IQI 04, Seminar 3

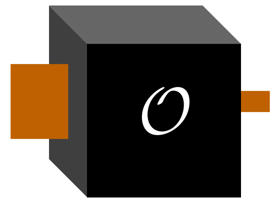
Produced with pdflatex and xfig

- Oracles
- The Classical Parity Problem.
- Quantum Oracles.
- The Quantum Parity Problem.
- Gate Set Limitations.
- Universality.

E. "Manny" Knill: knill@boulder.nist.gov

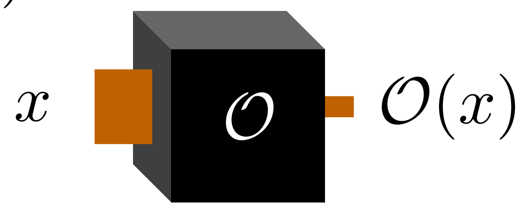
Classical Oracles

- A classical oracle $\mathcal{O}$ is a device that takes an input x and outputs an answer $\mathcal{O}(x)$.

x  $\mathcal{O}(x)$

Classical Oracles

- A classical oracle $\mathcal{O}$ is a device that takes an input x and outputs an answer $\mathcal{O}(x)$.

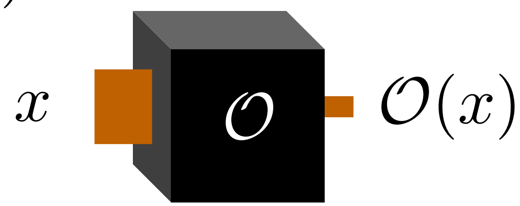


Examples:

- $\mathcal{O}_1(x) = 1$ if x is a true statement about numbers, $\mathcal{O}_1(x) = 0$ otherwise.

Classical Oracles

- A classical oracle $\mathcal{O}$ is a device that takes an input x and outputs an answer $\mathcal{O}(x)$.

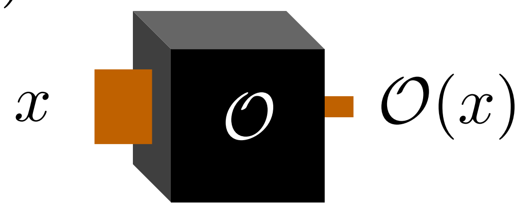


Examples:

- $\mathcal{O}_1(x) = 1$ if x is a true statement about numbers, $\mathcal{O}_1(x) = 0$ otherwise.
- $\mathcal{O}_2(x) = 1$ if x is a satisfiable boolean formula, $\mathcal{O}_2(x) = 0$ otherwise.

Classical Oracles

- A classical oracle $\mathcal{O}$ is a device that takes an input x and outputs an answer $\mathcal{O}(x)$.



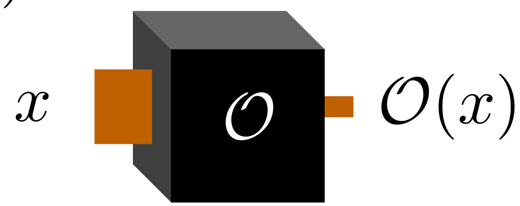
Examples:

- $\mathcal{O}_1(x) = 1$ if x is a true statement about numbers, $\mathcal{O}_1(x) = 0$ otherwise.
- $\mathcal{O}_2(x) = 1$ if x is a satisfiable boolean formula, $\mathcal{O}_2(x) = 0$ otherwise.

…Oracles can be used to add computational power.

Classical Oracles

- A classical oracle $\mathcal{O}$ is a device that takes an input x and outputs an answer $\mathcal{O}(x)$.



Examples:

- $\mathcal{O}_1(x) = 1$ if x is a true statement about numbers, $\mathcal{O}_1(x) = 0$ otherwise.
- $\mathcal{O}_2(x) = 1$ if x is a satisfiable boolean formula, $\mathcal{O}_2(x) = 0$ otherwise.

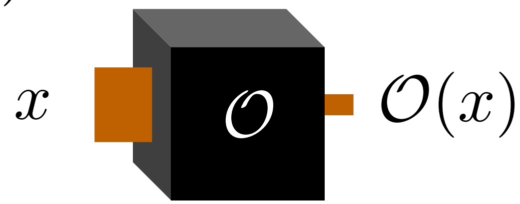
  ...Oracles can be used to add computational power.

- $\mathcal{O}_3(x)$ computes an unknown parity of x.

  Determine the parity.

Classical Oracles

- A classical oracle $\mathcal{O}$ is a device that takes an input x and outputs an answer $\mathcal{O}(x)$.



Examples:

- $\mathcal{O}_1(x) = 1$ if x is a true statement about numbers,
  $\mathcal{O}_1(x) = 0$ otherwise.
- $\mathcal{O}_2(x) = 1$ if x is a satisfiable boolean formula,
  $\mathcal{O}_2(x) = 0$ otherwise.

  ...Oracles can be used to add computational power.

- $\mathcal{O}_3(x)$ computes an unknown parity of x.
  Determine the parity.

...Oracles can act as black boxes to be analyzed.

Parity Oracles

- Bit strings may be identified with 0-1 vectors.
  Example: $\mathtt{0110} \leftrightarrow (0,1,1,0)^T$

Parity Oracles

- Bit strings may be identified with 0-1 vectors.
  Example: $\mathbf{0110} \leftrightarrow (0,1,1,0)^T$
- The parity of bitstring $\mathbf{s}$ is the number of $\mathbf{1}$'s in $\mathbf{s}$ modulo 2.
  Example: $P(\mathbf{0110}) = (1,1,1,1)(0,1,1,0)^T$

Parity Oracles

- Bit strings may be identified with 0-1 vectors.
  Example: $\mathsf{0110} \leftrightarrow (0,1,1,0)^T$
- The parity of bitstring s is the number of $\mathsf{1}$'s in s modulo 2.
  Example: $P(\mathsf{0110}) = (1,1,1,1)(0,1,1,0)^T = 2 \bmod 2 = 0$

Parity Oracles

- Bit strings may be identified with 0-1 vectors.
  Example: $\mathtt{0110} \leftrightarrow (0,1,1,0)^T$
- The parity of bitstring $\mathtt{s}$ is the number of $\mathtt{1}$'s in $\mathtt{s}$ modulo 2.
  Example: $P(\mathtt{1101}) = (1,1,1,1)(1,1,0,1)^T$

Parity Oracles

- Bit strings may be identified with 0-1 vectors.
  Example: $$\mathtt{0110} \leftrightarrow (0,1,1,0)^T$$
- The parity of bitstring $\mathtt{s}$ is the number of $\mathtt{1}$'s in $\mathtt{s}$ modulo 2.
  Example: $$P(\mathtt{1101}) = (1,1,1,1)(1,1,0,1)^T = 3 \bmod 2 = 1$$

Parity Oracles

- Bit strings may be identified with 0-1 vectors.
  Example: $0110 \leftrightarrow (0,1,1,0)^T$

- The parity of bitstring s is the number of 1's in s modulo 2.
  Example: $P(1101) = (1,1,1,1)(1,1,0,1)^T = 3 \bmod 2 = 1$

  . . . computations with 0-1 entities are modulo 2.

Parity Oracles

- Bit strings may be identified with 0-1 vectors.
  Example: $\quad 0110 \leftrightarrow (0,1,1,0)^T$

- The parity of bitstring s is the number of 1's in s modulo 2.
  Example: $\quad P(1101) = (1,1,1,1)(1,1,0,1)^T = 3 \bmod 2 = 1$

  ...computations with 0-1 entities are modulo 2.

- Parity of a substring.
  Examples:
  $$P_{(0,1,0,1)}(0110) = (0,1,0,1)(0,1,1,0)^T$$

Parity Oracles

- Bit strings may be identified with 0-1 vectors.
  Example: $$\mathtt{0110} \leftrightarrow (0,1,1,0)^T$$
- The parity of bitstring $\mathtt{s}$ is the number of $\mathtt{1}$'s in $\mathtt{s}$ modulo 2.
  Example: $$P(\mathtt{1101}) = (1,1,1,1)(1,1,0,1)^T = 3 \bmod 2 = 1$$
  ... computations with 0-1 entities are modulo 2.
- Parity of a substring.
  Examples:
  $$P_{(0,1,0,1)}(\mathtt{0110}) = (0,1,0,1)(0,1,1,0)^T = 1 \bmod 2 = 1$$

Parity Oracles

- Bit strings may be identified with 0-1 vectors.
  Example: $$0110 \leftrightarrow (0,1,1,0)^T$$
- The parity of bitstring s is the number of 1's in s modulo 2.
  Example: $$P(1101) = (1,1,1,1)(1,1,0,1)^T = 3 \bmod 2 = 1$$
  ...computations with 0-1 entities are modulo 2.
- Parity of a substring.
  Examples:
  $$P_{(1,1,1,0)}(0110) = (1,1,1,0)(0,1,1,0)^T$$

Parity Oracles

- Bit strings may be identified with 0-1 vectors.

  Example: $$0110 \leftrightarrow (0,1,1,0)^T$$

- The parity of bitstring s is the number of 1's in s modulo 2.

  Example: $P(1101) = (1,1,1,1)(1,1,0,1)^T = 3 \bmod 2 = 1$

  ...computations with 0-1 entities are modulo 2.

- Parity of a substring.

  Examples:

  $$P_{(1,1,1,0)}(0110) = (1,1,1,0)(0,1,1,0)^T = 2 \bmod 2 = 0$$

Parity Oracles

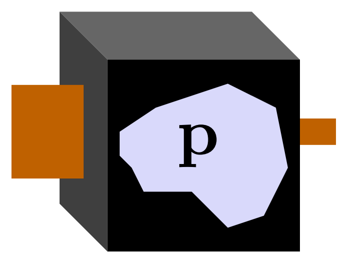
- Bit strings may be identified with 0-1 vectors.
  Example: $\mathtt{0110} \leftrightarrow (0,1,1,0)^T$
- The parity of bitstring $\mathbf{s}$ is the number of $\mathtt{1}$'s in $\mathbf{s}$ modulo 2.
  Example: $P(\mathtt{1101}) = (1,1,1,1)(1,1,0,1)^T = 3 \bmod 2 = 1$

  …computations with 0-1 entities are modulo 2.
- Parity of a substring.
  Examples:
  $$P_{\mathbf{p}}(\mathbf{s}) = \mathbf{p} \cdot \mathbf{s}$$

Parity Oracles

- Bit strings may be identified with 0-1 vectors.
  Example: $\mathtt{0110} \leftrightarrow (0, 1, 1, 0)^T$
- The parity of bitstring $\mathbf{s}$ is the number of 1's in $\mathbf{s}$ modulo 2.
  Example: $P(\mathtt{1101}) = (1, 1, 1, 1)(1, 1, 0, 1)^T = 3 \bmod 2 = 1$

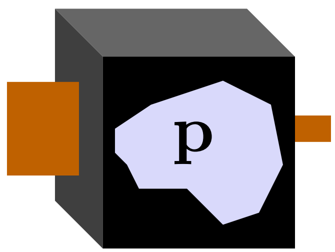
  . . . computations with 0-1 entities are modulo 2.
- Parity of a substring.
  Examples:
  $$P_{\mathbf{p}}(\mathbf{s}) = \mathbf{p} \cdot \mathbf{s}$$
- A parity oracle.

$\mathbf{s}$  $\mathbf{p} \cdot \mathbf{s}$

How many "queries" does it take to learn $\mathbf{p}$?

Parity Oracles

- Bit strings may be identified with 0-1 vectors.
  Example: $$0110 \leftrightarrow (0,1,1,0)^T$$
- The parity of bitstring $\mathbf{s}$ is the number of 1's in $\mathbf{s}$ modulo 2.
  Example: $P(1101) = (1,1,1,1)(1,1,0,1)^T = 3 \bmod 2 = 1$

  …computations with 0-1 entities are modulo 2.
- Parity of a substring.
  Examples:
  $$P_{\mathbf{p}}(\mathbf{s}) = \mathbf{p} \cdot \mathbf{s}$$
- A parity oracle. $(a,b)^T$ 

$(p_1,p_2)(a,b)^T$

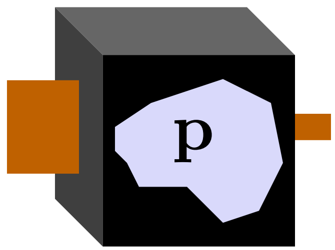
How many "queries" does it take to learn $\mathbf{p}$?

Parity Oracles

- Bit strings may be identified with 0-1 vectors.
  Example: $\qquad 0110 \leftrightarrow (0,1,1,0)^T$
- The parity of bitstring $\mathbf{s}$ is the number of 1's in $\mathbf{s}$ modulo 2.
  Example: $\quad P(1101) = (1,1,1,1)(1,1,0,1)^T = 3 \bmod 2 = 1$

  ...computations with 0-1 entities are modulo 2.
- Parity of a substring.
  Examples:
  $$P_{\mathbf{p}}(\mathbf{s}) = \mathbf{p} \cdot \mathbf{s}$$
- A parity oracle.

$(a,b)^T$
$(1,0)^T$



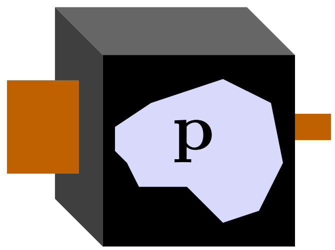
$(p_1,p_2)(a,b)^T$
$(p_1,p_2)(1,0)^T = p_1$

How many "queries" does it take to learn $\mathbf{p}$?

Parity Oracles

- Bit strings may be identified with 0-1 vectors.
  Example: $$0110 \leftrightarrow (0,1,1,0)^T$$
- The parity of bitstring $\mathbf{s}$ is the number of 1's in $\mathbf{s}$ modulo 2.
  Example: $$P(1101) = (1,1,1,1)(1,1,0,1)^T = 3 \bmod 2 = 1$$
  $\ldots$ computations with 0-1 entities are modulo 2.
- Parity of a substring.
  Examples:
  $$P_{\mathbf{p}}(\mathbf{s}) = \mathbf{p} \cdot \mathbf{s}$$
- A parity oracle.

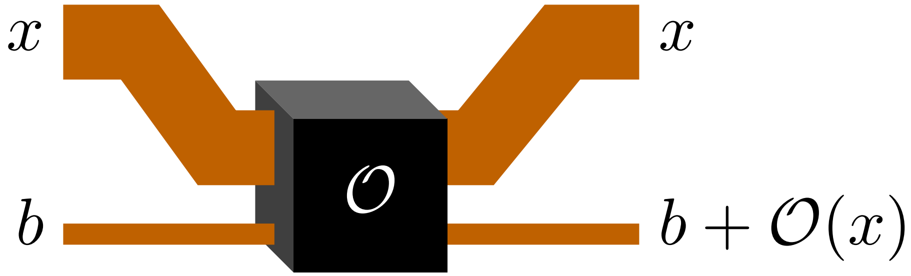
$$(a,b)^T \qquad (p_1,p_2)(a,b)^T$$
$$(1,0)^T \qquad (p_1,p_2)(1,0)^T = p_1$$
$$(0,1)^T \qquad (p_1,p_2)(0,1)^T = p_2$$



How many "queries" does it take to learn $\mathbf{p}$?

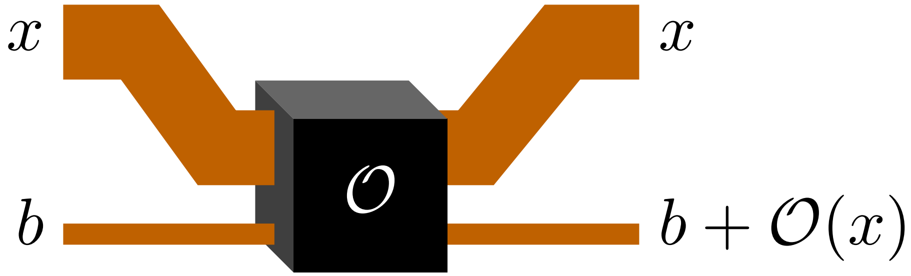
Reversible Oracles

- Reversible oracles add the answer to a register.

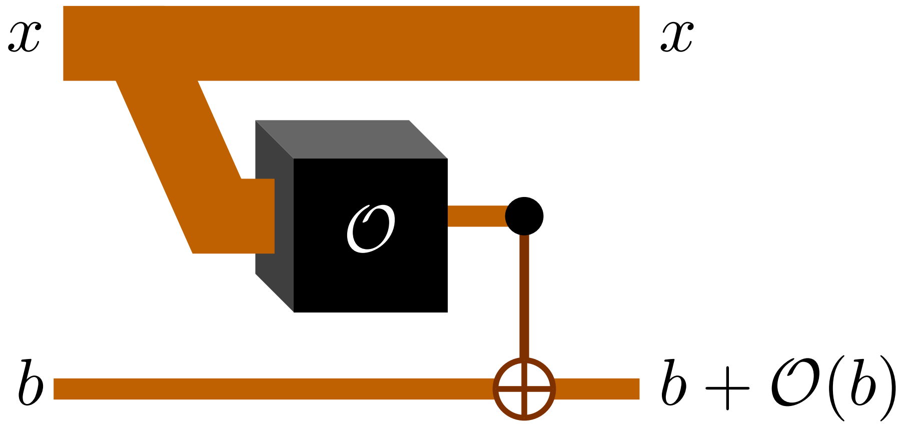


Reversible Oracles

- Reversible oracles add the answer to a register.

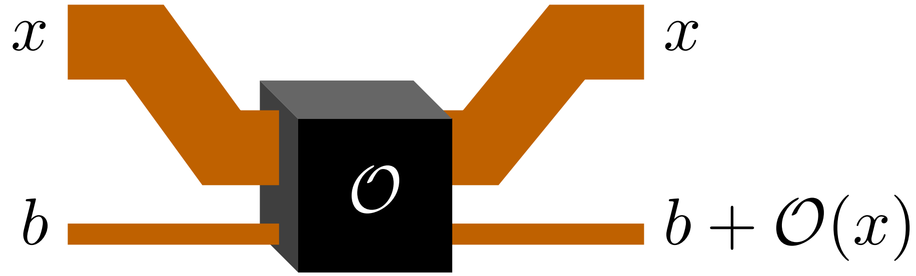


- Simulation, using a standard oracle.

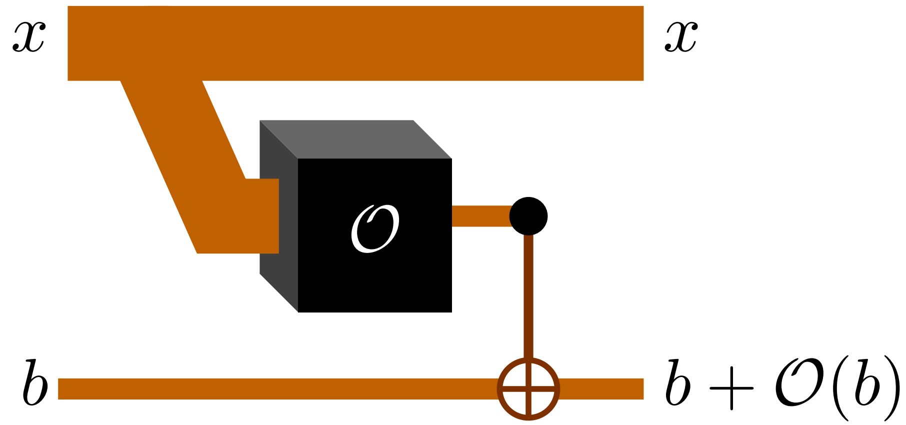


Reversible Oracles

- Reversible oracles add the answer to a register.



- Simulation, using a standard oracle.

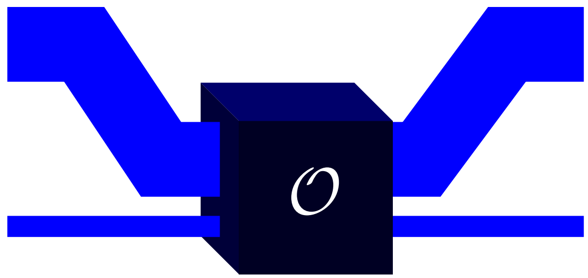


- Is the simulation equivalent to a reversible oracle?

Quantum Oracles

- A Quantum Oracle is the linear extension of a classical reversible oracle.

$$\sum_{x,b} \alpha_{x,b} |x\rangle_{\mathsf{I}} |b\rangle_{\mathsf{O}} \left\{ \vphantom{\int} \right.$$

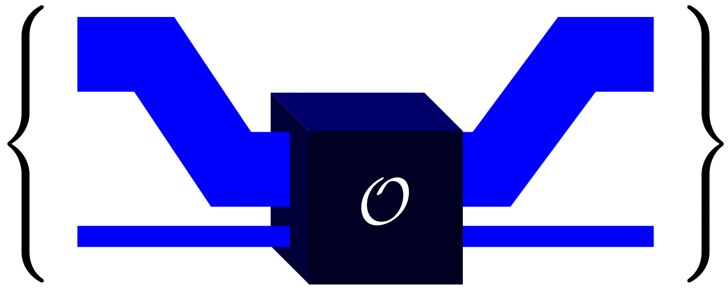


$$\left. \vphantom{\int} \right\} \sum_{x,b} \alpha_{x,b} |x\rangle_{\mathsf{I}} |b + \mathcal{O}(x)\rangle_{\mathsf{O}}$$

Quantum Oracles

- A Quantum Oracle is the linear extension of a classical reversible oracle.

$$\sum_{x,b}\alpha_{x,b}|x\rangle_{\mathsf{I}}|b\rangle_{\mathsf{O}}$$



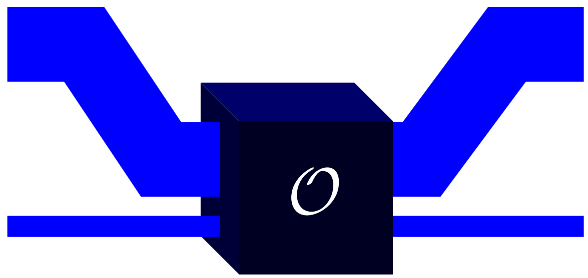
$$\sum_{x,b}\alpha_{x,b}|x\rangle_{\mathsf{I}}|b+\mathcal{O}(x)\rangle_{\mathsf{O}}$$

- Quantum oracles versus classical reversible oracles?

Quantum Oracles

- A Quantum Oracle is the linear extension of a classical reversible oracle.

$$\sum_{x,b} \alpha_{x,b} |x\rangle_{\mathsf{I}} |b\rangle_{\mathsf{O}} \left\{ \right.$$



$$\left. \right\} \sum_{x,b} \alpha_{x,b} |x\rangle_{\mathsf{I}} |b + \mathcal{O}(x)\rangle_{\mathsf{O}}$$

- Quantum oracles versus classical reversible oracles?
  - Does it help to use a quantum computer to analyze a classical reversible oracle?

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.
- Solution in two tricks.

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.

  Def.: $\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}(|\mathfrak{0}\rangle + |\mathfrak{1}\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|\mathfrak{0}\rangle - |\mathfrak{1}\rangle) \end{cases}$

  1. Parity and the Hadamard basis.
     - Which logical states $|\mathfrak{ab}\rangle_{\text{AB}}$ have a minus sign in

       $|+\rangle_{\text{A}}|+\rangle_{\text{B}}$

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.

  Def.: $\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}(|\mathfrak{o}\rangle + |\mathfrak{1}\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|\mathfrak{o}\rangle - |\mathfrak{1}\rangle) \end{cases}$

  1. Parity and the Hadamard basis.
     - Which logical states $|\mathfrak{ab}\rangle_{\mathsf{AB}}$ have a minus sign in

       $|+\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}}, \quad |+\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}}$

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.
  1. Parity and the Hadamard basis.
     - Which logical states $|\mathfrak{ab}\rangle_{AB}$ have a minus sign in

$$|+\rangle_A|+\rangle_B, \quad |+\rangle_A|-\rangle_B, \quad |-\rangle_A|+\rangle_B$$

Def.: $\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}(|\mathfrak{0}\rangle + |\mathfrak{1}\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|\mathfrak{0}\rangle - |\mathfrak{1}\rangle) \end{cases}$

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.
- Solution in two tricks.

Def.: $\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$

  1. Parity and the Hadamard basis.
     - Which logical states $|\mathfrak{ab}\rangle_{\mathsf{AB}}$ have a minus sign in

$$|+\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\quad |+\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}},\quad |-\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\quad |-\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}}?$$

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.

  Def.: $\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$

  1. Parity and the Hadamard basis.
     - Which logical states $|\mathfrak{ab}\rangle_{\mathsf{AB}}$ have a minus sign in
       $$|+\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\quad |+\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}},\quad |-\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\quad |-\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}}?$$
     - Ans.: States with odd parity w.r.t. the $|-\rangle$-qubits.

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.

  Def.: $\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$

  1. Parity and the Hadamard basis.
     - Which logical states $|\mathfrak{ab}\rangle_{\mathsf{AB}}$ have a minus sign in
       $$|+\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\quad |+\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}},\quad |-\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\quad |-\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}}?$$
     - Ans.: States with odd parity w.r.t. the $|-\rangle$-qubits.
     - Are these states distinguishable?

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

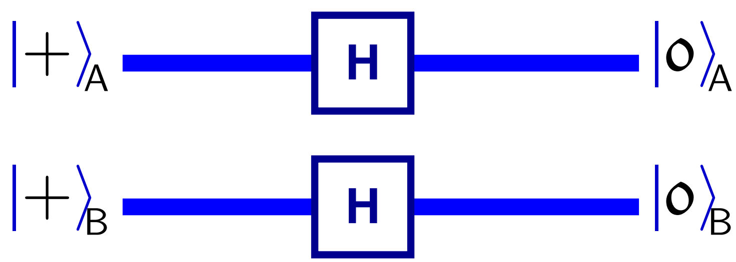
- Solution in two tricks.

  Def.: $\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}(|\mathfrak{0}\rangle + |\mathfrak{1}\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|\mathfrak{0}\rangle - |\mathfrak{1}\rangle) \end{cases}$

  1. Parity and the Hadamard basis.
     - Which logical states $|\mathfrak{a}\mathfrak{b}\rangle_{AB}$ have a minus sign in

       $$|+\rangle_A|+\rangle_B,\quad |+\rangle_A|-\rangle_B,\quad |-\rangle_A|+\rangle_B,\quad |-\rangle_A|-\rangle_B?$$

     - Ans.: States with odd parity w.r.t. the $|-\rangle$-qubits.
     - Are these states distinguishable?



Product state convention:
Multiply states associated with different qubit lines.

The Quantum Parity Problem

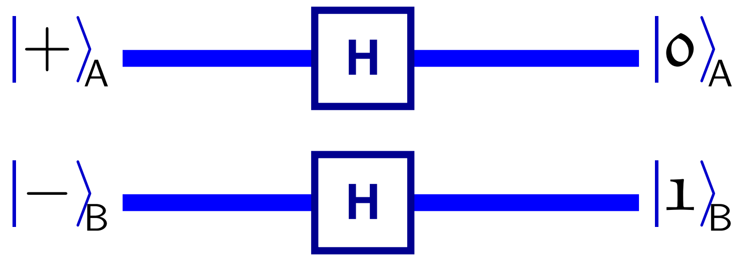
- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.
- Solution in two tricks.

  Def.: $\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}(|\mathfrak{0}\rangle + |\mathfrak{1}\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|\mathfrak{0}\rangle - |\mathfrak{1}\rangle) \end{cases}$

  1. Parity and the Hadamard basis.
     - Which logical states $|\mathfrak{a}\mathfrak{b}\rangle_{\mathsf{AB}}$ have a minus sign in

       $$|+\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\quad |+\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}},\quad |-\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\quad |-\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}}?$$

     - Ans.: States with odd parity w.r.t. the $|-\rangle$-qubits.
     - Are these states distinguishable?



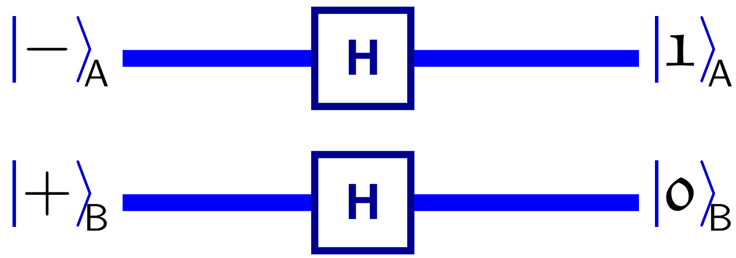
The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.

  Def.: $\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$

  1. Parity and the Hadamard basis.
     - Which logical states $|\mathfrak{ab}\rangle_{\mathsf{AB}}$ have a minus sign in
       $$|+\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\quad |+\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}},\quad |-\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\quad |-\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}}?$$
     - Ans.: States with odd parity w.r.t. the $|-\rangle$-qubits.
     - Are these states distinguishable?



The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

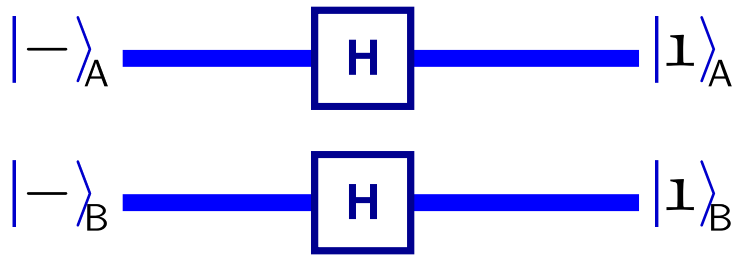
- Solution in two tricks.

  Def.: $\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$

  1. Parity and the Hadamard basis.
     - Which logical states $|\mathfrak{a}\mathfrak{b}\rangle_{\mathsf{AB}}$ have a minus sign in

       $$|+\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\quad |+\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}},\quad |-\rangle_{\mathsf{A}}|+\rangle_{\mathsf{B}},\quad |-\rangle_{\mathsf{A}}|-\rangle_{\mathsf{B}}?$$

     - Ans.: States with odd parity w.r.t. the $|-\rangle$-qubits.
     - Are these states distinguishable?



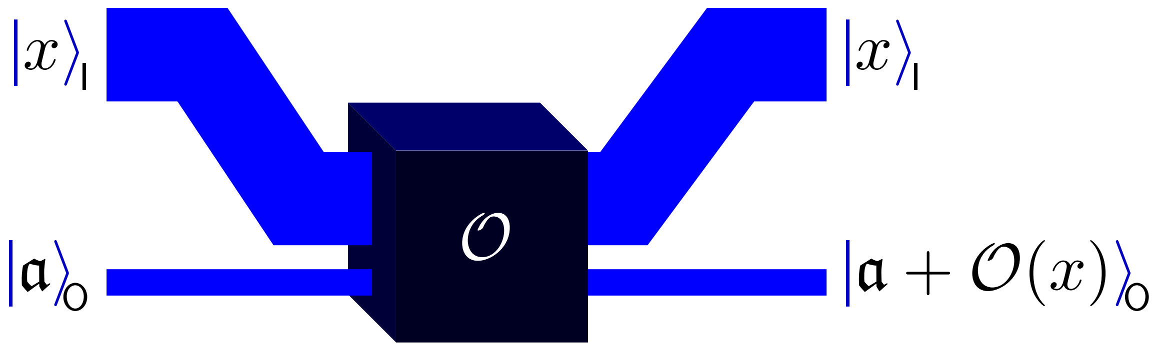
The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.

The Quantum Parity Problem

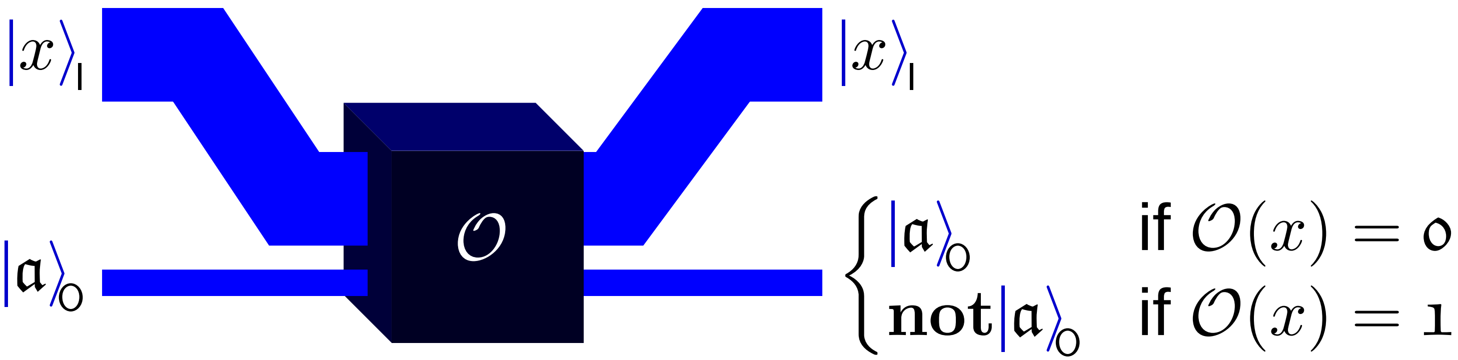
- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.
- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.



The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

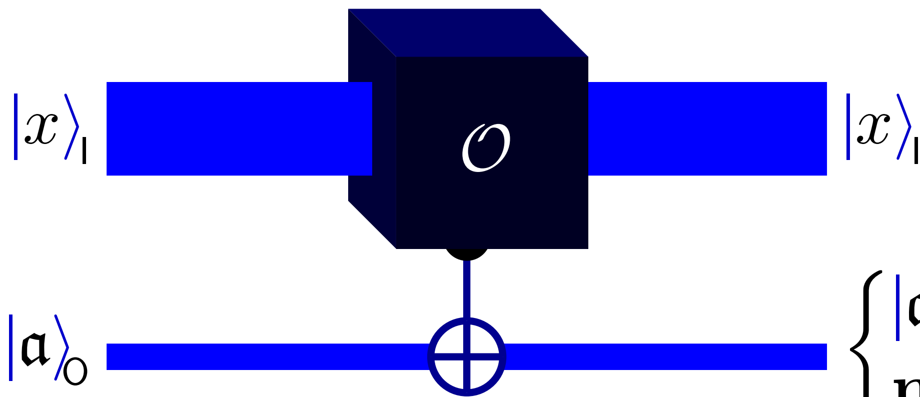
- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.



The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.

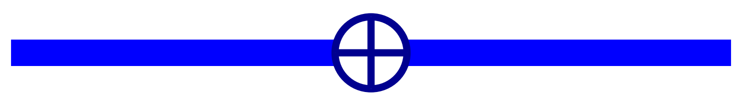


$$\begin{cases} |\mathfrak{a}\rangle_{\mathsf{0}} & \text{if } \mathcal{O}(x) = 0 \\ \mathbf{not}|\mathfrak{a}\rangle_{\mathsf{0}} & \text{if } \mathcal{O}(x) = 1 \end{cases}$$

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

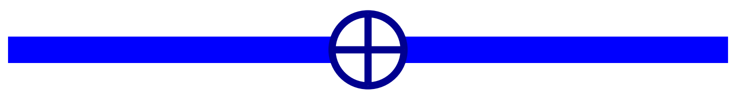
- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.



The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.
- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.

$$\frac{1}{\sqrt{2}}(|0\rangle_0 + |1\rangle_0)$$

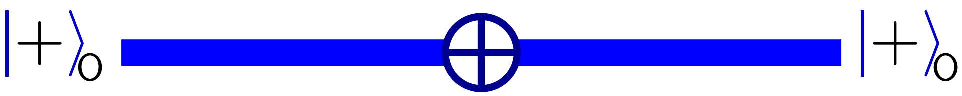


$$\frac{1}{\sqrt{2}}(|0\rangle_0 + |1\rangle_0)$$

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.

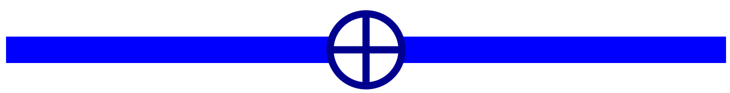


The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.

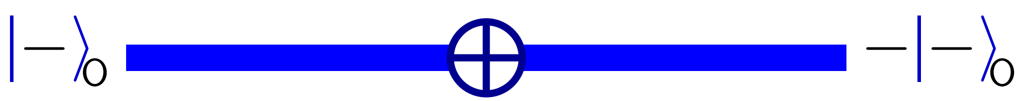
$$\frac{1}{\sqrt{2}}\big(|0\rangle_0 - |1\rangle_0\big)$$



$$-\frac{1}{\sqrt{2}}\big(|0\rangle_0 - |1\rangle_0\big)$$

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.
- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.

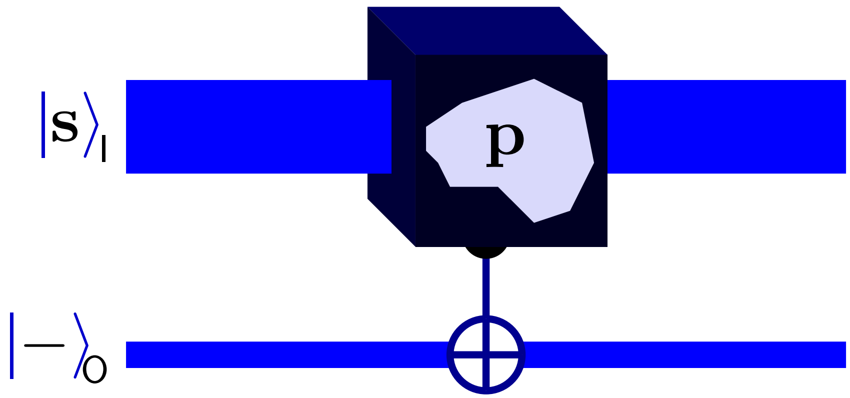


  - $|-\rangle$ is an eigenstate of $\mathbf{not}$ with eigenvalue -1.

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.

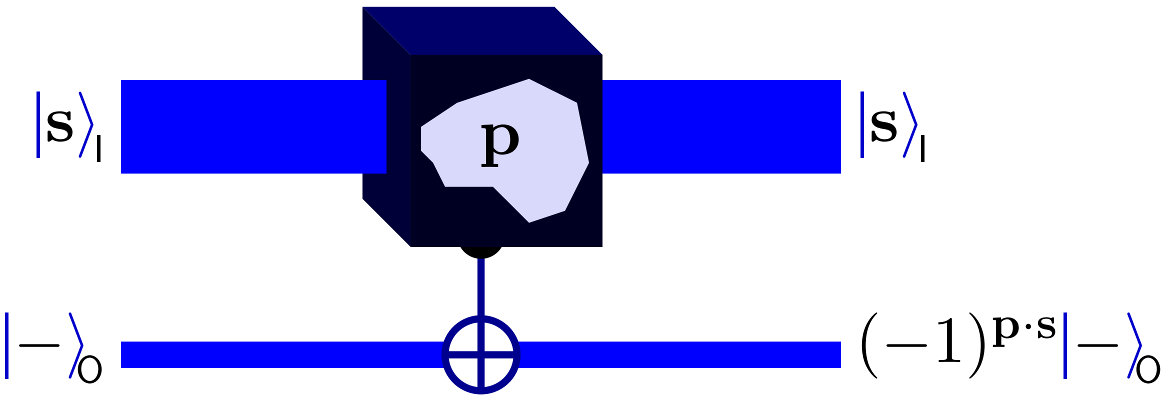


  - $|-\rangle$ is an eigenstate of $\mathbf{not}$ with eigenvalue -1.

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.

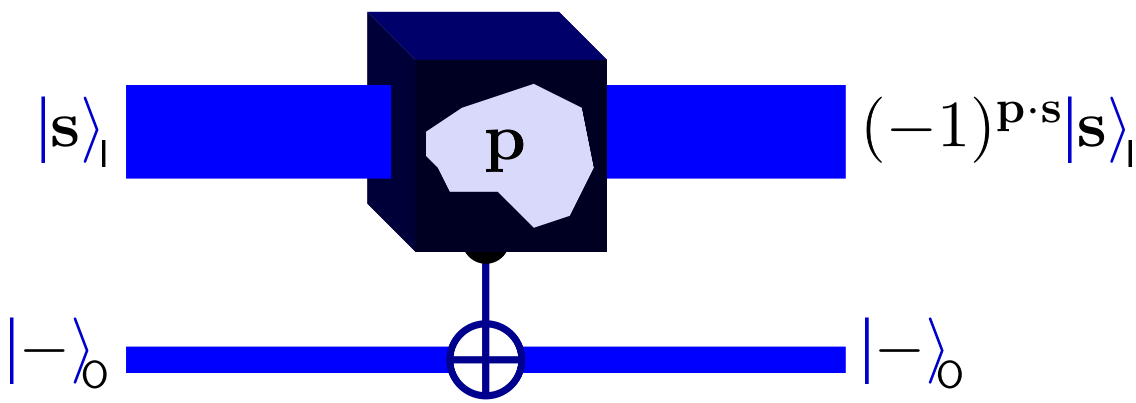


  - $|-\rangle$ is an eigenstate of $\mathbf{not}$ with eigenvalue -1.

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.

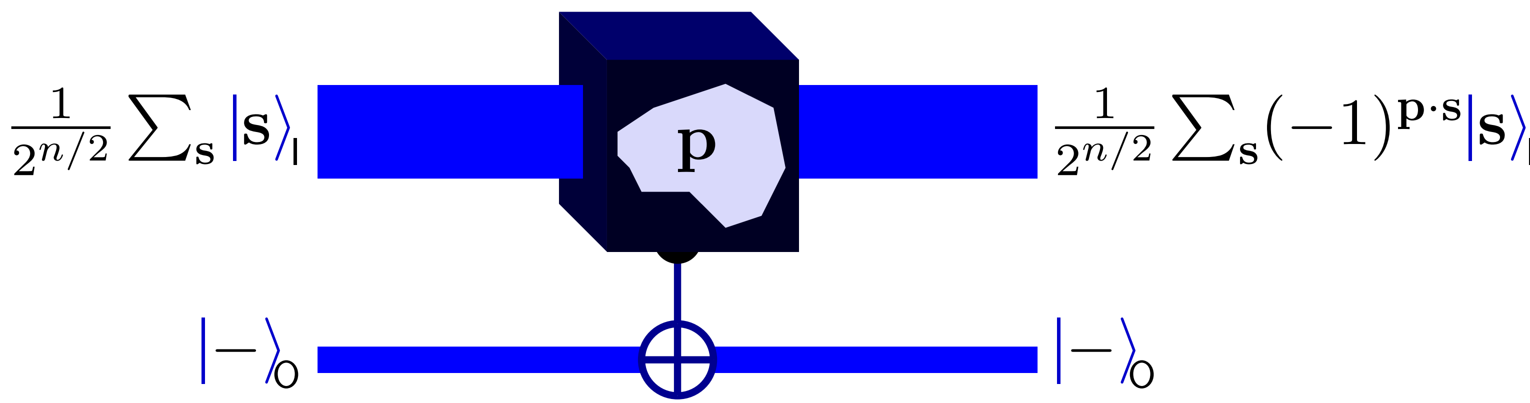


  - $|-\rangle$ is an eigenstate of $\mathbf{not}$ with eigenvalue -1.

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

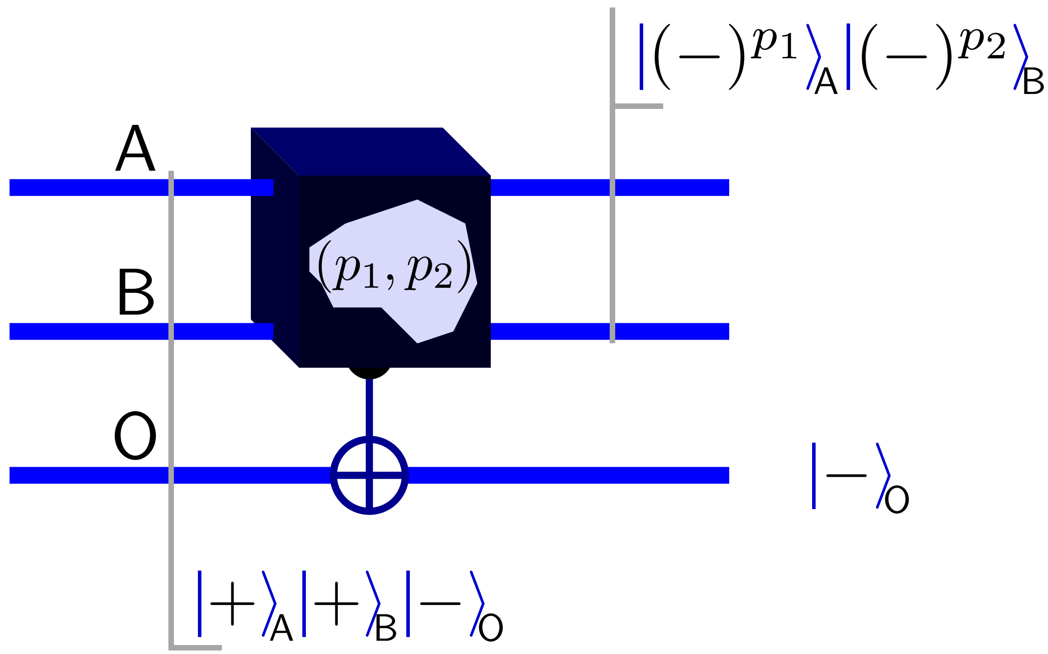
- Solution in two tricks.
  2. Sign kickback for oracles with one-bit answers.



  - $|-\rangle$ is an eigenstate of $\mathbf{not}$ with eigenvalue -1.

The Quantum Parity Problem

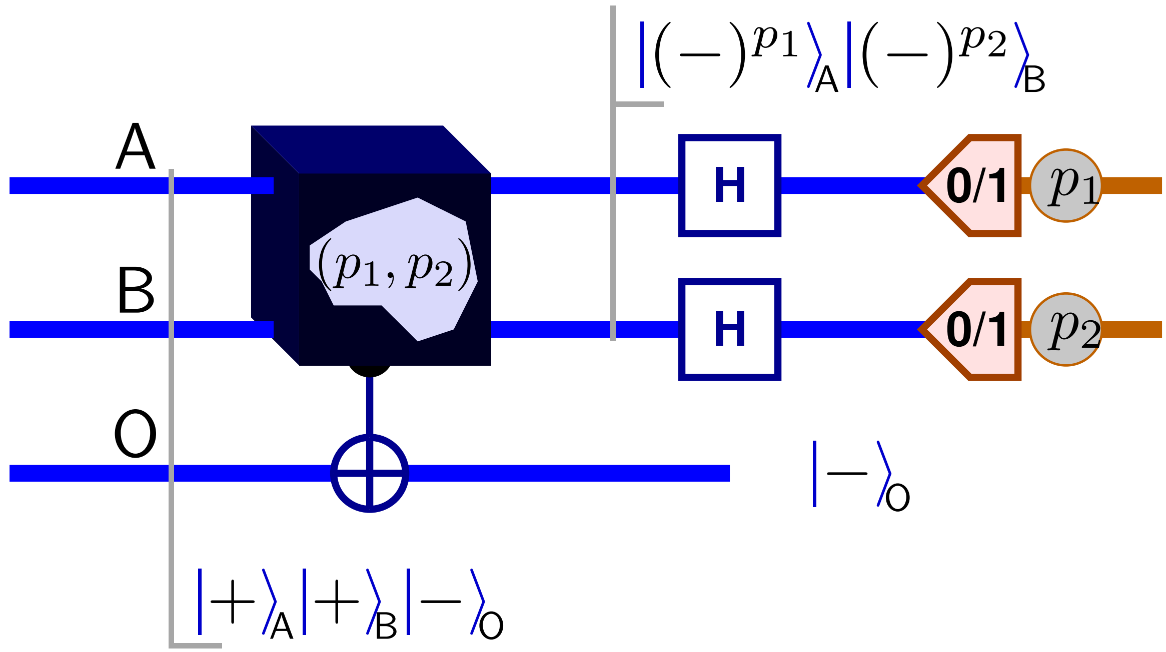
- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.
- Solution in two tricks.
  1.&2.



The Quantum Parity Problem

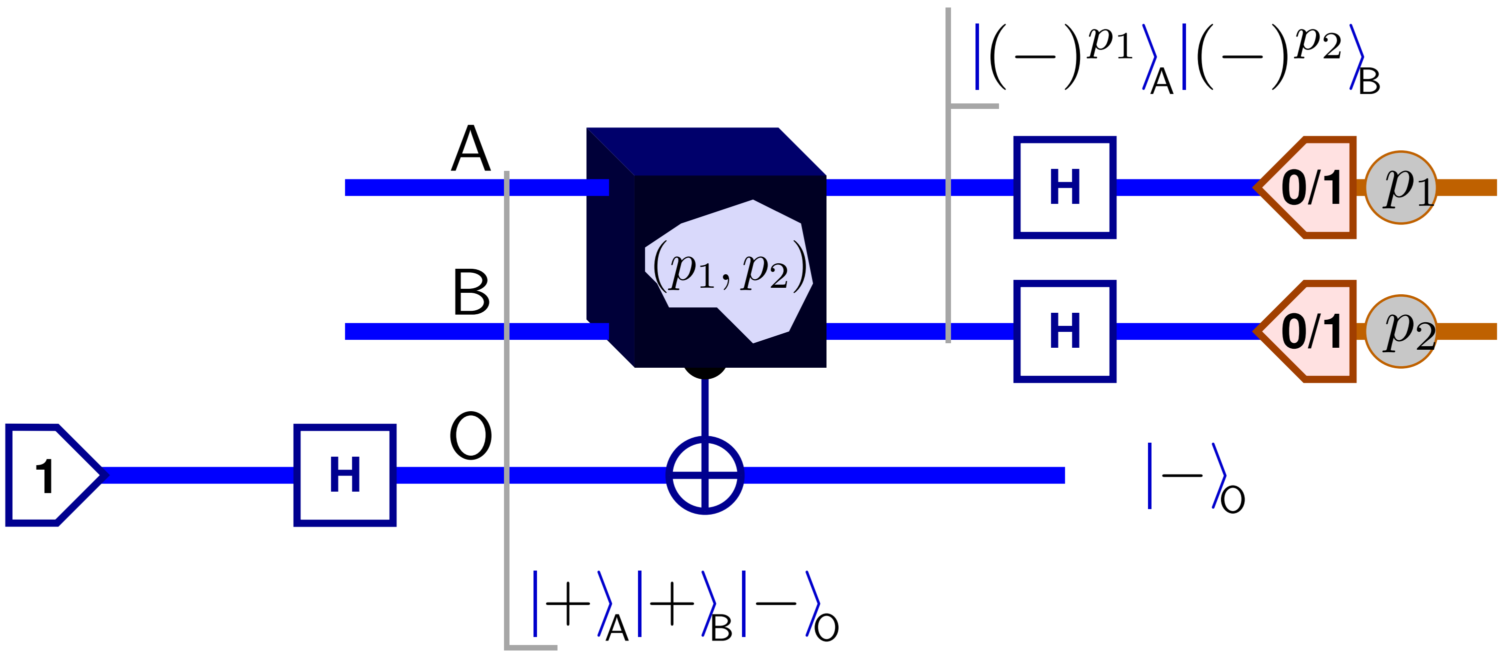
- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.
  1.&2.



The Quantum Parity Problem

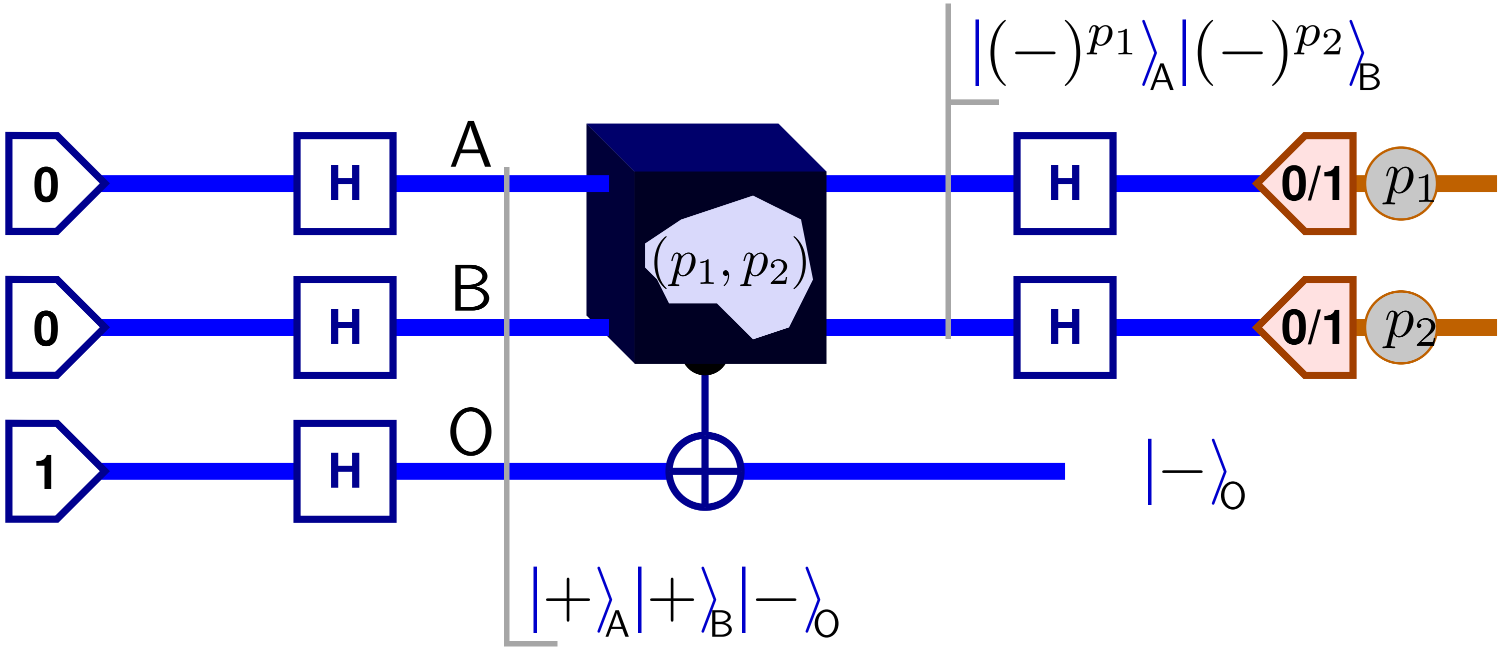
- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.
- Solution in two tricks.
  1.&2.



The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

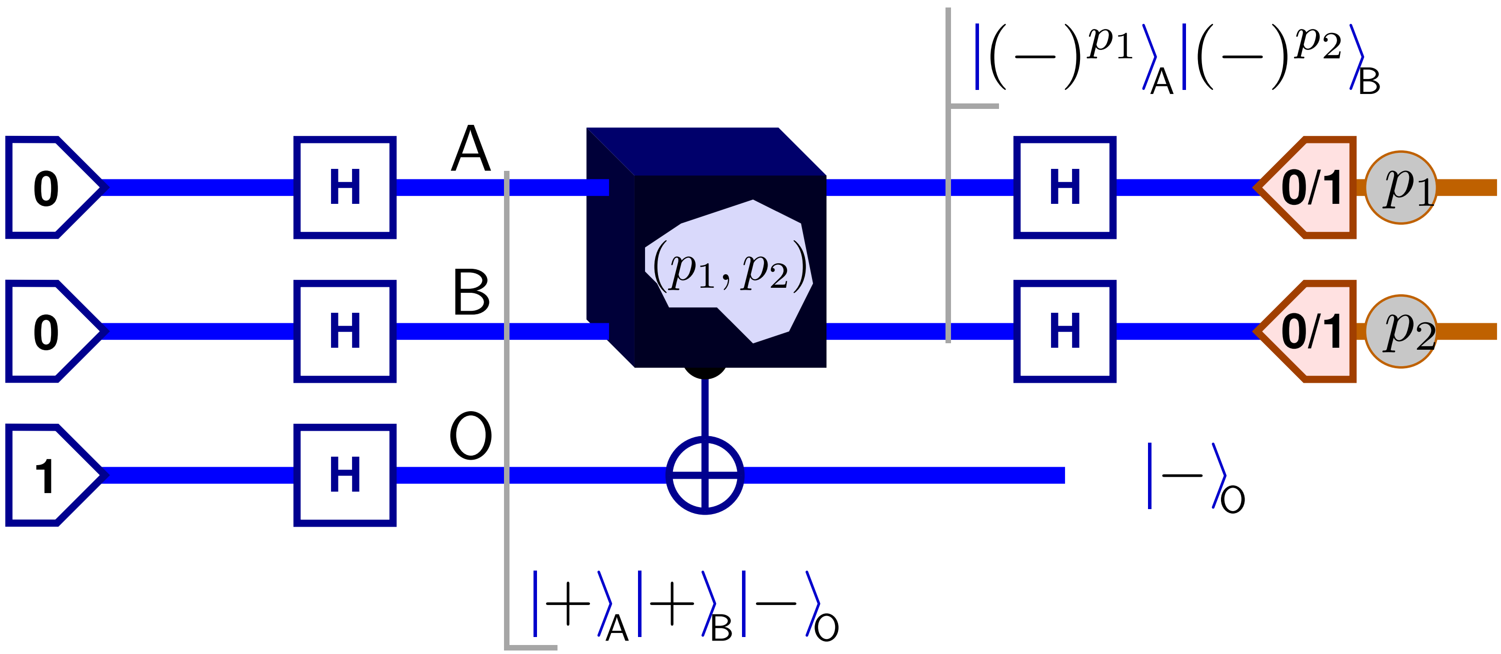
- Solution in two tricks.
  1.&2.



The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

- Solution in two tricks.
  1.&2.

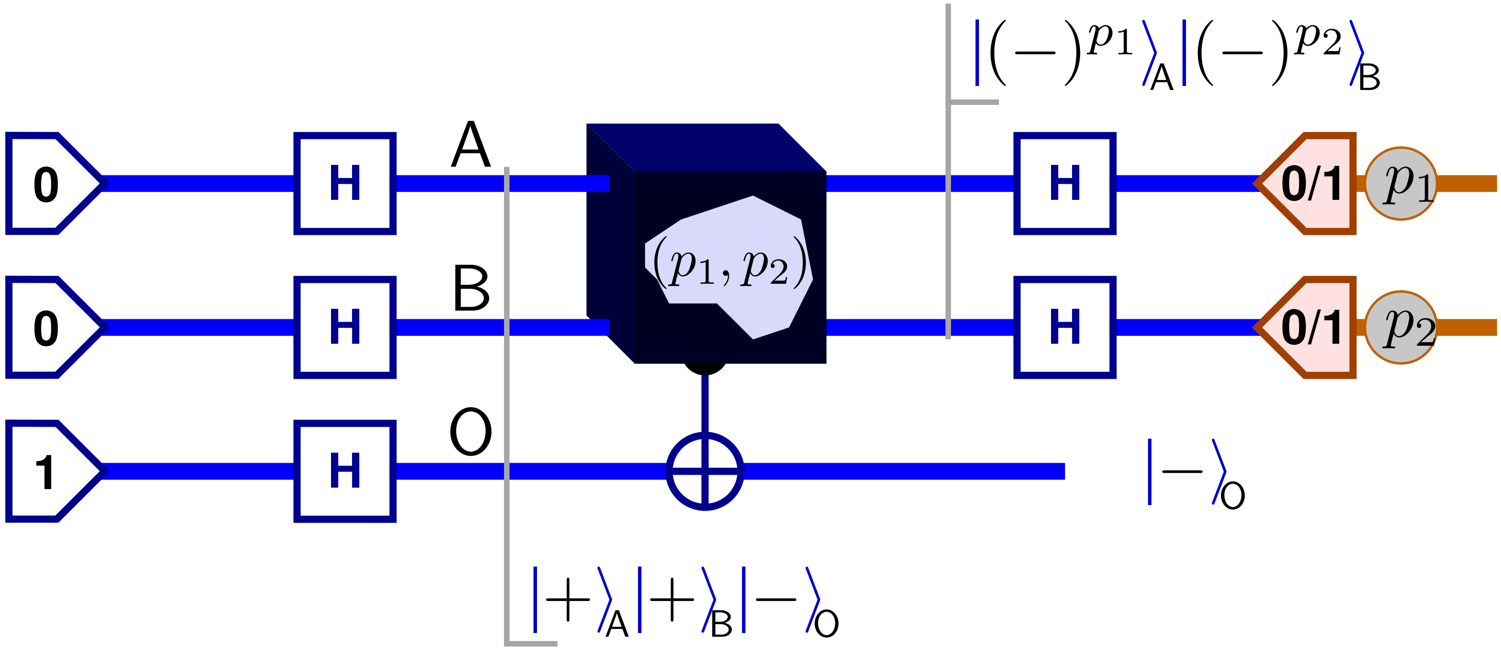


- One query suffices for solving the n-qubit parity problem.

The Quantum Parity Problem

- Promise: $\mathcal{O}$ is a quantum 2-qubit parity oracle.
  Problem: Determine the parity vector with one query.

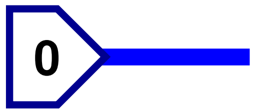
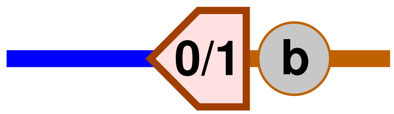
- Solution in two tricks.
  1.&2.



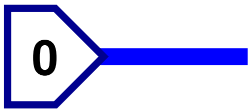
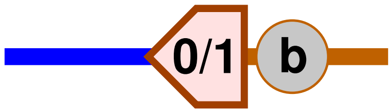
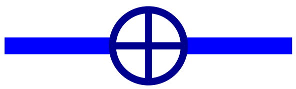
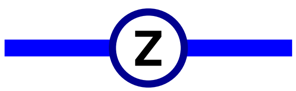
- One query suffices for solving the n-qubit parity problem.

. . . note use of “quantum parallelism”.

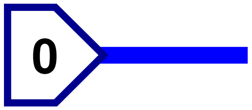
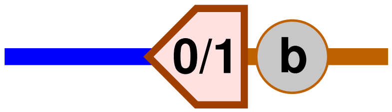
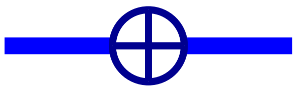
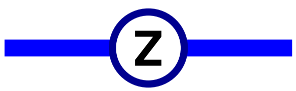
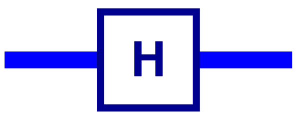
Summary of Gates Introduced So Far

Gate picture	Symbol	Matrix form
	$\mathbf{prep}(0)$	
	$\mathbf{meas}(Z\mapsto b)$	

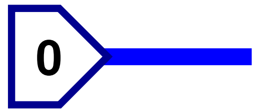
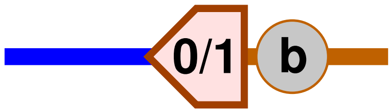
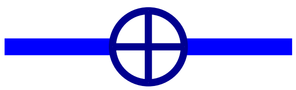
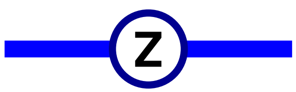
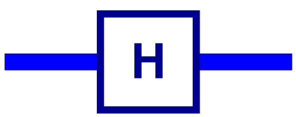
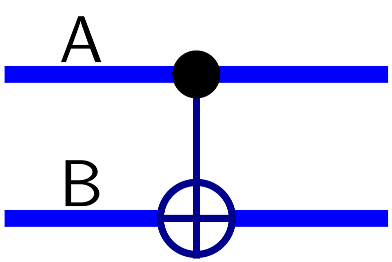
Summary of Gates Introduced So Far

Gate picture	Symbol	Matrix form
	$\mathbf{prep}(\mathtt{0})$	
	$\mathbf{meas}(Z\mapsto b)$	
	$\mathbf{not}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
	$\mathbf{sgn}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

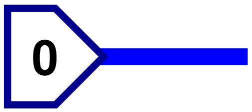
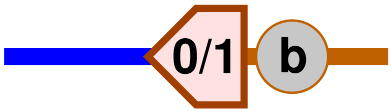
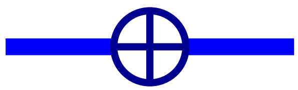
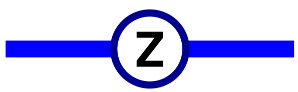
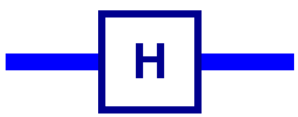
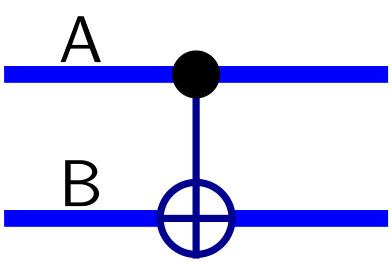
Summary of Gates Introduced So Far

Gate picture	Symbol	Matrix form
	$\mathbf{prep}(0)$	
	$\mathbf{meas}(Z\mapsto b)$	
	$\mathbf{not}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
	$\mathbf{sgn}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
	$\mathbf{had}$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Summary of Gates Introduced So Far

Gate picture	Symbol	Matrix form
	$\mathbf{prep}(0)$	
	$\mathbf{meas}(Z \mapsto b)$	
	$\mathbf{not}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
	$\mathbf{sgn}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
	$\mathbf{had}$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
	$\mathbf{cnot}^{(\mathsf{AB})}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Summary of Gates Introduced So Far

Gate picture	Symbol	Matrix form
	**prep**(0)	
	**meas**$(Z{\mapsto}b)$	
	**not**	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
	**sgn**	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
	**had**	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
	**cnot**$^{(\mathrm{AB})}$	$\begin{array}{c} \\ \lvert 00\rangle_{\mathrm{AB}} \\ \lvert 01\rangle_{\mathrm{AB}} \\ \lvert 10\rangle_{\mathrm{AB}} \\ \lvert 11\rangle_{\mathrm{AB}} \end{array} \begin{array}{c} \begin{array}{cccc} \lvert 00\rangle_{\mathrm{AB}} & \lvert 01\rangle_{\mathrm{AB}} & \lvert 10\rangle_{\mathrm{AB}} & \lvert 11\rangle_{\mathrm{AB}} \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.

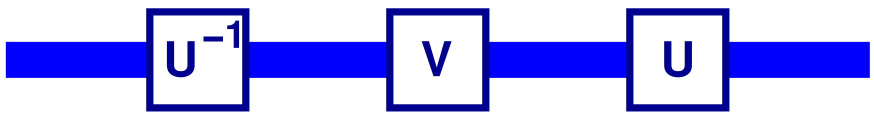
Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...

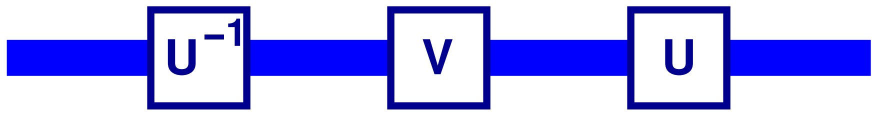
- Conjugating V by U gives $U^{-1}.V.U$.



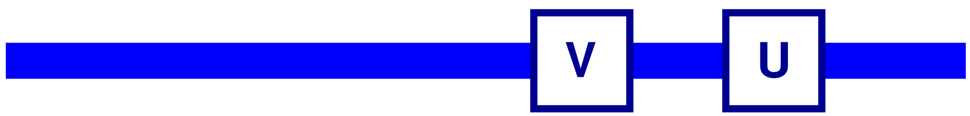
Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties…

- Conjugating V by U gives $U^{-1}.V.U$.



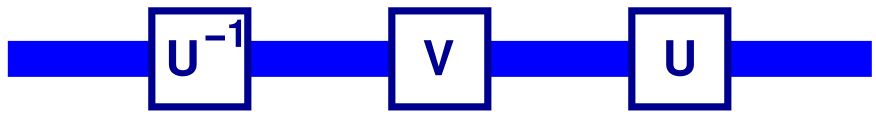
  - Applications: Network rearrangements.



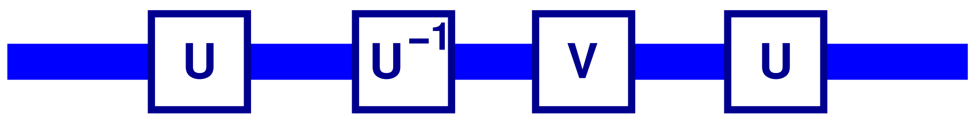
Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties. . .

- Conjugating V by U gives $U^{-1}.V.U$.



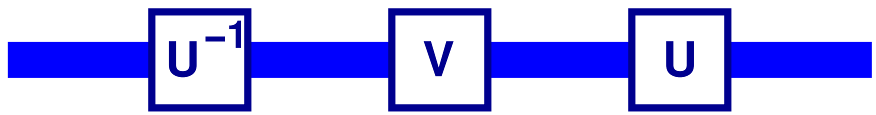
  - Applications: Network rearrangements.



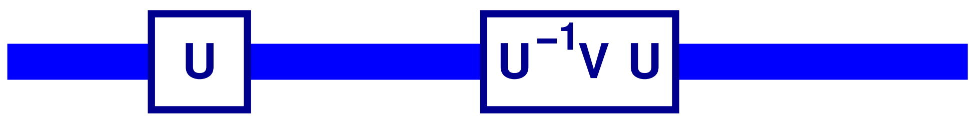
Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...

- Conjugating V by U gives $U^{-1}.V.U$.



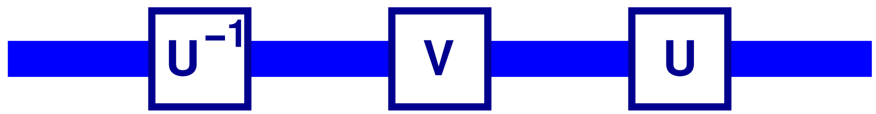
  - Applications: Network rearrangements.



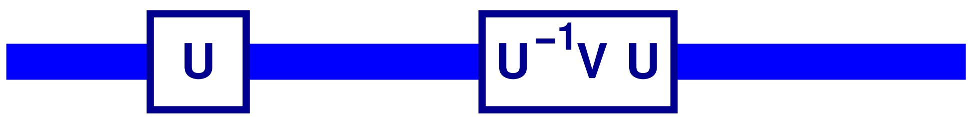
Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...

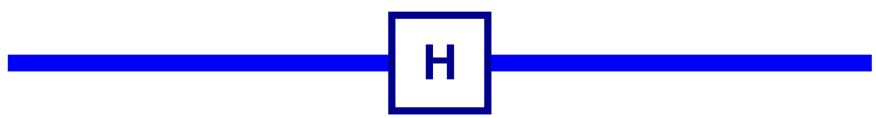
- Conjugating V by U gives $U^{-1}.V.U$.



  - Applications: Network rearrangements.



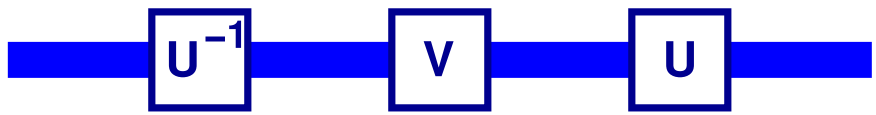
Error effect determination.



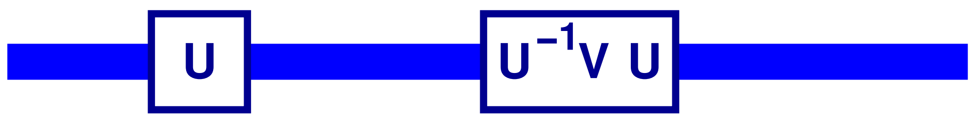
Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...

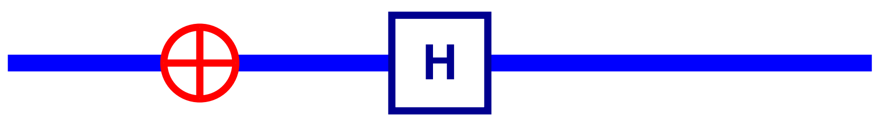
- Conjugating V by U gives $U^{-1}.V.U$.



  - Applications: Network rearrangements.



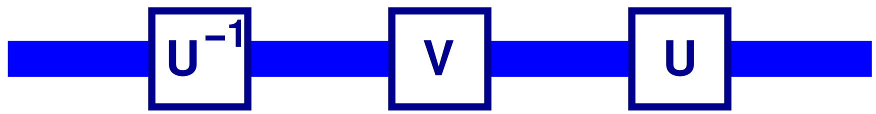
Error effect determination.



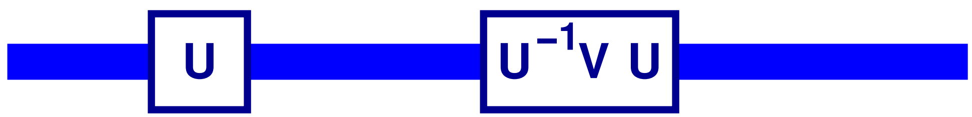
Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties. . .

- Conjugating V by U gives $U^{-1}.V.U$.



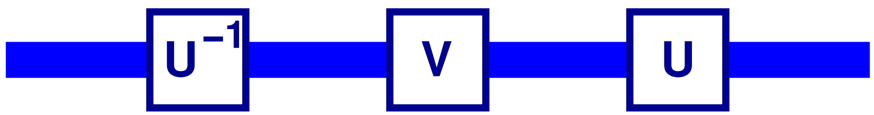
  - Applications: Network rearrangements.



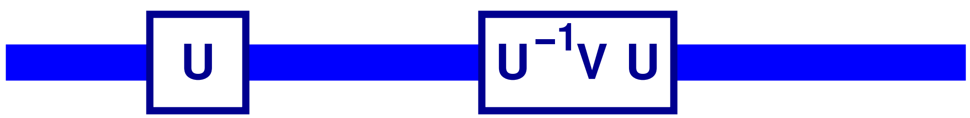
Error effect determination.

Properties of Reversible Gates

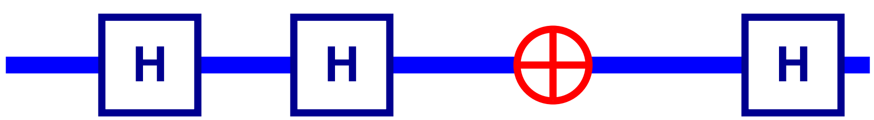
- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...
- Conjugating V by U gives $U^{-1}.V.U$.



  - Applications: Network rearrangements.



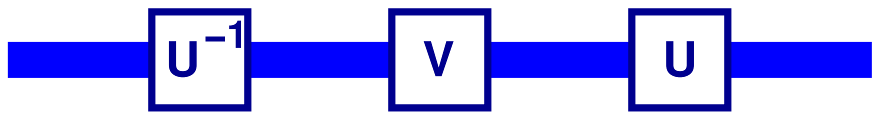
Error effect determination.



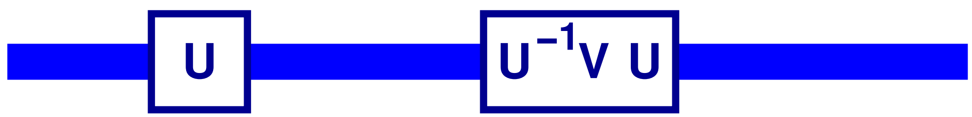
Properties of Reversible Gates

- Consider **not**, **sgn**, **had** and **cnot**. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties. . .

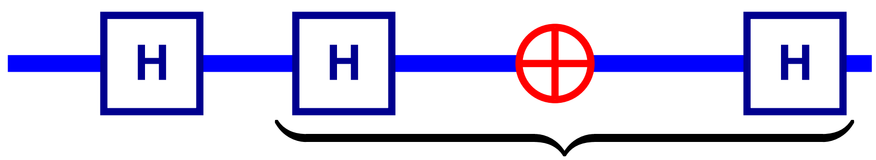
- Conjugating V by U gives $U^{-1}.V.U$.



  - Applications: Network rearrangements.



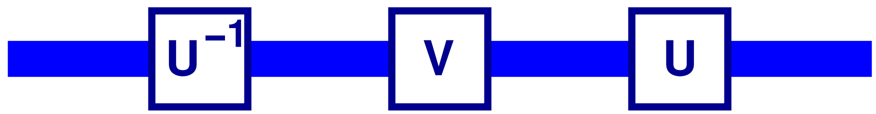
Error effect determination.



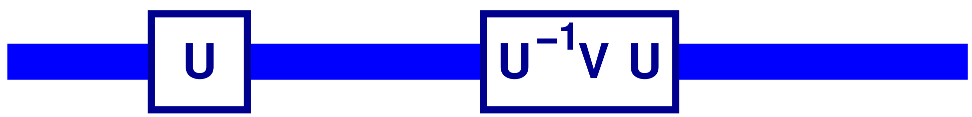
Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties. . .

- Conjugating V by U gives $U^{-1}.V.U$.



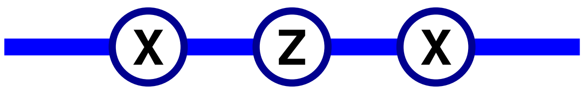
  - Applications: Network rearrangements.



Error effect determination.

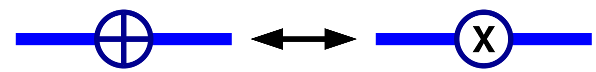
Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties. . .
- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}$, $\mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}$.

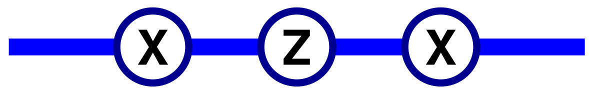


Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties. . .

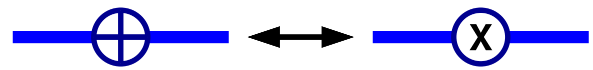


- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}, \;\; \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$

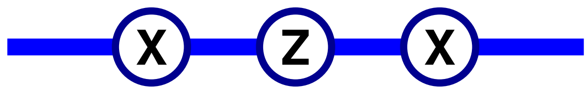


Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



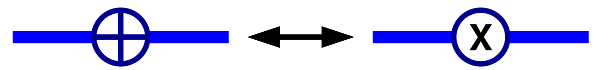
- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}, \;\; \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$



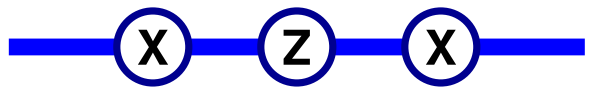
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



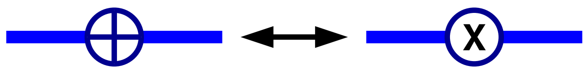
- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}, \ \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$



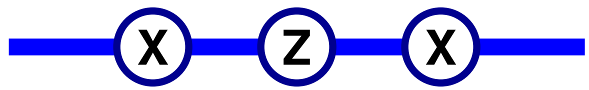
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



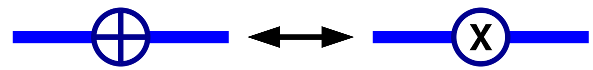
- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}, \ \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$



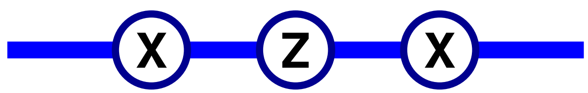
$$\underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



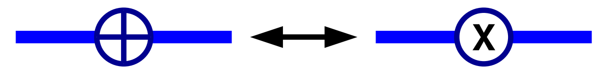
- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}, \; \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$



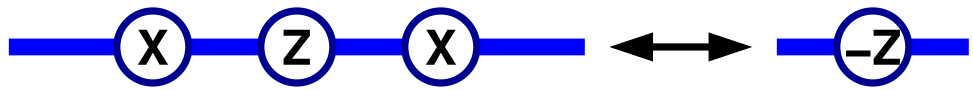
$$\underbrace{\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}}_{\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



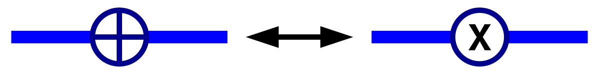
- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}$, $\mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}$.



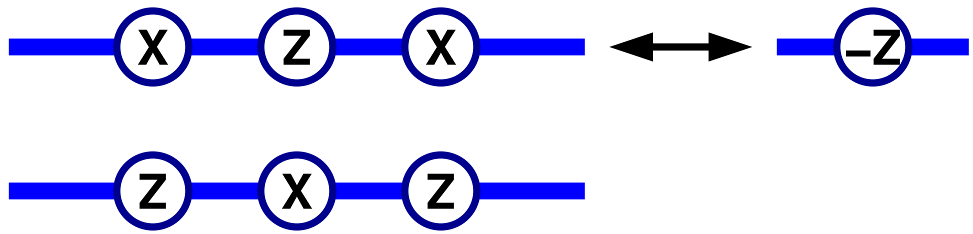
$$\underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}_{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties. . .

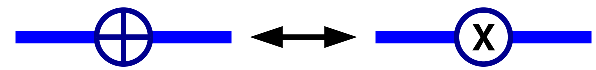


- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}, \;\; \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$

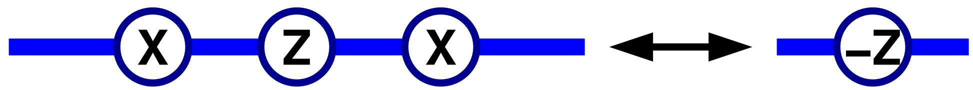


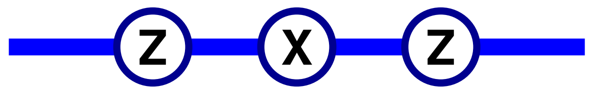
Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn},\ \ \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$

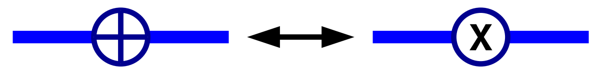




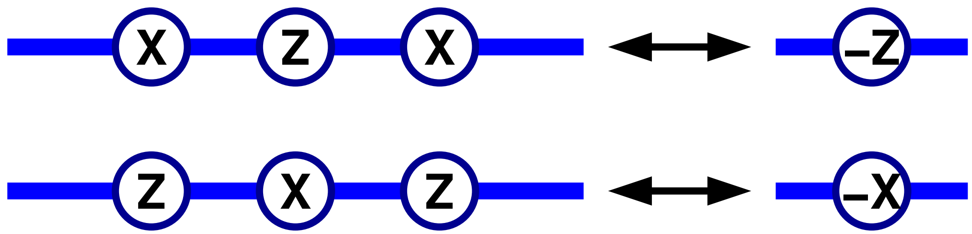
$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



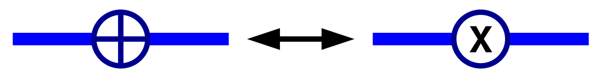
- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}, \ \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$



$$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\cdot\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \qquad \begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}$$

Properties of Reversible Gates

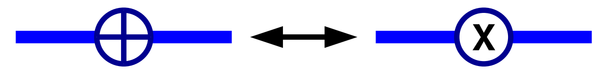
- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}, \; \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



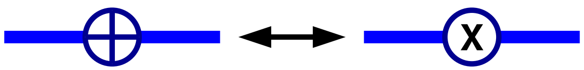
- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn},\ \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$

- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{had}$.

$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not},\ \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$

Properties of Reversible Gates

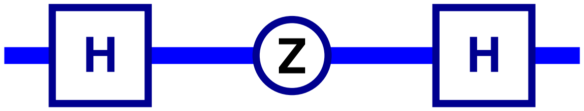
- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...

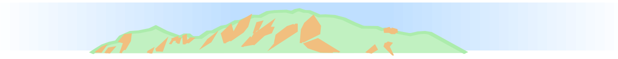


- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn},\ \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$

- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{had}$.

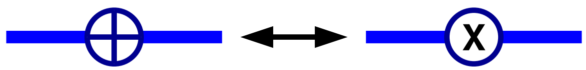
$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not},\ \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$





Properties of Reversible Gates

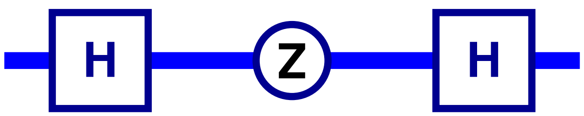
- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}, \;\; \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$

- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{had}$.

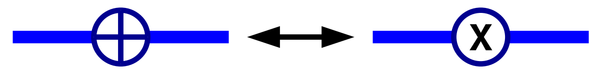
$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not}, \;\; \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$



$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}.\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

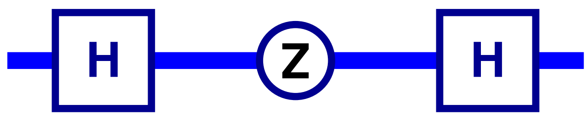
Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn},\ \ \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}$.
- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{had}$.

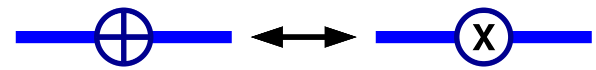
$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not},\ \ \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$



$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

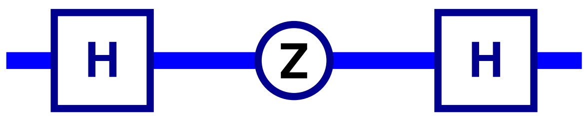
Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn},\ \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$
- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{had}$.

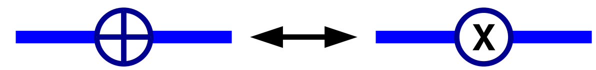
$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not},\ \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$



$$\frac{1}{\sqrt{2}}\underbrace{\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

Properties of Reversible Gates

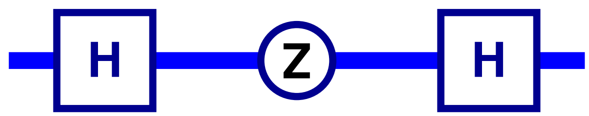
- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn},\ \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$

- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{had}$.

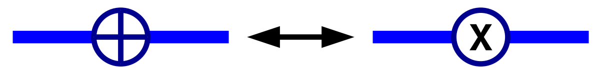
$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not},\ \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$



$$\underbrace{\tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}}_{\tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}}\tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

Properties of Reversible Gates

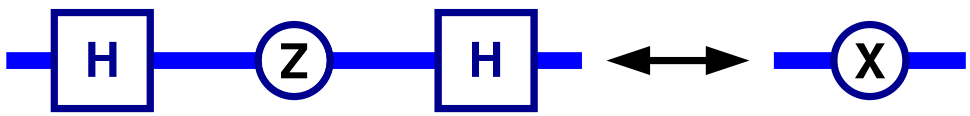
- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties. . .



- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}, \;\; \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$

- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{had}$.

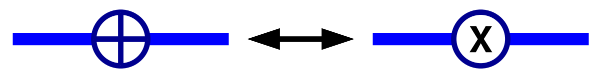
$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not}, \;\; \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$



$$\underbrace{\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}}_{\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

Properties of Reversible Gates

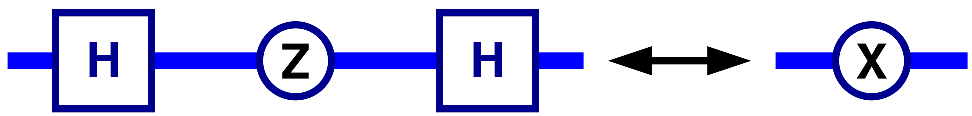
- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}, \ \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$

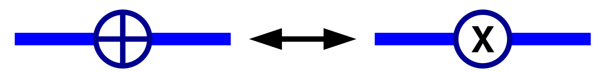
- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{had}$.

$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not}, \ \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$



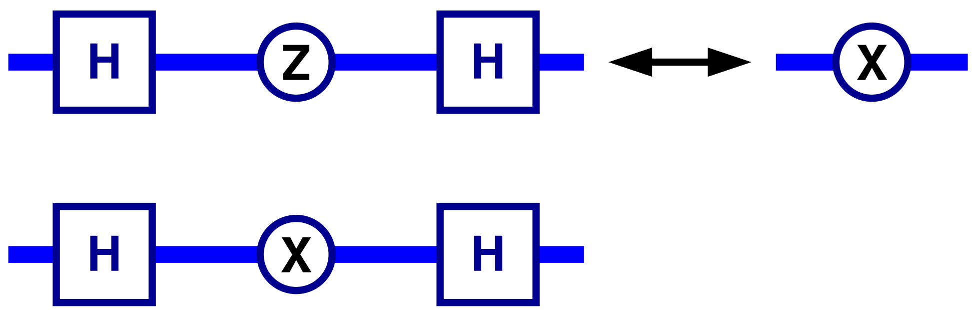
Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



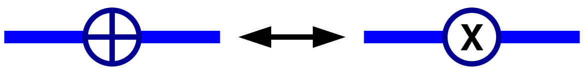
- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}$, $\mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}$.
- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{had}$.

$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not}, \;\; \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$



Properties of Reversible Gates

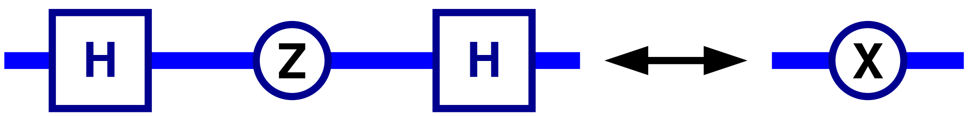
- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties. . .

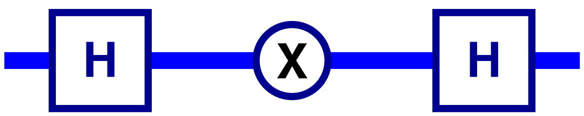


- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn}, \;\; \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$

- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{had}$.

$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not}, \;\; \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$

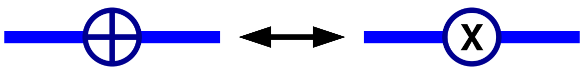




$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}.\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

Properties of Reversible Gates

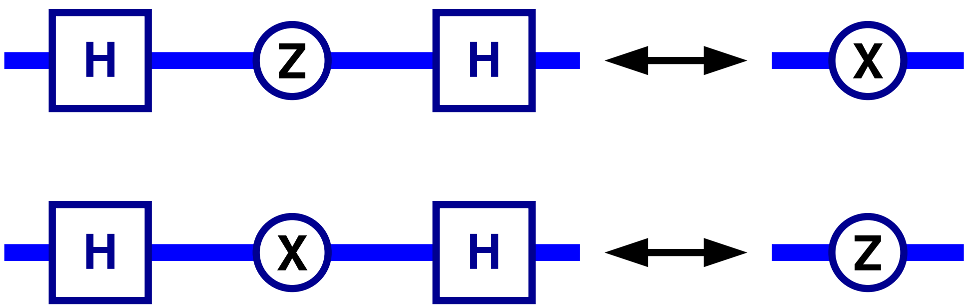
- Consider **not**, **sgn**, **had** and **cnot**. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



- **sgn** and **not**: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn},\ \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}.$

- **sgn** and **not** conjugated by **had**.

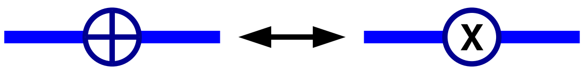
$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not},\ \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$



$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}.\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...

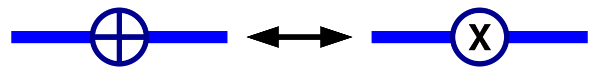


- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn},\ \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}$.
- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{had}$.

$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not},\ \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$

Properties of Reversible Gates

- Consider $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{had}$ and $\mathbf{cnot}$. They satisfy:
  - Only real coefficients.
  - $U^2 = \mathbb{1}$.
  - Conjugation properties...



- $\mathbf{sgn}$ and $\mathbf{not}$: $\mathbf{not}^{-1}.\mathbf{sgn}.\mathbf{not} = -\mathbf{sgn},\ \mathbf{sgn}^{-1}.\mathbf{not}.\mathbf{sgn} = -\mathbf{not}$.

- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{had}$.

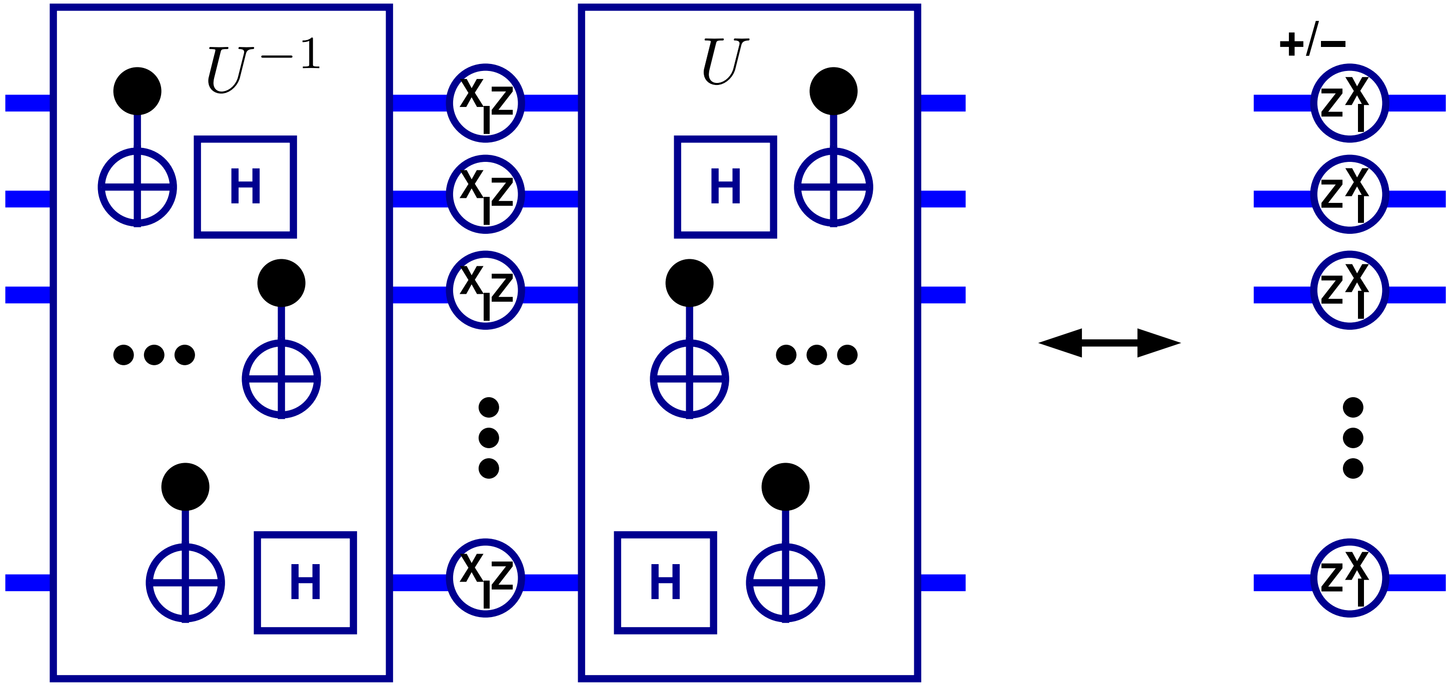
$$\mathbf{had}^{-1}.\mathbf{sgn}.\mathbf{had} = \mathbf{not},\ \mathbf{had}^{-1}.\mathbf{not}.\mathbf{had} = \mathbf{sgn}.$$

- $\mathbf{sgn}$ and $\mathbf{not}$ conjugated by $\mathbf{cnot}$.

$$\begin{aligned}
\mathbf{cnot}^{(\mathsf{AB})\,-1}.\mathbf{not}^{(\mathsf{B})}.\mathbf{cnot}^{(\mathsf{AB})} &= \mathbf{not}^{(\mathsf{B})},\\
\mathbf{cnot}^{(\mathsf{AB})\,-1}.\mathbf{sgn}^{(\mathsf{A})}.\mathbf{cnot}^{(\mathsf{AB})} &= \mathbf{sgn}^{(\mathsf{A})},\\
\mathbf{cnot}^{(\mathsf{AB})\,-1}.\mathbf{not}^{(\mathsf{A})}.\mathbf{cnot}^{(\mathsf{AB})} &= \mathbf{not}^{(\mathsf{A})}.\mathbf{not}^{(\mathsf{B})},\\
\mathbf{cnot}^{(\mathsf{AB})\,-1}.\mathbf{sgn}^{(\mathsf{B})}.\mathbf{cnot}^{(\mathsf{AB})} &= \mathbf{sgn}^{(\mathsf{A})}.\mathbf{sgn}^{(\mathsf{B})}
\end{aligned}$$

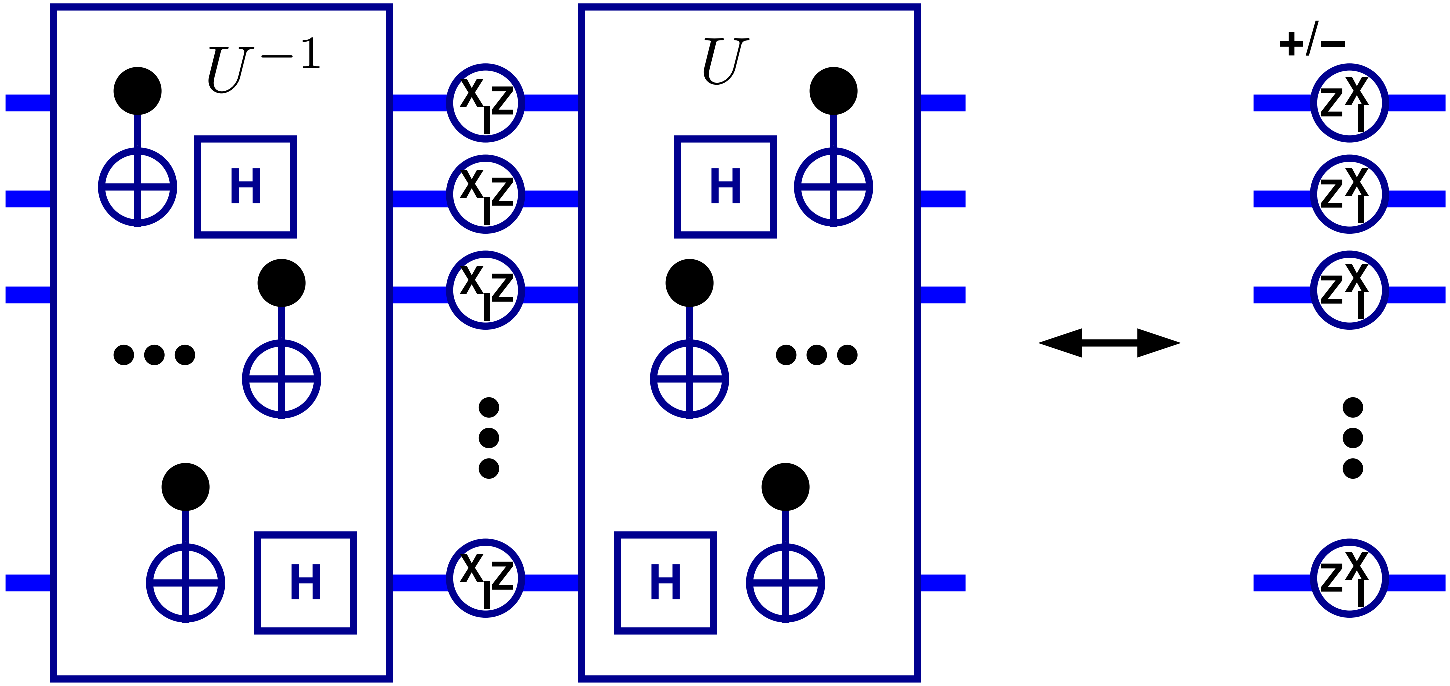
Preservation of Products of “Flips”

- Products of $\mathbf{not}$ and $\mathbf{sgn}$ are preserved under conjugation by operators composed of $\mathbf{cnot}$’s and $\mathbf{had}$’s.



Preservation of Products of “Flips”

- Products of $\mathbf{not}$ and $\mathbf{sgn}$ are preserved under conjugation by operators composed of $\mathbf{cnot}$’s and $\mathbf{had}$’s.



  - What is the power of this gate set?

Physically Allowed Reversible Operators

- Define an operator U by linear extension of

$$U|x\rangle_S = \sum_y u_{yx}|y\rangle_S$$

Physically Allowed Reversible Operators

- Define an operator U by linear extension of

$$U|x\rangle_S = \sum_y u_{yx}|y\rangle_S$$

  - To be well-defined, $U|x\rangle_S$ must be a state:

$$\sum_y |u_{yx}|^2 = 1.$$

Physically Allowed Reversible Operators

- Define an operator U by linear extension of

$$U|x\rangle_{\mathsf{S}} = \sum_y u_{yx}|y\rangle_{\mathsf{S}}$$

  - To be well-defined, $U|x\rangle_{\mathsf{S}}$ must be a state:

$$\sum_y |u_{yx}|^2 = 1.$$

  - U's linear extension must preserve states.

Physically Allowed Reversible Operators

- Define an operator U by linear extension of
$$U|x\rangle_S = \sum_y u_{yx}|y\rangle_S$$
  - To be well-defined, $U|x\rangle_S$ must be a state:
$$\sum_y |u_{yx}|^2 = 1.$$
  - U's linear extension must preserve states.
Consider $U\frac{1}{\sqrt{2}}(|x\rangle_S + e^{i\phi}|z\rangle_S) = \sum_y \frac{1}{\sqrt{2}}(u_{yx} + e^{i\phi}u_{yz})|y\rangle_S$.

Physically Allowed Reversible Operators

- Define an operator U by linear extension of
$$U|x\rangle_S = \sum_y u_{yx}|y\rangle_S$$
  - To be well-defined, $U|x\rangle_S$ must be a state:
$$\sum_y |u_{yx}|^2 = 1.$$
  - U's linear extension must preserve states.
Consider $U\frac{1}{\sqrt{2}}(|x\rangle_S + e^{i\phi}|z\rangle_S) = \sum_y \frac{1}{\sqrt{2}}(u_{yx} + e^{i\phi}u_{yz})|y\rangle_S$.
$$1 \;=\; \sum_y \tfrac{1}{2}|u_{yx} + e^{i\phi}u_{yz}|^2$$

Physically Allowed Reversible Operators

- Define an operator U by linear extension of

$$U|x\rangle_S = \sum_y u_{yx}|y\rangle_S$$

  - To be well-defined, $U|x\rangle_S$ must be a state:

$$\sum_y |u_{yx}|^2 = 1.$$

  - U's linear extension must preserve states.
    Consider $U\frac{1}{\sqrt{2}}(|x\rangle_S + e^{i\phi}|z\rangle_S) = \sum_y \frac{1}{\sqrt{2}}(u_{yx} + e^{i\phi}u_{yz})|y\rangle_S$.

$$\begin{aligned} 1 &= \sum_y \tfrac{1}{2}|u_{yx} + e^{i\phi}u_{yz}|^2 \\ &= \sum_y \tfrac{1}{2}(|u_{yx}|^2 + |u_{yz}|^2 + e^{i\phi}\bar{u}_{yx}u_{yz} + e^{-i\phi}u_{yx}\bar{u}_{yz}) \end{aligned}$$

Physically Allowed Reversible Operators

- Define an operator U by linear extension of

$$U|x\rangle_{\mathsf{S}} = \sum_y u_{yx}|y\rangle_{\mathsf{S}}$$

  - To be well-defined, $U|x\rangle_{\mathsf{S}}$ must be a state:

$$\sum_y |u_{yx}|^2 = 1.$$

  - U's linear extension must preserve states. Consider $U\frac{1}{\sqrt{2}}(|x\rangle_{\mathsf{S}} + e^{i\phi}|z\rangle_{\mathsf{S}}) = \sum_y \frac{1}{\sqrt{2}}(u_{yx} + e^{i\phi}u_{yz})|y\rangle_{\mathsf{S}}$.

$$\begin{aligned} 1 &= \sum_y \tfrac{1}{2}|u_{yx} + e^{i\phi}u_{yz}|^2 \\ &= \sum_y \tfrac{1}{2}(|u_{yx}|^2 + |u_{yz}|^2 + e^{i\phi}\bar{u}_{yx}u_{yz} + e^{-i\phi}u_{yx}\bar{u}_{yz}) \\ &= 1 + 2\sum_y \mathrm{Re}(e^{i\phi}\bar{u}_{yx}u_{yz}) \end{aligned}$$

Physically Allowed Reversible Operators

- Define an operator U by linear extension of
$$U|x\rangle_S = \sum_y u_{yx}|y\rangle_S$$
  - To be well-defined, $U|x\rangle_S$ must be a state:
$$\sum_y |u_{yx}|^2 = 1.$$
  - U's linear extension must preserve states.
Consider $U\frac{1}{\sqrt{2}}(|x\rangle_S + e^{i\phi}|z\rangle_S) = \sum_y \frac{1}{\sqrt{2}}(u_{yx} + e^{i\phi}u_{yz})|y\rangle_S$.
$$\begin{aligned} 1 &= \sum_y \tfrac{1}{2}|u_{yx} + e^{i\phi}u_{yz}|^2 \\ &= \sum_y \tfrac{1}{2}(|u_{yx}|^2 + |u_{yz}|^2 + e^{i\phi}\bar{u}_{yx}u_{yz} + e^{-i\phi}u_{yx}\bar{u}_{yz}) \\ &= 1 + 2\sum_y \mathrm{Re}(e^{i\phi}\bar{u}_{yx}u_{yz}) \\ &= 1 + 2\mathrm{Re}(e^{i\phi}\sum_y \bar{u}_{yx}u_{yz}). \end{aligned}$$

Physically Allowed Reversible Operators

- Define an operator U by linear extension of

$$U|x\rangle_S = \sum_y u_{yx}|y\rangle_S$$

  - To be well-defined, $U|x\rangle_S$ must be a state:

$$\sum_y |u_{yx}|^2 = 1.$$

  - U's linear extension must preserve states.
    Consider $U\frac{1}{\sqrt{2}}(|x\rangle_S + e^{i\phi}|z\rangle_S) = \sum_y \frac{1}{\sqrt{2}}(u_{yx} + e^{i\phi}u_{yz})|y\rangle_S$.

$$\begin{aligned} 1 &= \sum_y \tfrac{1}{2}|u_{yx} + e^{i\phi}u_{yz}|^2 \\ &= \sum_y \tfrac{1}{2}(|u_{yx}|^2 + |u_{yz}|^2 + e^{i\phi}\bar{u}_{yx}u_{yz} + e^{-i\phi}u_{yx}\bar{u}_{yz}) \\ &= 1 + 2\sum_y \mathrm{Re}(e^{i\phi}\bar{u}_{yx}u_{yz}) \\ &= 1 + 2\mathrm{Re}(e^{i\phi}\sum_y \bar{u}_{yx}u_{yz}). \end{aligned}$$

    Hence $\sum_y \bar{u}_{yx}u_{yz} = 0$.

Physically Allowed Reversible Operators

- Define an operator U by linear extension of
$$U|x\rangle_S = \sum_y u_{yx}|y\rangle_S$$
  - To be well-defined, $U|x\rangle_S$ must be a state:
$$\sum_y |u_{yx}|^2 = 1.$$
  - U's linear extension must preserve states.
Consider $U\frac{1}{\sqrt{2}}(|x\rangle_S + e^{i\phi}|z\rangle_S) = \sum_y \frac{1}{\sqrt{2}}(u_{yx} + e^{i\phi}u_{yz})|y\rangle_S$.
Hence $\sum_y \bar{u}_{yx}u_{yz} = 0$.

Physically Allowed Reversible Operators

- Define an operator U by linear extension of
$$U|x\rangle_{\mathsf{S}} = \sum_y u_{yx}|y\rangle_{\mathsf{S}}$$
  - To be well-defined, $U|x\rangle_{\mathsf{S}}$ must be a state:
  $$\sum_y |u_{yx}|^2 = 1.$$
  - U's linear extension must preserve states.
  Consider $U\frac{1}{\sqrt{2}}(|x\rangle_{\mathsf{S}} + e^{i\phi}|z\rangle_{\mathsf{S}}) = \sum_y \frac{1}{\sqrt{2}}(u_{yx} + e^{i\phi}u_{yz})|y\rangle_{\mathsf{S}}$.
  Hence $\sum_y \bar{u}_{yx}u_{yz} = 0$.
- U is *unitary*.

Physically Allowed Reversible Operators

- Define an operator U by linear extension of

$$U|x\rangle_{\mathsf{S}} = \sum_y u_{yx}|y\rangle_{\mathsf{S}}$$

  - To be well-defined, $U|x\rangle_{\mathsf{S}}$ must be a state:

$$\sum_y |u_{yx}|^2 = 1.$$

  - U's linear extension must preserve states.
    Consider $U\frac{1}{\sqrt{2}}(|x\rangle_{\mathsf{S}} + e^{i\phi}|z\rangle_{\mathsf{S}}) = \sum_y \frac{1}{\sqrt{2}}(u_{yx} + e^{i\phi}u_{yz})|y\rangle_{\mathsf{S}}$.
    Hence $\sum_y \bar{u}_{yx}u_{yz} = 0$.

- U is *unitary*. In matrix form with $x \in \{1, 2, \ldots, N\}$:

$$\begin{array}{ccccc} U^\dagger & U & & \mathbb{1} \\ \begin{pmatrix} \bar{u}_{11} & \bar{u}_{21} & \ldots & \bar{u}_{N1} \\ \bar{u}_{12} & \bar{u}_{22} & \ldots & \bar{u}_{N2} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{u}_{1N} & \bar{u}_{2N} & \ldots & \bar{u}_{NN} \end{pmatrix} & \begin{pmatrix} u_{11} & u_{12} & \ldots & u_{1N} \\ u_{21} & u_{22} & \ldots & u_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ u_{N1} & u_{N2} & \ldots & u_{NN} \end{pmatrix} & = & \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \end{array}$$

Physically Allowed Reversible Operators

- Define an operator U by linear extension of

$$U|x\rangle_{S} = \sum_y u_{yx}|y\rangle_{S}$$

  - To be well-defined, $U|x\rangle_{S}$ must be a state:

$$\sum_y |u_{yx}|^2 = 1.$$

  - U's linear extension must preserve states.
    Consider $U\frac{1}{\sqrt{2}}(|x\rangle_{S} + e^{i\phi}|z\rangle_{S}) = \sum_y \frac{1}{\sqrt{2}}(u_{yx} + e^{i\phi}u_{yz})|y\rangle_{S}$.
    Hence $\sum_y \bar{u}_{yx}u_{yz} = 0$.

- U is *unitary*. In matrix form with $x \in \{1, 2, \ldots, N\}$:

$$\begin{array}{ccccc} U^\dagger & & U & & \mathbb{1} \\ \begin{pmatrix} \bar{u}_{11} & \bar{u}_{21} & \ldots & \bar{u}_{N1} \\ \bar{u}_{12} & \bar{u}_{22} & \ldots & \bar{u}_{N2} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{u}_{1N} & \bar{u}_{2N} & \ldots & \bar{u}_{NN} \end{pmatrix} & & \begin{pmatrix} u_{11} & u_{12} & \ldots & u_{1N} \\ u_{21} & u_{22} & \ldots & u_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ u_{N1} & u_{N2} & \ldots & u_{NN} \end{pmatrix} & = & \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \end{array}$$

- Should every unitary operator be implementable?

Universality for Gate Sets

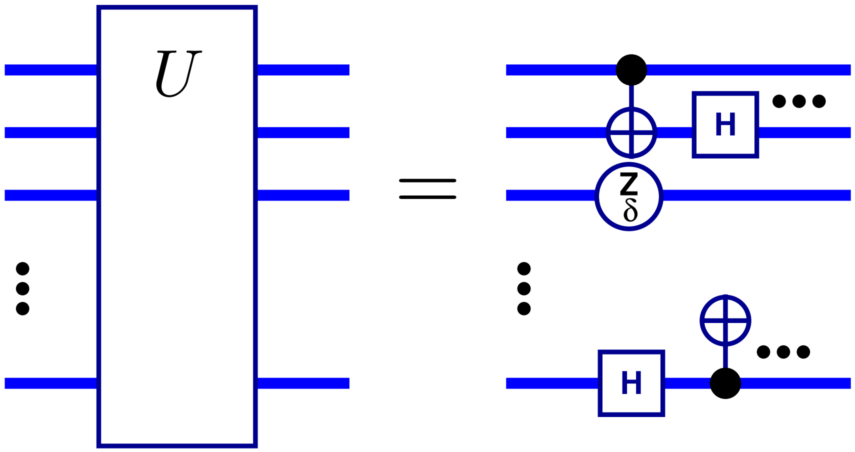
- Should every unitary operator be implementable?

Universality for Gate Sets

- Should every unitary operator be implementable?
- A set of gates is *universal* if every unitary n-qubit operator can be implemented with a network.

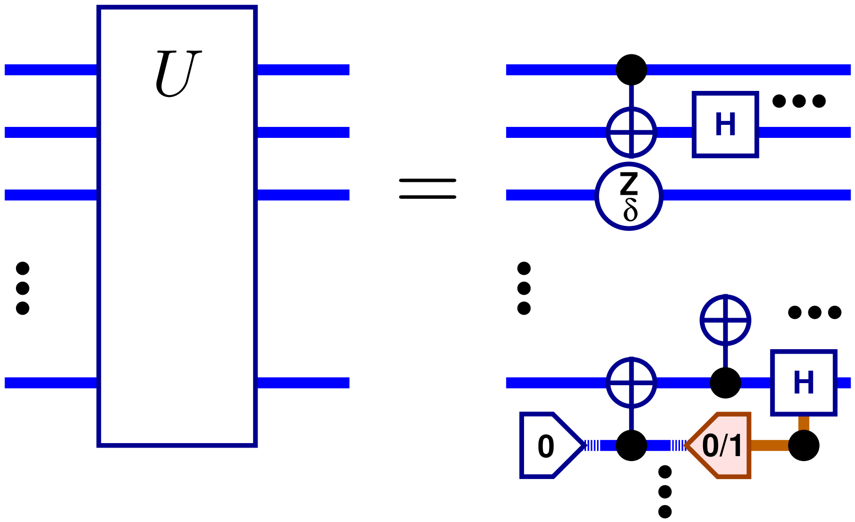
Universality for Gate Sets

- Should every unitary operator be implementable?
- A set of gates is *universal* if every unitary n-qubit operator can be implemented with a network.



Universality for Gate Sets

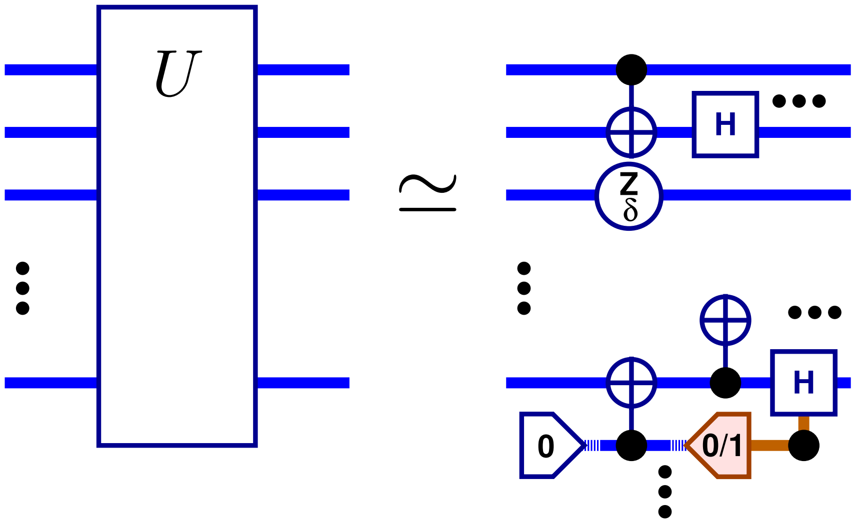
- Should every unitary operator be implementable?
- A set of gates is *universal* if every unitary n-qubit operator can be implemented with a network.



- Other notions of universality:
  - Allow use of ancillas and measurements.

Universality for Gate Sets

- Should every unitary operator be implementable?
- A set of gates is *universal* if every unitary n-qubit operator can be implemented with a network.



- Other notions of universality:
  - Allow use of ancillas and measurements.
  - Allow approximation to within arbitrarily small error.

Locality Constraints on Gate Sets

- Can any n-qubit unitary operator be a gate?

Locality Constraints on Gate Sets

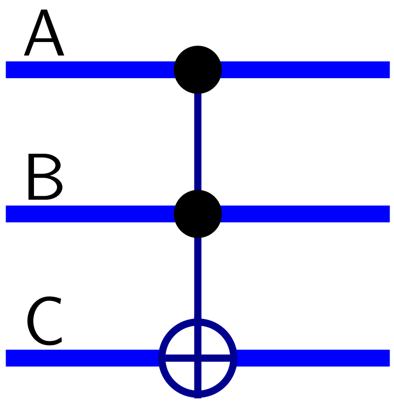
- Can any n-qubit unitary operator be a gate?
  - "Good" gates are physically realizable in one step.

Locality Constraints on Gate Sets

- Can any n-qubit unitary operator be a gate?
  - “Good” gates are physically realizable in one step.
  - Locality: Elementary gates act on at most three qubits.

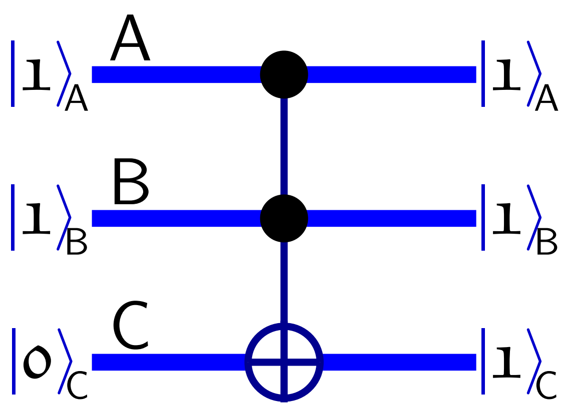
Locality Constraints on Gate Sets

- Can any n-qubit unitary operator be a gate?
  - "Good" gates are physically realizable in one step.
  - Locality: Elementary gates act on at most three qubits.
    The Toffoli gate: $\mathbf{c^2not}^{(\mathsf{ABC})} \;=\; \underline{\textbf{if}}$ A&B $\underline{\textbf{then}}$ $\mathbf{not}^{(\mathsf{C})}$.



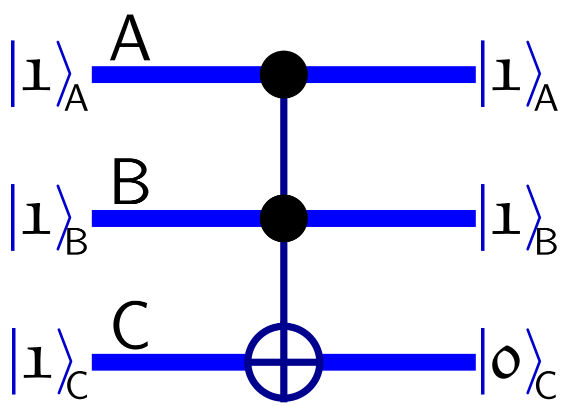
Locality Constraints on Gate Sets

- Can any n-qubit unitary operator be a gate?
  - "Good" gates are physically realizable in one step.
  - Locality: Elementary gates act on at most three qubits.
    The Toffoli gate: $\mathbf{c^2not}^{(\mathsf{ABC})} = \underline{\textbf{if}}\ \mathsf{A}\&\mathsf{B}\ \underline{\textbf{then}}\ \mathbf{not}^{(\mathsf{C})}$.



Locality Constraints on Gate Sets

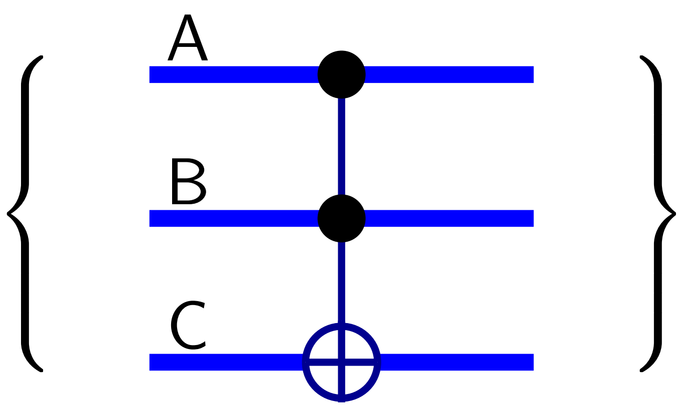
- Can any n-qubit unitary operator be a gate?
  - "Good" gates are physically realizable in one step.
  - Locality: Elementary gates act on at most three qubits.
    The Toffoli gate: $\mathbf{c^2not}^{(\mathsf{ABC})} \;=\; \underline{\textbf{if}}\;\; \mathsf{A}\&\mathsf{B}\; \underline{\textbf{then}}\;\; \mathbf{not}^{(\mathsf{C})}$.



Locality Constraints on Gate Sets

- Can any n-qubit unitary operator be a gate?
  - "Good" gates are physically realizable in one step.
  - Locality: Elementary gates act on at most three qubits. The Toffoli gate: $\mathbf{c^2not}^{(\mathsf{ABC})} = \underline{\textbf{if}}\ \mathsf{A}\&\mathsf{B}\ \underline{\textbf{then}}\ \mathbf{not}^{(\mathsf{C})}$.

$$|\mathfrak{abc}\rangle_{\mathsf{ABC}}$$

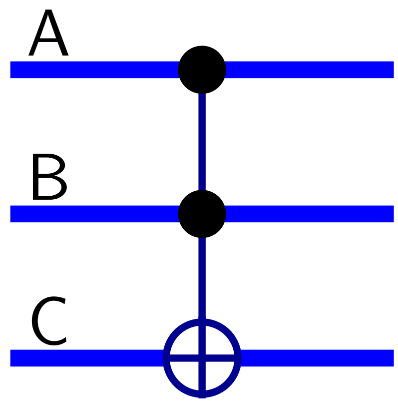


$$|\mathfrak{ab}(c+\mathfrak{a}\cdot\mathfrak{b})\rangle_{\mathsf{ABC}}$$

Locality Constraints on Gate Sets

- Can any n-qubit unitary operator be a gate?
  - "Good" gates are physically realizable in one step.
  - Locality: Elementary gates act on at most three qubits. The Toffoli gate: $\mathbf{c^2not}^{(\mathsf{ABC})} = \underline{\textbf{if}}\ \mathsf{A}\&\mathsf{B}\ \underline{\textbf{then}}\ \mathbf{not}^{(\mathsf{C})}$.

$$|\mathfrak{abc}\rangle_{\mathsf{ABC}} \quad \Bigg\{$$



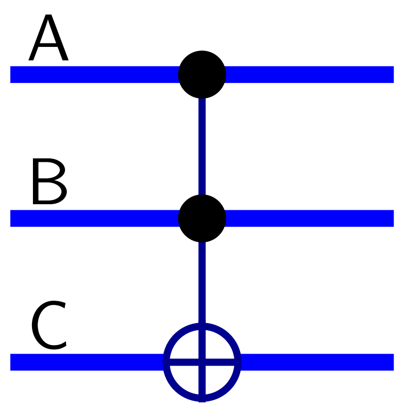
$$\Bigg\} \quad |\mathfrak{ab}(c + \mathfrak{a}\cdot\mathfrak{b})\rangle_{\mathsf{ABC}}$$

  - Discreteness: Finite gate sets are preferred.

Locality Constraints on Gate Sets

- Can any n-qubit unitary operator be a gate?
  - "Good" gates are physically realizable in one step.
  - Locality: Elementary gates act on at most three qubits. The Toffoli gate: $\mathbf{c^2not}^{(\mathsf{ABC})} \;=\; \underline{\textbf{if}}\ \mathsf{A}\&\mathsf{B}\ \underline{\textbf{then}}\ \mathbf{not}^{(\mathsf{C})}$.

$$|\mathfrak{abc}\rangle_{\mathsf{ABC}} \left\{ \quad \right.$$



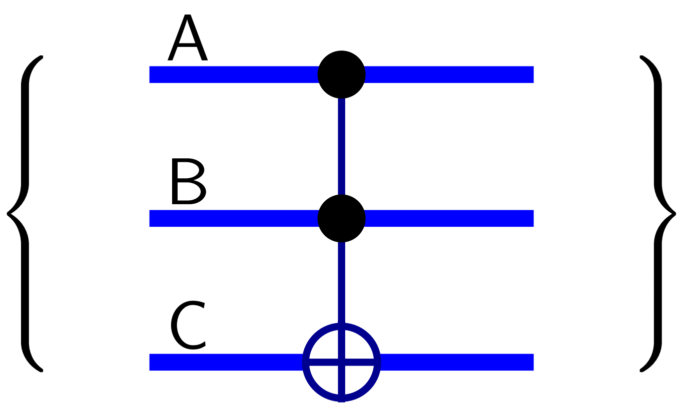
$$\left. \quad \right\} |\mathfrak{ab}(c+\mathfrak{a}\cdot\mathfrak{b})\rangle_{\mathsf{ABC}}$$

  - Discreteness: Finite gate sets are preferred.
  - Fault tolerance: Elementary gates should be experimentally verifiable and readily made stable.

Locality Constraints on Gate Sets

- Can any n-qubit unitary operator be a gate?
  - “Good” gates are physically realizable in one step.
  - Locality: Elementary gates act on at most three qubits. The Toffoli gate: $\mathbf{c^2not}^{(\mathsf{ABC})} = \underline{\mathbf{if}}\ \mathsf{A}\&\mathsf{B}\ \underline{\mathbf{then}}\ \mathbf{not}^{(\mathsf{C})}$.

$|\mathfrak{abc}\rangle_{\mathsf{ABC}}$



$|\mathfrak{ab}(c+\mathfrak{a}\cdot\mathfrak{b})\rangle_{\mathsf{ABC}}$

  - Discreteness: Finite gate sets are preferred.
  - Fault tolerance: Elementary gates should be experimentally verifiable and readily made stable.
- . . . but do investigate other gate sets.

Contents

References

[1] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26:1411–1473, 1997.

[2] L. K. Grover. Quantum computers can search arbitrarily large databases by a single query. *Phys. Rev. Lett.*, 79:4709–4712, 1997.

[3] D. A. Meyer. Sophisticated quantum search without entanglement. *Phys. Rev. Lett.*, 85:2014–2017, 2000.