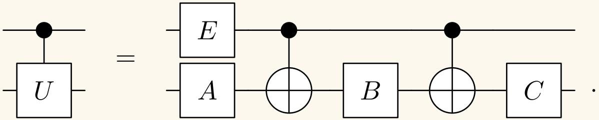
Controlled Unitary Gates

Andreas Klappenecker

Texas A&M University

Theorem

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



Dramatis Personae

Phase shift matrix

$$S(b) = \begin{pmatrix} e^{-ib} & 0 \\ 0 & e^{ib} \end{pmatrix}$$

Rotation matrix

$$R(c) = \begin{pmatrix} \cos c & -\sin c \\ \sin c & \cos c \end{pmatrix}.$$

Lemma

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

$$U = e^{ia} \begin{pmatrix} e^{-ib} & 0 \\ 0 & e^{ib} \end{pmatrix} \begin{pmatrix} \cos c & -\sin c \\ \sin c & \cos c \end{pmatrix} \begin{pmatrix} e^{-id} & 0 \\ 0 & e^{id} \end{pmatrix}$$
$$= e^{ia} S(b) R(c) S(d),$$

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

Proof of the Lemma (1/2)

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

$$V = \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix}.$$

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.

Proof of the Lemma (2/2)

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

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

which proves the claim.

Key Observation

Let

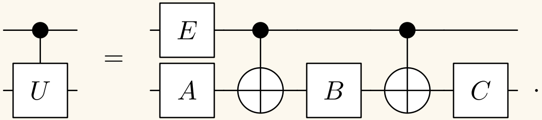
$$S(b) = \begin{pmatrix} e^{-ib} & 0 \\ 0 & e^{ib} \end{pmatrix} \quad \text{and} \quad R(c) = \begin{pmatrix} \cos c & -\sin c \\ \sin c & \cos c \end{pmatrix}.$$

Then

$$\begin{aligned} S(-b) &= XS(b)X, \\ R(-c) &= XR(c)X. \end{aligned}$$

Theorem

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



Proof of the Theorem (1/3)

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

$$E = \mathrm{diag}(1, e^{ia}),$$

$$\begin{aligned} C &= S(b)R(c/2), \\ B &= R(-c/2)S(-(d+b)/2), \\ A &= S((d-b)/2), \end{aligned}$$

yields the desired result. Indeed, we have $CBA = I$. Therefore, the circuit on the right hand side yields on input of $|00\rangle$ and $|01\rangle$ the same result as $\Lambda_{0;1}(U)$.

Using $X^2 = I$, 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

$$\begin{aligned} CXBXA &= S(b)R(c/2)R(c/2)S((d+b)/2)S((d-b)/2) \\ &= S(b)R(c)S(d). \end{aligned}$$

Proof of the Theorem (3/3)

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 $\Lambda_{0;1}(U)$.

Done!