Quantum Gates with Multiple Controls
Andreas Klappenecker
Theorem 2 A unitary gate controlled by two control bits can be expressed in terms of singly controlled quantum gates as follows:

$$\begin{bmatrix} U \\ V \end{bmatrix} = \begin{bmatrix} V & V \dagger \\ \end{bmatrix}$$

where $V$ is a $2 \times 2$ unitary matrix such that $U = V^2$. 
Proof. The gate on the left hand side acts on basis states in the following way:

\[
\begin{align*}
|00\rangle \otimes |x\rangle &\mapsto |00\rangle \otimes |x\rangle \\
|01\rangle \otimes |x\rangle &\mapsto |01\rangle \otimes |x\rangle \\
|10\rangle \otimes |x\rangle &\mapsto |10\rangle \otimes |x\rangle \\
|11\rangle \otimes |x\rangle &\mapsto |11\rangle \otimes U|x\rangle 
\end{align*}
\]
Proof

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

\[
\begin{align*}
|00\rangle \otimes |x\rangle &\rightarrow |00\rangle \otimes |x\rangle &\rightarrow |00\rangle \otimes |x\rangle &\rightarrow |00\rangle \otimes |x\rangle &\rightarrow |00\rangle \otimes |x\rangle \\
|01\rangle \otimes |x\rangle &\rightarrow |01\rangle \otimes V|x\rangle &\rightarrow |01\rangle \otimes V|x\rangle &\rightarrow |01\rangle \otimes V^\dagger|x\rangle &\rightarrow |01\rangle \otimes |x\rangle \\
|10\rangle \otimes |x\rangle &\rightarrow |10\rangle \otimes |x\rangle &\rightarrow |10\rangle \otimes V^\dagger|x\rangle &\rightarrow |10\rangle \otimes V^\dagger|x\rangle &\rightarrow |10\rangle \otimes |x\rangle \\
|11\rangle \otimes |x\rangle &\rightarrow |11\rangle \otimes V|x\rangle &\rightarrow |10\rangle \otimes V|x\rangle &\rightarrow |10\rangle \otimes V|x\rangle &\rightarrow |11\rangle \otimes V^2|x\rangle
\end{align*}
\]
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.
Lemma 2 Let $U$ be a unitary $2 \times 2$ matrix that is not a multiple of the identity matrix $I$. Then

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

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 $\text{tr} U \pm 2\sqrt{\det U} = 0$. Let $\lambda_1, \lambda_2$ be the eigenvalues of $U$. We have $\det U = \lambda_1\lambda_2$ and $\text{tr} U = \lambda_1 + \lambda_2$. It follows that

$$\lambda_1 + \lambda_2 = \text{tr} U = \mp 2\sqrt{\det U} = 2\sqrt[2]{\lambda_1\lambda_2}.$$

Since $U$ is unitary, $|\lambda_1| = |\lambda_2| = 1$. Therefore, $|\lambda_1 + \lambda_2| = 2|\sqrt[2]{\lambda_1\lambda_2}| = 2$. 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 $\lambda_1$ and $\lambda_2$ must be the same. This would imply that $U$ is a multiple of the identity, contradicting our hypothesis. Therefore, $\text{tr} U \pm 2\sqrt{\det U}$ is nonzero and the matrix $V$ is well-defined.
Proof of Square Root Lemma

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

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

Using this relation, we obtain

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

$$= \frac{1}{\text{tr } U \pm \sqrt{\det U}} (U^2 + (\det U)I \pm 2\sqrt{\det U} U)$$

$$= \frac{1}{\text{tr } U \pm 2\sqrt{\det U}} (\text{tr } U \pm 2\sqrt{\det U}) U = U$$
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 $\text{diag}(\lambda_1, \lambda_2) = PUP^\dagger$. Then $P$ diagonalizes $V$ as well, so $PVP^\dagger = \text{diag}(a, b)$. Since

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

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