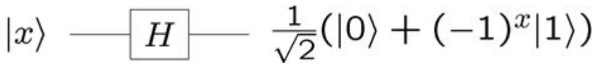
Practical Quantum Computing

Lecture 6

Phase kickback, Toffoli, Fredkin, CtrlSwap

Phase Kickback



Quantum parallelism

- classical algorithm that computes some function f:$\{0,1\}^n \rightarrow \{0,1\}^m$
- build a quantum circuit U
  - consisting only of Toffoli gates
  - maps $|z\rangle|0\rangle \rightarrow |z\rangle|f(z)\rangle$ for every $z \in \{0,1\}^n$

$$U\left(\frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}|z\rangle|0\rangle\right)=\frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}|z\rangle|f(z)\rangle.$$

- applied U just once, and the final superposition contains f(z) for all 2^n input values z!
- *not very useful and does not give more than classical randomization*
  - observing the final superposition will give just one uniformly random $|z\rangle|f(z)\rangle$
  - all other information will be lost

https://quantumcomputing.stackexchange.com/questions/16897/do-global-phases-matter-when-a-gate-is-converted-into-a-controlled-gate

Phase Kickback

Solution: Store the output of the function in the phase of the qubit

$$|x\rangle \;—\boxed{H}—\; \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)$$

$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow |x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |\bar{f}(x)\rangle)$$

$$f(x) = 0 \quad |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$f(x) = 1 \; -|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Phase Kickback

Solution: Store the output of the function in the phase of the qubit

$$|x\rangle \;\text{—}\boxed{H}\text{—}\; \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)$$

$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow |x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |\bar{f}(x)\rangle)$$

$$\begin{array}{ll} f(x) = 0 & |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ f(x) = 1 & -|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array}$$

$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Eigenvalues, Eigenvectors, Measurement

Assume the function f is U=X/Y/Z

$$
\begin{array}{llll}
X: & |0\rangle + |1\rangle & -X: & |0\rangle - |1\rangle \\
Y: & |0\rangle + i\,|1\rangle & -Y: & |0\rangle - i\,|1\rangle \\
Z: & |0\rangle & -Z: & |1\rangle
\end{array}
$$

Useful also for (some) circuit simulations

Qiskit qubit order: first qubit is on the right and having CNOT for C-X

$$
\begin{aligned}
\mathrm{CNOT}|-\boxed{0}\rangle &= |-\rangle \otimes |0\rangle \\
&= |-0\rangle
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{CNOT}|-\boxed{1}\rangle &= X|-\rangle \otimes |1\rangle \\
&= -|-\rangle \otimes |1\rangle \\
&= -|-1\rangle
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{CNOT}\boxed{|-+\rangle} &= \frac{1}{\sqrt{2}}(\mathrm{CNOT}|-0\rangle + \mathrm{CNOT}|-1\rangle) \\
&= \frac{1}{\sqrt{2}}(|-0\rangle + X|-1\rangle) \\
&= \frac{1}{\sqrt{2}}(|-0\rangle - |-1\rangle)
\end{aligned}
$$

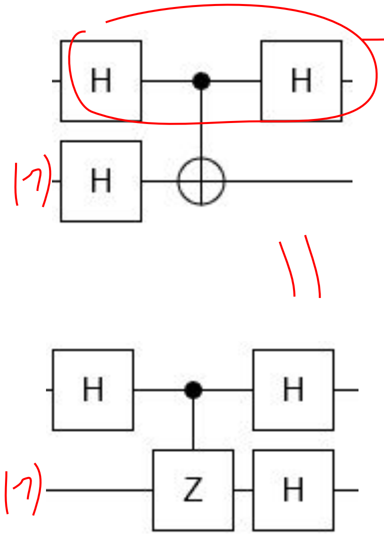
$=\boxed{|-\rangle|-\rangle}$

the phase from input |-> is kicked back to output

Eigenvalues, Eigenvectors, Measurement

$$\begin{array}{llll} X: & |0\rangle + |1\rangle & -X: & |0\rangle - |1\rangle \\ Y: & |0\rangle + i\,|1\rangle & -Y: & |0\rangle - i\,|1\rangle \\ Z: & |0\rangle & -Z: & |1\rangle \end{array}$$

Useful also for (some) circuit simulations



Qiskit qubit order

$$\begin{aligned} \mathrm{CNOT}|{-}\boxed{0}\rangle &= |{-}\rangle \otimes |0\rangle \\ &= |{-}0\rangle \end{aligned}$$

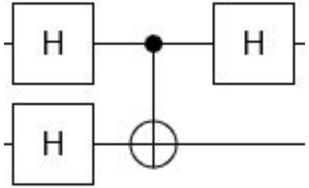
$$\begin{aligned} \mathrm{CNOT}|{-}\boxed{1}\rangle &= X|{-}\rangle \otimes |1\rangle \\ &= -|{-}\rangle \otimes |1\rangle \\ &= -|{-}1\rangle \end{aligned}$$

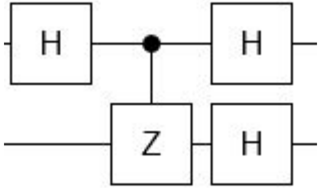
$$\begin{aligned} \mathrm{CNOT}|{-}\boxed{+}\rangle &= \tfrac{1}{\sqrt{2}}(\mathrm{CNOT}|{-}0\rangle + \mathrm{CNOT}|{-}1\rangle) \\ &= \tfrac{1}{\sqrt{2}}(|{-}0\rangle + X|{-}1\rangle) \\ &= \tfrac{1}{\sqrt{2}}(|{-}0\rangle - |{-}1\rangle) \end{aligned}$$

Eigenvalues, Eigenvectors, Measurement

$$\begin{array}{ll} X: \; |0\rangle + |1\rangle & -X: \; |0\rangle - |1\rangle \\ Y: \; |0\rangle + i\,|1\rangle & -Y: \; |0\rangle - i\,|1\rangle \\ Z: \; |0\rangle & -Z: \; |1\rangle \end{array}$$

Useful also for (some) circuit simulations





Qiskit qubit order

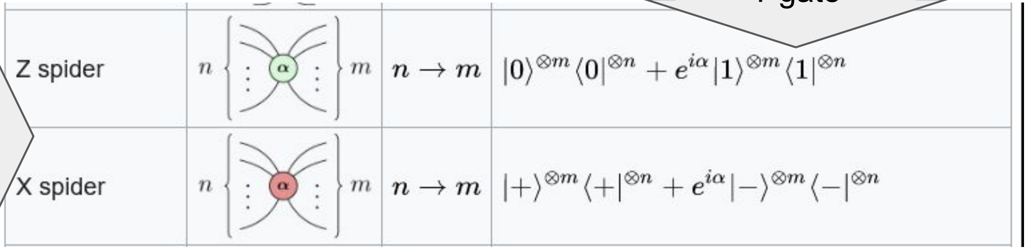
$$\begin{aligned} \mathrm{CNOT}|{-}0\rangle &= |{-}\rangle \otimes |0\rangle \\ &= |{-}0\rangle \end{aligned}$$

$$\begin{aligned} \mathrm{CNOT}|{-}1\rangle &= X|{-}\rangle \otimes |1\rangle \\ &= -|{-}\rangle \otimes |1\rangle \\ &= -|{-}1\rangle \end{aligned}$$

$$\begin{aligned} \mathrm{CNOT}|{-}{+}\rangle &= \tfrac{1}{\sqrt{2}}(\mathrm{CNOT}|{-}0\rangle + \mathrm{CNOT}|{-}1\rangle) \\ &= \tfrac{1}{\sqrt{2}}(|{-}0\rangle + X|{-}1\rangle) \\ &= \tfrac{1}{\sqrt{2}}(|{-}0\rangle - |{-}1\rangle) \end{aligned}$$

n=1
m=1
alpha=pi/4
T gate

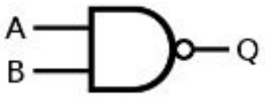
More types of phases
(not only +-1)



Z spider	$n \{ \vdots \; \alpha \; \vdots \} m$	$n \to m$	$\|0\rangle^{\otimes m}\langle 0\|^{\otimes n} + e^{i\alpha}\|1\rangle^{\otimes m}\langle 1\|^{\otimes n}$
X spider	$n \{ \vdots \; \alpha \; \vdots \} m$	$n \to m$	$\|+\rangle^{\otimes m}\langle +\|^{\otimes n} + e^{i\alpha}\|-\rangle^{\otimes m}\langle -\|^{\otimes n}$

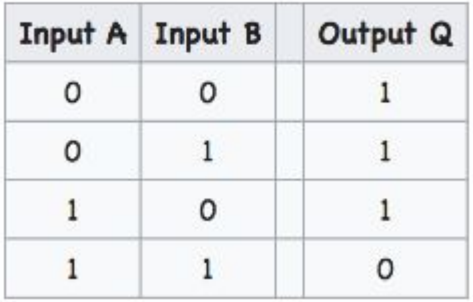
Toffoli Gate

The NAND gate is universal for classical circuits.



Q = A NAND B

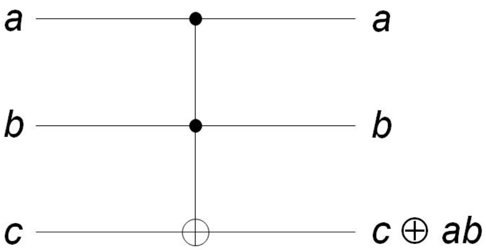
Truth Table



Input A	Input B	Output Q
0	0	1
0	1	1
1	0	1
1	1	0

We can perform the same operation

using a Toffoli gate.



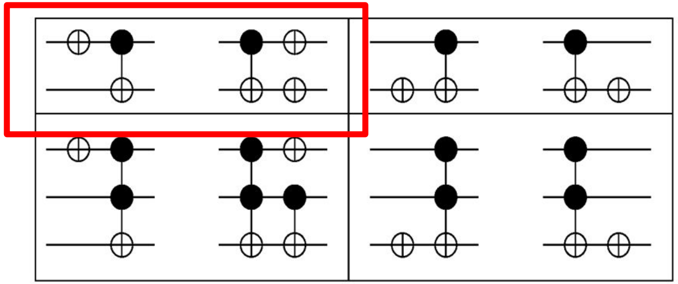
c=1 -> NAND

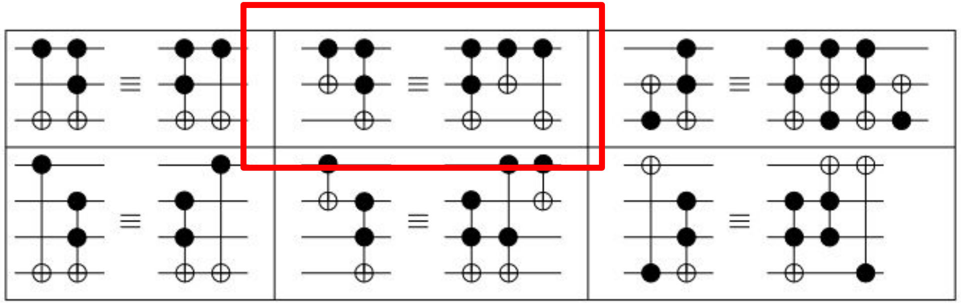
Convert any classical algorithm into a quantum algorithm, replacing the NAND gates with Toffolis, and keeping the extra qubits.

Reversible Computation and Circuits

A gate is **reversible** if the (Boolean) function it computes is **bijective**.

A k-CNOT is a (k+1)×(k+1) gate. It leaves the first k inputs unchanged, and inverts the last iff all others are 1. The unchanged lines are referred to as control lines.





Equivalences between reversible circuits -> Can be used for circuit optimisation

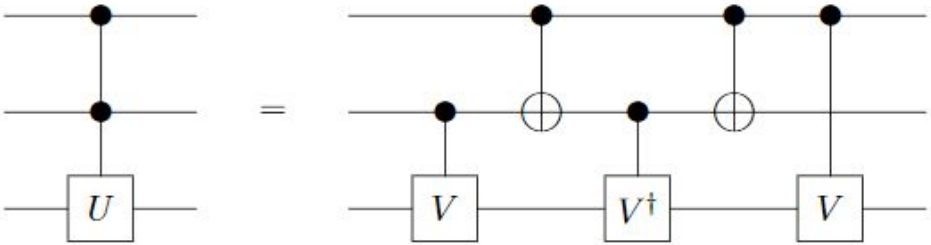
https://arxiv.org/pdf/quant-ph/0207001.pdf

Toffoli Gate Decomposition

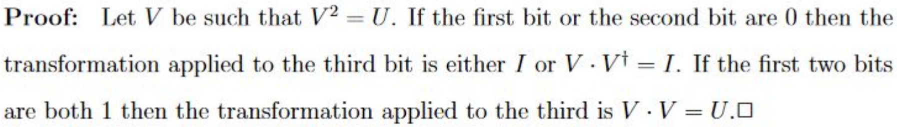
Some of the intuition behind the construction when the first two input bits are x1 and x2, the sequence of operations performed on the third bit is:

- V iff x1 = 1,
- V iff x2 = 1,
- $V^\dagger$ iff x1⊕x2= 1

$$x_1 + x_2 - (x_1 \oplus x_2) = 2 \cdot (x_1 \wedge x_2)$$



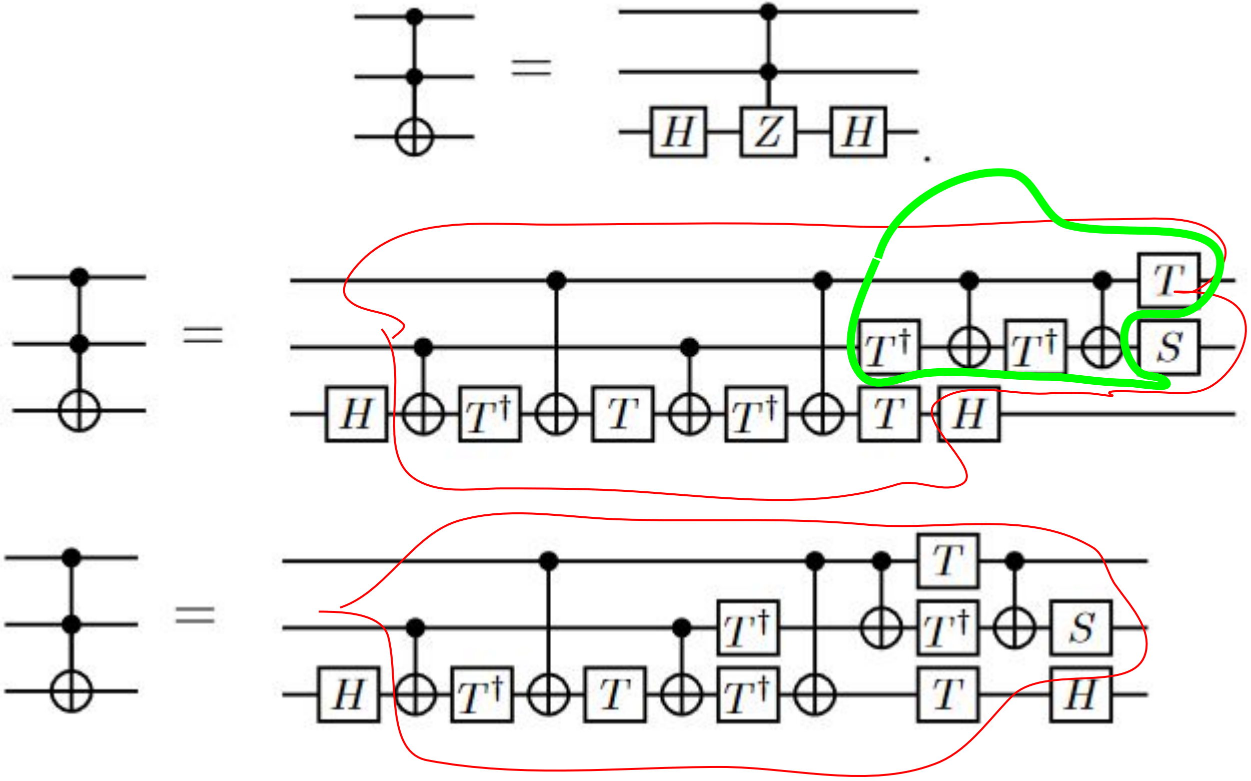
The above sequence of operations is equivalent to performing V^2 on the third bit iff x1∧x2 = 1, which is the gate.



Proof: Let V be such that $V^2 = U$. If the first bit or the second bit are 0 then the transformation applied to the third bit is either I or $V \cdot V^\dagger = I$. If the first two bits are both 1 then the transformation applied to the third is $V \cdot V = U$.□

https://arxiv.org/pdf/quant-ph/9503016.pdf

Toffoli and Clifford+T



https://arxiv.org/pdf/1210.0974.pdf

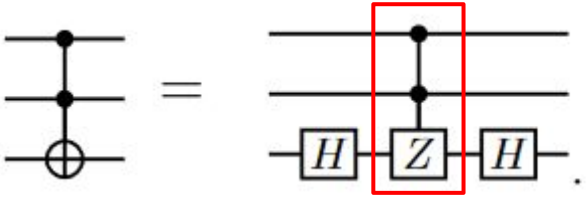
Toffoli and Clifford + T

$$4xyz = x+y+z-(x\oplus y)-(y\oplus z)-(x\oplus z)+(x\oplus y\oplus z).$$

$$x \oplus y = x + y - 2xy.$$

$$\omega = (-1)^{1/4} = e^{i\pi/4}.$$

root of unity



$$\boxed{(-1)}^{xyz} = \boxed{\omega^4}^{xyz}$$
$$= \omega^x\ \omega^y\ \omega^z\ (\omega^\dagger)^{x\oplus y}\ (\omega^\dagger)^{y\oplus z}\ (\omega^\dagger)^{x\oplus z}\ \omega^{x\oplus y\oplus z}.$$

phase polynomial

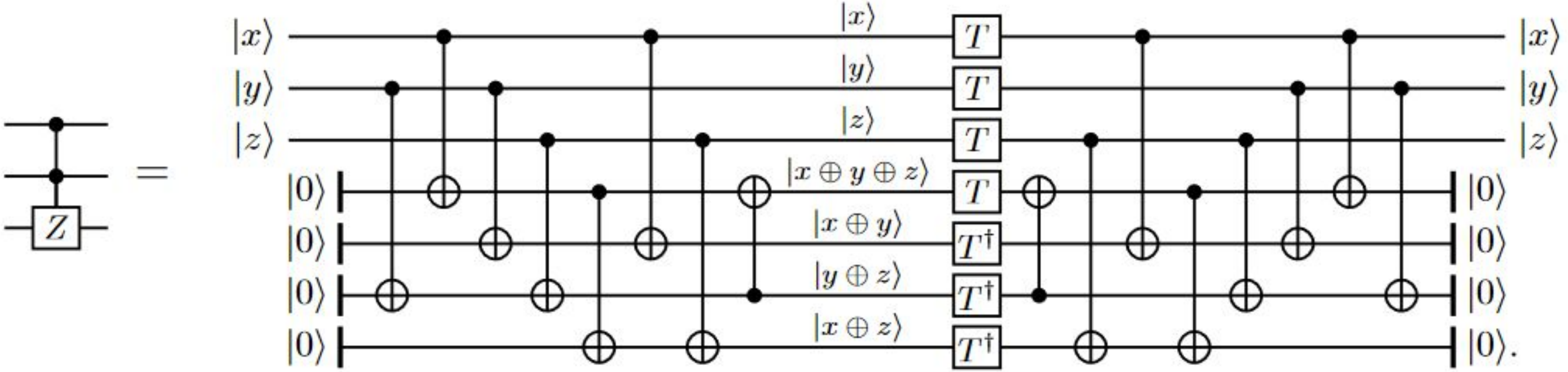
https://arxiv.org/pdf/1210.0974.pdf

Toffoli and Clifford + T

$$(-1)^{xyz} = \omega^{4xyz}$$

$$= \omega^x \, \omega^y \, \omega^z \, (\omega^\dagger)^{x\oplus y} \, (\omega^\dagger)^{y\oplus z} \, (\omega^\dagger)^{x\oplus z} \, \omega^{x\oplus y\oplus z}.$$

$$\boxed{T|x\rangle \; = \; \omega^x|x\rangle}$$

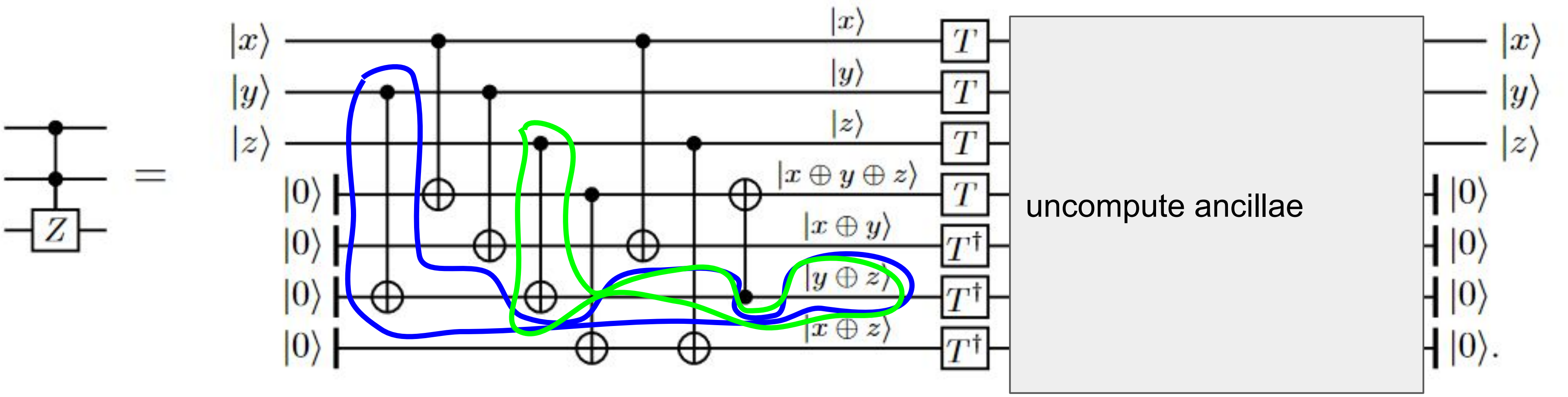


https://arxiv.org/pdf/1210.0974.pdf

Toffoli and Clifford + T

$$
\begin{aligned}
(-1)^{xyz} &= \omega^{4xyz} \\
&= \omega^{x}\,\omega^{y}\,\omega^{z}\,(\omega^{\dagger})^{x\oplus y}\,(\omega^{\dagger})^{y\oplus z}\,(\omega^{\dagger})^{x\oplus z}\,\omega^{x\oplus y\oplus z}.
\end{aligned}
$$

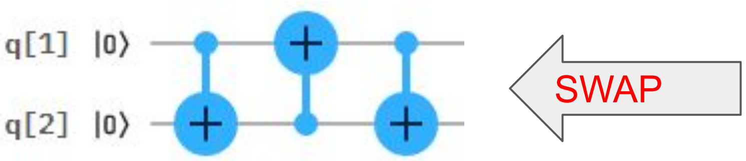
$$\boxed{T|x\rangle \;=\; \omega^{x}|x\rangle}$$



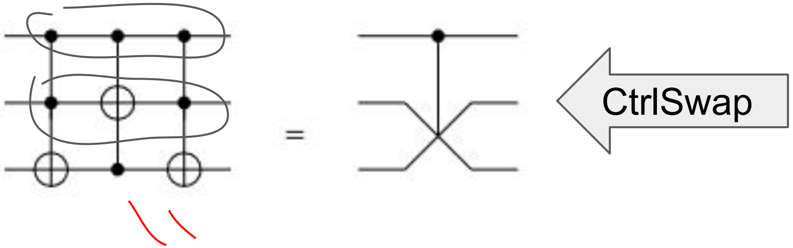
uncompute ancillae

https://arxiv.org/pdf/1210.0974.pdf

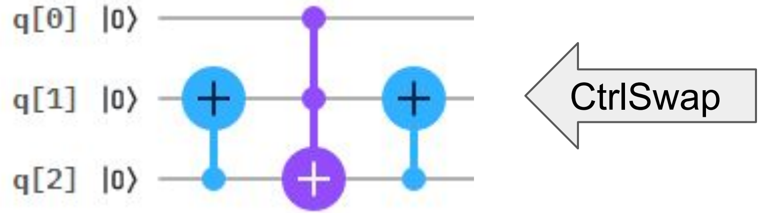
Fredkin Gate - Conservative Logic



SWAP

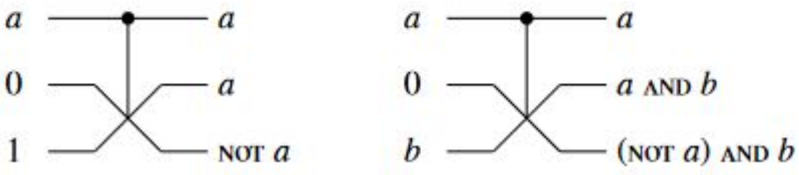


CtrlSwap



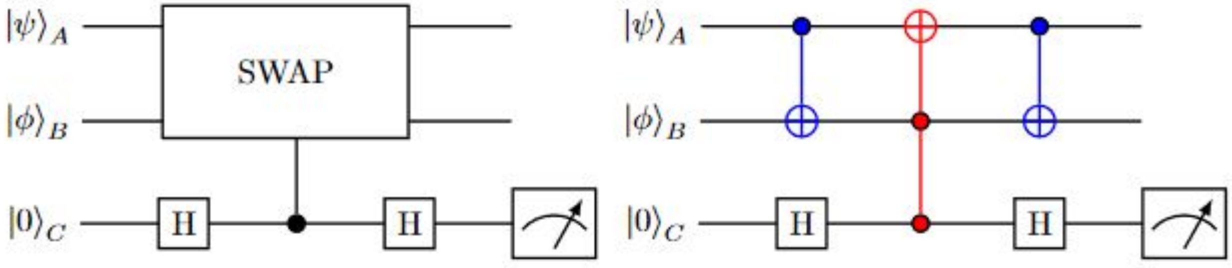
CtrlSwap

NOT and AND gates can be built from Fredkin gates with appropriate patterns of inputs



$$F = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Controlled Swap



(a)

(b)

Figure 1: The quantum circuit for an equivalency SWAP test on the two states $|\psi\rangle$ and $|\phi\rangle$. H is a Hadamard gate from equation (7). (a) The SWAP gate swaps all qubits in the test states on the condition that the control qubit is in state $|1\rangle$. (b) shows the SWAP gate broken down into individual gates for the one-qubit test state case. The central gate, shown in red, is a Toffoli gate from equation (9) and the two gates either side in blue are CNOT gates from equation (8), where the crossed circles are controlled on the dots. The final CNOT gate – not necessary for the test outcome – returns the system to its initial state in the case of equivalent states.

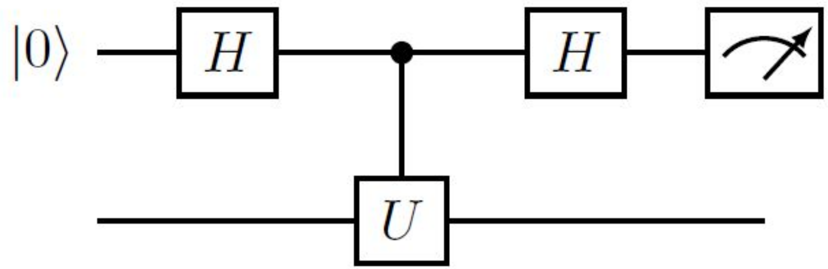
https://arxiv.org/pdf/2009.07613.pdf

$$\mathrm{H}\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \tag{7}$$
$$\mathrm{H}\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{8}$$

$$\mathrm{T} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{9}$$

Controlled Swap



The CtrlSwap simulates measurement of the SWAP operator as an observable (as opposed to a unitary transformation).

Swap is Hermitian
because $U^2 = I$
eigenvalues are ±1

Measure eigenvalue using the relative phase

$$\frac{1}{2}(|0,\phi,\psi\rangle + |1,\phi,\psi\rangle + |0,\psi,\phi\rangle - |1,\psi,\phi\rangle) = \frac{1}{2}|0\rangle(|\phi,\psi\rangle + |\psi,\phi\rangle) + \frac{1}{2}|1\rangle(|\phi,\psi\rangle - |\psi,\phi\rangle)$$

$$P(\text{First qubit} = 0) = \frac{1}{2}\Big(\langle\phi|\langle\psi| + \langle\psi|\langle\phi|\Big)\frac{1}{2}\Big(|\phi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle\Big) = \frac{1}{2} + \frac{1}{2}|\langle\psi|\phi\rangle|^2$$

If **states are orthogonal** -> the probability that 0 is measured is **0.5**

If **states are equal** -> the probability that 0 is measured is **1**

Handwritten notes to derive ctrl-swap measurement