Quantum Complexity and Riemannian Geometry

Dong Pyo Chi, [*]

Department of Mathematical Sciences, Seoul National University, Seoul 151-742, Korea

Abstract

Quantum computers hold great promise, but it remains a challenge to find efficient quantum circuits that solve interesting computational problems. Recently, Nielsen *et al*[Science **311**, 1133-1135 (2006)] showed that finding optimal quantum circuits is essentially equivalent to finding the shortest path between two points in a certain curved geometry. By recasting the problem of finding quantum circuits as a geometric problem, it was proposed that the possibility of using Riemannian geometry to suggest new quantum algorithms, or to prove limitations on the power of quantum computers.

Quantum computational algorithms can be executed in parallel on superpositions of exponentially many input states, and their outcomes can be properly measured by virtue of quantum interference. These enable exponential speedups in the solutions of certain problems, and allow one to distinguish between the quantum computational complexity classes and the classical ones [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]. Despite this great promise, as yet there is no general method for constructing good quantum algorithms, and very little is known about the potential power (or limitations) of quantum computers.

A quantum computation is usually described as a sequence of logical gates, each coupling only a small number of qubits. The sequence of gates determines a unitary evolution U performed by the computer. The difficulty of performing the computation is characterized by the number of gates used by the algorithm, which is said to be efficient if the number of gates required grows only polynomially with the size of problem.

Here, in this paper, an alternate approach is proposed to understand the difficulty of implementing a unitary operation U. We suppose that U is generated by some time-dependent Hamiltonian $H(t)$ according to the Schrödinger equation $dU/dt = -iHU$, with the requirement that at an appropriate final time $U(t_f) = U$. We characterize the difficulty of the computation by imposing a cost $F(H(t))$ on the Hamiltonian control, $H(t)$ and then, we choose a cost function on $H(t)$ that defines a Riemannian geometry on the space of unitary operations. Finding the optimal control function $H(t)$ for synthesizing a desired unitary U then corresponds to finding minimal geodesics of the Riemannian geometry and consequently, it can be shown that the minimal geodesic distance between the identity operation and U is essentially equivalent to the number of gates required to synthesize U.

In order to choose a cost function on the control Hamiltonian $H(t)$, we first write $H(t)$ in terms of the Pauli operator expansion $H = \sum_\sigma' h_\sigma \sigma + \sum_\sigma'' h_\sigma \sigma$, where: (1) in the first sum σ ranges over all possible one- and two-body interactions, that is all products of either one or two Pauli matrices acting on n qubits; (2) in the second sum σ ranges over all other tensor products of Pauli matrices and the identity; and (3) the h_σ are real coefficients. We then define a measure of the cost of applying a particular Hamiltonian during

[*] E-mail addresses: dpchi@math.snu.ac.kr .

synthesis of a desired unitary operation

$$F(H) \equiv \sqrt{\sum_{\sigma}^{\prime} h_\sigma^2 + p^2 \sum_{\sigma}^{\prime\prime} h_\sigma^2}. \tag{1}$$

The parameter p is a penalty paid for applying three- and more-body terms. This definition of control cost leads us to a natural notion of distance in $SU(2^n)$.

Let $[U]$ be a curve between the identity operation I and the desired operation U

$$U : [0, t_f] \to SU(2^n)$$

such that $U(0) = I$ and $U(t_f) = U$. The length of this curve can then be defined by the total cost of synthesizing the Hamiltonian that generates evolution along the curve:

$$d([U]) \equiv \int_0^{t_f} dt\, F(H(t)). \tag{2}$$

Since $d([U])$ is invariant with respect to different parameterizations of $[U]$, we can always rescale the Hamiltonian $H(t)$ such that $F(H(t)) = 1$ and the desired unitary U is generated at time $t_f = d([U])$. From now on we assume that we are working with such normalized curves. Finally, the distance $d(I, U)$ between I and U is defined to be the minimum of $d([U])$ over all curves $[U]$ connecting I and U.

What is to be shown here is that for any family of unitaries U there is a quantum circuit containing a number of gates polynomial in $d(I, U)$ that approximates U to high accuracy. Conversely, the metric we construct has the property, that up to a constant factor the distance $d(I, U)$ is a lower bound on the number of one- and two-qubit quantum gates required to exactly synthesize U. Thus, the distance $d(I, U)$ is a good measure of the difficulty of implementing the operation U on a quantum computer.

The function $F(H)$ specified by Eq. 1 can be thought of as the norm associated to a (right invariant) Riemannian metric whose metric tensor g has components:

$$g_{\sigma\tau} \quad = \quad \begin{cases} 0 \text{ if } \sigma \neq \tau \\ 1 \text{ if } \sigma = \tau \text{ and } \sigma \text{ is one- or two-body} \\ p^2 \text{ if } \sigma = \tau \text{ and } \sigma \text{ is three- or more-body.} \end{cases} \tag{3}$$

These components are written with respect to a basis for the local tangent space corresponding to the Pauli expansion coefficients h_σ. The distance $d(I, U)$ is equal to the minimal length solution to the geodesic equation, which may be written as [11]

$$\langle dH/dt, K \rangle = i \langle H, [H, K] \rangle,$$

where $\langle \cdot, \cdot \rangle$ is the inner product on the tangent space $su(2^n)$ defined by the metric components of Eq. 3, and K is an arbitrary operator. For our particular choice of metric components, this geodesic equation may be rewritten as:

$$p_\sigma^2 \dot{h}_\sigma \quad = \quad i \sum_\tau p_\tau^2 h_\tau \tilde{h}_{[\sigma,\tau]}, \tag{4}$$

where $\tilde{h}_{[\sigma,\tau]} = \mathrm{tr}(H[\sigma, \tau])/2^n$.

Our goal is to use the optimal control Hamiltonian $H(t)$ to explicitly construct a quantum circuit containing a number of gates polynomial in $d(I, U)$, and which approximates U closely. The construction combines three main ideas, which we express through three separate lemmas.

The first lemma shows that the error that arises by simply ignoring the many-body interactions in $H(t)$ can be made small by choosing the penalty p appropriately. We define H_P to be the projected Hamiltonian formed by deleting all three- and more-body terms in the Pauli expansion.

Lemma 1: Let $H_P(t)$ be the projected Hamiltonian obtained from a Hamiltonian $H(t)$ generating a unitary U. Let U_P be the corresponding unitary generated by $H_P(t)$. Then

$$\|U - U_P\| \leq \frac{2^n d([U])}{p}, \tag{5}$$

where $\|\cdot\|$ is the operator norm and p is the penalty parameter appearing in the definition of the metric. Thus, by choosing p sufficiently large, say $p = 4^n$, we can ensure that $\|U - U_P\| \leq d([U])/2^n$.

Motivated by lemma 1, we change our aim from accurately synthesizing U to accurately synthesizing U_P. To do this, we break the evolution according to $H_P(t)$ up into many small intervals, each of length Δ. The next lemma shows that evolution according to the time-dependent Hamiltonian $H_P(t)$ over such a small time interval can always be accurately simulated by a constant mean Hamiltonian, which we denote $\bar{H}_P^\Delta$.

Lemma 2: Let U be an n-qubit unitary generated by applying a time-dependent Hamiltonian $H(t)$ satisfying $\|H(t)\| \leq c$ over a time interval $[0, \Delta]$. Then defining the mean Hamiltonian $\bar{H} \equiv \frac{1}{\Delta}\int_0^\Delta dt\, H(t)$ we have:

$$\|U - \exp(-i\bar{H}\Delta)\| \leq 2(e^{c\Delta} - 1 - c\Delta) = O(c^2\Delta^2). \tag{6}$$

To apply this lemma to $H_P(t)$, note that elementary norm inequalities and the observation $F(H_P(t)) \leq 1$ imply that $\|H_P(t)\| \leq \frac{3}{\sqrt{2}} n F(H_P(t)) \leq \frac{3}{\sqrt{2}} n$. Lemma 2 implies that over a time interval Δ we have:

$$\|U_P^\Delta - \exp(-i\bar{H}_P^\Delta \Delta)\| \leq 2\left(e^{3/\sqrt{2}n\Delta} - \left(1 + \frac{3}{\sqrt{2}}n\Delta\right)\right) = O(n^2\Delta^2), \tag{7}$$

where U_P^Δ is the evolution generated by $H_P(t)$ over the time interval Δ, and $\bar{H}_P^\Delta$ is the corresponding mean Hamiltonian.

Our third and final lemma shows that evolution according to a time-independent Hamiltonian H containing only one- and two-body terms can be very accurately simulated using a number of quantum gates that is not too large.

Lemma 3: Suppose H is an n-qubit two-body Hamiltonian whose Pauli expansion coefficients satisfy $|h_\sigma| \leq 1$. Then there exists a unitary U_A, satisfying

$$\|e^{-iH\Delta} - U_A\| \leq c_2 n^4 \Delta^3, \tag{8}$$

that can be synthesized using at most $c_1 n^2/\Delta$ one- and two-qubit gates, where c_1 and c_2 are constants. Note that the average Hamiltonian $\bar{H}_P^\Delta$ provided by Lemma 2 satisfies the assumptions of Lemma 3, since the Pauli expansion coefficients of $H_P(t)$ satisfy $|h_\sigma| \leq 1$ for all times.

To integrate Lemmas 1-3, suppose $H(t)$ is the time-dependent normalized Hamiltonian generating the minimal geodesic of length $d(I, U)$. Let $H_P(t)$ be the corresponding projected Hamiltonian, which generates U_P and satisfies $\|U - U_P\| \leq d(I, U)/2^n$, as guaranteed by Lemma 1, and where we have chosen $p = 4^n$ as the penalty. Now divide the time interval $[0, d(I, U)]$ up into a large number N of time intervals each of length $\Delta = d(I, U)/N$. Let U_P^j be the unitary operation generated by $H_P(t)$ over the jth time interval. Let

U_M^j be the unitary operation generated by the corresponding mean Hamiltonian. Then Lemma 2 implies that:

$$\|U_P^j - U_M^j\| \leq 2(e^{3/\sqrt{2}n\Delta} - (1 + \frac{3}{\sqrt{2}}n\Delta)). \tag{9}$$

Lemma 3 implies that we can synthesize a unitary operation U_A^j using at most $c_1 n^2/\Delta$ one- and two-qubit gates, and satisfying $\|U_M^j - U_A^j\| \leq c_2 n^4 \Delta^3$.

Putting all these results together and applying the triangle inequality repeatedly, we obtain:

$$\begin{aligned}
\|U - U_A\| &\leq \|U - U_P\| + \|U_P - U_A\| && (10)\\
&\leq \frac{d(I,U)}{2^n} + \sum_{j=1}^{N} \|U_P^j - U_A^j\| && (11)\\
&\leq \frac{d(I,U)}{2^n} + \sum_{j=1}^{N} \left(\|U_P^j - U_M^j\| + \|U_M^j - U_A^j\|\right) && (12)\\
&\leq \frac{d(I,U)}{2^n} + 2\frac{d(I,U)}{\Delta}\left(e^{(3/\sqrt{2})n\Delta} - \left(1 + \frac{3}{\sqrt{2}}n\Delta\right)\right) + c_2 d(I,U) n^4 \Delta^2. && (13)
\end{aligned}$$

Provided we choose Δ to scale at most as $1/(n^2 d(I,U))$, we can ensure that the error in our approximation U_A to U is small, while the number of gates scales as $n^6 d(I,U)^3$. Summing up, we have the following theorem:

Theorem: Using $O(n^6 d(I,U)^3)$ one- and two-qubit gates it is possible to synthesize a unitary U_A satisfying $\|U - U_A\| \leq c$, where c is any constant, say $c = 1/10$.

In this paper it is demonstrated that, up to polynomial factors, the optimal way of generating a unitary operation is to move along the minimal geodesic curve connecting I and U. Since the length of such geodesics also provides a lower bound on the minimal number of quantum gates required to generate U. Thus the geometric formulation offers an alternative approach which may suggest efficient quantum algorithms, or provide a way of proving that a given algorithm is indeed optimal.

References

[1] D. Deutsch, Proc. R. Soc. A **400**, 97 (1985); D. Deutsch and R. Jozsa, Proc. R. Soc. A **439**, 553 (1992).

[2] A. Berthiaume and G. Brassard, J. Mod. Optic. **41**, 2521 (1994).

[3] E. Bernstein and U. Vazirani, SIAM J. Comput. **26**, 1411 (1997).

[4] D. R. Simon, SIAM J. Comput. **26**, 1474 (1997).

[5] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).

[6] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[7] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, Fortschritte der Physik **46**, 493 (1998).

[8] C. H. Bennette, E. Bernstein, G. Brassard, and U. Vazirani, SIAM J. Comput. **26**, 1510 (1997).

[9] G. Brassard and P. Høyer, quant-ph/9704027, 1997.

[10] S. Hallgren, Proceedings of the thiry-fourth annual ACM Symposium on Theory of Computing, 2002, pp. 653–658; R. Jozsa, quant-ph/0302134, 2003.

[11] V. I. Arnold, B. A. Khesin, Applied Mathematical Sciences, vol. 125 (Springer, New York, 1998).