Controlled Quantum Gates

Andreas Klappenecker
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

\[ U = EBA. \]
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 $V = \left(\begin{array}{cc} \alpha & -\beta \\ \beta & \alpha \end{array}\right)$. Indeed, the columns of a unitary matrix are orthogonal, hence the right column of $V$ has to be a multiple of $(-\beta, \alpha)^t$; and the determinant constraint forces $V$ to be of the given form. We can write $\alpha$ and $\beta$ in the form $\alpha = e^{ih}\cos c$ and $\beta = e^{-ik}\sin c$ for some real numbers $h, k, c$, because $\alpha$ and $\beta$ 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

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

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 $a, b, c, d \in \mathbb{R}$. Notice that

$XR(c)X = R(-c)$ and $XS(b)X = S(-b)$. 

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

![Circuit Diagram]

Thursday, September 25, 2014
Proof. If $U = e^{ia}S(b)R(c)S(d)$, choosing the matrices

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

yields the desired result. Indeed, we have $CBA = 1$. 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 $X^2 = 1$, we obtain for $CXBXA$ the expression

$$CXBXA = S(b)R(c/2) X R(-c/2)X X S(-(d + b)/2) X S((d - b)/2),$$

with $C$, $B$, and $A$. 

Thursday, September 25, 2014
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 $\Lambda_{0;1}(U)$. ■