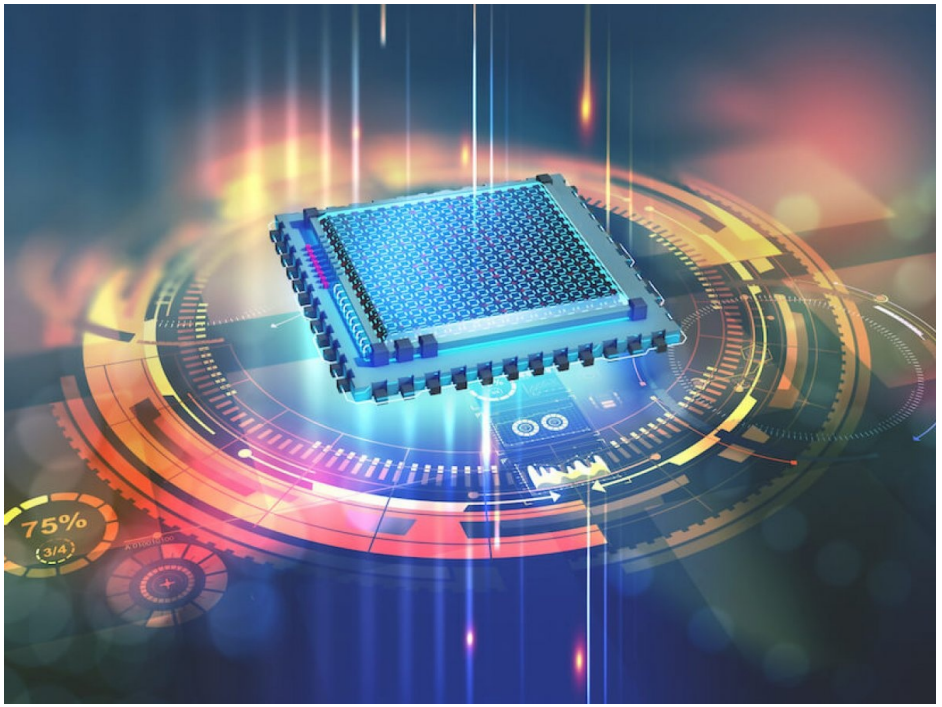
Classical VS quantum



Last class

- We can implement any unitary matrix with a small set of gates
- E.g., {H,T,CNOT}

Today

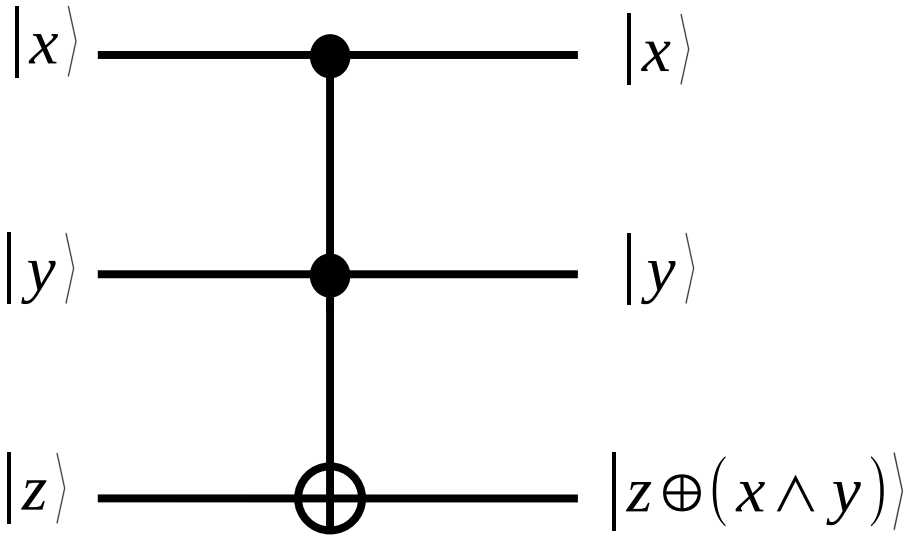
- Can we implement any Boolean function?
- Can we compute functions not classically computable?

Implement Boolean functions

- We know that NAND gate is (classically) universal
- If we could obtain NAND with quantum gate then we could implement any Boolean function
- However, NAND is not reversible

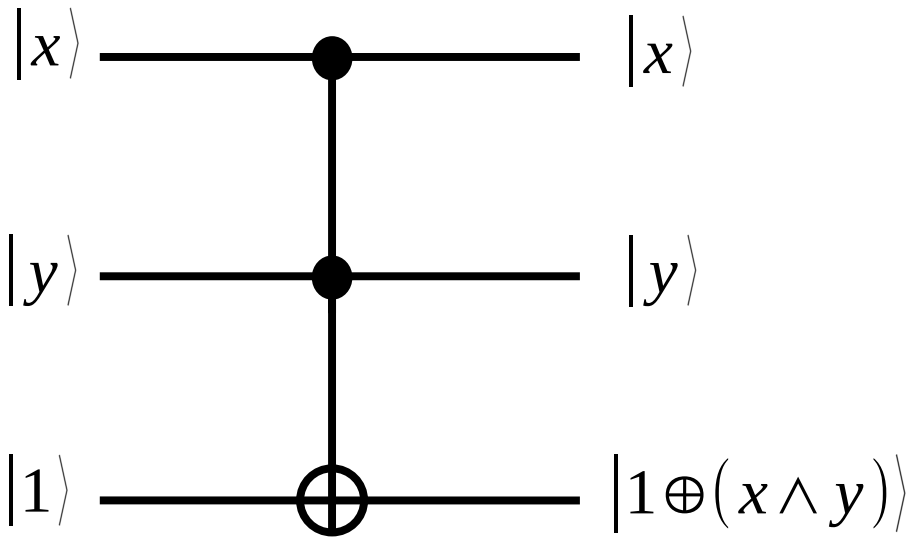
Toffoli gate

- Also known as controlled-controlled NOT
- 3-qubit gate, negates the third qubit iff the first two are both 1
- That is, if their AND is 1



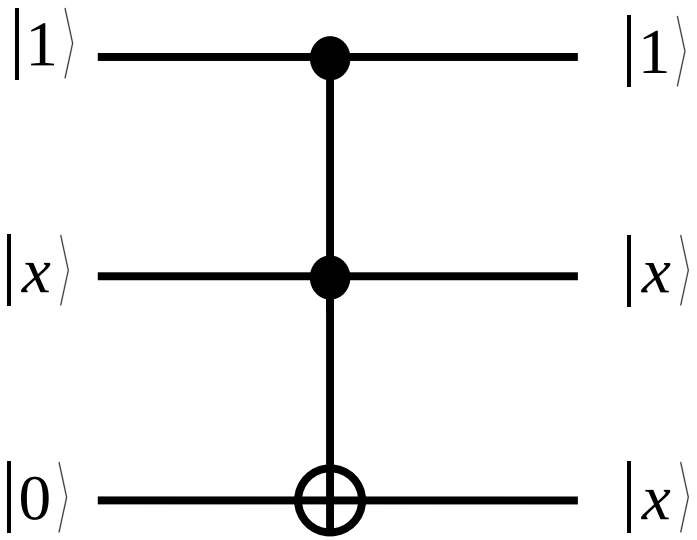
From Toffoli to NAND

- Toffoli can implement NAND
- We need an ancilla bit



From Toffoli to fanout

- In classical computing we can also duplicate bits
- We can do this as well with Toffoli
- Not in contrast with the no-cloning theorem since we are only duplicating classical bits



From Toffoli to classical

- Toffoli can implement both NAND and fanout
- Hence Toffoli can implement any Boolean function
- We need many ancilla bits

Would CNOT be enough?

- CNOT is not enough
- Given a CNOT circuits, all outputs can be expressed as XOR of inputs
- Select an input: the set of outputs which include the selected input in their expression flip, the others stay the same
- The set of outputs that flip does not depend on the actual values of other inputs
- Toffoli has a different behavior: the output flips by flipping the first bit only if the second is 1

Probabilistic computing

- Quantum provides perfect probabilistic choices
- Put a state in a superposition and measure it
- Hence quantum can simulate any algorithm doable with classical computing + probabilities

Exercise

- Construct a quantum circuit to add two two-bit numbers x and y modulo 4. That is, the circuit should perform the transformation $|x, y\rangle \rightarrow |x, x + y \bmod 4\rangle$.

Simulating quantum circuits

- We can always simulate quantum circuits using classical gates up to an arbitrary small approximation
- Basic idea: store all the coefficients in the vector representing the state, and mimic what unitaries do
- Note: for n qubits, we have 2^n coefficients, hence we have in the worst case an exponential slowdown

Consequences

- Quantum circuits cannot compute non-classically computable functions (e.g., termination)
- Quantum computing can provide at most an exponential speed-up
- There is no exponential speed-up without entanglement
  - If I have no entanglement I can decompose the state in a tensor product, which can be represented using 2n coefficients