Multi-qubit gates

With only single-qubit gates, we could never produce **entangled** states like $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ since

$$(U \otimes V)|\psi\rangle \otimes |\varphi\rangle = U|\psi\rangle \otimes V|\varphi\rangle$$

Multi-qubit gates are needed to generate entanglement and access the full power of QC

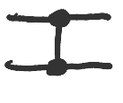
Recall:

A state of n bits is a vector in $\mathbb{C}^{2^n}$

An n-qubit gate is thus a unitary $U: \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$

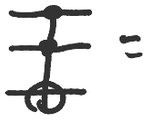
Ex. Important multi-qubit unitaries include

CNOT =  $= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

CZ =  $= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$

SWAP =  $= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

(also written )

Toffoli = 

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Intuitive view ($x, y, z \in \mathbb{F}_2$)

$\text{CNOT}|x\rangle|y\rangle = |x\rangle|x \oplus y\rangle$

$\text{CZ}|x\rangle|y\rangle = (-1)^{xy}|x\rangle|y\rangle$

$\text{SWAP}|x\rangle|y\rangle = |y\rangle|x\rangle$

$\text{Toff}|x\rangle|y\rangle|z\rangle = |x\rangle|y\rangle|z \oplus xy\rangle$

Controlled gates

CNOT, CZ, Toffoli are examples of **controlled** gates. Controlled gates apply a unitary U on the **target(s)** if and only if the computational basis state of the **control** is $|1\rangle$

Ex.

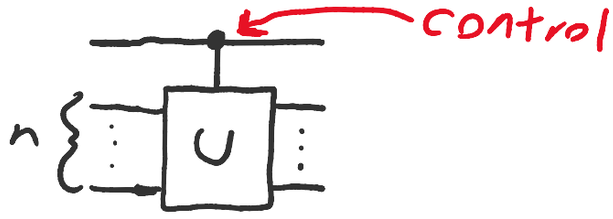
Given an n-qubit unitary U, the controlled-U gate is an $n+1$-qubit gate that sends

$$|0\rangle|\psi\rangle \longmapsto |0\rangle|\psi\rangle$$

$$|1\rangle|\psi\rangle \longmapsto |1\rangle(U|\psi\rangle)$$

$$(\alpha|0\rangle + \beta|1\rangle)|\psi\rangle \longmapsto \alpha|0\rangle|\psi\rangle + \beta|1\rangle(U|\psi\rangle)$$

The controlled-U gate is written



The CNOT gate is a controlled-X gate

CZ gate is a controlled-Z gate

Ex. The CNOT gate is entangling

Let $|\psi\rangle = |+\rangle|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

Then $\text{CNOT}|\psi\rangle = \frac{1}{\sqrt{2}}(\text{CNOT}|00\rangle + \text{CNOT}|10\rangle)$

$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$= |\Phi\rangle$

Matrix of a controlled gate

Given a unitary U, the controlled-U gate can be written as

$$CU = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

Ex. // CNOT

$$CX = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes I + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes X$$

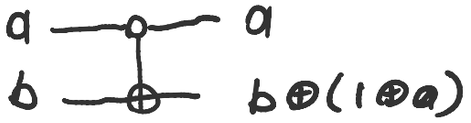
$$= \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

(Negative controls)

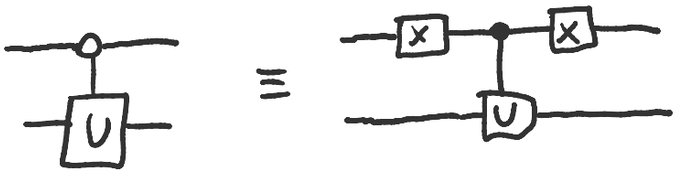
We sometimes want to apply a gate if and only if the control is in the 0 state. We call this a negative control and denote it by.

Ex.

Negating the control on a CNOT flips the target bit if and only if the control is 0



Fact

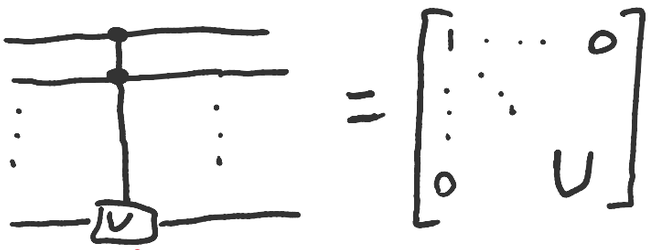


Multiply-controlled gates

Observe that the Toffoli gate is a controlled-CNOT gate:

$$\text{Toffoli}: |0\rangle|y\rangle|z\rangle \longmapsto |0\rangle|y\rangle|z\rangle$$
$$|1\rangle|y\rangle|z\rangle \longmapsto |1\rangle|y\rangle|z\oplus y\rangle = |i\rangle(\text{CNOT}|y\rangle|z\rangle)$$

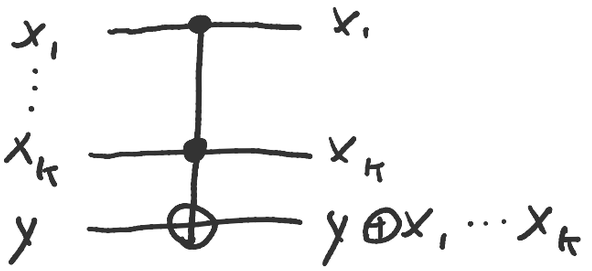
Controlled-controlled gates like the Toffoli gate are called multi-controlled gates. We draw each control with a dot:



↖ U is applied if and only if each control is 1

(Multiply-controlled Toffolis)

An important multiply-controlled gate is the multiply-controlled X gate:



multiply-controlled Toffoli ↓

Such a gate is often called an MCT gate and computes the product of its k controls

$$|x_1 \cdots x_k\rangle|y\rangle \longmapsto |x_1 \cdots x_k\rangle|y \oplus x_1 \cdots x_k\rangle$$

concatenation ← product

It's confusing, I know

Construction of controlled gates

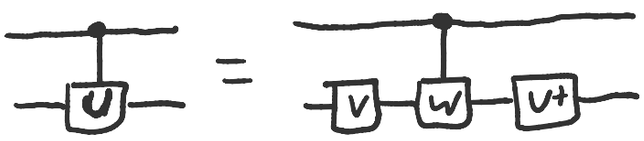
The construction of (multi-)controlled gates is another fundamental problem in Quantum compilation.

Barenco et. al
Elementary gates for quantum computation
lays the foundation for this problem

Our first goal is to show that *multi-controlled gates* may be implemented using only *CNOT & single-qubit gates*

(*Basic Construction of controlled gates*)

Observe that if $U = V^\dagger W V$, then

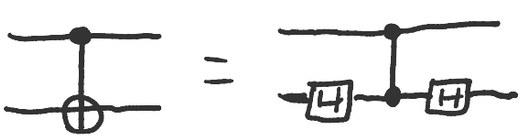


In particular, the rhs sends

$$|0\rangle|\psi\rangle \longmapsto |0\rangle(V^\dagger V|\psi\rangle) = |0\rangle|\psi\rangle$$
$$|1\rangle|\psi\rangle \longmapsto |0\rangle(V^\dagger W V|\psi\rangle) = |0\rangle(U|\psi\rangle)$$

Ex.

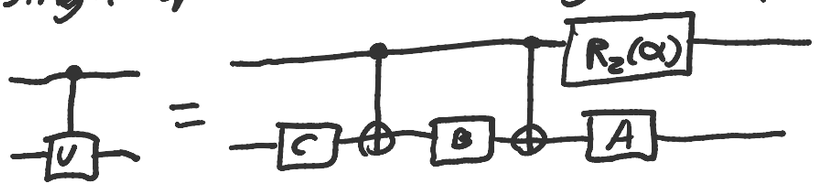
Recall that $X = HZH$. We can construct the controlled-X (CNOT) gate as



Universal 1-control gate construction

Prop.

For any 1-qubit unitary U, CU can be constructed from single-qubit and CNOT gates. Specifically,



For some α, A, B, C satisfying $ABC = I$ and $U = e^{i\alpha} AXBXC$

Pf.

Observe that the above circuit sends

$$|0\rangle|\psi\rangle \longmapsto (R_z(\alpha)|0\rangle) \otimes (ABC|\psi\rangle) = e^{-i\alpha/2}|0\rangle|\psi\rangle$$
$$|1\rangle|\psi\rangle \longmapsto (R_z(\alpha)|1\rangle) \otimes (AXBXC|\psi\rangle) = e^{i\alpha/2}|1\rangle(U|\psi\rangle)$$

$\therefore$ equal up to a global phase of $e^{i\alpha/2}$

Now let $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$. Then

$$A = R_z(\beta) R_y(\gamma/2), \quad B = R_y(-\gamma/2) R_z\left(-\frac{\delta+\beta}{2}\right), \quad C = R_z\left(\frac{\delta-\beta}{2}\right)$$

satisfies the above constraints

Ex.

$T^2 = S$

Note that $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = e^{i\pi/4} \begin{bmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

$$= e^{i\pi/4} R_z(0) R_y(0) R_z(\pi/2)$$

Setting $A = R_z(0) R_y(0)$

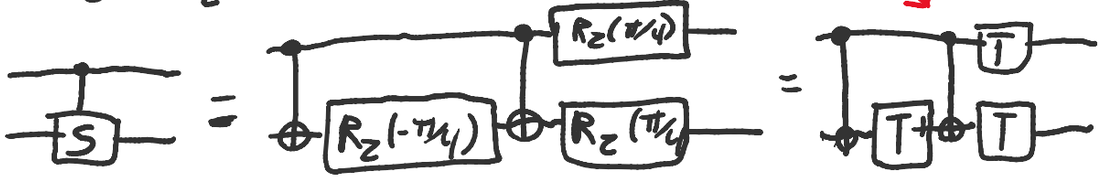
$B = R_y(0) R_z(-\pi/4)$

$C = R_z(\pi/4)$

up to global phase $e^{i\pi/8}$

correct global phase

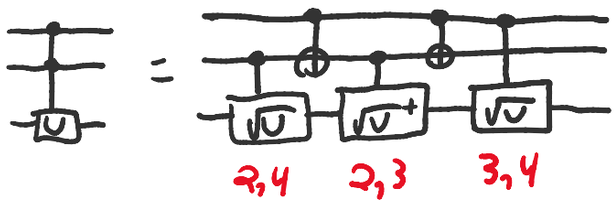
we get



Construction of 2-control gates

Prop. over SQ & CNOT

For any 1-qubit unitary V, CCU can be constructed as



Pf.

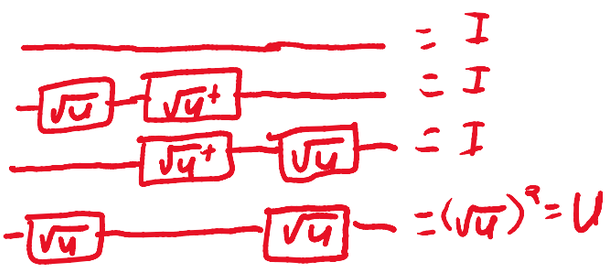
We have 4 cases:

① 00 $= I$

② 01 $= I$

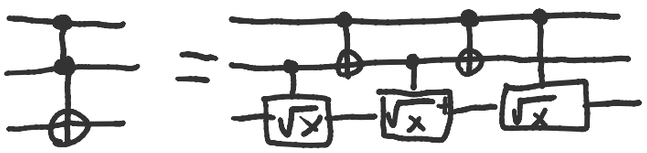
③ 10 $= I$

④ 11 $= (\sqrt{U})^2 = U$

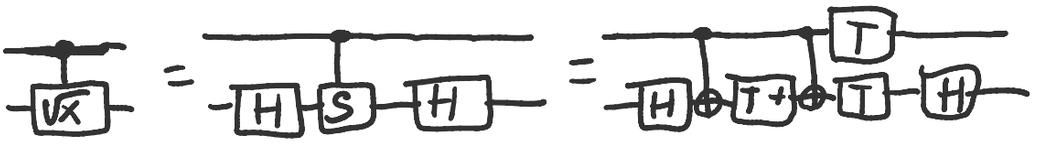


Ex.

Recall that the Toffoli gate is an X gate with two controls. In classical computing, the Toffoli gate can not be constructed (reversibly) by a circuit of < 3 bit gates. Quantumly, by the above



Note also that $\sqrt{X} = S$ and $\sqrt{S} = T$, so



Thm. For the Toffoli gate,

- 5 two-qubit gates is minimal
- 7 T-gates is minimal over $\{CNOT, H, T\}$

Construction of multi-controlled gates

Multiply-controlled gates are used in most top-down universal constructions (and often in algorithms). We now look at general techniques for decomposing into fewer controls.

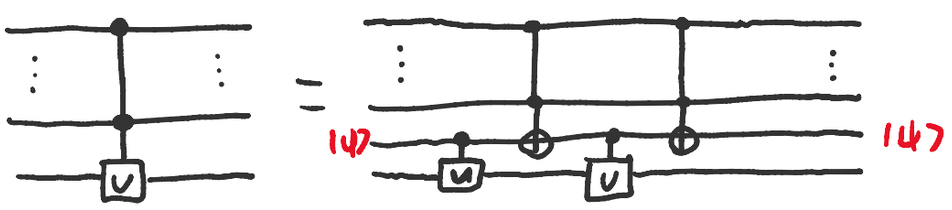
(Decomposition with 1 ancilla)

Note that $C^k U$ ("k-controlled U") "fires" if and only if all k-controls are 1.

$$x_1 = 1 \wedge x_2 = 1 \wedge \cdots \wedge x_k = 1 \iff x_1 x_2 \cdots x_k = 1$$

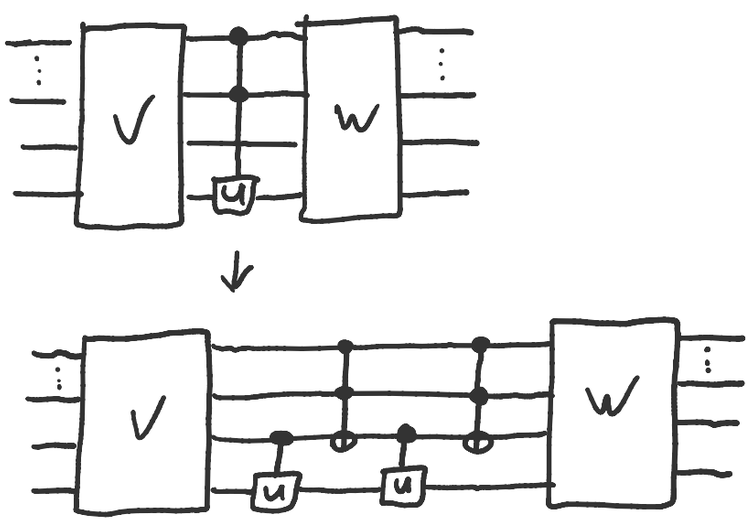
(Decomposition with 1 ancilla in an unknown state)

If $U^2 = I$, then



The ancilla here is called dirty and can in fact be a qubit used elsewhere in the circuit!

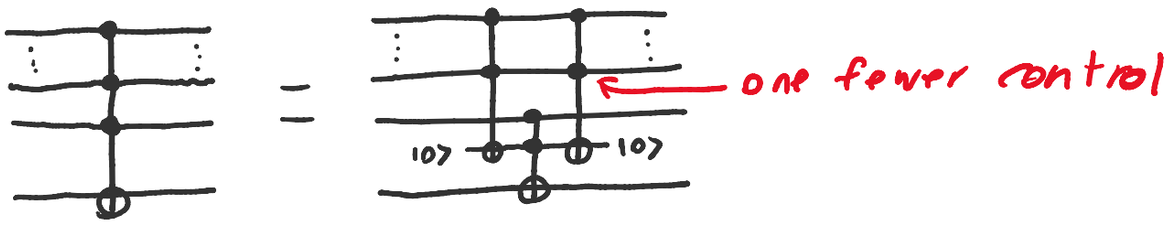
E.g.



Multi-controlled Toffoli gates

The previous constructions didn't **reduce** the number of controls, just **shifted** them to multi-controlled Toffoli **(MCT)** gates. To get things down to single-qubit and CNOT we need a construction which reduces controls

(MCT with linear clean ancillas)



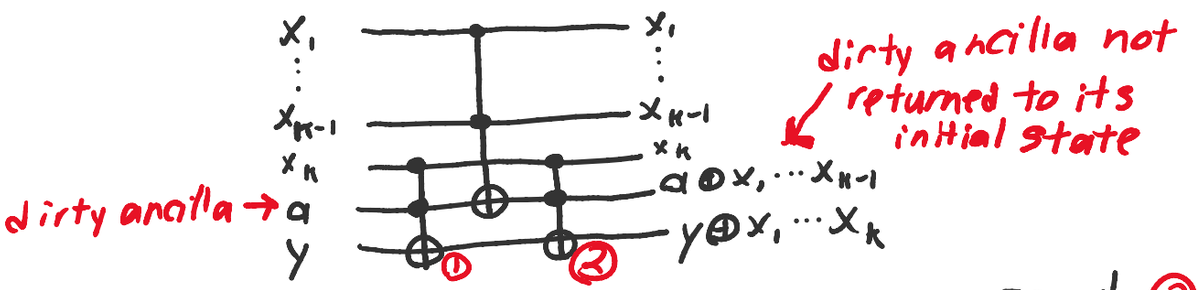
Prop.

A k-control Toffoli can be implemented with

- $k-2$ **clean** ancillas
- $2(k-2)+1$ Toffoli gates

(MCT with linear dirty ancillas)

A similar result holds for **dirty** ancillas, but its construction is slightly trickier. First observe:

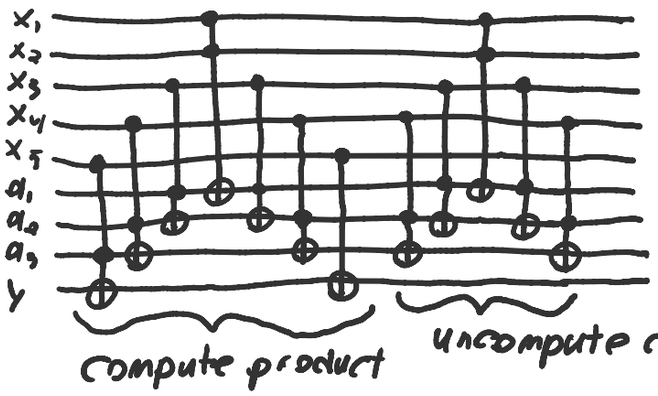


This is because at ① we have $y \oplus a x_k$, so at ②

$$y \oplus a x_k \oplus (a \oplus x_1 \cdots x_{k-1}) x_k = y \oplus x_1 \cdots x_k$$

We can recursively apply this construction, giving $k-2$ dirty ancillas and $2(k-2)+1$ Toffoli gates, but this will leave the $k-2$ dirty ancillas in an **unclean** state

To return the ancillas to their initial state, we need to clean them by reversing the intermediate k-1 control Toffoli computation. The circuit for 5 controls is

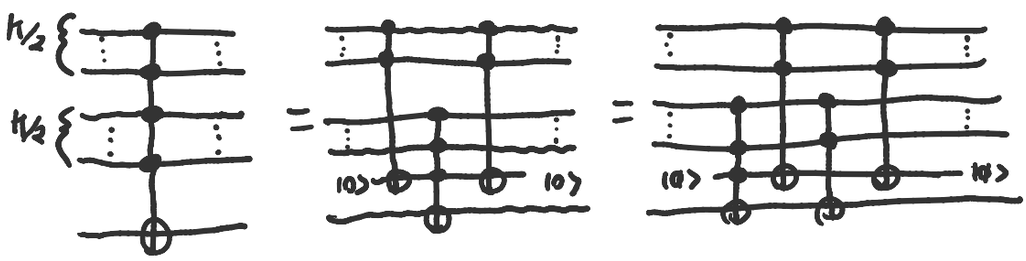


Prop

A k-control MCT gate can be implemented with
- k-2 dirty ancillas
- $2(k-2)+1 + 2(k-3)+1$ Toffoli gates

(MCT gate with a single ancilla)

Finally we show that an MCT gate may be implemented with just 1 ancilla (dirty or clean)



This decomposes a k-control MCT into k/2 and k/2 +1 control MCT gates. We can then use the other k/2-1 bits as dirty ancillas to apply the previous linear simulation!

Prop. A k-control MCT gate can be implemented with
- 1 ancilla (dirty or clean)
- $O(n)$ Toffoli gates

A note about efficiency

In quantum computing, the constants matter. Physically realizable circuit depths double in years, and error-resistance means saving 1/2 on circuit depth can reduce time and space resources by orders of magnitude.

The Barenco et. al. single-ancilla construction was just recently beaten* (kind of) by Amy & Ross ☺
With a single ancilla, the number of Toffoli gates to implement an MCT gate with the Barenco method scales roughly as

- $4(4k/2) = 8k$ (dirty)
- $3(4k/3) = 6k$ (clean)

Prep.

If X,Z basis changes (conjugation by Hadamard gates) are allowed, an MCT gate can be implemented with 1 ancilla and ~4k CCX gates