CSE 468T Intro Quantum computing

Who am I

How did I get to this
- Walter Burke
- Nathan Mester
- Collin Szczepanski
- Arthur Rattew
- Finn Voichick

What will this course be like?
- Study group
- Must show up
- Must participate
- Hopefully you TA

Why are we doing this?
- Interesting → mind blowing
- Future of QC ← many places teach now
- NSF QCFF program
- Put you in reach of other dept courses

QC = Physics + Math + CS

Physics - studies the observable universe
Math - logic & reasoning
CS - apply computation to solve problems

Many sources for this course
Texts
Videos
Lecture Notes

Challenge – teach this to CS
as effectively as possible

Teach you what I've learned
+ what I don't yet know

For this to work
Any question is OK – strangeness ahead
It's not OK to not understand
Need your help to make this
work on larger scale
Agree I'm gone Oct 31 – Nov 13

Prereq

Linear algebra	Math 309	Lots
Prob/stat	ESE 326	Some
Circuits	CSE 260M	Little

We cover
Physics so you believe QC effects
Math quantum ops are matrices
CS to solve interesting problems

Leveraging physical phenomena for computation

* Fluid computer square roots
* Can you use gravity to compute square roots?

$$d = \frac{1}{2} a t^2$$

$$t = \sqrt{\frac{2d}{a}}$$

To compute $\sqrt{n}$
drop a ball from height

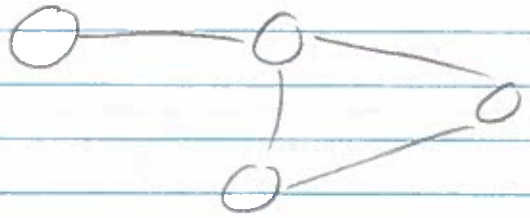
$$d = \frac{a n}{2}$$

and count the seconds until it hits the ground

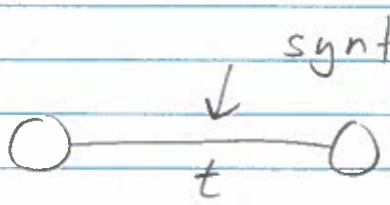
$a = 9.8\ m/s^2$
$n = 81$

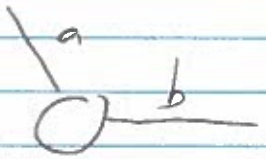
$d = 396.9$ meters

DNA computer

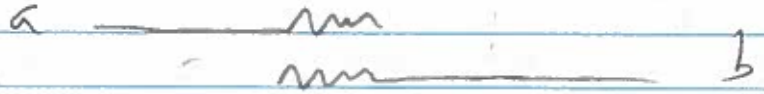


TSP visit nodes in a tour spending the least time

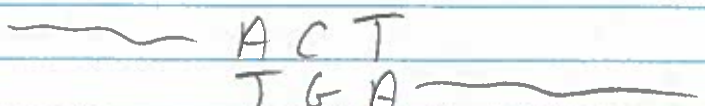




If two edges are incident on a node

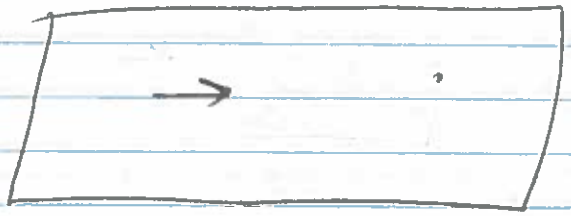


Allow ligation using unique ends



[lots more details]

Sort on a gel



fastest fragment is shortest

Wikipedia has a blurb about this

Review of classical gates 0 ≡ false 1 ≡ true

Boolean functions of 2 inputs a, b

a	b	a ? b
0	0	0 or 1
0	1	0 or 1
1	0	⋮
1	1	

} 16 possible functions

Define and ∧

a	b	a ∧ b ≡ ab
0	0	0
0	1	0
1	0	0
1	1	1

or ∨

a	b	a ∨ b ≡ a + b
0	0	0
0	1	1
1	0	1
1	1	1

Defin $\bar{a}$

a	$\bar{a}$
0	1
1	0

Universality

Take any function

a	b	a ? b
0	0	r_{00}
0	1	r_{01}
1	0	r_{10}
1	1	r_{11}

$$\bar{a}\,\bar{b}\,r_{00} + \bar{a}b\,r_{01} + a\bar{b}\,r_{10} + ab\,r_{11}$$

yields the above table

So $\neg$ $\wedge$ $\vee$ are universal:
Any of the 16 possible functions can be written in terms of those 3 operators

$$\text{NAND} = \overline{ab}$$

$$\bar{a} = \overline{a1}$$

$$a \wedge b = \overline{\overline{ab}}$$

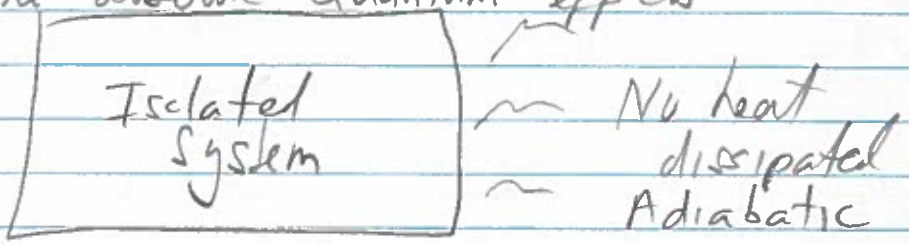
$$a \vee b = \overline{\bar{a}\bar{b}}$$

} NAND is universal

* What about NOR?
* What about AND?

Why reversible circuits?

Quantum systems are ideally isolated (closed) & do not interact with their environment or surroundings. This is needed to observe Quantum effects



the work taking place in the isolated system should not dissipate heat

2 units of energy IN, 1 out

The energy must go somewhere

HEAT!

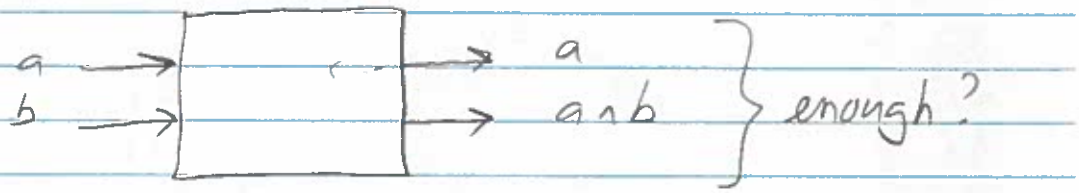
See the billiard-ball computer [1982]
It takes energy to stop the ball going downwards

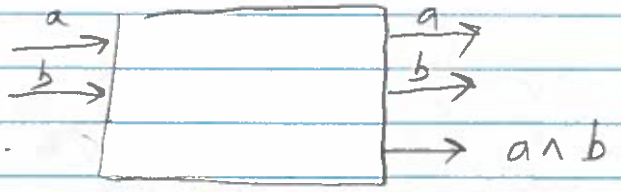
Reversible gates (p12 text)

Reversible: can uniquely recover inputs from outputs

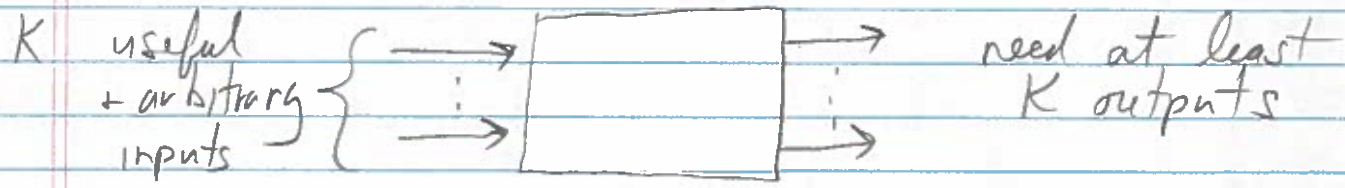
$\bar{a}$ is reversible

$a \wedge b$ is not reversible





We can construct $a \wedge b$ in reverse



But the above AND in reverse is

The reverse computation must also use its inputs & create the same number of outputs or the reverse computation dissipates heat

In theory, a reversible circuit need not dissipate any energy

p 12 Text Kaye

$c = 0 \rightarrow$ we get $a \wedge b$
$c = 1 \rightarrow$ we get $\overline{a \wedge b}$

* Work out the reversal part

If I know $a \wedge b$ the third output is either that (so $c=0$) or NOT that (so $c=1$)

Also called the Toffoli gate

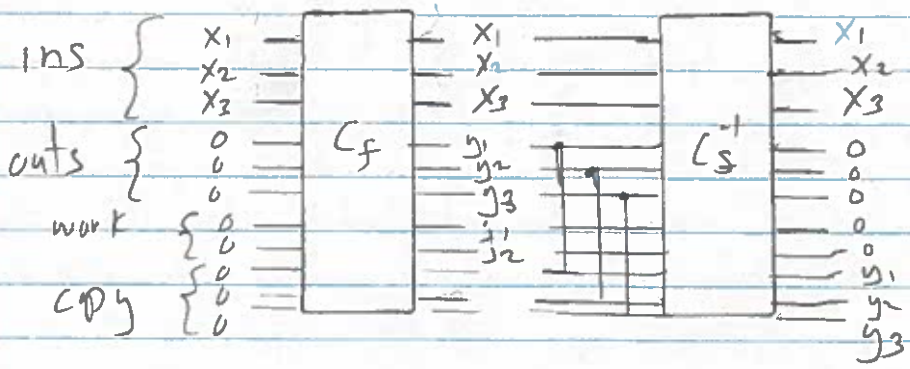
More on reversible computations

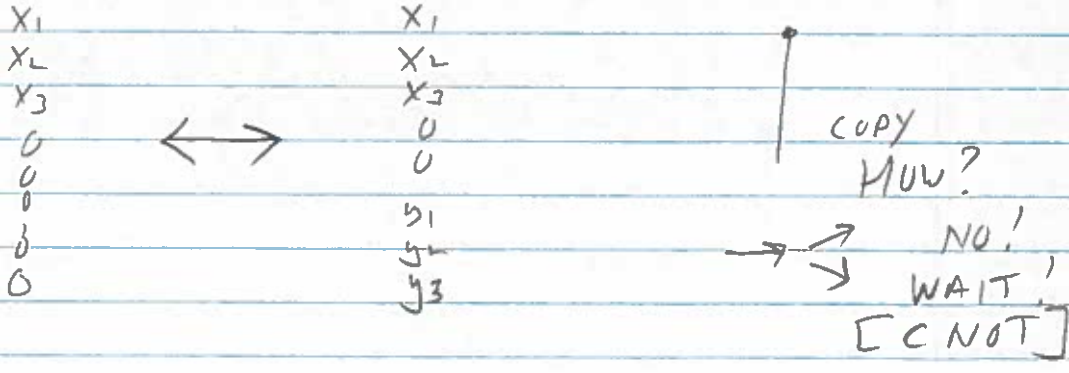
In theory, reversible

But if we build an adder using standard 2-in 1-out gates, NOT reversible

p. 14 Kaye text

Any function $f(x)$ can be computed reversibly, even if f is not itself invertible





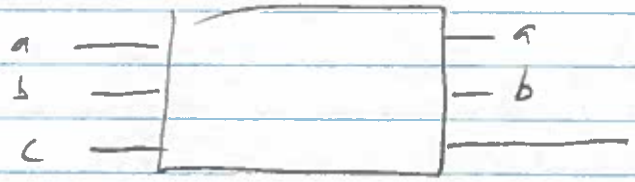
Mathematically, we need the gate to realize a bijection to be reversible

a	b	c
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

a	b	$c \oplus (a \wedge b)$
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	1
1	1	0

We go for think of c as controlling whether we compute $a \wedge b$ vs. $\overline{a \wedge b}$, AND vs. NAND

But another view is this



When a & b both true, the third output is the flip of c

Otherwise c passes through

Toffoli gate, a/k/a CCNOT controlled controlled NOT

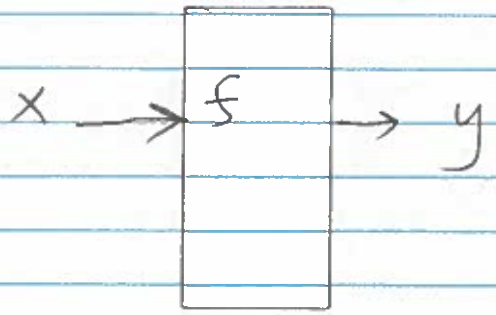
The 2-bit version is CNOT

a	c	a	c⊕a
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

* IMPLEMENT COPY USING CNOT
* EXERCISE USING CNOT + CCNOT

TMs
NP, P, NP-Completeness

Example problems



What value of x produces a given y

This is sometimes easy if we know something about f

$$f(x) = 2x + 5$$

$$f(?) = 105 \qquad x = 50$$

Sometimes, even if we know much about f, this is hard because f may be a one-way function

Easy example: square x and take the middle 3 digits

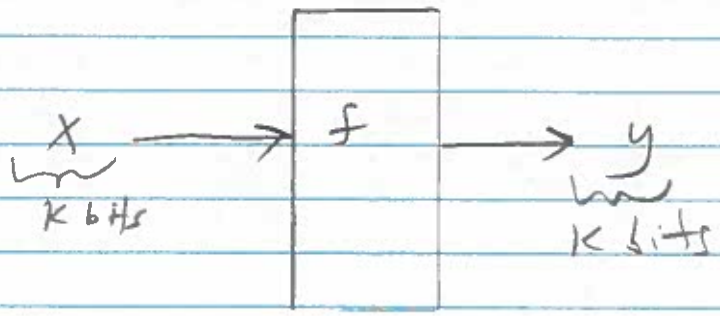
$$468 \times 468 = 0219024$$

$$f(468) = 190$$

but how do you go the other way?

More practical examples are SHA, MD5 – see web page

Formally consider



Let's say x & y are each k bits wide. domain and range are $\{0,1\}^n$

Given some output y, what x causes

$$f(x) = y \quad ?$$

We might have to try all x to find our last probe is the right one $N = 2^n$ be the size of the domain

Classically the best we can do is

$$\Theta(N) \quad \text{time}$$

If we can do parallel processing with p processors, the best is

$$\Theta(N/p)$$

For p constant this doesn't improve the complexity

GROVER'S Quantum Algorithm

$$\Theta(\sqrt{N}) \quad \text{time}$$

So $N = 2^k$ for k-bit SHA

$2^{32} = 4$ billion possibilities

say broken using $2^{16} = 64K$ iterations of Grover

Similarly discrete log

$$y = g^x \bmod p$$

g & c are known, p usually a large prime

Smaller example

$$13 = 3^x \bmod 17$$

$x = 4$ works

Computationally intractable — but GROVER can be applied

Used by Diffie Hellman

Alice Bob

Agree $p = 23$ $g = 5$

Secret a Secret b

→ sends g^a sends g^b ←

computes $(g^b)^a$ computes $(g^a)^b$

→ Shared secret ←

Eve in the middle

Given g^a compute a
Given g^b compute b

Now knows the shared secret!

Because of Grover, key sizes need to double in bits

Companies are moving to systems ~~that~~ QC can't break (yet)
Post-quantum Crypto

Physics
Quantum Mechanics
UV Double Slit part 1
Young's double slit experiment
nature of light

Some background –

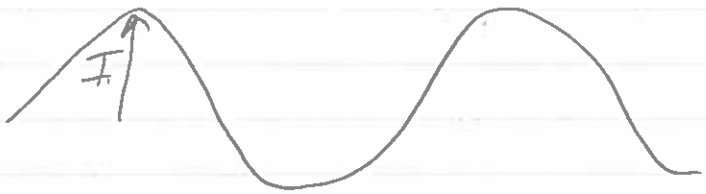
We live in a continuous world
– or do we
We model continuity by
discrete events

A movie may be shot
or rendered 24 fps
We are tricked into seeing
a continuous world

↓ light
▭ → electrons

Like a solar cell

Wave theory



energy is a function of the wave's
amplitude – in fact I^2

Light

Intensity is # of photons
dim to bright

Frequency is the color of the light

Pre Einstein
expect — more photons
brighter light
→ more electrons
ejected

NO

[1 Chan]

[4 V] Capture $P_1(x) + P_2(x)$

Energy of wave is wave^2 Height of Hook: $F = -Kx$

$$\int_0^d Kx\,dx = \frac{Kd^2}{2}$$

Why does the light, when determining if the electron went through slit 1 or 2, destroy the interference pattern?

Prepare a system by observation

* What if we could know, but don't look?

* UV on random use of slot 1 or slot 2

Einstein: God does not play dice with the universe

Bohr: Don't tell God what to do with Gods dice!

Anyone who is not shocked by Quantum theory has not understood a single word

Polarized light

First Rupes
What propagates through a slit?

Now the filters

Quantum games 1-3