Practical Quantum Computing

Lecture 07

Phase kickback, Toffoli, Fredkin

Week	**Tuesday** (3h)			**Wednesday** (3h)			**Deadlines**	
1. The Basics	Introduction	Gates	Circuit Identities	Qiskit	Cirq/Qualtran	Q&A		
	Programming Assignment 1: The basics of a quantum circuit simulator			**Programming Assignment 1:** The building blocks of a quantum circuit simulator				
2. Entanglement and its Applications	Teleportation	Superdense Coding	Quantum Key Distribution	Qualtran/ Assignment2	Terminology of Projects	Q&A		
	Programming Assignment 2: The basics of a quantum circuit optimizer			**Programming Assignment 2:** The building blocks of a quantum circuit optimizer				
3. Computing	Phase Kickback and Toffoli	Distinguishing quantum states and The First Algorithms	Grover's Algorithm	Invited TBA	PennyLane	Q&A		11 May 2024
4. Advanced Topics*	Arithmetic Circuits*	Fault-Tolerance*	QML*	Invited TBA	Crumble	Q&A	18 May 2024	

* not evaluated

Learning goals - 07 Superposition and Phase Kickback (Computing)

1. What you have learned by now
   a. Quantum circuits: mathematics, diagrams and circuit identities
   b. Entanglement: teleportation, superdense coding, more powerful correlations and winning games by using entanglement
   c. Quantum Key Distribution Networks
2. **Quantum Parallelism and State Superposition**
   a. What it is, and how to built it with single qubit (Hadamard) gates
   b. The phase: encoding information into state superpositions
3. **Phase Kickback**
   a. What it is and how it works
   b. How to use it for signaling properties of Boolean functions
   c. Deriving the phase kickback using circuit identities
4. **Phase Polynomials for *complicated* quantum gates**
   a. Construction of phase polynomials
   b. Deriving a quantum circuit from a phase polynomial
   c. The Toffoli gate and its phase polynomial

- Deadline for programming Assignment 1
- 11 May 2024

Quantum Parallelism

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

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

Phase Kickback

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

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

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

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

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

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

Phase Kickback

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

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

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

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

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

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

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

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

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

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

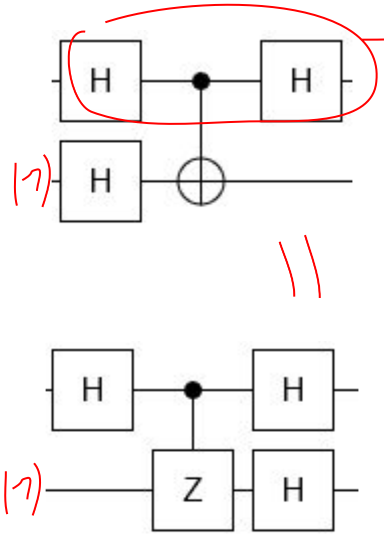
=|->|->

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

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

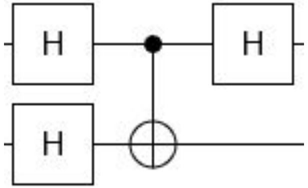
$$
\begin{aligned}
\mathrm{CNOT}|{-}1\rangle &= X|-\rangle \otimes |1\rangle \\
&= -|-\rangle \otimes |1\rangle \\
&= -|{-}1\rangle
\end{aligned}
$$

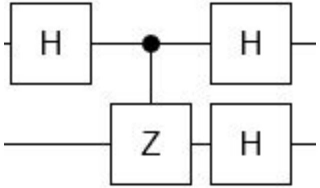
$$
\begin{aligned}
\mathrm{CNOT}|{-}{+}\rangle &= \tfrac{1}{\sqrt{2}}(\mathrm{CNOT}|{-}0\rangle + \mathrm{CNOT}|{-}1\rangle) \\
&= \tfrac{1}{\sqrt{2}}(|{-}0\rangle + X|{-}1\rangle) \\
&= \tfrac{1}{\sqrt{2}}(|{-}0\rangle - |{-}1\rangle)
\end{aligned}
$$

Eigenvalues, Eigenvectors, Measurement

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

Useful also for (some) circuit simulations





Qiskit qubit order

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

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

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

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

More types of phases
(not only +-1)

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

Learning goals - 07 Superposition and Phase Kickback (Computing)

1. What you have learned by now
   a. Quantum circuits: mathematics, diagrams and circuit identities
   b. Entanglement: teleportation, superdense coding, more powerful correlations and winning games by using entanglement
   c. Quantum Key Distribution Networks
2. **Quantum Parallelism and State Superposition**
   a. What it is, and how to built it with single qubit (Hadamard) gates
   b. The phase: encoding information into state superpositions
3. **Phase Kickback**
   a. What it is and how it works
   b. How to use it for signaling properties of Boolean functions
   c. Deriving the phase kickback using circuit identities
4. **Phase Polynomials for *complicated* quantum gates**
   a. Construction of phase polynomials
   b. Deriving a quantum circuit from a phase polynomial
   c. The Toffoli gate and its phase polynomial

- Deadline for programming Assignment 1
- 11 May 2024

Classical computations,
More phases and Toffoli gates

Toffoli Gate

The NAND gate is universal for classical circuits.

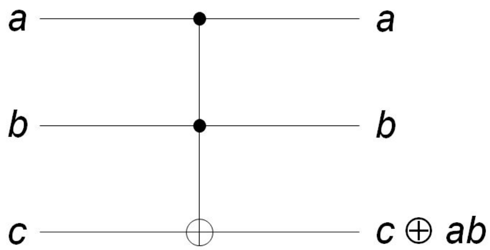
Q = A NAND B

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.



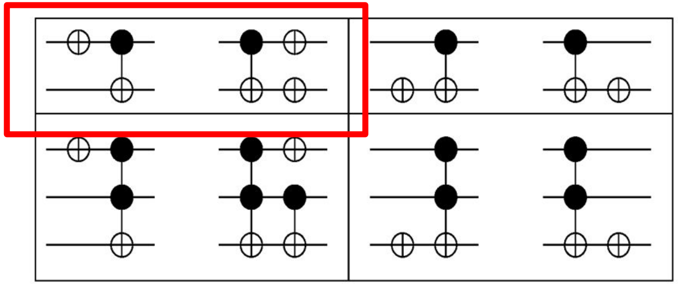
c=1 -> NAND

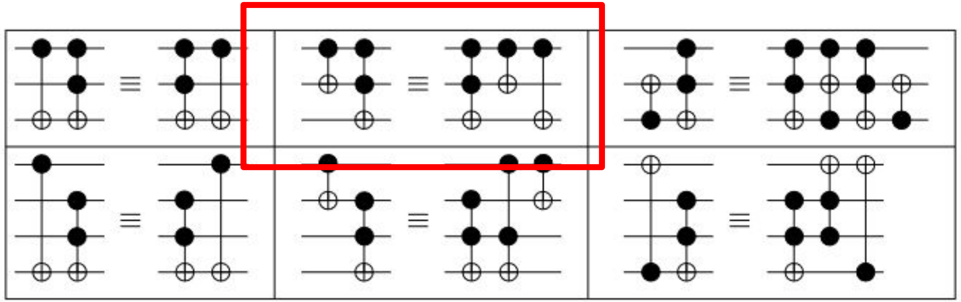
Convert any classical algorithm into a quantum algorithm, replacing the NAND gates with Toffolis, and keeping the extra qubits.

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

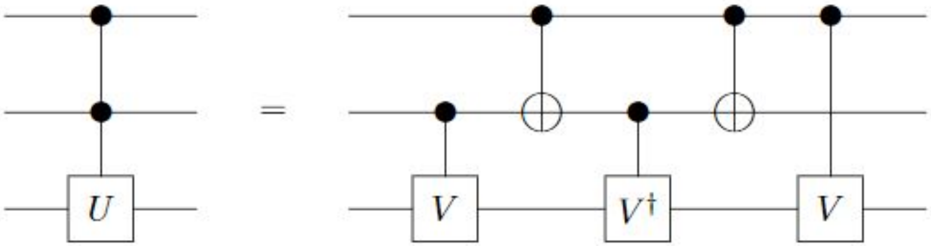
Toffoli Gate Decomposition

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

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

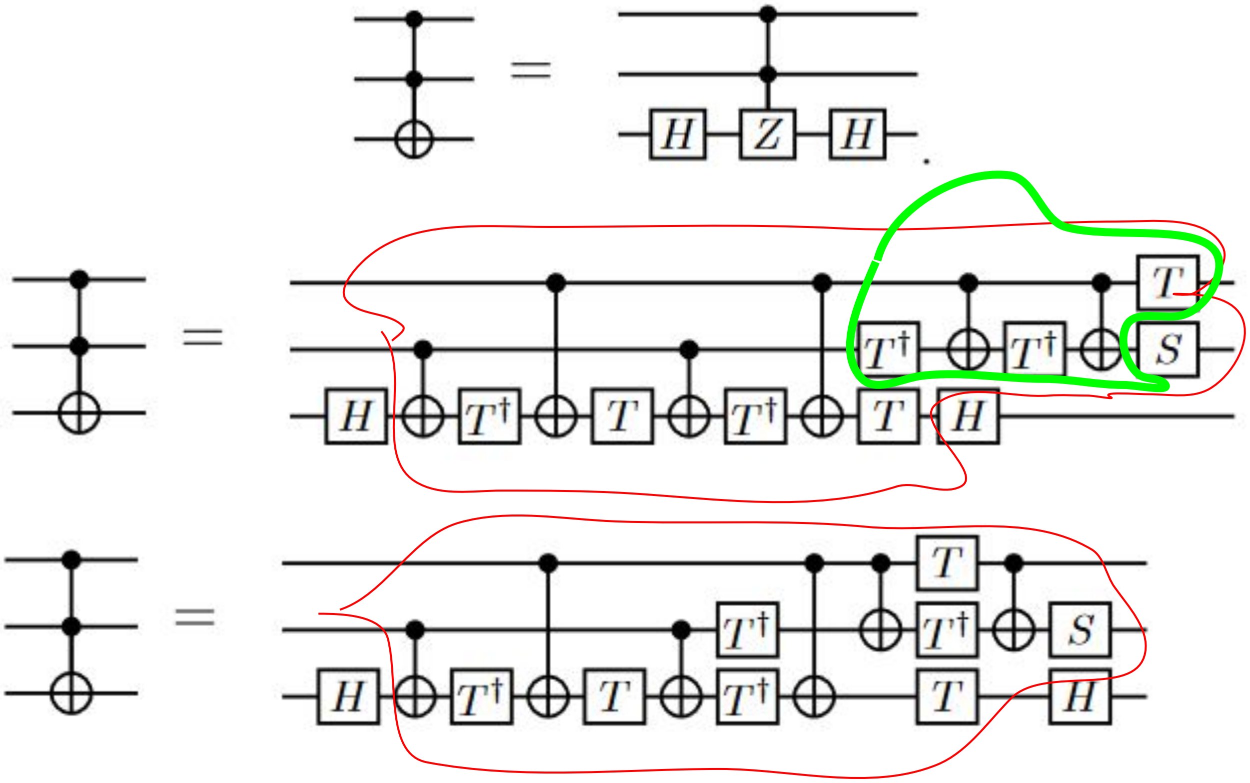
The above sequence of operations is equivalent to performing V^2 on the third bit iff x1∧x2 = 1, which is the gate.



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

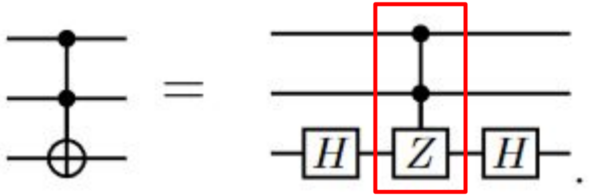
Toffoli and Clifford + T

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

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

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

root of unity



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

phase polynomial

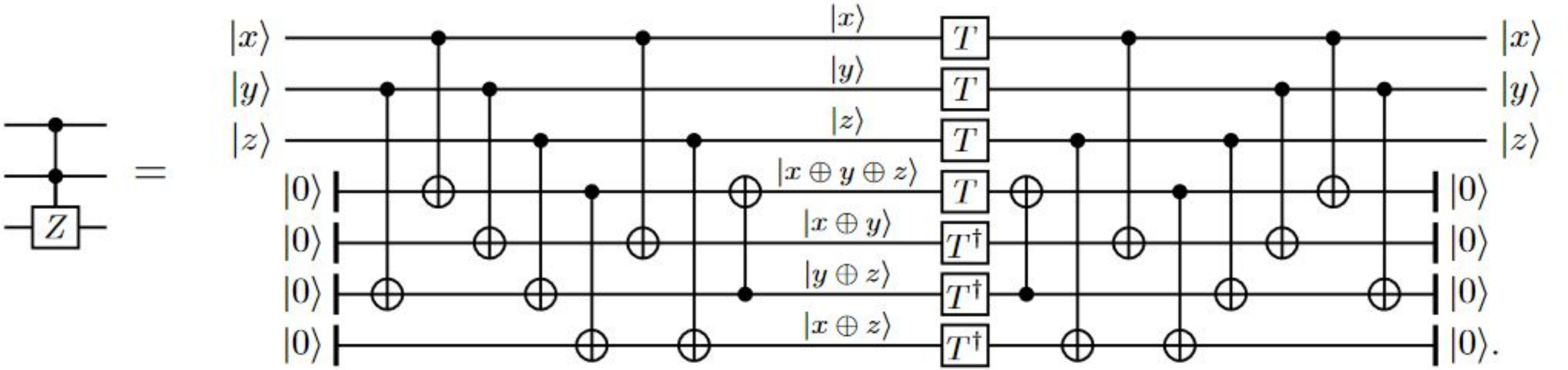
$$= \omega^{x}\ \omega^{y}\ \omega^{z}\ (\omega^{\dagger})^{x\oplus y}\ (\omega^{\dagger})^{y\oplus z}\ (\omega^{\dagger})^{x\oplus z}\ \omega^{x\oplus y\oplus z}.$$

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

Toffoli and Clifford + T

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

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

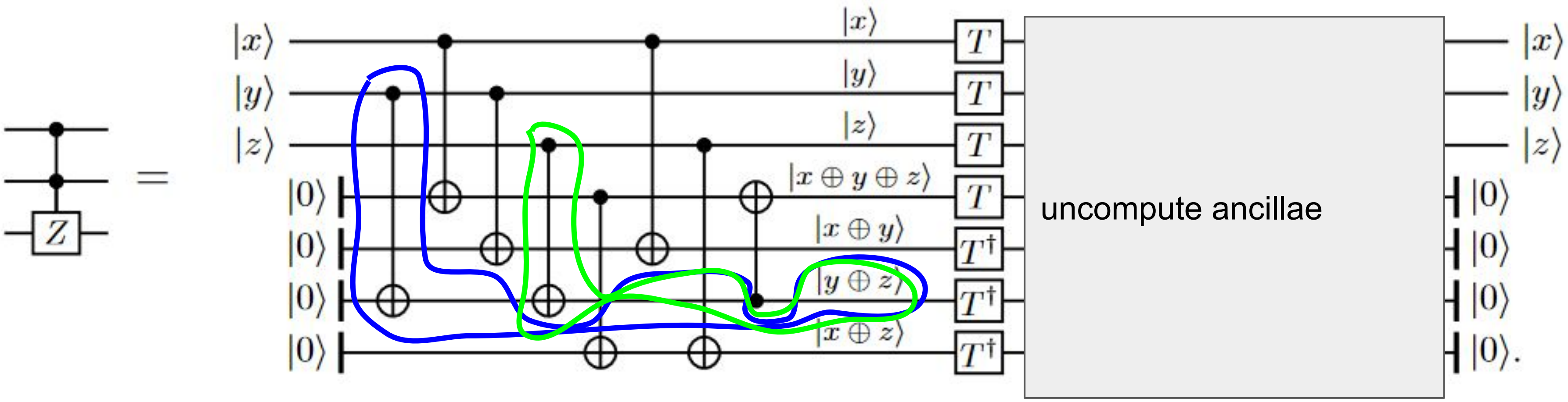


https://arxiv.org/pdf/1210.0974.pdf

Toffoli and Clifford + T

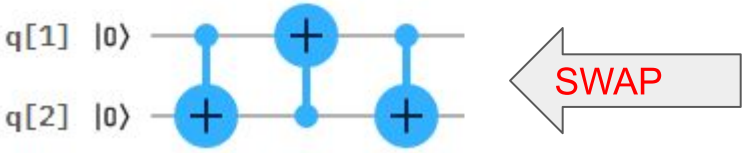
$$(-1)^{xyz} = \omega^{4xyz}$$
$$= \omega^{x}\, \omega^{y}\, \omega^{z}\, (\omega^{\dagger})^{x \oplus y}\, (\omega^{\dagger})^{y \oplus z}\, (\omega^{\dagger})^{x \oplus z}\, \omega^{x \oplus y \oplus z}.$$

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

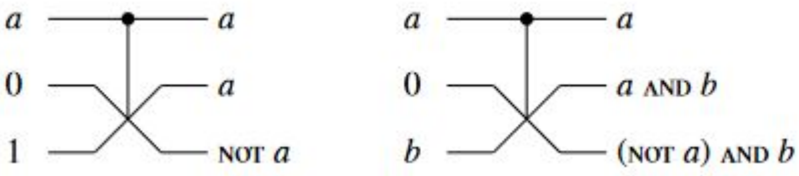


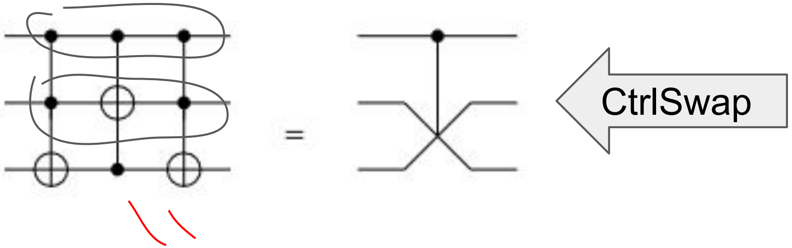
https://arxiv.org/pdf/1210.0974.pdf

Fredkin Gate - Conservative Logic



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





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