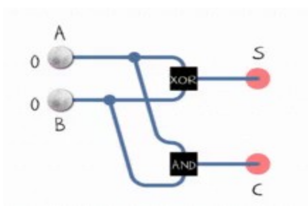
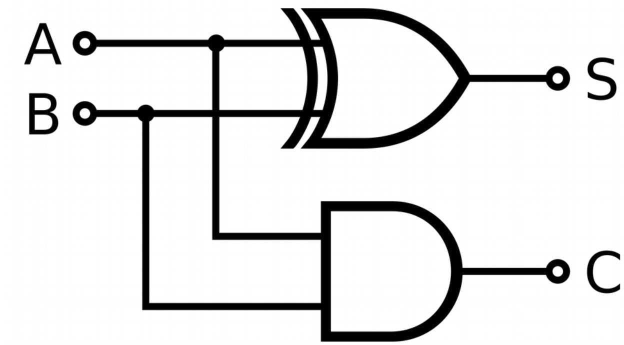
1) Basics of quantum computing

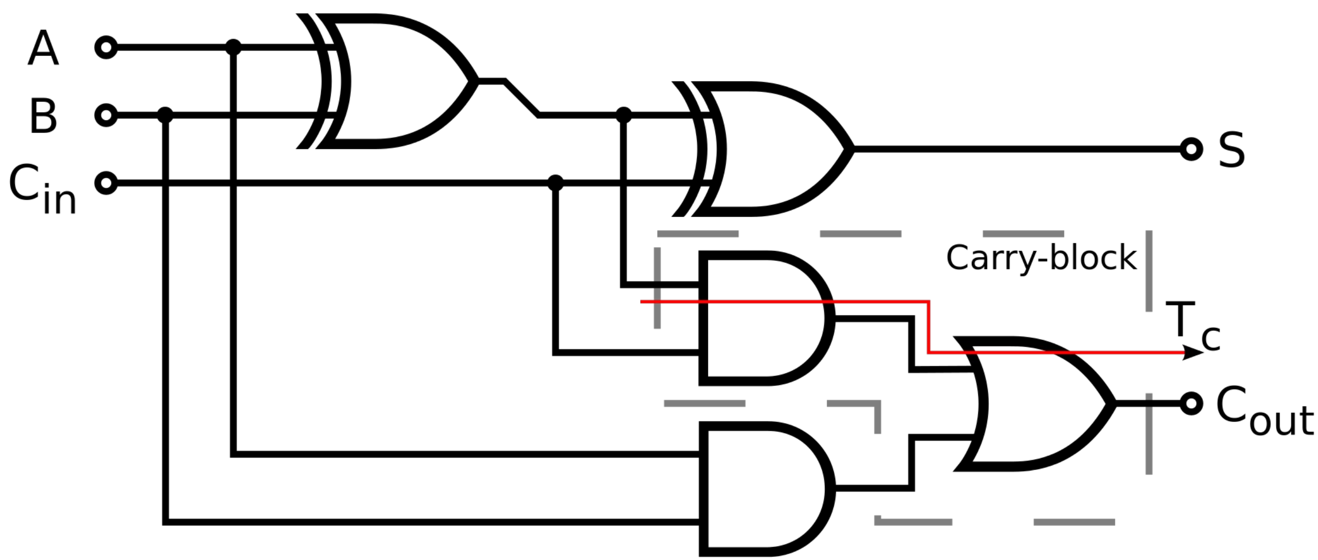
Discrete Information Processing is described by logic circuits



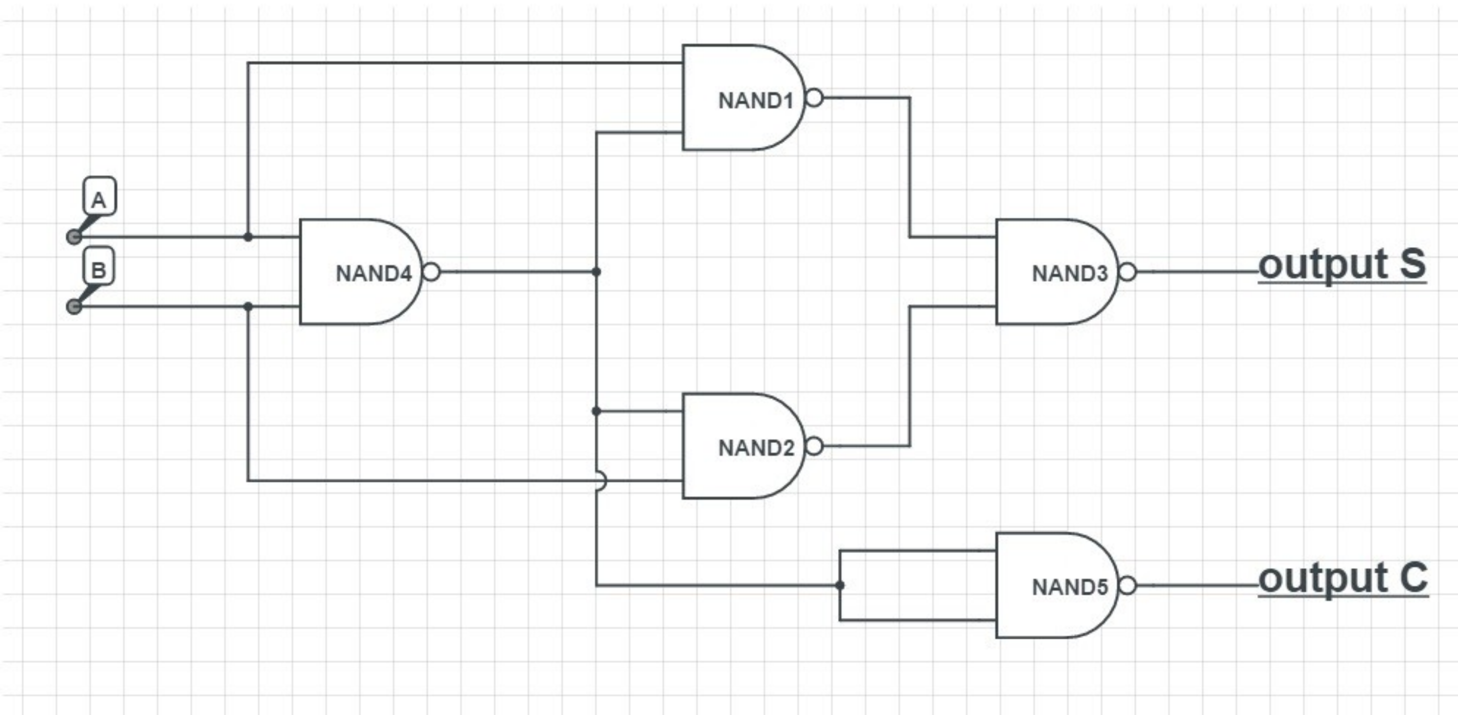


Binary adder
"half adder"

Programming = combining logic circuit units
e.g. binary adder for 3 bits:



Universal logic gate set: Fanout and NAND → cheaper construction of logic gates



Requirements on bits for good computer

- Scalable: many bits on one chip
- Reliable initialization
- Logic gates (universal gate set = fanout, NAND)
- Precise readout
- Maintain value (frequent readout-rewrite)

Qubit: has superposition

abstract

$|0\rangle$

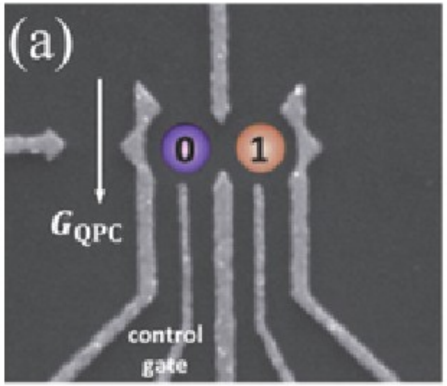
$|1\rangle$

spin

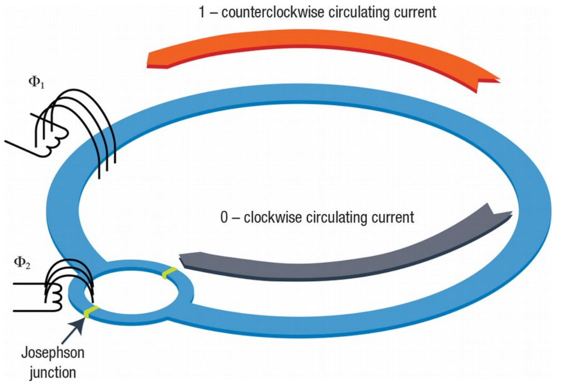
$|\uparrow\rangle$

$|\downarrow\rangle$

charge



superconducting current



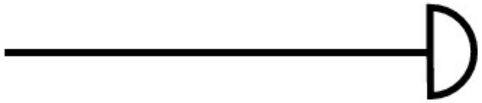
[Mooij, Delft, 2001]

Superposition:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

Measurement produces 1 or 0, probabilistically

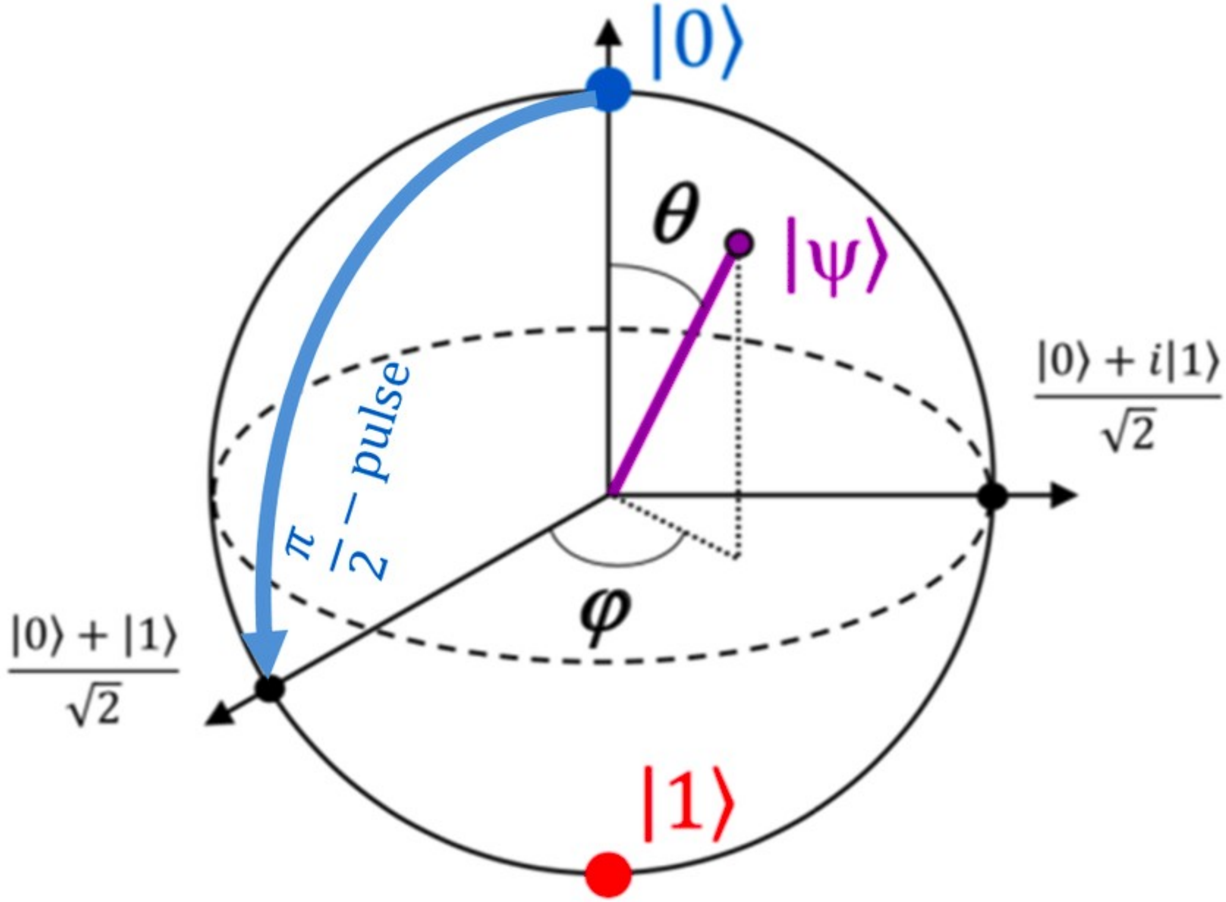
$|\Psi\rangle$



$$|\alpha|^2 \to 0$$

$$|\beta|^2 \to 1$$

States of a qubit = directions a spin-1/2 can point in



$$|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\varphi}sin\frac{\theta}{2}|1\rangle$$

Quantum Logical Circuits: single-qubit gates "rotate" qubit

Defined as classical NOT (bit flip):

$$|0\rangle \text{—}\oplus\text{—} |1\rangle$$

$$|1\rangle \text{—}\oplus\text{—} |0\rangle$$

Action on superposition states:

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

$$|\Psi\rangle \text{—}\oplus\text{—} \beta|0\rangle + \alpha|1\rangle$$

Purely quantum gate, changes phase:

$$|0\rangle \text{—}\boxed{Z}\text{—} |0\rangle$$

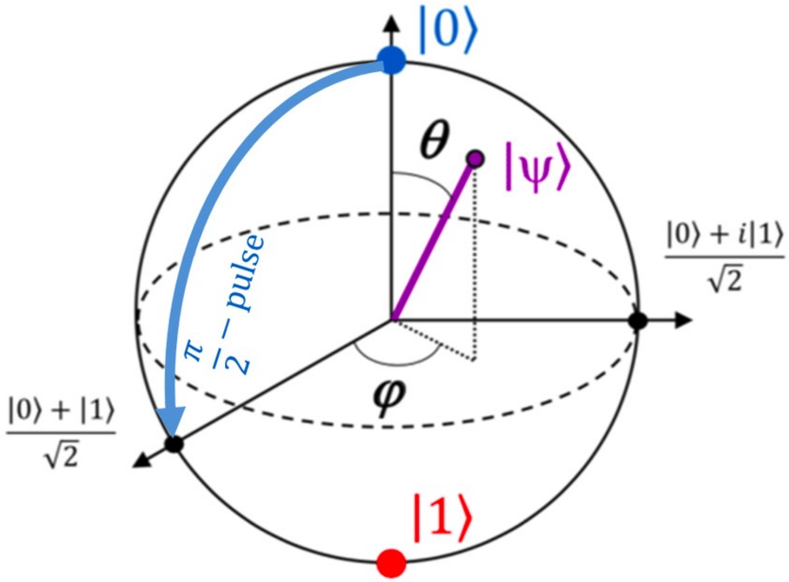
$$|1\rangle \text{—}\boxed{Z}\text{—} -|1\rangle$$

Action on superposition states:

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

$$|\Psi\rangle \text{—}\boxed{Z}\text{—} \alpha|0\rangle - \beta|1\rangle$$

Universal single-qubit gate set: two rotation gates

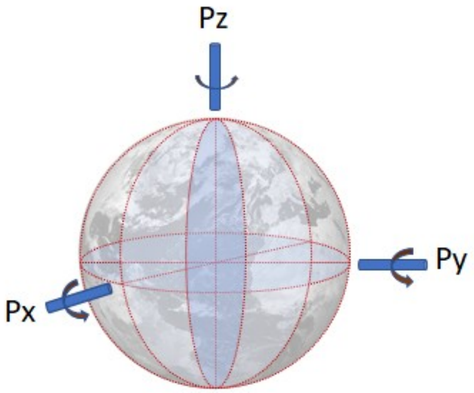


$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

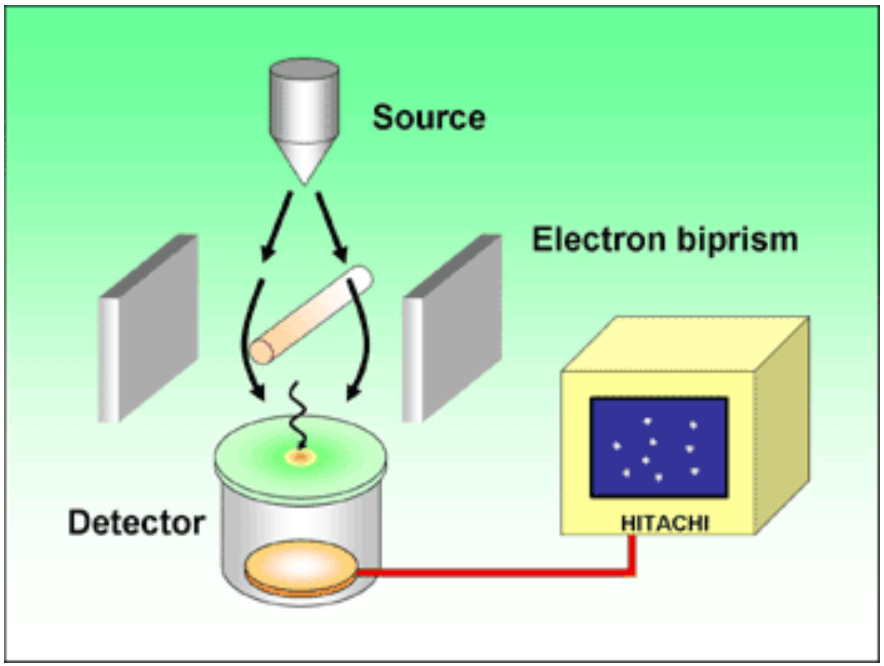
Universal gate set:

Can approximate any rotation by a (polynomially long) sequence of incommensurate rotations
= Solovay-Kitaev theorem

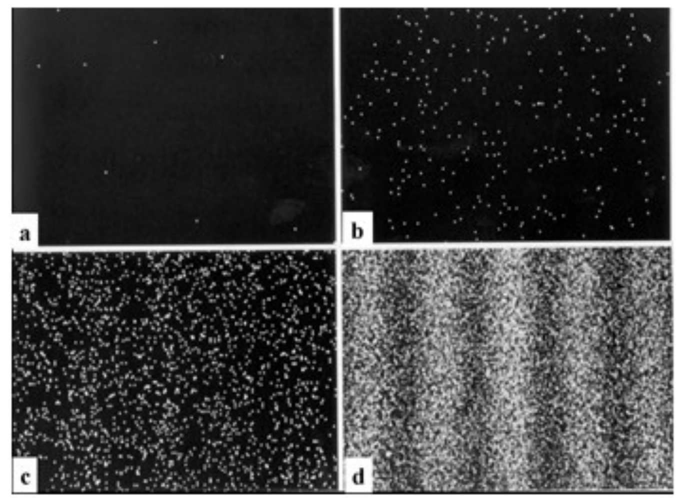
example:
T gate + Hadamard gate



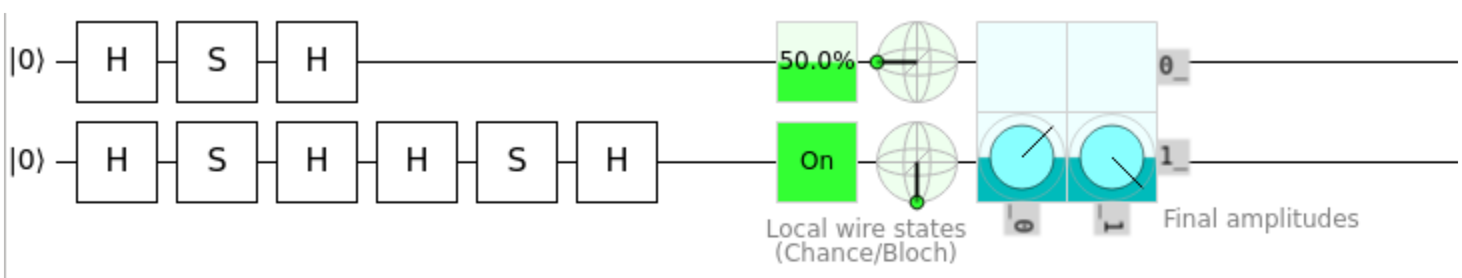
Difference between superposition and statistical mixture testable by interferometry



double slit experiment w electrons, Tonomura, Hitachi, 1989



2 subsequent 90 rotations = 180 rotation
https://algassert.com/quirk

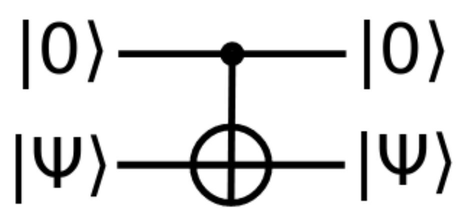


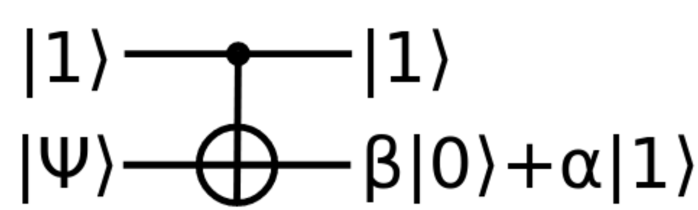
Nice online tool for playing with quantum logic circuits: Quirk

https://algassert.com/quirk

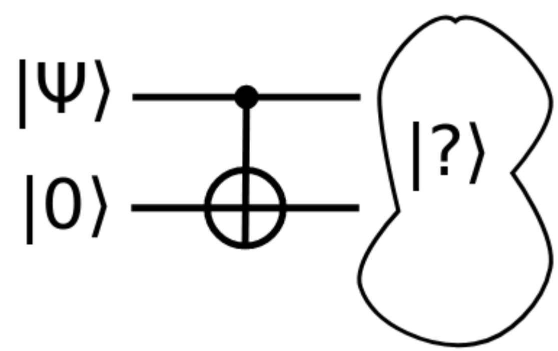
Two-qubit CNOT (controlled-NOT) gate copies classical information

Defined for simple values of control bit,
arbitrary target bit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$



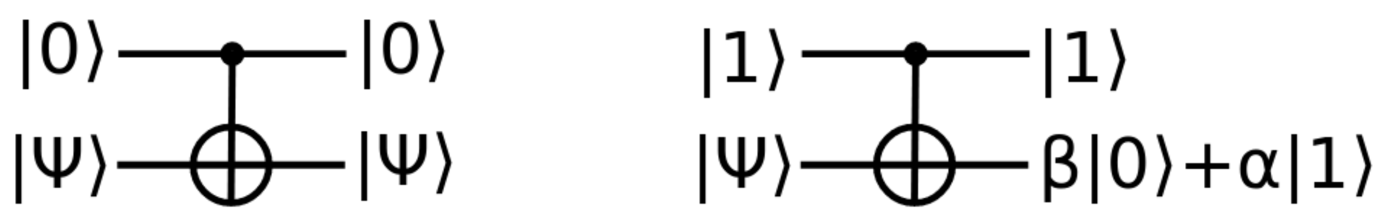


Is it a quantum copier?

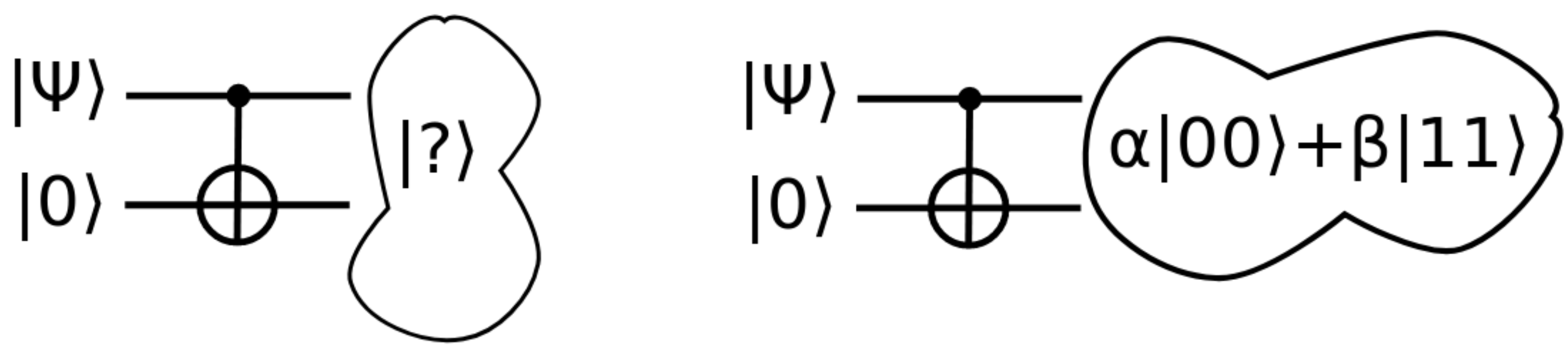


Two-qubit CNOT (controlled-NOT) gate copies classical information, entangles quantum bits

Defined for simple values of control bit, arbitrary target bit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$



Is it a quantum copier? No, it is a quantum entangler



Entanglement gives quantum computers their advantage

Entanglement → exponentially growing Hilbert-space
n qubits: 2^n amplitudes

Quantum computing:

1. - start with simple product state
2. - Run computation in large Hilbert space
3. - Finish with almost product state
4. - Measure → project probabilistically to a product state

Entanglement alone not enough, e.g., Clifford gates efficiently simulatable in Heisenberg picture (CNOT included, T not)

Technical requirements for qubits: Di Vincenzo criteria (2000)

- Scalable: many bits on one chip
- Reliable initialization
- Logic gates (universal gate set ~~fanout, NAND~~
  → e.g. T, H, CNOT)
- Precise readout
- Maintain value? (~~frequent readout-rewrite~~
  → Quantum Error Correction)

1. A scalable physical system with well characterized qubit
2. The ability to initialize the state of the qubits to a simple fiducial state
3. Long relevant decoherence times
4. A "universal" set of quantum gates
5. A qubit-specific measurement capability

Di Vincenzo criteria fulfilled by superconducting qubits

QC Approach	#1	#2	#3	#4	#5
NMR	🔴	🟡	🟡	🟢	🟡
Trapped Ion	🟡	🟢	🟢	🟢	🟢
Neutral Atom	🟡	🟢	🟢	🟢	🟢
Cavity QED	🟡	🟢	🟢	🟡	🟢
Photonic	🟡	🟢	🟢	🟢	🟢
Solid State	🟡	🟢	🟢	🟢	🟢
Superconducting	🟢	🟢	🟢	🟢	🟢

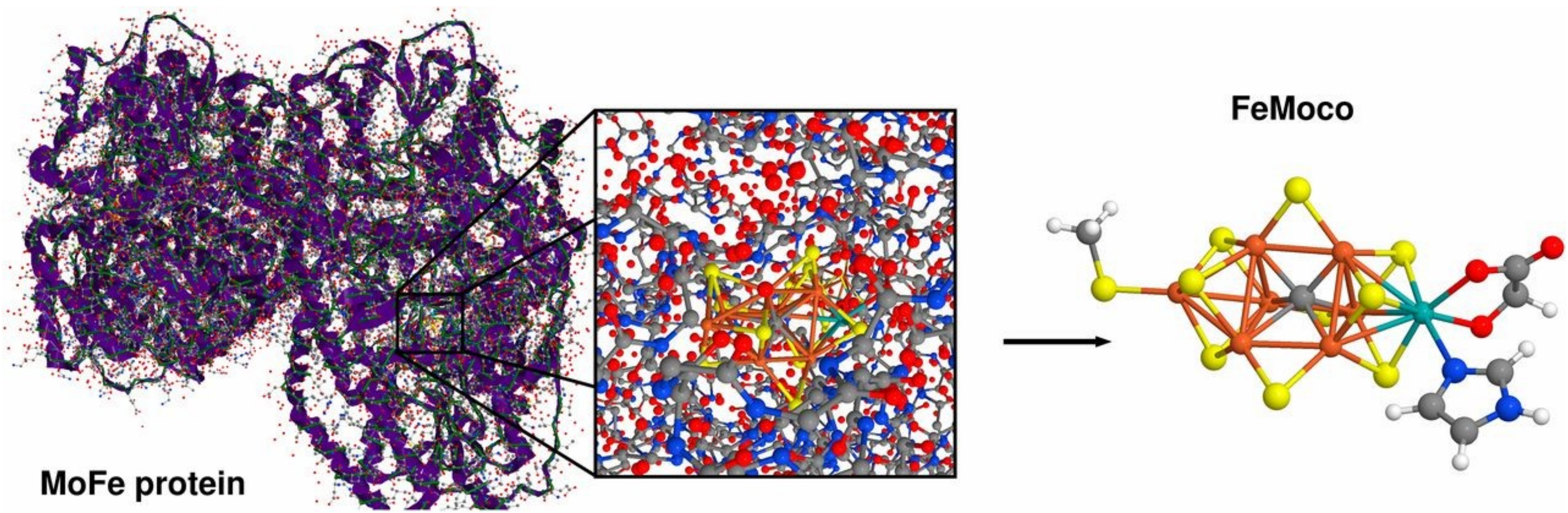
🟢 = a potentially viable approach has achieved sufficient proof of principle

🟡 = a potentially viable approach has been proposed, but there has not been sufficient proof of principle

🔴 = no viable approach is known

1. A scalable physical system with well characterized qubit
2. The ability to initialize the state of the qubits to a simple fiducial state
3. Long relevant decoherence times
4. A "universal" set of quantum gates
5. A qubit-specific measurement capability

Quantum Computers good for some problems.
List is growing slowly



- Break RSA using Shor algorithm
- Quantum chemistry for better fertilizer
- ....
- ?

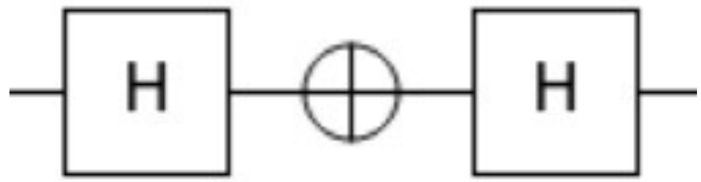
needs 10 million qubits

Comprehensive list (62 algorithms):
https://quantumalgorithmzoo.org/

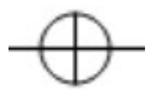
IBM quantum computers available online, after free registration

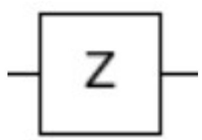
https://quantum-computing.ibm.com/

Control question: Simplify the following quantum logic circuit!



= ?

A)  Pauli X

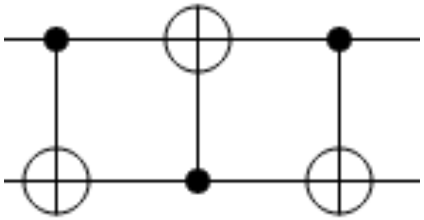
B) 

Pauli Z

C) nothing

D) none of the above

Control question: What does this quantum logic circuit do?



A) swaps states of the two qubits

B) flips the second qubit only if the first is 0

C) complicated way to “do nothing”

D) Hadamard operation on both qubits