Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 221 (2008) 61–69

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

An Algorithmic Construction of Quantum Circuits of High Descriptive Complexity

Willem L. Fouché[1,2]

Department of Decision Sciences
University of South Africa
Pretoria, South Africa

Abstract

We discuss an algorithmic construction which, for any finite but universal set of computable quantum gates and a given measurement basis, will produce a *rational* quantum circuit whose shortest ϵ-approximations from products of instances of the gates have sizes which grow at least exponentially in the input sizes of the circuits and logarithmically in the reciprocal of ϵ. We also discuss the constructive content of the Solovay-Kitaev theorem by considering the algorithmic enumeration of all quantum circuits of a given input size.

Keywords: Large quantum circuits, Solovay-Kitaev theorem. computable representations.

1 Introduction

In [3], we find a discussion, among other things, of the programmability of universal quantum Turing machines. In this paper, we expand on this discussion and consider algorithmic and complexity issues around the effective construction of quantum circuits. Many beautiful papers have been written on this subject and many open problems still remain to be addressed. We shall consider an algorithmic version of a converse of the Solovay-Kitaev theorem. (A proof of this theorem can be found in Appendix 3 of the book [7].)

We shall look at the problem of finding a computable enumeration of unitary operators on a given finite-dimensional complex Hilbert space and the implications of such an enumeration for the algorithmic content of the Solovay-Kitaev theorem.

The proof of the lower bounds in this paper was inspired by the techniques developed by Knill [4] and Nielsen and Chuang [7]. The reader is also referred to [4] for a critique of the claims in [2].

[1] This work supported

[2] Email: fouchwl@gmail.com

doi:10.1016/j.entcs.2008.12.007

We introduce oracle computations relative to Rabin's computable representation of the field of algebraic numbers in order to find effective enumerations of algebraic unitary operators on a given finite-dimensional complex Hilbert space. The latter discussions are perhaps (or definitely) of less importance to quantum computation per se, but do pose interesting arithmetical and computational challenges ...

2 The Solovay-Kitaev theorem

In principle, in the quantum gate model, a quantum computation works as follows.

- The first step typically involves the preprocessing of the input data on a *classical* computer. For example, in the Shor algorithm for the factoring problem we must ensure in a classical way that the input number m is not a prime power.
- Based on these preprocessed data, we have to prepare the quantum register. This means in the most simple case to prepare classical data, e.g., a binary string x of length N, say, as the state $|x\rangle$ in 2^N-dimensional Hilbert space. In most cases, however, one would be required to prepare a superposition of states $|x\rangle$.
- Next we apply the quantum circuit C, which is a sequence of local quantum operators, to the input state $|\phi\rangle$ and after the calculation we get the output state $|U\phi\rangle$ where U is the unitary operator corresponding to C.
- To read out the data we perform a von Neumann measurement on the computational basis.
- Finally, we may have to postprocess the value on a classical computer. In general we obtain a correct result with probability less than one which means we have to check the validity of the result with a polynomial time algorithm and if wrong, we have to go back to the third step.

Hence, in this model, a quantum computation is a *hybrid* of classical and probabilistic algorithms coupled with quantum evolutions of prepared quantum states.

In order to discuss programmability in this context, we recall the notion of instruction sets. (For more on this idea, see, for example the book [7] and [1].) An *instruction set* G for a multiqubit input of a fixed length d is a *finite* set of quantum gates satisfying

- All gates $V \in G$ are in $SU(2^d)$, that is, they are unitary operators on the 2^d-dimensional Hilbert space $H^{\otimes d}$ where H is 2-dimensional over $\mathbf{C}$ and each has determinant one.
- For each $V \in G$ the inverse operation $V^\dagger$ also belongs to G.
- The group generated by G is topologically dense in $SU(2^d)$. This means that for any given quantum gate $U \in SU(d)$ and any measure of accuracy $\epsilon > 0$, there exists a finite product $V = V_1 V_2 \dots V_k$ of instances of gates from G which is an ϵ-approximation to U, that is to say, such that $||U - V_1 V_2 \dots V_k|| < \epsilon$. Here $||.||$ denotes the standard operator norm.

Suppose V is a unitary operator acting on $H^{\otimes f}$. For $d \geq f$, we call a unitary operator on $H^{\otimes d}$ an *instance* of V if it is any operator acting like V on a fixed f of the possible d qubits and as the identity on the remaining qubits.

Suppose U and V are two unitary operators on the same state space with U the target unitary operator that we wish to implement and $V = V_1 V_2 \dots V_k$ is the unitary operator that is actually implemented from an instruction set as above. Let M be a positive operator valued measure (POVM) element associated with the measurement and let P_U (or P_V) be the probability of obtaining the corresponding, measurement outcome if the operation U (or V) was performed with a starting state $|\phi\rangle$. Then it can be shown that

$$|P_U - P_V| = |\langle\phi|U^\dagger M U|\phi\rangle - \langle\phi|V^\dagger M V|\phi\rangle| \leq 2||U - V||.$$

(See [7].) This inequality gives quantitative expression to the idea that when the error $||U-V||$ is small, the difference in probabilities between measurement outcomes is also small.

An example of universal gates is one "generated" by instances of T, the Toffoli gate, and H, the Hadamard gate and the phase gates. It is "generated" in the following sense: We consider all unitary operators for d-qubits which is a tensor product of instances of H, T, the phase gates together with their inverses. Then this set G is an instruction set for multiqubits of length d. (See[7].)

The problem of quantum compilation is the following: Given an instruction set G, how may we approximate an arbitrary quantum gate by means of a finite sequence of instructions from G in a manner which is both effective (i.e., computable in the classical sense), and efficient as far as both the time and space complexity are concerned. The Solovay-Kitaev theorem gives a truly remarkable contribution to this problem.

Theorem 2.1 *Let G be an instruction set for $SU(2^d)$, and let a desired measure of accuracy $\epsilon > 0$ be given. There is a universal constant c such that for any U in $SU(2^d)$, there exists a finite sequence S of instances of gates from G of length $O_d(\log^c(1/\epsilon))$ such that the product of the sequence S is within ϵ of U with respect to the operator norm.*

More precisely, an arbitrary unitary operator U on d qubits can be approximated to within a distance ϵ by using $O(d^2 4^d \log^c(d^2 4^d/\epsilon))$ instances of gates from G. This can be shown to be close to optimal in the following sense: For a given instruction set G and a measure of accuracy $\epsilon > 0$, there are unitary transformations U on d qubits which take $\Omega(2^d \log(1/\epsilon)/\log(d))$ instances of gates from G to implement an approximation V such that $||U - V|| < \epsilon$. We shall later discuss how such a unitary operator U can be algorithmically constructed from the instruction set G.

Many authors state that the Solovay-Kitaev approximation can be done in an effective and efficient manner. This must be read with some care! We call a unitary operation *recursive* with respect to the chosen measurement basis if all its matrix entries relative to this basis are recursive complex numbers. Recall that a complex number is a recursive complex number provided both its real and imaginary parts are recursive real numbers. A real number x is recursive if there is an algorithmic

procedure which with input a natural number n will yield a binary rational number of the form $k/2^n$ such that $|x - k/2^m| < 1/2^n$.

Suppose now that all the matrix entries of the gates in G with respect to the orthonormal basis in which the measurement is performed are recursive complex numbers, but that U is not recursive relative to this basis. Suppose we have an effective procedure that will yield for any given natural n descriptions of instances of gates $V_1, \ldots, V_m$ from G such that $||U - V_1 \cdots V_m|| < 1/n$. Then it is clear that all the matrix coefficients of U with respect to the measurement basis are complex recursive numbers – contradiction.

However, algorithmically, this will turn out to be possible provided U is recursive with respect to the measurement basis as we will explain in the next section.

It is also claimed that this accuracy can be obtained in general using $O_d(\log^{2.71}(1/\epsilon)$ computational steps. As we understand matters at this stage this is correct if the computation is relative to an *oracle* that has complete information about U with respect to the measurement basis.

Much remains to be investigated as to how the computational complexity or arithmetical structure of U affects this claim. In the following three sections we shall begin to look at this problem from various perspectives.

3 Effective enumeration of quantum circuits

We write H for the 2-dimensional Hilbert space over the complex numbers and $H^{\otimes n}$ for the tensor product of n copies of H.

Definition 3.1 For a natural number n, and a fixed (ordered) measurement basis B on $H^{\otimes n}$, an effective enumeration of the recursive quantum gates on $H^{\otimes n}$ is an enumeration (U_j) of *all* the unitary operators on $H^{\otimes n}$, such that there is an algorithmic procedure which will, for given natural numbers j, k, l and n, yield integers k_1, k_2, with the property that

$$|u_{kl} - (\frac{k_1}{2^n} + i\frac{k_2}{2^n})| < \frac{1}{2^n},$$

where u_{kl} is the kl-th entry of the matrix representation of U_j with respect to the measurement basis B. (A quantum circuit U is recursive, relatively to a measurement basis of course, if all its matrix entries are recursive complex numbers.)

In order to construct such an effective enumeration, we must side-step the fact that for a given effective enumeration of recursive complex numbers, it is *not* possible to algorithmically decide equality between two recursive complex numbers from their programs (codes).

Proposition 3.2 *For a natural number n, and a fixed (ordered) measurement basis B on $H^{\otimes n}$, there is an effective enumeration of all the recursive (relatively to B) quantum gates on $H^{\otimes n}$.*

Proof. It follows from Eulers characterisation of Pythagorean triples that the points with rational coordinates on the unit circle is dense in the unit circle. This

means that the set of real numbers θ such that both $\sin\theta$ and $\cos\theta$ are rational numbers, is dense in the set of real numbers. By using spherical coordinates for the points on the unit sphere in real finite-dimensional Euclidean space, we thus see that the set of points with rational coordinates is dense in the unit sphere.

We fix B and an effective enumeration of all the recursive complex numbers. We write S for the unit sphere in $H^{\otimes n}$ and S_r for the points in S whose coordinates relative to B are rational complex numbers. Since S_r is dense in S, it follows that, for any linear operator M on $H^{\otimes n}$ and a natural number k,

$$||M\phi|| < k \leftrightarrow \exists_{\phi \in S_r} ||M\phi|| < k.$$

We can thus effectively enumerate all operators with recursive coefficients (relatively to B) on $H^{\otimes n}$ as (M_{jk}) such that, for every k, the associated M_{jk} are all the operators satisfying $||M_{jk}|| < k$.

With every M_{jk} we associate the selfadjoint operator $H_{jk} = (M_{jk} + M_{jk}^{\dagger})/2$. Note that $H_{jk} = M_{jk}$ when M_{jk} happens to be selfadjoint. Finaly define the unitary operators V_{jk} by $V_{jk} = e^{iH_{jk}}$. By using the Taylor series expansion of the exponential funtion, the sequence (V_{jk}) can be effectively enumerated. This sequence contains all the unitary operators on $H^{\otimes n}$ since for any unitary V, there is a selfadjoint H such that $V = e^{iH}$. This is a simple consequence of the spectral theorem. Finally let $\eta : \omega \to \omega^2$ be a recursive bijection and define U_j by $U_j = V_{\eta(j)}$. Then the sequence (U_j) is an effective enumeration of all the recursive quantum circuits of input size n. This concludes the proof of the proposition.

4 Large rational quantum circuits

We write H for the 2-dimensional Hilbert space over the complex numbers. We fix a natural number n and consider the approximations of unitary operators U on $H^{\otimes n}$ by products P of instances on $H^{\otimes n}$ of sequences of elements in G. We shall frequently refer to such a product P as a unitary operator on $H^{\otimes n}$ generated by G. For a natural number ℓ, we denote by G_ℓ all unitary operators on $H^{\otimes n}$ generated by G which can be written as the product of at most ℓ instances of elements in G. We shall call a unitary operator U *rational* if the matrix coefficients (with respect to the measurement basis) are rational complex numbers.

We shall prove the following

Theorem 4.1 *Let G be an instruction set with recursive gates relative to a chosen measurement basis for $H^{\otimes n}$. There is a uniform algorithm which, for a given n and a rational ϵ with $0 < \epsilon < \frac{1}{2}$, will yield a rational unitary operator on U on $H^{\otimes n}$, such that, if ℓ is such that for some $V \in G_\ell$ it is the case that $||U - V|| < \epsilon$, then*

$$\ell \geq \frac{1}{3}\frac{(2^{n+1}-1)}{gf\log n}\log\frac{1}{2\epsilon}. \tag{1}$$

Here g is the number of gates in G and f is the largest number of qubit inputs to a gate in G.

Proof. Set $N = 2^n$. Let m be the smallest natural number ℓ, such that each

unitary operator U on $H^{\otimes n}$ can be approximated within ϵ by some element in G_ℓ. The existence of such a number ℓ follows directly from the Solavay-Kitaev theorem. It also follows from the fact that $\cup_{\ell \geq 1} G_\ell$ is dense in the compact group $SU(N)$.

Let ϕ_0 in $H^{\otimes n}$ be an element of the (pre-given) measurement basis and let L be the number of unit vectors in $H^{\otimes n}$ of the form $P\phi_0$ with $P \in G_m$. Denote these vectors by $\psi_1, \ldots, \psi_L$. It is clear that

$$L \leq \left[\binom{n}{f} g \right]^m \leq n^{fgm}. \tag{2}$$

Each element in $H^{\otimes n}$ can be presented as a point on the unit sphere S in the $2N$-dimensional real vector space over the real numbers where $N = 2^n$. For a point $u \in S$ write $B(u, \epsilon)$ for the ϵ-neighbourhood of u in S with respect to standard l^2-norm. We note that

$$S \subseteq \bigcup_{i=1}^{L} B(\psi_i, \epsilon).$$

Indeed, let $\phi \in S$ and choose an unitary operator U such that $\phi = U\phi_0$. Such an unitary operator can be found by an application of the Gram-Schmidt orthogonalisation procedure. By construction, there is some $P \in G_m$ such that

$$||P - U|| < \epsilon.$$

In particular,

$$||\phi - P\phi|| < \epsilon.$$

If $P\phi = \psi_i$, say, then $||\phi - \psi_i|| < \epsilon$.

Since

$$S \subseteq \bigcup_{i=1}^{L} B(\psi_i, \epsilon),$$

writing μ for the standard spherical measure on S, it follows that

$$\mu(S) \leq L\mu(B(\psi_1, \epsilon)).$$

It follows from Lemma 2.4 of [4] that

$$\frac{\mu(B(\psi_1, \epsilon))}{\mu(S)} \geq \frac{(\epsilon\sqrt{1 - \epsilon^2/4})^{2N-1}}{\sqrt{2N-1}\,(1 - \epsilon^2/2)}.$$

Consequently,

$$m \geq \frac{1}{3} \frac{(2^{n+1} - 1)}{gf \log n} \log \frac{1}{\epsilon}.$$

We now show that the rational unitary operators are dense in the group $SU(N)$. Choose an instruction set $\mathcal{G}$ consisting of 2-dimensional gates. Since the rational points are dense in the unit circle, for every $\eta > 0$, we can find, for all gates G in $\mathcal{G}$, some rational gate which is an η-approximation to G. Let m be the smallest natural number ℓ, such that each unitary operator U on $H^{\otimes n}$ can be approximated within ϵ by some element in $\mathcal{G}_\ell$. For a given $\epsilon > 0$, choose $\eta > 0$ such that $m\eta < \epsilon$. Then, for $U \in SU(N)$, there is some rational V such that

$$||U - V|| < \epsilon + m\eta < 2\epsilon.$$

Fix $\epsilon > 0$ and choose U such that if ℓ is such that, for some $V \in G_\ell$ it is the case that $||V - U|| < 2\epsilon$, then

$$\ell \geq \frac{1}{3}\frac{(2^{n+1}-1)}{gf \log n}\log \frac{1}{2\epsilon}.$$

Let U_r be a rational unitary operator such that $||U_r - U|| < \epsilon$. Then, if $V \in G_\ell$ and $||V - U_r|| < \epsilon$, it will follow that

$$||V - U|| < 2\epsilon.$$

Consequently, U_r is a rational unitary operator that satisfies the conclusion of the theorem.

We now turn to the construction of such U_r's. We can recursively enumerate all the rational unitary operators $H^{\otimes n}$ as $U_1, U_2, \ldots$, say. By this we mean that there is an algorithm which, for any given j, computes all the codes of the matrix entries of U_j.

For given n and ϵ as in the formulation of the theorem, let $M(n, \epsilon)$ be given by the right-hand side of (1). We have shown that

$$\exists_i \forall_{\ell < M(n,\epsilon)} \forall_{V \in G_\ell} \; ||U_i - V|| > \epsilon. \tag{3}$$

Note that if we have a description of V as a product of ℓ instances of gates in G, then since

$$||U_i - V|| > \epsilon \leftrightarrow \exists_{\phi \in S_r} \; ||U_i\phi - V\phi|| > \epsilon,$$

it follows from (3) that some U_i with the required property can be computed from n and ϵ. This concludes the proof of the theorem.

5 Algebraic circuits

In this section we consider the computational issues that arise from the construction of quantum circuits whose matrix coefficients are algebraic numbers.

Let $\mathbf{A}$ be the algebraic closure of the field of rational numbers in the field of complex numbers. It was shown by Rabin in [8] that there is a one-to-one map Φ from $\mathbf{A}$ onto a recursive subset B of $\omega = \{0, 1, 2, \ldots\}$ such that the field operations correspond under this map with recursive functions. Such a Φ will be called a computable representation of $\mathbf{A}$. We fix such a function Φ in the sequel.

A predicate P on $\mathbf{A}^k$ is said to be Φ-decidable if there is a decidable predicate Q on ω^k with the property that, for $(\alpha_1, \ldots, \alpha_k) \in \mathbf{A}^k$, it is the case that $P(\alpha_1, \ldots, \alpha_k)$ holds if and only $Q(n_1, \ldots, n_k)$ holds, where $n_i = \Phi(\alpha_i)$ for $i = 1, \ldots, k$. For example, if p is a polynomial with integer coeffients, then the question $p(\alpha) = 0$ is Φ-decidable. Similarly, a function

$$f : \mathbf{A}^k \to \mathbf{A}$$

is said to be Φ-recursive if the correspondinding function on B^k is recursive. One can in this way develop all Φ-versions of arithmetic predicates and functions on tuples of elements in ω.

Since one can Φ-decide whether or not an algebraic number is 1, or 0, one can Φ-effectively enumerate all algebraic unitary operators on $H^{\otimes n}$.

Let $\pi : B \times \omega \to \mathbf{Q}[i]$, where $\mathbf{Q}[i]$ denote the rationals, be any function which maps any element of the form (n, k) to a complex rational number α_k such that, if $\Phi(\alpha) = n$, then $|\alpha - \alpha_k| < \left(\frac{1}{2}\right)^k$.

It is an interesting problem to determine the extent the function π can be computed from Φ. As was noted by van den Dries [9], there is a standard algorithm which, given the code for a algebraic number α, will yield the coefficients of the irreducible polynomial of which α is the root. Following Lachlan and Madison [5], a *notation* for an algebraic number α, is any triple (f, ρ, n) where f is a polynomial in one variable with integer coefficients, ρ is a complex rational, and n is a rational number such that $\xi = \alpha$ is the unique solution of

$$f(\xi) = 0 \wedge |\xi - \rho| < \frac{1}{n}.$$

It was pointed out in [9], that, for a given triple (f, ρ, n) we can effectively decide whether or not it a notation for some algebraic α by using Tarski's decision method for real closed fields. If we now take van den Dries's remark into account, we can conclude that the U_i enumeration has the additional property that for given i one can, relatively to Φ, effectively find arbitrarily accurate complex rational approximations to all the roots of the irreducible polynomials of every matrix entry of U_i. The problem is that we do not know which rational approximation belongs to which root.

Acknowledgement

The author wishes to express his sincere thanks to the co-authors of [3], namely Johannes Heidema, Glyn Jones and Petrus Potgieter, for many long and sometimes intense discussions on the meaning of universality in quantum computation. Moreover, many thanks are due to Chris Swanepoel and Petrus Potgieter for creating a stable and attractive computing environment for me.

References

[1] C. M. Dawson, M. A. Nielsen The Solovay-Kitaev algorithm, quant-ph/0505030v2.
URL http://arxiv.org/abs/quant-ph/0505030

[2] D. Deutsch, A. Barenko, A. Ekert, Univerality in Quantum Computation, Proceedings of the Royal Society of London 449 (1995) 669-677.

[3] W. L. Fouché, J. Heidema, G. Jones, P. H. Potgieter, Universality and Programmability of Quantum Computers, Theoretical Computer Science 403 (2008) 121-129.

[4] E. Knill, Approxiximation by Quantum Circuits, quant-ph/9508006.
URL http://arxiv.org/abs/quant-ph/9508006

[5] A.H. Lachlan, E.D. Madison, Computable Fields and Arithmetically Definable Fields, Proceedings of the American Mathematical Society 24 (1970) 803-807.

[6] M. A. Nielsen, A Geometric Approach to Quantum Circuits Lower Bounds, quant-ph/0502070v1.
URL http://arxiv.org/abs/quant-ph/0502070v1

[7] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000.

[8] M. O. Rabin, Computable algebra: General Theory and Theory of Computable Fields, Transactions of the American Mathematical Society 95 (1960) 341-360.

[9] L. van den Dries, New Decidable Fields of Algebraic Numbers, Proceedings of the American Mathematical Society 77 (1979) 251-256.