Amsterdam University of Applied Sciences

Quantum Computing Introduction

Basic Quantum Algorithms

Bernardo Villalba Frías, PhD

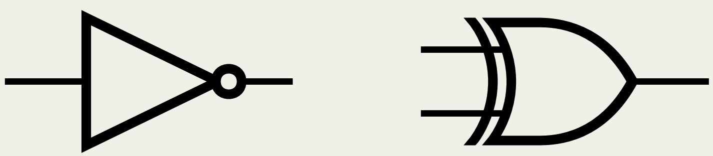
b.r.villalba.frias@hva.nl

Classic computing

- n bits can be in N exclusive states:
  - $n \rightarrow$ Number of bits
  - $N \rightarrow 2^n$
- Logic gates are non–reversible

NOT/XOR

No interesting computational power



NAND/NOR

Universal logic gates

- Chips (NAND) $\rightarrow$ Efficient transistor implementation

Quantum computing

- n qubits can be in a superposition of N states
  - $n \rightarrow$ Number of bits
  - $N \rightarrow 2^n$
- n qubits store N complex probability amplitudes
- In vector notation:
  - N–D complex vector space
  - Known as the Hilbert space:

"Hilbert space is a big place!"

Gate groups

Pauli gates

- Finite group
- Single–qubit only
- I, X, Y, Z

Clifford gates

- Finite group
- Single– and two–qubit
- E.g. H, S, CNOT, CZ

Non–Clifford gates

- Infinite group
- Single– and multi–qubit only
- E.g. Toffoli, T, Rx, Ry, Rz

Gate groups

Pauli gates

- Finite group
- Single–qubit only
- I, X, Y, Z

No interesting computational capabilities

Clifford gates

- Finite group
- Single– and two–qubit
- E.g. H, S, CNOT, CZ

Includes Pauli group

Superposition and *entanglement*

Can be *simulated efficiently* by classic computers

Non–Clifford gates

- Infinite group
- Single– and multi–qubit only
- E.g. Toffoli, T, Rx, Ry, Rz

Required for *universal quantum computing*

Exponentially hard to simulate

Universal set of gates

Amsterdam University of Applied Sciences

- A set of gates that can be used to implement an arbitrary unitary operation on any number of qubits
- Required:
  - Full Clifford group (and Pauli group)
  - One or more non–Clifford gates
- A standard choice:

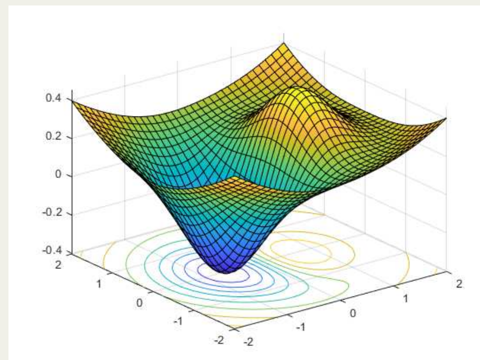
$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \qquad T = \begin{bmatrix}1 & 0\\ 0 & e^{\frac{\pi}{4}i}\end{bmatrix} \qquad \mathit{CNOT} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

  - It may require MANY of these gates!

Applications

- Promise to solve problems intractable by classic computers

Simulation



Optimization

En/Decryption

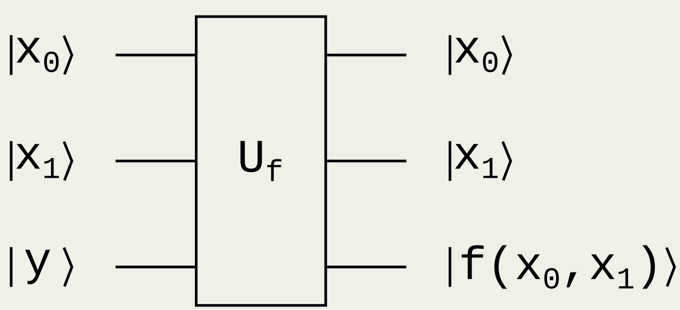
New drugs

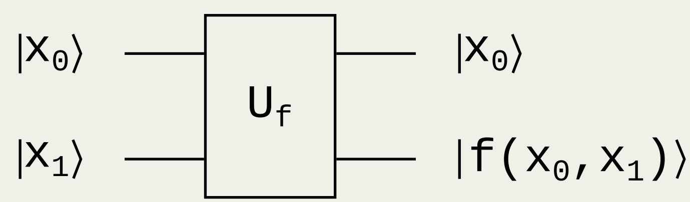
Catalyst analysis

Machine learning

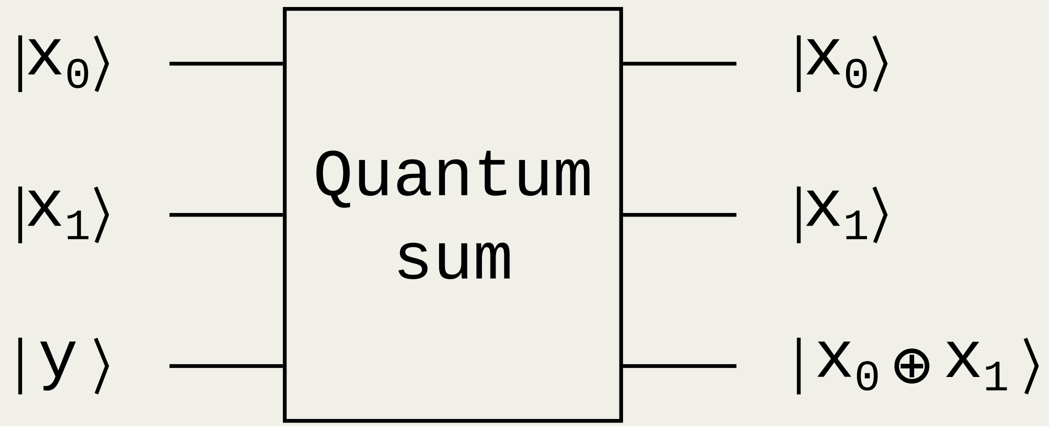
Quantum Arithmetic

- Quantum versions of classic arithmetic functions
  - Often based on X, CNOT, and Toffoli gates (CCNOT)
- Circuits are reversible
  - Number of input qubits = number of output qubits
  - y can be 0 (or any other value)

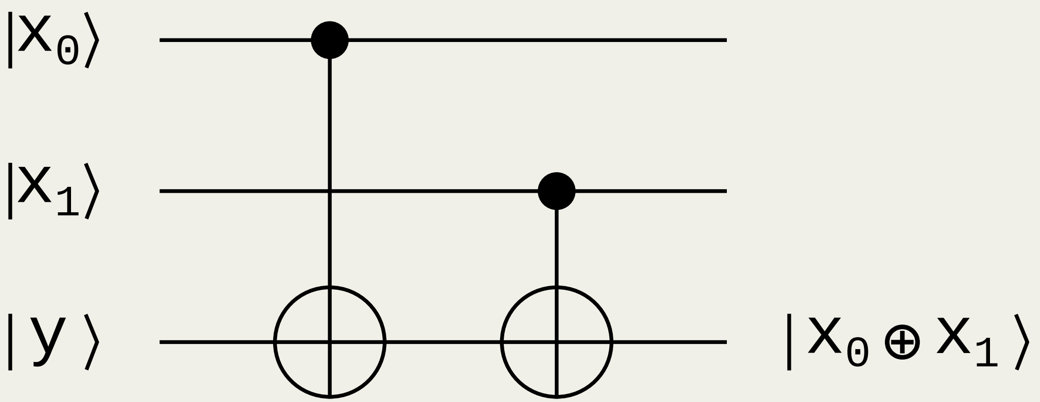




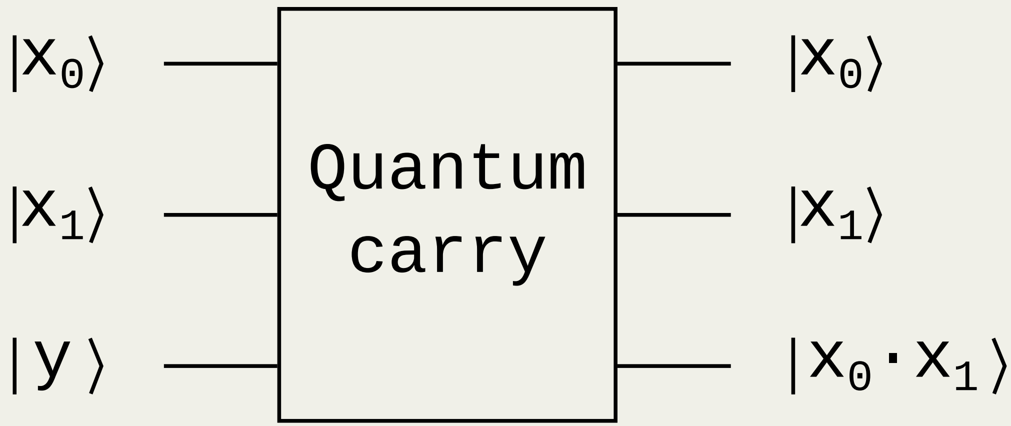
Quantum Sum



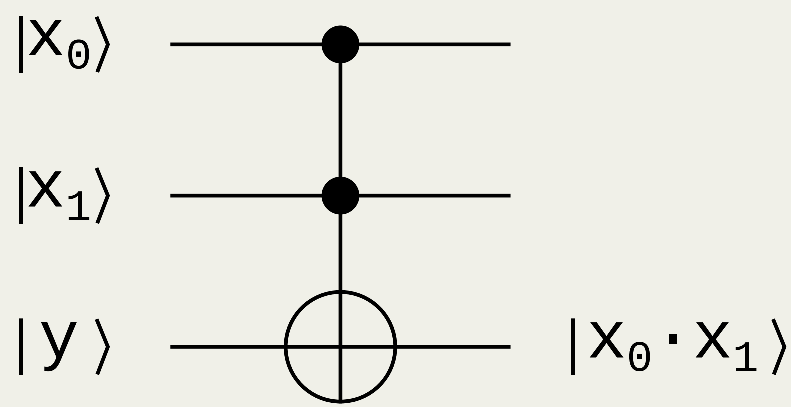
x_0	x_1	s
0	0	0
0	1	1
1	0	1
1	1	0



Quantum Carry



x_0	x_1	c
0	0	0
0	1	0
1	0	0
1	1	1



Question # 4

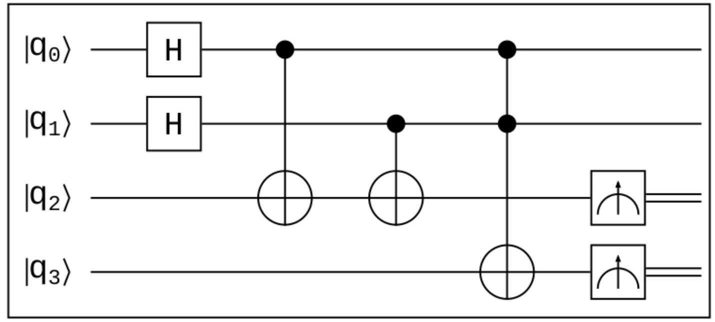


Figure 3: An arbitrary quantum circuit.

Question 4 *Consider the quantum circuit presented in Figure 3 and assume* $|q_3q_2q_1q_0\rangle = |0000\rangle$. *Determine, by using the Dirac notation, what is the state vector of the quantum circuit just before the measurement?*

`Write down your solution here:`

Single qubit functions

Amsterdam University of Applied Sciences

$$|x\rangle \;-\!\!\!-\!\!\!-\boxed{U_f}-\!\!\!-\!\!\!-\; |f(x)\rangle$$

- Very simple one–qubit functions
- Associated with a truth table:

Identity

$f_I(x) = x$

x	$f_I(x)$
0	0
1	1

NOT

$f_N(x) = \widetilde{x}$

x	$f_N(x)$
0	1
1	0

Set

$f_S(x) = 1$

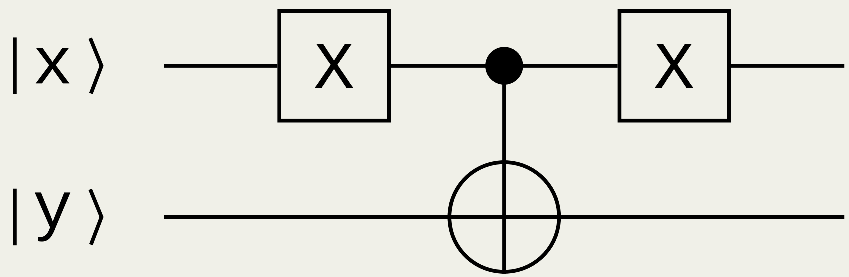
x	$f_S(x)$
0	1
1	1

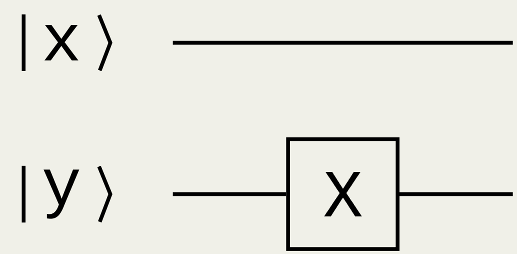
Reset

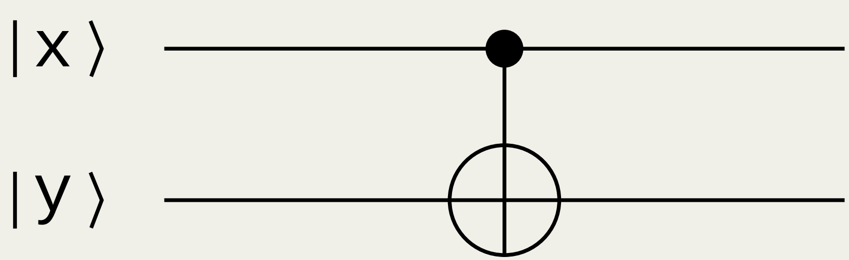
$f_R(x) = 0$

x	$f_R(x)$
0	0
1	0

Single qubit functions

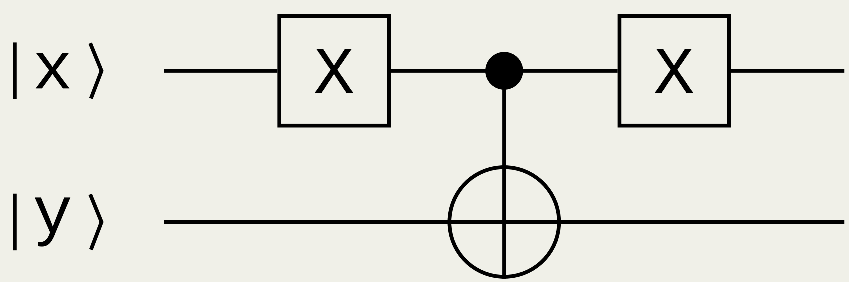




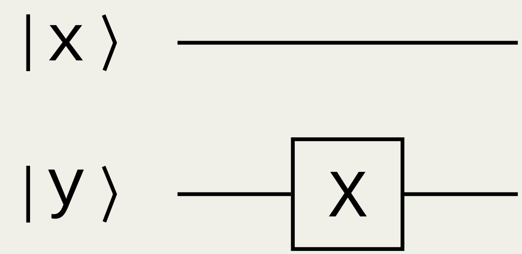


Single qubit functions

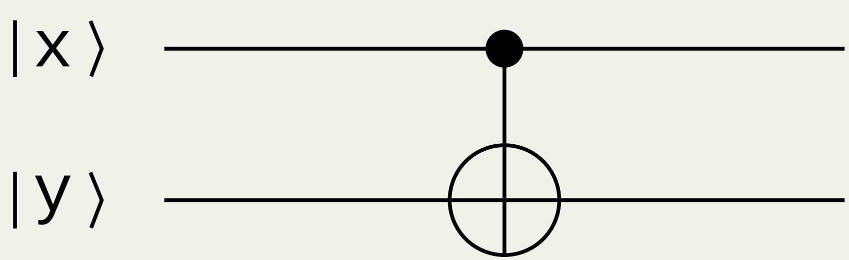
NOT
$f_N(x) = \widetilde{x}$



Set
$f_S(x) = 1$



Identity
$f_I(x) = x$



Reset
$f_R(x) = 0$

Single qubit functions

- A function whose output yields as many 0s as 1s over its input set is called: **balanced**

Balanced

Identity

$f_I(x) = x$

x	$f_I(x)$
0	0
1	1

NOT

$f_N(x) = \widetilde{x}$

x	$f_N(x)$
0	1
1	0

Constant

Set

$f_S(x) = 1$

x	$f_S(x)$
0	1
1	1

Reset

$f_R(x) = 0$

x	$f_R(x)$
0	0
1	0

Question # 6

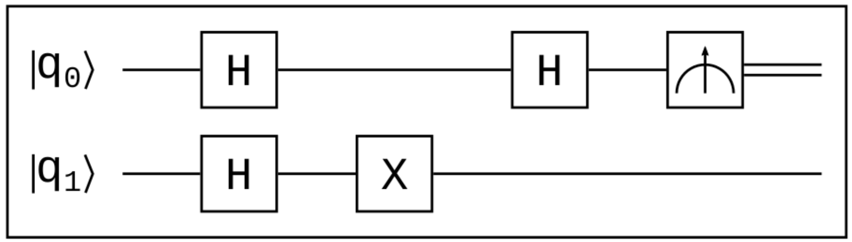


Figure 4: An arbitrary quantum circuit.

Question 6 *Consider the quantum circuit presented in Figure 4 and assume* $|q_1 q_0\rangle = |10\rangle$. *Determine, by using the matrix–vector multiplication, what is the state vector of the quantum circuit just before the measurement?*

`Write down your solution here:`

Deutsch’s problem

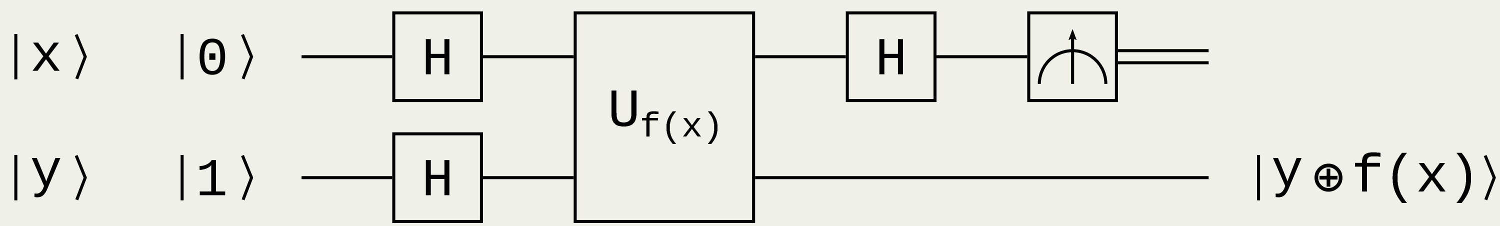
- Classic version:
  - You have a “**black box/oracle**” with one of the four one–bit functions, but you are not told which one. Determine if the function is: *balanced* or *constant*
    - Two calls to the “oracle” required

Deutsch's problem

Amsterdam University of Applied Sciences

- Quantum version:
  - You have a “**quantum black box/oracle**” with one of the four one–bit functions, but you are not told which one. Determine if the function is: *balanced* or *constant*
    - Can we do better? (i.e. less calls to the “quantum oracle”)

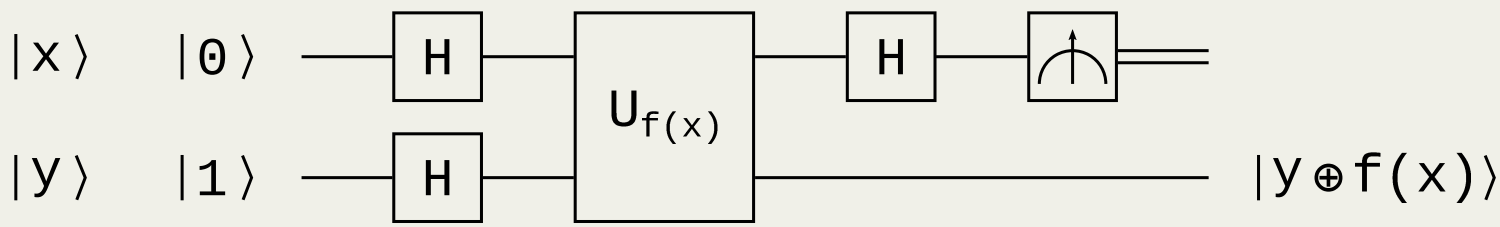
Deutsch's algorithm



$$
\begin{aligned}
&\rightarrow |10\rangle \\
H_x &\rightarrow \frac{1}{\sqrt{2}}\left(|10\rangle + |11\rangle\right) \\
H_y &\rightarrow \frac{1}{2}\left(|00\rangle - |10\rangle + |01\rangle - |11\rangle\right) \\
U_{f(x)} &\rightarrow \frac{1}{2}\left(|(0 \oplus f(0))0\rangle - |(1 \oplus f(0))0\rangle + |(0 \oplus f(1))1\rangle - |(1 \oplus f(1))1\rangle\right) \\
&\rightarrow \frac{1}{2}\Big(|f(0)0\rangle - |\widetilde{f(0)}0\rangle + |f(1)1\rangle - |\widetilde{f(1)}1\rangle\Big)
\end{aligned}
$$

- We do not know what $f(x)$ is, but...
- ... 2 options: balanced or constant

Deutsch’s algorithm

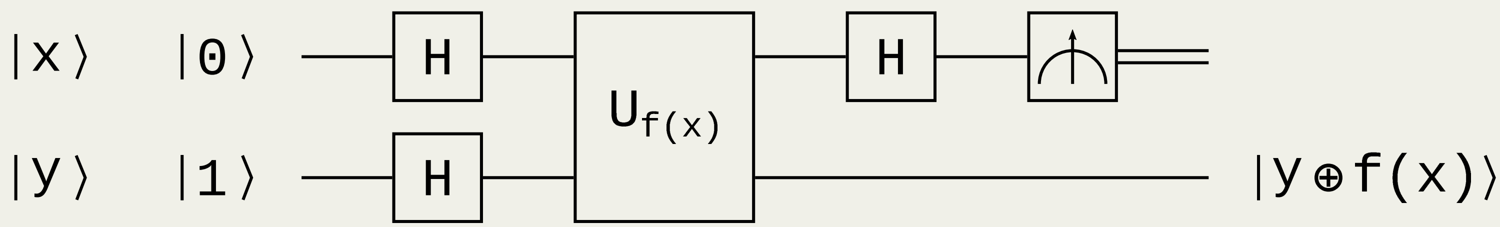


- If $f(x)$ is constant, then $f(0) = f(1) \wedge \widetilde{f(0)} = \widetilde{f(1)}$

$$
\begin{aligned}
&\rightarrow \frac{1}{2}\Big(|f(0)0\rangle - |\widetilde{f(0)}0\rangle + |f(1)1\rangle - |\widetilde{f(1)}1\rangle\Big)\\
&\rightarrow \frac{1}{2}\Big(|f(0)0\rangle + |f(0)1\rangle - |\widetilde{f(0)}0\rangle - |\widetilde{f(0)}1\rangle\Big)\\
&\rightarrow \frac{1}{2}\Big(\big(|f(0)\rangle \otimes \big(|0\rangle + |1\rangle\big)\big) - \big(|\widetilde{f(0)}\rangle \otimes \big(|0\rangle + |1\rangle\big)\big)\Big)\\
&\rightarrow \frac{1}{2}\Big(\big(|f(0)\rangle - |\widetilde{f(0)}\rangle\big) \otimes \big(|0\rangle + |1\rangle\big)\Big)\\
&\rightarrow \frac{1}{\sqrt{2}}\big(|f(0)\rangle - |\widetilde{f(0)}\rangle\big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)\\
H_x &\rightarrow \frac{1}{\sqrt{2}}\big(|f(0)\rangle - |\widetilde{f(0)}\rangle\big) \otimes |0\rangle
\end{aligned}
$$

Deutsch's algorithm

Amsterdam University of Applied Sciences



- If $f(x)$ is balanced, then $f(0) = \widetilde{f(1)} \wedge f(1) = \widetilde{f(0)}$

$$\rightarrow \frac{1}{2}\left(|f(0)0\rangle - |\widetilde{f(0)}0\rangle + |f(1)1\rangle - |\widetilde{f(1)}1\rangle\right)$$

$$\rightarrow \frac{1}{2}\left(|f(0)0\rangle - |f(0)1\rangle - |\widetilde{f(0)}0\rangle + |\widetilde{f(0)}1\rangle\right)$$

$$\rightarrow \frac{1}{2}\left(\left(|f(0)\rangle \otimes \left(|0\rangle - |1\rangle\right)\right) - \left(|\widetilde{f(0)}\rangle \otimes \left(|0\rangle - |1\rangle\right)\right)\right)$$

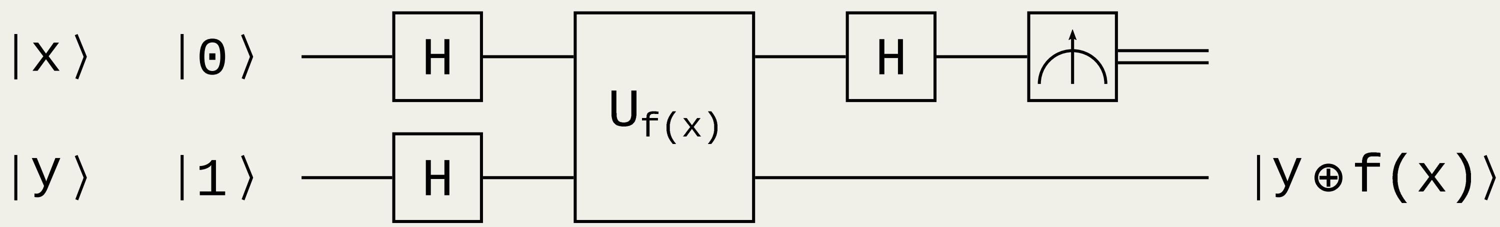
$$\rightarrow \frac{1}{2}\left(\left(|f(0)\rangle - |\widetilde{f(0)}\rangle\right) \otimes \left(|0\rangle - |1\rangle\right)\right)$$

$$\rightarrow \frac{1}{\sqrt{2}}\left(|f(0)\rangle - |\widetilde{f(0)}\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$H_x \rightarrow \frac{1}{\sqrt{2}}\left(|f(0)\rangle - |\widetilde{f(0)}\rangle\right) \otimes |1\rangle$$

Deutsch's algorithm

Amsterdam University of Applied Sciences



- Finally, measure the register x:
  - $M(x) = 0 \Rightarrow$ constant function
  - $M(x) = 1 \Rightarrow$ balanced function
- The result was in register x
  - Register y was not even measured!
- Only 1 call to the "quantum oracle"

Question # 8

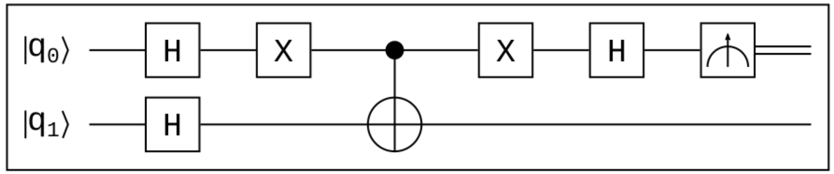
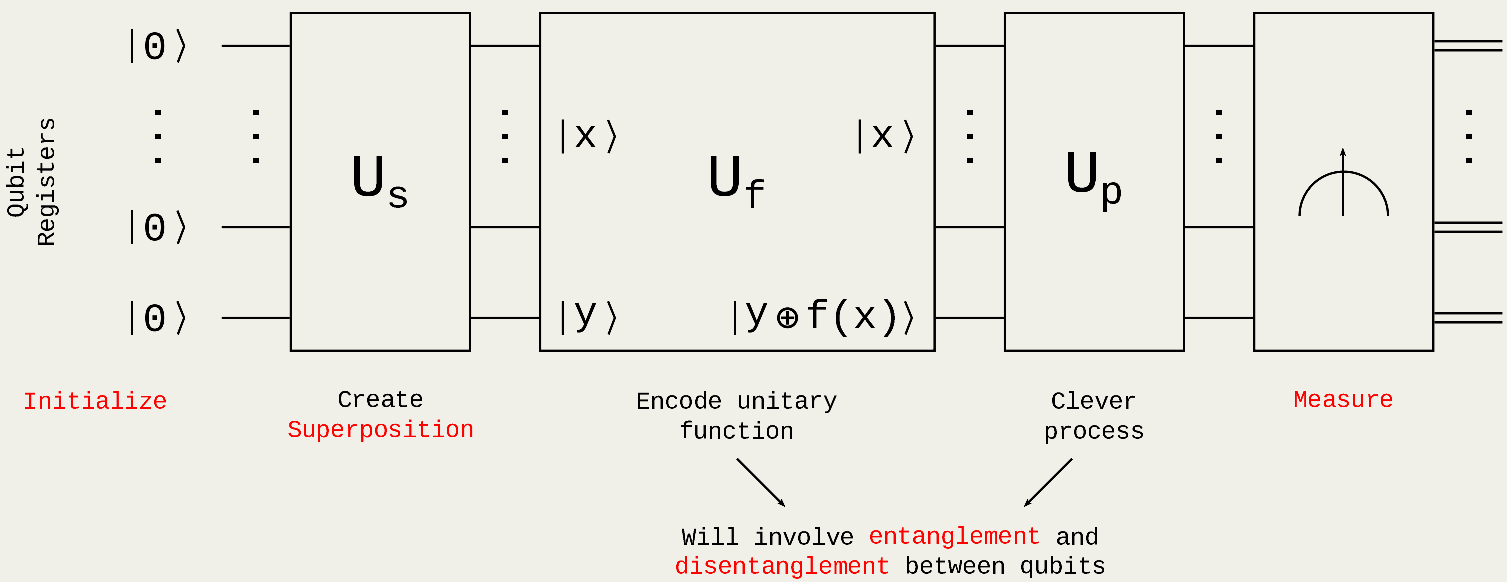


Figure 5: An arbitrary quantum circuit.

Question 8 *At this point, I assume that you noticed that Figure 4 represents the Deutsch circuit for a constant function. Likewise, the quantum circuit presented in Figure 5 represents the Deutsch circuit for a balanced function. Assume* $|q_1q_0\rangle = |10\rangle$ *and corroborate, by using the Dirac notation, that* $M(|q_0\rangle) = 1$ *with 100% probability.*

`Write down your solution here:`

Anatomy of a quantum algorithm



1. Start in superposition:
   - Parallelism: calculate for all inputs at once
2. Perform the desired function
3. Somehow, transform the result to computational basis states
   - The “magic” of a properly designed algorithm

What is next?

- Assignment is already available (check DLO)
- ESK Wiskunde lectures and workshops
- Q & A, Discussion
  - Questions about the assignment or the material
  - Feel free to propose any discussion
  - You can always write me an email


Questions?