of $\mathbf{SU}_4$ as a product of two matrices $\mathcal{X}, \mathcal{Y}$ such that $\mathcal{X}^2 = \mathcal{Y}^2 = \mathcal{I}$.

$\{\mathcal{C}_i\}$ is then a set of gates over 6 qubits such that $\mathcal{C}_i$ acts as $\mathcal{A}_i$ only if the 4 last qubits are equal to $|\mathbf{0}\rangle$ or equal to $|\mathbf{1}\rangle$. $\mathcal{C}_i$ is then defined over the canonical basis by $\mathcal{C}_i |\nu\rangle |\omega\rangle = (\mathcal{A}_i |\nu\rangle) \otimes |\omega\rangle$ if ω is identically $\mathbf{0}$ or identically $\mathbf{1}$, and $\mathcal{C}_i |\nu\rangle |\omega\rangle = |\nu\rangle |\omega\rangle$ otherwise.

The following point is clear

Lemma 3. *$\{\mathcal{C}_i\}$ is not $(0,0)$-universal.*

Proof. We use the same idea as in the preceding proof. If we note E the vector space generated by all qubits $|\omega\rangle$ where ω has 3 letters set to $\mathbf{0}$ and 3 letters set to $\mathbf{1}$, then every quantum circuit over $\{\mathcal{C}_i\}$ preserves E (as this is true over the generating set).

Hence any quantum gate which sends some vector of E to a vector of $E^\perp$ cannot be approached by circuits over $\{\mathcal{C}_i\}$. □

However, it is not easy to see why circuits in $\{\mathcal{C}_i\}$ can approach any quantum gates over 9 qubits. This is our next lemma.

Lemma 4. *$\{\mathcal{C}_i\}$ is $(3,0)$-universal.*

Proof. The idea is the following: Given 7 bits, we can find 4 bits to $\mathbf{0}$ or 4 bits to $\mathbf{1}$. As we do not know which bits are equal, we test all combinations.

Formally, for any choice S of 4 elements into $\{3 \dots 7\}$, we consider a permutation σ_S such that $\sigma_S(1) = 1, \sigma_S(2) = 2, \sigma_S(2+k) = S_k$ for $k \in \{1,4\}$. We note $\mathcal{D}_i^S$ the gate $(\mathcal{C}_i \otimes \mathcal{I})[\sigma_S]$. Intuitively, $\mathcal{D}_i^S$ connects the last 4 wires of the gate $\mathcal{C}_i$ to the wires S_1, S_2, S_3, S_4. Now consider the circuit $\mathcal{D}_i = \prod_S \mathcal{D}_i^S$.

Let ω be any word of length 7 which has more bits set to $\mathbf{1}$ than bits set to $\mathbf{0}$. If ω is identically $\mathbf{1}$ then any choice of 4 letters will give 4 bits to $\mathbf{1}$. There are $\binom{7}{4} = 35$ such choices. If ω has only 6 bits set to $\mathbf{1}$, then only $\binom{6}{4} = 15$ choices of 4 bits will give 4 bits to $\mathbf{1}$. We obtain respectively 5 and 1 choices that give 4 bits to $\mathbf{1}$ for the other cases. A similar result is obtained when ω has more bits to $\mathbf{0}$ than bits to $\mathbf{1}$. This means that on input $|\nu\rangle |\omega\rangle$, the circuit $\mathcal{D}_i$ will give the qubit $\mathcal{D}_i |\nu\rangle |\omega\rangle = (\mathcal{A}_i^k |\nu\rangle) \otimes |\omega\rangle$, with $k \in \{1, 5, 15, 35\}$. As $\mathcal{A}_i^2 = \mathcal{I}$, this gives $\mathcal{D}_i |\nu\rangle |\omega\rangle = (\mathcal{A}_i |\nu\rangle) \otimes |\omega\rangle = (\mathcal{A}_i \otimes \mathcal{I}) |\nu\rangle |\omega\rangle$. As this is true over a basis, this is true for the whole space, that is $\mathcal{D}_i = (\mathcal{A}_i \otimes \mathcal{I})$.

We have obtained quantum circuits representing the gates $(\mathcal{A}_i \otimes \mathcal{I})$. That establishes universality of the set $\{\mathcal{C}_i\}$. □

Remark The key point is that $\binom{2^k+p}{2^k}$ is always odd. The whole argumentation can be reproduced to prove for all $k \geq 2$ the existence of a set of quantum gates over $2^k + 2$ qubits which is $(2^k - 1, 0)$-universal but not $(2^{k-1} - 2, 0)$-universal.

3 Deciding Density

We now give a polynomial time algorithm to decide whether a subgroup of a unitary group is dense. The algorithm is in fact more powerful as it deals with a larger class of groups, namely groups with a simple Lie algebra.

Note that for many classical groups, the adequate notion is the density for the Zariski topology of real spaces, rather than the density for the usual, Euclidean, topology. For compact matrix groups, these notions are equivalent [12].

The algorithm is then extended to the case of $\mathbf{SO}_4$, the only group in $\mathbf{SO}_n, \mathbf{SU}_n$ that cannot be handled by the previous approach (as its Lie algebra is not simple). We then are able to give an algorithm for universality.

3.1 Lie algebras

We give here some elements of the theory of Lie algebras that we will use later. We refer the reader to [12] for more precise definitions.

Let A be a subset of $\mathbb{R}^n$. A is Zariski-closed if there exists a polynomial p such that $(x_1 \dots x_n) \in A \iff p(x_1 \dots x_n) = 0$. The Zariski closure of a set A is the smallest Zariski-closed set that contains A.

A linear algebraic group is a subgroup of $\mathbf{GL}_n(\mathbb{R})$ (seen as a subset of $\mathbb{R}^{n^2}$) which is also Zariski-closed. Note that we will see subgroups of $\mathbf{GL}_n(\mathbb{C})$ as subgroups of $\mathbf{GL}_{2n}(\mathbb{R})$, as $\mathbf{U}_n$ is Zariski-closed considered as a real variety, but not as a complex one. Many classical groups (and all compact groups) are Zariski-closed: It is the case for $\mathbf{SL}_n, \mathbf{U}_n, \mathbf{O}_n, \mathbf{SO}_n \dots$.

The Lie algebra $\mathfrak{g}$ of a group G is the tangent space at the identity: $\mathcal{M}$ is in $\mathfrak{g}$ if there exists a differentiable curve τ in G, $\tau : [a, b] \mapsto G$ such that $\tau(0) = \mathcal{I}$ and its derivative $\tau'(0)$ is equal to $\mathcal{M}$ (Thus $\mathfrak{g}$ is a subset of $\mathbf{M}_n(\mathbb{R})$).

If G is an infinite linear algebraic group, $\mathfrak{g}$ is not trivial. Lie algebras determines in some way the groups. Indeed, if H is a subgroup of G such that G and H have the same Lie algebra and are connected, then $H = G$.

There is a natural structure over $\mathfrak{g}$: $\mathfrak{g}$ is a vector space closed under the operation $[\mathcal{A}, \mathcal{B}] = \mathcal{A}\mathcal{B} - \mathcal{B}\mathcal{A}$. A sub-algebra of $\mathfrak{g}$ is a subspace closed by the bracket operator. A sub-algebra $\mathfrak{h}$ such that for all $\mathcal{M} \in \mathfrak{g}, \mathcal{N} \in \mathfrak{h}$, $[\mathcal{M}, \mathcal{N}] \in \mathfrak{h}$ is called an ideal of $\mathfrak{g}$. The Lie algebra of a closed normal subgroup of G is an ideal of $\mathfrak{g}$, hence ideal of Lie Algebras in some way measure the simplicity of the groups.

We will use the following property:

Proposition 5 *Let G be a linear algebraic group and $\mathfrak{g}$ its Lie algebra.*

Let $\mathfrak{h}$ be a sub-algebra of $\mathfrak{g}$. If $\mathfrak{h}$ is closed under conjugation by G (that is by the homomorphisms $\mathcal{X} \mapsto \mathcal{M}\mathcal{X}\mathcal{M}^{-1}$ for $\mathcal{M} \in G$), then $\mathfrak{h}$ is an ideal of $\mathfrak{g}$.

Proof. Let $\mathcal{M} \in \mathfrak{g}$, and τ such that $\tau(0) = \mathcal{I}, \tau'(0) = \mathcal{M}$. Let $\mathcal{X} \in \mathfrak{h}$. We know that the function $\theta : t \mapsto \tau(t)\mathcal{X}\tau(t)^{-1}$ takes value on $\mathfrak{h}$, hence $\theta'(0) \in \mathfrak{h}$. A straightforward computation gives $\theta'(t) = \tau'(t)\mathcal{X}\tau(t)^{-1} - \tau(t)\mathcal{X}\tau(t)^{-1}\tau'(t)\tau(t)^{-1}$ Hence, $\theta'(0) = \mathcal{M}\mathcal{X} - \mathcal{X}\mathcal{M} \in \mathfrak{h}$. ☐

A Lie algebra such that the bracket operator is identically zero is called abelian. A Lie algebra with no proper nonzero ideals and non-abelian is called simple. Simple Lie algebras will be the cornerstone of the proofs below.

3.2 Deciding density for connected groups with a simple Lie algebra

We now introduce a standard construction that will simplify the statements of the theorem and of the proofs. Let ϕ be the function over $n \times n$ matrices given by $\phi(\mathcal{X}) = \mathcal{X} \otimes \left(\mathcal{X}^{-1}\right)^T$. If $\mathcal{X}$ is unitary, $\phi(\mathcal{X})$ is simply $\mathcal{X} \otimes \overline{\mathcal{X}}$ where $\overline{\mathcal{X}}$ is the conjugate of $\mathcal{X}$. For any matrix $\mathcal{Y}$, note $\operatorname{Vec}\mathcal{Y}$ the column vector consisting of the juxtaposition of all columns of $\mathcal{Y}$. The following lemma is clear [13]:

Lemma 5. *$\phi(\mathcal{X}) \operatorname{Vec}\mathcal{Y} = \operatorname{Vec}\mathcal{X}^{-1}\mathcal{Y}\mathcal{X}$.*

Hence, the operator ϕ captures the notion of conjugation in a vector space. For any group G, note $\operatorname{env} G$ the enveloping algebra of G, that is the linear closure over $\mathbb{R}$ of all matrices of G.

Theorem 6. *Let $G \subseteq \mathbf{GL}_n(\mathbb{R})$ be a (Zariski) closed connected group with a simple Lie algebra. Then a subgroup H of G is (Zariski) dense in G if and only if H is infinite and $\operatorname{env}\phi(H) = \operatorname{env}\phi(G)$.*

Remark The requirement on H to be infinite is necessary. In $\mathbf{SO}_3$, the group of all isometries of the icosahedron is finite but satisfies $\operatorname{env}\phi(H) = \operatorname{env}\phi(\mathbf{SO}_3)$.

Proof. Suppose H is dense in G. Obviously, H is infinite. $\operatorname{env}\phi(H)$ is a vector space, and is hence Zariski-closed. It must therefore contain the Zariski-closure of $\phi(H)$, that is $\phi(G)$. $\operatorname{env}\phi(H) = \operatorname{env}\phi(G)$ follows.

Conversely, note Γ the Zariski-closure of H. As H is infinite, Γ is of non-zero dimension, hence its Lie algebra γ is not trivial. Now, $\operatorname{env}\phi(H) = \operatorname{env}\phi(G)$ entails that γ is stable by conjugation by G. Indeed, as γ is stable by conjugation by H, $\operatorname{Vec}\gamma$ is stable by multiplication by $\phi(h)$ for any $h \in H$ using lemma 5. By linearity, $\operatorname{Vec}\gamma$ is then stable by multiplication by any element of $\operatorname{env}\phi(H)$, hence by multiplication by any $\phi(g), g \in G$, as $\phi(G) \subseteq \operatorname{env}\phi(H)$. By lemma 5, this means that γ is stable by conjugation by G.

Then γ is an ideal of $\mathfrak{g}$, the lie algebra of G, by proposition5. γ is not trivial, and $\mathfrak{g}$ is simple, hence $\gamma = \mathfrak{g}$, and $\Gamma = G$. □

Remark The hypotheses of the theorem can be loosened by requiring that the Lie algebra of G has no proper nonzero ideals. The hypothesis of simplicity also implies that the Lie algebra is non-abelian but we do not use this fact here. Hence, the theorem is also true for $G = \mathbf{SU}_1, G = \mathbf{SO}_2 \ldots$

Many classical groups have a simple Lie algebra ($\mathbf{SO}_n(\mathbb{R})$ for $n \notin \{1, 2, 4\}$, $\mathbf{SU}_n$ for $n \geq 2$, ...) and this theorem directly provides an algorithm for these groups.

Theorem 7. *There is a polynomial-time algorithm which given a finitely generated subgroup of* $\mathbf{SU}_n$ *decides if* H *is dense over* $\mathbf{SU}_n$*. The algorithm checks if* H *is infinite then computes the enveloping algebra of* $\phi(H)$ *and compare it with the enveloping algebra of* $\phi(G)$*.*

There are many polynomial time algorithms to decide whether a group is finite or not [14], and computing the enveloping algebra can also be done in polynomial time, hence providing the announced complexity.

3.3 Deciding density for $\mathbf{SO}_4(\mathbb{R})$

If the Lie algebra $\mathfrak{g}$ of G is not simple, the algorithm will not work: The Lie algebra $\mathfrak{h}$ might be a proper ideal of $\mathfrak{g}$ and we cannot directly deduce to the equality $\mathfrak{g} = \mathfrak{h}$.

This is the case for $G = \mathbf{SO}_4(\mathbb{R})$. First set

$$\sigma_1(a,b,c,d) = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \quad \sigma_2(a,b,c,d) = \begin{pmatrix} a & b & c & -d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$$

G is not simple and contains two infinite closed normal subgroups [15] defined by $G_i = \left\{\sigma_i(a,b,c,d), a^2+b^2+c^2+d^2 = 1\right\}$ for $i \in \{1,2\}$, which give rise to the simple Lie algebras $\mathfrak{g}_i = \left\{\sigma_i(0,a,b,c), (a,b,c) \in \mathbb{R}^3\right\}$ ($\mathfrak{so}_4 = \mathfrak{g}_1 + \mathfrak{g}_2$).

Now, some computations prove that the subgroup H generated by G_1 and the matrices $\sigma_2(0,0,1,0)$ and $\sigma_2(1/2,1/2,1/2,1/2)$ is infinite (as it contains G_1), with $\mathfrak{g}_1$ as its Lie algebra, and satisfies $\operatorname{env}\phi(H) = \operatorname{env}\phi(\mathbf{SO}_4)$. We must therefore strengthen the hypotheses.

If the Lie algebra of H is $\mathfrak{g}_1$, then H/G_1 (the image of H in the quotient group G/G_1) is finite. we will hence require H/G_1 to be infinite. This gives:

Theorem 8. *Let* H *be a subgroup of* $\mathbf{SO}_4$*. Then* H *is dense if and only if* $\operatorname{env}\phi(H) = \operatorname{env}\phi(\mathbf{SO}_4)$ *and the groups* H/G_1 *and* H/G_2 *are infinite.*

Deciding if H/G_1 is infinite is easy. Indeed, $\mathbf{SO}_4/G_1$ is an affine group, and for this particular case, we know a representation of $\mathbf{SO}_4/G_1$.

Theorem 9. *Let* ψ_1 *be the morphism*

$$\begin{array}{cccc} \psi_1 : & \mathbf{SO}_4 & \mapsto & \mathbf{SO}_4 \\ & \begin{pmatrix} a & e & i & m \\ b & f & j & n \\ c & g & k & o \\ d & h & l & p \end{pmatrix} & \mapsto & \sigma_1(a,b,c,d)^T \begin{pmatrix} a & e & i & m \\ b & f & j & n \\ c & g & k & o \\ d & h & l & p \end{pmatrix} \end{array}$$

Then ψ_1 *is a morphism of kernel* G_1*.*

Hence, testing for H/G_1 to be infinite is the same as testing for $\psi_1(H)$ to be infinite. The same result holds for G_2 with the morphism:

$$\begin{array}{rccl} \psi_2 : & \mathbf{SO}_4 & \mapsto & \mathbf{SO}_4 \\ & \begin{pmatrix} a & e & i & m \\ b & f & j & n \\ c & g & k & o \\ d & h & l & p \end{pmatrix} & \mapsto & \begin{pmatrix} a & e & i & m \\ b & f & j & n \\ c & g & k & o \\ d & h & l & p \end{pmatrix} \sigma_2(a,e,i,m)^T \end{array}$$

This gives the theorem:

Theorem 10. *A subgroup H of $\mathbf{SO}_4(\mathbb{R})$ is dense in $\mathbf{SO}_4$ if and only if* $\operatorname{env}\phi(H) = \operatorname{env}\phi(\mathbf{SO}_4(\mathbb{R}))$ *and the groups $\psi_1(H)$ and $\psi_2(H)$ are infinite.*

We thus obtain an algorithm to test the density of a subgroup of $\mathbf{SO}_4(\mathbb{R})$.

3.4 Universality

The discussion of the previous section can be generalised to $\mathbf{U}_n$ which has two normal connected subgroups $\mathbf{SU}_n$ and $\mathbf{U}_1\mathcal{I}$.

Theorem 11. *Let H be a subgroup of $\mathbf{U}_n$. Then H is dense if and only if* $\operatorname{env}\phi(H) = \operatorname{env}\phi(G)$ *and the groups* $\det H$ *and $\phi(H)$ are infinite.*

Proof. Just note that $\phi(\mathcal{M}) = \mathcal{I}$ if and only if $\mathcal{M} \in \mathbf{U}_1\mathcal{I}$. Hence $\phi(H)$ infinite means that $\mathbf{U}_n/\mathbf{U}_1\mathcal{I}$ is infinite, whereas $\det H$ infinite means that $\mathbf{U}_n/\mathbf{SU}_n$ is infinite. ☐

The following corollary is useful for our purposes :

Corollary 12 *Let H be a subgroup of $\mathbf{U}_n$. Then $\mathbf{U}_1 H$ is dense if and only if* $\operatorname{env}\phi(H) = \operatorname{env}\phi(G)$*, and $\phi(H)$ is infinite.*

This gives an algorithm for the $(k,0)$-universality

Theorem 13. *There is an algorithm which, given a set S of gates over n-qubits, decides if S is $(k,0)$-universal.*

The algorithm works as follows: compute the gates $(\mathcal{M} \otimes \mathcal{I}_{2^k})[\sigma]$ for any $\mathcal{M} \in S$, then decide whether the group H generated by these gates is such that $\mathbf{U}_1 H$ is dense by computing $\operatorname{env}\phi(H)$, $\operatorname{env}\phi(\mathbf{U}_{2^{k+n}})$ and $\phi(H)$ and applying corollary 12. The size of the matrices is 2^{k+n}, and there are $(k+n)!\,|S|$ such matrices, hence the algorithm will be at least exponential in k and n. However, if k and n are fixed, the algorithm is polynomial in $|S|$ and the size of the coefficients.

Based on the same ideas, we can give a theorem about $(0,1)$-universality. Let write $\mathcal{A} \odot \mathcal{B}$ the block diagonal matrix $\operatorname{diag}(\mathcal{A}, \mathcal{B})$. Note that $(0,1)$-universality means that for any quantum gate $\mathcal{M}$ over n qubits, there exists $\lambda \in \mathbf{U}_1$ and a quantum gate $\mathcal{N}$ in $\overline{G_{n+1}(S)}$ such that $P_{n,n+1}(\mathcal{N}) = \lambda\mathcal{M}$ (that is, as $\mathcal{M}$ is unitary, $\mathcal{N} = \lambda\mathcal{M} \odot \mathcal{C}$ for some $\mathcal{C}$).

We note Δ_n the subspace of $\mathbf{M}_{2^{n+2}}(\mathbb{C})$ spanned by matrices of the form $\mathcal{A}_1 \odot \mathcal{A}_2 \odot \mathcal{A}_3 \odot \mathcal{A}_4$, $\mathcal{A}_i \in \mathbf{M}_{2^n}(\mathbb{C})$. For every subspace H of $\mathbf{M}_{2^{n+2}}(\mathbb{C})$, we will note $E_n(H)$ the set of matrices $\mathcal{M}$ such that $\mathcal{M} \odot \mathcal{A}_2 \odot \mathcal{A}_3 \odot \mathcal{A}_4 \in H$ for some $\mathcal{A}_i \in \mathbf{M}_{2^n(\mathbb{C})}$

Theorem 14. *Let $\mathcal{S}$ be a set of quantum gates over n qubits. We will note $H = G_{n+1}(\mathcal{S})$. Then $\mathcal{S}$ is $(0,1)$-universal if and only if $E_{2n}(\phi(H))$ is infinite and* $\operatorname{env}\phi(\mathbf{U}_{2^n}) \subseteq P_{2n,2n+2}(\operatorname{env}\phi(H) \cap \Delta_{2n})$.

The second condition basically means that for every $\mathcal{G} \in \mathbf{U}_{2^n}$, there exists an $\mathcal{M} \in \operatorname{env}\phi(H)$ such that $\mathcal{M} = \phi(\mathcal{G}) \odot \mathcal{H}_1 \odot \mathcal{H}_2 \odot \mathcal{H}_3$ for some $\mathcal{H}_i$.

Proof. The first condition is obviously necessary. If S is $(0,1)$-universal, for every $\mathcal{G} \in \mathbf{U}_{2^n}$, there exists a $\mathcal{N} \in \overline{H}$ such that $\mathcal{N} = \lambda\mathcal{G} \odot \mathcal{C}$ for some $\mathcal{C}$ and λ. Then $\phi(\mathcal{N}) = \phi(\mathcal{G}) \odot (\lambda\mathcal{G} \otimes \overline{\mathcal{C}}) \odot (\mathcal{C} \otimes \overline{\lambda\mathcal{G}}) \odot \phi(\mathcal{C})$, hence the second condition.

Conversely, we note X the set of matrices $\mathcal{A}$ such that there exists $\mathcal{B}$ with $\mathcal{A} \odot \mathcal{B} \in \mathfrak{h}$, the Lie Algebra of $\overline{H}$. X is obviously a subalgebra of $\mathfrak{u}_{2^n}$. The first condition states that $X \cap \mathfrak{su}_{2^n} \neq \{0\}$.

We now interpret the second condition. A straightforward computation shows that $(\phi(\mathcal{G}) \odot \mathcal{H}_1 \odot \mathcal{H}_2 \odot \mathcal{H}_3)\operatorname{Vec}(\mathcal{A} \odot \mathcal{B}) = \operatorname{Vec}(\mathcal{G}^T \mathcal{A}\mathcal{G} \odot \mathcal{C})$ with $\operatorname{Vec}\mathcal{C} = \mathcal{H}_3 \operatorname{Vec}\mathcal{B}$. Hence X is stable by conjugation by any $\mathcal{G} \in \mathbf{U}_{2^n}$.

X is therefore an ideal of $\mathfrak{u}_{2^n}$, and by simplicity we obtain $\mathfrak{su}_{2^n} \subseteq X$. By definition of X, H contains for all $\mathcal{G} \in \mathbf{SU}_{2^n}$ an element of the form $\mathcal{G} \odot \mathcal{C}$ for some $\mathcal{C}$. Hence $\mathcal{G}U_1H$ contains for all $\mathcal{G} \in \mathbf{U}_{2^n}$ an element of the form $\mathcal{G} \odot \mathcal{C}$. $\square$

The condition about the enveloping algebra uses basic notions of linear algebra, hence is easy to test. The finiteness of $E_{2n}(\phi(H))$ is more difficult to test, as we do not know generators of this group. However, if S is $(0,1)$-universal, then $\phi(H)$ must obviously be infinite.

Conversely, suppose $\operatorname{env}\phi(\mathbf{U}_{2^n}) \subseteq P_{2n,2n+2}(\operatorname{env}\phi(H) \cap \Delta_{2n})$ and $\phi(H)$ is infinite. Then, using the same kind of arguments, we can prove that S is $(1,1)$-universal. We then have the following theorem

Theorem 15. *Let S be a set of quantum gates over n qubits, $H = G_{n+1}(S)$.*

- *If S is $(0,1)$-universal then* $\operatorname{env}\phi(\mathbf{U}_{2^n}) \subseteq P_{2n,2n+2}(\operatorname{env}\phi(H) \cap \Delta_{2n})$ *and $\phi(H)$ is infinite.*
- *If* $\operatorname{env}\phi(\mathbf{U}_{2^n}) \subseteq P_{2n,2n+2}(\operatorname{env}\phi(H) \cap \Delta_{2n})$ *and $\phi(H)$ is infinite, then S is $(1,1)$-universal.*

This theorem can obviously be extended to (k,p)-universality. It doesn't provide a direct characterisation of (k,p)-universality, but if one is just interested in the number of ancillas (that is p) necessary for S to be universal, this will give a decent algorithm.

4 Conclusion

We have given a new definition of universality for quantum gates and several examples which prove that many of these notions of universality are distinct. The basic open question is about (k,∞)-universality. If we can approach any gate with some set of gates S using some ancillas, is the number of necessary ancillas related to the required precision, or can we find a bound on the number of ancillas to be used ? We conjecture that a set S is (k,∞)-universal if and only if it is (k,p)-universal for some p.

We also give an algorithm which, in polynomial time decides if some subgroup of a classical group $(\mathbf{SU}_n, \mathbf{SL}_n, \mathbf{SO}_n \ldots)$ is (Zariski-)dense. This gives an algorithm to decide $(k,0)$-universality. We only provide a partial result for (k,p)-universality. It would be interesting to give polynomial time algorithms for other decision problems about Zariski-closed groups, like deciding if the intersection of two Zariski-closed groups is non trivial, as this would lead to a polynomial time algorithm for the (k,p)-universality.

References

1. Post, E.: The two-valued iterative systems of mathematical logic. Volume 5 of Annals Mathematical Studies. Princeton University Press (1941)
2. Fredkin, E., Toffoli, T.: Conservative Logic. International Journal of Theoretical Physics **21** (1982) 219–253
3. Lloyd, S.: Almost any quantum logic gate is universal. Physical Review Letters **75** (1995) 346–349
4. DiVincenzo, D.P.: Two-bit gates are universal for quantum computation. Physical Review A **51** (1995) 1015–1022
5. Deutsch, D.: Quantum computational networks. Proceedings of the Royal Society of London Ser. A **425** (1989) 73–90
6. Deutsch, D., Barenco, A., Ekert, A.: Universality in quantum computation. Proceedings of the Royal Society of London, Series A **449** (1995) 669–677
7. Barenco, A., Bennett, C.H., Cleve, R., DiVincenzo, D.P., Margolus, N.H., Shor, P.W., Sleator, T., Smolin, J.A., Weinfurter, H.: Elementary gates for quantum computation. Physical Review A **52** (1995) 3457–3467
8. Barenco, A.: A universal two-bit gate for quantum computation. Proceedings of the Royal Society of London, Series A **449** (1995) 679–683
9. Kitaev, A., Shen, Vyalyi: Classical and Quantum computation. Volume 47 of Graduate Studies in Mathematics. American Mathematical Society (2003)
10. Brylinski, J.L., Brylinski, R.: Universal Quantum Gates. In: Mathematics of Quantum Computation. Chapman & Hall (2002)
11. Derksen, H., Jeandel, E., Koiran, P.: Quantum automata and algebraic groups. to appear (2004)
12. Onishchik, A., Vinberg, E.: Lie groups and algebraic groups (1990)
13. Graham, A.: Kronecker Products and Matrix Calculus: with Applications. Ellis Horwood Limited (1981)
14. Babai, L., Beals, R., Rockmore, D.N.: Deciding finiteness for matrix groups in deterministic polynomial time. ISSAC' 93, ACM Press, New York (1993) 117–126
15. Mneimné, R., Testard, F.: Introduction à la théorie des groupes de Lie classiques. Hermann (1986)