Lecture 3
Quantum circuits

January 22, 2020

Classical computation on a quantum computer

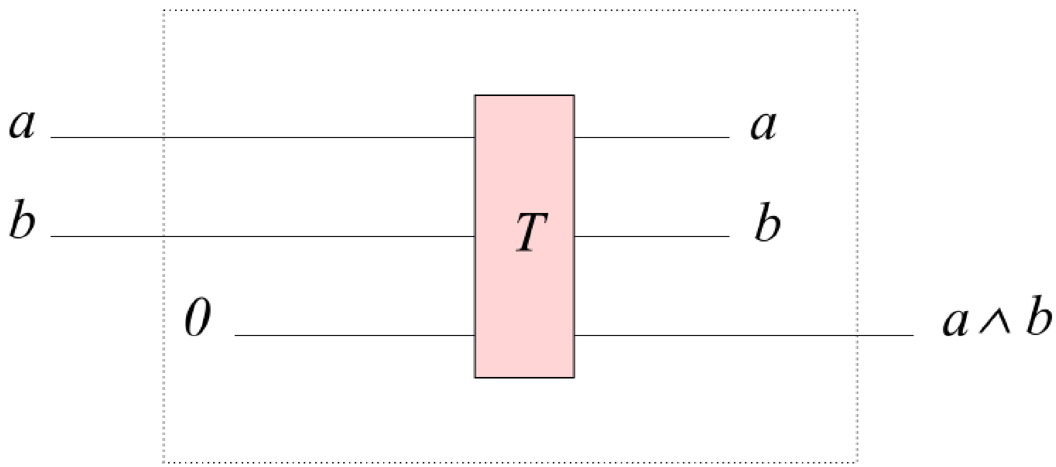
- Efficient classical computation $\Rightarrow$ efficient quantum computer ?
- Unitary transform $\rightarrow$ reversible computation

First example, computing $a \wedge b$

- The Toffoli gate

$$T|a\rangle|b\rangle|c\rangle = |a\rangle|b\rangle|c \oplus (a \wedge b)\rangle$$

- Implementing $a \wedge b$



Exercise : NOT, XOR, OR, COPY

Give a quantum gate or circuit based on $\mathbf{X}$, c-**NOT** and the Toffoli gate for computing for a, $b \in \{0, 1\}$:

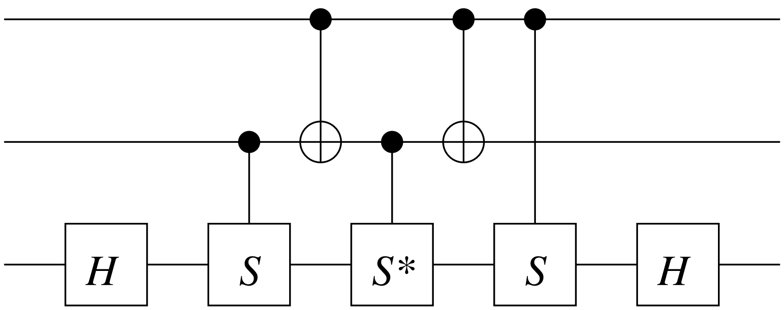
1. $\bar{a}$
2. $a \oplus b$
3. $a \vee b$
4. a copy of a, namely $a \mapsto (a, a)$

Exercise : implementing the classical Toffoli gate with 1 and 2-bit permutation gates ?

Is it possible to implement the Toffoli gate by using only 1 and 2 permutation gates ?

Exercise

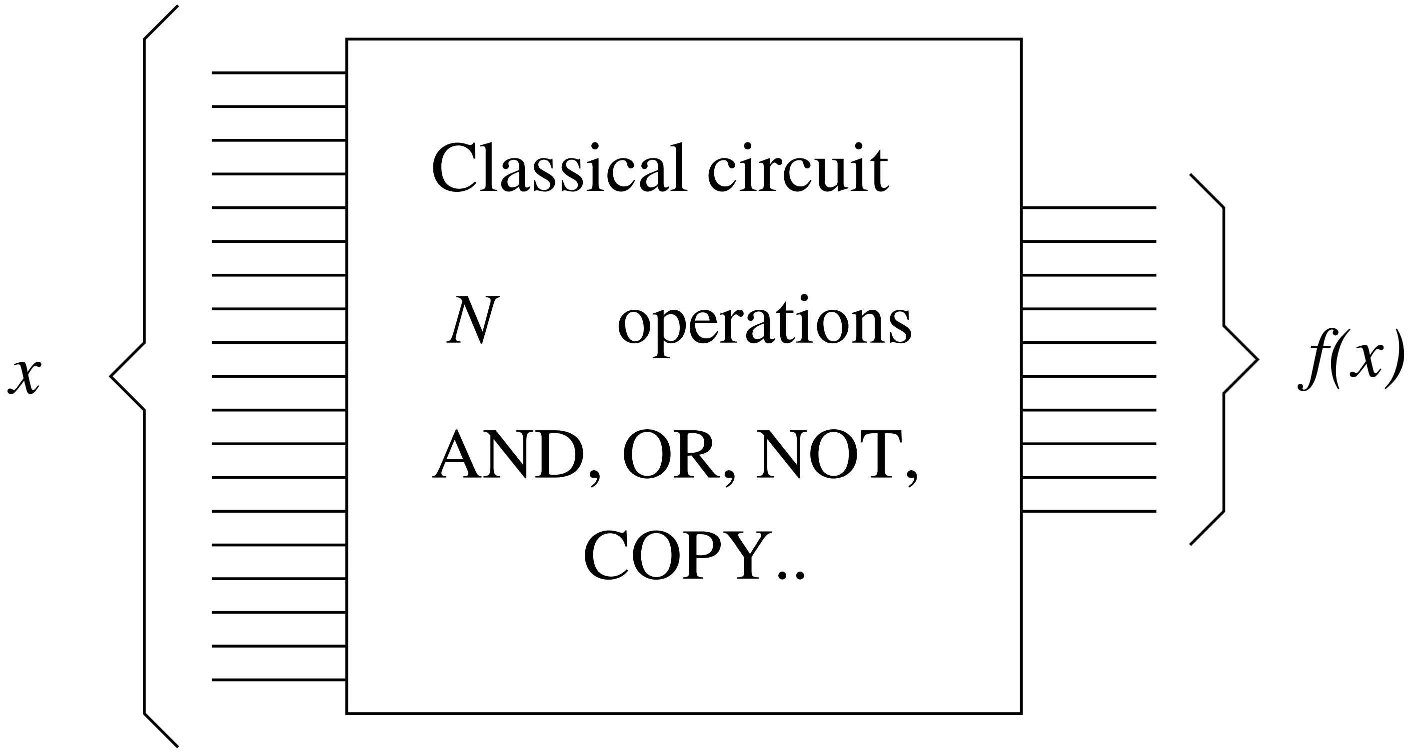
Show that the following circuit implements the Toffoli gate



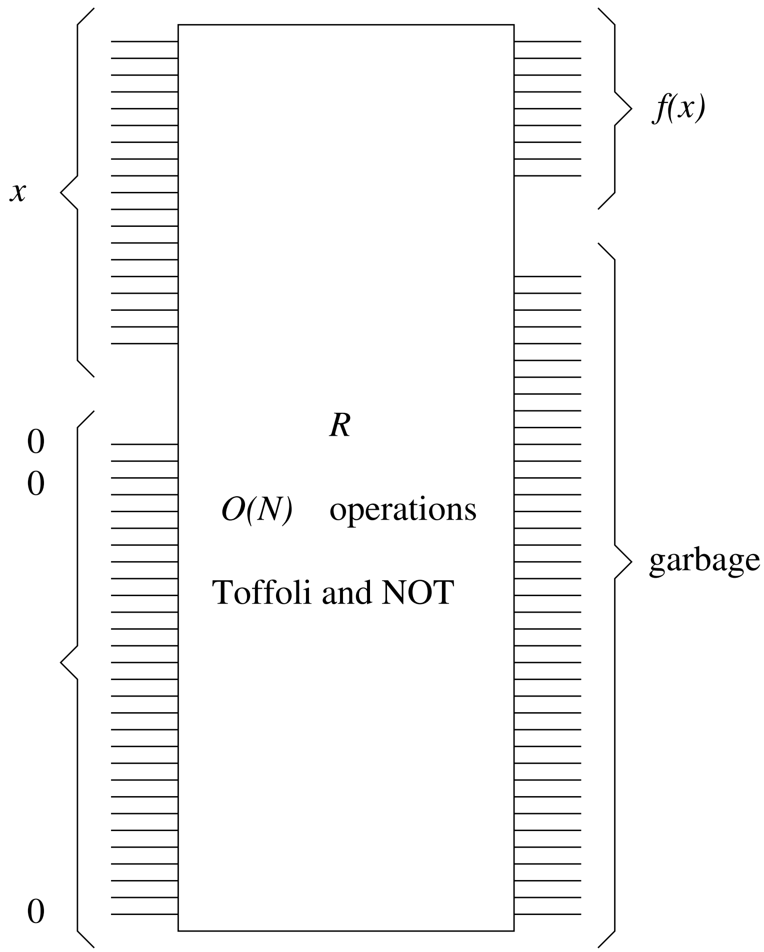
where S is the following transform

$$S\left(\alpha\left|0\right\rangle + \beta\left|1\right\rangle\right) = \alpha\left|0\right\rangle + \beta i\left|1\right\rangle$$

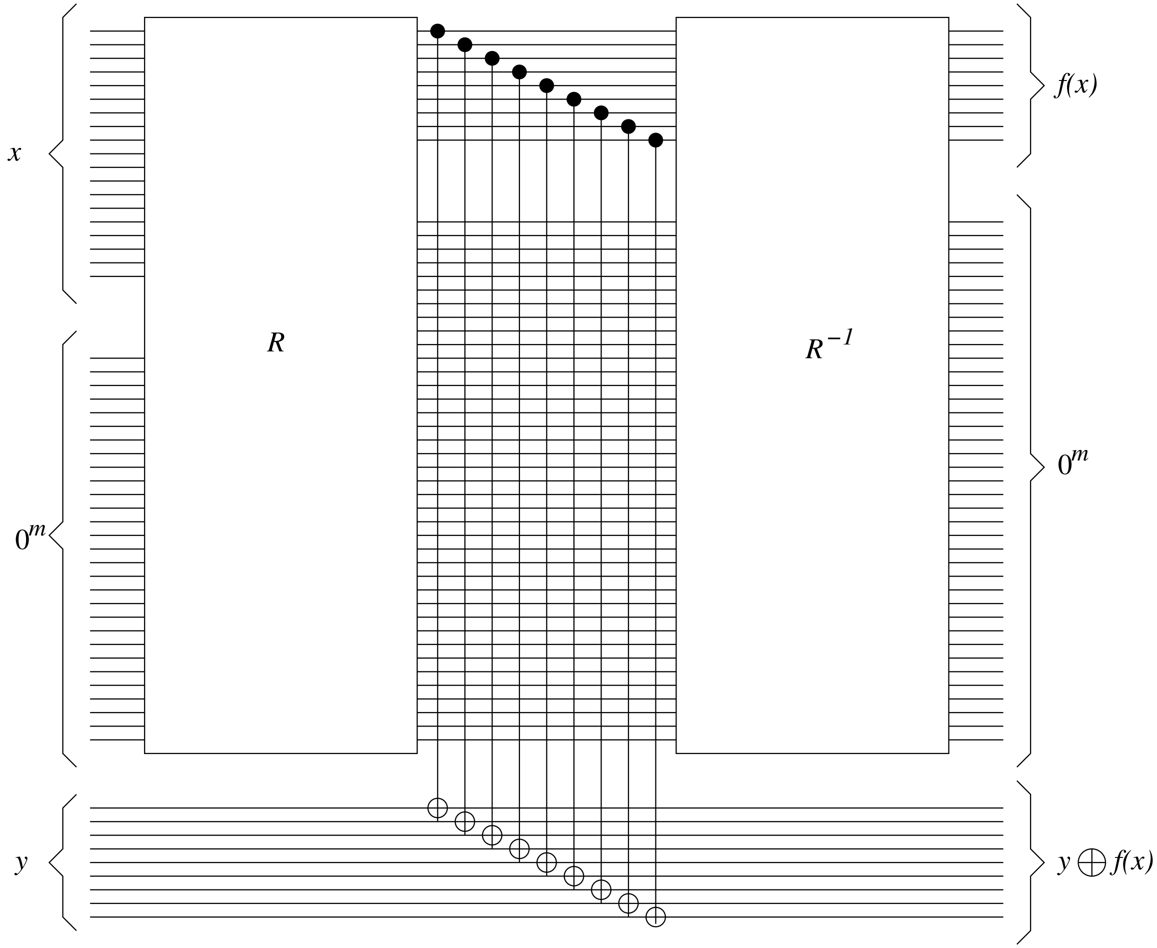
Classical circuit



Reversible circuit



A better reversible circuit



Universal Quantum Computation with one or two qubit gates

- Universal quantum computation with one qubit gates + CNOT gate
- Approximation with accuracy ε of one qubit unitaries with $O(\log^c(1/\varepsilon))$ gates $\mathbf{H}$, $\mathbf{S}$ and $\mathbf{T}$ where $c \approx 2$ and

$$\begin{aligned}
\mathbf{H} &\stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\
\mathbf{S} &\stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \\
\mathbf{T} &\stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}
\end{aligned}$$

- Approximation with accuracy ε of every n qubit gate with $O\left(n^2 4^n \log^c(n^2 4^n/\varepsilon)\right)$ gates $\mathbf{H}$, $\mathbf{T}$ and c-**NOT**.

The fundamental theorem

Theorem 1. *The basis consisting of all one-qubit and two-qubit unitary operators allows the realization of an arbitrary unitary operator*

Breaking up a unitary into two-level unitaries

Lemma 1. *An arbitrary unitary operator* $\mathbf{U}$ *on* $\mathbb{C}^m$ *can be represented as a product of at most* $m(m-1)/2$ *two-level unitary matrices, i.e. matrices of the form*

$$\begin{pmatrix} 1 & 0 & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & \ddots & 0 & \dots & \dots & \dots & \dots & \vdots \\ \vdots & \dots & 1 & 0 & \dots & \dots & \dots & \vdots \\ \vdots & \dots & \dots & a & b & \dots & \dots & \vdots \\ \vdots & \dots & \dots & c & d & 0 & \dots & \vdots \\ \vdots & \dots & \dots & \dots & 0 & 1 & \ddots & \vdots \\ \vdots & \dots & \dots & \dots & \dots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 & 1 \end{pmatrix}$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{U}(2)$

Proof

For any numbers c_1, c_2 there exists $\mathbf{V} \in \mathbb{U}(2)$ s.t.

$$\mathbf{V}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} \sqrt{|c_1|^2 + |c_2|^2} \\ 0 \end{pmatrix}$$

$$\mathbf{U} \quad = \quad \begin{pmatrix} u_{11} & u_{12} & \dots & u_{1m} \\ u_{21} & u_{22} & \dots & u_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ u_{m1} & u_{m2} & \dots & \ddots \end{pmatrix}$$

$$\mathbf{U}_{m-1}\cdots\mathbf{U}_1\mathbf{U} \quad = \quad \begin{pmatrix} * & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \dots & * \end{pmatrix} = \mathbf{U}^{(1)}$$

$$\mathbf{U}^{(1)} \quad = \quad \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \dots & * \end{pmatrix}$$

Corollary

- A unitary acting on n qubits can be decomposed as a product of $2^{n-1}(2^n - 1)$ two-level unitary matrices

Exercise

Show that there is a unitary on n qubits that can not be decomposed in a product of less than $2^n - 1$ two-level unitary matrices

Implementing a 2-level unitary with a c-U unitary

$$\text{c-}\mathbf{U}^{n} \left|x_1 \cdots x_n\right\rangle \left|\psi\right\rangle \quad = \quad \left|x_1 \cdots x_n\right\rangle \mathbf{U}^{x_1 \cdots x_m} \left|\psi\right\rangle$$

corresponds to

$$\begin{pmatrix} 1 & 0 & \dots & \dots & \dots & 0 \\ 0 & 1 & 0 & \dots & \dots & \vdots \\ \vdots & \ddots & \ddots & \dots & \dots & \vdots \\ \vdots & \dots & \dots & 1 & 0 & 0 \\ \vdots & \dots & \dots & 0 & a & b \\ 0 & \dots & \dots & 0 & c & d \end{pmatrix}$$

where $\mathbf{U} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Exercise

1. Give a quantum circuit that realizes c-$\mathbf{U}^2$ from c-$\mathbf{U}$, c-**NOT** and one qubit gates
2. Give a quantum circuit that realizes c-$\mathbf{U}^n$ from c-$\mathbf{U}$, c-**NOT** and one qubit gates. What is its complexity (in the number of gates) ? What is its depth ?

c-U with c-NOT and one qubit gates

Lemma 2. *Any unitary* $\mathbf{U} \in \mathbb{U}(2)$ *can be written as*

$$\mathbf{U} = e^{i\alpha}\mathbf{AXBXC}$$

where $\mathbf{ABC} = \mathbf{Id}$.

Proof

$$\mathbf{R}_y(\theta) \stackrel{\text{def}}{=} \begin{pmatrix} \cos\theta/2 & -\sin\theta/2 \\ \sin\theta/2 & \cos\theta/2 \end{pmatrix}$$

$$\mathbf{R}_z(\theta) \stackrel{\text{def}}{=} \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{pmatrix}$$

Lemma 3. *Suppose $\mathbf{U} \in \mathbb{U}(2)$, then there exist real numbers α, β, γ and δ such that*

$$\mathbf{U} = e^{i\alpha}\mathbf{R}_z(\beta)\mathbf{R}_y(\gamma)\mathbf{R}_z(\delta)$$

Set

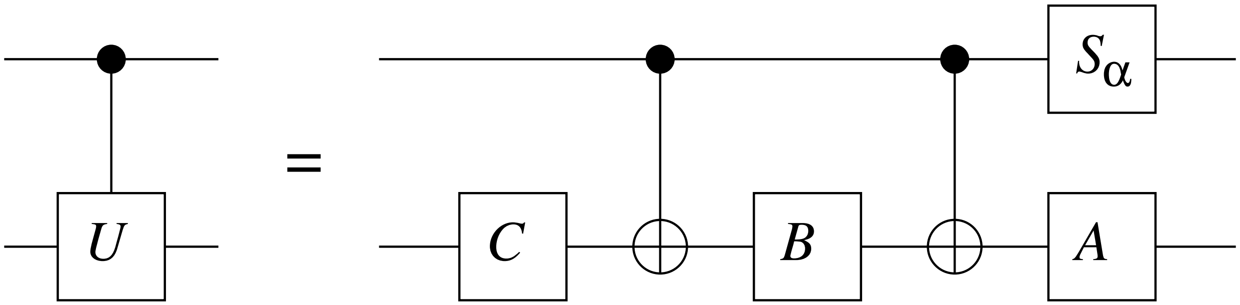
$$\mathbf{A} \stackrel{\text{def}}{=} \mathbf{R}_z(\beta)\mathbf{R}_y(\gamma/2)$$

$$\mathbf{B} \stackrel{\text{def}}{=} \mathbf{R}_y(-\gamma/2)\mathbf{R}_z(-(\beta+\delta)/2)$$

$$\mathbf{C} \stackrel{\text{def}}{=} \mathbf{R}_z((\delta-\beta)/2)$$

Exercise

Show that



where

$$\mathbf{S}_\alpha \left(a \left| 0 \right\rangle + b \left| 1 \right\rangle \right) = a \left| 0 \right\rangle + b e^{i\alpha} \left| 1 \right\rangle$$

Exercise : implementing an arbitrary unitary two-level matrix in $\mathbb{U}(2^n)$ with a c-$\mathbf{U}$

Show how to implement an arbitrary two-level matrix in $\mathbb{U}(2^n)$ with a non trivial two-level part $\mathbf{U} \in \mathbb{U}(2)$ with c-$\mathbf{U}^n$ and $\mathbf{X}$ and c-**NOT** gates with gate complexity $O(n^2)$.

Approximating any one qubit gate with a discrete gate set

$$\mathbf{H} \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\mathbf{T} \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

- Up to a global phase $\mathbf{T}$ and $\mathbf{HTH}$ are rotations around the $\hat{z}$ axis and the $\hat{x}$ axis of the Bloch sphere
- Composing them gives a rotation about an axis along $\mathbf{n} = (\cos\pi/8, \sin\pi/8, \cos\pi/8)$ of an angle θ defined by $\cos\theta/2 = \cos^2\pi/8$
- approximate any unitary $\mathbf{U} \in \mathbb{U}(2)$

Approximating arbitrary unitary gates is generically hard

- With $O(1)$ different types of gates acting each on $O(1)$ qubits we have $\mathrm{poly}(n)$ different gates on n qubits

$$\begin{aligned} |0^n\rangle &\xrightarrow{\mathbf{U}} |\psi\rangle \\ |0^n\rangle &\xrightarrow{\mathbf{U}_\varepsilon} |\psi_\varepsilon\rangle \\ \| |\psi\rangle - |\psi_\varepsilon\rangle \| &\leq \varepsilon \end{aligned}$$

-

$$\#\text{dif. } \mathbf{U}_\varepsilon \text{ obtained by a circuit with } m \text{ gates} = \mathrm{poly}(n)^m$$

Approximating arbitrary unitary gates is generically hard (II)

- $|\psi\rangle$ and $|\psi_\varepsilon\rangle$ belong to the $2^{n+1}-1$-sphere and are at distance $\leq \varepsilon$

$$
\begin{aligned}
\#\text{dif. } \mathbf{U}_\varepsilon \times \text{Vol}(\text{ball of radius } \varepsilon \text{ in } S^{2^{n+1}-1}) &\geq \text{Vol}(S^{2^{n+1}-1}) \\
\frac{\text{Vol}(S^{2^{n+1}-1})}{\text{Vol}(\text{ball of radius } \varepsilon \text{ in } S^{2^{n+1}-1})} &= \frac{\sqrt{\pi}\,\Gamma(2^n - 1/2)(2^{n+1}-1)}{\Gamma(2^n)\varepsilon^{2^{n+1}-1}} \\
&= \Omega\left(\frac{1}{\varepsilon^{2^{n+1}-1}}\right)
\end{aligned}
$$

- We should therefore have

$$
\begin{aligned}
\text{poly}(n)^m &\geq \left(\frac{1}{\varepsilon^{2^{n+1}-1}}\right) \\
&\Downarrow \\
m &= \Omega\left(\frac{2^n \log(1/\varepsilon)}{\log n}\right)
\end{aligned}
$$

- Solovay-Kitaev $m = O\left(n^2 4^n \log^c(n^2 4^n/\varepsilon)\right)$