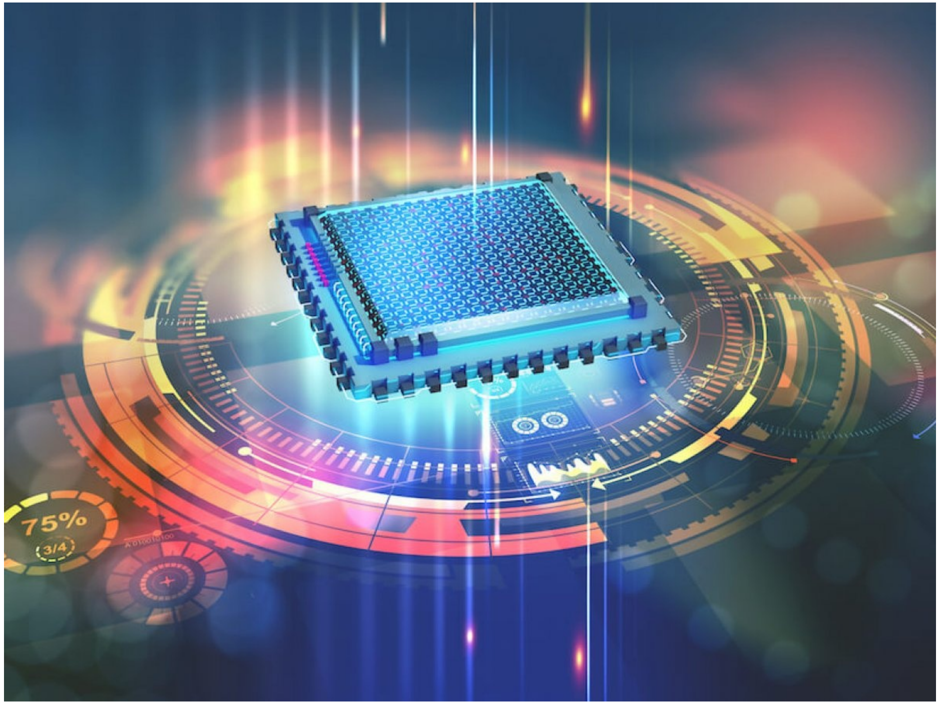
The General Computational Process



A joke before we start

Last class

- Gates and measurements on multiple qubit systems
- Examples of one and two qubit gates and what they can do
- State preparation

Today

- Superposition
- Quantum parallelism
- No cloning

Tensor test

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- What is the dimension of the matrix $CNOT \otimes H$?

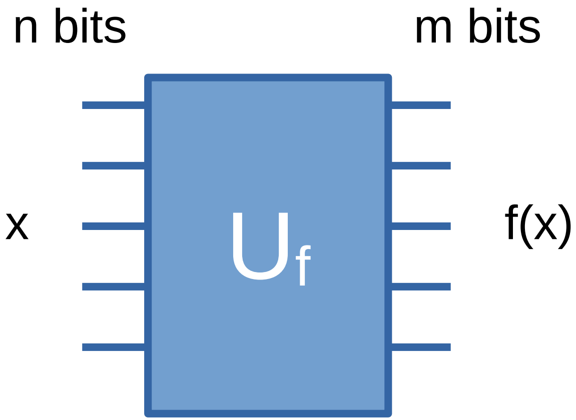
Classical computing

- Computers act on number x to produce another number f(x)
- Treat these numbers as non-negative integers less than 2^k for some k
- Each integer is represented in the computer as a k bit-string

Quantum computing

- Quantum computer acts on number x to produce another number f(x)
- Treat these numbers as non-negative integers less than 2^k for some k
- Each integer is represented in the quantum computer with the corresponding computational-basis state of k qubits

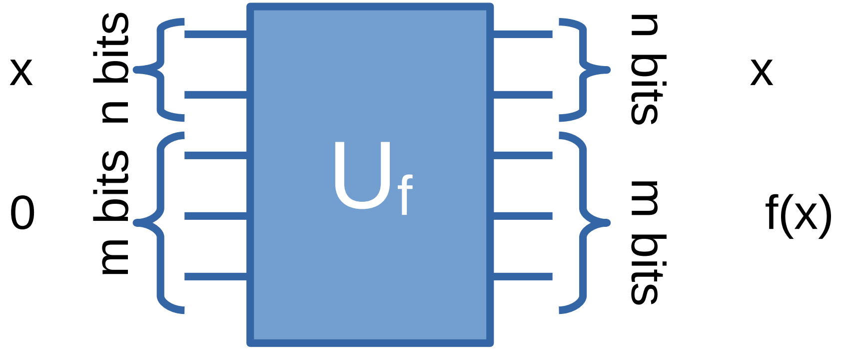
General quantum computation



Is this reversible?

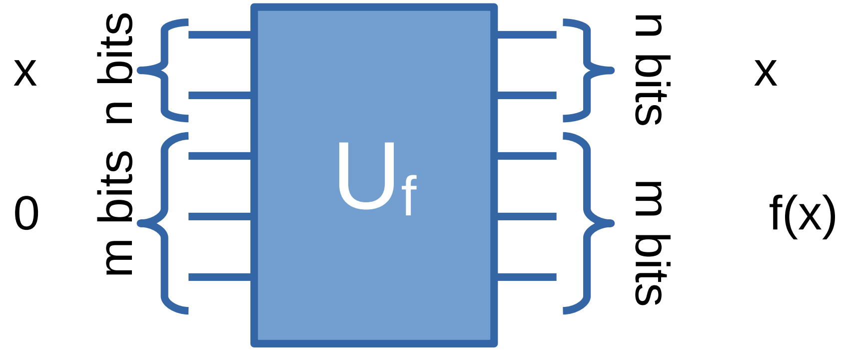
General quantum computation

- To ensure reversibility we split input and output register



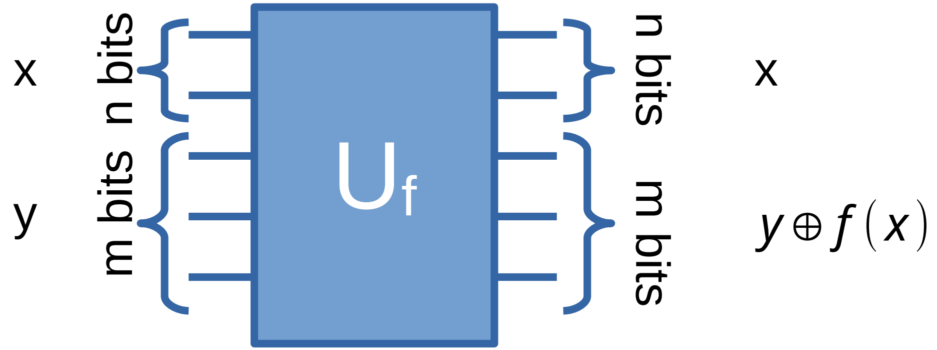
- This is standard even if qubits are scarce

General quantum computation



- We define the transformation U_f as a reversible transformation (unitary), we give its values for computational basis states, and extend by linearity

General quantum computation



$$U_f |x\rangle_n \otimes |0\rangle_m = |x\rangle_n |y \oplus f(x)\rangle_m$$

- If the output register is not 0 initially
- This is reversible, actually self-inverse
- XOR is bitwise
- The input register keeps its value

XOR test

- If x and y are arbitrary n-bit strings, what is $x \oplus x \oplus y \oplus y$?

A very important trick

- Using two Hadamards we can get an uniform superposition on two qubits

$$H \otimes H|0\rangle \otimes |0\rangle = (H|0\rangle) \otimes (H|0\rangle) =$$

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

$$= \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

The trick, generalized

- We can generalize it to n Hadamards

$$H^{\otimes n}|0\rangle^n = \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} |x\rangle_n$$

$$\text{where}\, H^{\otimes n} = H \otimes H \otimes \ldots \otimes H\,,\, n\,\text{times}$$

Computing on superpositions

- If we apply U_f to that superposition, with 0 in the output register, we get by linearity:

$$U_f\left(H^{\otimes n}\otimes 1_m\right)|0\rangle_n|0\rangle_m=\frac{1}{2^{n/2}}\sum_{0\leq x<2^n}U_f\left(|x\rangle_n|0\rangle_m\right)=$$

$$=\frac{1}{2^{n/2}}\sum_{0<x\leq 2^n}|x\rangle_n|f(x)\rangle_m$$

Quantum parallelism

- Is this a miracle?
- We get all possible evaluations of f
- For just 100 qubits, there are 2^{100} evaluations
- This magic is called Quantum Parallelism

Quantum parallelism, but…

- Is this a miracle? Well…
- We cannot say that the result of the computation is all 2^n evaluations of f
- No way to find out what the state is unless we measure
- In which case the state collapses in one value!!

Quantum parallelism, actually

- When we measure the input register, with equal probability, we get any of the values of x
- When we measure the output register, we get the value f(x) for that x
- So the result is learning a single random x_0 as well as the value of f in x_0
- State collapses to $\left|x_0\right\rangle\left|f\left(x_0\right)\right\rangle$
- Nothing more we could learn, could have done this with a classical computer, choosing a random value of x and evaluating f

Quantum “weirdness”

- Quantum “weirdness”: the selection of the random x for which f(x) was learned is only made after (!!) the computation has been carried out
- Quite possibly long after
- No practical difference though

No cloning

- If we could copy the output register, then we could learn values of f(x) for many random values of x with one computation
- No cloning for quantum!
- Not even approximate cloning

No Cloning Theorem

- "There is no unitary transformation U that takes the state $|y\rangle_n|0\rangle_n$ into $|y\rangle_n|y\rangle_n$ for arbitrary y"
- Proof is immediate consequence of linearity

Linearity test

- If $|y\rangle$ and $|x\rangle$ are qubits and U is a unitary such that:

  $U|y\rangle|0\rangle = |y\rangle|y\rangle$ and $U|x\rangle|0\rangle = |x\rangle|x\rangle$

  what is $U((a|y\rangle + b|x\rangle)|0\rangle)$?

No Cloning Theorem

- “There is no unitary transformation U that takes the state $|y\rangle_n|0\rangle_n$ into $|y\rangle_n|y\rangle_n$ for arbitrary y”

- It follows from linearity that:
$$U((a|y\rangle+b|x\rangle)|0\rangle)=$$
$$=aU(|y\rangle|0\rangle)+bU(|x\rangle|0\rangle)=a|y\rangle|y\rangle+b|x\rangle|x\rangle$$
- But since U clones arbitrary inputs we have:
$$U((a|y\rangle+b|x\rangle)|0\rangle)=$$
$$=(a|y\rangle+b|x\rangle)(a|y\rangle+b|x\rangle)=$$
$$=a^2|y\rangle|y\rangle+b^2|x\rangle|x\rangle+ab|y\rangle|x\rangle+ab|x\rangle|y\rangle$$

No Cloning Theorem

- “There is no unitary transformation U that takes the state $|y\rangle_n |0\rangle_n$ into $|y\rangle_n |y\rangle_n$ for arbitrary y”
- Cloning compatible with linearity only if

$$ab|y\rangle|x\rangle + ab|x\rangle|y\rangle = 0$$

- Only possible if one of a and b are 0

No Approximate Cloning Th.

- The ability to clone to a reasonable degree of approximation would also be useful
- But this is impossible as well
- Suppose U approximately clones:

$$U|y\rangle|0\rangle \sim |y\rangle|y\rangle \text{ and } U|x\rangle|0\rangle \sim |x\rangle|x\rangle$$

Properties of inner products

- Inner products of tensors is ordinary product of inner products:

$$\langle \psi_1 \otimes \psi_2 | \phi_1 \otimes \phi_2 \rangle = \langle \psi_1 | \phi_1 \rangle \langle \psi_2 | \phi_2 \rangle$$

- Unitaries preserve inner product:

$$\langle \psi | \phi \rangle = \langle U \psi | U \phi \rangle$$

- Inner product of unitary vectors with themselves is 1

$$\langle \psi | \psi \rangle = 1$$

No Approximate Cloning Th.

- Suppose U approximately clones:

  $U|y\rangle|0\rangle \sim |y\rangle|y\rangle$ and $U|x\rangle|0\rangle \sim |x\rangle|x\rangle$

- Given that U preserves inner products:

$$\langle y\,0|x\,0\rangle \sim \langle y\,y|x\,x\rangle$$
$$\langle y|x\rangle\langle 0|0\rangle \sim \langle y|x\rangle\langle y|x\rangle$$
$$\langle y|x\rangle \sim \langle y|x\rangle^2$$

- True only if inner product close to 0 (orthogonal) or to 1 (equal)

Is this it for quantum?

- We can be more clever, apply more unitaries to the qubits before or after applying U_f
- We can learn something about the relations between different values of f(x)
- We however lose the information of f(x)
- This tradeoff of information is typical of physics: Heisenberg Uncertainty principle.

Is this it for quantum?

- Reversible Computation of functions
- Uniform superposition of everything
- How much information is in a quantum state?
- No cloning
- Heisenberg Uncertainty principle