Introduction to Quantum Algorithms-Lecture 1

Costas Daskaloyannis

2015/16

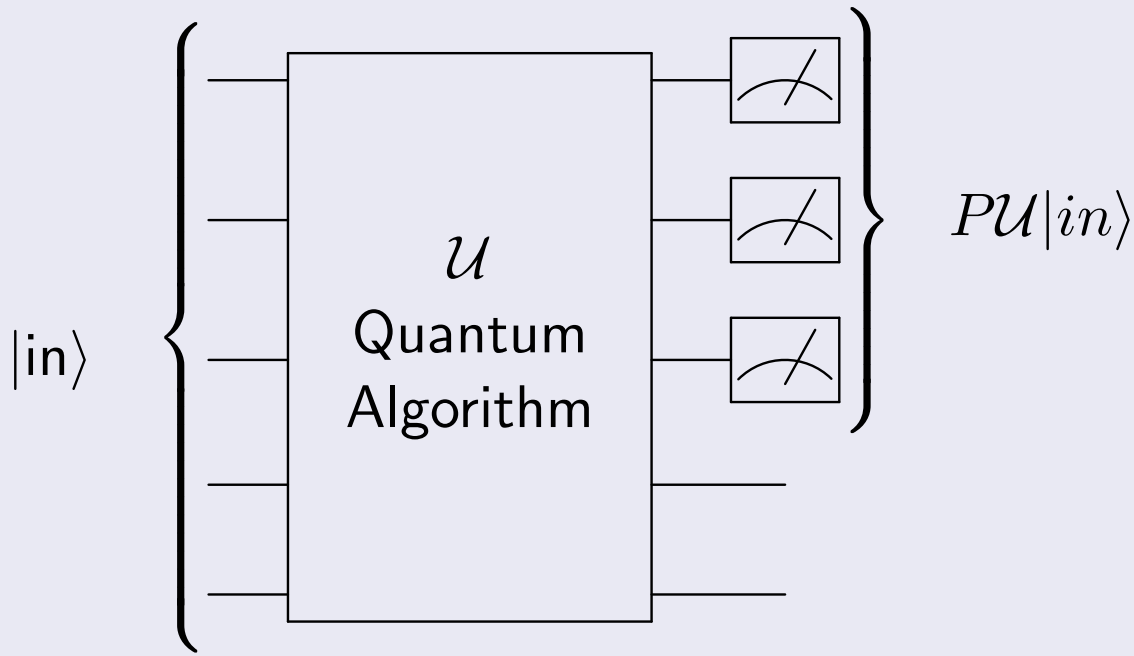
Contents

Definition: Quantum Algorithm

Quantum Algorithm is a unitary operator $\mathcal{U}$ acting on one input state $|\text{in}\rangle$ and a measure of the values of some q-bits in the output state.

$$|\text{in}\rangle \xrightarrow[\text{QuAlg}]{\mathcal{U}} \mathcal{U}|\text{in}\rangle \xrightarrow[\text{meas.}]{P} P\mathcal{U}|\text{in}\rangle$$

(P is the projection corresponding to the measure)



Necessary Steps to Construct a Quantum Algorithm

- Theory to construct an Unitary Operator $\mathcal{U}$ using Quantum Gates
  - (i) What are the set of necessary gates for the construction of any Unitary Operators ? (Universal Quantum Gates set)
  - (ii) How to construct one Unitary Operator from the set of Universal Quantum Gates?
- What are the Problems, which can be treated by applying a Quantum Algorithm?
  - (i) Oracles (Deutsch Algorithm)
  - (ii) Factorization (Shor Algorithm)
  - (iii) Searching (Grove Algorithm)

Universal Quantum Gates

Definition Universal Quantum Gates

Universal Quantum Gates $\equiv$ Set of gates such that, any unitary operator is approximated by a quantum circuit using only these gates

Theorem

The "two level" Unitary Matrices are Universal for the set of the Unitary Matrices

$$U \text{ unitary matrix} \quad \rightsquigarrow \quad U = V_1 V_2 \cdots V_N D$$

where V_k two level matrices and D a diagonal

Example for the 7×7 matrices

$$V_k = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & b & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & c & 0 & 0 & d & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Step 1

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

$$W_1 = \begin{pmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & -\frac{a}{\sqrt{|a|^2+|b|^2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad W_1 W_1^\dagger = \mathbb{I}$$

$$U_1 = W_1 U = \begin{pmatrix} a' & \bullet' & \bullet' & \bullet' \\ 0 & \bullet' & \bullet' & \bullet' \\ c & \bullet' & \bullet' & \bullet' \\ d & \bullet' & \bullet' & \bullet' \end{pmatrix}$$

Step 2

$$U_1 = \begin{pmatrix} a' & \bullet' & \bullet' & \bullet' \\ 0 & \bullet & \bullet' & \bullet' \\ c & \bullet' & \bullet' & \bullet' \\ d & \bullet' & \bullet' & \bullet' \end{pmatrix}, \; W_2 = \begin{pmatrix} \frac{(a')^*}{\sqrt{|a'|^2+|c|^2}} & 0 & \frac{(c)^*}{\sqrt{|a'|^2+|c'|^2}} & 0 \\ 0 & 1 & 0 & 0 \\ \frac{c}{\sqrt{|a'|^2+|c|^2}} & & -\frac{a'}{\sqrt{|a'|^2+|c|^2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$W_2 W_2^\dagger = \mathbb{I}, \; U_2 = W_2 U_1 = W_2 W_1 U = \begin{pmatrix} a'' & \bullet'' & \bullet'' & \bullet'' \\ 0 & \bullet'' & \bullet'' & \bullet'' \\ 0 & \bullet'' & \bullet'' & \bullet'' \\ d & \bullet'' & \bullet'' & \bullet'' \end{pmatrix}$$

$$W_3 W_3^\dagger = \mathbb{I}, \; U_3 = W_3 U_2 = W_3 W_2 W_1 U = \begin{pmatrix} a''' & \bullet''' & \bullet''' & \bullet''' \\ 0 & \bullet''' & \bullet''' & \bullet''' \\ 0 & \bullet''' & \bullet''' & \bullet''' \\ 0 & \bullet''' & \bullet''' & \bullet''' \end{pmatrix}$$

$$U_3 = \begin{pmatrix} a''' & \bullet_1''' & \bullet_1''' & \bullet_1''' \\ 0 & \bullet''' & \bullet''' & \bullet''' \\ 0 & \bullet''' & \bullet''' & \bullet''' \\ 0 & \bullet''' & \bullet''' & \bullet''' \end{pmatrix} \quad \text{is unitary matrix}$$

$$U_3 U_3^\dagger = \mathbb{I}, \rightsquigarrow \ |a'''|^2 = 1 \ \rightsquigarrow \ a''' = \mathrm{e}^{\mathrm{i}\phi_1}$$

$$U_3^\dagger U_3 = \mathbb{I}, \rightsquigarrow \ |a'''|^2 + |\bullet_1'''|^2 + |\bullet_1'''|^2 + |\bullet_1'''|^2 = 1 \ \rightsquigarrow \ \bullet_1''' = 0$$

$$U_3 = \left(\begin{array}{c|ccc} \mathrm{e}^{\mathrm{i}\phi_1} & 0 & 0 & 0 \\ \hline 0 & \bullet''' & \bullet''' & \bullet''' \\ 0 & \bullet''' & \bullet''' & \bullet''' \\ 0 & \bullet''' & \bullet''' & \bullet''' \end{array}\right) \quad \text{is unitary matrix}$$

$$U \longrightarrow U_1 \longrightarrow U_2 \longrightarrow U_3 \qquad \cdots\cdots \qquad \longrightarrow U_{2^n-1}$$

$$\begin{pmatrix} a & \bullet & \bullet & \bullet \\ b & \bullet & \bullet & \bullet \\ c & \bullet & \bullet & \bullet \\ d & \bullet & \bullet & \bullet \\ \vdots & \vdots & \vdots & \vdots \\ y & \bullet & \bullet & \bullet \\ z & \bullet & \bullet & \bullet \end{pmatrix} \rightarrow \begin{pmatrix} a' & \bullet & \bullet & \bullet \\ 0 & \bullet & \bullet & \bullet \\ c' & \bullet & \bullet & \bullet \\ d' & \bullet & \bullet & \bullet \\ \vdots & \vdots & \vdots & \vdots \\ y' & \bullet & \bullet & \bullet \\ z' & \bullet & \bullet & \bullet \end{pmatrix} \rightarrow \begin{pmatrix} a'' & \bullet & \bullet & \bullet \\ 0 & \bullet & \bullet & \bullet \\ 0 & \bullet & \bullet & \bullet \\ d'' & \bullet & \bullet & \bullet \\ \vdots & \vdots & \vdots & \vdots \\ y'' & \bullet & \bullet & \bullet \\ z'' & \bullet & \bullet & \bullet \end{pmatrix} \rightarrow \cdots\cdots \rightarrow \begin{pmatrix} \mathrm{e}^{\mathrm{i}\phi_1} & \bullet & \bullet & \bullet \\ 0 & \bullet & \bullet & \bullet \\ 0 & \bullet & \bullet & \bullet \\ 0 & \bullet & \bullet & \bullet \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \bullet & \bullet & \bullet \\ 0 & \bullet & \bullet & \bullet \end{pmatrix}$$

$$U_{2^n-1}^{\dagger} U_{2^n-1} = \mathbb{I} \rightsquigarrow U_{2^n-1} = \begin{pmatrix} \mathrm{e}^{\mathrm{i}\phi_1} & 0 & 0 & 0 & \cdots \\ 0 & \bullet & \bullet & \bullet & \cdots \\ 0 & \bullet & \bullet & \bullet & \cdots \\ 0 & \bullet & \bullet & \bullet & \cdots \\ \vdots & \vdots & \vdots & \vdots & \\ 0 & \bullet & \bullet & \bullet & \cdots \\ 0 & \bullet & \bullet & \bullet & \cdots \end{pmatrix}$$

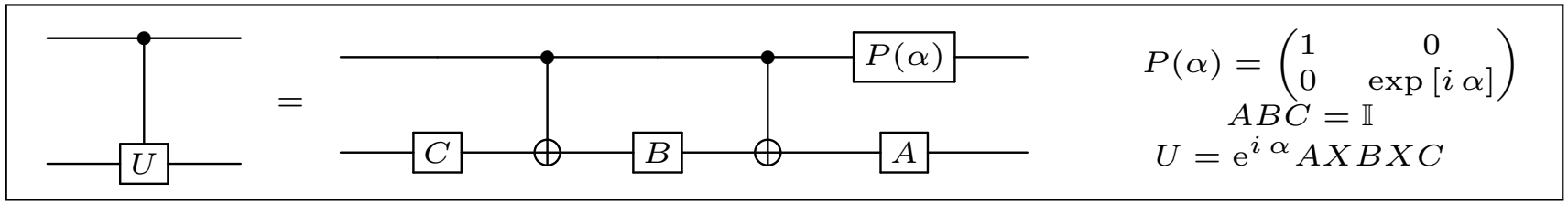
$$\begin{pmatrix} \bullet & \bullet & \bullet & \bullet & \cdots \\ \bullet & \bullet & \bullet & \bullet & \cdots \\ \bullet & \bullet & \bullet & \bullet & \cdots \\ \bullet & \bullet & \bullet & \bullet & \cdots \\ \vdots & \vdots & \vdots & \vdots & \\ \bullet & \bullet & \bullet & \bullet & \cdots \\ \bullet & \bullet & \bullet & \bullet & \cdots \end{pmatrix} \rightarrow \begin{pmatrix} e^{i\phi_1} & 0 & 0 & 0 & \cdots \\ 0 & \bullet & \bullet & \bullet & \cdots \\ 0 & \bullet & \bullet & \bullet & \cdots \\ 0 & \bullet & \bullet & \bullet & \cdots \\ \vdots & \vdots & \vdots & \vdots & \\ 0 & \bullet & \bullet & \bullet & \cdots \\ 0 & \bullet & \bullet & \bullet & \cdots \end{pmatrix} \rightarrow$$

$$\rightarrow \begin{pmatrix} e^{i\phi_1} & 0 & 0 & 0 & \cdots \\ 0 & e^{i\phi_2} & 0 & 0 & \cdots \\ 0 & 0 & \bullet & \bullet & \cdots \\ 0 & 0 & \bullet & \bullet & \cdots \\ \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & \bullet & \bullet & \cdots \\ 0 & 0 & \bullet & \bullet & \cdots \end{pmatrix} \cdots \rightarrow \begin{pmatrix} e^{i\phi_1} & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & e^{i\phi_2} & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & e^{i\phi_3} & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & e^{i\phi_4} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & 0 & \cdots & e^{i\phi_{N-1}} & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & e^{i\phi_N} \end{pmatrix}$$

$$W_m W_{m-1} \cdots\cdots W_3 W_2 W_1 U = D \rightsquigarrow$$

$$\rightsquigarrow \quad \boxed{U = V_1 V_2 V_3 \cdots\cdots V_m D} \qquad V_k = W_k^{-1} = W_k^{\dagger}$$

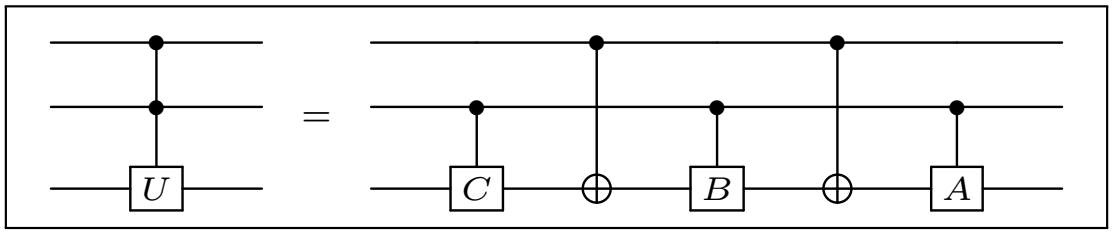
Any Control $C^n(U)$ gate is analyzed in one q-bit gates and and control-NOT gates

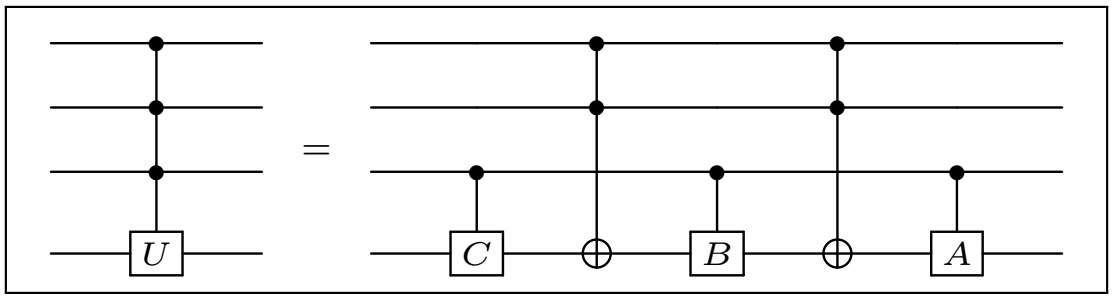


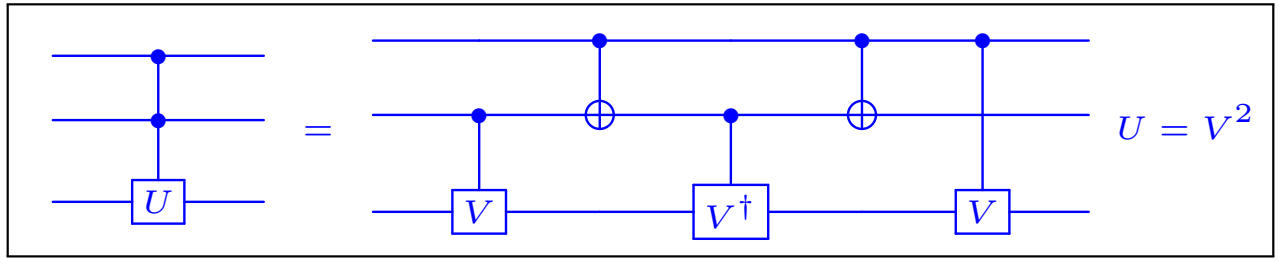
$$P(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & \exp[i\,\alpha] \end{pmatrix}$$

$$ABC = \mathbb{I}$$

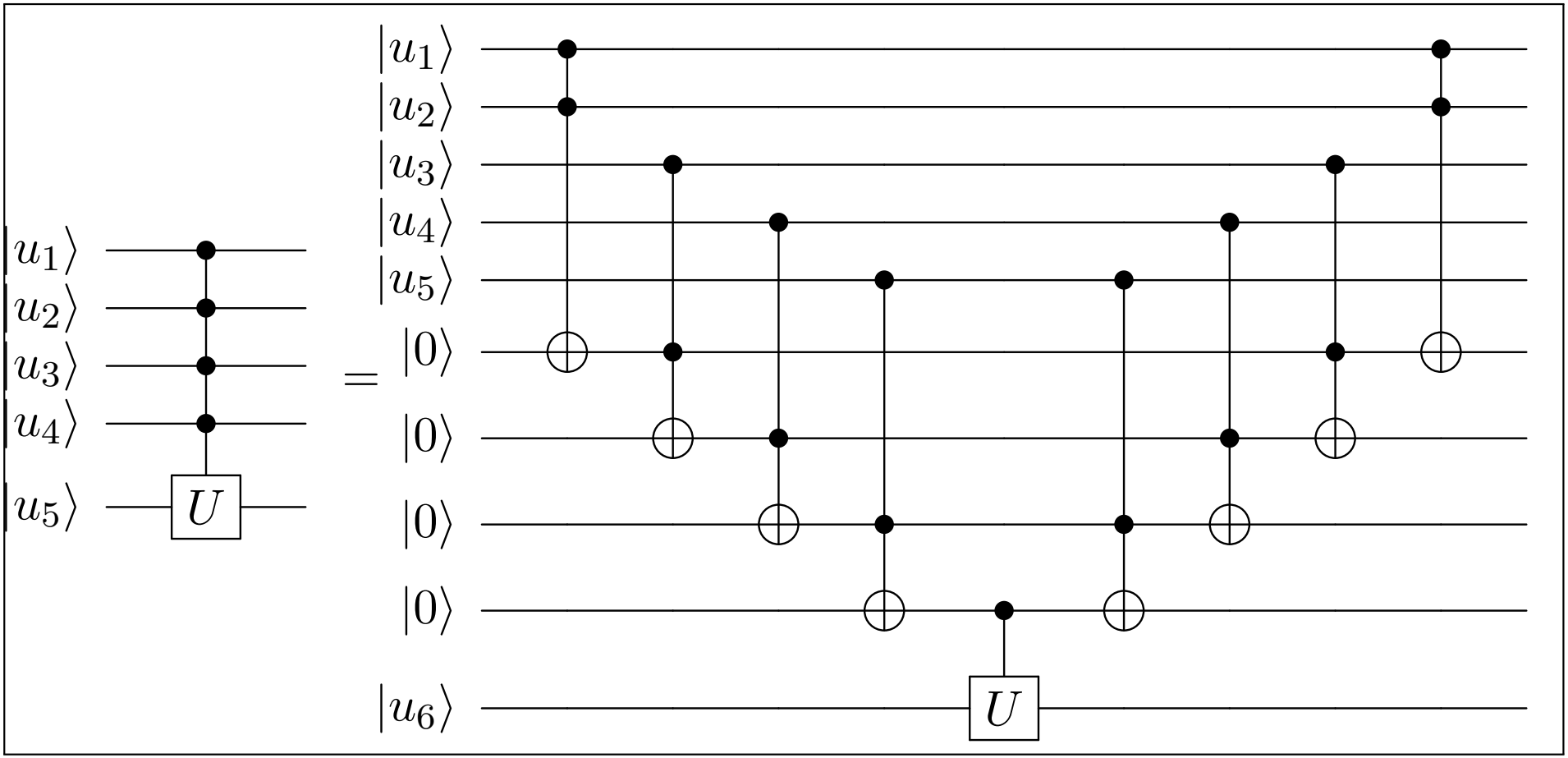
$$U = \mathrm{e}^{i\,\alpha} AXBXC$$







For the Toffoli gate $V = \frac{1-i}{2}\left(\mathbb{I} + i\,X\right)$


$|u_1\rangle$
$|u_2\rangle$
$|u_3\rangle$
$|u_4\rangle$
$|u_5\rangle$
U
=
$|u_1\rangle$
$|u_2\rangle$
$|u_3\rangle$
$|u_4\rangle$
$|u_5\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|u_6\rangle$
U

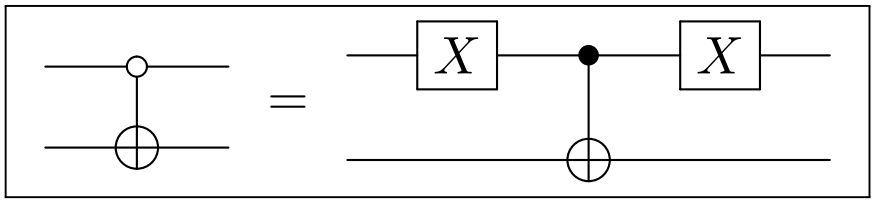
Corollary: Structure of n q-bit gates

Any n q-bit gate (i.e. 2^n Unitary Matrices) can be analyzed in two level matrices and diagonal matrices

Corollary: Structure of control $C^n(U)$ gates

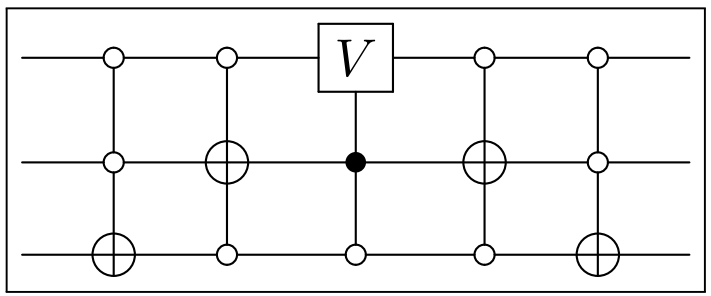
Any control $C^n(U)$ gate can be analyzed by a quantum circuit containing one-qbit and control-NOT gates

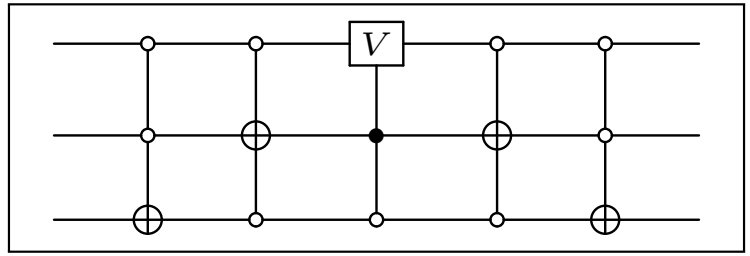
Gray Codes- Gate analysis of a two-level matrix

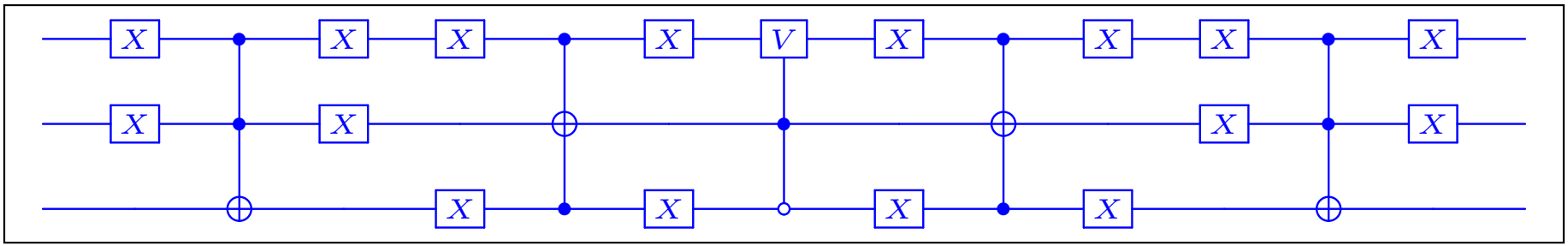


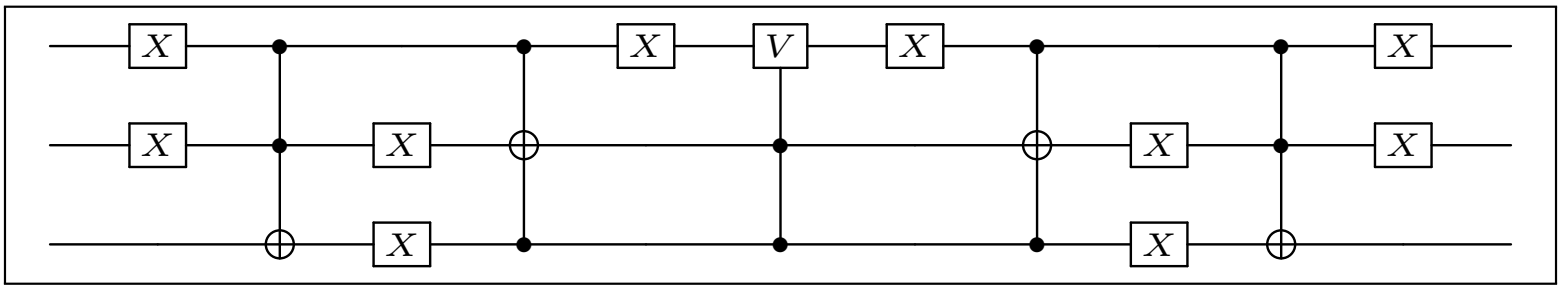
$$V_{[\overline{1},\overline{6}]} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & c & 0 & 0 & 0 & 0 & d & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad V = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

	Gray code	
initial	001	$\lvert\overline{1}\rangle$
	000	$\lvert\overline{0}\rangle$
	010	$\lvert\overline{2}\rangle$
final	110	$\lvert\overline{6}\rangle$



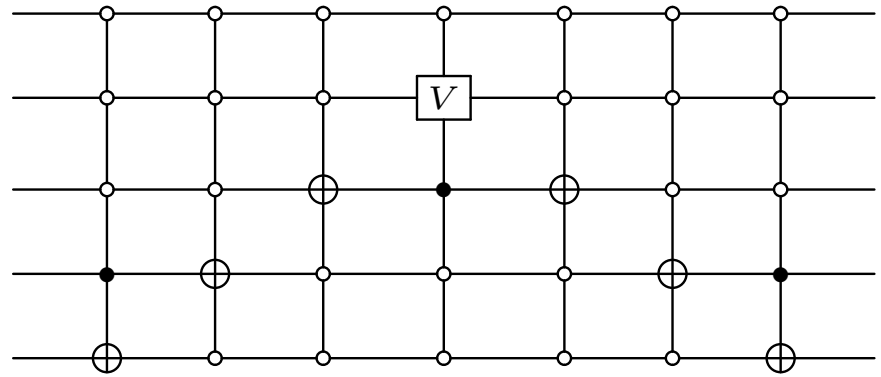

V


X
X
X
X
X
X
V
X
X
X
X
X
X
X
X
X
X
X
X
X
X
X
X
X


X
X
X
X
X
V
X
X
X
X
X
X
X
X
X
X

initial	$\|00011\rangle$	$\|\overline{3}\rangle$
	$\|00010\rangle$	$\|\overline{2}\rangle$
	$\|00000\rangle$	$\|\overline{0}\rangle$
	$\|00100\rangle$	$\|\overline{4}\rangle$
final	$\|01100\rangle$	$\|\overline{12}\rangle$

$\leftrightsquigarrow$ $V_{[\overline{3},\overline{12}]} =$

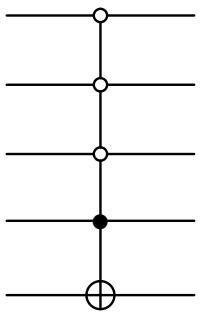


Definition: Gray Code

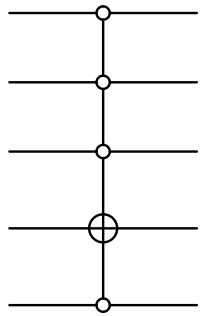
A list of binary numbers, such that any adjacent numbers differ by one bit

ex. $|\overline{3}\rangle \to |\overline{2}\rangle \to |\overline{0}\rangle \to |\overline{4}\rangle \to |\overline{12}\rangle$

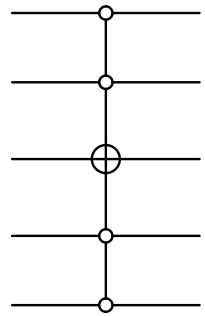
$|\overline{3}\rangle \to |\overline{2}\rangle$
$|00011\rangle \to |00010\rangle$



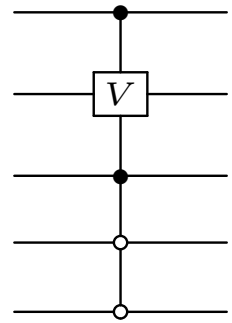
$|\overline{2}\rangle \to |\overline{0}\rangle$
$|00010\rangle \to |00000\rangle$



$|\overline{0}\rangle \to |\overline{4}\rangle$
$|00000\rangle \to |00100\rangle$



$|\overline{4}\rangle \to |\overline{12}\rangle$
$|00100\rangle \to |01100\rangle$



Corollary: Structure of n q-bit gates

Any n q-bit gate (i.e. 2^n Unitary Matrices) can be analyzed in two level and diagonal matrices

Corollary: Structure of control $C^n(U)$ gates

Any control $C^n(U)$ gate can be analyzed by a quantum circuit containing one-qbit and control-NOT gates

Corollary: Structure of level two gates

Any control two level gate can be analyzed by a quantum circuit containing one-qbit and control-NOT gates

Theorem: The one-qbit and control-NOT gates are Universal Gates

Any gate can be analyzed by a quantum circuit containing one-qbit and control-NOT gates

The Deutsch Oracle

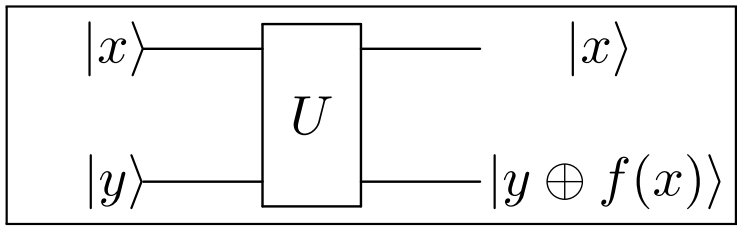
This oracle (Deutsch 1989) answers the following question:
Suppose we have a function

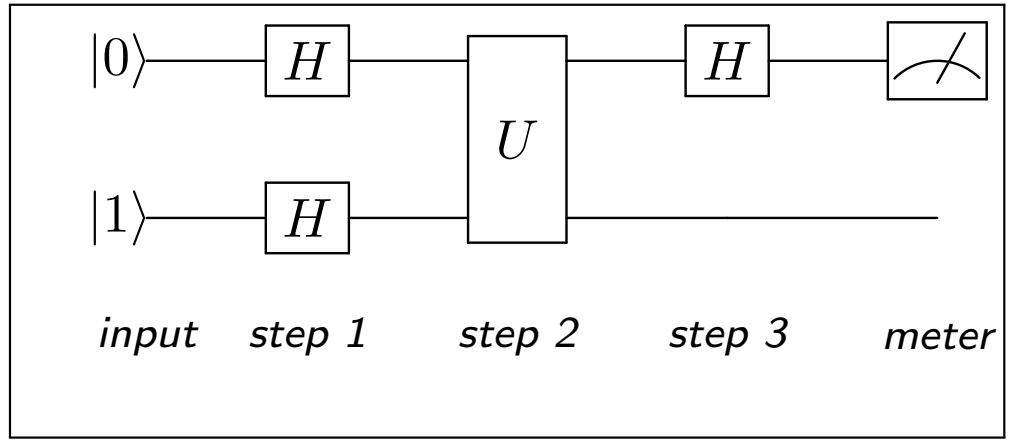
$$f : \{0, 1\} \to \{0, 1\}$$

which can be either **constant** or **balanced**.

The function is **constant if** $f(0) = f(1)$
balanced if $f(0) \neq f(1)$

Classically it would take **two evaluations** of the function to tell whether it is one or the other.
In **Quantum Mechanics** we need only **one quantum evaluation** of the function.





input		$\|0\rangle \otimes \|1\rangle$
step 1	$\mathbf{H} \otimes \mathbf{H}$	$\frac{\|0\rangle + \|1\rangle}{\sqrt{2}} \otimes \frac{\|0\rangle - \|1\rangle}{\sqrt{2}} = \frac{1}{2}\left(\|00\rangle - \|01\rangle + \|10\rangle - \|11\rangle\right)$
step2	$\mathbf{U}$	$\frac{1}{2}\left(\|0\rangle \otimes \|f(0)\rangle - \|0\rangle \otimes \|1 \oplus f(0)\rangle + \|1\rangle \otimes \|f(1)\rangle - \|1\rangle \otimes \|1 \oplus f(1)\rangle\right) =$ $= (-1)^{f(0)} \left(\delta_{f(0),f(1)} \frac{\|0\rangle + \|1\rangle}{\sqrt{2}} + \delta_{f(0),1\oplus f(1)} \frac{\|0\rangle - \|1\rangle}{\sqrt{2}}\right) \otimes \frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$
step3	$\mathbf{H} \otimes \mathbb{I}$	$\begin{cases} \text{if } f(0) = f(1) \rightsquigarrow \|0\rangle \otimes \frac{\|0\rangle - \|1\rangle}{\sqrt{2}} \\ \text{if } f(0) \neq f(1) \rightsquigarrow \|1\rangle \otimes \frac{\|0\rangle - \|1\rangle}{\sqrt{2}} \end{cases}$
measure		

$$D = (H \otimes \mathbb{I}) \cdot U \cdot (H \otimes H)$$

The Deutsch- Jozsa Oracle

This oracle (Deutsch-Jozsa 1992) answers the following question:
Suppose we have a function

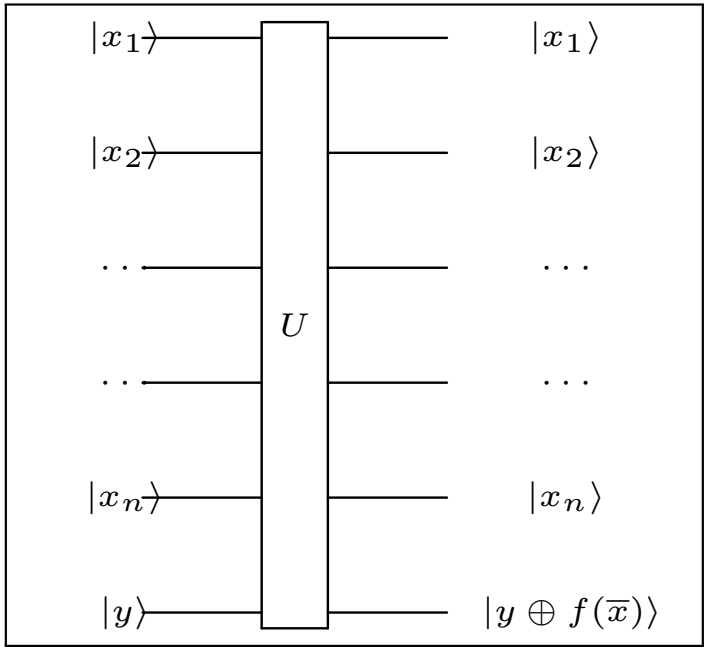
$$f : \{0,1\}^n \ni \overline{x} \rightarrow f(\overline{x}) \in \{0,1\}$$

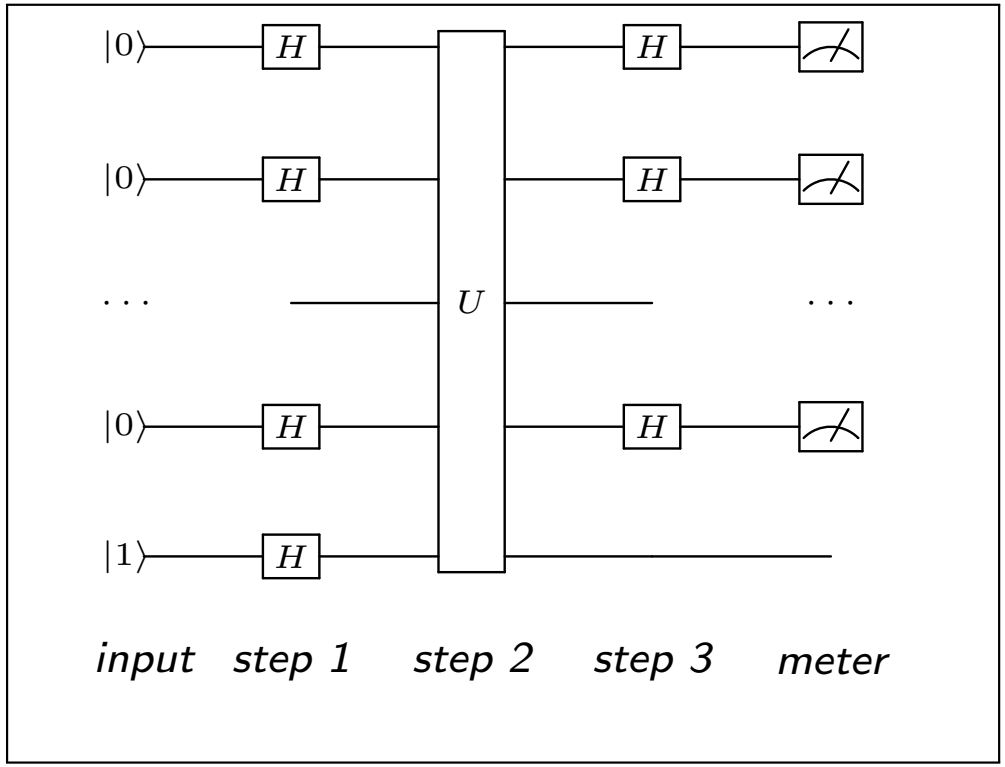
which can be either **constant** or **balanced**.

The function is
constant if $\forall\, \overline{x}$ **and** $\overline{y} \in \{0,1\}^n \rightsquigarrow f(\overline{x}) = f(\overline{y})$
balanced if the function is 0 **on half of its arguments and** 1 **on the other half**

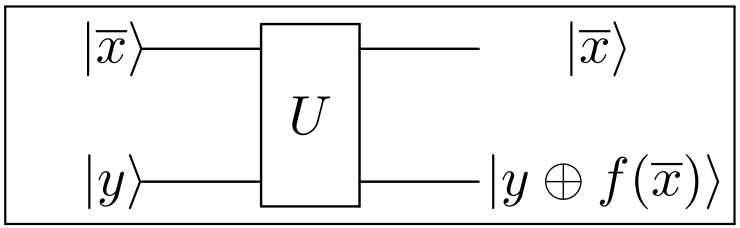
Classically it would take $\mathbf{2^{n-1}+1}$ **evaluations** of the function to tell whether it is one or the other.
In **Quantum Mechanics** we need only **one quantum evaluation** of the function.

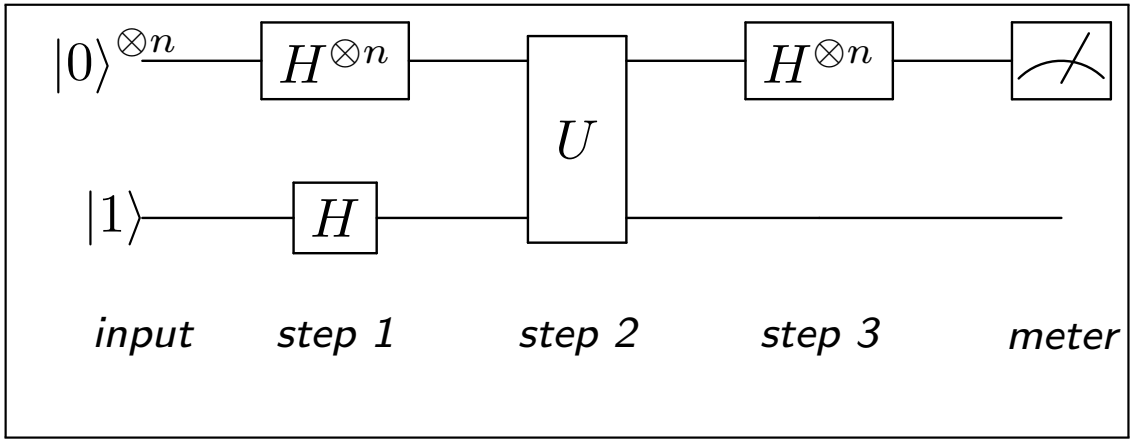
$$H^{\otimes n}\left|\overline{0}\right\rangle = \left(\frac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}}\right)^{\otimes n} = \frac{1}{\sqrt{2^{n+1}}}\sum_{k=0}^{2^n-1}\left|\overline{k}\right\rangle$$





$$D = (H^{\otimes n} \otimes \mathbb{I}) \cdot U \cdot (H^{\otimes n} \otimes H)$$





input		$\|0\rangle \otimes \|1\rangle$
step 1	$\mathbf{H^{\otimes n} \otimes H}$	$\left(\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}\right)^{\otimes n} \otimes \frac{\|0\rangle - \|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2^{n+1}}} \sum_{k=0}^{2^n-1} (\|k\rangle \otimes \|0\rangle - \|k\rangle \otimes \|1\rangle)$
step2	$\mathbf{U}$	$\frac{1}{\sqrt{2^{n+1}}} \left(\sum_{k=0}^{2^n-1} \|\mathbf{k}\rangle \otimes \|\mathbf{f(k)}\rangle\right) - \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{\ell=0}^{2^n-1} \|\ell\rangle \otimes \|\mathbf{1} \oplus \mathbf{f}(\ell)\rangle\right) =$ $= \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{k, f(k)=0} \|\mathbf{k}\rangle - \sum_{\ell, f(\ell)=1} \|\ell\rangle\right) \otimes \|\mathbf{0}\rangle +$ $+ \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{k, f(k)=1} \|\mathbf{k}\rangle - \sum_{\ell, f(\ell)=0} \|\ell\rangle\right) \otimes \|\mathbf{1}\rangle$
step3	$\mathbf{H^{\otimes n} \otimes \mathbb{I}}$	$\begin{cases} \text{if } f(k) \text{ constant } \rightsquigarrow \pm\|\overline{0}\rangle \otimes \frac{\|0\rangle - \|1\rangle}{\sqrt{2}} \end{cases}$
measure		

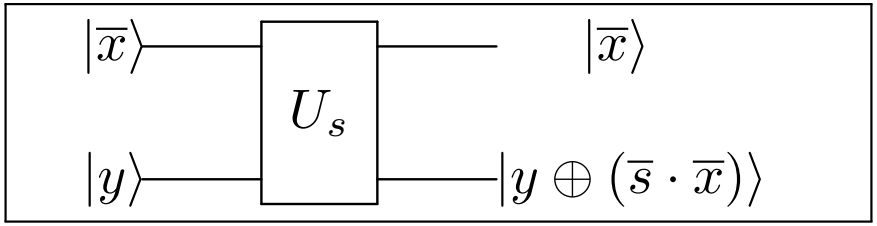
$$D = (H^{\otimes n} \otimes \mathbb{I}) \cdot U \cdot (H^{\otimes n} \otimes H)$$

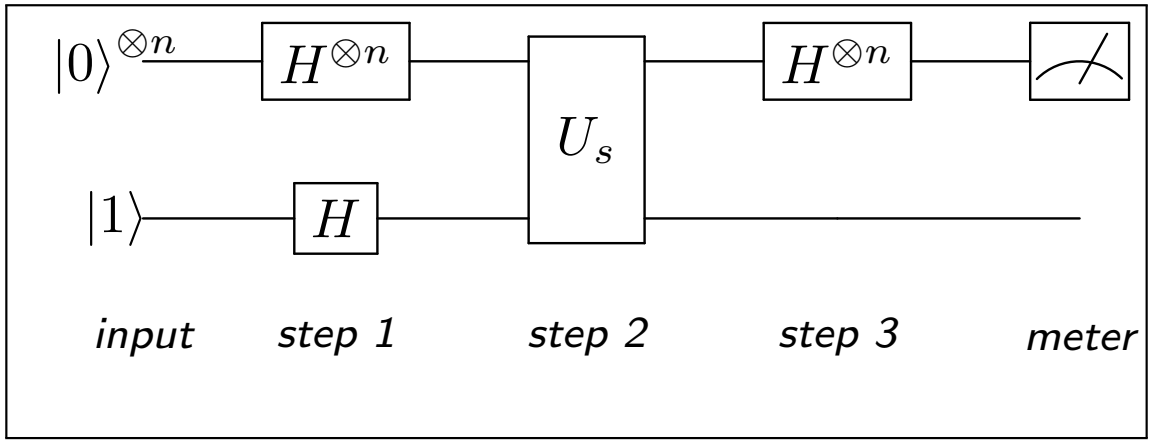
The Bernstein-Vazirani Oracle

This oracle answers the following question:
Suppose we have a function

$$f : \{0,1\}^n \ni \overline{x} \rightarrow f(\overline{x}) = \overline{s} \cdot \overline{x} \in \{0,1\}$$

Find $\overline{s}$
Classically it would take $\mathbf{2^n}$ **evaluations** of the function to find $\overline{s}$
In **Quantum Mechanics** we need only **one quantum evaluation** of the function.





The result of the measure is $\overline{s}$