2.6.3 Operator Approximation

Let U be an arbitrary single-qubit operator to be synthesized. In general, U cannot be synthesized exactly using a discrete set of gates. So, we seek an approximation V to U.

The measure of approximation is given by the sup norm of $U - V$,

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

where the maximum is over all vectors with unit length. The sup norm equals the spectral radius, i.e., the maximum over the absolute value of the eigenvalues. The justification of this norm is given by the following

Theorem 1 *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 $|a\rangle$.

Proof. Homework assignment.

Thus, as far as the probabilities of measurement outcomes are concerned (and this is the only thing that really matters), the sup norm is an adequate measure of how good the approximation is.

Now, let U_i be a sequence of transformations and V_i approximations to U_i. Define

$$|\Psi_m\rangle = U_m U_{m-1} \cdots U_1 |\Psi_0\rangle,$$
$$|\tilde{\Psi}_m\rangle = V_m V_{m-1} \cdots V_1 |\Psi_0\rangle.$$

Then,

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

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

More generally,

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

In the above, the error terms are defined in general by

$$|E_i\rangle = (V_i - U_i)|\Psi_i\rangle.$$

Now, we notice that

$$\begin{aligned} ||\,|\tilde{\Psi}_m\rangle - |\Psi_m\rangle|| &\leq ||\,|E_m\rangle|| + \cdots + ||V_m \cdots V_1|E_1\rangle|| \\ &= ||\,|E_m\rangle|| + \cdots + ||\,|E_1\rangle|| \end{aligned}$$

which follows by the unitarity of the transformations V_i. Next, we observe that

$$|| \, |E_i\rangle|| = ||(V_i - U_i)|\Psi_i\rangle|| \leq E(U_i, V_i)$$

since $|\Psi_i\rangle$ are normalized vectors. Thus,

$$|| \, |\tilde{\Psi}_m\rangle - |\Psi_m\rangle|| \leq \sum_{i=1}^{m} E(U_i, V_i),$$

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

2.6.4 Universality of Hadamard and $\pi/8$ Gates

Theorem 2 *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

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

where

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

and θ is such that

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

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

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 successive rotations about $\hat{n}$ and $\hat{m}$, i.e., by a sequence $R_{\hat{n}}(\theta_1)R_{\hat{m}}(\phi_1)R_{\hat{n}}(\theta_2)R_{\hat{m}}(\phi_2)\cdots R_{\hat{n}}(\theta_t)R_{\hat{m}}(\phi_t)$. This completes the proof.

This also completes the proof of universality that we set out to prove in this section. To summarize, we have shown that 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.

2.6.5 Complementary remarks

Solovay and Kitaev, in independent work, proved that single-qubit transformations can be approximated using H and T gates in a more efficient manner than we have been able to show above.

Theorem 3 *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.*

Proof. See Appendix 3 of Nielsen and Chuang.

Solovay-Kitaev result is the best possible result in that it is known that there exist n-qubit transformations that require

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

gates to approximate to an accuracy of ϵ.