Circuit Approximation

U: Operation to be synthesized.

V: Apprximation to U.

Measure of distance: Supremum norm

$$E(U,V) = \max_{|\Psi\rangle} ||(U-V)|\Psi\rangle||,$$

equals the spectral radius

Fact: For any $|\Psi\rangle$ and any set of orthonormal states $\{|a\rangle\}$,

$$\sum_a |P_U(a) - P_V(a)| \leq 2E(U,V)$$

where

$$P_U(a) = |\langle a|U|\Psi\rangle|^2; \;\; P_V(a) = |\langle a|V|\Psi\rangle|^2$$

are the probabilities of measuring state $|a\rangle$.

Approximation (cont'd)

Let U_i be a sequence of transformations and V_i approximations to U_i. Define

$$|\Psi_m\rangle = U_m U_{m-1} \cdots U_1 |\Psi_0\rangle,$$

$$|\tilde{\Psi}_m\rangle = V_m V_{m-1} \cdots V_1 |\Psi_0\rangle.$$

$$\begin{aligned} |\tilde{\Psi}_1\rangle &= V_1|\Psi_0\rangle = |\Psi_1\rangle + (V_1 - U_1)|\Psi_0 \\ &= |\Psi_1\rangle + |E_1\rangle. \end{aligned}$$

$$\begin{aligned} |\tilde{\Psi}_2\rangle &= V_2|\tilde{\Psi}_1\rangle = V_2|\Psi_1\rangle + V_2|E_1\rangle \\ &= |\Psi_2\rangle + |E_2\rangle + V_2|E_1\rangle. \end{aligned}$$

$$\begin{aligned} |\tilde{\Psi}_m\rangle &= V_m|\tilde{\Psi}_{m-1}\rangle \\ &= V_m|\Psi_{m-1}\rangle + V_m|E_{m-1}\rangle + \cdot + V_m \cdots V_2|E_1\rangle. \end{aligned}$$

$$\begin{aligned} ||\,|\tilde{\Psi}_m\rangle - |\Psi_m\rangle|| &\leq ||\,|E_m\rangle|| + \cdots ||V_m \cdots V_1|E_1\rangle|| \\ &= ||\,|E_m\rangle|| + \cdots ||\,|E_1\rangle|| \\ &\leq \sum_{i=1}^{m} E(U_i, V_i). \end{aligned}$$

Thus, error grows linearly with number of transformations if each transformation is approximated with a uniformly bounded error.

Universality of Hadamard and $\pi/8$ Gates

Theorem 1 *Any single qubit transformation U can be approximated to any desired degree of accuracy by Hadamard and $\pi/8$ gates.*

Proof. Recall that the $\pi/8$ gate is given by the matrix

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} = R_z(\pi/4),$$

and since $HZH = X$,

$$HTH = R_x(\pi/4).$$

Composition of these two operations is

$$\begin{aligned}(HTH)T &= R_x(\pi/4)R_z(\pi/4) = e^{-i(\pi/8)Z}e^{-i(\pi/8)X} \\ &= R_{\widehat{n}}(\theta)\end{aligned}$$

where

$$\widehat{n} = (\cos(\pi/8), \sin(\pi/8), \cos(\pi/8))$$

and θ is such that

$$\cos(\theta/2) = \cos^2(\pi/8).$$

It turns out θ is incommensurate with π, so powers of $R_{\widehat{n}}(\theta)$ can be used to generate rotation by any angle about $\widehat{n}$.

Proof of Universality (cont'd)

We also have that

$$T(HTH) = R_{\hat{m}}(\theta)$$

where

$$\hat{m} = (\cos(\pi/8), -\sin(\pi/8), \cos(\pi/8))$$

and $\cos(\theta) = \cos^2(\pi/8)$.

The directions $\hat{m}$ and $\hat{n}$ are non-parallel. All points on the Bloch sphere can be generated by combinations of rotations about $\hat{n}$ and $\hat{m}$.

Universality

Single qubit transformations can be apprxoximated by H and T gates.

Contolled operations, in particular the Toffoli gate, can be generated with the additional help of CNOT.

Thus, CNOT, H, and T gates form a universal set of gates.

Solovay-Kitaev Theorem

Arbitrary single qubit gates can be approximated to an accuracy of ϵ using $O(\log^c(1/\epsilon))$ H and T gates, where c is a constant between 1 and 2.

A circuit contatining m CNOT and single qubit gates can be approximated by $O(m \log^c(m/\epsilon))$ gates from the universal set.

Proof. See Appendix 3 of Nielsen and Chuang.

Existence of Hard Transformations

There are n-qubit transformations that require

$$m = \Omega(\frac{2^n \log(1/\epsilon)}{\log(n)})$$

gates to approximate to an accuracy of ϵ.