Quantum Computation & Cryptography
Day 2

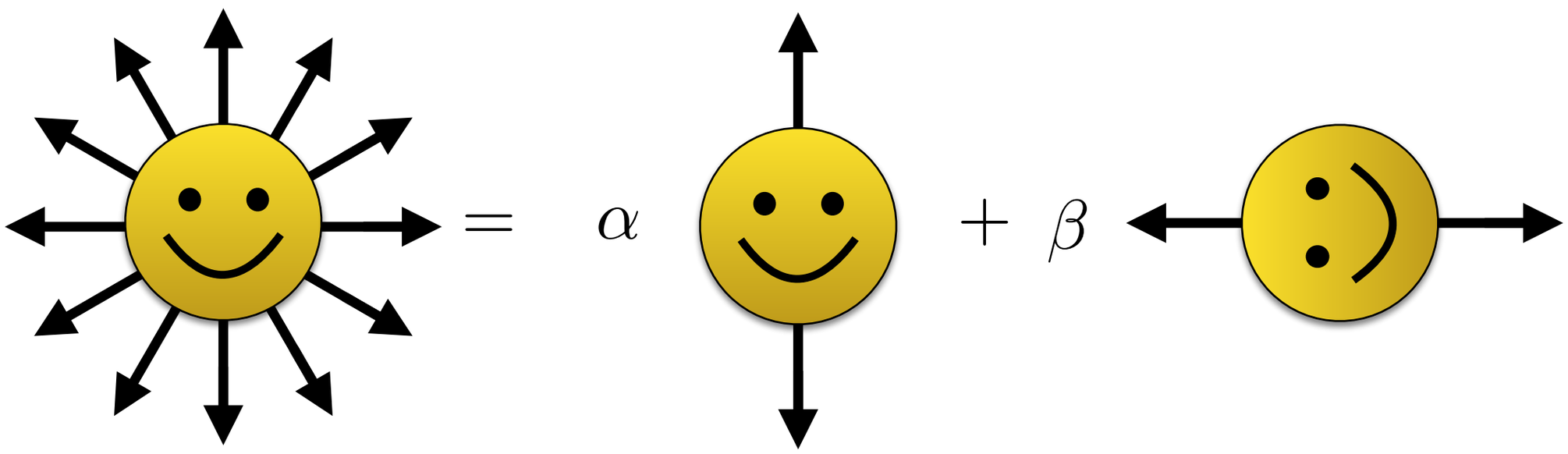
Quantum information basics

Andru Gheorghiu

Qubits

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$



$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Qubits

Consider the states:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\langle +|-\rangle =$$

Qubits

Consider the states:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\langle +|-\rangle = \frac{1}{\sqrt{2}}(\langle 0| + \langle 1|)\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Qubits

Consider the states:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\langle +|-\rangle = \frac{1}{2}(\langle 0| + \langle 1|)(|0\rangle - |1\rangle)$$

Qubits

Consider the states:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\langle +|-\rangle = \frac{1}{2}(\langle 0|0\rangle - \langle 0|1\rangle + \langle 1|0\rangle - \langle 1|1\rangle)$$

Qubits

Consider the states:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\langle +|-\rangle = \frac{1}{2}(1 - 0 + 0 - 1)$$

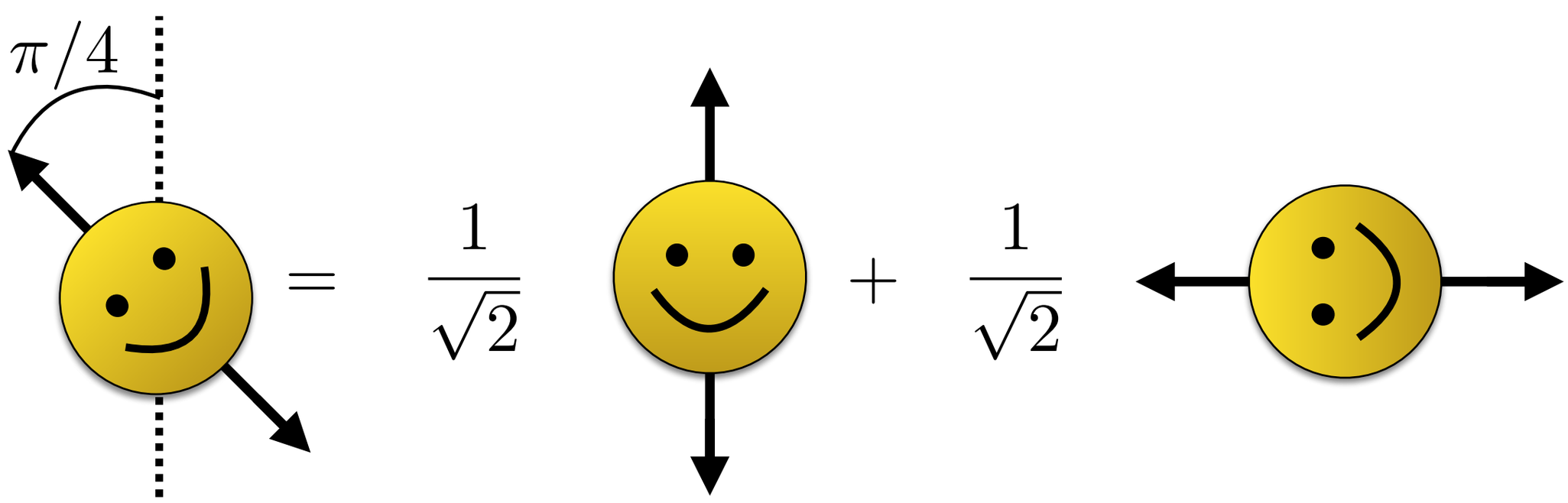
Qubits

Consider the states:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\langle +|-\rangle = 0 \;\; \langle -|+\rangle = 0 \;\; \langle +|+\rangle = 1 \;\; \langle -|-\rangle = 1$$

The states form an orthonormal basis!



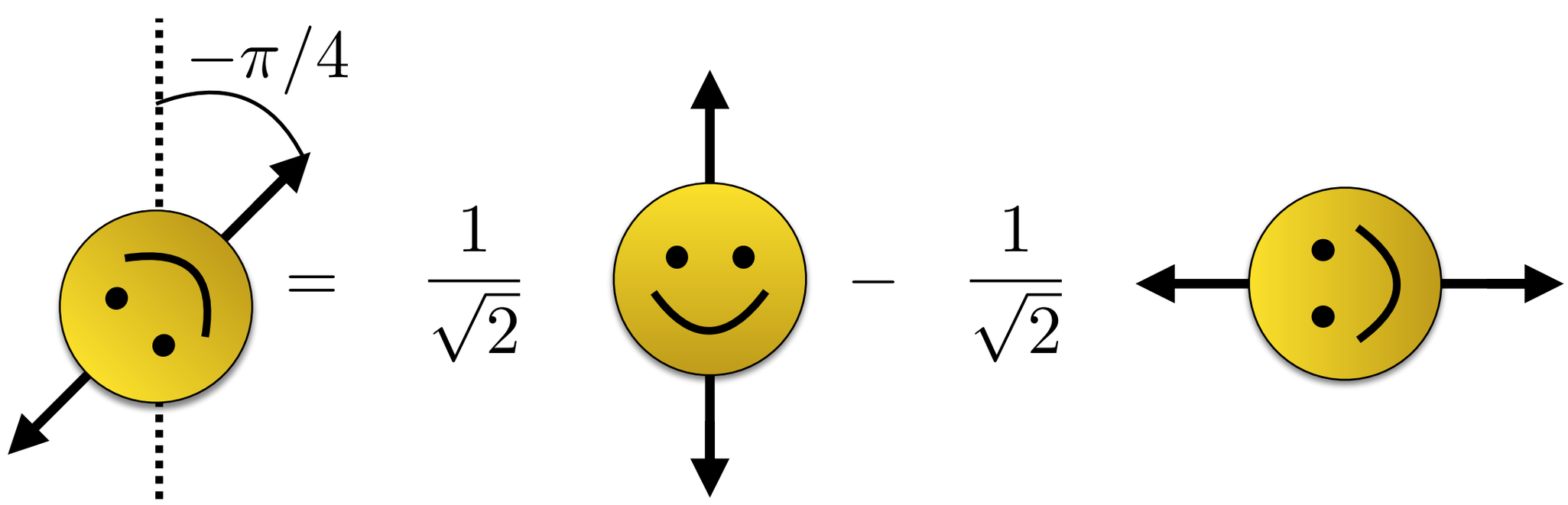
Qubits

Consider the states:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\langle +|-\rangle = 0 \;\; \langle -|+\rangle = 0 \;\; \langle +|+\rangle = 1 \;\; \langle -|-\rangle = 1$$

The states form an orthonormal basis!



Single-qubit unitaries

The X gate

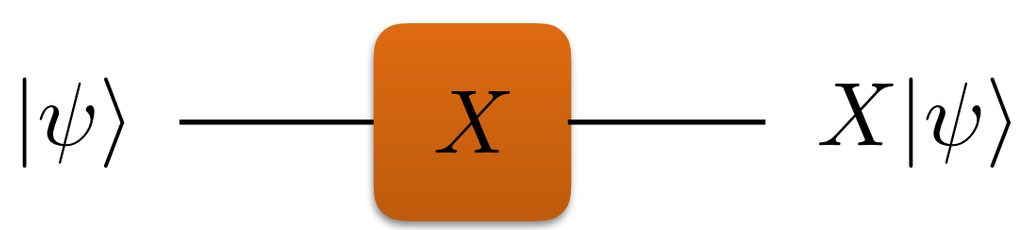
$$X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle$$

$$X|+\rangle = |+\rangle \qquad X|-\rangle = -|-\rangle$$

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

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$$



Single-qubit unitaries

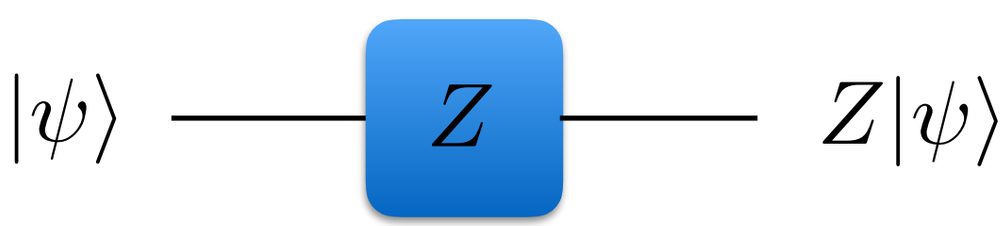
The Z gate

$$Z|0\rangle = |0\rangle \qquad Z|1\rangle = -|1\rangle$$

$$Z|+\rangle = |-\rangle \qquad Z|-\rangle = |+\rangle$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$



Single-qubit unitaries

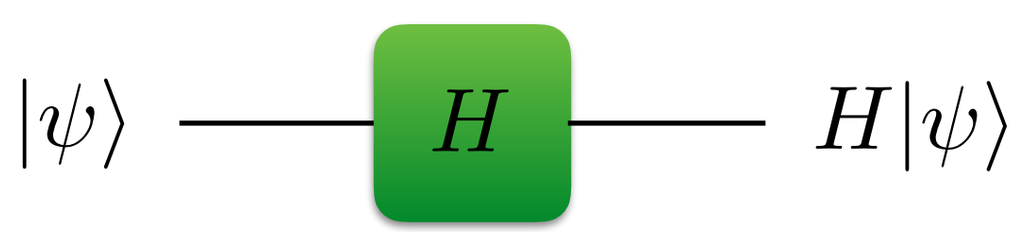
The H gate

$$H|0\rangle = |+\rangle \qquad H|1\rangle = |-\rangle$$

$$H|+\rangle = |0\rangle \qquad H|-\rangle = |1\rangle$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$H|\psi\rangle = \alpha|+\rangle + \beta|-\rangle$$



Single-qubit unitaries

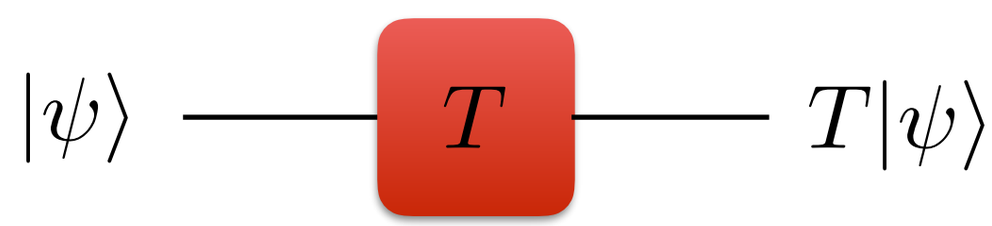
The T gate

$$T|0\rangle = |0\rangle \qquad T|1\rangle = e^{i\pi/4}|1\rangle$$

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

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$T|\psi\rangle = \alpha|0\rangle + \beta\, e^{i\pi/4}|1\rangle$$



The H, T gates are universal for single-qubit unitaries!

Two-qubit unitaries

The $CNOT$ gate

$$CNOT|00\rangle = |00\rangle \qquad CNOT|01\rangle = |01\rangle$$
$$CNOT|10\rangle = |11\rangle \qquad CNOT|11\rangle = |10\rangle$$

$$CNOT|x\rangle|y\rangle = |x\rangle|x \oplus y\rangle$$

$|x\rangle$ is called **control** qubit

$|y\rangle$ is called **target** qubit

Two-qubit unitaries

The $CNOT$ gate

$$CNOT|00\rangle = |00\rangle \qquad CNOT|01\rangle = |01\rangle$$
$$CNOT|10\rangle = |11\rangle \qquad CNOT|11\rangle = |10\rangle$$

$$CNOT|x\rangle|y\rangle = |x\rangle|x \oplus y\rangle$$

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

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$
$$CNOT|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + \delta|10\rangle$$

Two-qubit unitaries

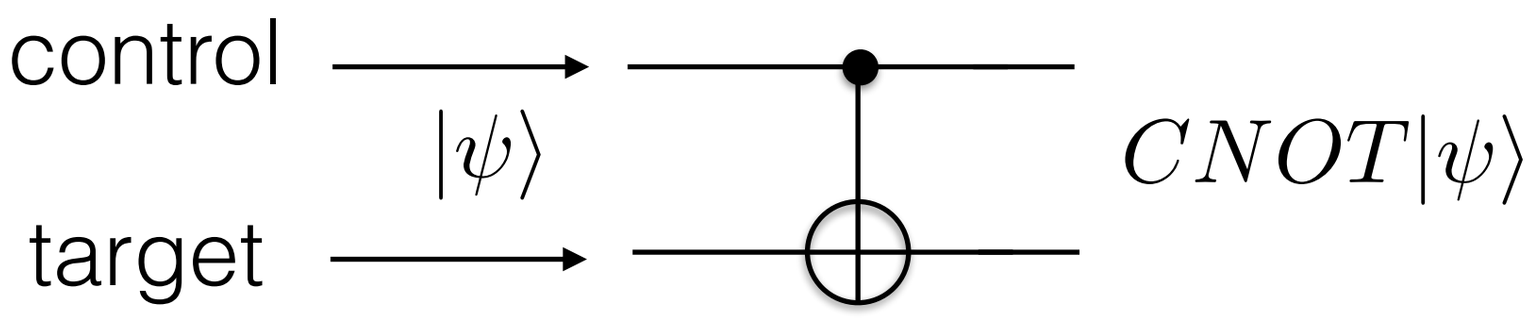
The $CNOT$ gate

$$CNOT \neq U_1 \otimes U_2$$

$$CNOT = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

$$|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$|1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$



Universality

Any N-qubit unitary can be approximated
to arbitrary precision with gates from the set:

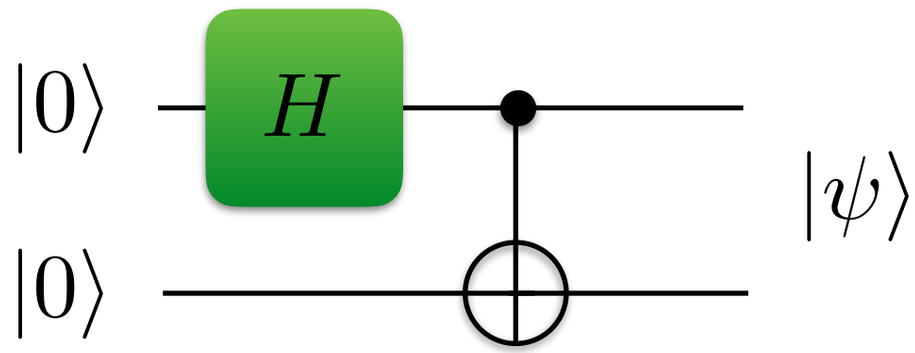
$$\{H, T, CNOT\}$$

This includes classical circuits as well!

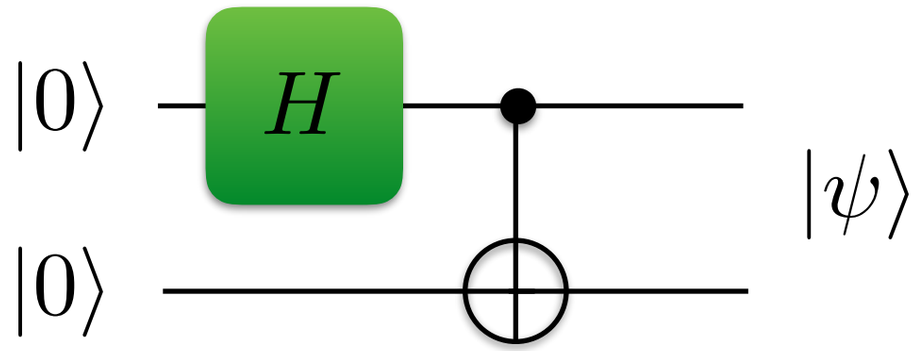
Quantum computers can implement
any classical computation efficiently

The classical computation will be reversible

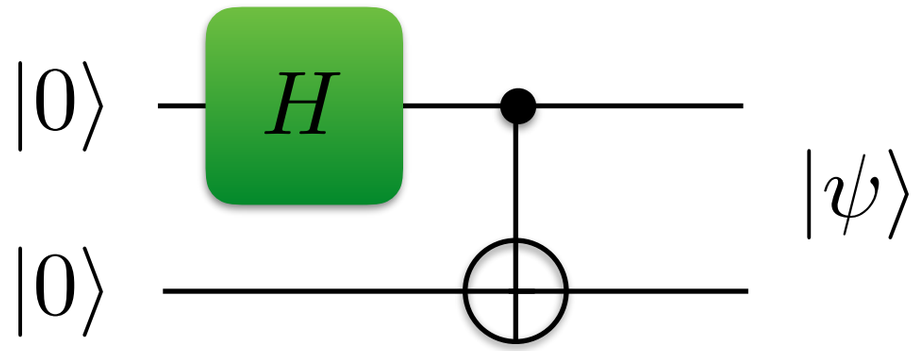
Let’s do some examples!



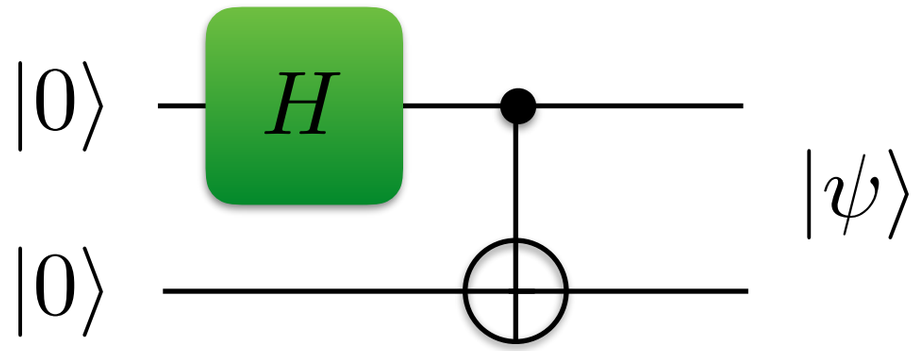
Input state	$|0\rangle|0\rangle$
After Hadamard	$|+\rangle|0\rangle$



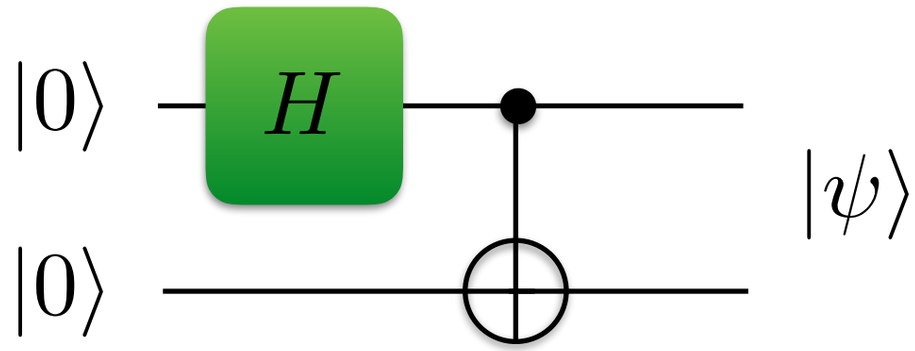
Input state	$\|0\rangle\|0\rangle$
After Hadamard	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\|0\rangle$



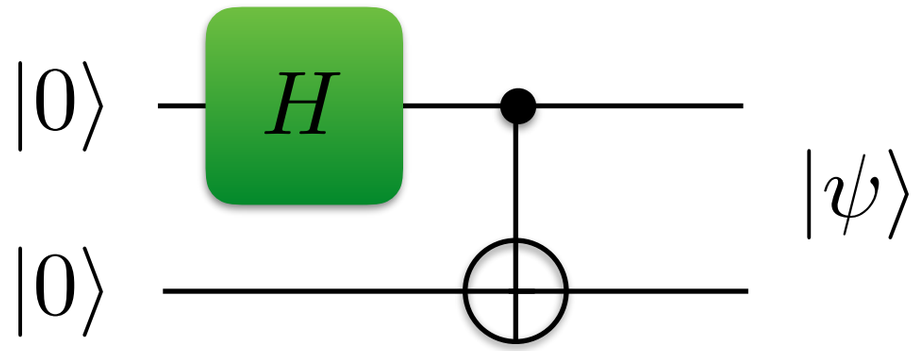
Input state	$\lvert 0\rangle\lvert 0\rangle$
After Hadamard	$\frac{1}{\sqrt{2}}(\lvert 0\rangle\lvert 0\rangle + \lvert 1\rangle\lvert 0\rangle)$



Input state	$\|0\rangle\|0\rangle$
After Hadamard	$\frac{1}{\sqrt{2}}(\|0\rangle\|0\rangle + \|1\rangle\|0\rangle)$
After CNOT	$\frac{1}{\sqrt{2}}(CNOT\|0\rangle\|0\rangle + CNOT\|1\rangle\|0\rangle)$



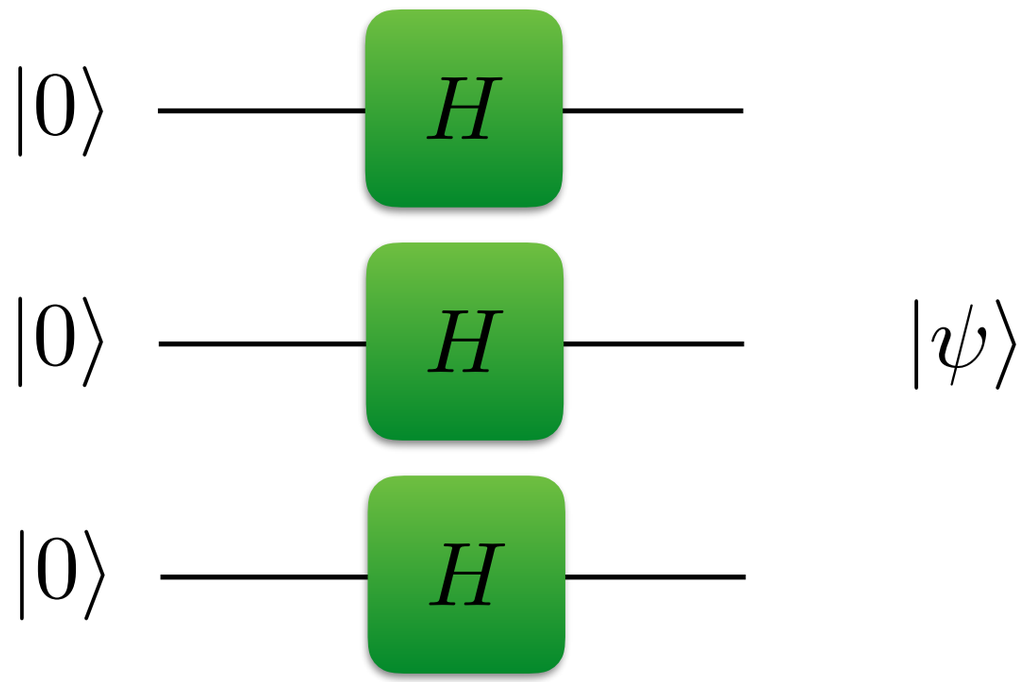
Input state	$\|0\rangle\|0\rangle$
After Hadamard	$\frac{1}{\sqrt{2}}(\|0\rangle\|0\rangle + \|1\rangle\|0\rangle)$
After CNOT	$\frac{1}{\sqrt{2}}(\|0\rangle\|0\rangle + \|1\rangle\|1\rangle)$



Input state	$\lvert 0\rangle\lvert 0\rangle$
After Hadamard	$\frac{1}{\sqrt{2}}(\lvert 0\rangle\lvert 0\rangle + \lvert 1\rangle\lvert 0\rangle)$
After CNOT	$\frac{1}{\sqrt{2}}(\lvert 0\rangle\lvert 0\rangle + \lvert 1\rangle\lvert 1\rangle)$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

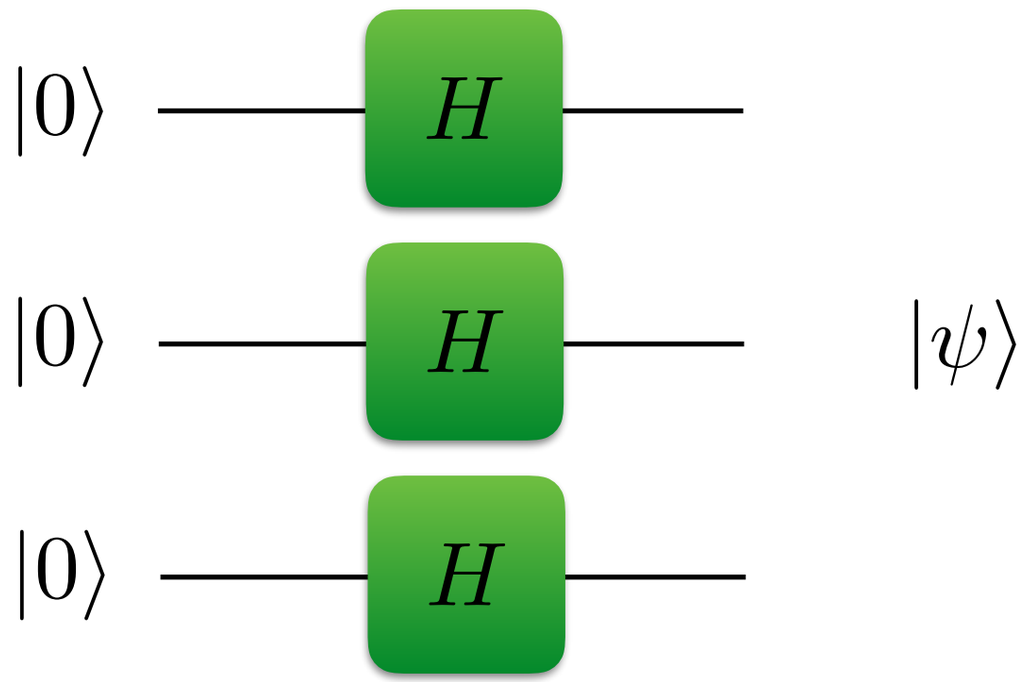
Recall that this state is entangled!



Input state $|0\rangle|0\rangle|0\rangle$

After Hadamards $|+\rangle|+\rangle|+\rangle$

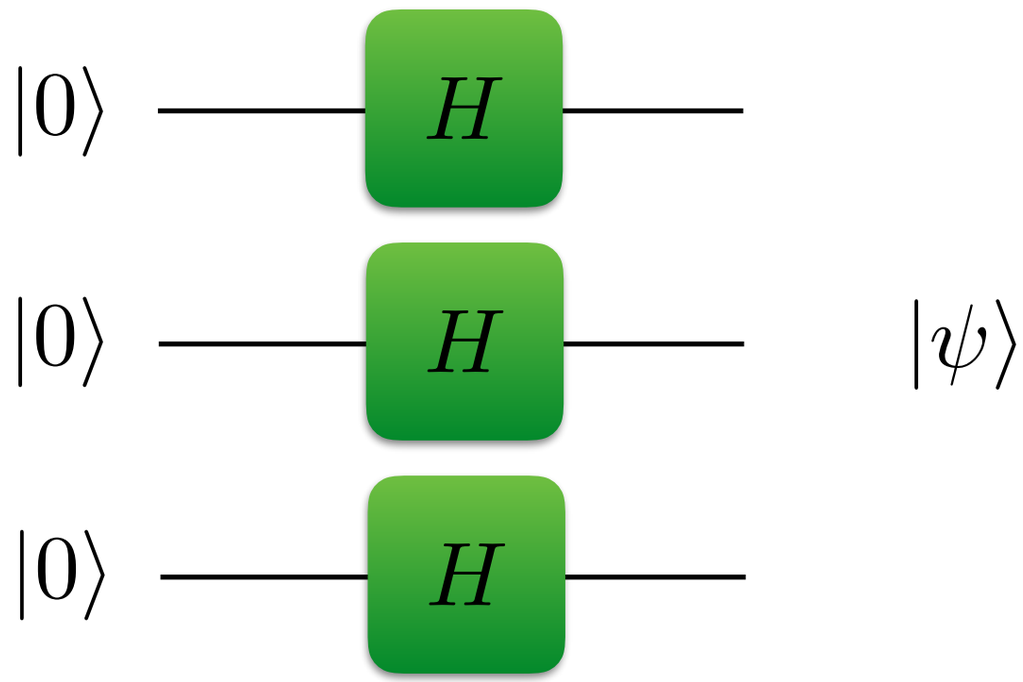
$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



Input state $|0\rangle|0\rangle|0\rangle$

After Hadamards $|+\rangle|+\rangle|+\rangle$

$$|\psi\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle +$$
$$+|100\rangle + |101\rangle + |110\rangle + |111\rangle)$$



Input state $|0\rangle|0\rangle|0\rangle$

After Hadamards $|+\rangle|+\rangle|+\rangle$

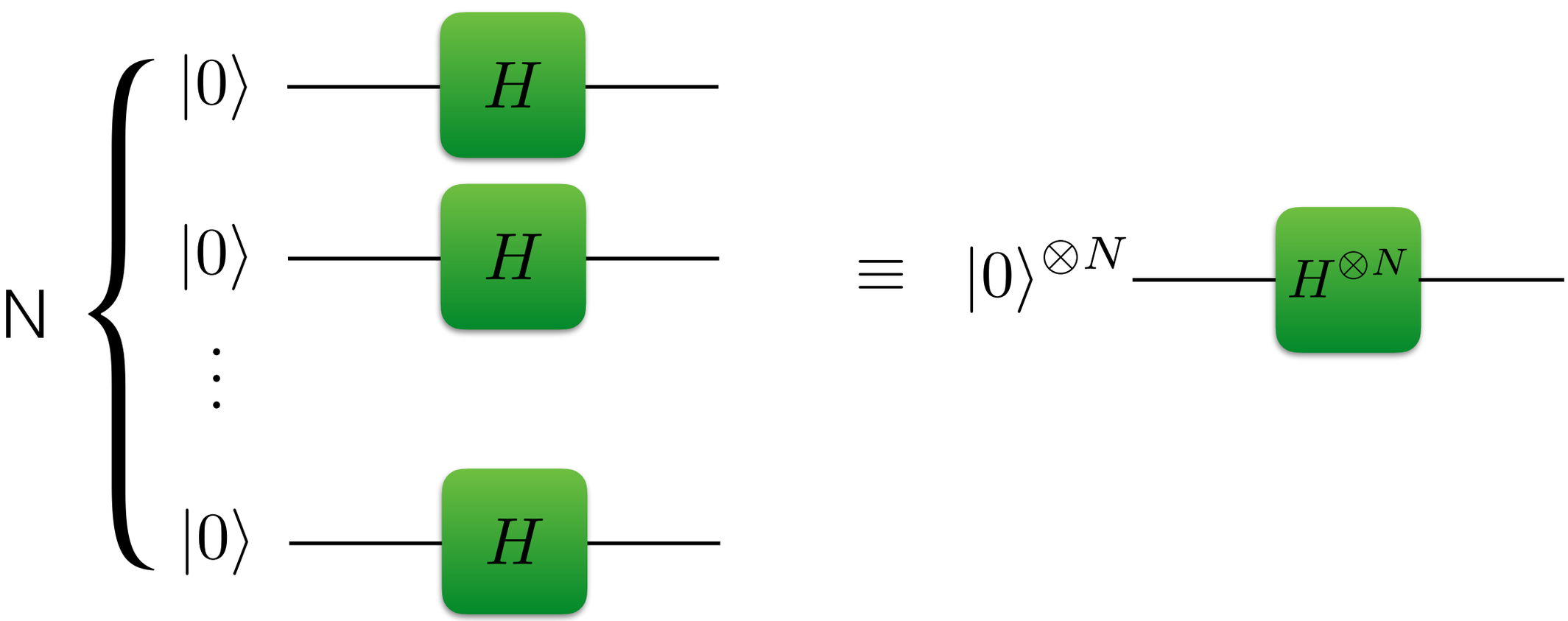
$$|\psi\rangle = \frac{1}{2\sqrt{2}} \sum_{x \in \{0,1\}^3} |x\rangle$$

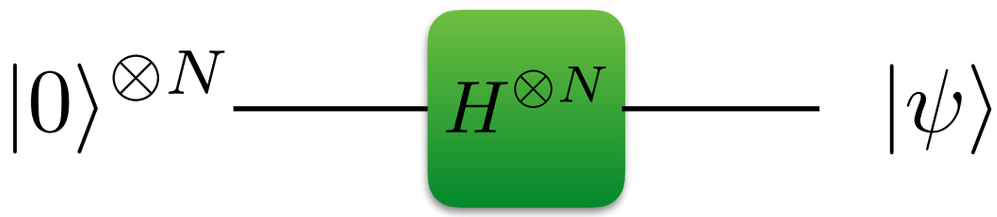
Note that this state is **not** entangled!

Useful notation

$$\underbrace{U \otimes U \otimes \ldots \otimes U}_{\text{N times}} = U^{\otimes N}$$

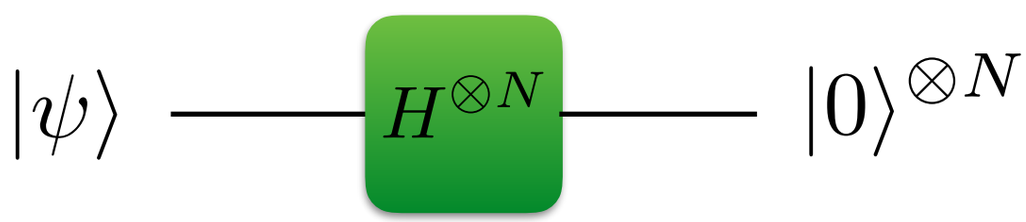
$$\underbrace{|\psi\rangle \otimes |\psi\rangle \otimes \ldots \otimes |\psi\rangle}_{\text{N times}} = |\psi\rangle^{\otimes N}$$





$$|\psi\rangle = \frac{1}{2^{N/2}} \sum_{x \in \{0,1\}^N} |x\rangle$$

Reverse is also true!



All gates we've seen, other than T, are self-inverse!

Measurement

Recall that measurements are performed in an orthonormal basis

For now, just consider measurements in the <u>computational basis</u>

$$\{|0\rangle, |1\rangle\}$$

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

$$\{|x\rangle\}, \text{ with } x \in \{0,1\}^N$$

Measurement

So for some general N-qubit state…

$$|\psi\rangle = \sum_{x \in \{0,1\}^N} \alpha_x |x\rangle$$

α_x is the **amplitude** for observing outcome $|x\rangle$

$|\alpha_x|^2$ is the **probability** for observing outcome $|x\rangle$

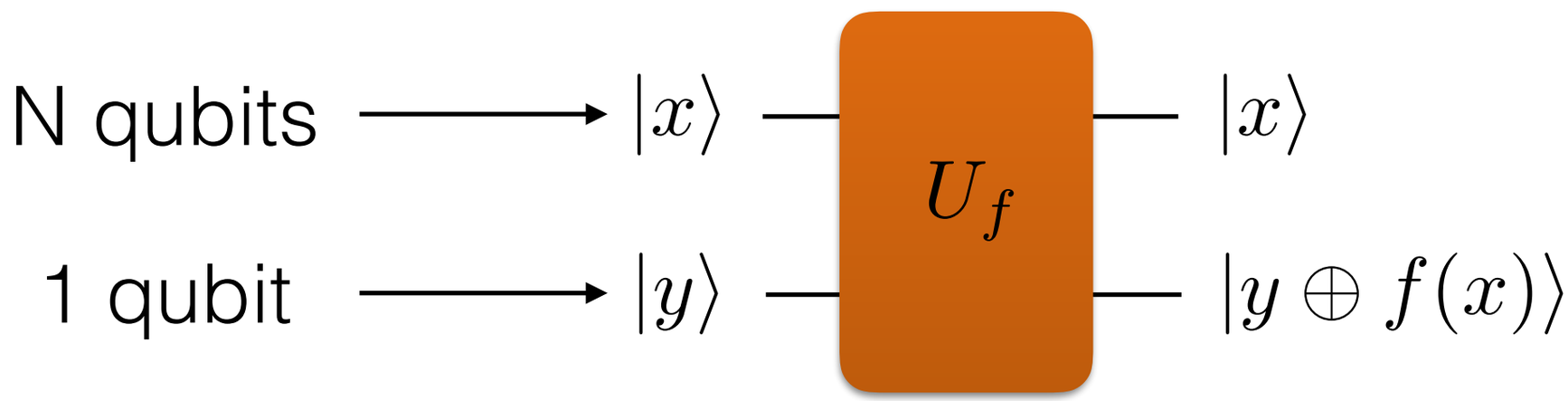
$$|\psi\rangle = \frac{1}{2^{N/2}} \sum_{x \in \{0,1\}^N} |x\rangle$$

Equal probability for each outcome $\frac{1}{2^N}$

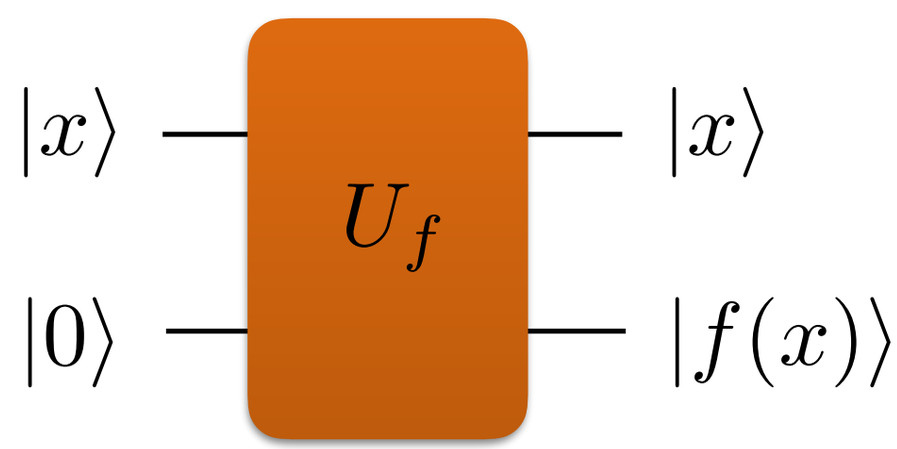
Boolean function unitary

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

Consider the (N+1)-qubit unitary



$$x \in \{0,1\}^N, y \in \{0,1\}$$

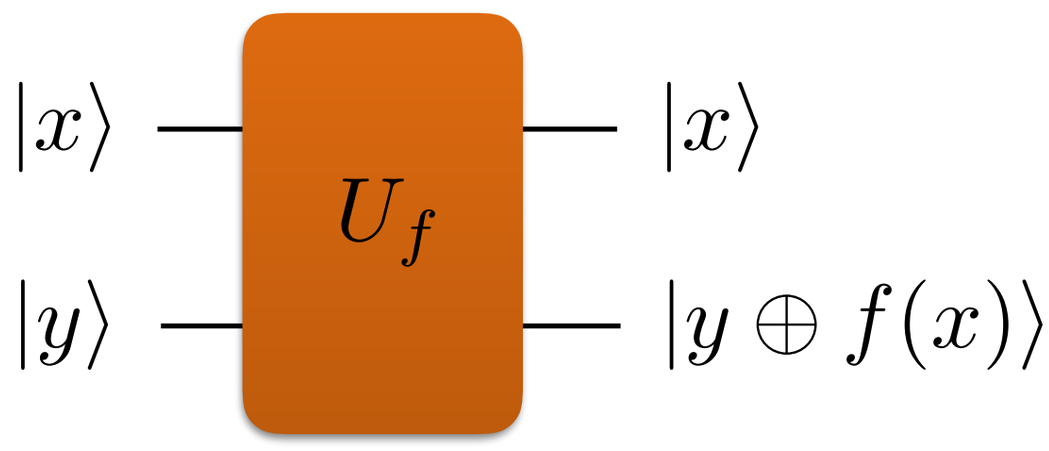


Boolean function unitary

Example for N=1

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

$$f(x) = x$$

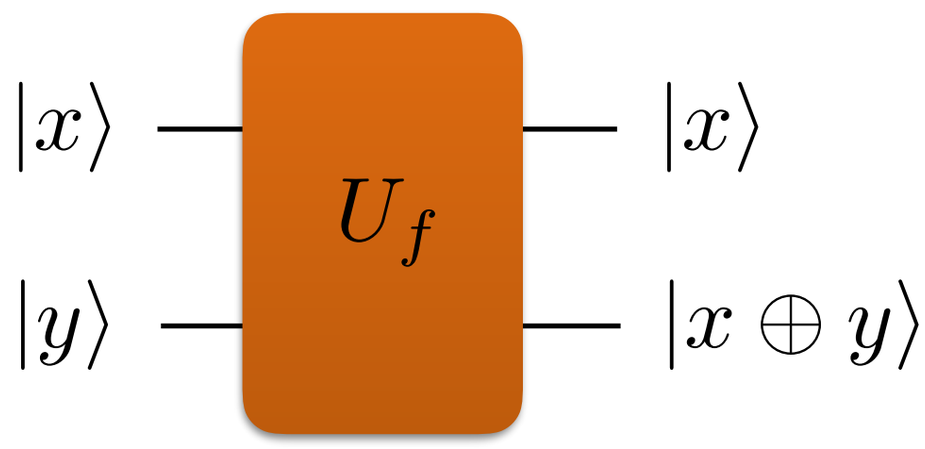


Boolean function unitary

Example for N=1

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

$$f(x) = x$$

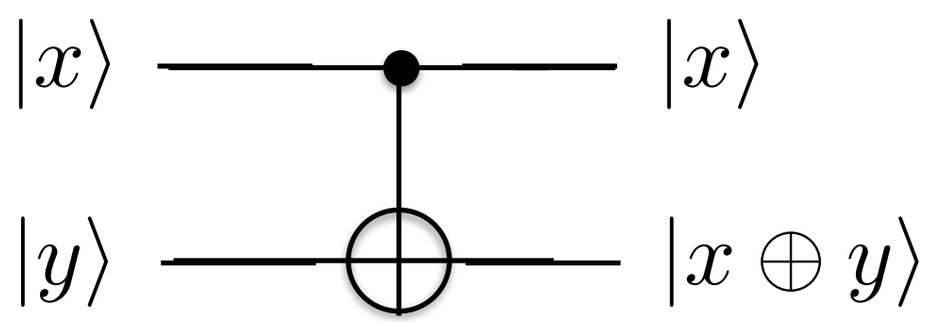


Boolean function unitary

Example for N=1

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

$$f(x) = x$$



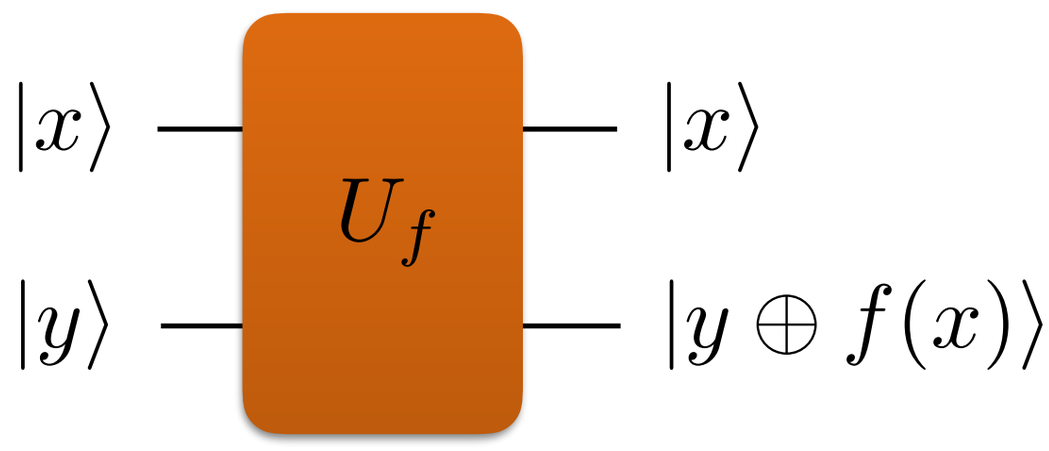
It's CNOT!

Boolean function unitary

Example for N=1

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

$$f(x) = 1$$

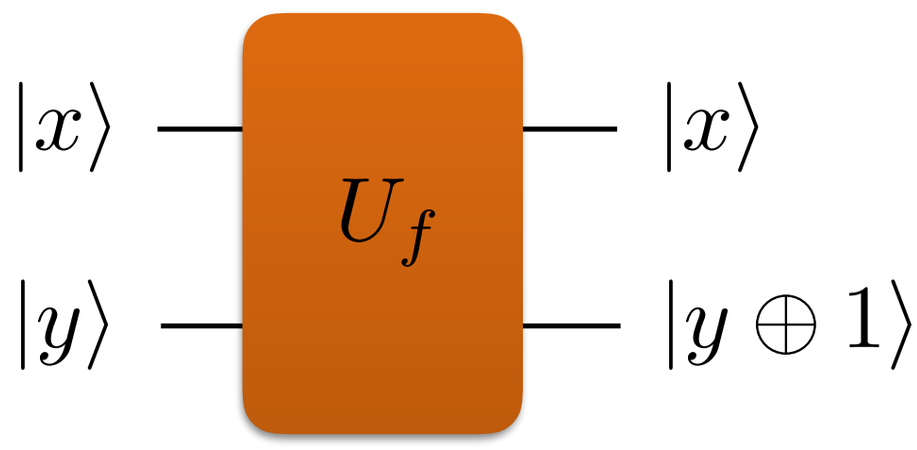


Boolean function unitary

Example for N=1

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

$$f(x) = 1$$

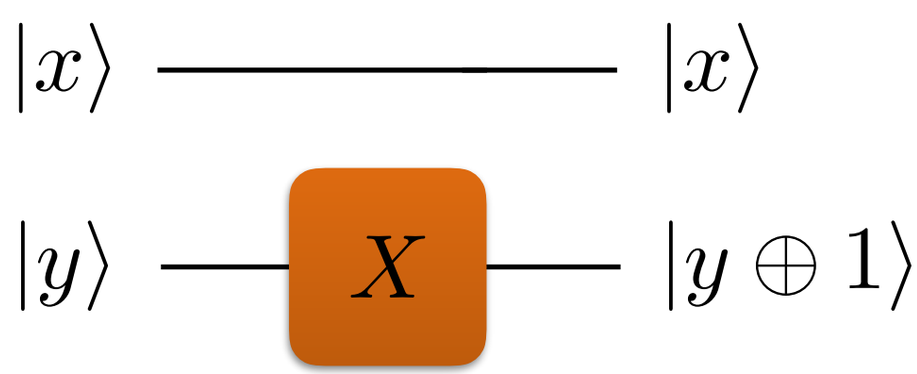


Boolean function unitary

Example for N=1

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

$$f(x) = 1$$



It's $I \otimes X$!

Deutsch-Josza problem

Suppose that…

$$f : \{0,1\}^N \rightarrow \{0,1\}$$

is either **constant** or **balanced**

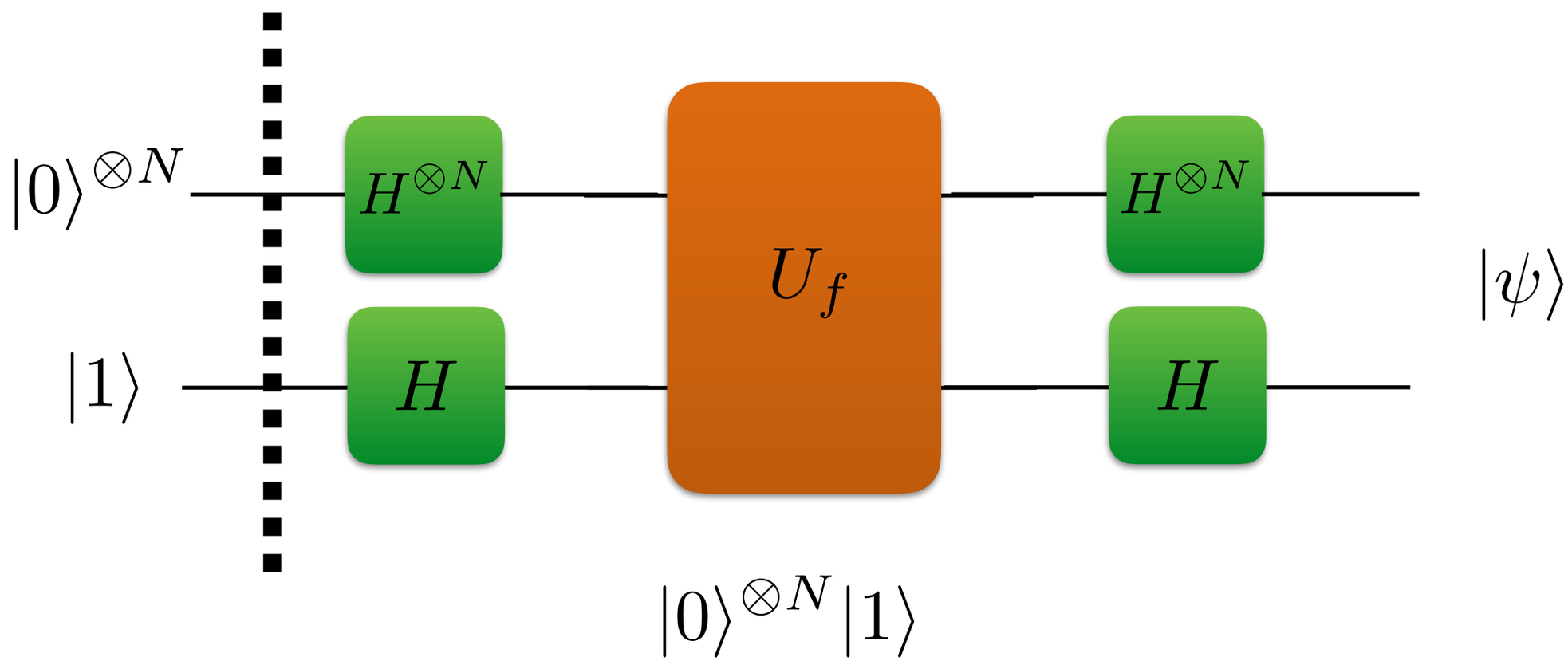
Constant: same value for all inputs
Balanced: 0 for half of inputs, 1 for other half

How many queries to U_f to determine type?

One!

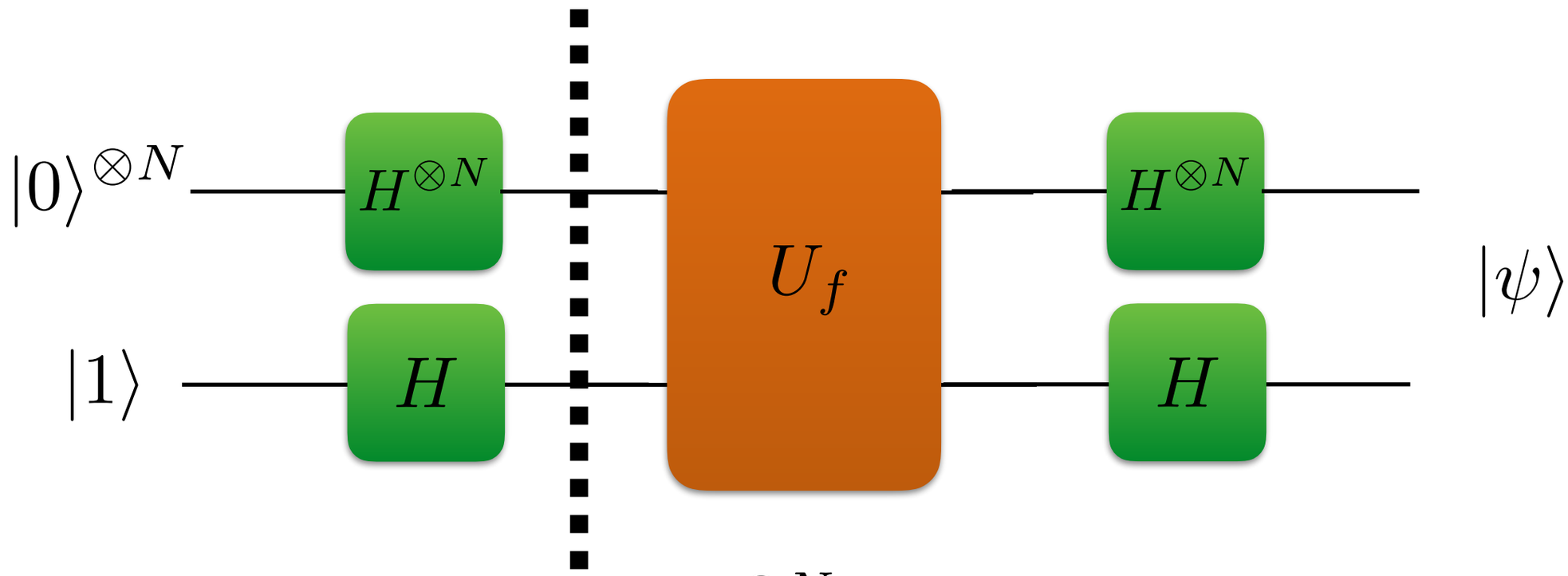
Deutsch-Josza algorithm

Consider the following (N+1) qubit circuit



Deutsch-Josza algorithm

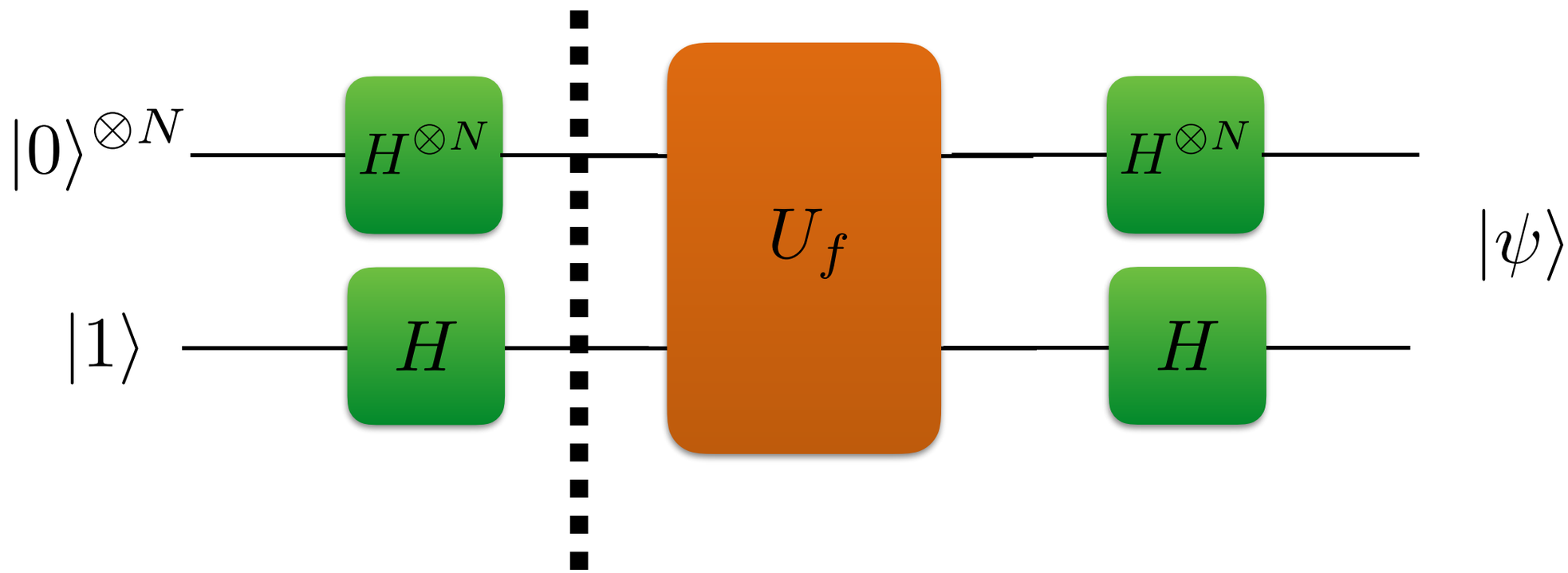
Consider the following (N+1) qubit circuit



$$|0\rangle^{\otimes N}|1\rangle$$

$$\left(\frac{1}{2^{N/2}}\sum_{x\in\{0,1\}^N}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

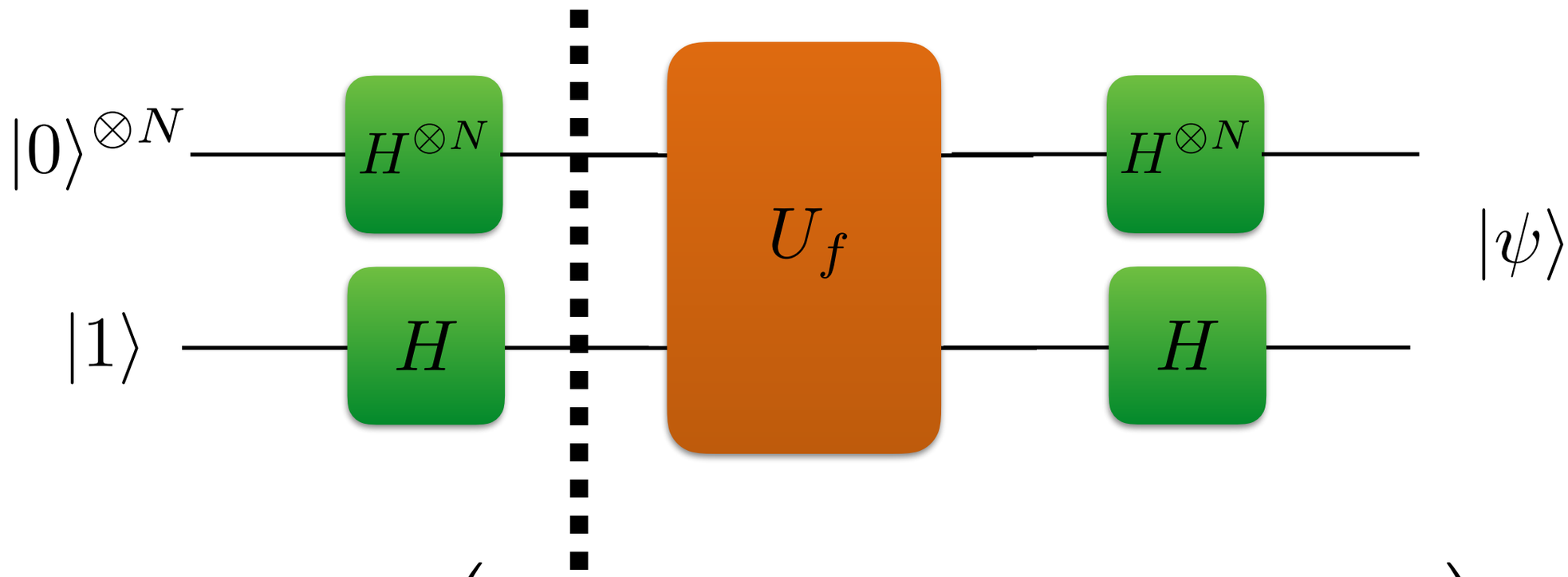
Deutsch-Josza algorithm



$$\left(\frac{1}{2^{N/2}}\sum_{x\in\{0,1\}^N}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

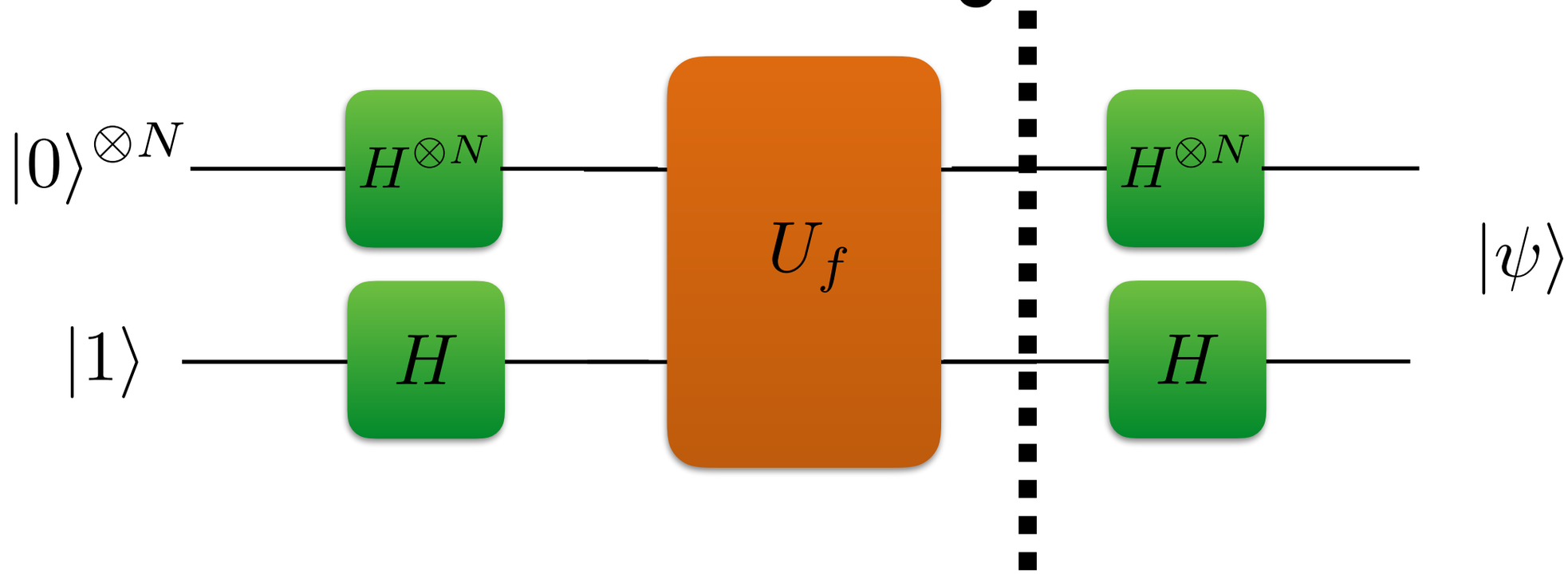
$$\frac{1}{2^{(N+1)/2}}\left(\sum_{x\in\{0,1\}^N}|x\rangle|0\rangle-\sum_{x\in\{0,1\}^N}|x\rangle|1\rangle\right)$$

Deutsch-Josza algorithm



$$\frac{1}{2^{(N+1)/2}}\left(\sum_{x\in\{0,1\}^N}|x\rangle|0\rangle-\sum_{x\in\{0,1\}^N}|x\rangle|1\rangle\right)$$

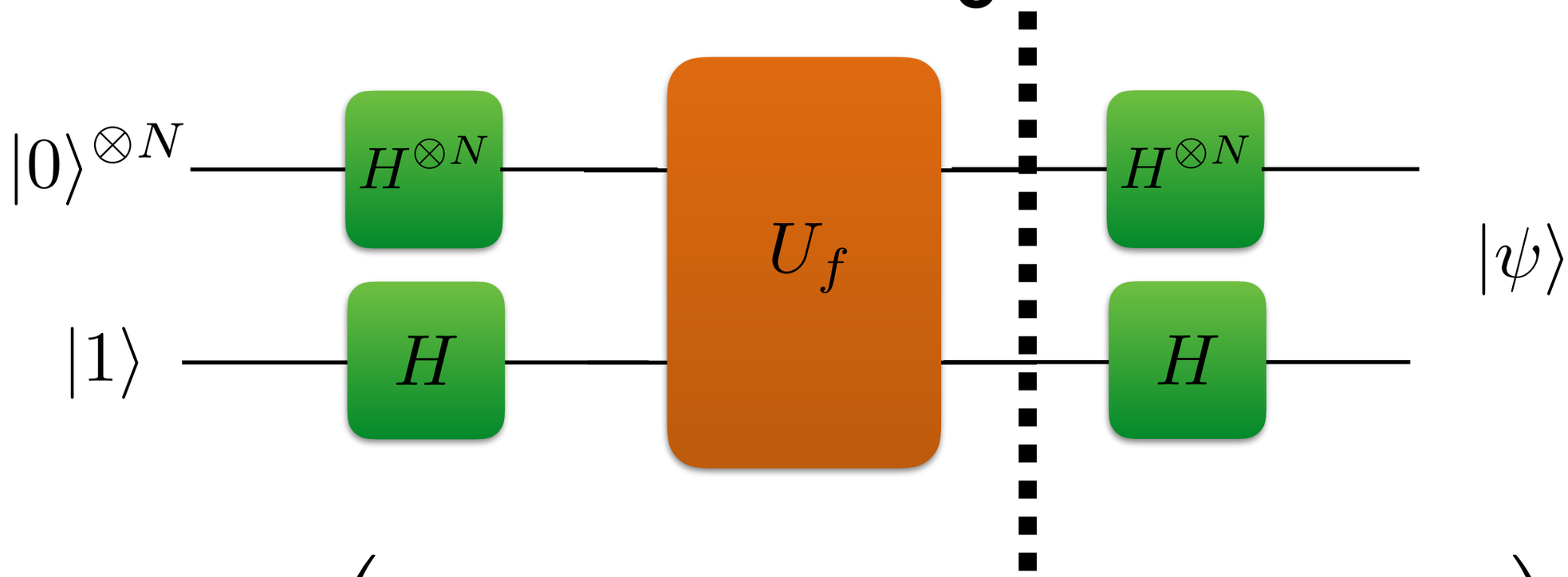
Deutsch-Josza algorithm



$$\frac{1}{2^{(N+1)/2}}\left(\sum_{x\in\{0,1\}^N}|x\rangle|0\rangle-\sum_{x\in\{0,1\}^N}|x\rangle|1\rangle\right)$$

$$\frac{1}{2^{(N+1)/2}}\left(\sum_{x\in\{0,1\}^N}U_f|x\rangle|0\rangle-\sum_{x\in\{0,1\}^N}U_f|x\rangle|1\rangle\right)$$

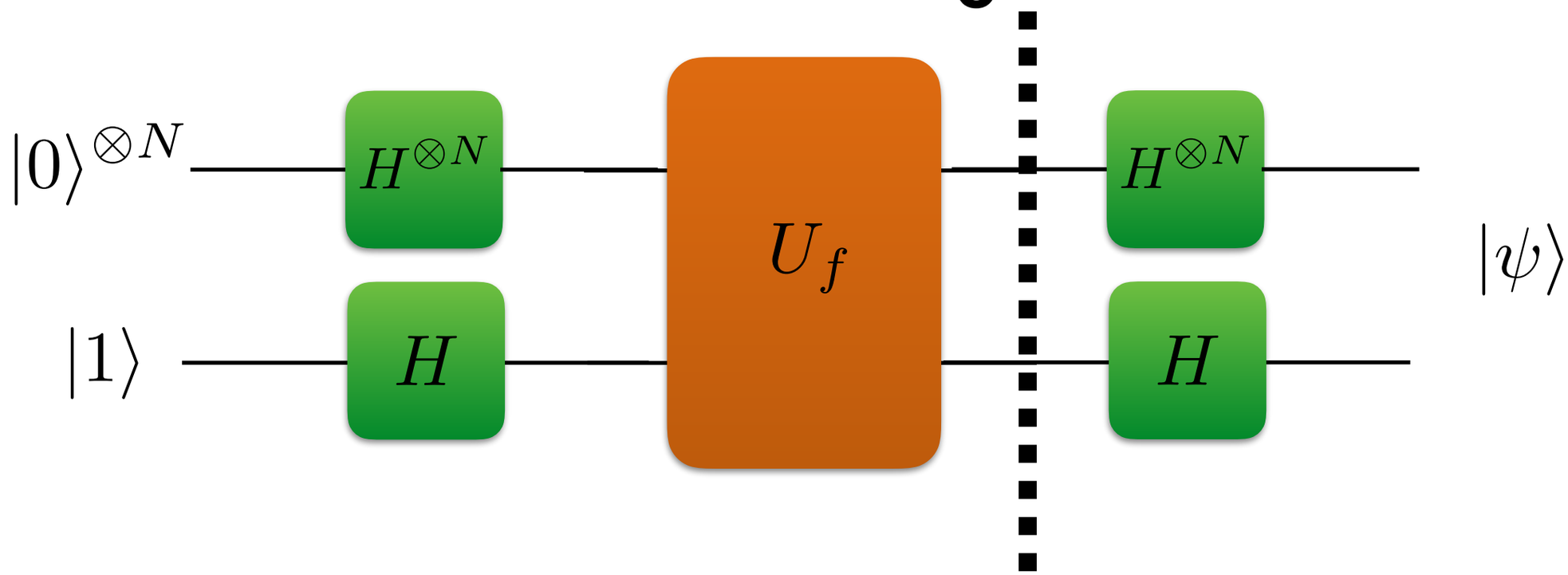
Deutsch-Josza algorithm



$$\frac{1}{2^{(N+1)/2}}\left(\sum_{x\in\{0,1\}^N} U_f|x\rangle|0\rangle - \sum_{x\in\{0,1\}^N} U_f|x\rangle|1\rangle\right)$$

$$\frac{1}{2^{(N+1)/2}}\left(\sum_{x\in\{0,1\}^N} |x\rangle|f(x)\rangle - \sum_{x\in\{0,1\}^N} |x\rangle|1\oplus f(x)\rangle\right)$$

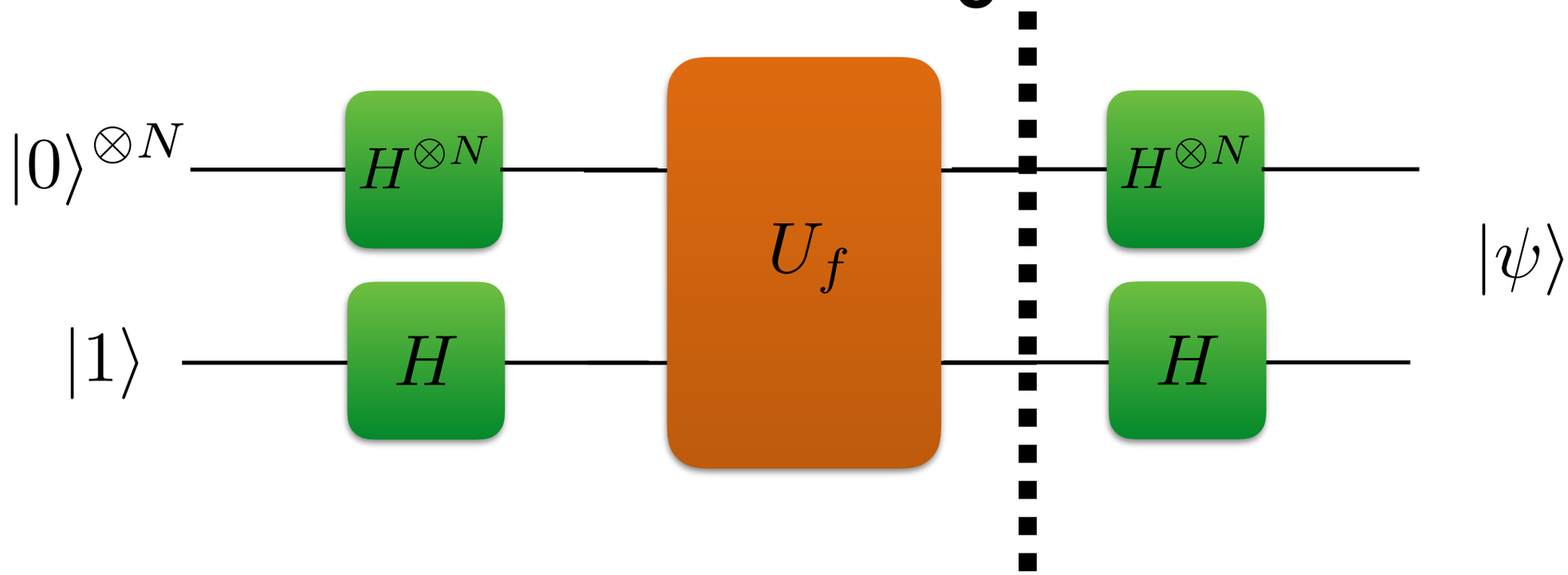
Deutsch-Josza algorithm



$$\frac{1}{2^{(N+1)/2}}\left(\sum_{x\in\{0,1\}^N}|x\rangle|f(x)\rangle-\sum_{x\in\{0,1\}^N}|x\rangle|1\oplus f(x)\rangle\right)$$

$$\frac{1}{2^{(N+1)/2}}\sum_{x\in\{0,1\}^N}|x\rangle(|f(x)\rangle-|1\oplus f(x)\rangle)$$

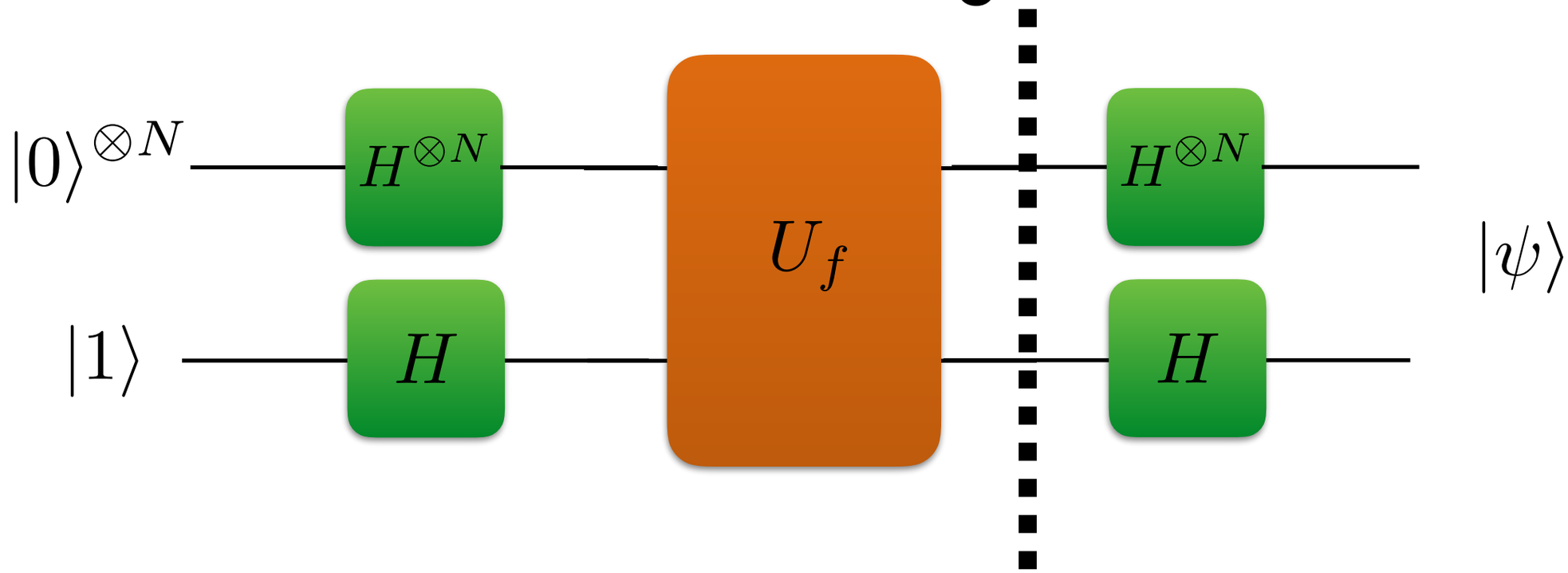
Deutsch-Josza algorithm



$$\frac{1}{2^{(N+1)/2}} \sum_{x \in \{0,1\}^N} |x\rangle(|f(x)\rangle - |1 \oplus f(x)\rangle)$$

$$\frac{1}{2^{(N+1)/2}} \sum_{x \in \{0,1\}^N} |x\rangle \;\; (-1)^{f(x)}(|0\rangle - |1\rangle)$$

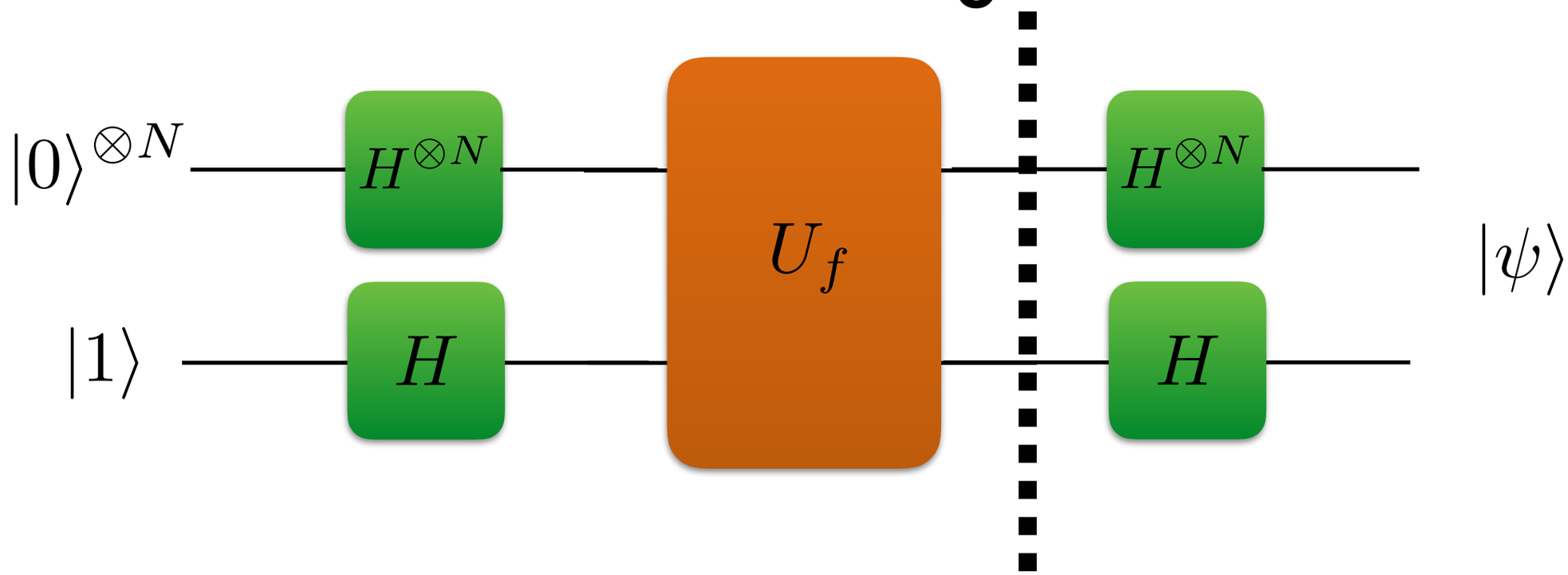
Deutsch-Josza algorithm



$$\frac{1}{2^{(N+1)/2}} \sum_{x \in \{0,1\}^N} |x\rangle \;\; (-1)^{f(x)} (|0\rangle - |1\rangle)$$

$$\left(\frac{1}{2^{N/2}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \right) |-\rangle$$

Deutsch-Josza algorithm

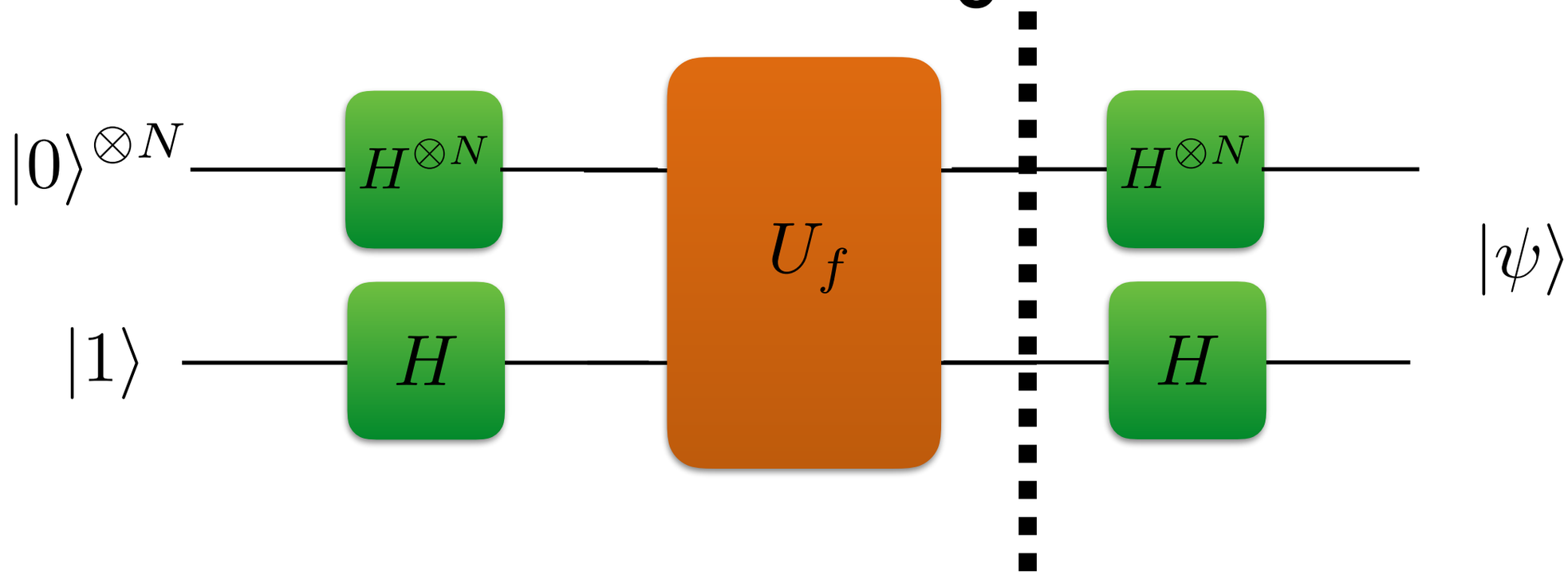


$$\left(\frac{1}{2^{N/2}}\sum_{x\in\{0,1\}^N}(-1)^{f(x)}|x\rangle\right)|-\rangle$$

Suppose function is constant!

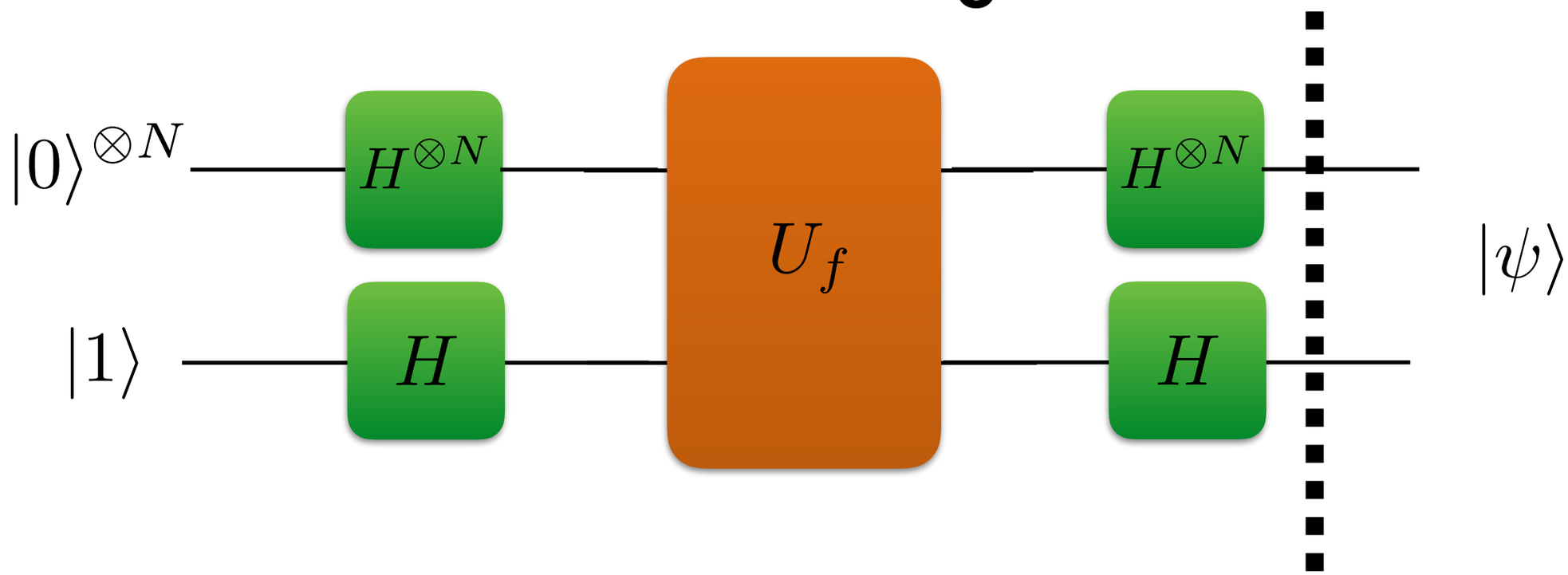
$$\pm\left(\frac{1}{2^{N/2}}\sum_{x\in\{0,1\}^N}|x\rangle\right)|-\rangle$$

Deutsch-Josza algorithm



$$\pm\left(\frac{1}{2^{N/2}}\sum_{x\in\{0,1\}^N}|x\rangle\right)|-\rangle$$

Deutsch-Josza algorithm

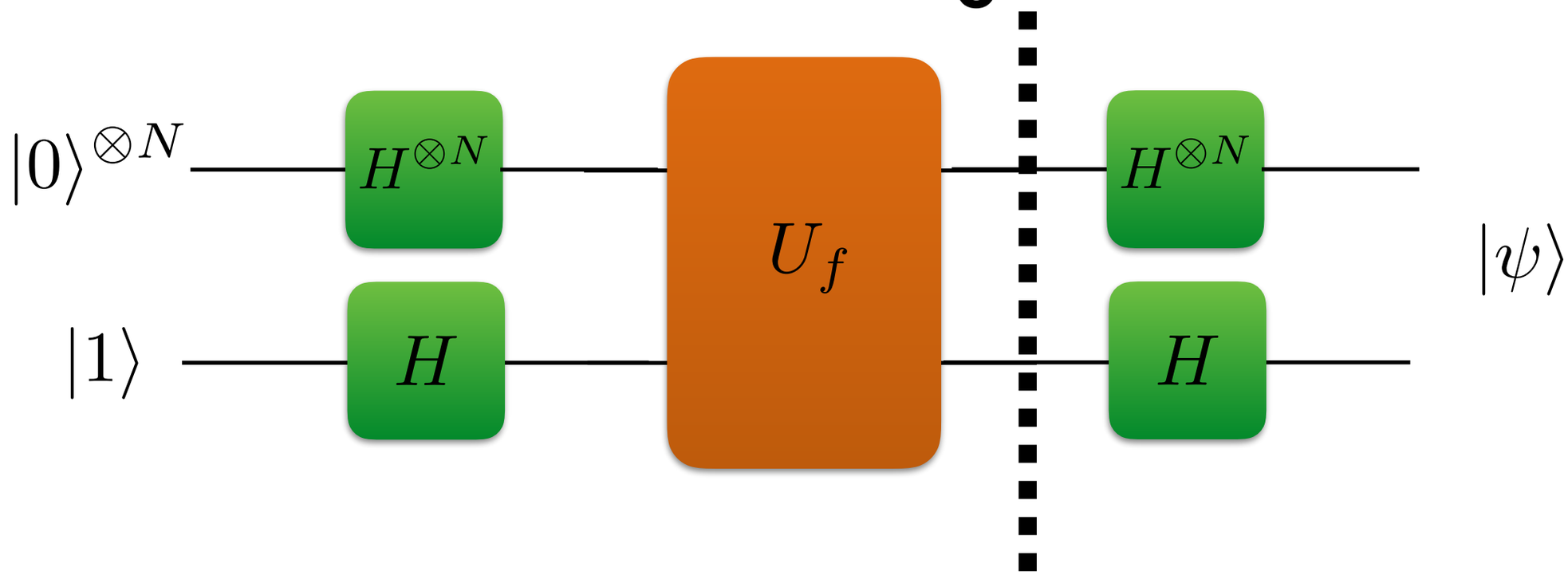


$$\pm\left(\frac{1}{2^{N/2}}\sum_{x\in\{0,1\}^N}|x\rangle\right)|-\rangle$$

$$\pm|0\rangle^{\otimes N}|1\rangle$$

If we measure all the first qubits as being 0
we know the function is constant!

Deutsch-Josza algorithm

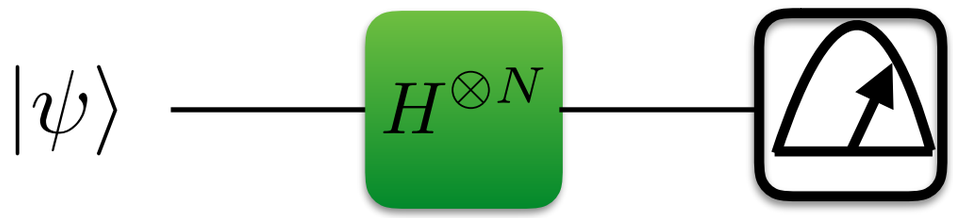


$$\left(\frac{1}{2^{N/2}}\sum_{x\in\{0,1\}^N}(-1)^{f(x)}|x\rangle\right)|-\rangle$$

Suppose function is balanced!

What is the probability of seeing the first N qubits as 0?

A trick



I want to know ${}^{N\otimes}\langle 0|H^{\otimes N}|\psi\rangle$

This is the same as…

$${}^{N\otimes}\langle +|\psi\rangle$$

Or…

$$\frac{1}{2^{N/2}} \sum_{y\in\{0,1\}^N} \langle y|\psi\rangle$$

A trick

$$\frac{1}{2^{N/2}} \sum_{y \in \{0,1\}^N} \langle y | \psi \rangle$$

In our case…

$$|\psi\rangle = \frac{1}{2^{N/2}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle$$

So we have…

$$\frac{1}{2^N} \sum_{x \in \{0,1\}^N} \sum_{y \in \{0,1\}^N} (-1)^{f(x)} \langle y | x \rangle$$

A trick

$$\frac{1}{2^N} \sum_{x \in \{0,1\}^N} \sum_{y \in \{0,1\}^N} (-1)^{f(x)} \langle y|x \rangle$$

But $\{|x\rangle\}, \text{ with } x \in \{0,1\}^N$ is an orthonormal basis

$$\langle y|x \rangle = 0, \; y \neq x$$

$$\langle y|x \rangle = 1, \; y = x$$

So the probability of seeing all 0 is:

$$\frac{1}{2^N} \sum_{x \in \{0,1\}^N} (-1)^{f(x)}$$

A trick

So the probability of seeing all 0 is:

$$\frac{1}{2^N} \sum_{x \in \{0,1\}^N} (-1)^{f(x)}$$

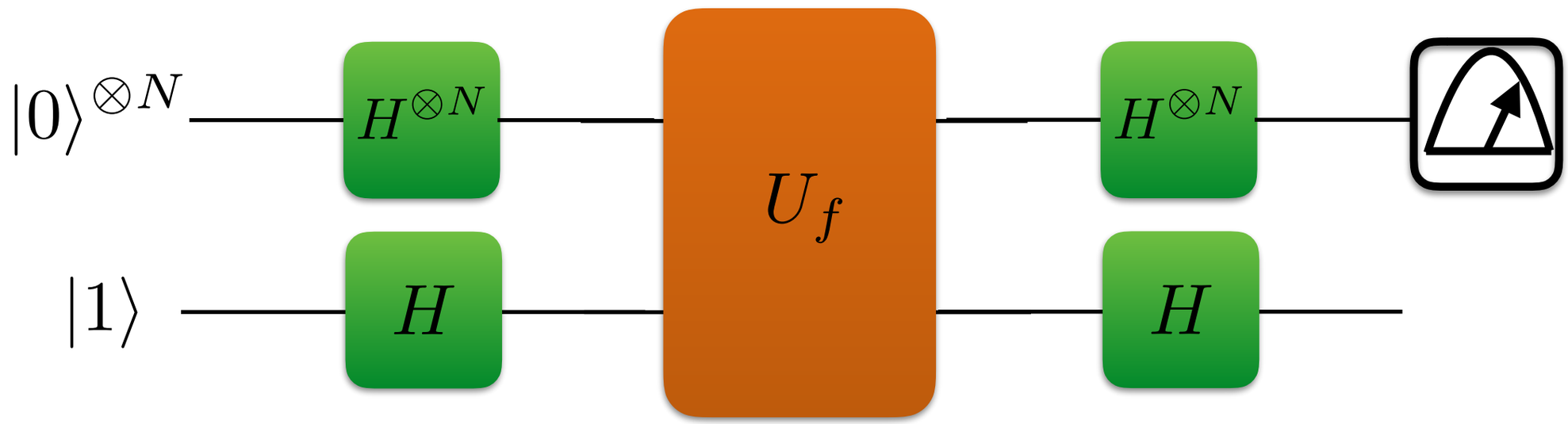
But the function is balanced!

Half of the terms will be +1, half will be -1

The probability is 0!

Interference

Deutsch-Josza algorithm



Measure first N qubits

If all zeroes, then function is constant

Otherwise, function is balanced

We have just implemented *interf*

References and resources

Decomposing unitaries into a universal gate set
https://arxiv.org/abs/quant-ph/0505030
https://arxiv.org/pdf/quant-ph/0504100.pdf

IBM quantum experience
https://quantumexperience.ng.bluemix.net/qx

Rigetti Forest
https://www.rigetti.com/products

Deutsch-Josza in the Liquid quantum simulator
https://github.com/StationQ/Liquid/tree/master/UserCode/AlexandruGheorghiu/Lab_2