Quantum Information and Computation, Vol. 3, No. 1 (2003) 084–092

BOTH TOFFOLI AND CONTROLLED-NOT NEED LITTLE HELP TO DO UNIVERSAL QUANTUM COMPUTING

Yaoyun Shi[a]
Electrical Engineering and Computer Science, University of Michigan
1301 Beal Avenue, Ann Arbor, MI 48109-2122, USA
E-mail: shiyy@eecs.umich.edu

Received June 6, 2002
Revised December 15, 2002

What additional gates are needed for a set of *classical* universal gates to do *universal quantum* computation? We prove that *any* single-qubit real gate suffices, except those that preserve the computational basis. The Gottesman-Knill Theorem implies that any quantum circuit involving only the Controlled-NOT and Hadamard gates can be efficiently simulated by a classical circuit. In contrast, we prove that Controlled-NOT plus any single-qubit real gate that does not preserve the computational basis and is not Hadamard (or its like) are universal for quantum computing. Previously only a generic gate, namely a rotation by an angle incommensurate with π, is known to be sufficient in both problems, if only one single-qubit gate is added.

Keywords: Quantum circuit, universal quantum computation, universal basis, Toffoli, Controlled-NOT.
Communicated by: R Cleve & J Watrous

1. Introduction

A set of quantum gates G (also called a *basis*) is said to be *universal for quantum computation* if any unitary operator can be approximated with arbitrary precision by a circuit involving only those gates (called a G-circuit). Since complex numbers do not help in quantum computation, we also call a set of real gates universal if it approximates arbitrary real orthogonal operators.

Which set of gates are universal for quantum computation? This basic question is important both in understanding the power of quantum computing and in the physical implementations of quantum computers, and has been studied extensively. Examples of universal bases are: (1) Toffoli, Hadamard, and $\frac{\pi}{4}$-gate, due to Kitaev [5] (2) Controlled-NOT, Hadamard, and $\frac{\pi}{8}$-gate, due to Boykin, Mor, Pulver, Roychowdhury, and Vatan [2], and (3) Controlled-NOT plus the set of all single-qubit gate, due to Barenco, Bennett, Cleve, DiVincenzo, Margolus, Shor, Sleator, Smolin, and Weinfurter [1].

Another basic question in understanding quantum computation is: Where does the power of quantum computing come from? Motivated by this question, we rephrase the universality question as follows: Suppose a set of gates G already contains universal classical gates, and

[a]This work was done when the author was at the Institute for Quantum Information at California Institute of Technology, and was supported in part by NSF Grant EIA-0086038, Grant 0049092, and The Charles Lee Powell Foundation.

thus can do universal classical computation, what additional quantum gate(s) does it need to do universal quantum computation? Are there some gates that are *more "quantum"* than some others in bringing more computational power?

Without loss of generality, we assume that G contains the Toffoli gate, since it is universal for classical computation. The above three examples of universal bases provide some answers to this question. It is clear that we need at least one additional gate that does not preserve the computational basis. Let us call such a gate *basis-changing*. Our main result is that essentially the basis-changing condition is the only condition we need:

Theorem 1 *The Toffoli gate and* any *basis-changing single-qubit real gate are universal for quantum computing.*

The beautiful Gottesman-Knill Theorem [3] implies that any circuit involving Controlled-NOT and Hadamard only can be simulated efficiently by a classical circuit. It is natural to ask what if Hadamard is replaced by some other gate. We know that if this replacement R is a rotation by an irrational (in degrees) angle, then R itself generates a dense subset of all rotations, and thus is universal together with Controlled-NOT, by Barenco et al. [1]. What if the replacement is a rotation of rational angles? We show that Hadamard and its compositions with the bit flip gate and the sign flip gate are the only exceptions for a basis-changing single-qubit real gate, in conjunction with Controlled-NOT, to be universal.

Theorem 2 *Let T be a single-qubit real gate and T^2 does not preserve the computational basis. Then $\{Controlled\text{-}NOT, T\}$ is universal for quantum computing.*

A basis is said to be complete if it generates a dense subgroup of $U(k)$ modulo a phase, or $O(k)$ for some $k \geq 2$. We actually prove that each of the two bases in the above theorems gives rise to a complete basis. By the fundamental theorem of Kitaev [5] and Solovay [9], any complete basis can *efficiently* approximate any gate (modulo a phase), or any real gate if the basis is real. Therefore, any real gate can be approximated with precision ϵ using $O(polylog(\frac{1}{\epsilon}))$ gates from either basis, and any circuit over any basis can be simulated with little blow-up in the size.

We also provide an alternative prove for Theorem 1 by directly constructing the approximation circuit for an arbitrary real single-qubit gate, instead of using Kitaev-Solovay theorem. The drawback of this construction is that the size of the approximating circuit is a polynomial in $\frac{1}{\epsilon}$; however, it is conceptually simpler, and uses some new ideas that do not seem to have appeared before (for example, in the approximation for Controlled-sign-flip).

There is a broader concept of universality based on computations on encoded qubits, that is, fault-tolerant quantum computing. We do not discuss this type of computation, an interested reader is referred to the survey of Preskill [8]. For a more detailed reference to related works, refer to the book of Nielsen and Chuang [7].

2. Technical Preliminary

Denote the set $\{1, 2, \cdots, n\}$ by $[n]$. We will mostly follow the notations and definitions from the book by Kitaev, Shen, and Vyalyi [6].

The (pure) state of a quantum system is a unit vector in its state space. The state space of one quantum bit, or qubit, is the two dimensional complex Hilbert space, denoted by $\mathcal{H}$. A prechosen orthonormal basis of $\mathcal{H}$ is called the computational basis and is denoted by

$\{|0\rangle, |1\rangle\}$. The state space of a set of n qubits is the tensor product of the state space of each qubit, and the computational basis is denoted by

$$\{|b\rangle = |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle : b = b_1 b_2 \cdots b_n \in \{0,1\}^n\}\,.$$

A gate is a unitary operator $\mathsf{U} \in \mathbf{U}(\mathcal{H}^{\otimes r})$, for some integer $r > 0$. For an ordered subset A of a set of n qubits, we write $\mathsf{U}[A]$ to denote applying U to the state space of those qubits. A set of gates is also called a *basis*. A *quantum circuit* over a basis G, or a G-circuit, on n qubits and of size m is a sequence $\mathsf{U}_1[A_1]$, $\mathsf{U}_2[A_2]$, $\cdots$, $\mathsf{U}_m[A_m]$, where each $\mathsf{U}_i \in G$ and $A_i \subseteq [n]$. Sometimes we use the same notation for a circuit and for the unitary operator that it defines. In order to carry out universal quantum computing using a finite basis, we need the following notion of approximating a gate using an ancilla state.

Definition 1 *The operator* $\mathsf{U} : \mathcal{H}^{\otimes r} \to \mathcal{H}^{\otimes r}$ *is approximated by the operator* $\tilde{\mathsf{U}} : \mathcal{H}^{\otimes N} \to \mathcal{H}^{\otimes N}$ *using the ancilla state* $|\Psi\rangle \in \mathcal{H}^{\otimes N-r}$ *if, for arbitrary vector* $|\xi\rangle \in \mathcal{H}^{\otimes r}$,

$$\left\| \tilde{\mathsf{U}}(|\xi\rangle \otimes |\Psi\rangle) - \mathsf{U}|\xi\rangle \otimes |\Psi\rangle \right\| \;\leq\; \epsilon \, \||\xi\rangle\| \,.$$

The above definition differs from that in [6] in that the ancilla state allowed can be arbitrary while in the latter it must be a fixed constant state (say $|00\cdots0\rangle$). A *G-ancilla state*, or an ancilla state when G is understood, of ℓ qubits is a state $\mathsf{A}|b\rangle$, for some G-circuit A and some $b \in \{0,1\}^\ell$. A basis G is said to be *universal for quantum computing* if any gate (modulo a phase), or any real gate when each gate in G is real, can be approximated with arbitrary precisions by G-circuits using G-ancillae. By a phase, we mean an element in $\{\exp(i\alpha) : \alpha \in \mathbb{R}\}$.

A basis is said to be *complete* if it generates a dense subgroup of $U(k)$ modulo a phase, or $O(k)$ when its real for some $k \geq 2$. A complete basis is clearly universal, while the reverse is not know to be true. However, it appears that all known universal bases are complete as well, and we note that in some literatures both the universal basis and complete basis are defined as our definition of the latter.

Now we introduce the standard notations for some gates that we shall use later. Denote the identity operator on $\mathcal{H}$ by I. We often identify a unitary operator by its action on the computational basis. The Pauli operators σ^x and σ^z, and the *Hadamard gate* H are

$$\sigma^x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma^z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathsf{H} := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

If U is a gate on r qubits, for some $r \geq 0$ (when $r = 0$, U is a phase factor), $\Lambda^k(\mathsf{U})$ is the gate on $k + r$ qubits that applies U to the last r qubits if and only if the first k qubits are in $|1\rangle^{\otimes k}$. The superscript k is omitted if $k = 1$. Changing the control condition to be $|0\rangle^{\otimes k}$, we obtain $\bar{\Lambda}^k(\mathsf{U})$. The Toffoli gate is $\Lambda^2(\sigma^x)$, and Controlled-NOT is $\Lambda(\sigma^x)$. Evidently the latter can be realized by the former. From now on we only consider real gates. As in the previous section, a gate g is said to be $b$asis-changing if it does not preserve the computational basis.

3. Completeness Proofs

We need the following two lemmas, which fortunately have been proved.

Lemma 1 (Włodarski [10]) *If α is not an integer multiple of $\pi/4$, and $\cos\beta = \cos^2\alpha$, then either α or β is an irrational multiple of π.*

Lemma 2 (Kitaev [5]) *Let $\mathcal{M}$ be a Hilbert space of dimension ≥ 3, $|\xi\rangle \in \mathcal{M}$ a unit vector, and $H \subset SO(\mathcal{M})$ be the stabilizer of the subspace $\mathbb{R}(|\xi\rangle)$. If $\mathsf{V} \in O(\mathcal{M})$ does not preserve $\mathbb{R}(|\xi\rangle)$, $H \bigcup \mathsf{V}^{-1} H \mathsf{V}$ generates a dense subgroup of $SO(\mathcal{M})$.*

We shall prove Theorem 2 first. After that, we need only to consider the special case of $\left\{\Lambda^2(\sigma^x), H\right\}$ to complete the proof for Theorem 1.

Proof of Theorem 2. Define

$$\mathsf{U} := \left(\mathsf{S} \otimes \mathsf{S} \cdot \Lambda(\sigma^x)[1,2]\right)^2.$$

It suffices to prove that U and $\Lambda(\sigma^x)$ generate a dense subgroup of $SO(4)$. Without loss of generality, we assume that U is a rotation by an angle θ, the other case can be proved similarly. Then by the assumption, θ is not an integer multiple of $\pi/4$.

Direct calculation shows that U has eigenvalues $\{1, 1, \exp(\pm i\alpha)\}$, where

$$\alpha = 2 \arccos \cos^2\theta.$$

The two eigenvectors with eigenvalue 1 are

$$|\xi_1\rangle := \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle),$$

and

$$|\xi_2\rangle := \frac{\sin\theta}{\sqrt{2}}(-|00\rangle + |01\rangle) + \frac{\cos\theta}{\sqrt{2}}(|10\rangle - |11\rangle).$$

Let $\{|\xi_i\rangle : i \in [4]\}$ be a set of orthonormal vectors.

By Lemma 1, α is incommensurate with π, therefore, U generates a dense subgroup of $H_1 := SO(\mathrm{span}\{|\xi_3\rangle, |\xi_4\rangle\})$. Note that $\Lambda(\sigma^x)[1,2]$ preserve $|\xi_1\rangle$, but not $\mathrm{span}\{|\xi_2\rangle\}$. Therefore, by Lemma 2, the set

$$H_1 \bigcup \Lambda(\sigma^x)[1,2]\ H_1\ \Lambda(\sigma^x)[1,2]$$

generates a dense subgroup of

$$SO(\mathrm{span}\{|\xi_i\rangle : i = 2,3,4\}) =: H_2,$$

thus so does $\{\mathsf{U}, \Lambda(\sigma^x)[1,2]\}$. Finally, observe that $\Lambda(\sigma^x)[2,1]$ does not preserve $\mathrm{span}\{|\xi_1\rangle\}$, therefore, apply Lemma 2 again we conclude that $\{\mathsf{U}, \Lambda(\sigma^x)[1,2], \Lambda(\sigma^x)[2,1]\}$ generates a dense subgroup of $SO(4)$.

Proof of Theorem 1. Since $\Lambda(\sigma^x)$ can be obtained from $\Lambda^2(\sigma^x)$, we need only to consider the case that the additional single-qubit real gate is basis changing while its square is not. Since all such gates can be obtained from the basis $\left\{H,\ \Lambda^2(\sigma^x)\right\}$, we need only to consider this basis.

Define

$$\mathsf{U} := \left(H \otimes H \otimes H \cdot \Lambda^2(\sigma^x)[1,2,3]\right)^2.$$

Direct calculation shows that U has eigenvalue 1 with multiplicity 6, and the other two eigenvalues $\lambda_\pm := \exp(\pm i\alpha)$, where $\alpha = \pi - \arccos\frac{3}{4}$. Since $\lambda_\pm$ are roots of the irreducible polynomial

$$\lambda^2 - \frac{3}{2}\lambda + 1,$$

which is not integral, therefore $\lambda_\pm$ are not algebraic integers. Thus α is incommensurate with π, which implies that U generates a dense subgroup of the rotations over the corresponding eigenspace (denote the eigenvectors by $|\xi_7\rangle$ and $|\xi_8\rangle$).

By direct calculation, the eigenvectors correspond to eigenvalue 1 are:

$$\{|000\rangle, |010\rangle, |100\rangle, |001\rangle + |011\rangle, |101\rangle + |110\rangle + |111\rangle, |011\rangle - |101\rangle\}.$$

Label the above eigenvectors by $|\xi_i\rangle$, $i \in [6]$. It is easy to verify that each U_i, $i \in [6]$, constructed below preserves $\{|\xi_j\rangle : 1 \le j < i\}$, but not $\mathrm{span}\{|\xi_i\rangle\}$.

$$\begin{aligned}
\mathsf{U}_1 &:= \mathsf{I} \otimes \mathsf{I} \otimes H, & \mathsf{U}_2 &:= \mathsf{U}_1 \cdot \Lambda^2(\sigma^x)[2,3,1] \cdot \mathsf{U}_1, \\
\mathsf{U}_3 &:= \mathsf{U}_1 \cdot \Lambda^2(\sigma^x)[1,3,2] \cdot \mathsf{U}_1, & \mathsf{U}_4 &:= \Lambda^2(\sigma^x)[2,3,1], \\
\mathsf{U}_5 &:= \mathsf{U}_1 \cdot \Lambda^2(\sigma^x)[2,3,1] \cdot \mathsf{U}_1, & \mathsf{U}_6 &:= \Lambda^2(\sigma^x)[1,3,2].
\end{aligned}$$

Applying Lemma 2 several times, we see that $\{\mathsf{U}, \mathsf{U}_i, \mathsf{U}_{i+1}, \cdots, \mathsf{U}_6\}$ generates a dense subgroup of $\mathrm{span}\{|\xi_j\rangle : i \le j \le 8\}$. Thus $\left\{\Lambda^2(\sigma^x), H\right\}$ generates a dense subgroup of $SO(8)$. We leave the details for the interested readers.

4. Alternative Proof for Theorem 1

Fix an arbitrary basis-changing real single-qubit gate S, and the basis

$$\mathfrak{B} := \left\{\mathsf{S}, \Lambda^2(\sigma^x)\right\}.$$

In this section we give an explicit construction to approximate an arbitrary real gate using the basis $\mathfrak{B}$. Due to the following result by Barenco et al. [1], we need only consider approximating single-qubit real gates:

Proposition 3 (Barenco et al. [1]) *Any gate on r qubits can be realized by $O(r^2 4^r)$ Controlled-NOT and single-qubit gates.*

Fix an arbitrary single-qubit gate W that we would like to approximate. Without loss of generality, we can assume that S and W are rotations, for otherwise $\sigma^x\mathsf{S}$ and $\sigma^x\mathsf{W}$ are. For any $\beta \in [0, 2\pi)$, define

$$|\phi_\beta\rangle := \cos\beta|0\rangle + \sin\beta|1\rangle, \qquad \text{and,} \qquad \mathsf{U}_\beta := \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix}.$$

Let $\theta, \alpha \in [0, 2\pi)$, and θ not an integral multiple of $\pi/2$, be such that $\mathsf{S} \equiv \mathsf{U}_\theta$ and $\mathsf{W} \equiv \mathsf{U}_\alpha$. The following proposition can be easily checked.

Proposition 4 *Let $\mathsf{W}_{\alpha/2}$ be a gate on $k+1$ qubits such that $\mathsf{W}_{\alpha/2}|0\rangle^{\otimes k+1} = |\phi_{\alpha/2}\rangle \otimes |0\rangle^{\otimes k}$. With*

$$\mathsf{W}_\alpha := \mathsf{W}_{\alpha/2}\left(-\bar{\Lambda}^{k+1}(-1)\right)\mathsf{W}_{\alpha/2}^\dagger\,\sigma^z[1], \tag{1}$$

for any vector $|\xi\rangle \in \mathcal{H}$,

$$\mathsf{U}_\alpha|\xi\rangle \otimes |0\rangle^{\otimes k} = \mathsf{W}_\alpha(|\xi\rangle \otimes |0\rangle^{\otimes k}). \tag{2}$$

Clearly $\bar{\Lambda}^{k+1}(-1)$ can be realized by $\Lambda^2(\sigma^x)$ and σ^z. Therefore, to approximate U_α, it suffices to approximate σ^z and $\mathsf{W}_{\alpha/2}$, which we will show in the following subsections. Define the constants

$$\delta_\theta := 1/\log\frac{1}{\cos^4\theta + \sin^4\theta}, \quad \text{and,} \qquad \delta'_\theta := 1/\log\frac{1}{\cos^2\theta}.$$

4.1. *Approximating* σ^z

If θ is a multiple of $\pi/4$, say $\theta = \pi/4$, then we can easily do a sign-flip by applying a bit-flip on $\mathsf{U}_\theta|1\rangle = \frac{1}{-\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.

But for a general θ, $\mathsf{U}_\theta|1\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle$ is "biased". The well-known idea of von Neumann on how to approximate a fair coin by tossing a sequence of coins of identical bias[b] immediately comes into mind. To illustrate the idea, consider

$$\mathsf{U}_\theta|0\rangle \otimes \mathsf{U}_\theta|1\rangle = \sin\theta\cos\theta(|11\rangle - |00\rangle) \; + \; \cos^2\theta|01\rangle - \sin^2\theta|10\rangle.$$

If we switch $|00\rangle$ and $|11\rangle$ and leave the other two base vectors unchanged, the first term on the right-hand side changes the sign, while the remaining two terms are unchanged. While we continue tossing pairs of "quantum coins" and do the $|00\rangle$-and-$|11\rangle$ switch, we approximate the sign-flip very quickly. The state defined below will serve the role of $\frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle$.

Definition 2 *For any integer* $k \geq 0$, *the* phase ancilla *of size* k *is the state*

$$|\Phi_k\rangle := (\mathsf{U}_\theta|0\rangle \otimes \mathsf{U}_\theta|1\rangle)^{\otimes k}.$$

Clearly $|\Phi_k\rangle$ can be prepared from $|0\rangle^{\otimes 2k}$ by a $\mathfrak{B}$-circuit of size $O(k)$.

Lemma 3 *The operator* σ^z *can be approximated with precision* ϵ, *for any* $\epsilon > 0$, *by a* $\mathfrak{B}$*-circuit of size* $O(k)$, *using the phase ancilla* $|\Phi_k\rangle$, *for some integer* $k = O\left(\delta_\theta \log\frac{1}{\epsilon}\right)$.

Proof: Let k be an integer to be determined later. The following algorithm is a description of a circuit approximating σ^z using $|\Phi_k\rangle$.

Algorithm 1 *A* $\mathfrak{B}$*-circuit* $\tilde{\sigma}^z$ *approximating* σ^z *using the phase ancilla* $|\Phi_k\rangle$.
Let $|b_0\rangle \otimes |b\rangle$ *be a computational base vector, where* $b_0 \in \{0,1\}$ *is the qubit to which* σ^z *is to applied, and* $b = b_1 b'_1 b_2 b'_2 \cdots b_k b'_k \in \{0,1\}^{2k}$ *are the ancilla qubits. Condition on* b_0 *(that is, if* $b_0 = 0$, *do nothing, otherwise do the following),*

> *Case 1: There is no* i *such that* $b_i \oplus b'_i = 0$, *do nothing.*
> *Case 2: Let* i *be the smallest index such that* $b_i \oplus b'_i = 0$, *flip* b_i *and* b'_i.

Clearly the above algorithm can be carried out by $O(k)$ applications of Toffoli. Fix an arbitrary unit vector $|\xi\rangle \in \mathcal{H}$. Since neither σ^z nor $\tilde{\sigma}^z$ changes $|0\rangle\langle 0|(|\xi\rangle \otimes |\Phi_k\rangle)$,

$$\|\sigma^z|\xi\rangle \otimes |\Phi_k\rangle - \tilde{\sigma}^z(|\xi\rangle \otimes |\Phi_k\rangle)\| \;\leq\; \|-|1\rangle \otimes |\Phi_k\rangle - \tilde{\sigma}^z(|1\rangle \otimes |\Phi_k\rangle)\|\,. \tag{3}$$

[b] That is, toss two coins, declare "0" if the outcomes are "01", declare "1" if the outcomes are "10", and continue the process otherwise.

Let $\left|\Phi_k^+\right\rangle$ ($\left|\Phi_k^-\right\rangle$) be the projection of $|\Phi_k\rangle$ to the subspace spanned by the base vectors satisfying Case (1) (Case (2)), it is easy to prove by induction that

$$\tilde{\sigma}^z(|1\rangle \otimes \left|\Phi_k^+\right\rangle) = |1\rangle \otimes \left|\Phi_k^+\right\rangle, \quad \text{and,} \quad \tilde{\sigma}^z(|1\rangle \otimes \left|\Phi_k^-\right\rangle) = -|1\rangle \otimes \left|\Phi_k^-\right\rangle.$$

Furthermore,

$$\left\|\left|\Phi_k^+\right\rangle\right\| = \left(\cos^4\theta + \sin^4\theta\right)^{k/2}.$$

Therefore, the left-hand side of Equation 3 is upper bounded by

$$2\left\|\left|\Phi_k^+\right\rangle\right\| = 2\left(\cos^4\theta + \sin^4\theta\right)^{k/2}.$$

Since θ is not a multiple of $\pi/2$, the right-hand side is < 1. Thus choosing $k = O(\delta_\theta \log \frac{1}{\epsilon})$, the right-hand side in the above can be made $\leq \epsilon$. $\square$.

4.2. *Creating* $\left|\phi_{\alpha/2}\right\rangle$

We would like to construct a circuit that maps $|0\rangle \otimes |0\rangle^{\otimes k}$ to a state close to $\left|\phi_{\alpha/2}\right\rangle \otimes |0\rangle^{\otimes k}$. The main idea is to create a "logical" $\left|\phi_{\alpha/2}\right\rangle$:

$$\left|\hat{\phi}_{\alpha/2}\right\rangle := \cos\frac{\alpha}{2}|\hat{0}\rangle + \sin\frac{\alpha}{2}|\hat{1}\rangle, \tag{4}$$

where $\left|\hat{0}\right\rangle$ and $\left|\hat{1}\right\rangle$ are two orthonormal vectors in a larger space spanned by ancillae, and then undo the encoding to come back to the computational basis. To create $\left|\hat{\phi}_{\alpha/2}\right\rangle$, we first create a state almost orthogonal to $\left|\hat{0}\right\rangle$, and then apply Grover's algorithm [4] to rotate this state toward $\left|\hat{\phi}_{\alpha/2}\right\rangle$. Define the operator T_θ on 2 qubits as

$$\mathsf{T}_\theta := \mathsf{U}_{-\theta}[1]\ \Lambda(\sigma^x)[1,2]\ \mathsf{U}_\theta[1]. \tag{5}$$

Since for any β, $\mathsf{U}_{-\beta} = \sigma^x \mathsf{U}_\beta \sigma^x$, T_θ and $\Lambda(\mathsf{T}_\theta)$ can be realized by the basis $\mathfrak{B}$. Let

$$\mathfrak{B}_1 := \left\{\Lambda^2(\sigma^x), \sigma^z, \mathsf{U}_\theta, \mathsf{U}_{-\theta}, \mathsf{T}_\theta, \Lambda(\mathsf{T}_\theta)\right\}.$$

Lemma 4 *For any $\epsilon > 0$ there exists a $\mathfrak{B}_1$-circuit $\tilde{\mathsf{W}}_{\alpha/2}$ of size $O(\delta'_\theta \frac{1}{\epsilon} \log \frac{1}{\epsilon})$ that uses $O(\delta'_\theta \log \frac{1}{\epsilon})$ ancillae and satisfies*

$$\left\|\tilde{\mathsf{W}}_{\alpha/2}|0\rangle^{\otimes k+1} - \left|\phi_{\alpha/2}\right\rangle \otimes |0\rangle^{\otimes k}\right\| \leq \epsilon.$$

Proof: Figure 1 illustrates our proof. Let $k > 0$ be an integer to be specified later. Define

$$\left|\hat{0}\right\rangle := |0\rangle^{\otimes 2k}, \qquad \left|\tilde{1}\right\rangle := \mathsf{T}_\theta^{\otimes k}\left|\hat{0}\right\rangle, \qquad \text{and,} \qquad \gamma := \arcsin\left(\cos^{2k}\theta\right).$$

Notice that $\pi/2 - \gamma$ is the angle between $\left|\hat{0}\right\rangle$ and $\left|\tilde{1}\right\rangle$, and $0 < \gamma < \pi/2$, since $\sin\gamma = \left\langle\hat{0}\right|\left.\tilde{1}\right\rangle$. Let S be the plane spanned by $\left|\hat{0}\right\rangle$ and $\left|\tilde{1}\right\rangle$ Let $\left|\hat{1}\right\rangle$ be the unit vector perpendicular to $\left|\hat{0}\right\rangle$ in S and the angle between $\left|\hat{1}\right\rangle$ and $\left|\tilde{1}\right\rangle$ is γ.

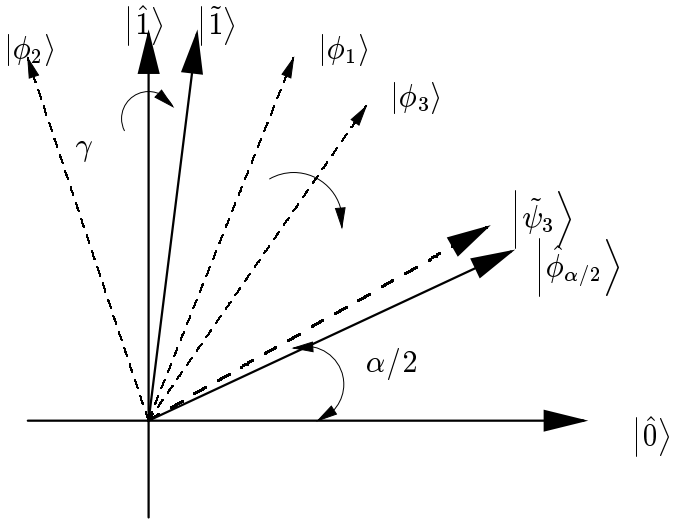

Fig. 1. Creating an approximate $\left|\hat{\phi}_{\alpha/2}\right\rangle$. In one iteration in Grover's algorithm, $|\phi_1\rangle \rightarrow |\phi_2\rangle \rightarrow |\phi_3\rangle$.

Observe that on S we can do the reflection along $\left|\hat{1}\right\rangle$ and the reflection along $\left|\tilde{1}\right\rangle$. The former is simply $\bar{\Lambda}^{2k}(\sigma^z)$, which can be implemented using $\Lambda^2(\sigma^x)$ and σ^z. Since $\mathsf{T}_\theta^{-1} = \mathsf{T}_\theta$, the reflection along $\left|\tilde{1}\right\rangle$ is

$$\mathsf{R} := {\mathsf{T}_\theta}^{\otimes k} \left(-\bar{\Lambda}^{2k}(\sigma^z)\right) {\mathsf{T}_\theta}^{\otimes k}.$$

Without loss of generality we can assume $\alpha/2 < \pi/2$; otherwise we will rotate $\left|\tilde{1}\right\rangle$ close to $\bar{\Lambda}^{2k}(\sigma^z)\left|\hat{\phi}_{\alpha/2}\right\rangle$ and then apply $\bar{\Lambda}^{2k}(\sigma^z)$. Choose k sufficiently large so that $\gamma < \pi/2 - \alpha/2$. Now we can apply Grover's algorithm to rotate $\left|\tilde{1}\right\rangle$ to a state very close to $\left|\hat{\phi}_{\alpha/2}\right\rangle$. After that we do a "controlled-roll-back" to map $\left|\hat{1}\right\rangle$ (approximately) to $|1\rangle^k$ and do not change $\left|\hat{0}\right\rangle$. This will give us an approximation of $\left|\phi_{\alpha/2}\right\rangle$ in the state space of the controlling qubit. The algorithm is as follows. Let T be the integer such that $|\pi/2 - (2T+1)\gamma - \alpha/2| < \gamma$. Then $T = O(1/\gamma)$.

Algorithm 2 *A $\mathfrak{B}_1$-circuit $\tilde{\mathsf{W}}_{\alpha/2}$ that maps $|0\rangle \otimes |0\rangle^{\otimes 2k}$ to a state close to $\left|\phi_{\alpha/2}\right\rangle \otimes |0\rangle^{\otimes 2k}$.*

1. *Apply $\mathsf{I} \otimes \mathsf{T}_\theta^{\otimes k}$.*
2. *(Grover's algorithm) Apply $\left(\mathsf{R}\ \bar{\Lambda}^{2k}(\sigma^z)\right)^T$.*
3. *(Sub-circuit A_3) For a computational base vector $|b\rangle$ of the ancillae, if $|b\rangle \neq \left|\hat{0}\right\rangle$, flip the first bit.*
4. *(Sub-circuit A_4) Use the first bit as the condition bit, apply $\Lambda(\mathsf{T}_\theta^{\otimes k})$.*

It can be easily verified that

$$\left\| \tilde{\mathsf{W}}_{\alpha/2}(|0\rangle \otimes |0\rangle^{\otimes 2k}) - \left|\phi_{\alpha/2}\right\rangle \otimes |0\rangle^{\otimes 2k} \right\| \ \leq \ 2\gamma.$$

Setting $\gamma \approx \epsilon/2$, by direct computation the number of ancillae is $O(k) = O(\delta'_\theta \log \frac{1}{\epsilon})$, and the size of $\tilde{\mathsf{W}}_{\alpha/2}$ is $O(k/\gamma) = O(\delta'_\theta \frac{1}{\epsilon} \log \frac{1}{\epsilon})$. □.

4.3. *Approximating* U_α

Theorem 1 is a straightforward corollary of the following theorem and Proposition 3.

Theorem 5 *For any $\epsilon > 0$, the operator U_α can be approximated with precision ϵ by a $\mathfrak{B}$-circuit of size $O\left(\delta_\theta \cdot \frac{1}{\epsilon} \cdot \log \frac{1}{\epsilon}\right)$ and using $O\left(\delta_\theta \cdot \log \frac{1}{\epsilon}\right)$ ancillae.*

Proof: We first compose a $\mathfrak{B}_1$-circuit that approximates U_α, according to Equation 1, 2, and Algorithm 2, and use k_1 (different) ancillae in each call to the latter, for an integer k_1 to be specified later. Let $\gamma := \cos^{2k_1}\theta$. Then the precision is $O(\gamma)$. After implementing T_θ and $\Lambda(\mathsf{T}_\theta)$, there are in total $O(\frac{1}{\epsilon})$ uses of σ^z.

Finally we apply Algorithm 1 to approximate each σ^z using the *same* phase ancilla $|\Phi_{k_2}\rangle$ for $k_2 = O(1/\gamma^3)$. Let $\delta_\theta := 2(\cos^4\theta + \sin^4\theta)^{k_2/2}$ be the error of one call to $\tilde{\sigma}^z$ using exactly $|\Phi_{k_2}\rangle$. Observe that using the same phase ancilla for $O(\frac{1}{\gamma})$ times causes error at most $1 + 2 + \cdots + O(\frac{1}{\gamma}) - 1 = O(\frac{1}{\gamma^2})$ Setting $\delta_\theta = \gamma^3$, the total error caused by $\tilde{\sigma}^z$ is $O(\gamma)$. Thus the total error of the whole circuit is still $O(\gamma)$. Setting $\gamma \approx \epsilon$, $k_1 = O(\delta'_\theta \log \frac{1}{\epsilon}) = O(\delta_\theta \log \frac{1}{\epsilon})$ and $k_2 = O(\delta_\theta \log \frac{1}{\epsilon})$. Therefore the number of ancillae is $O(k_1 + k_2) = O(\delta_\theta \log \frac{1}{\epsilon})$. The size of the circuit is $O((k_1 + k_2)\frac{1}{\epsilon}) = O(\delta_\theta \frac{1}{\epsilon} \log \frac{1}{\epsilon})$. □.

Acknowledgments

I would like to thank Barbara Terhal, Alexei Kitaev, and Zhenghan Wang for stimulating and helpful discussions, and thanks to Ronald de Wolf and two anonymous referees for valuable comments.

References

1. A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. H. Margolus, P. W. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457–3467, 1995.
2. P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan. A new universal and fault-tolerant quantum basis. *Information Processing Letters*, 75(3):101–107, Aug. 2000.
3. D. Gottesman. The Heisenberg representation of quantum computers. In S. P. Corney, R. Delbourgo, and P. D. Jarvis, editors, *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, pages 32–43, Cambridge, MA, 1999. International Press. Long version: quant-ph/9807006.
4. L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 212–219, Philadelphia, Pennsylvania, May 1996.
5. A. Y. Kitaev. Quantum computations: Algorithms and error correction. *RMS: Russian Mathematical Surveys*, 52(6):1191–1249, 1997.
6. A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and quantum computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002. Translated from the 1999 Russian original by Lester J. Senechal.
7. M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.
8. J. Preskill. Reliable quantum computers. 1997. quant-ph/9705031.
9. R. Solovay. Unpublished manuscript, 1995.
10. Ł. Włodarski. On the equation $\cos\alpha_1 + \cos\alpha_2\cos\alpha_3 + \cos\alpha_4 = 0$. *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.*, 12:147–155, 1969.