Proof

Since U is unitary, the rows and columns of U are orthonormal, from which it follows that there exist real numbers α, β, γ,and δ such that

$$U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2} \end{bmatrix}. \tag{4.12}$$

Equation (4.11) now follows immediately from the definition of the rotation matrices and matrix multiplication. □

Exercise 4.9: Explain why any single qubit unitary operator may be written in the form (4.12).

Exercise 4.10: (**X-Y decomposition of rotations**) Give a decomposition analogous to Theorem 4.1 but using R_x instead of R_z.

Exercise 4.11: Suppose $\hat{m}$ and $\hat{n}$ are non-parallel real unit vectors in three dimensions. Show that an arbitrary single qubit unitary U may be written as

$$U = e^{i\alpha}R_{\hat{n}}(\beta_1)R_{\hat{m}}(\gamma_1)R_{\hat{n}}(\beta_2)R_{\hat{m}}(\gamma_2)\dots, \tag{4.13}$$

for appropriate choices of α and β_k, γ_k.

The utility of Theorem 4.1 lies in the following mysterious looking corollary, which is the key to the construction of controlled multi-qubit unitary operations, as explained in the next section.

Corollary 4.2: Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha}AXBXC$, where α is some overall phase factor.

Proof

In the notation of Theorem 4.1, set $A \equiv R_z(\beta)R_y(\gamma/2)$, $B \equiv R_y(-\gamma/2)R_z(-(\delta+\beta)/2)$ and $C \equiv R_z((\delta-\beta)/2)$. Note that

$$ABC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) = I. \tag{4.14}$$

Since $X^2 = I$, and using Exercise 4.7, we see that

$$XBX = XR_y\left(-\frac{\gamma}{2}\right)XXR_z\left(-\frac{\delta+\beta}{2}\right)X = R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right). \tag{4.15}$$

Thus

$$AXBXC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) \tag{4.16}$$

$$= R_z(\beta)R_y(\gamma)R_z(\delta). \tag{4.17}$$

Thus $U = e^{i\alpha}AXBXC$ and $ABC = I$, as required. □

Exercise 4.12: Give A, B, C, and α for the Hadamard gate.