The General Computational Process

PHYS/CSCI 3090

Prof. Alexandra Kolla

Alexandra.Kolla@Colorado.edu
ECES 122

Prof. Graeme Smith

Graeme.Smith@Colorado.edu
JILA S326

https://home.cs.colorado.edu/~alko5368/indexCSCI3090.html

Today


HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.
Dilbert.com DilbertCartoonist@gmail.com
4-17-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick

Homework

- HW 1 is out, due next Monday at noon.
- HW 0 solutions are posted

Come see us!

- Alexandra Kolla/ Graeme Smith: Friday 3:00-4:00 pm, JILA X317.
- Ariel Shlosberg: Tu/Th 2:00-4:00pm, DUANG2B90 (physics help room)
- Steven Kordonowy: Th 11am-12pm, ECAE 124.

Last Class

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

Today

- More on tensor Products
- More on unitary evolution
- Superposition
- No cloning

Tensor Test

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

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

A) 6x6

B)8x8

C)4x4

D)16x16

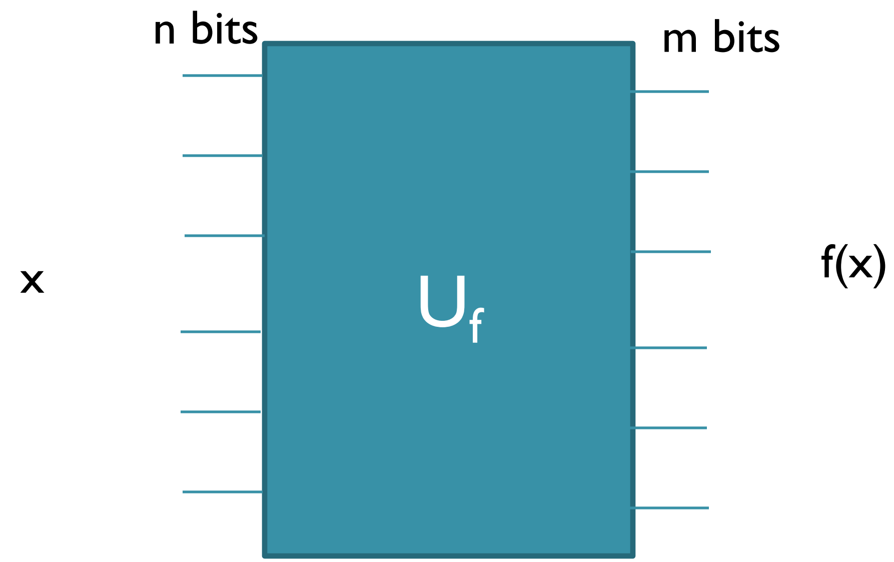
Today

- 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.

Today

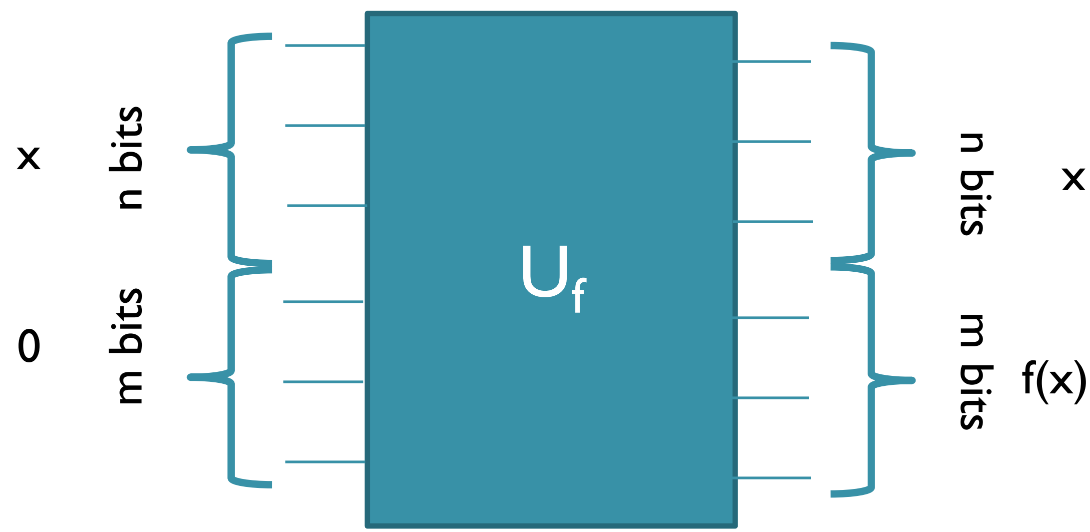
- Quantum computer acts on number x to produce another number f(x).
- Treat these numbers as non-negative integers less than 2^k for some k.
- Each integer is represented in the quantum computer with the corresponding computational-basis state of k Qubits.

The general quantum computational process



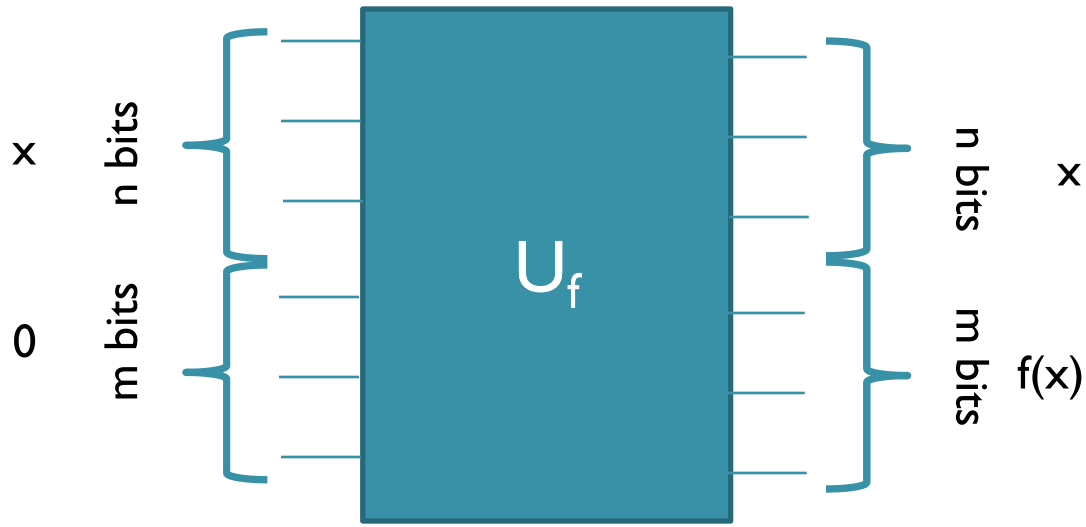
Is this reversible?

The general quantum computational process



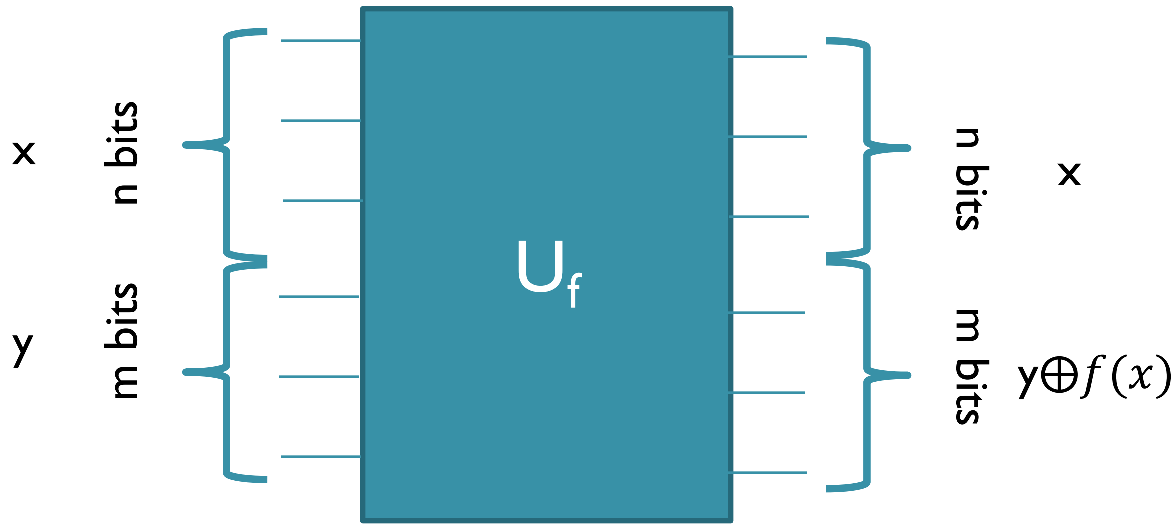
Even though qubits are scarce resource, having separate registers for input and output is standard practice in reversible computation.

The general quantum computational process

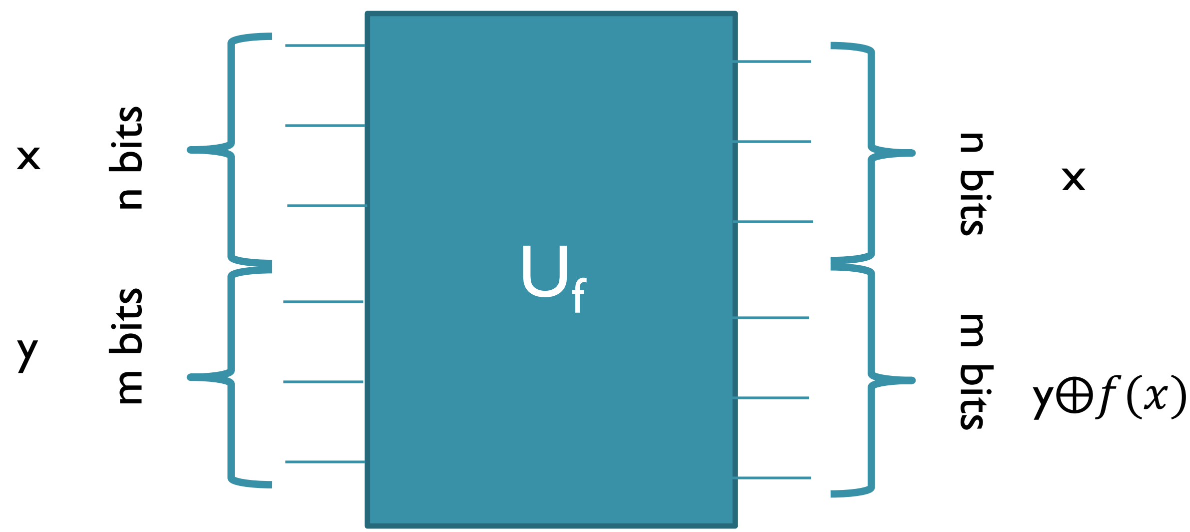


We define the transformation U_f as a reversible transformation (unitary), taking computational basis states into computational basis states, and extend by linearity.

The general quantum computational process



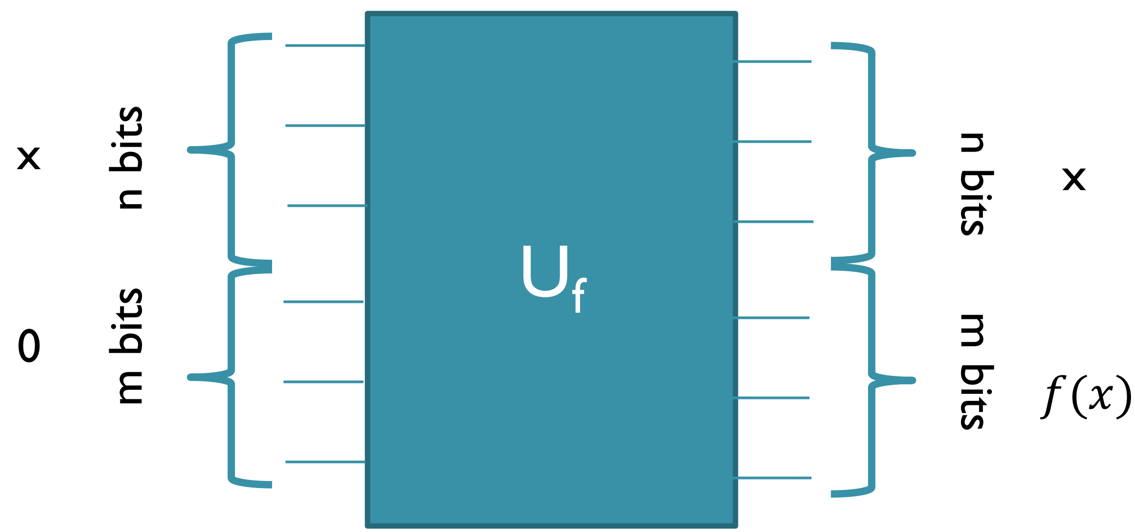
The general quantum computational process



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

e.g: $1101 \oplus 0111 = 1010$, bitwise XOR

The general quantum computational process



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

Regardless of initial value of y, the input register remains in its initial state $|x\rangle$

XOR test

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

A) The n bit string x

B) The n bit string y

C) The n bit string $x \oplus y$

D) the n bit string with all 0

The general quantum computational process

U_f is invertible, in fact it is its own inverse!

$$\mathrm{U_f U_f}|x\rangle_n|y\rangle_m = U_f|x\rangle_n|y\oplus f(x)\rangle_m$$
$$= |x\rangle_n|y\oplus f(x)\oplus f(x)\rangle_m = |x\rangle_n|y\rangle_m$$

This inspires the most important trick of quantum computation: If we apply H to each qubit in the 2-Qubit state $|0\rangle|0\rangle$ we get a uniform superposition of everything!

The general quantum computational process

$$H \otimes H|0\rangle \otimes |0\rangle = (H|0\rangle)(H|0\rangle) =$$
$$= \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) =$$
$$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Generalizes to n-fold tensor product of n Hadamards

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

- $H^{\otimes n}$=H ⊗H… ⊗H, n times

The general quantum computational process

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

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

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

Quantum Parallelism

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

Quantum Parallelism

- We cannot say that the result of the calculation 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

- 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 value of f, as well as a signle random x_0, at which f has that value.
- State collapses to $|x_0\rangle|f(x_0)\rangle$
- Nothing more we could learn, could have done this with a classical computer, choosing a random value of x and evaluating f

Quantum Parallelism

- 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!
- No cloning also for approximate state

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

A) $a|y\rangle|0\rangle + b|x\rangle|0\rangle$

B) $a|y\rangle|y\rangle + b|x\rangle|x\rangle$

C) $(a|y\rangle|y\rangle + b|x\rangle|x\rangle)|0\rangle$

D) $(a|y\rangle + b|x\rangle)(a|y\rangle + b|x\rangle)$

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 $\mathrm{U}\big((\mathrm{a}|y\rangle + b|x\rangle)|0\rangle\big) = \ \mathrm{aU}(|y\rangle|0\rangle) + bU(|x\rangle|0\rangle) = \mathrm{a}|y\rangle|y\rangle + b|x\rangle|x\rangle$

No Cloning Theorem

"There is no unitary transformationU that takes the state $|y\rangle_n|0\rangle_n$ into $|y\rangle_n|y\rangle_n$ for arbitrary y!"

But if U cloned arbitrary inputs,

$\mathrm{U}\big((\mathrm{a}|y\rangle + b|x\rangle)|0\rangle\big) = (\mathrm{a}|y\rangle + b|x\rangle)$

$(\mathrm{a}|y\rangle + b|x\rangle)$= $\mathrm{a}^2|y\rangle|y\rangle + b^2|x\rangle|x\rangle +$

$\mathrm{ab}|y\rangle|x\rangle + ab|x\rangle|y\rangle$

No Cloning Theorem

By linearity:

$$\begin{aligned} &\mathrm{U}\big((\mathrm{a}|y\rangle + b|x\rangle)|0\rangle\big) \\ &= \mathrm{aU}(|y\rangle|0\rangle) + bU(|x\rangle|0\rangle) \\ &= \mathrm{a}|y\rangle|y\rangle + b|x\rangle|x\rangle \end{aligned}$$

If U cloned arbitrary inputs:

$$\mathrm{U}\big((\mathrm{a}|y\rangle + b|x\rangle)|0\rangle\big) = (\mathrm{a}|y\rangle + b|x\rangle)$$

$$(\mathrm{a}|y\rangle + b|x\rangle) =$$

$$\mathrm{a}^2|y\rangle|y\rangle + b^2|x\rangle|x\rangle + \mathrm{ab}|y\rangle|x\rangle + ab|x\rangle|y\rangle$$

Only possible if one of a, b is zero!

Meaning I can only copy classical bits (duh!)

No Approximate Cloning Theorem

The ability to clone to a reasonable degree of approximation would also be useful. But this is also impossible.

Suppose U approximately cloned $|y\rangle, |x\rangle$

$$\mathrm{U}(|y\rangle|0\rangle) \sim |y\rangle|y\rangle, \mathrm{U}(|x\rangle|0\rangle \sim |x\rangle|x\rangle$$

Inner Product test

Assume $|y\rangle$, $|x\rangle$, $|w\rangle$, $|k\rangle$ are arbitrary vectors.
What is the inner product $(|y\rangle \otimes |w\rangle, |x\rangle \otimes |k\rangle)$?

A) 0

B) $\langle x|y\rangle \cdot \langle w|k\rangle$

C) $\langle x|k\rangle \cdot \langle y|w\rangle$

D) $\langle x|w\rangle \cdot \langle y|k\rangle$

No Approximate Cloning Theorem

The ability to clone to a reasonable degree of approximation would also be useful. But this is also impossible.

Suppose U approximately cloned $|y\rangle$, $|x\rangle$

$$\mathrm{U}(|y\rangle|0\rangle) \sim |y\rangle|y\rangle, \mathrm{U}(|x\rangle|0\rangle \sim |x\rangle|x\rangle$$

Since U preserves inner products, and $\langle 0|0\rangle = 1$, we would have $\langle x|y\rangle \sim \langle x|y\rangle^2$.

This requires $\langle x|y\rangle$ to be either close to 1 or 0. So this can work only if the two states are very close together or very close to orthogonal.

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 lose the information of f(x)
- This tradeoff of information is typical of physics: Uncertainty principle.

Summary:

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

Reading

- We have finished Chapter 2.1
- Please read 2.2-2.4 for Friday