18-859BB: Quantum Computation & Quantum Information

- 10^{500} parallel universes
- Rotate, compute, rotate

(two leitmotifs for the course)

David Deutsch, cofounder of quantum computing:

"Quantum computing is... nothing less than a distinctively new way of harnessing nature... it will be the first technology that allows useful tasks to be performed in collaboration between parallel universes."

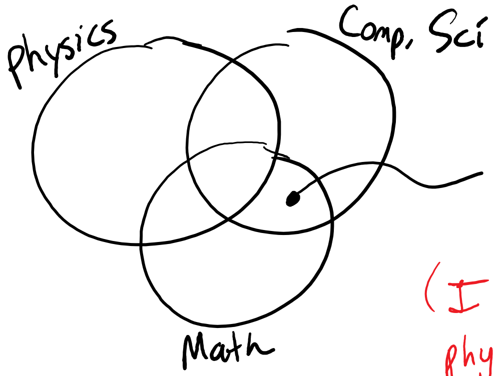
– from book "Fabric of Reality"

(!!! Ain't that great? Who wouldn't want to take a class learning about that? Now, I agree with the first part of the quote – second part is... a bit grand sounding ☺. Brings us to 2nd leitmotif, which we'll discuss in 2nd lecture: how Q.C. is also not so mystical/grand at all – just a small twist ("rotation") on everyday computing.

Dual themes in course:

- Q.C. is otherworldly/extraordinary — lec. 1
- Q.C. is straightforward & easy to learn.) — lec. 2

Q.Comp
&
Q.Info →



me, Ryan O'Donnell
odonnell@cs

(I don't know **anything** about physics. Luckily, don't need to...)

(B/c ~~of~~ my biases, major overarching theme in course will be...)

Computational complexity/efficiency

- Are Q. computers more "powerful" than classical ones? (oft-used word meaning "non-quantum")
- For which computational (/communication/info.) tasks?
- Near-term prospects for demonstrating such? (Already done for some info-theoretic tasks)

(Want to spend a chunk of this lecture talking about computational efficiency, Independent of quantum vs. classical distinction.)

Physical vs. unphysical numbers

(For TCS connossieurs, I'm sketching $O(\cdot)$ and P vs. EXP ideas here...)

10 – fingers (We normally care about #'s because they count physical quantities)

100 . (# of blocks needed to build a 10x10 wall in Minecraft)

$1000 = 2^{10}$ (I'm a C.S.ist, we count in powers of 2 ☺ You've been in a room w/ 1000 people before)

$1\text{mil} = 10^6 = 2^{20}$ (Still not too hard to imagine, People in Pittsburgh. Jellybeans in jellybean book – would fit in a car. 1 mil sec. = 11.5 days.)

$1\text{bil} = 10^9 = 2^{30}$ (Starts to get serious. 1B sec. = 31.5 years, OTOH, 1 GHz = 1 bil/sec is clock speed of a crappy cell phone. 1GB HDD no biggie: has 8bil little magnetized regions.)

$1\text{tril} = 2^{40}$ (1 tril sec. = 30k years. FLOPS of a PlayStation. 1TB HDD still no biggie, but don't try to alloc. an array this size.)

2^{50} (1000 1TB HDD's. 50 20 TB HDDS)

2^{60} (Storage of huge Google/NSA data center? FLOPS of world's fastest supercomputer)

2^{64} (# of mem. locs. nameable on a std. 64-bit computer)

$10^{50} \approx 2^{150}$ (Gillions of supercomputers operating for the age of the universe could do this many operations???)

10^{80} → elem. particles in observable universe.

$$\underbrace{\phantom{10^{80}}}$$

Physical #'s (they could conceivably count something)

Unphysical #: 10^{500}, e.g.

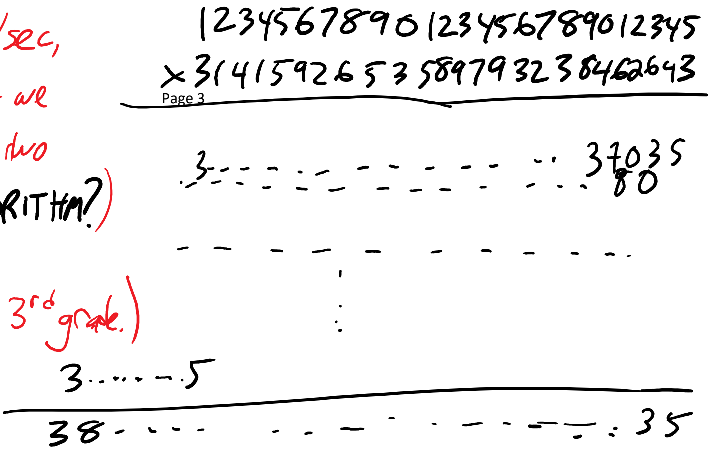
Note: it's easy to write the name of such a # 500 digits (0.5kB – could do it by hand in 5 mins. Just would not represent any phys. quantity.)

Computational challenge 1: multiply two given 500-digit numbers.

(WHY would you want to do this is a good q. Doesn't corresp. to any physical concept like blocks in a Minecraft wall. As title says, just consider it to be a "challenge".)

(Your phone/comp. has a chip that can, 1B/sec, mult. two 64-bit = 20-digit #'s. But we have 500-digit #'s, so need to store in two 25-register chunks. We need an ALGORITHM?)

(In C, need to write a 10-line prog. Built into Python. You know one from 3rd grade.)



Complexity/efficiency

steps alg. takes ...
and how that scales as fcn. of input length.

if 500 digs × 500 digs,
tableau is $\approx 500^2$ digits,
steps is $\approx 500^2$ .. maybe 1 mil
(phone can do in 1 millisec.)

n-digit mult.: $\approx n^2$ operations

← a **P**-algorithm (P = physical, P = polynomial # of steps)

(emphasize: if $n = 10^6 = 1$ mil: the 2 numbers represent unphysical qtys. But as computer alg. input/outputs, they're of physically ok lens.) Can mult. two mil-digit #'s in 1 sec on a PlayStation.)

(Well, 1 sec is OK, but Comp. Cxty always asks...)

Faster Alg.?? (Possibly you hadn't even considered other mult. algs!)

→ Yes! (Schönhage & Strassen ca. 1970.)

n-digit × n-digit mult. in $\approx n$ (well, $\approx n \cdot \log n$) steps!

Uses Fast Fourier Transform

(with this, can mult two mil-dig. #'s in a microsec. on PS4)

Comp. challenge 2: Factoring (the "reverse" of multiplication)

Input: e.g., 91. Output: 7 × 13. (prime factors)

• a 500-digit # ??

3rd-grade alg.: · check if divisible by 2? ≈ 500 steps

· ~~~~~~~~ 3 " "

· ~~~~~~~~ 5 " "

7 " "

11 " "

13 " "

(at some point, more trouble than it's worth to → 15 " "
identify primes. Just do odds.)

⋮

n digits → $\sqrt{10^n} \approx 3^n$ steps ☹ } ≈ $\sqrt{\text{input}} \approx \sqrt{10^{500}} \approx 10^{250}$ steps,

<u>un</u>physical →

Not a "P" algorithm.

Faster alg?

Yes... but: [Pollard '96]: maybe $10^{6\cdot\sqrt[3]{n}}$ steps.

(Still expon, & totally infeasible even for $n=500$.)

(3 weeks ago they set a new record by successfully factoring a special challenge # called...) RSA-$\underbrace{230}_{\#\text{ digits}}$ (multi-comp, multi-year)

RSA-$\underbrace{1024}_{\#\text{ bits}}$: worth $\$10^5$ to factor. (Maybe doable w/ enormous effort in some years)

RSA-2048: (Not physically doable ever with known algs.)
(What about unknown algs?)

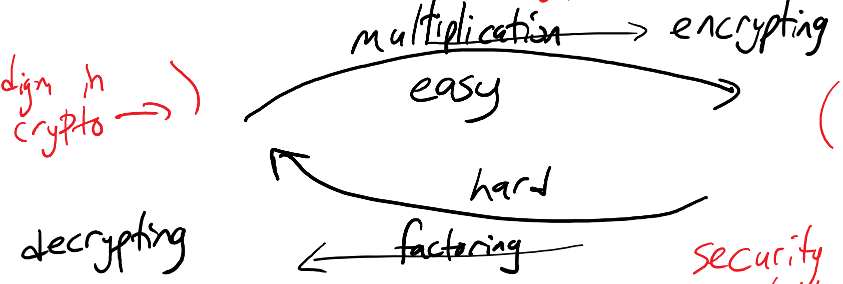
$$\boxed{\text{No one knows if there's a "P" alg. for factoring.}}$$ ⊛

[Majority(?) of people believe there isn't. At least, they <u>bank</u> on it.]

(The assumption that it's <u>not</u> in P is basis of almost all crypto.)

(What does factoring have to do w/ crypto? Presumably you know a little about RSA, but...)

(the central paradigm in crypto →)



(Any time you go to a webpage w/ https, ← "secure"
security relies on de facto impossibility of factoring ~~1024~~-bit #'s)
2048, as of 2013

Punchline: [Probably not a spoiler if you know even a little about Q.C.]

Peter Shor, 1994: A Q.C. (if built) could factor n-bit #'s in $\approx n^2$ steps. In **P**! (on Q.C.)

Factors 500-digit # in a few mil. steps. ⟦1 second, if at speed of cell phones
↓
destroys all past crypto!!⟧

(How?! We'll see, but relies on "distinctively new way of harnessing nature")

Uses basic fact of quantum mechanics:
given, e.g., 1000 photons/electrons/..., their joint "state" is defined by 2^{1000} numbers ("amplitudes")
↳ stored by Nature (It would seem! According to many many confirmed experiments.)

(Q.C. expert Umesh Vazirani (of the videos):
"We would like to hack into Nature's computer!")

(Q.C. cofounder Deutsch: Shor's alg. is a dramatic illustration of existence of parallel universes (!!!??!!?). 10^{500} of them, if you're factoring 500-digit #'s...)

"When a quantum factorization engine is factorizing a 250-digit number, the number of interfering universes will be of the order of 10^500. This staggeringly large number is the reason why Shor's algorithm makes factorization tractable. I said [earlier in the book] that the algorithm requires only a few thousand [or maybe a million] operations. I meant, of course, a few thousand parallel operations in each universe that contributes to the answer. All those computations are performed in parallel, in different universes, and share their results through interference."

(Here Deutsch is espousing a certain "interpretation" of Q.M. called the) Many Worlds Interpretation — Hugh Everett, 1956/57

(There are a lot of philosophical q's surrounding Q.M.'s. Not around the math, or the physical predictions it makes. These all 100% solid. But what to make of this 2^{1000} #'s to store for 1000 particles? Or of the "measurement issue" — Schrödinger's Cat, etc.? Don't need to know, for this course. But for fun, I'll tell you a teeny bit about Everett & MWI, which is a minority opinion — but not overwhelming minority. Definitely preferred by many serious, non-fringe physicists (e.g. Deutsch) I kinda like it...)

(Everett: M.Sc. with Albert Tucker, a proto CSist, on military game theory.)

Tucker

M.Sc.

Minsky
|
M. Blum (CMU)
|
U. Vazirani
|
Sudan
|
me

Everett

Ph.D. on MWI

Wheeler (famous physicist – "black hole", "wormhole")

Feynman

Deutsch

(Scorned by physicists.
Everett went to Pentagon,
did computer modeling of nukes.
Switched to O.R. Became computer
consultant.)

(Early '70s: physicist Bryce DeWitt began
promoting Everett's work.
Late '70s: started to get taken seriously,
including by Wheeler's student.)

(Other cofounder
of Q.C.
More on him
later.)

Griffiths
(CMU, 1964–retirement)

(But around a lot,
has PhD student...)

(1956 MWI thesis typed by Everett's future
wife Nancy – their kid Mark (aka "E")
is frontman of band Eels.)

(In case your soul is shaken by the concept of 10^{500} parallel universes, let me offer some novocaine:

- don't have to accept/understand MWI for Q.C.; just for fun
- Leitmotif 2, "rotate, compute, rotate": as I'll sketch next time, Q.C. is not too complicated.)

Feynman: "It is safe to say that nobody understands quantum mechanics."

(But that's just the 'interpretation'; in the end, it's just math.)

Von Neumann [founder of the mathematics of Q.M.]:

"In mathematics, you don't understand things. You just get used to them."

Me: "It is safe to say that any old graduate student can understand quantum computation."

(In this course, we'll spend a bunch of lectures getting used to the math of Q.M. & Q.C. We'll also see lots of simple & fun applications of very basic quantum info theory — quantum money, secret key exchange, teleportation... then we'll get into Quantum computation, and finish Shor's alg... & still there will be half the course to go. So really Shor's not too bad...)

(Shor's alg. from '94. He was a well-known TCS-ist at the time, worked on comp geom, online algs.

↳ Directly based on ("inspired" - Shor) a slightly earlier (first-rejected) quantum alg. of → Dan Simon)

(CS PhD student at Univ. Montreal. Advisor: G. Brassard, influential early Q.C.-ist.

Basically into crypto. Brassard asked him to look into Q.C.
He did for a bit, published "Simon's Alg."
Got interested in networking, left academia, went to networking & security product group at MSFT.

Many years later, C. Fuchs polled some Q.C. luminaries (Deutsch, Shor, etc.) about their work, and if Everett's MWI was influential in their thinking...

Simon: "Who's Everett, and what's his interpretation?"

"I was approaching the problem purely from a computer scientist's perspective. I learned the absolute bare minimum of physics I needed to be able to understand the computer science question, which (as I saw it) was, "these crazy people are claiming that if you add these very-weird-yet-theoretically-physically-implementable functions to a computer, then you should be able to do amazing things with them. Prove them right or wrong." I actually started out trying to prove that quantum computing was useless, and eventually narrowed down the difficult, unsimulateable part [of QC's power] to, "Rotate, compute, rotate". That helped guide my search for a computationally interesting quantum algorithm."

(We'll talk about "rotate, compute, rotate" in Lecture 2.
In brief, the one thing a Q.C. can do is...
the Fourier Transform. Which is a rotation.
In 10^{500}-dimensional space.)

(As he says, don't need physics, QC can be boiled down to
classical comp. with a lin. alg. twist.
Shor's response also emphasized he didn't think about
10^{500} parallel universes, and he thought that gave
a misleading picture of Q.C.'s power. E.g. we
don't think Q.C.'s can efficiently solve "NP-complete probs.")

(So next time I want to convince you that Q.C.
is not mysterious & crazy.
But it is fun to talk about the mysteries of 10^{500}
parallel universes some times ☺).