CSE 596: Introduction to Theory of Computation

Quantum Computation III

Kelin Luo

Institute of Computer Science
University of Bonn, Germany
kluo@uni-bonn.de

Content

- Recall: Single Qubit and Operator Matrices
- The Bloch Sphere
- Two Qubits
- Three Qubits and More

Content

- **Recall: Qubits and Matrices**
- The Bloch Sphere
- Two Qubits
- Three Qubits and More

Recall: qubits and Dirac notation

- A qubit in state 0, also write as $|0\rangle$ **(Dirac notation):**

$$e_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

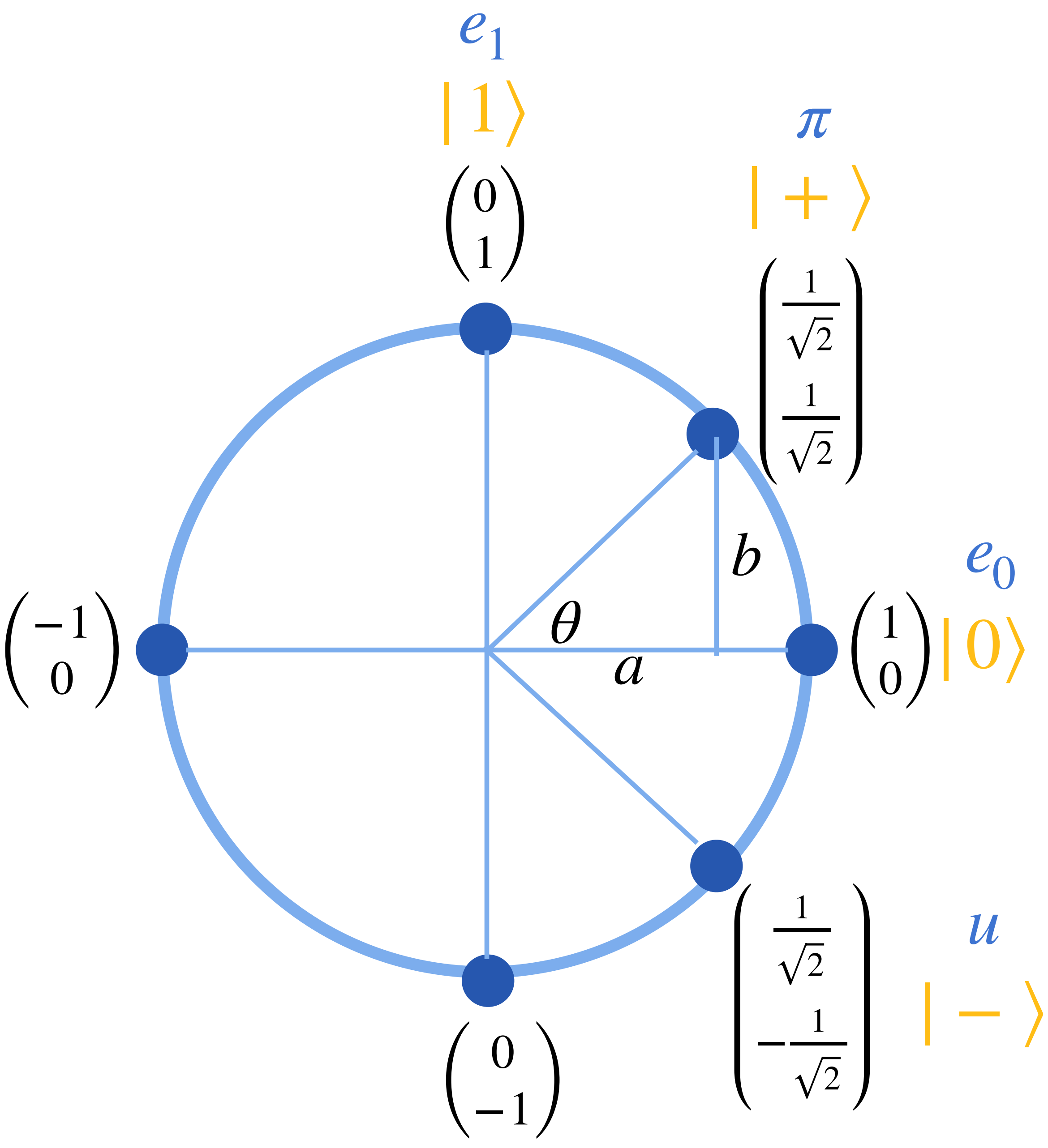
- A qubit in state 1, also write as $|1\rangle$:

$$e_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- A qubit in a superposition state is described by:

$$\begin{pmatrix} a \\ b \end{pmatrix} \text{ with } |a|^2 + |b|^2 = 1$$

also write as $a|0\rangle + b|1\rangle$.



Recall: basic arithmetic operations

- Matrix multiplication:

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

- Tensor products:

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

Recall: from a single bit to multiple bits

Examples:

$$|00\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \qquad |01\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|111\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\1\end{pmatrix}$$

Recall: unitary matrices (operators / gates)

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

- Pauli matrices

$$\begin{cases} X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} & \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{cases}$$

- Identity matrix: $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Content

- Recall: Qubits and Circuits
- **The Bloch Sphere**
- Two Qubits
- Three Qubits and More

Bloch sphere

Definition (Equivalent)

Two quantum states $\phi,\ \phi'$ are equivalent if there is a **unit complex number** c such that

$$\phi' = c\phi.$$

- The principle is that a unit complex number is only a "global phase difference" which is physically arbitrary and doesn't matter.

Bloch sphere

Definition (Equivalent)

Two quantum states $\phi,\ \phi'$ are equivalent if there is a **unit complex number** c such that

$$\phi' = \mathrm{c}\phi.$$

- The principle is that a unit complex number is only a "global phase difference" which is physically arbitrary and doesn't matter.

Example:

$\frac{1}{\sqrt{2}}(-1,1)$ is equivalent to $\frac{1}{\sqrt{2}}(1,-1)$

ie_1 is equivalent to e_1; $-ie_0$ is equivalent to e_0

Bloch sphere

Definition (Equivalent)

Two quantum states $\phi,\ \phi'$ are equivalent if there is a **unit complex number** c such that

$$\phi' = \mathrm{c}\phi.$$

Complex conjugate of c:

$$\frac{1}{c} = \frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a-bi}{1} = a - bi = \bar{c}$$

is also a unit complex number.

Since $\phi = \bar{c}\phi'$, then $\phi' = \mathrm{c}\phi$.

[Equivalence relation]
transitive, reflexive, and symmetric

Bloch sphere

Definition (Equivalent)

Two quantum states $\phi,\ \phi'$ are equivalent if there is a **unit complex number** c such that

$$\phi' = \mathrm{c}\phi.$$

Unit complex number in polar coordinate: $c = e^{i\gamma}$.

Bloch sphere

Definition (Equivalent)

Two quantum states $\phi,\ \phi'$ are equivalent if there is a **unit complex number** c such that

$$\phi' = c\phi.$$

Unit complex number in polar coordinate: $c = e^{i\gamma}$.

A quantum state ϕ in polar coordinates: $(ae^{i\alpha}, be^{i\beta})$.

Bloch sphere

Definition (Equivalent)

Two quantum states ϕ, ϕ' are equivalent if there is a **unit complex number** c such that

$$\phi' = c\phi.$$

Unit complex number in polar coordinate: $c = e^{i\gamma}$.

A quantum state ϕ in polar coordinates: $(ae^{i\alpha}, be^{i\beta})$.

Choose $\gamma = -\alpha$ then: $c\phi = (a, be^{i\varphi})$ with $\varphi = \beta - \alpha$.

Bloch sphere

Definition (Equivalent)

Two quantum states ϕ, ϕ' are equivalent if there is a **unit complex number** c such that

$$\phi' = c\phi.$$

Unit complex number in polar coordinate: $c = e^{i\gamma}$.

A quantum state ϕ in polar coordinates: $(ae^{i\alpha}, be^{i\beta})$.

Choose $\gamma = -\alpha$ then: $c\phi = (a, be^{i\varphi})$ with $\varphi = \beta - \alpha$.

Since $a^2 + b^2 = 1$, b is fixed once we specify a.

Bloch sphere

Definition (Equivalent)

Two quantum states ϕ, ϕ' are equivalent if there is a **unit complex number** c such that

$$\phi' = c\phi.$$

Unit complex number in polar coordinate: $c = e^{i\gamma}$.

A quantum state ϕ in polar coordinates: $(ae^{i\alpha}, be^{i\beta})$.

Choose $\gamma = -\alpha$ then: $c\phi = (a, be^{i\varphi})$ with $\varphi = \beta - \alpha$.

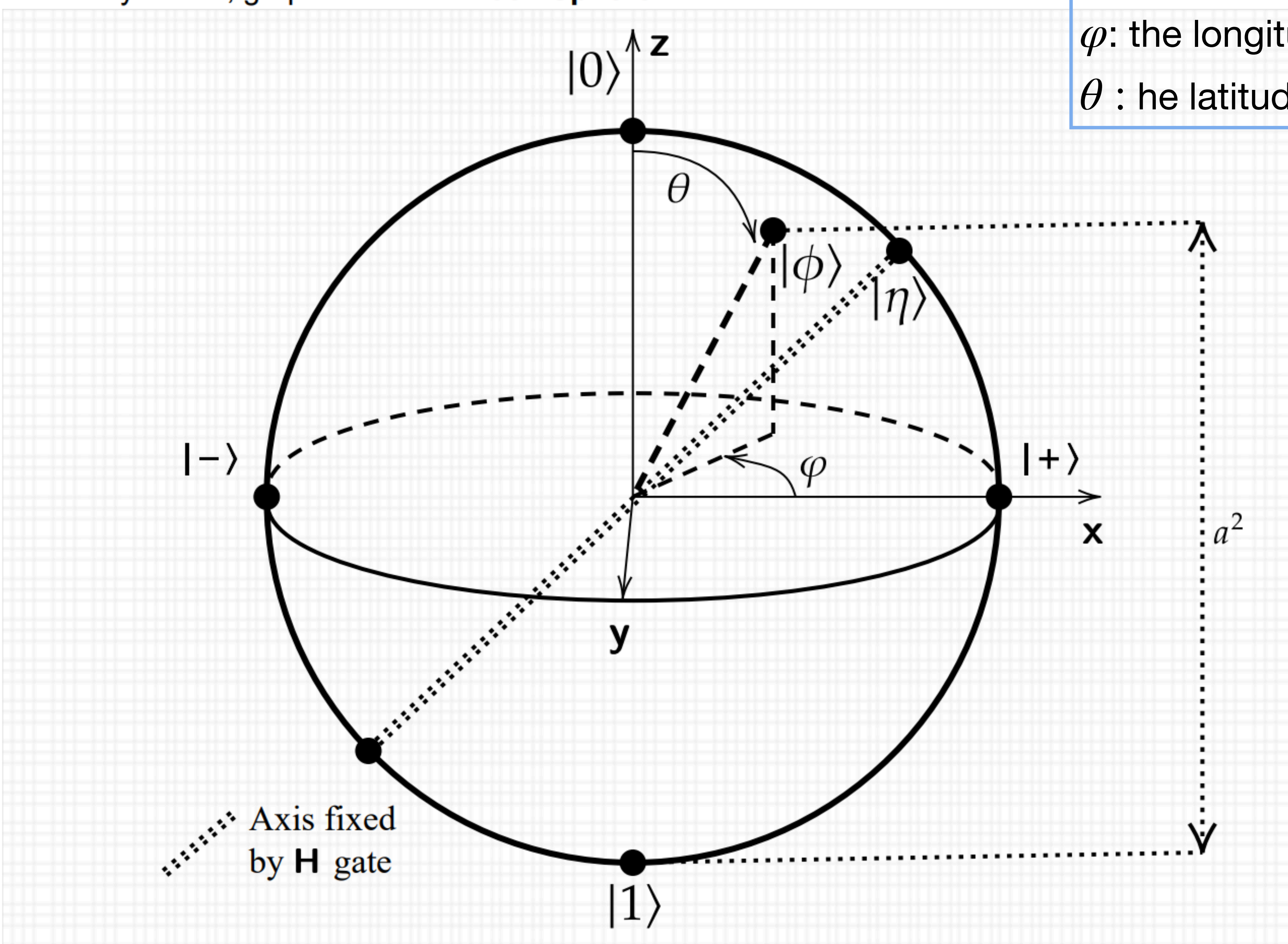
Since $a^2 + b^2 = 1$, b is fixed once we specify a.

So a and φ are enough to specify a state.

Bloch sphere

So a and φ are enough to specify a state.

Here they all are, graphed on the **Bloch Sphere**:

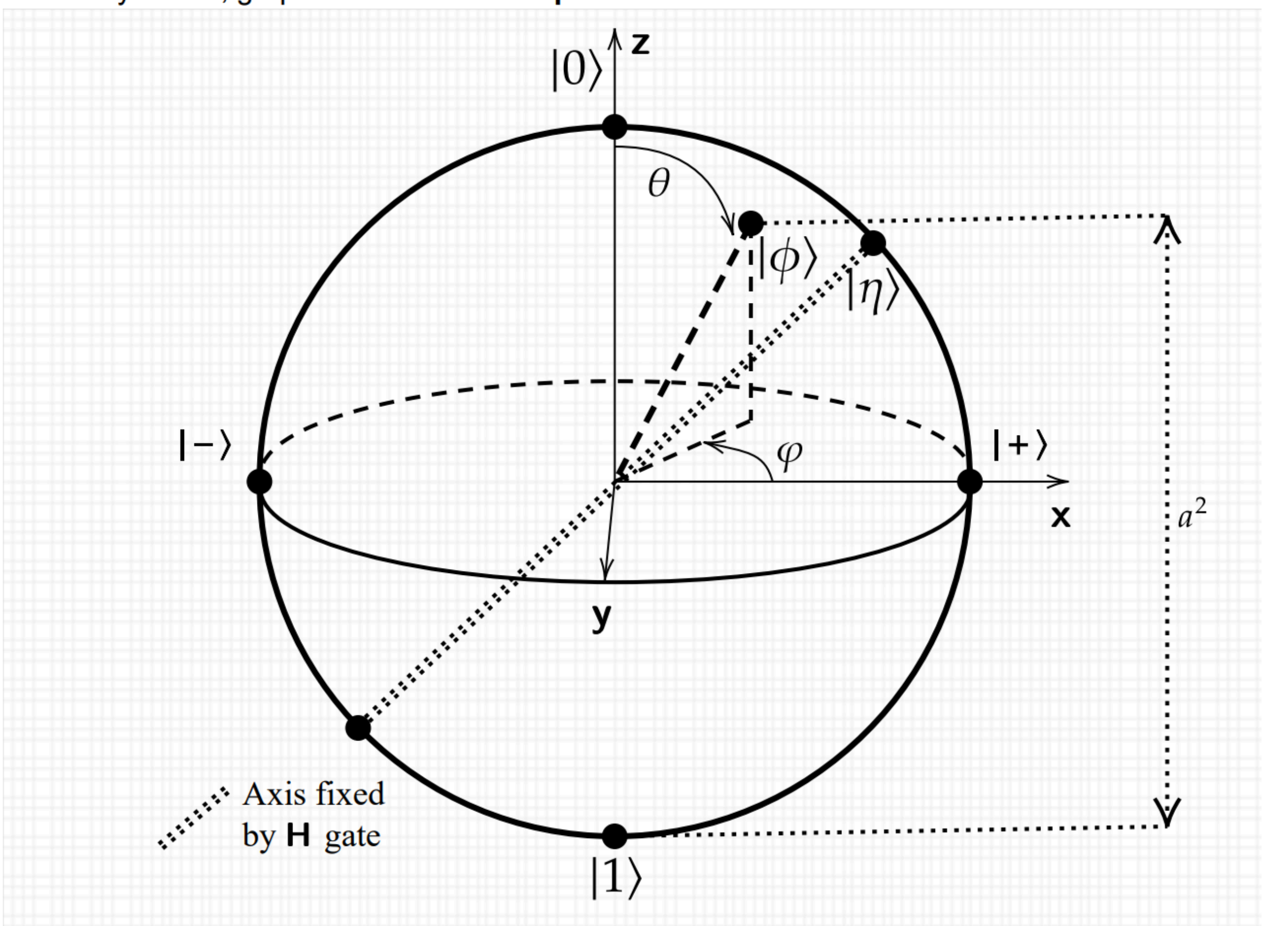


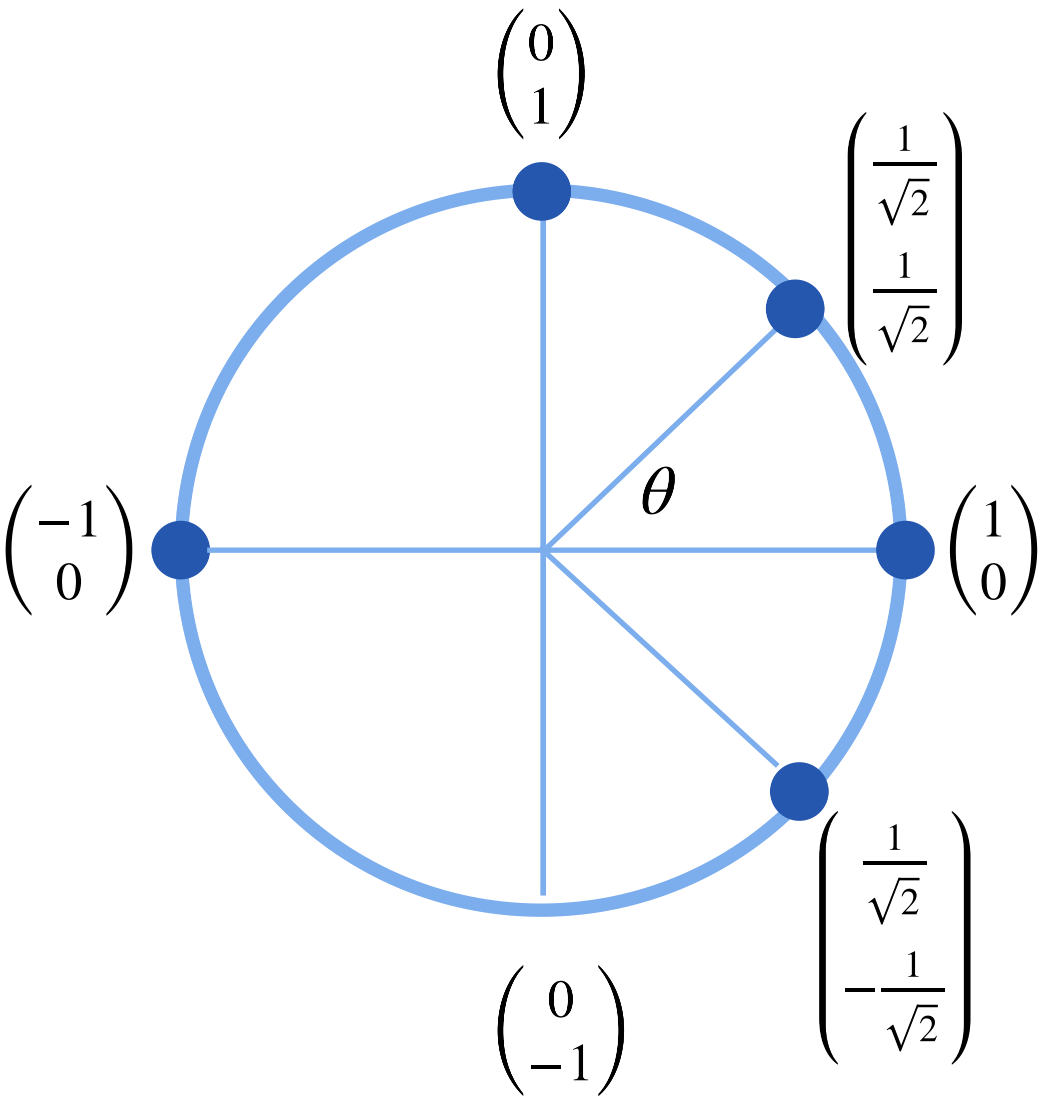
φ: the longitude of point

θ : he latitude of point

Comparing Cartesian and Bloch

Here they all are, graphed on the **Bloch Sphere**:





Cartesian: $\cos^2\theta$ is the probability of a measurement giving 0

$\sin^2\theta$ the probability of getting 1

Right angles are orthogonal

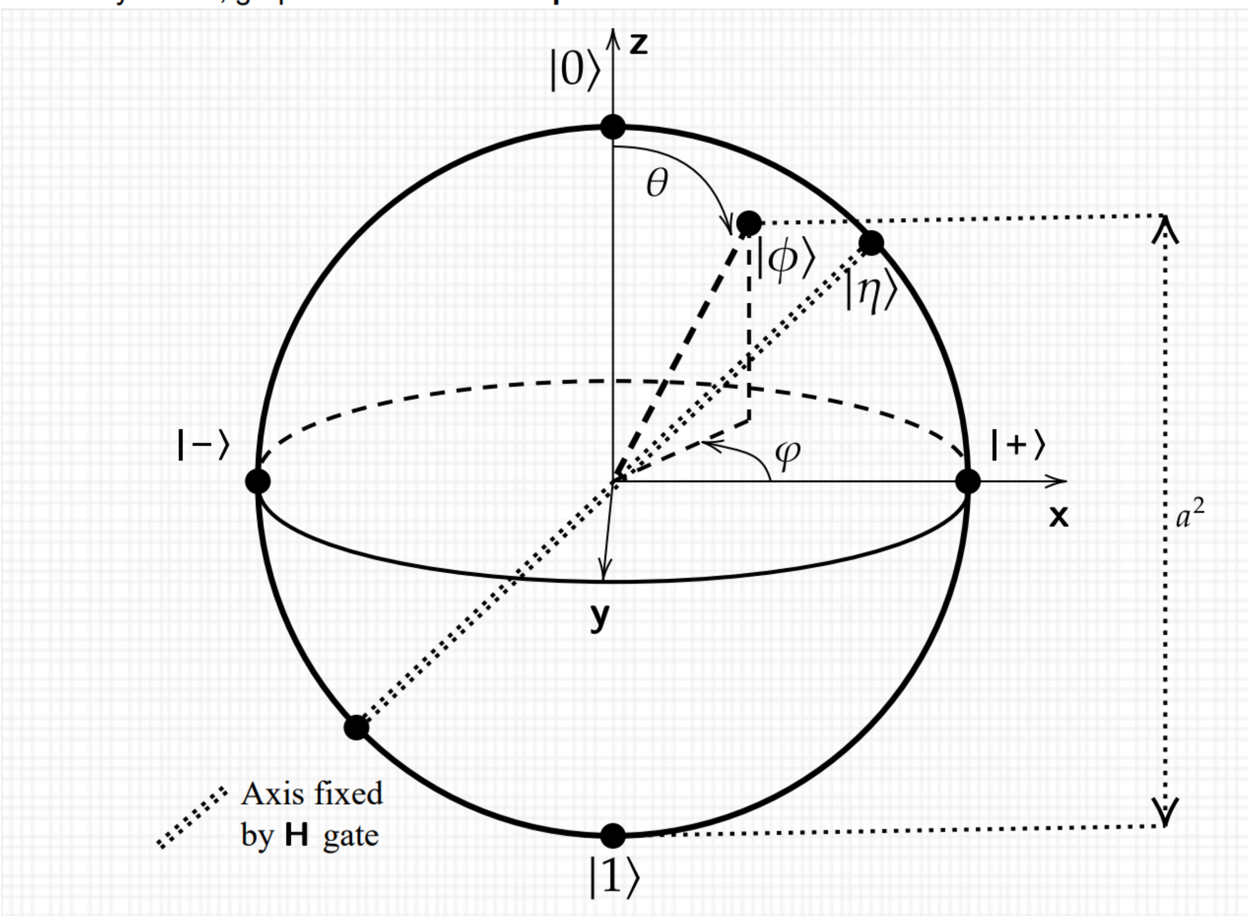
Bloch: the **latitude** is the probability of getting 0

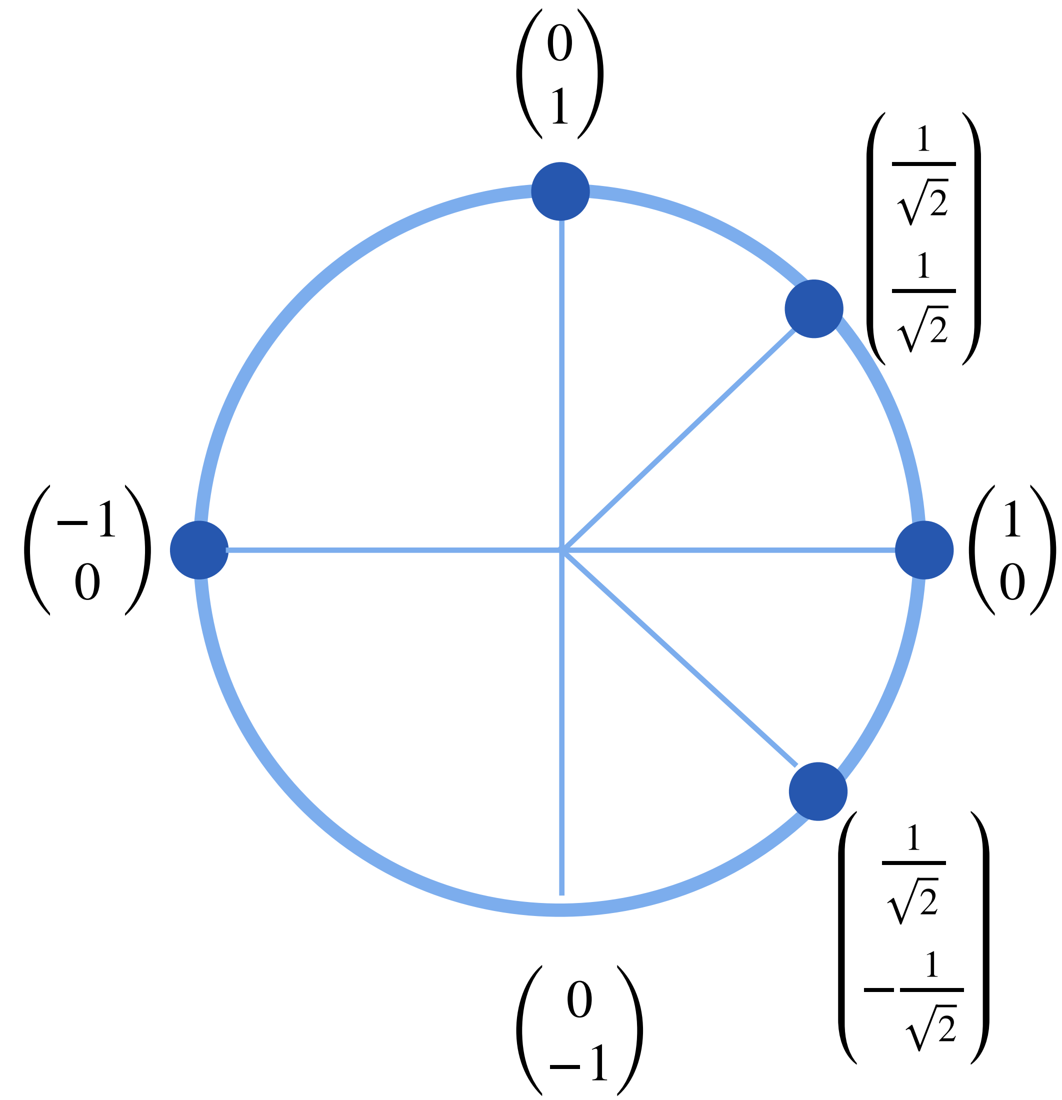
the north pole has latitude 1 and the south pole has latitude 0

Opposite poles are orthogonal.

Comparing Cartesian and Bloch

Here they all are, graphed on the **Bloch Sphere**:





Bloch: All points at the Bloch equator have equal probability of 0 and 1.

$|+\rangle$ and $|-\rangle$ are different quantum states with same outcome probabilities.

state $\frac{1}{\sqrt{2}}\begin{pmatrix}-1\\1\end{pmatrix}$ is not considered to be a different state from $|-\rangle$.

Two More Matrices (operators / gates)

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$S^4 = I$$

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

$$T^8 = I$$

Two More Matrices (operators / gates)

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$S^4 = I$

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

$T^8 = I$

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \quad \theta = \pi/2,\ \pi/4,\ \pi/8,\ \ldots$$

θ-angled phase gates

https://wybiral.github.io/quantum/

Content

- Recall: Qubits and Circuits
- The Bloch Sphere
- **Two Qubits**
- Three Qubits and More

Two qubits: basis states

One qubit state: $|0\rangle, |1\rangle$

$$e_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad e_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Two qubits: basis states

One qubit state: $|0\rangle, |1\rangle$

$$e_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad e_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Two qubits state: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ or $e_{00}, e_{01}, e_{10}, e_{11}$

$$e_{00} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad e_{01} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad e_{10} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad e_{11} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$e_{00} = e_0 \otimes e_0 \quad e_{01} = e_0 \otimes e_1 \quad e_{10} = e_1 \otimes e_0 \quad e_{11} = e_1 \otimes e_1$$

$$|00\rangle = |0\rangle \otimes |0\rangle \quad |01\rangle = |0\rangle \otimes |1\rangle \quad |10\rangle = |1\rangle \otimes |0\rangle \quad |11\rangle = |1\rangle \otimes |1\rangle$$

Two qubits, more states

Two qubits state: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ or $e_{00}, e_{01}, e_{10}, e_{11}$

$$e_{00} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad e_{01} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad e_{10} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad e_{11} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Two qubits, more states

Two qubits state: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ or $e_{00}, e_{01}, e_{10}, e_{11}$

$$e_{00} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad e_{01} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad e_{10} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad e_{11} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Another set of basis states: from "plus" and "minus" states

$$|++\rangle = |+\rangle \otimes |+\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

$$|+-\rangle = |+\rangle \otimes |-\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

$$|-+\rangle = |-\rangle \otimes |+\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|00\rangle + |01\rangle - |10\rangle - |11\rangle}{2}$$

$$|--\rangle = |-\rangle \otimes |-\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{|00\rangle - |01\rangle - |10\rangle + |11\rangle}{2}$$

Two qubits, more states

More two qubits states: "plus" and "minus" states

$$|++\rangle = |+\rangle \otimes |+\rangle = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix} \otimes \begin{pmatrix}1\\1\end{pmatrix} = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

$$|+-\rangle = |+\rangle \otimes |-\rangle = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix} \otimes \begin{pmatrix}1\\-1\end{pmatrix} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

$$|-+\rangle = |-\rangle \otimes |+\rangle = \frac{1}{2}\begin{pmatrix}1\\-1\end{pmatrix} \otimes \begin{pmatrix}1\\1\end{pmatrix} = \frac{|00\rangle + |01\rangle - |10\rangle - |11\rangle}{2}$$

$$|--\rangle = |-\rangle \otimes |-\rangle = \frac{1}{2}\begin{pmatrix}1\\-1\end{pmatrix} \otimes \begin{pmatrix}1\\-1\end{pmatrix} = \frac{|00\rangle - |01\rangle - |10\rangle + |11\rangle}{2}$$

Two qubits, more states

More two qubits states: “plus” and “minus” states

$$|++\rangle = |+\rangle \otimes |+\rangle = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix} \otimes \begin{pmatrix}1\\1\end{pmatrix} = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

$$|+-\rangle = |+\rangle \otimes |-\rangle = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix} \otimes \begin{pmatrix}1\\-1\end{pmatrix} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

$$|-+\rangle = |-\rangle \otimes |+\rangle = \frac{1}{2}\begin{pmatrix}1\\-1\end{pmatrix} \otimes \begin{pmatrix}1\\1\end{pmatrix} = \frac{|00\rangle + |01\rangle - |10\rangle - |11\rangle}{2}$$

$$|--\rangle = |-\rangle \otimes |-\rangle = \frac{1}{2}\begin{pmatrix}1\\-1\end{pmatrix} \otimes \begin{pmatrix}1\\-1\end{pmatrix} = \frac{|00\rangle - |01\rangle - |10\rangle + |11\rangle}{2}$$

Orthonormal basis: Linearly independent and mutually orthogonal vectors.

Two qubits, more states

More two qubits states: "plus" and "minus" states

$$|++\rangle = |+\rangle \otimes |+\rangle = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix} \otimes \begin{pmatrix}1\\1\end{pmatrix} = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

$$|+-\rangle = |+\rangle \otimes |-\rangle = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix} \otimes \begin{pmatrix}1\\-1\end{pmatrix} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

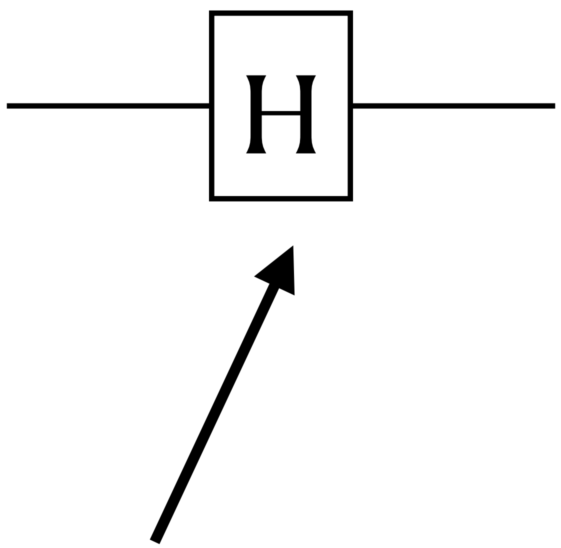
$$|-+\rangle = |-\rangle \otimes |+\rangle = \frac{1}{2}\begin{pmatrix}1\\-1\end{pmatrix} \otimes \begin{pmatrix}1\\1\end{pmatrix} = \frac{|00\rangle + |01\rangle - |10\rangle - |11\rangle}{2}$$

$$|--\rangle = |-\rangle \otimes |-\rangle = \frac{1}{2}\begin{pmatrix}1\\-1\end{pmatrix} \otimes \begin{pmatrix}1\\-1\end{pmatrix} = \frac{|00\rangle - |01\rangle - |10\rangle + |11\rangle}{2}$$

Orthonormal basis: Linearly independent and mutually orthogonal vectors.

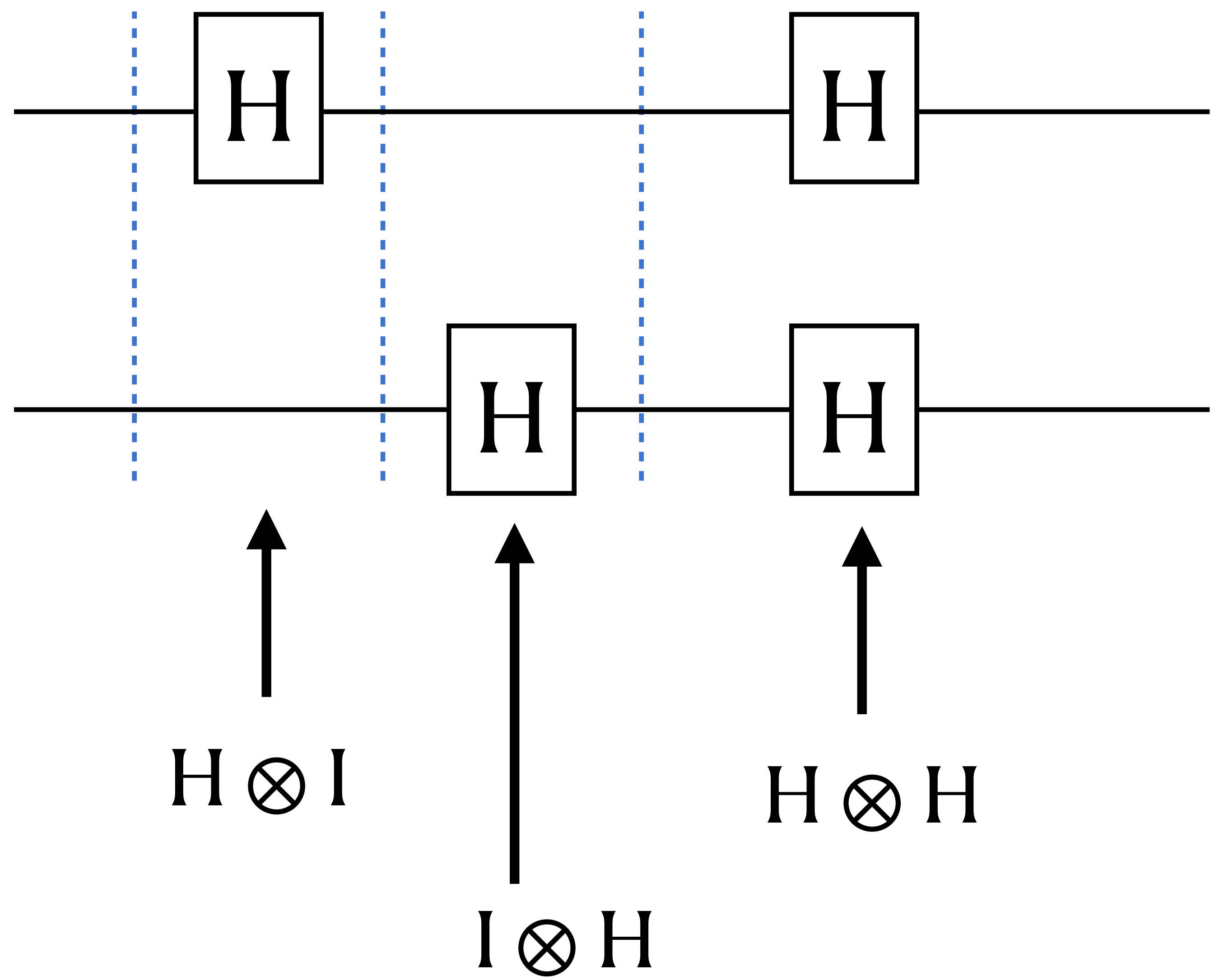
$$\frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\1 & -1 & 1 & -1\\1 & 1 & -1 & -1\\1 & -1 & -1 & 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} = \mathrm{H} \otimes \mathrm{H} = H^{\otimes 2}$$

2-qubit gate: from single-qubit gates



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

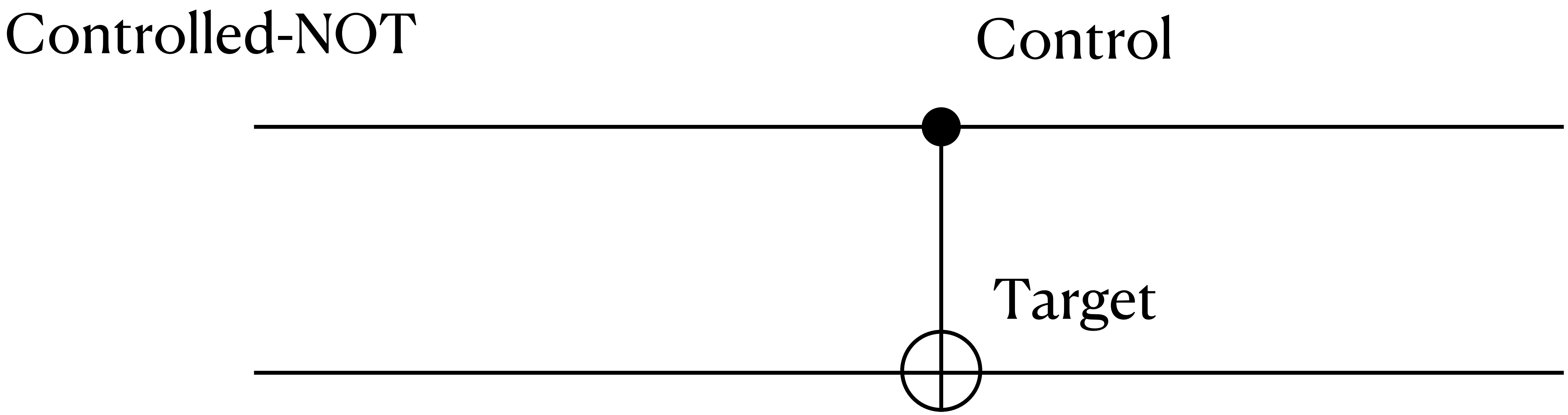
Example: $H|0\rangle = |+\rangle$



Quantum circuit: go left-to-right, like music on a staff,
but we apply matrices to vectors going right-to-left.

Example: $(H \otimes I)|01\rangle = (H|0\rangle) \otimes (I|1\rangle) = |+\rangle \otimes |1\rangle$

2-qubit gate: CNOT gate



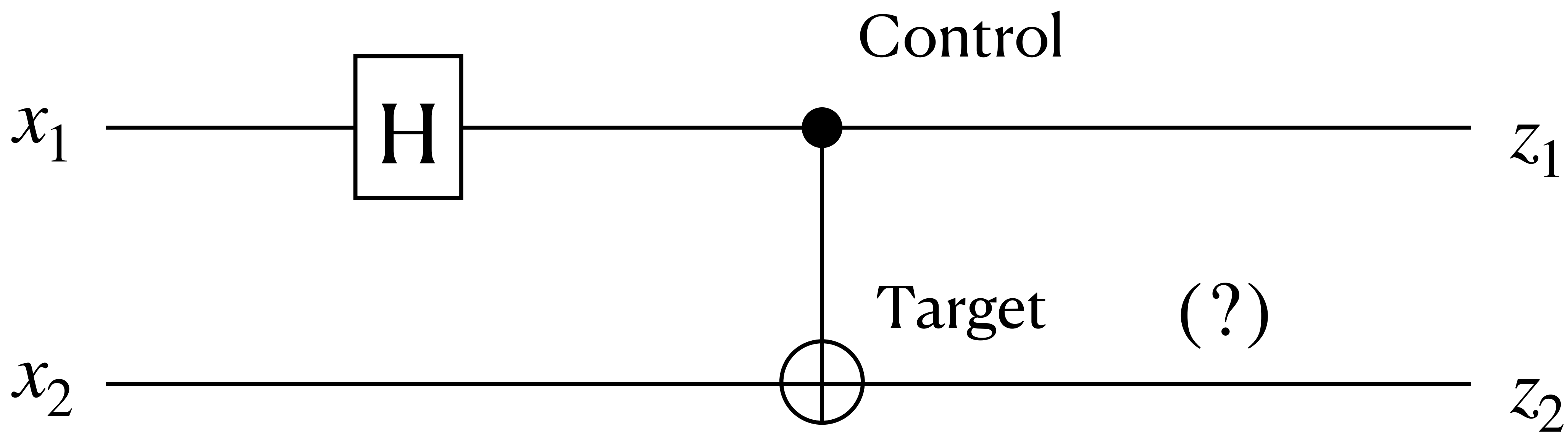
If the first qubit is 0, then the whole gate acts as the identity;

If the first qubit is 1, then the basis value of the second qubits flipped (Not gate X)

$$\mathrm{CNOT} = \begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & 1 & 0 & 0 & 0 \\ 01 & 0 & 1 & 0 & 0 \\ 10 & 0 & 0 & 0 & 1 \\ 11 & 0 & 0 & 1 & 0 \end{array}$$

Example: $\mathrm{CNOT}\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \\ d \\ c \end{pmatrix}$

Example: H gate and CNOT gate

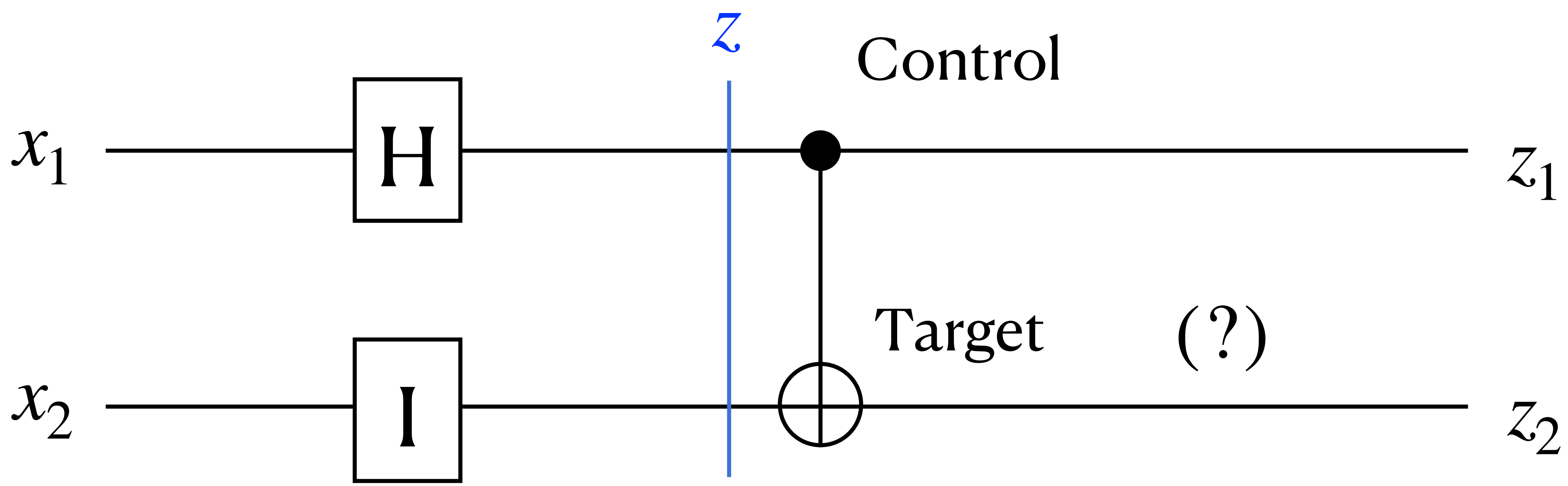


What's the output?

$$z_1 = \mathrm{H}x_1$$
$$z_2 = x_2 \oplus z_1$$

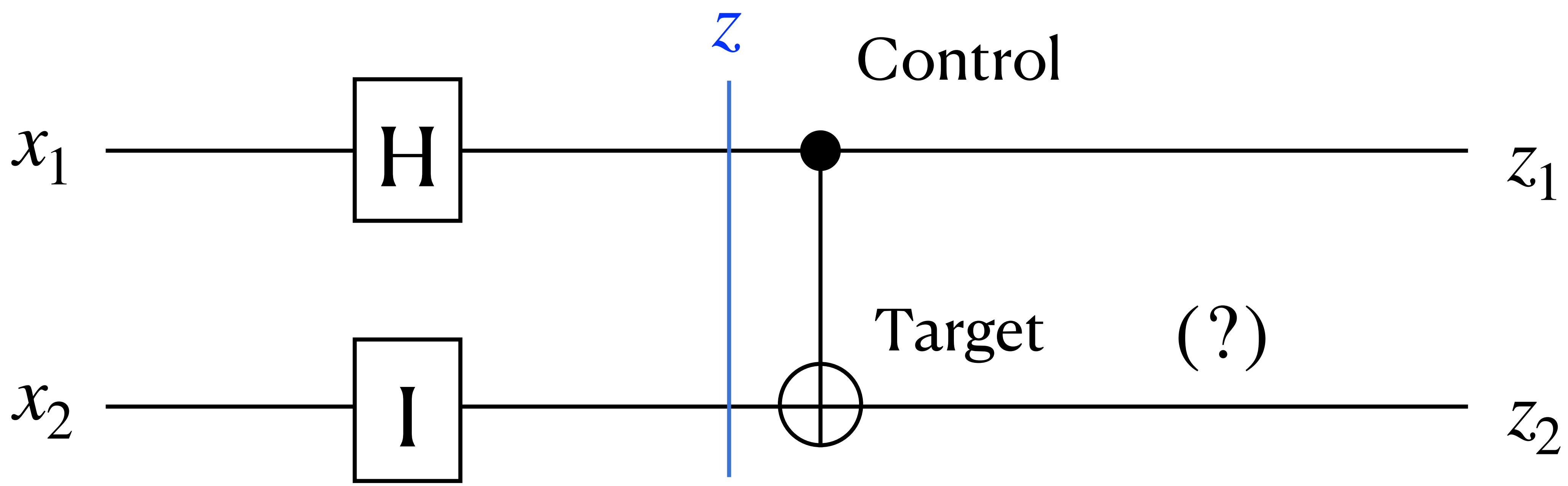
} Symbolic outputs

Example: H gate and CNOT gate



For example, if $|x_1 x_2\rangle = e_{00}$,

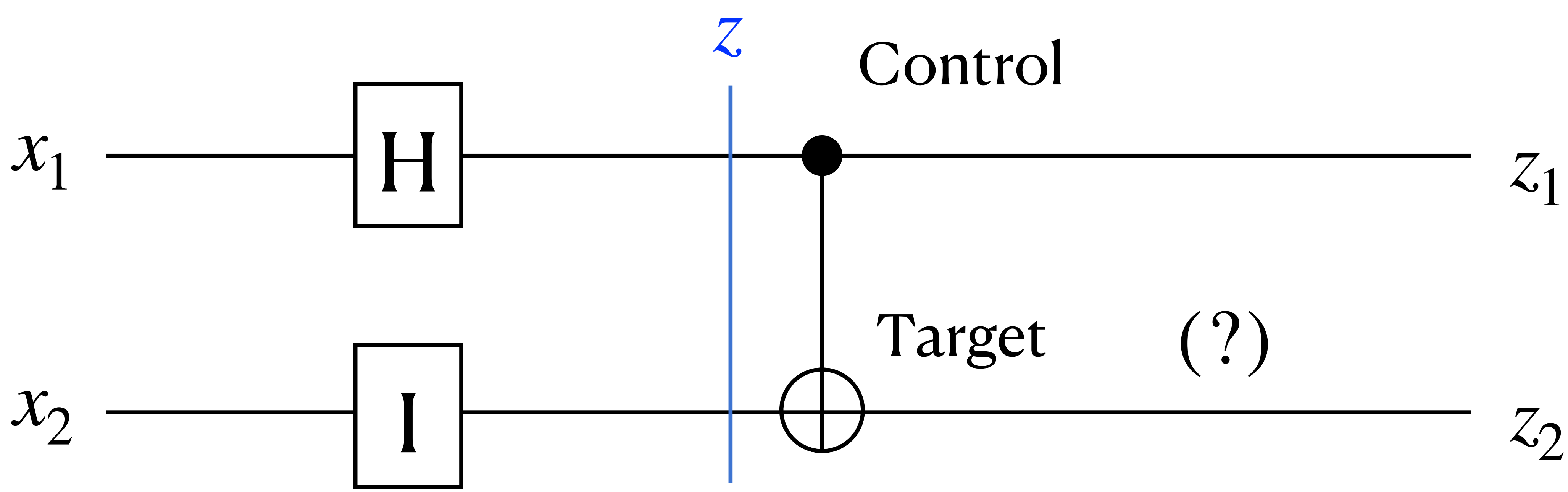
Example: H gate and CNOT gate



For example, if $|x_1 x_2\rangle = e_{00}$,

$$\mathrm{H} \otimes \mathrm{I} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

Example: H gate and CNOT gate

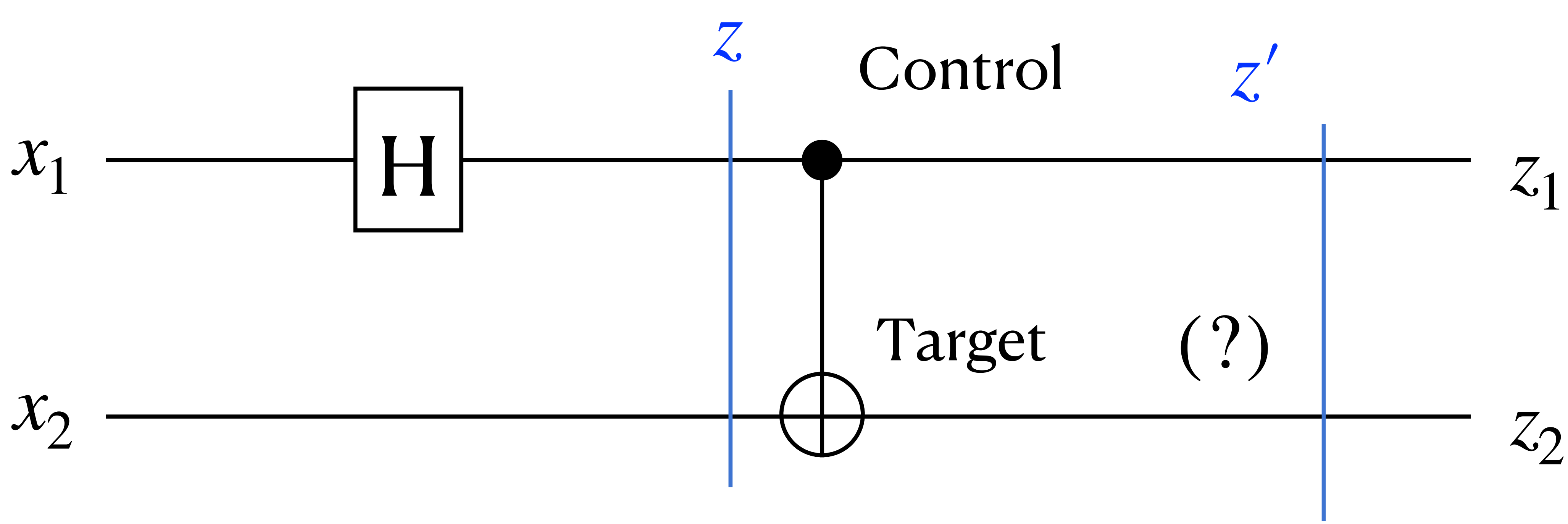


For example, if $|x_1x_2\rangle = e_{00}$,

$$H \otimes I = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{pmatrix}$$

$$z = (H \otimes I)e_{00} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\\ 0\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 0\\ 1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}|+\rangle \otimes |0\rangle$$

Example: H gate and CNOT gate

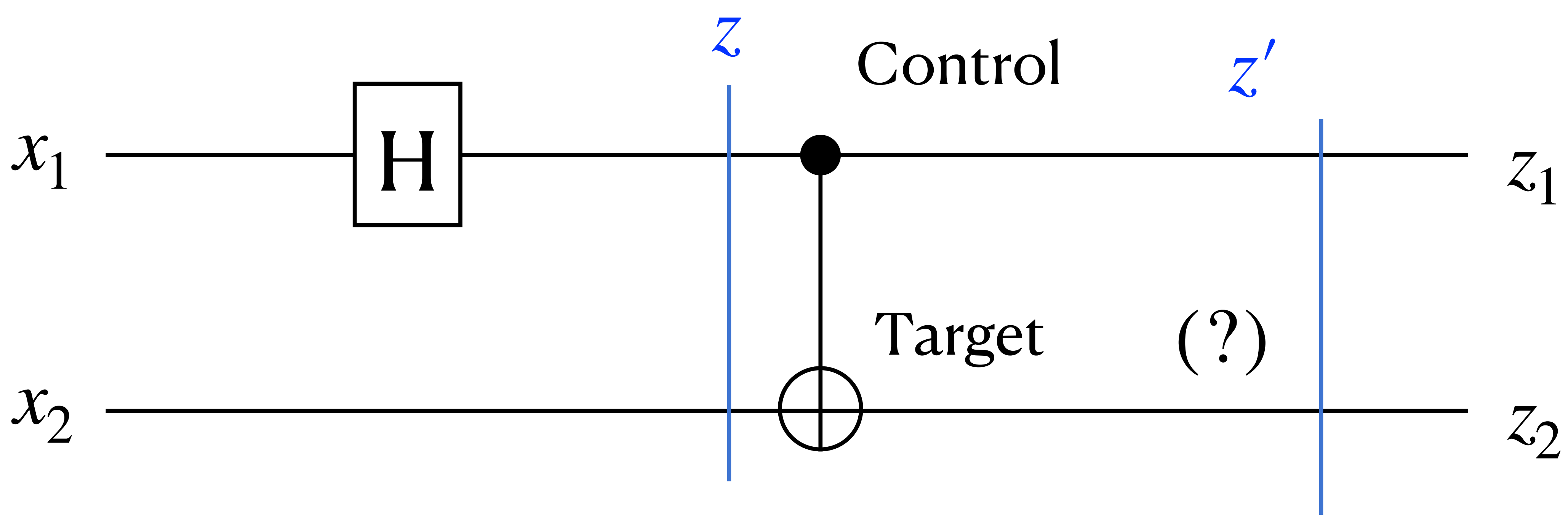


For example, if $|x_1x_2\rangle = e_{00}$,

$$z = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}|+\rangle \otimes |0\rangle$$

$$z' = \text{CNOT}\ z = \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1\\0\\1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$$

Example: H gate and CNOT gate

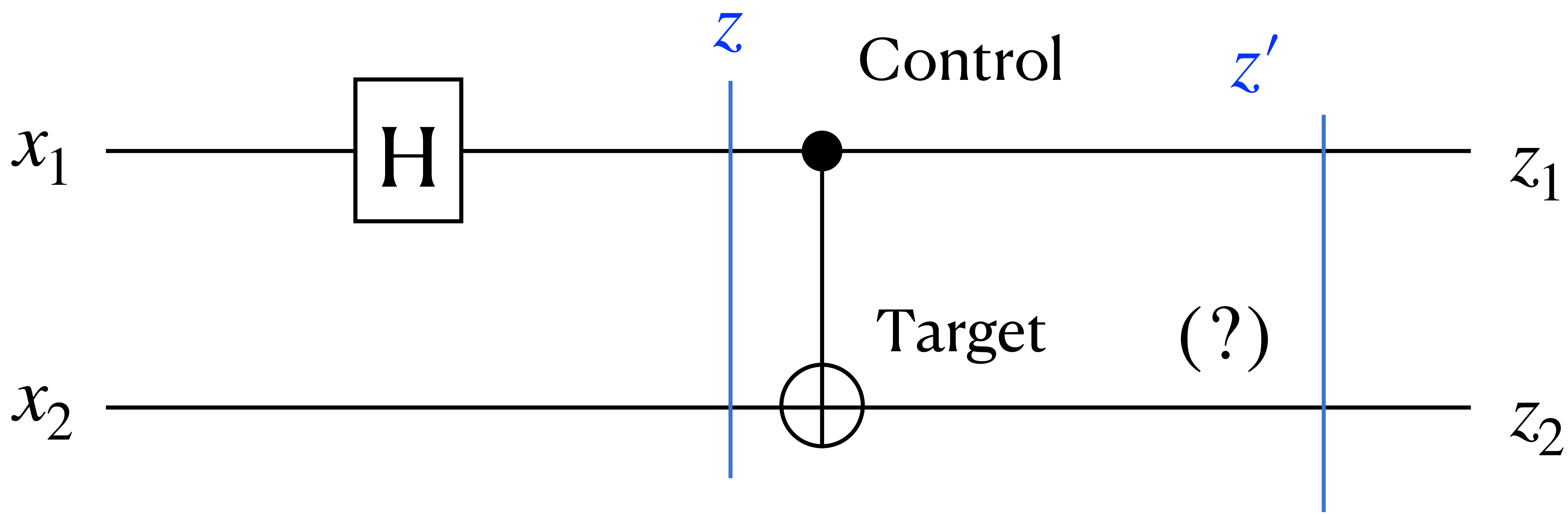


For example, if $|x_1x_2\rangle = e_{00}$,

$$z = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}|+\rangle \otimes |0\rangle$$

$$z' = \text{CNOT}\ z = \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1\\0\\1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Example: H gate and CNOT gate



For example, if $|x_1x_2\rangle = e_{00}$,

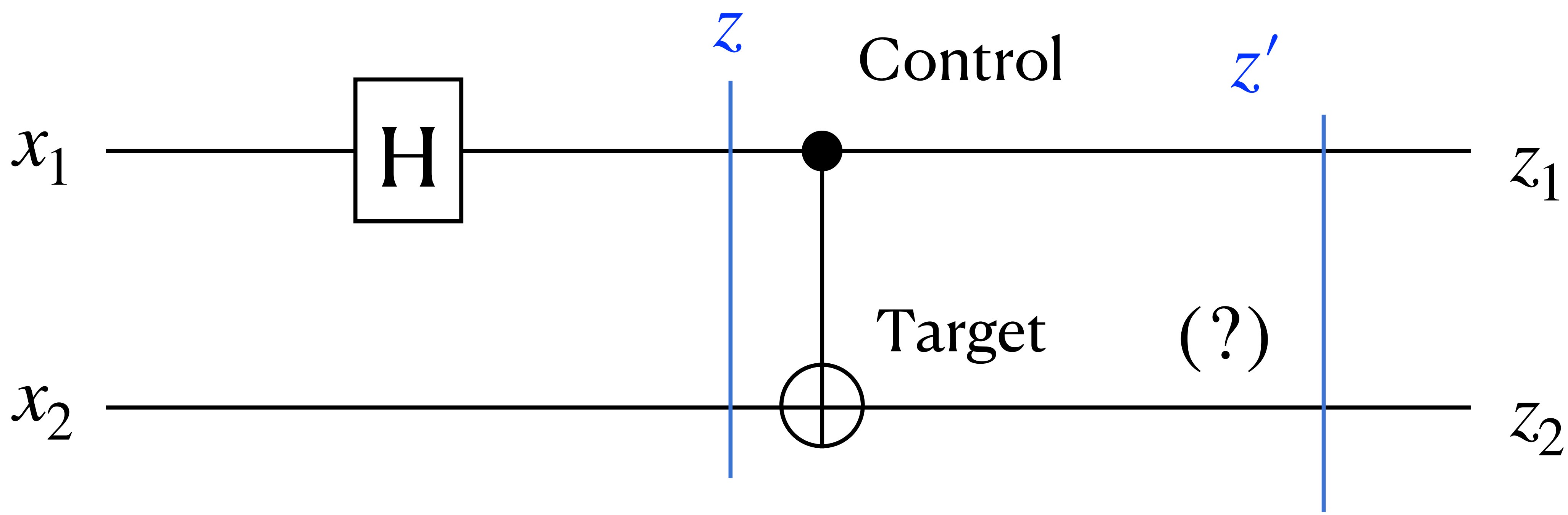
$$z = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}|+\rangle \otimes |0\rangle$$

Separatable

$$z' = \text{CNOT}\ z = \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1\\0\\1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Entangled

Example: H gate and CNOT gate



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

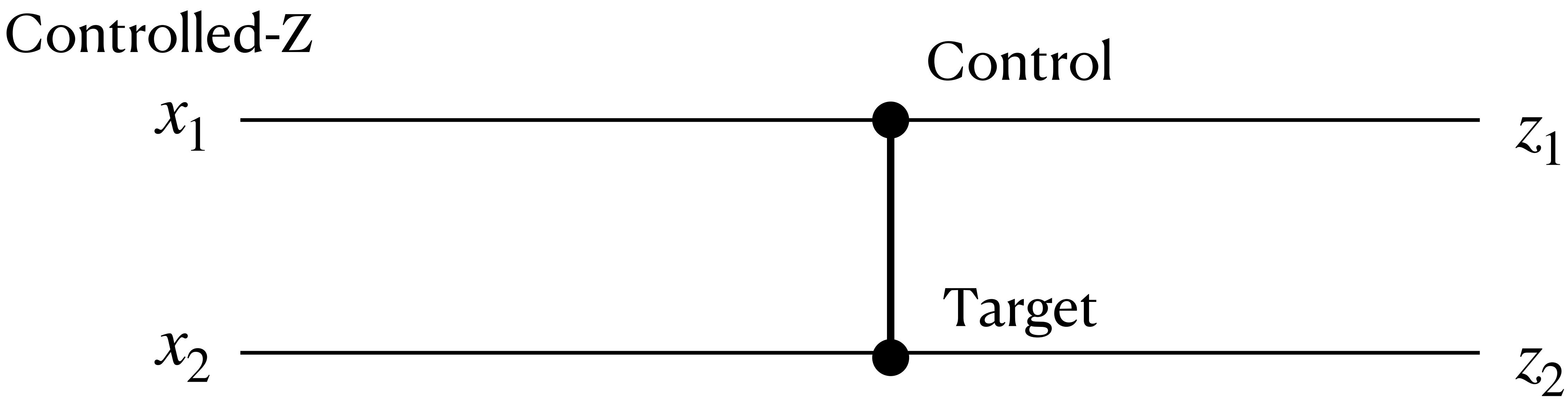
Entangled

Definition: A quantum state is **entangled** if it cannot be written as a tensor product of smaller states.

https://wybiral.github.io/quantum/

https://algassert.com/quirk#circuit=%7B%22cols%22:%5B%5D%7D

2-qubit gate: CZ gate

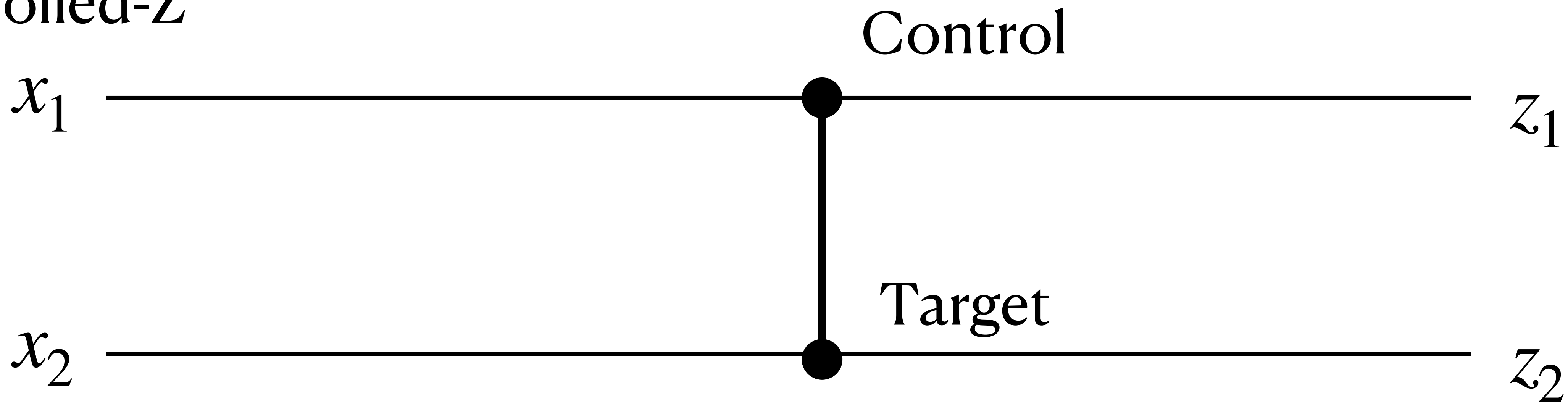


$$\mathrm{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

If both bits are 1, flip the sign;
Else, do nothing

2-qubit gate: CZ gate

Controlled-Z



Example:

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

$$\mathrm{CZ}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad \mathrm{CZ}\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -1 \end{pmatrix}$$

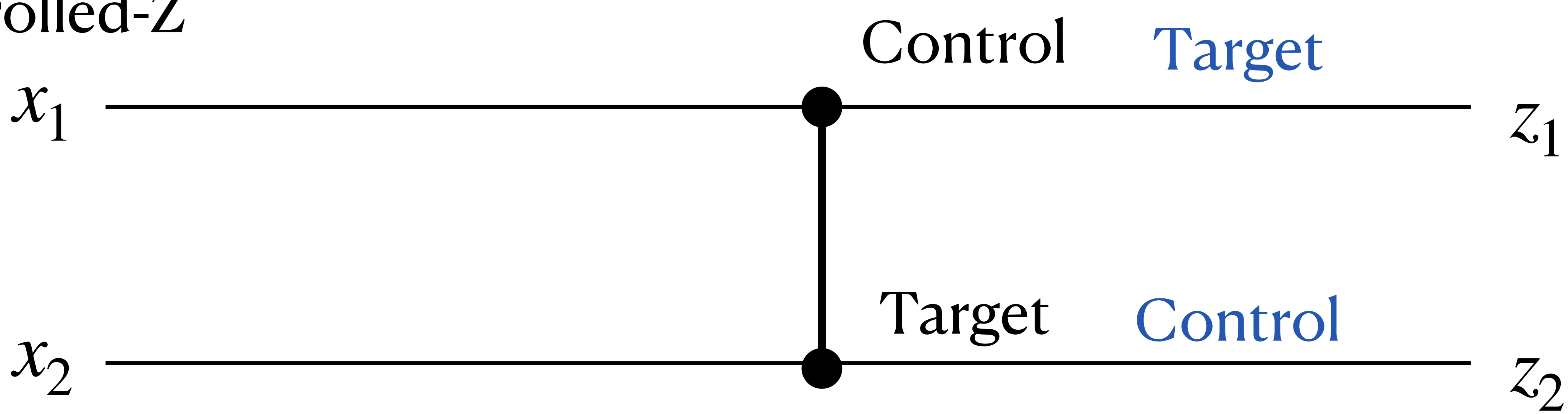
$$\mathrm{CZ}|01\rangle = |01\rangle \qquad \mathrm{CZ}|11\rangle = |1\rangle \otimes (-|1\rangle)$$

$$= |1\rangle \otimes e^{i\pi}|1\rangle$$

If both bits are 1, flip the sign;
Else, do nothing

2-qubit gate: CZ gate

Controlled-Z



Example:

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

$$CZ \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad CZ \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -1 \end{pmatrix}$$

$$CZ|01\rangle = |01\rangle \qquad CZ|11\rangle = |1\rangle \otimes (-|1\rangle)$$

$$= |1\rangle \otimes e^{i\pi}|1\rangle$$

If both bits are 1, flip the sign;
Else, do nothing

Symmetric

Other 2-qubit (symmetric) gates: CA gate

$$\mathrm{CA} = \begin{pmatrix} \mathrm{I} & 0 \\ 0 & \mathrm{A} \end{pmatrix}$$

$2r \times 2r$ matrix for general $r \times r$ matrix A

Other 2-qubit (symmetric) gates: CA gate

$$\mathrm{CA} = \begin{pmatrix} \mathrm{I} & 0 \\ 0 & \mathrm{A} \end{pmatrix}$$

$2r \times 2r$ matrix for general $r \times r$ matrix A

Example:

$$\mathrm{CS} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}$$

$$\mathrm{CS}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$\mathrm{CS}\,|01\rangle = |01\rangle$$

$$\mathrm{CS}\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ i \end{pmatrix}$$

$$\mathrm{CS}\,|11\rangle = |1\rangle \otimes (i\,|1\rangle) = |1\rangle \otimes e^{i\pi/2}\,|1\rangle$$

Other 2-qubit (symmetric) gates: CA gate

$$CA = \begin{pmatrix} I & 0 \\ 0 & A \end{pmatrix}$$

$2r \times 2r$ matrix for general $r \times r$ matrix A

Example:

$$CS = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}$$

$$CS \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$CS\,|01\rangle = |01\rangle$$

$$CS \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ i \end{pmatrix}$$

$$CS\,|11\rangle = |1\rangle \otimes (i\,|1\rangle) = |1\rangle \otimes e^{i\pi/2}\,|1\rangle$$

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

$$CT \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

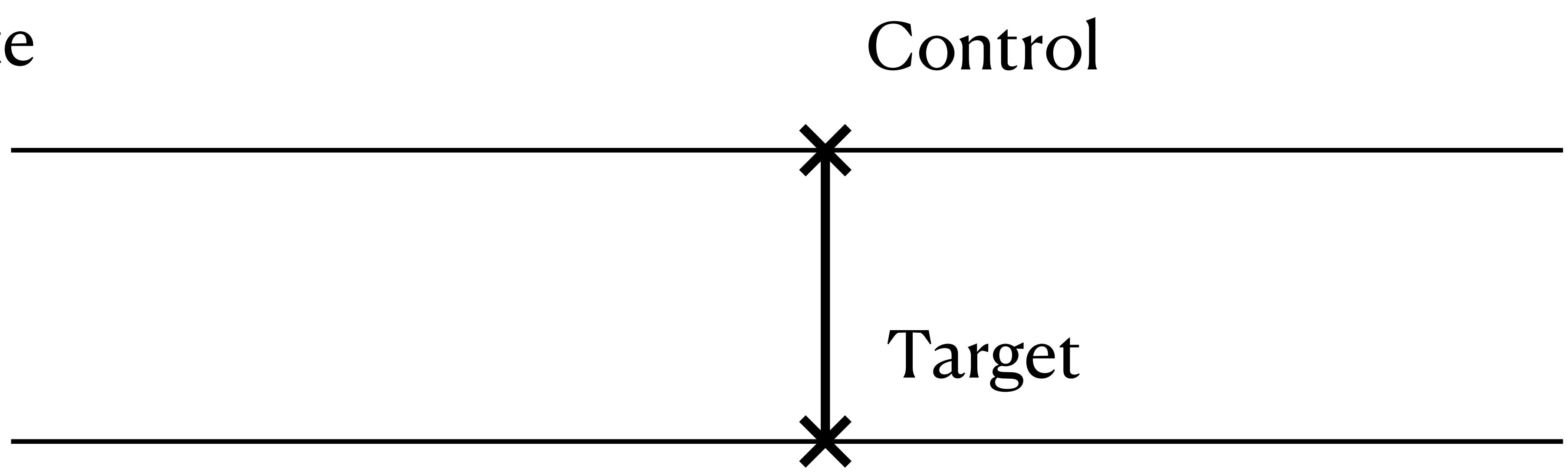
$$CT\,|01\rangle = |01\rangle$$

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

$$CT\,|11\rangle = |1\rangle \otimes e^{i\pi/4}\,|1\rangle$$

2-qubit gate: SWAP gate

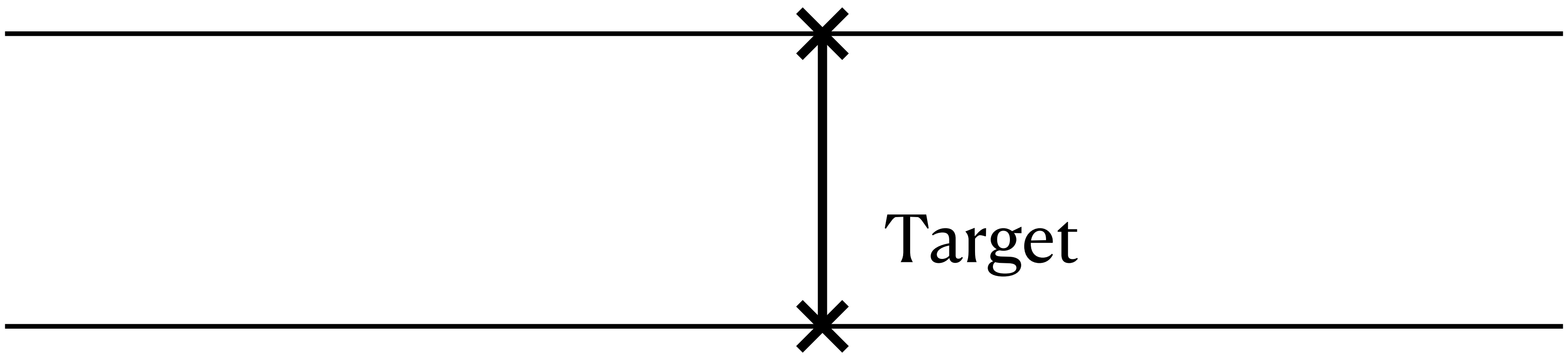
SWAP gate



$$\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

2-qubit gate: SWAP gate

SWAP gate



Example:

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\text{SWAP}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad \text{SWAP}\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$\text{SWAP}\,|01\rangle = |10\rangle \qquad \text{SWAP}\,|10\rangle = |01\rangle$

Content

- Recall: Qubits and Circuits
- The Bloch Sphere
- Two Qubits
- **Three Qubits and More**

More qubits, basic basis

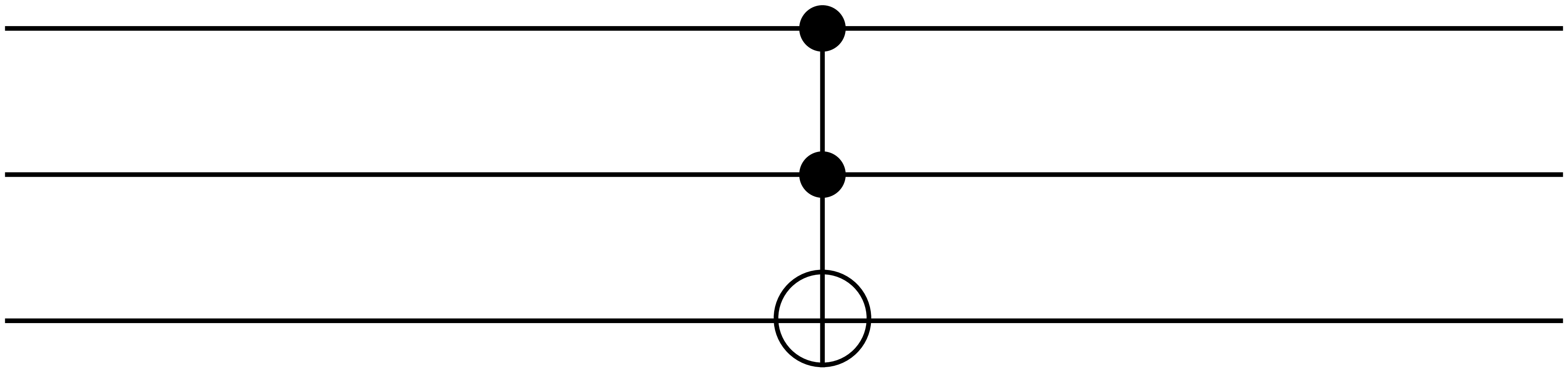
Three qubits state: $|000\rangle, |001\rangle, |010\rangle, \ldots$

Four qubits state: $|0000\rangle, |0001\rangle, |0010\rangle, \ldots$

n qubits state: 2^n basic or standard states

3-qubit gate: Toffoli gate (Tof)

Toffoli gate

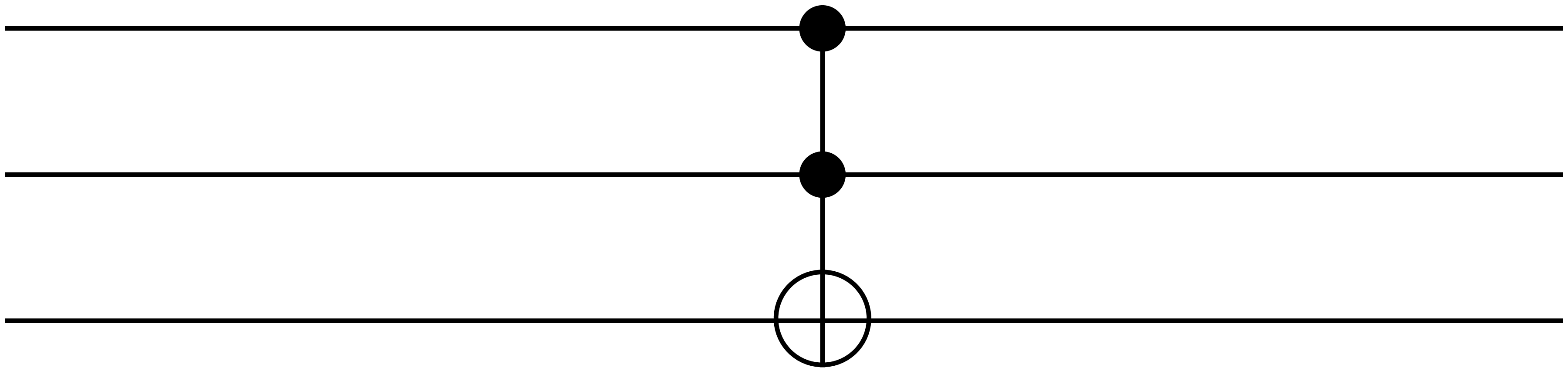


If the first two qubit are 1, then the basis value of the **third** qubits flipped

Otherwise, the whole gate acts as the identity;

3-qubit gate: toffoli gate (Tof)

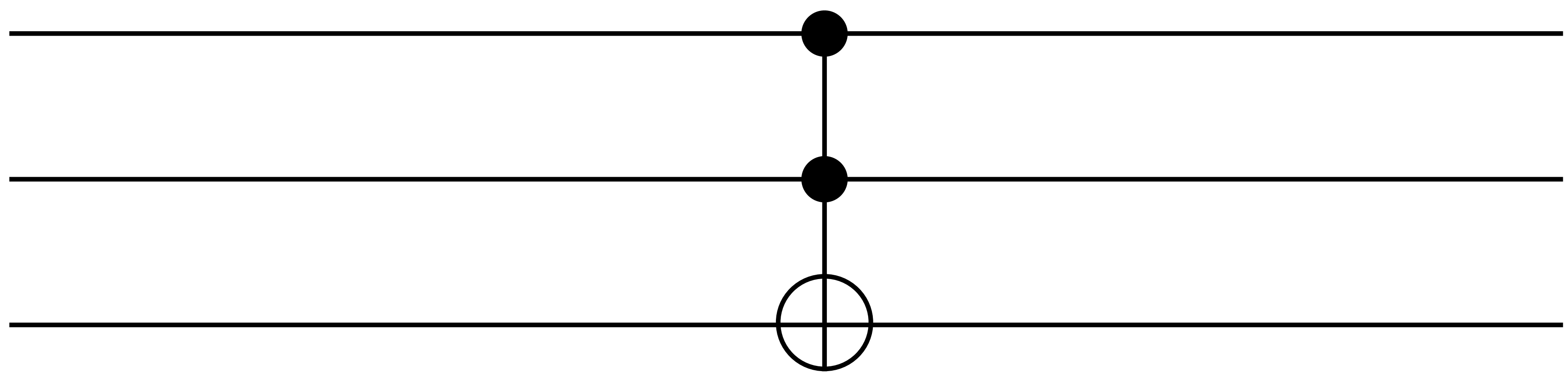
Toffoli gate



$$\mathrm{Tof} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

3-qubit gate: toffoli gate (Tof)

Toffoli gate

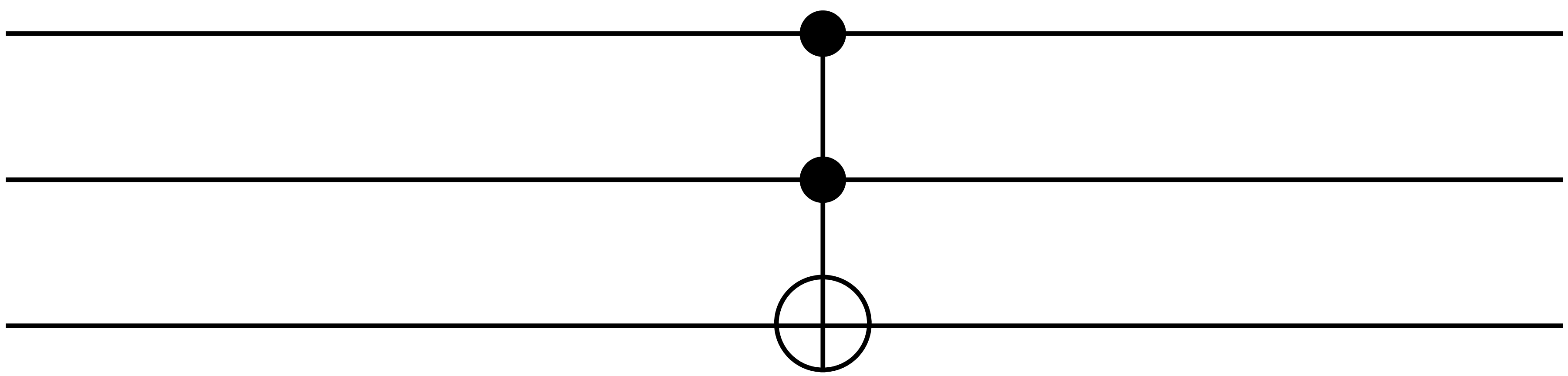


Tof =

	000	001	010	011	100	101	110	111
000	1	0	0	0	0	0	0	0
001	0	1	0	0	0	0	0	0
010	0	0	1	0	0	0	0	0
011	0	0	0	1	0	0	0	0
100	0	0	0	0	1	0	0	0
101	0	0	0	0	0	1	0	0
110	0	0	0	0	0	0	0	1
111	0	0	0	0	0	0	1	0

3-qubit gate: toffoli gate (Tof)

Toffoli gate



Tof =

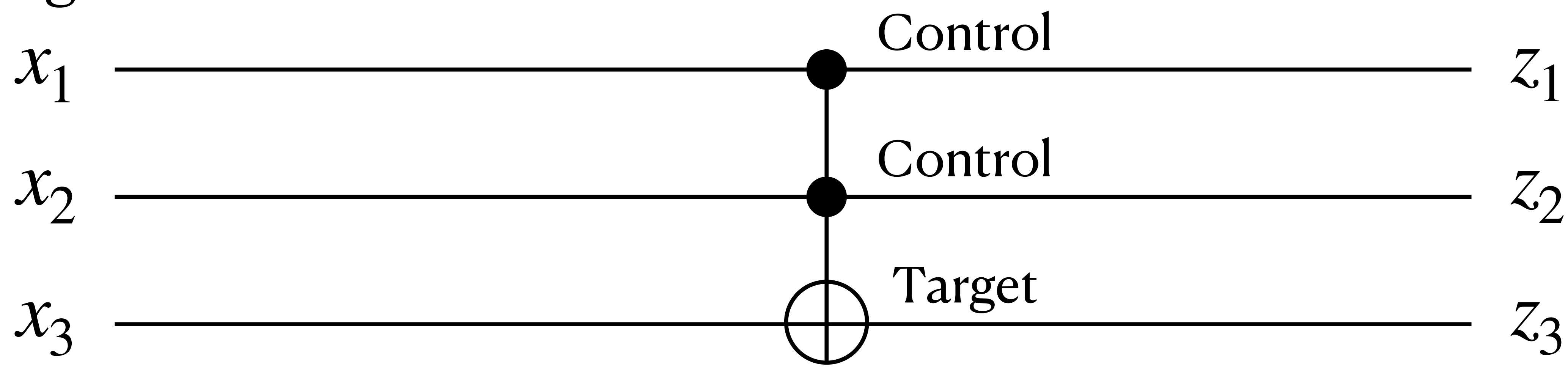
	000	001	010	011	100	101	110	111
000	1	0	0	0	0	0	0	0
001	0	1	0	0	0	0	0	0
010	0	0	1	0	0	0	0	0
011	0	0	0	1	0	0	0	0
100	0	0	0	0	1	0	0	0
101	0	0	0	0	0	1	0	0
110	0	0	0	0	0	0	0	1
111	0	0	0	0	0	0	1	0

Example:

$$\text{Tof}\begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \\ h \\ g \end{pmatrix}$$

3-qubit gate: Toffoli gate (Tof)

Toffoli gate



What's the output?

$$z_1 = x_1$$

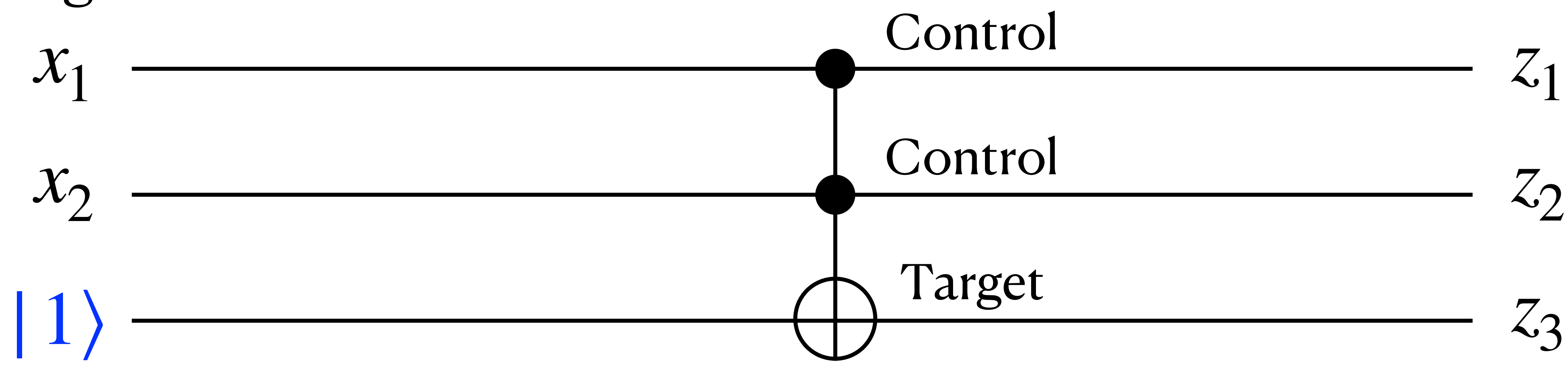
$$z_2 = x_2$$

$$z_3 = x_3 \oplus (x_1 \wedge x_2)$$

Symbolic outputs

3-qubit gate: Toffoli gate (Tof)

Toffoli gate



What's the output?

$$z_1 = x_1$$

$$z_2 = x_2$$

$$z_3 = |1\rangle \oplus (x_1 \wedge x_2) = \neg(x_1 \wedge x_2) = \text{NAND}(x_1, x_2)$$

Theorem

For fully time-constructible $t(n)$ between linear and exponential,

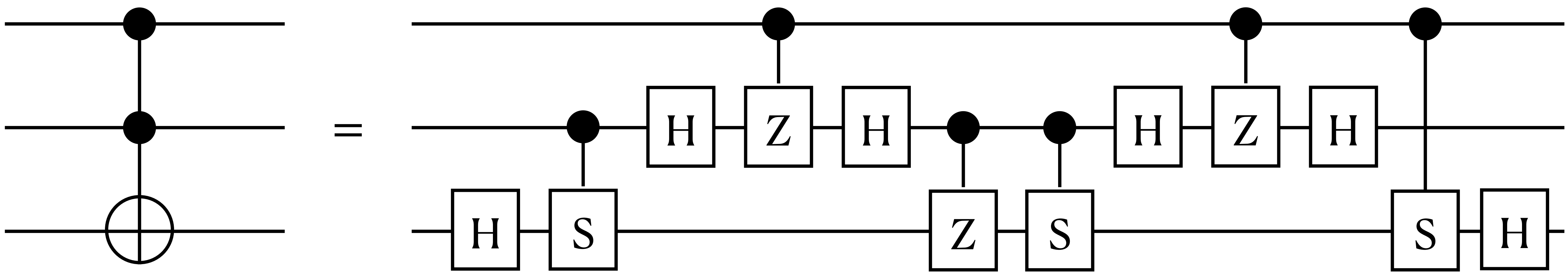
$$\mathrm{DTIME}[t(n)] \subseteq \mathrm{DQ}[\tilde{O}(t(n))]$$

Hadamard is the only **quantum-nondeterministic** gate one needs to add in order to extend the notion of *classical-feasible* to *quantum-feasible*.

The main point of the next two lectures, focusing on chapters 7 and 8 of the text, is to show the extra powers that this gives.

More about Toffoli gate

Toffoli gate

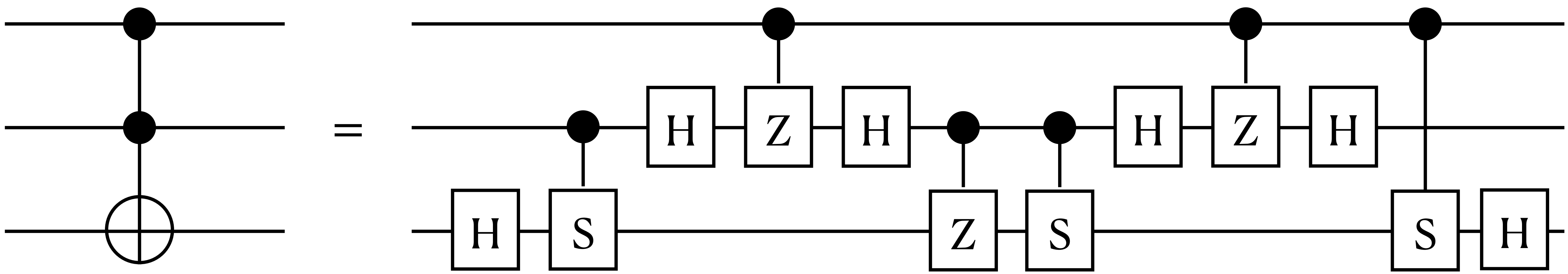


$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Only need to look at the effect on basis states.

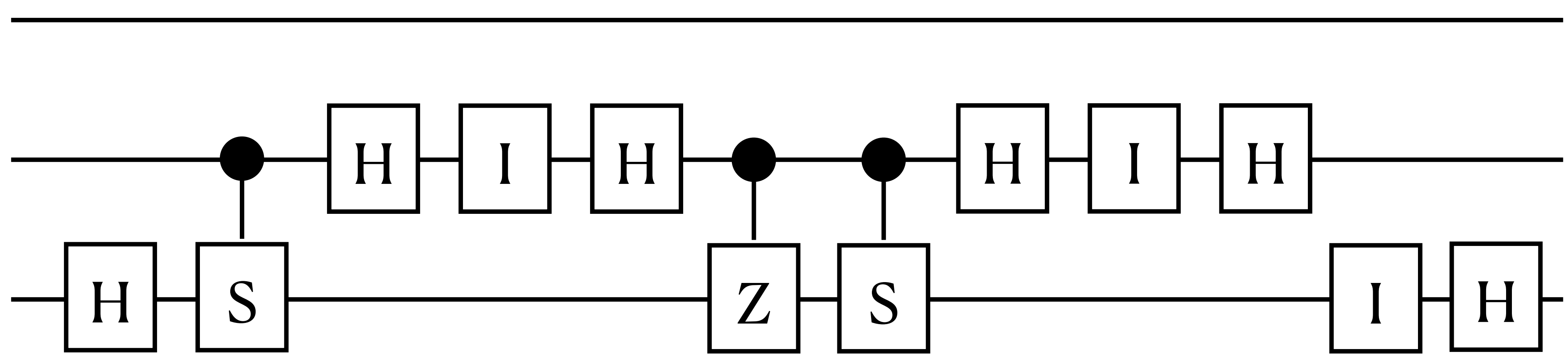
More about Toffoli gate

Toffoli gate



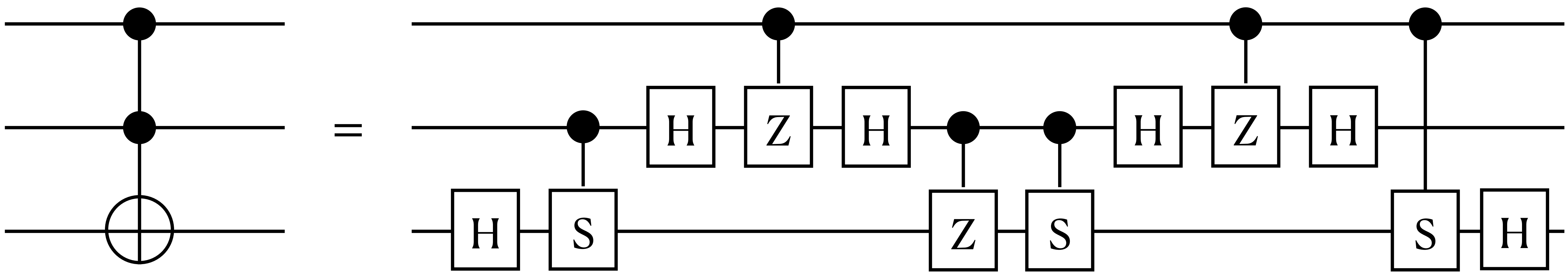
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Case 1: $x_1 = 0$



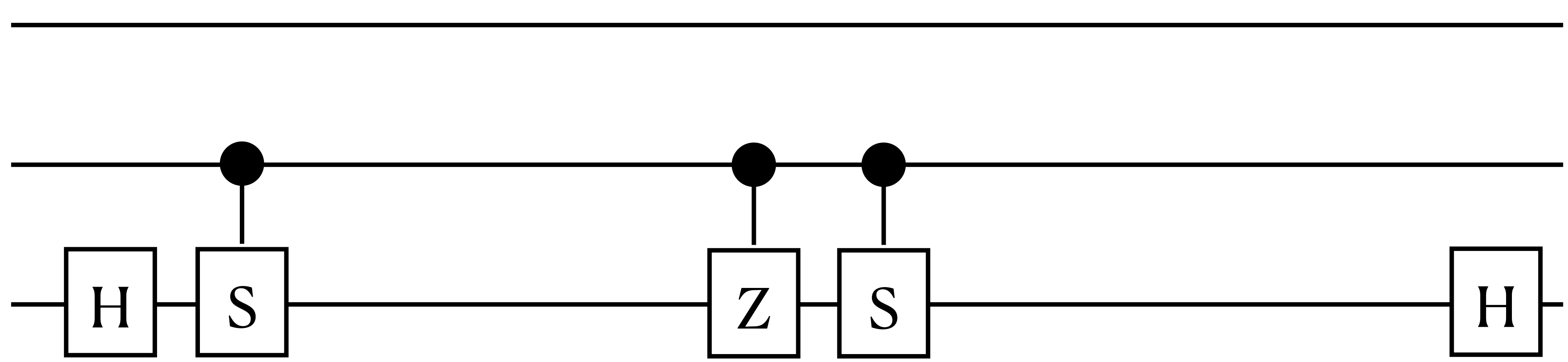
More about Toffoli gate

Toffoli gate



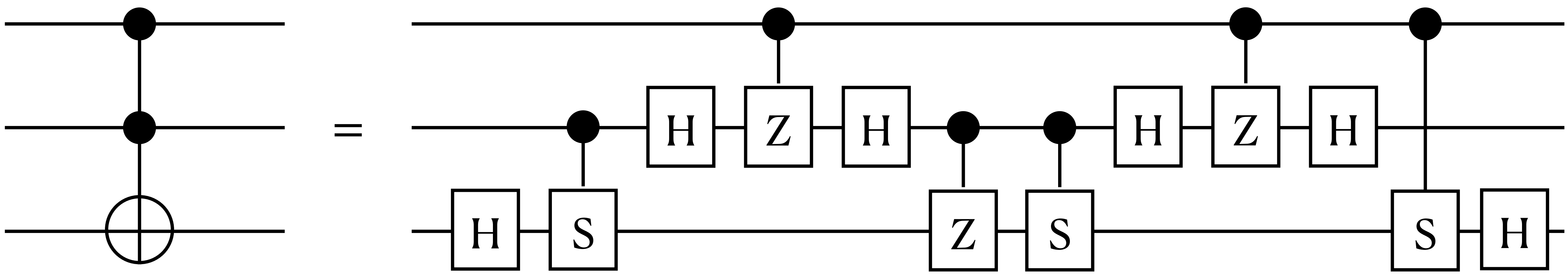
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Case 1: $x_1 = 0$



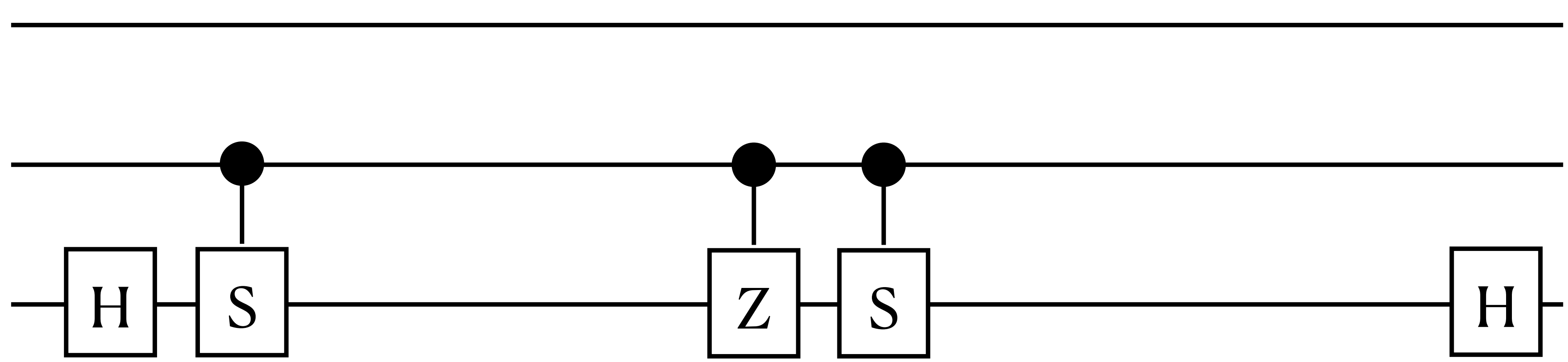
More about Toffoli gate

Toffoli gate



$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

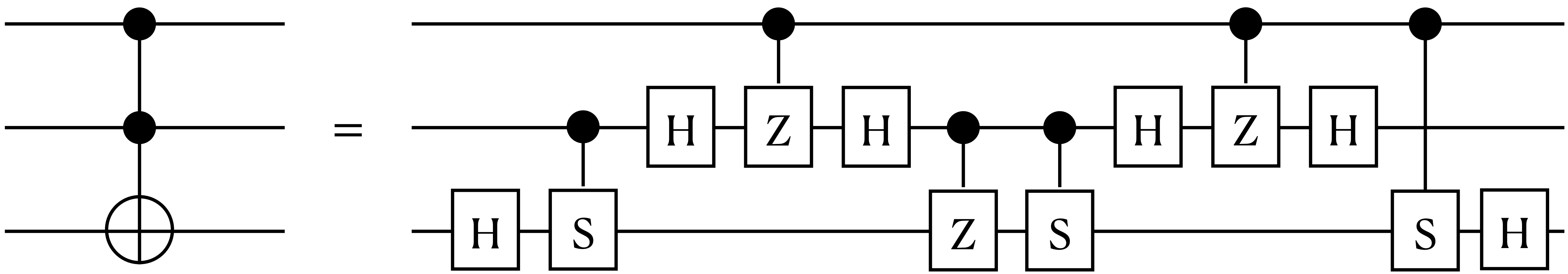
Case 1: $x_1 = 0$



SZS = I HH = I

More about Toffoli gate

Toffoli gate

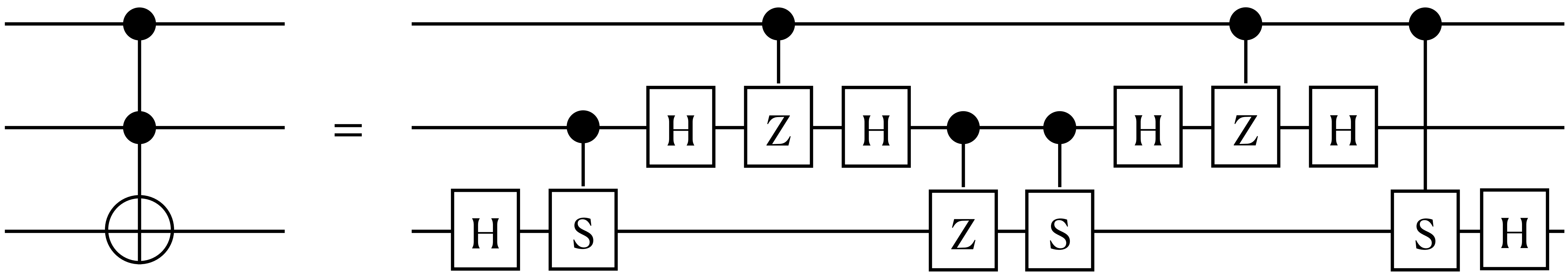


$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Case 1: $x_1 = 0$

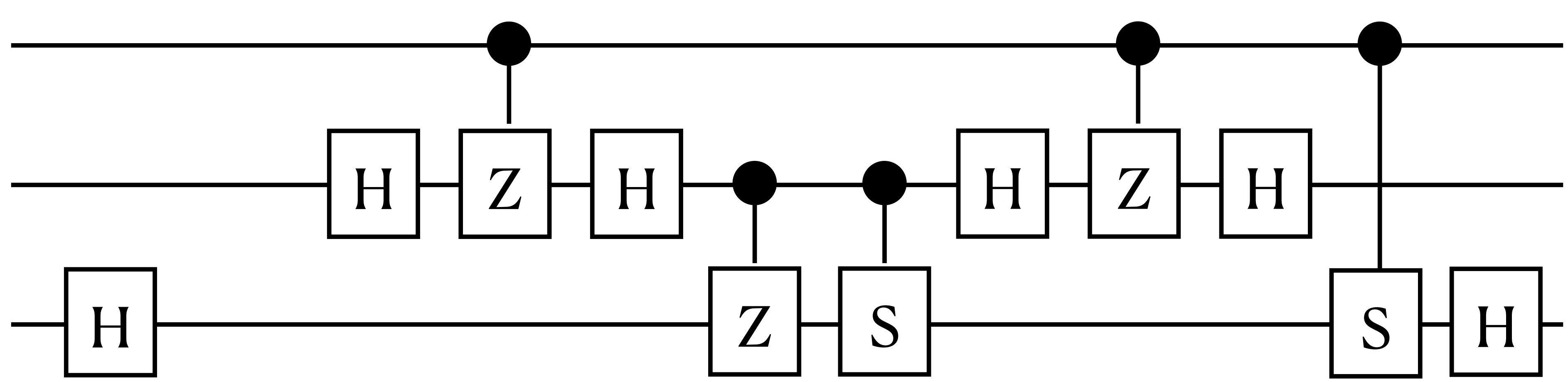
More about Toffoli gate

Toffoli gate



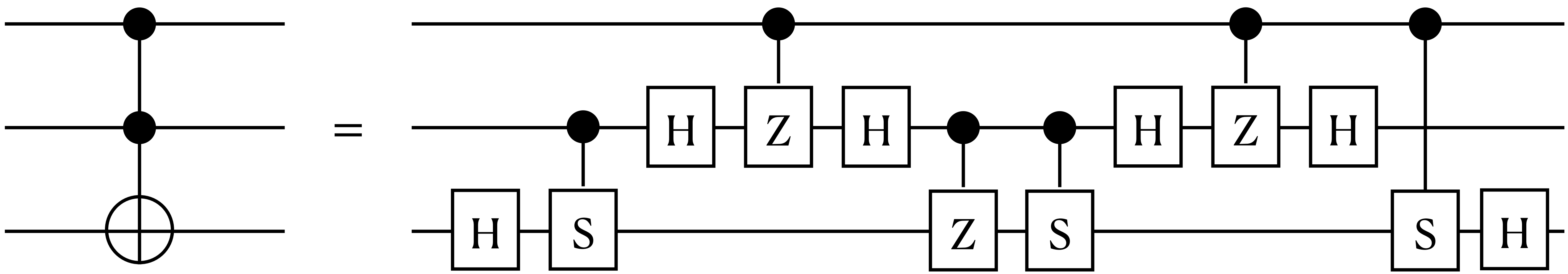
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Case 2: $x_1 = 1$
$x_2 = 0$



More about Toffoli gate

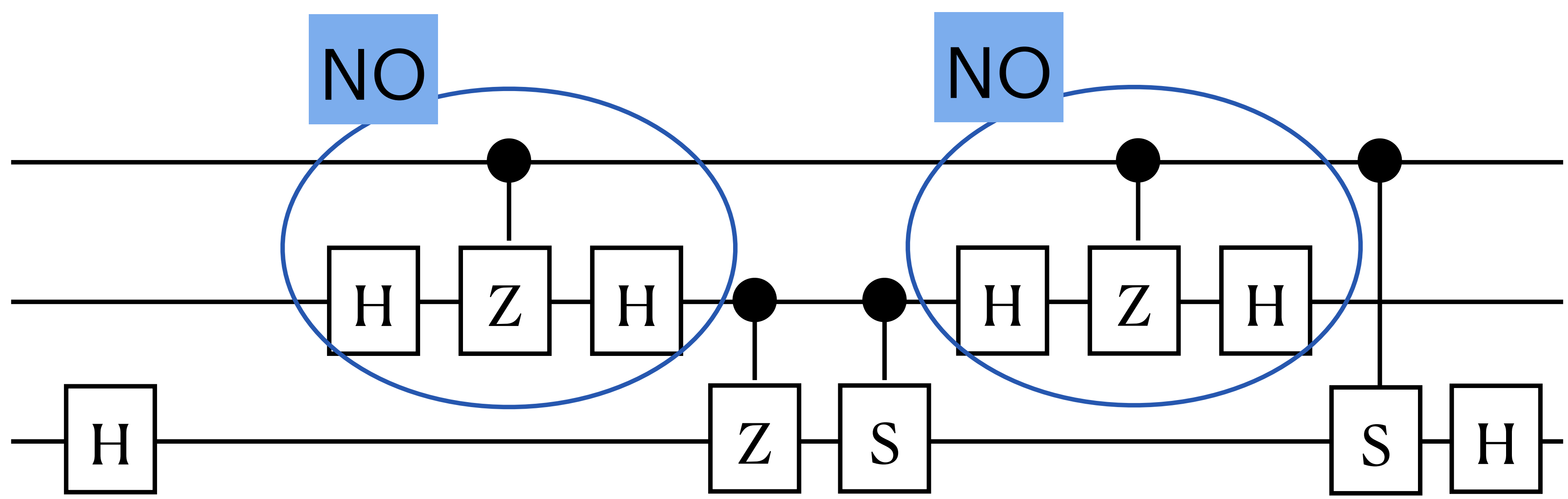
Toffoli gate



$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

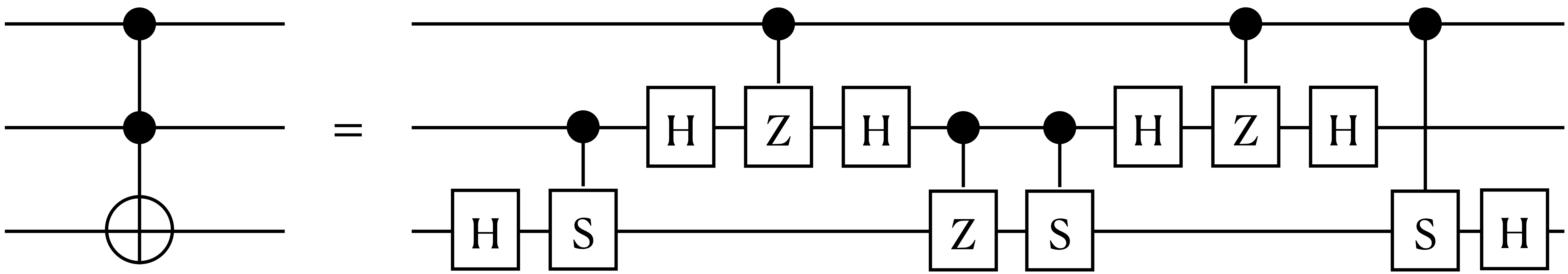
Case 2: $x_1 = 1$

$x_2 = 0$



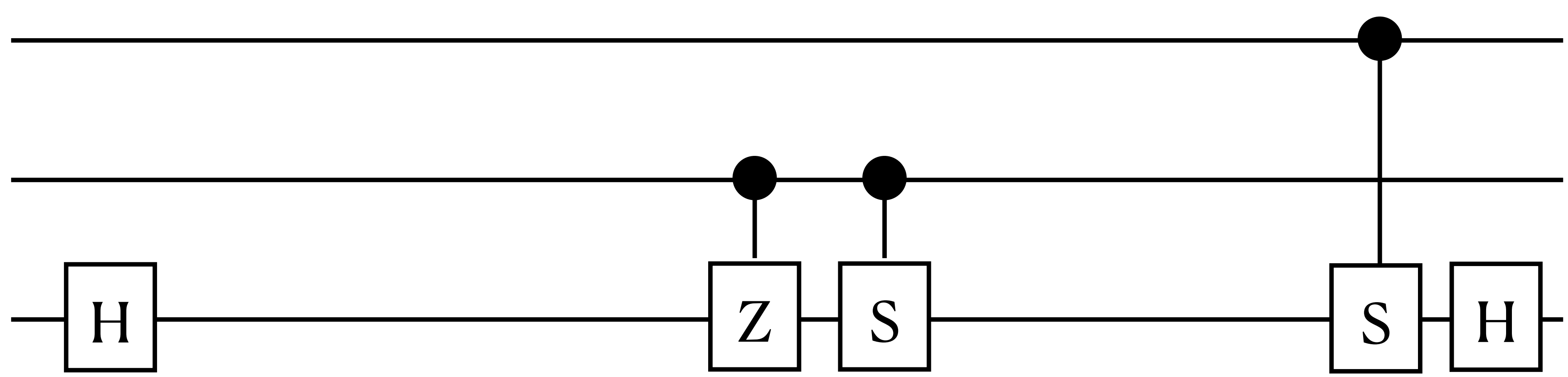
More about Toffoli gate

Toffoli gate



$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

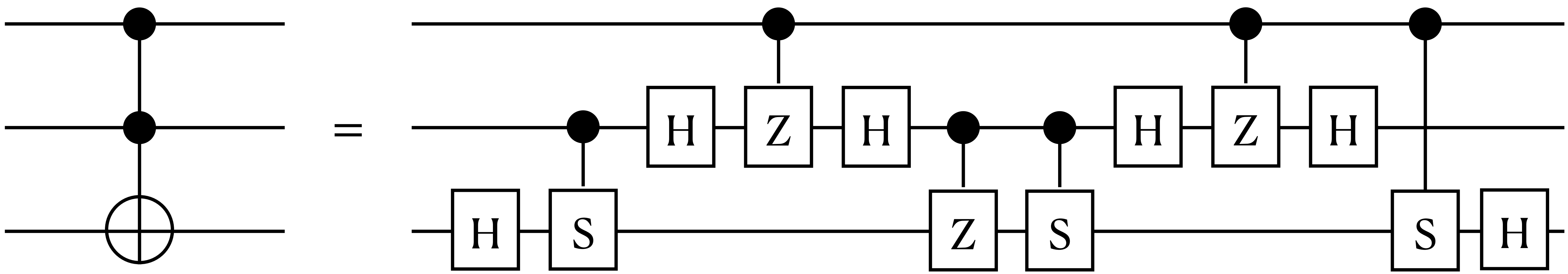
Case 2: $x_1 = 1$
$x_2 = 0$



ZSS = I   HH = I

More about Toffoli gate

Toffoli gate



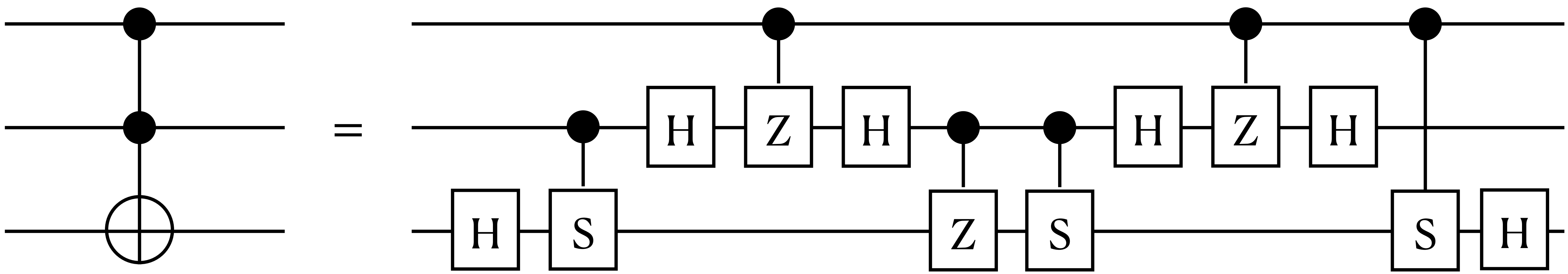
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Case 2: $x_1 = 1$

$x_2 = 0$

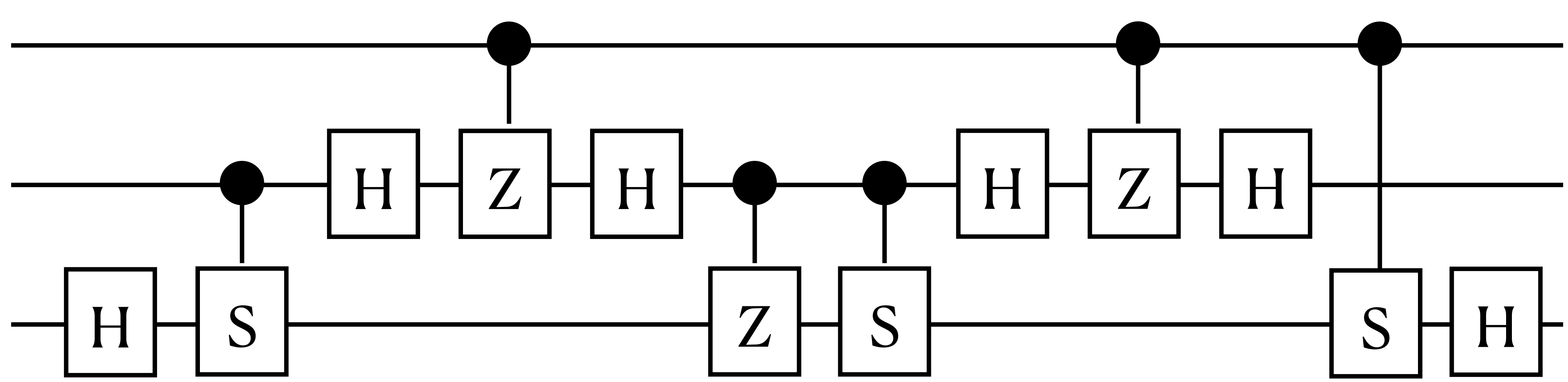
More about Toffoli gate

Toffoli gate



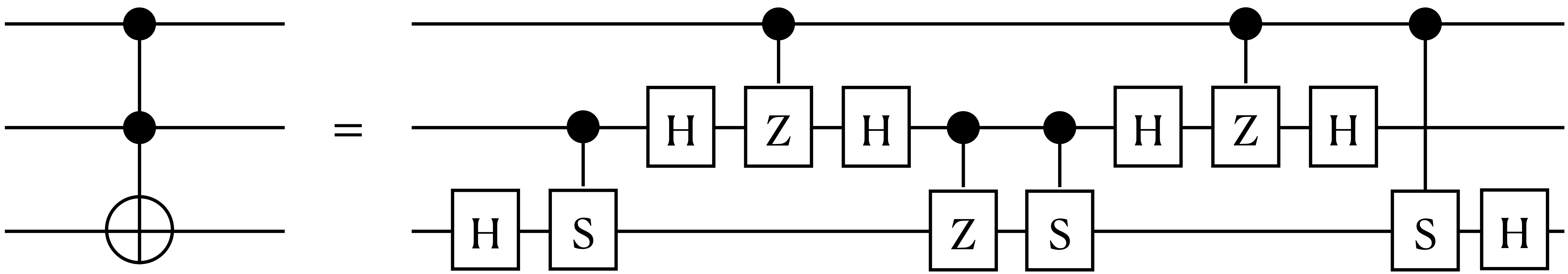
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Case 2: $x_1 = 1$
$x_2 = 1$



More about Toffoli gate

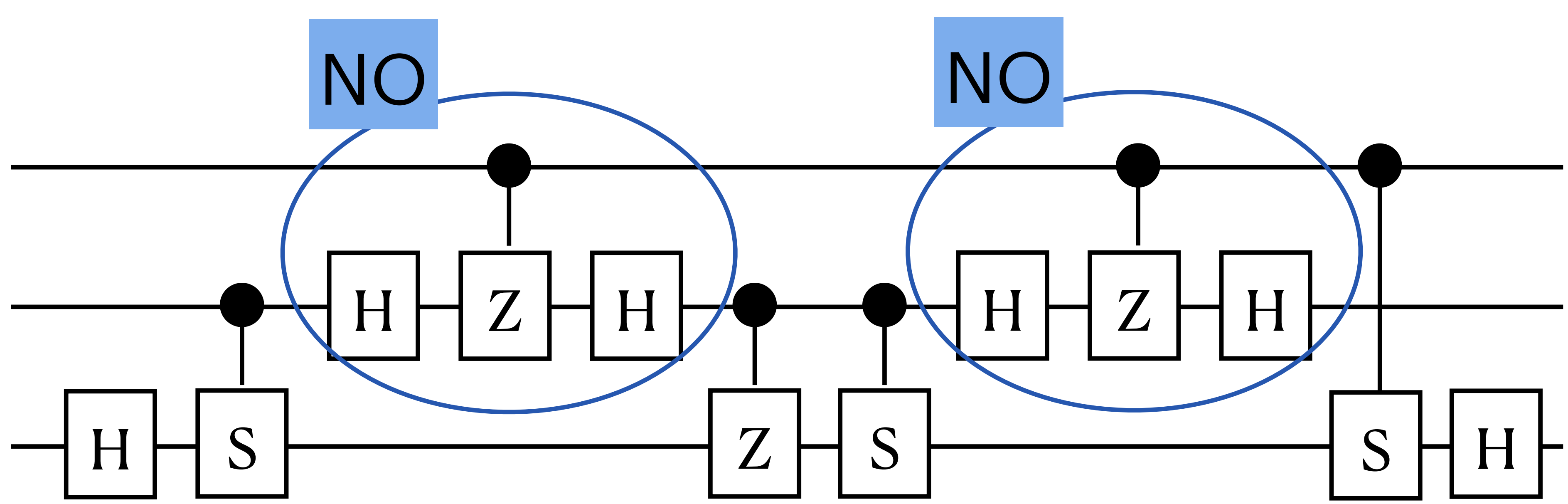
Toffoli gate



$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

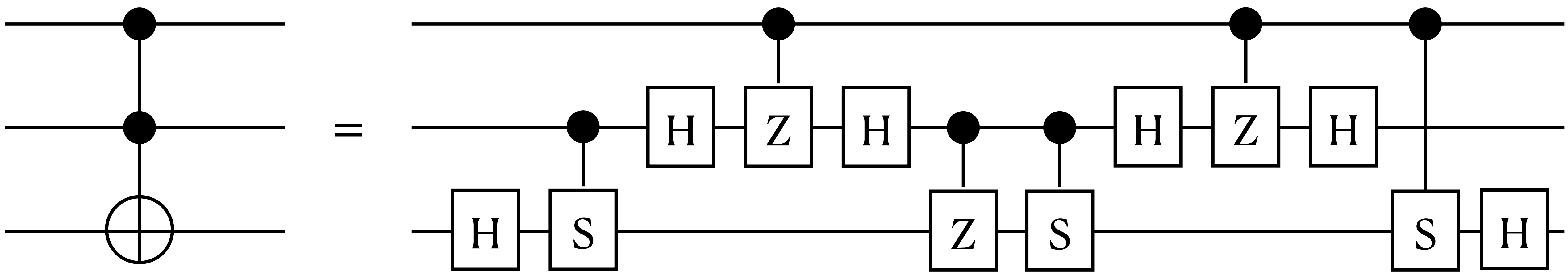
Case 2: $x_1 = 1$

$x_2 = 1$



More about Toffoli gate

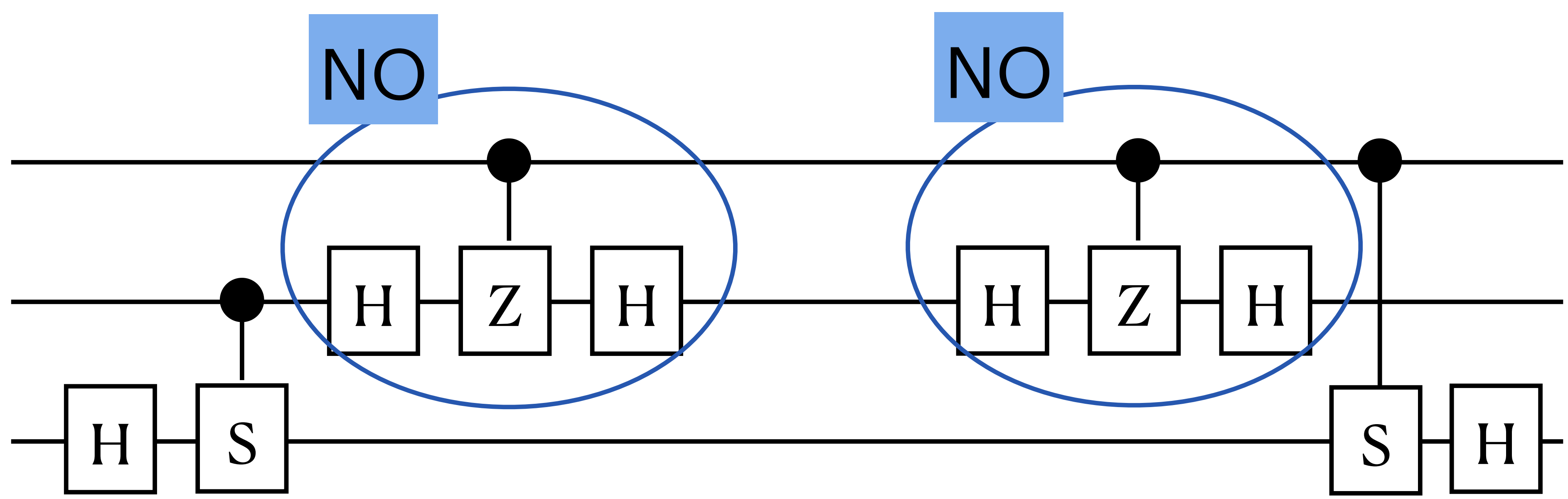
Toffoli gate



$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \mathrm{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad \mathrm{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

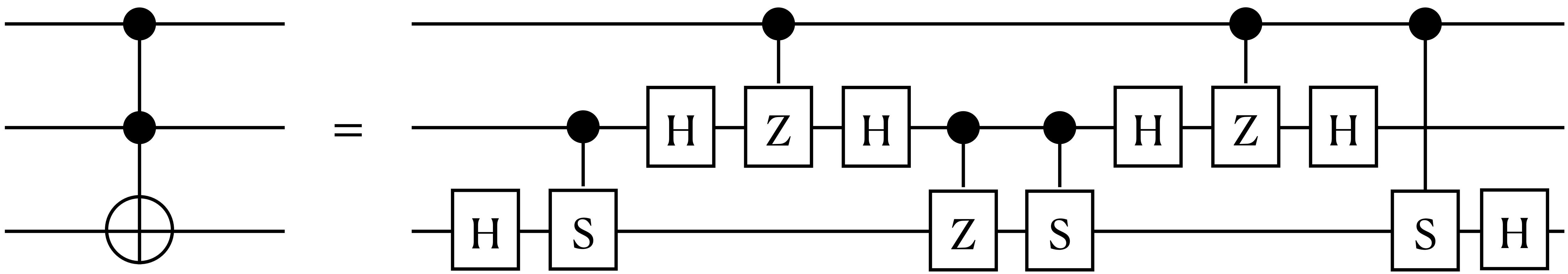
Case 2: $x_1 = 1$

$x_2 = 1$



More about Toffoli gate

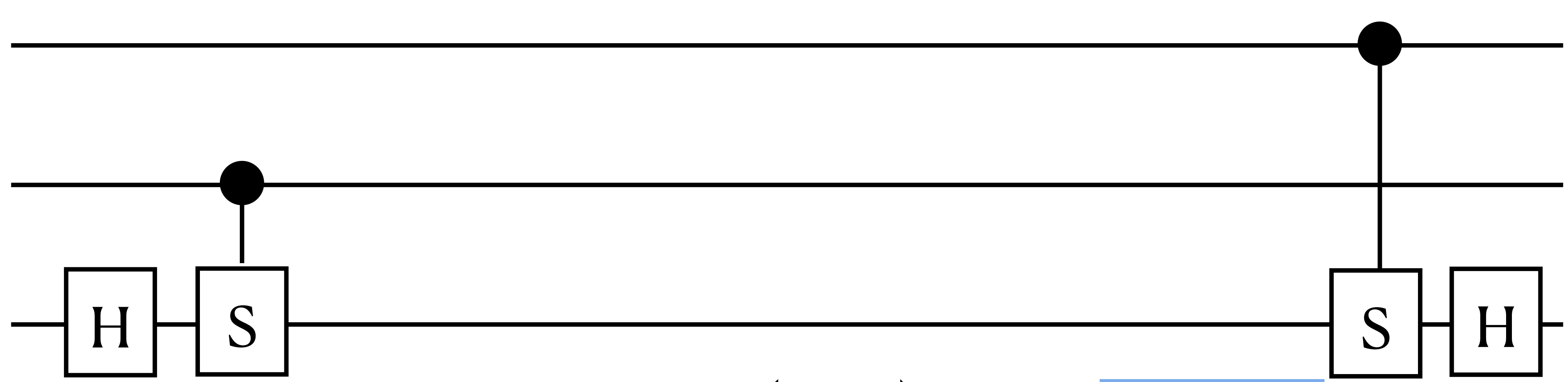
Toffoli gate



$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Case 2: $x_1 = 1$

$x_2 = 1$



$$\mathrm{HSSH} = \mathrm{HZH} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \mathrm{X}$$ Flip x_3

Quantum computation

Quantum algorithm applies a series of **unitary** matrices to a start vector.

- Keep the number k of arguments for any operation to a constant!

- Any unitary matrix B of dimension 2^k with $k = 1,\ 2,\ 3$ is **feasible**.
- Gates involving with more qubits is OK if they can be built up out of small gates

Quantum computation

Definition

A quantum computation C on s qubits is **feasible** provided ,

$$C = U_t U_{t-1} \dots U_1$$

Where each U_i is feasible operation, and s and t are bounded by a polynomial in the designated number n of input qubits.

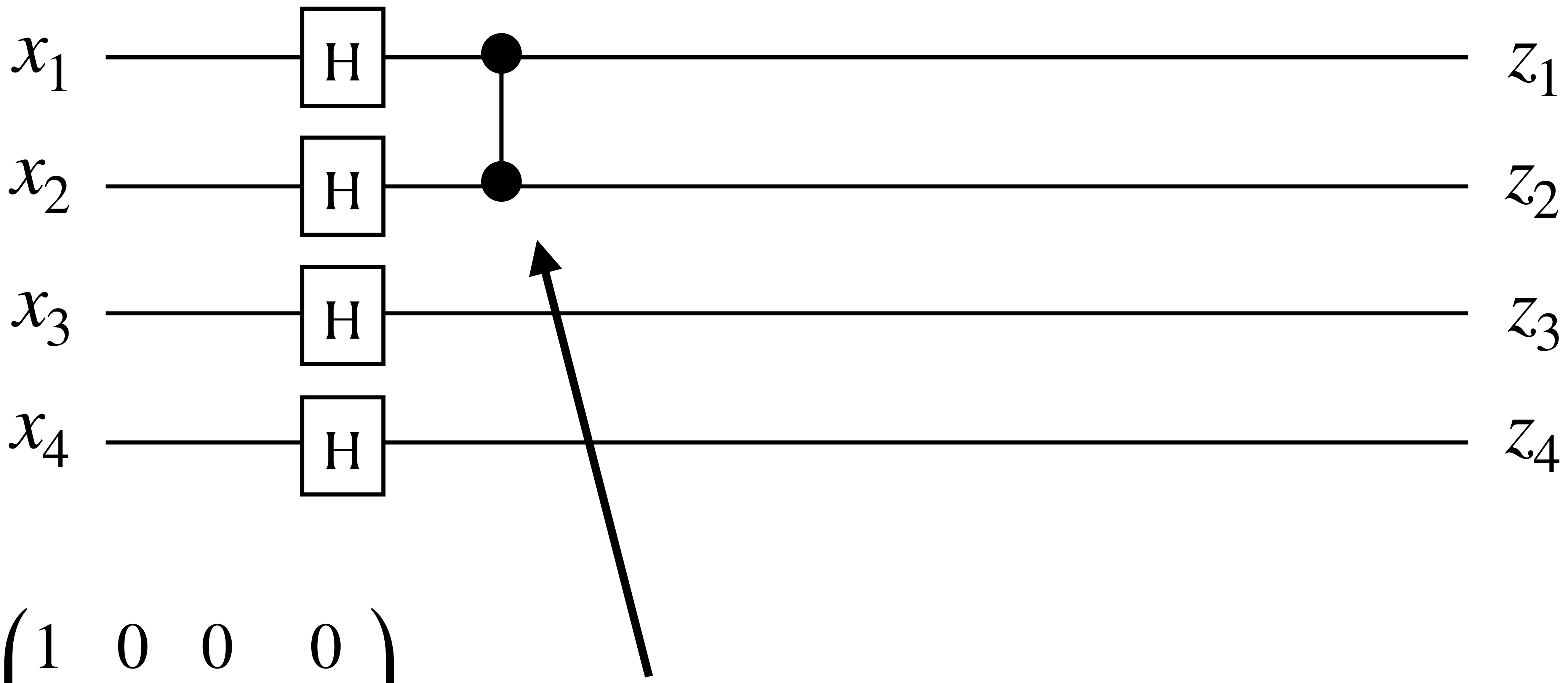
Example: H gates

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

$$H^{\otimes 4} = \frac{1}{4} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

A 16×16 matrix

Example: H gates and CZ gates

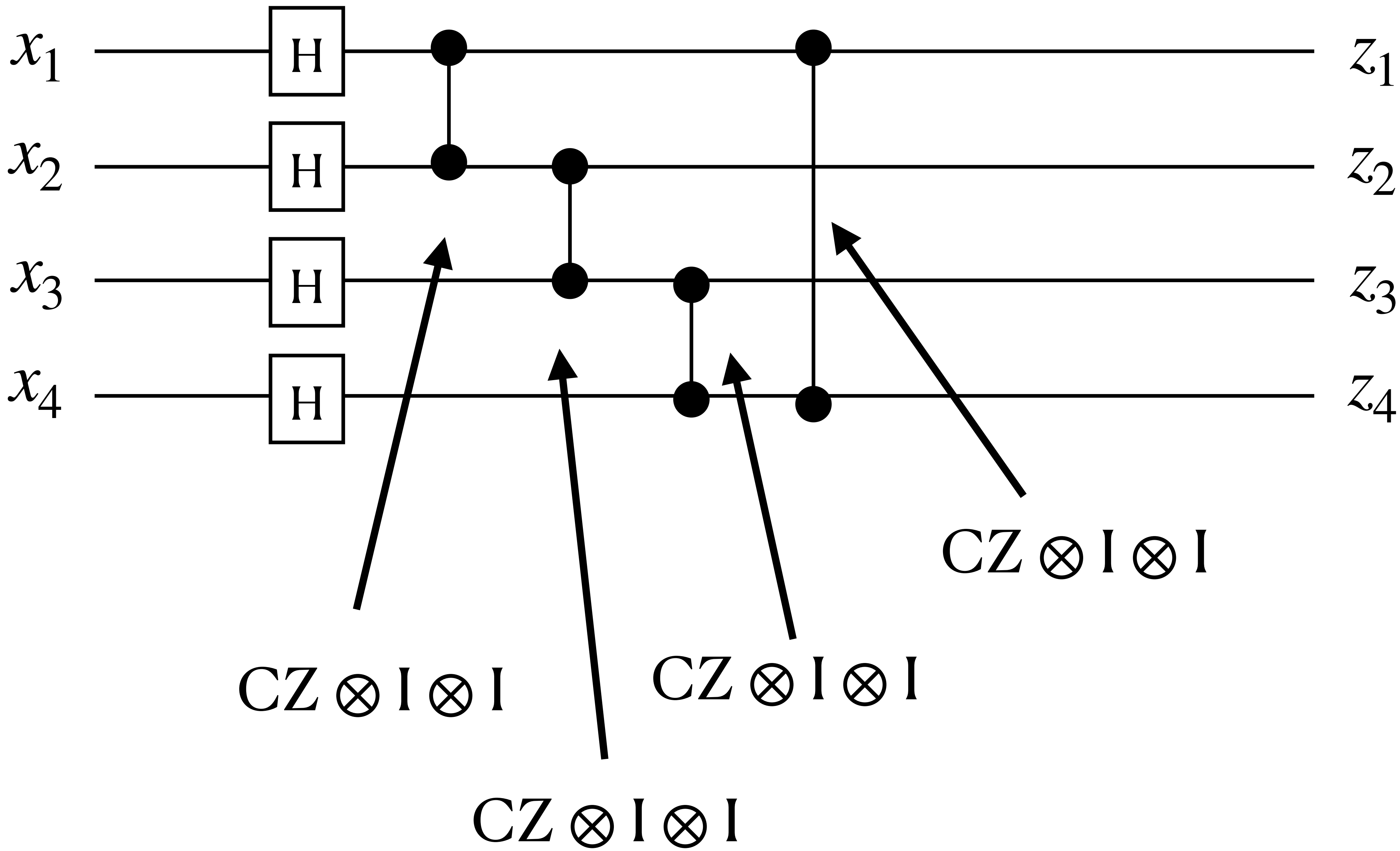


$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$CZ \otimes I \otimes I$

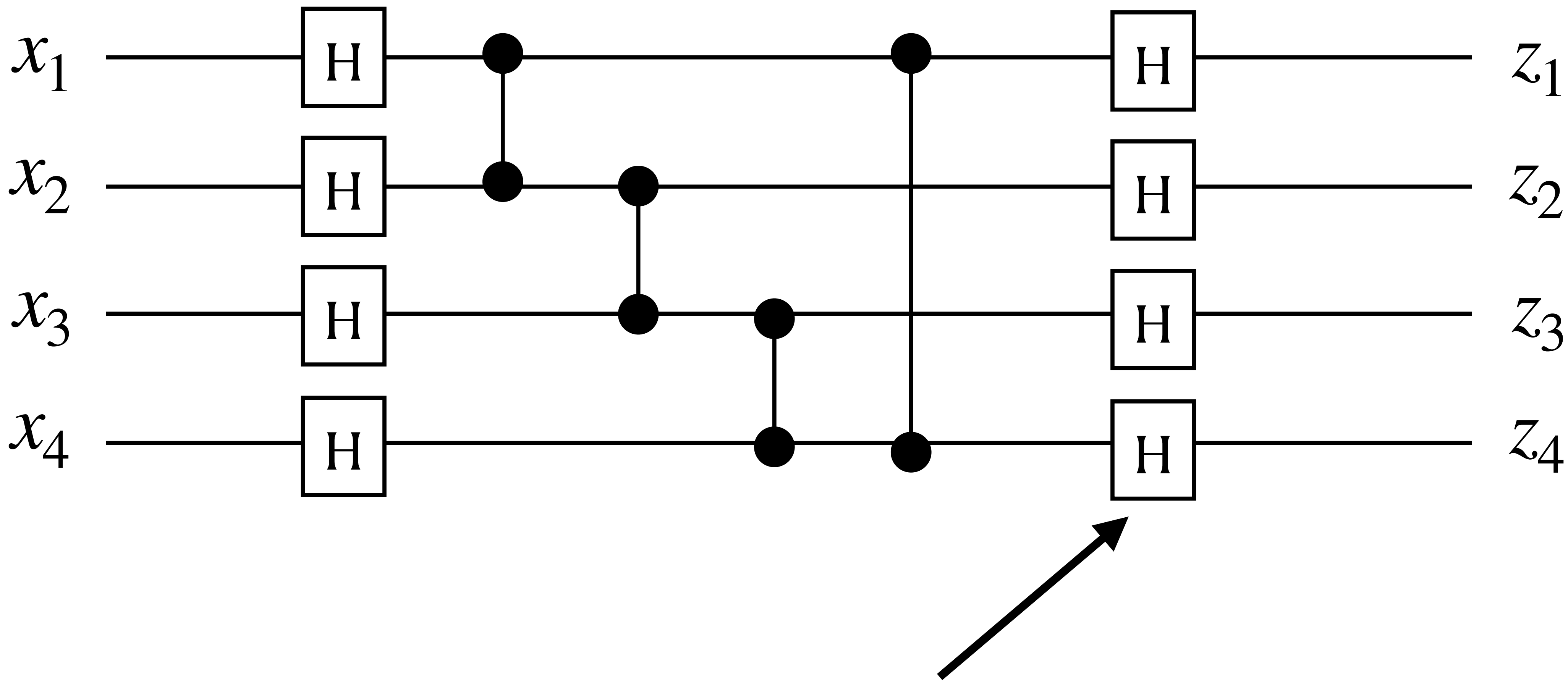
A 16×16 matrix multiple a 16×16 matrix

Example: H gates and CZ gates



A 16×16 matrix multiple four 16×16 matrix

Example: H gates and CZ gates



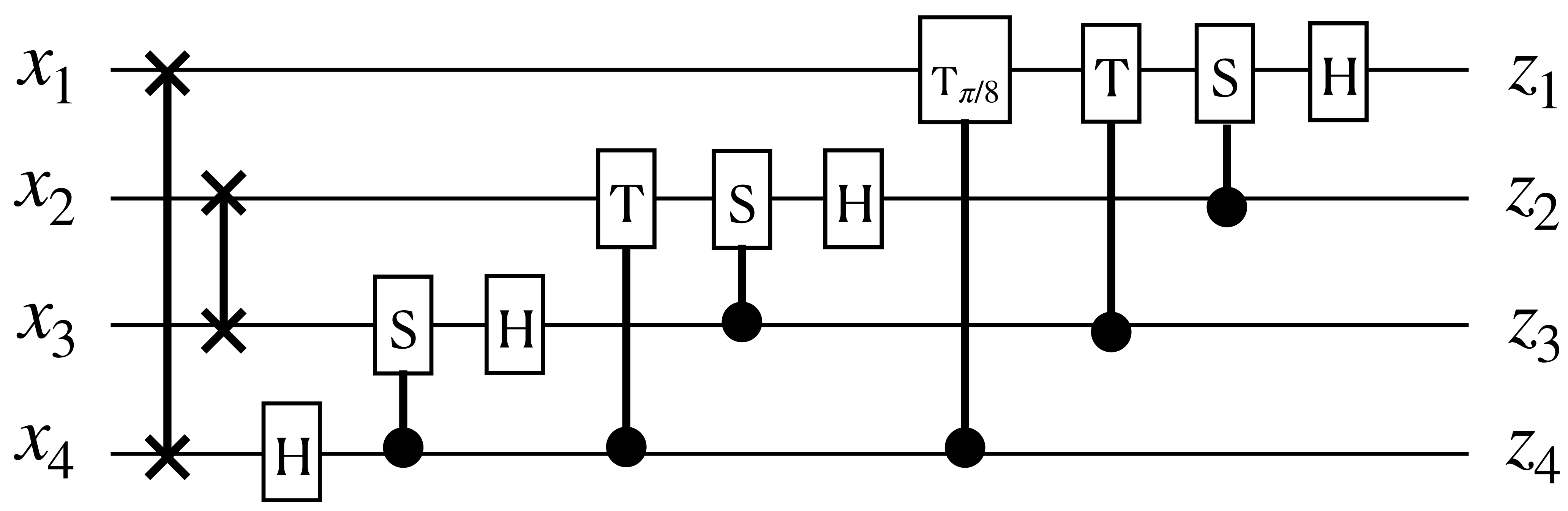
$$H^{\otimes 4} = \frac{1}{4}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

A 16×16 matrix multiple four 16×16 matrix multiple a 16×16 matrix

Example: quantum Fourier transform (QFT)

The n-qubit quantum Fourier transform (QFT) can be built up of $O(n^2)$ smaller gates.

Example: $n = 4$, $N = 2^4$



$$\mathrm{T}_{\pi/8} = \begin{pmatrix} 1 & 0 \\ 0 & w' \end{pmatrix} \text{ with } w' = e^{i\pi/8}$$

Thank you!