Classical Computing

bits

gates

Examples:

NOT

in	out
0	1
1	0

AND

in	out
00	0
01	0
10	0
11	1

NAND

in	out
00	1
01	1
10	1
11	0

Can compute any function $f: \{0,1\}^n \to \{0,1\}^k$

Quantum Computing

qubits

quantum gates

↳ unitary matrices

Def^n. A matrix U is unitary if $UU^\dagger = I = U^\dagger U$

where $U^\dagger$ = conjugate transpose.

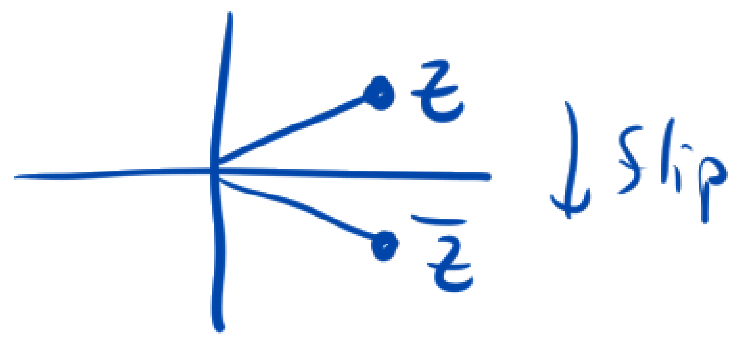
e.g. 2×2. $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $U^T = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ $U^\dagger = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$

In geometric terms, U is unitary if $|U\vec{v}| = |\vec{v}|$ $\forall \vec{v} \in \mathbb{C}^n$

Conjugation in $\mathbb{C}$:

$z = a + bi$

$\bar{z} = a - bi$



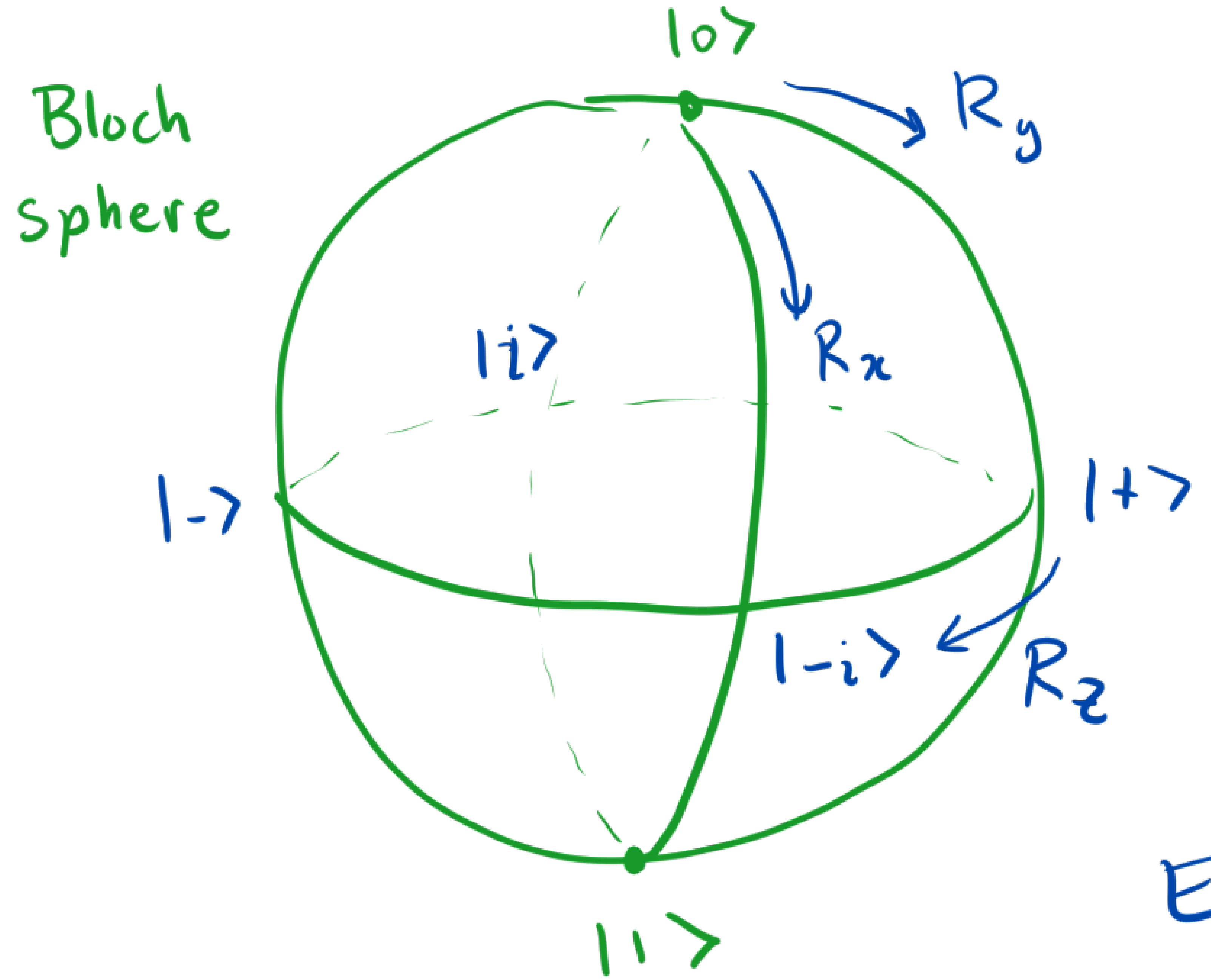
$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Examples: (in basis $|0\rangle$ $|1\rangle$)

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

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

name	matrix	conj. transpose	behaviour	
Pauli X or NOT	$\begin{array}{c} \begin{array}{cc} M\|0\rangle & M\|1\rangle \end{array} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{array}{c} \|0\rangle \\ \|1\rangle \end{array} \end{array}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\|0\rangle \mapsto \|1\rangle$ $\|1\rangle \mapsto \|0\rangle$ $a\|0\rangle + b\|1\rangle \mapsto b\|0\rangle + a\|1\rangle$	$X^2 = I = XX^\dagger = X^\dagger X$
Pauli Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\|0\rangle \mapsto \|0\rangle$ $\|1\rangle \mapsto -\|1\rangle$ $a\|0\rangle + b\|1\rangle \mapsto a\|0\rangle - b\|1\rangle$	$\|+\rangle \mapsto \|-\rangle$ $\|-\rangle \mapsto \|+\rangle$ $Z^2 = I$
Hadamard H	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$\|0\rangle \mapsto \|+\rangle$ $\|1\rangle \mapsto \|-\rangle$ $a\|0\rangle + b\|1\rangle \mapsto \frac{a+b}{\sqrt{2}}\|0\rangle + \frac{a-b}{\sqrt{2}}\|1\rangle$	$H^2 = I$
Pauli Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$\|0\rangle \mapsto i\|1\rangle$ $\|1\rangle \mapsto -i\|0\rangle$	$Y^2 = I$



$$R_{x,\theta} = \begin{bmatrix} \cos\theta/2 & -i\sin\theta/2 \\ -i\sin\theta/2 & \cos\theta/2 \end{bmatrix}$$

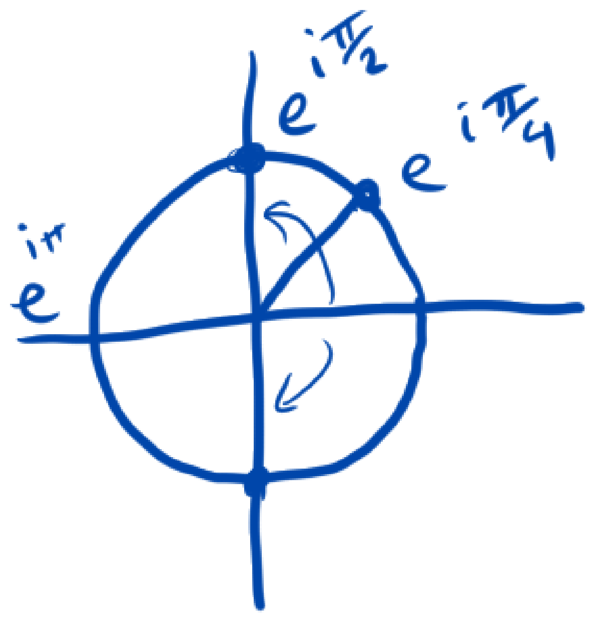
$|0\rangle, |1\rangle$ basis

$$R_{y,\theta} = \begin{bmatrix} \cos\theta/2 & -\sin\theta/2 \\ \sin\theta/2 & \cos\theta/2 \end{bmatrix}$$

$$R_{z,\theta} = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

Example: $R_{z,\theta}|+\rangle =$

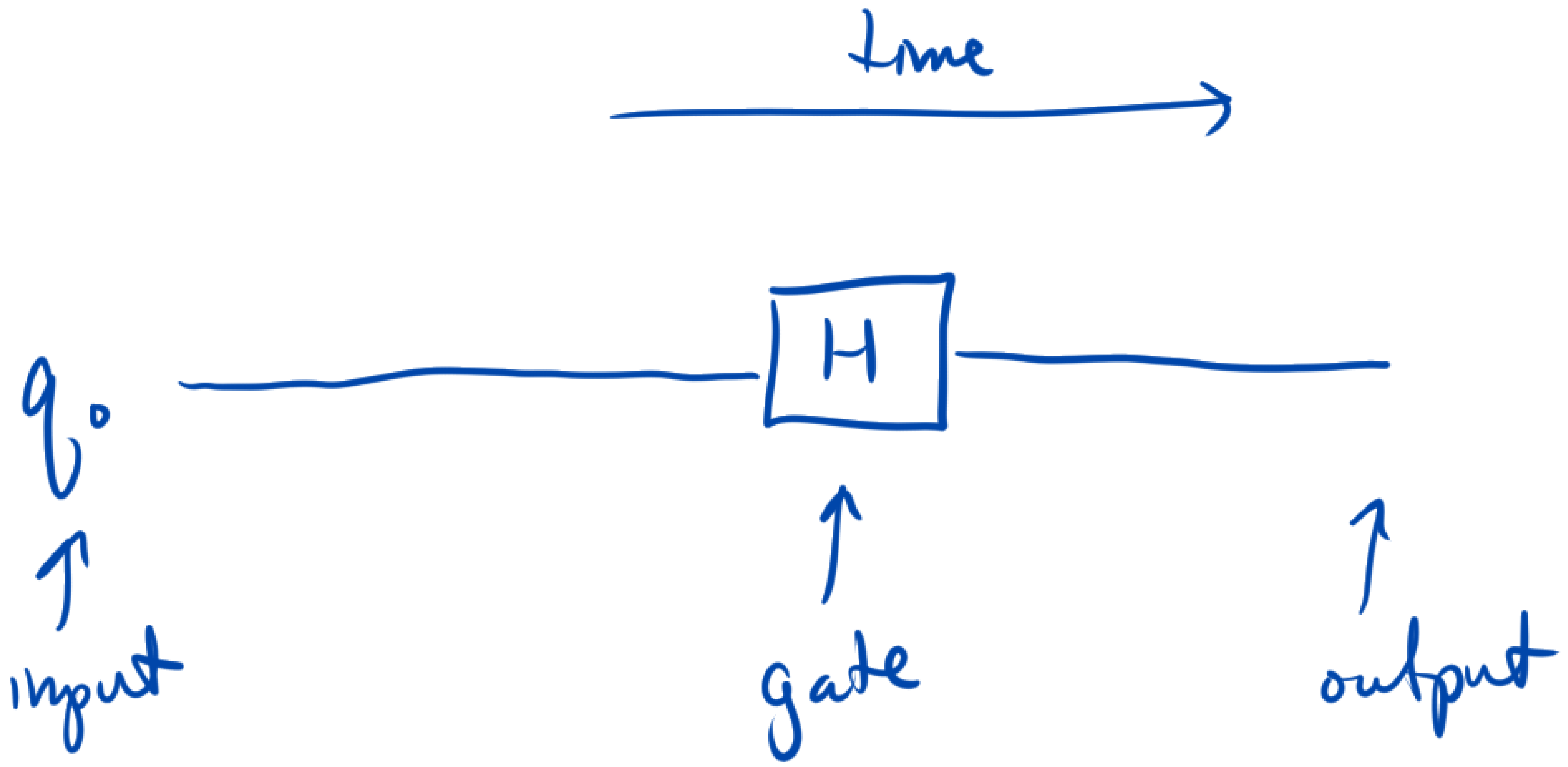
$$\begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} \frac{e^{-i\theta/2}}{\sqrt{2}} \\ \frac{e^{i\theta/2}}{\sqrt{2}} \end{pmatrix}$$



If $\theta = \pi$ then this is

$$\frac{1}{\sqrt{2}}\begin{pmatrix} e^{-i\pi/2} \\ e^{i\pi/2} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} -i \\ i \end{pmatrix} = \frac{-i}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = -i|-\rangle.$$

Circuit Notation:



Two-Qubit Gates

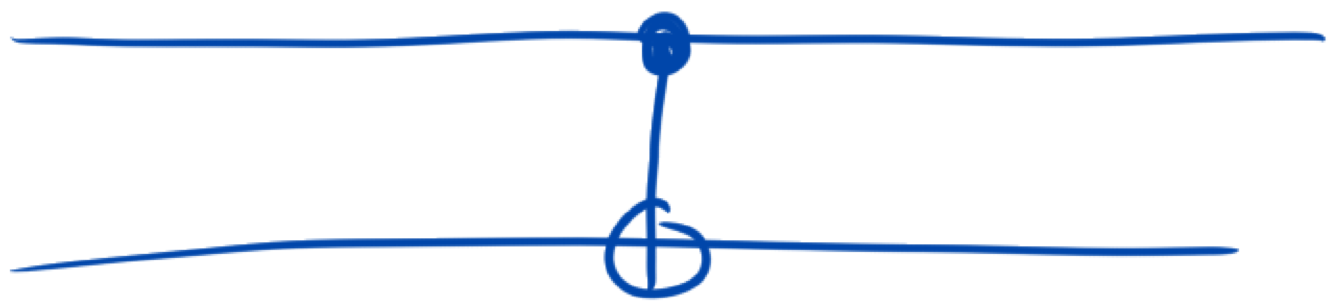
(basis: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$)

CNOT Gate:

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

$|00\rangle \longmapsto |00\rangle$
$|01\rangle \longmapsto |01\rangle$
$|10\rangle \longmapsto |11\rangle$
$|11\rangle \longmapsto |10\rangle$

Switch target bit (2^{nd}) if control bit (1^{st}) is set



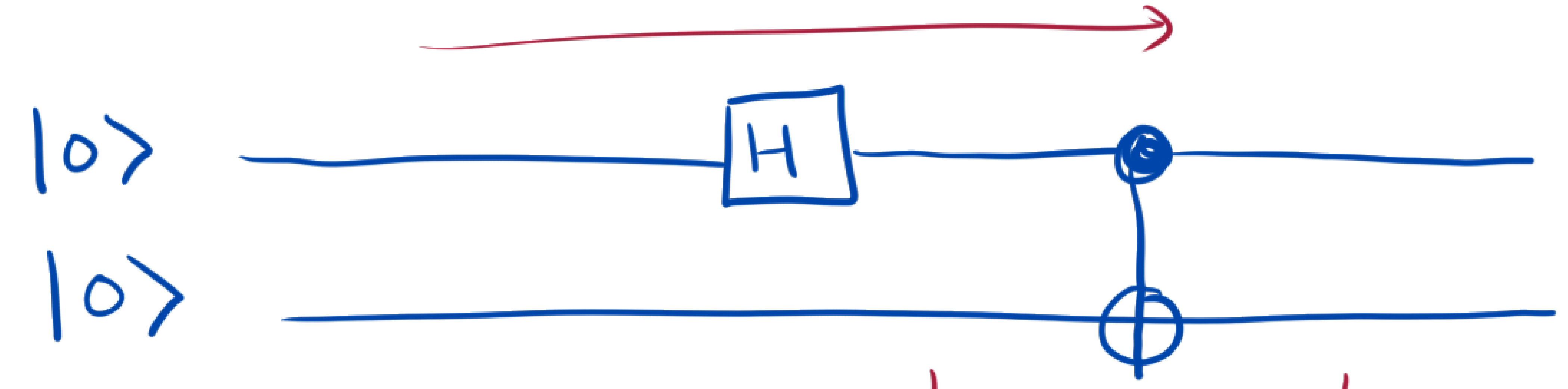
Example: Circuit to generate a Bell state

input:

$|0\rangle \otimes |0\rangle$

$= |0\rangle|0\rangle$

$= |00\rangle$



After H

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

$$= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

After CNOT

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 1/\sqrt{2} \\ 0 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{pmatrix}$$

ie.

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Gate Sets

$\mathcal{U}(2^n)$ = unitary $2^n \times 2^n$ matrices ← infinite ← continuous

In classical case: NAND is universal: combinations can create anything

in quantum case: best hope is to approximate needed gates w/ a small set of gates.

Clifford + T:

$$H, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad CNOT, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

What can we compute?

"reversible (classical) circuit" = computes a bijection $\{0,1\}^n \to \{0,1\}^n$

Example: CNOT

in	out
0 0	0 0
0 1	0 1
1 0	1 1
1 1	1 0

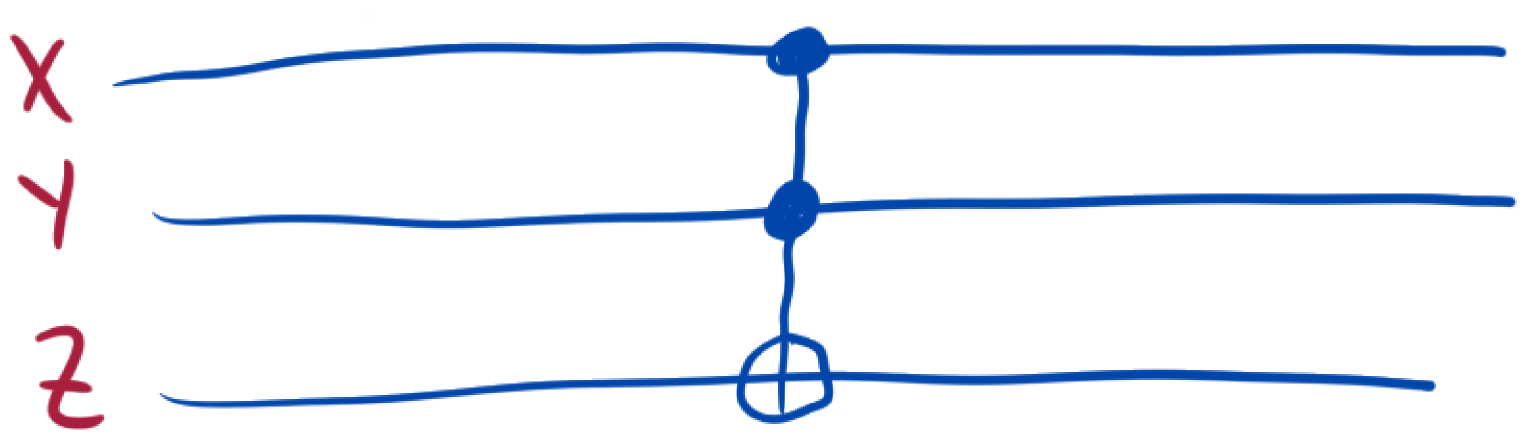
Can you create a reversible AND?

in	out	
0 0 0	0 0 0	AND
0 1 0	0 1 0	
1 0 0	1 0 0	
1 1 0	1 1 1	
0 0 1	0 0 1	NAND
0 1 1	0 1 1	
1 0 1	1 0 1	
1 1 1	1 1 0	

bijection $\{0,1\}^3 \longrightarrow \{0,1\}^3$

Toffli Gate

$X, Y, Z \longmapsto X, Y, Z \text{ xor } (X \wedge Y)$



in	out	
0 0 0	0 0 0	AND
0 1 0	0 1 0	
1 0 0	1 0 0	
1 1 0	1 1 1	
0 0 1	0 0 1	NAND
0 1 1	0 1 1	
1 0 1	1 0 1	
1 1 1	1 1 0	

This is universal for reversible classical circuits

bijection $\{0,1\}^3 \longrightarrow \{0,1\}^3$

Classical Reversible Circuits:

Can construct any bijection $f: \{0,1\}^n \to \{0,1\}^n$ as a reversible circuit s.t.

$$\underbrace{x}_{n \text{ bit}} \; \underbrace{0}_{n+k \text{ bits}} \longmapsto \underbrace{x}_{n \text{ bit}} \; \underbrace{f(x)}_{n \text{ bits}} \; \underbrace{0}_{k \text{ bits}}$$

Classical Reversible Circuits on a Quantum Computer:

$$|x\rangle|0\rangle|0\rangle \longmapsto |x\rangle|f(x)\rangle|0\rangle$$