Controlled Unitary Gates

Andreas Klappenecker

Lemma 1 *A unitary matrix $U \in \mathcal{U}(2)$ can be expressed in the form*

$$U = e^{ia} \begin{pmatrix} e^{-ib} & 0 \\ 0 & e^{ib} \end{pmatrix} \begin{pmatrix} \cos c & -\sin c \\ \sin c & \cos c \end{pmatrix} \begin{pmatrix} e^{-id} & 0 \\ 0 & e^{id} \end{pmatrix},$$

for some real numbers $a, b, c,$ and d.

Proof. We can write U in the form $U = e^{ia}V$, where V is some unitary matrix with determinant 1. The matrix V has to be of the form $V = \left(\begin{smallmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{smallmatrix}\right)$. Indeed, the columns of a unitary matrix are orthogonal, hence the right column of V has to be a multiple of $(-\overline{\beta}, \overline{\alpha})^t$; and the determinant constraint forces V to be of the given form. We can write α and β in the form $\alpha = e^{ih}\cos c$ and $\beta = e^{ik}\sin c$ for some real numbers h, k, c, because α and β satisfy $|\alpha|^2 + |\beta|^2 = 1$; it follows that

$$V = \begin{pmatrix} e^{ih}\cos c & -e^{ik}\sin c \\ e^{-ik}\sin c & e^{-ih}\cos c \end{pmatrix}.$$

We can find real numbers b and d satisfying $h = -d - b$ and $k = d - b$, hence

$$V = \begin{pmatrix} e^{-i(b+d)}\cos c & -e^{i(d-b)}\sin c \\ e^{i(b-d)}\sin c & e^{i(b+d)}\cos c \end{pmatrix} = \begin{pmatrix} e^{-ib} & 0 \\ 0 & e^{ib} \end{pmatrix} \begin{pmatrix} \cos c & -\sin c \\ \sin c & \cos c \end{pmatrix} \begin{pmatrix} e^{-id} & 0 \\ 0 & e^{id} \end{pmatrix},$$

which proves the claim. ∎

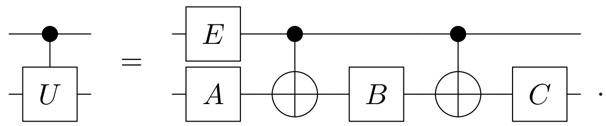
Let us denote by $S(b)$ and $R(c)$ the matrices

$$S(b) = \begin{pmatrix} e^{-ib} & 0 \\ 0 & e^{ib} \end{pmatrix} \quad \text{and} \quad R(c) = \begin{pmatrix} \cos c & -\sin c \\ \sin c & \cos c \end{pmatrix}.$$

The statement of the previous lemma is that a unitary matrix can be written in the form $U = e^{ia}S(b)R(c)S(d)$ for some $a, b, c, d \in \mathbf{R}$. Notice that

$$XR(c)X = R(-c) \quad \text{and} \quad XS(b)X = S(-b).$$

Theorem 1 *For each unitary matrix $U \in \mathcal{U}(2)$ there exist matrices A, B, C, and E in $\mathcal{U}(2)$ such that*



Proof. If $U = e^{ia} S(b) R(c) S(d)$, choosing the matrices

$$C = S(b)R(c/2), \qquad B = R(-c/2)S(-(d+b)/2),$$
$$A = S((d-b)/2), \qquad E = \mathrm{diag}(1, e^{ia}),$$

yields the desired result. Indeed, we have $CBA = \mathbf{1}$. Therefore, the circuit on the right hand side yields on input of $|00\rangle$ and $|01\rangle$ the same result as the controlled-U gate. Using $X^2 = \mathbf{1}$, we obtain for $CXBXA$ the expression

$$CXBXA = \underbrace{S(b)R(c/2)}_{C}\ X\ \underbrace{R(-c/2)XXS(-(d+b)/2)}_{B}\ X\ \underbrace{S((d-b)/2)}_{A},$$

which simplifies to $CXBXA = S(b)R(c/2)R(c/2)S((d+b)/2)S((d-b)/2) = S(b)R(c)S(d)$. It follows that $|1\rangle \otimes |\psi\rangle$ is transformed by the circuit on the right hand side to

$$e^{ia}|1\rangle \otimes S(b)R(c)S(d)|\psi\rangle = |1\rangle \otimes U|\psi\rangle,$$

which coincides with the action of the controlled-U gate. ■