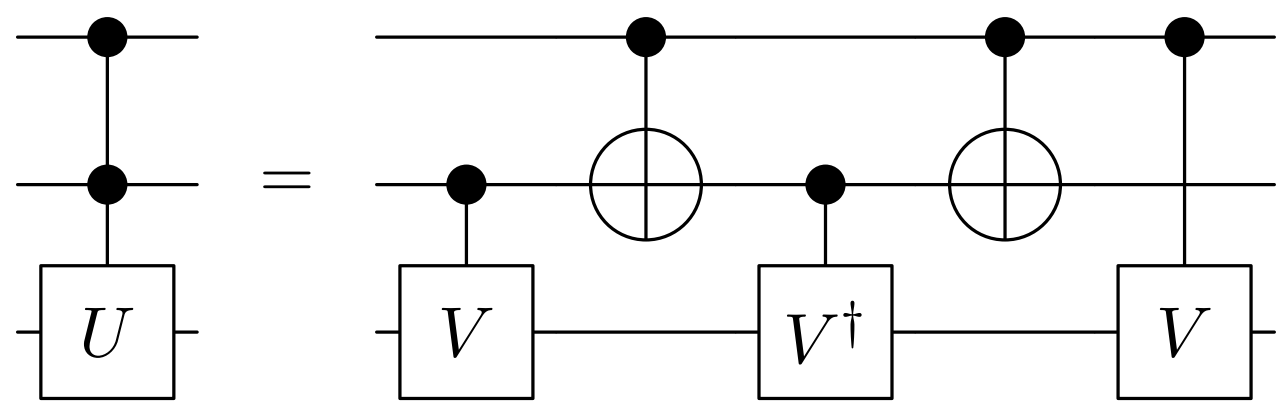
Quantum Gates with Multiple Controls

Andreas Klappenecker

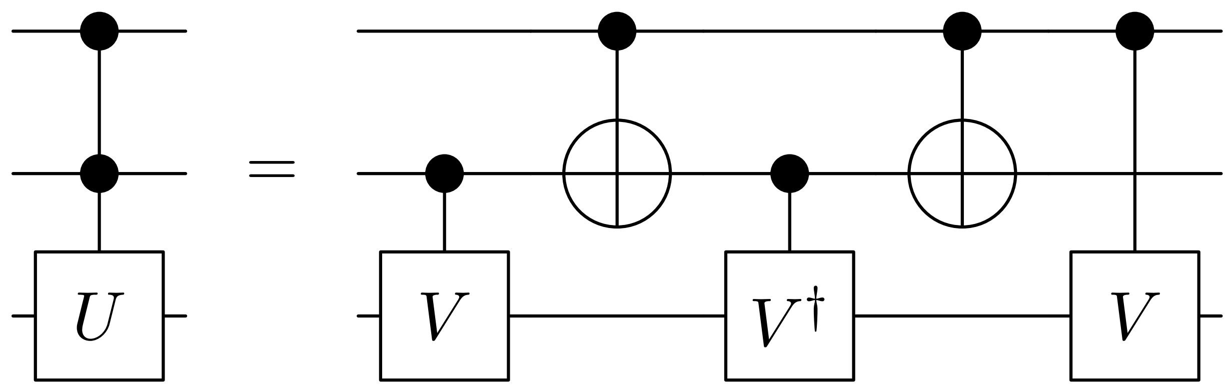
Goal

Theorem 2 *A unitary gate controlled by two control bits can be expressed in terms of singly controlled quantum gates as follows:*



where V *is a* 2×2 *unitary matrix such that* $U = V^2$.

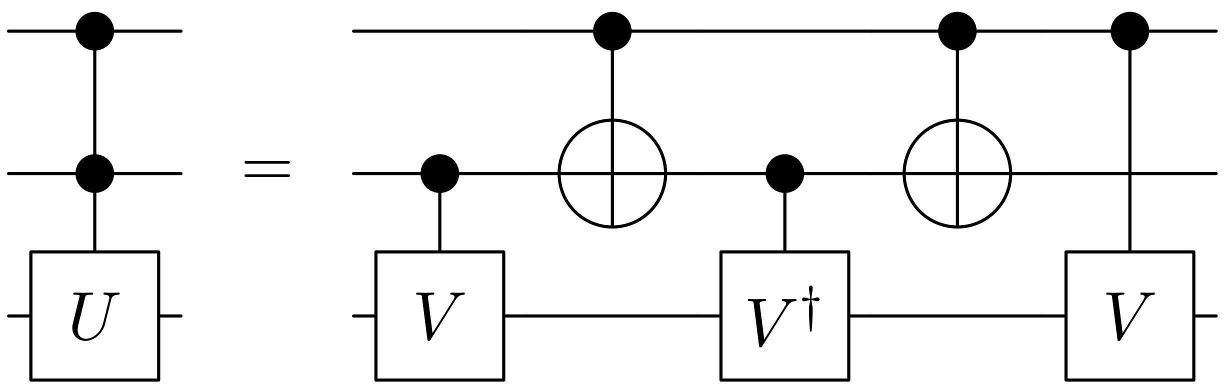
Proof



Proof. The gate on the left hand side acts on basis states in the following way:

$$\begin{aligned}
|00\rangle \otimes |x\rangle &\quad\mapsto\quad |00\rangle \otimes |x\rangle \\
|01\rangle \otimes |x\rangle &\quad\mapsto\quad |01\rangle \otimes |x\rangle \\
|10\rangle \otimes |x\rangle &\quad\mapsto\quad |10\rangle \otimes |x\rangle \\
|11\rangle \otimes |x\rangle &\quad\mapsto\quad |11\rangle \otimes U|x\rangle
\end{aligned}$$

Proof



for $x \in \{0,1\}$. The five gates in circuit on the right hand side act on the basis states as follows:

$$
\begin{aligned}
|00\rangle \otimes |x\rangle &\mapsto |00\rangle \otimes |x\rangle \mapsto |00\rangle \otimes |x\rangle \mapsto |00\rangle \otimes |x\rangle \mapsto |00\rangle \otimes |x\rangle \mapsto |00\rangle \otimes |x\rangle \\
|01\rangle \otimes |x\rangle &\mapsto |01\rangle \otimes V|x\rangle \mapsto |01\rangle \otimes V|x\rangle \mapsto |01\rangle \otimes V^\dagger V|x\rangle \mapsto |01\rangle \otimes |x\rangle \mapsto |01\rangle \otimes |x\rangle \\
|10\rangle \otimes |x\rangle &\mapsto |10\rangle \otimes |x\rangle \mapsto |11\rangle \otimes |x\rangle \mapsto |11\rangle \otimes V^\dagger|x\rangle \mapsto |10\rangle \otimes V^\dagger|x\rangle \mapsto |10\rangle \otimes |x\rangle \\
|11\rangle \otimes |x\rangle &\mapsto |11\rangle \otimes V|x\rangle \mapsto |10\rangle \otimes V|x\rangle \mapsto |10\rangle \otimes V|x\rangle \mapsto |11\rangle \otimes V|x\rangle \mapsto |11\rangle \otimes V^2|x\rangle
\end{aligned}
$$

Loose Ends...

It remains to show that for a given 2x2 unitary matrix U, there really exists a unitary 2x2 matrix V that is the "square-root" of U.

Convenient Squareroot Lemma

Lemma 2 *Let U be a unitary 2×2 matrix that is not a multiple of the identity matrix I. Then*

$$V = \frac{1}{\sqrt{\operatorname{tr} U \pm 2\sqrt{\det U}}}(U \pm \sqrt{\det U}\, I)$$

is a unitary matrix satisfying $U = V^2$.

Proof of Squareroot Lemma

Proof. Let us first show that V is a well-defined matrix. Seeking a contradiction, we assume that $\operatorname{tr} U \pm 2\sqrt{\det U} = 0$. Let λ_1, λ_2 be the eigenvalues of U. We have $\det U = \lambda_1\lambda_2$ and $\operatorname{tr} U = \lambda_1 + \lambda_2$. It follows that

$$\lambda_1 + \lambda_2 = \operatorname{tr} U = \mp 2\sqrt{\det U} = 2\sqrt{\lambda_1\lambda_2}.$$

Since U is unitary, $|\lambda_1| = |\lambda_2| = 1$. Therefore, $|\lambda_1 + \lambda_2| = 2|\sqrt{\lambda_1\lambda_2}| = 2$. This means that the triangle inequality $|\lambda_1 + \lambda_2| \leq 2 = |\lambda_1| + |\lambda_2|$ holds with equality, which implies that $\lambda_1 = r\lambda_2$ for some positive real number r. Since $|\lambda_1| = |\lambda_2| = 1$, we have $|r| = r = 1$, which means that the eigenvalues λ_1 and λ_2 must be the same. This would imply that U is a multiple of the identity, contradicting our hypothesis. Therefore, $\operatorname{tr} U \pm 2\sqrt{\det U}$ is nonzero and the matrix V is well-defined.

Proof of Squareroot Lemma

By the Cayley-Hamilton theorem, the unitary 2×2 matrix U satisfies its characteristic equation $U^2 + (\operatorname{tr} U)U + (\det U)I = 0$; thus,

$$(\operatorname{tr} U)U = U^2 + (\det U)I.$$

Using this relation, we obtain

$$\begin{aligned} V^2 &= \frac{1}{\operatorname{tr} U \pm 2\sqrt{\det U}}(U \pm \sqrt{\det U}\, I)^2 \\ &= \frac{1}{\operatorname{tr} U \pm \sqrt{\det U}}(U^2 + (\det U)I \pm 2\sqrt{\det U}\, U) \\ &= \frac{1}{\operatorname{tr} U \pm 2\sqrt{\det U}}(\operatorname{tr} U \pm 2\sqrt{\det U})U = U \end{aligned}$$

Proof of Squareroot Lemma

It remains to show that V is a unitary matrix. Recall that the unitary matrix U can be diagonalized by a base change with some unitary matrix P, say $\mathrm{diag}(\lambda_1, \lambda_2) = PUP^\dagger$. Then P diagonalizes V as well, so $PVP^\dagger = \mathrm{diag}(a, b)$. Since

$$\mathrm{diag}(\lambda_1, \lambda_2) = PUP^\dagger = (PVP^\dagger)(PVP^\dagger) = \mathrm{diag}(a^2, b^2),$$

it follows that $a = \sqrt{\lambda_1}$ and $b = \sqrt{\lambda_2}$ are complex numbers of absolute value 1. Therefore, $\mathrm{diag}(a, b)$ is a unitary matrix and we can conclude that $V = P^\dagger \mathrm{diag}(a, b) P$ is a unitary matrix as well. ■

Conclusions

A quantum gate with 2 control bits can be realized with quantum gates that have just a single control bit.

More generally, a quantum gate with m control bits can be realized with quantum gates that have m-1 control bits.

In summary, a quantum gates with multiple controls can be realized by quantum gates that have just single controls, and those can be realized by single quantum bit gates and controlled-not gates.