Monday, November 7, 2022

Lecture 17 - Learning a Mystery Rotation

Last time: Grover's alg on n-input circuit C.

Let's write p = frac. of $x \in \{0,1\}^n$ s.t. $C(x)=1$.

(i) Classical random guessing: $\approx 1/p$ trials

(ii) If you know p (up to 10%)

↳ know Grover rot. (up to 5%)

↳ know good # of "combos" to do

$\approx \frac{\pi}{4} \cdot \sqrt{\frac{1}{p}}$

unique case: $p = \frac{1}{2^n} = \frac{1}{N}$

Today: #SAT (approximate) : Estimate p up to $\pm 10\%$, (with high confidence)

First: Classical alg. for estimating of p?

Plug a random string string to C

$\rightsquigarrow \begin{cases} 1 & \text{w. prob. } p \\ 0 & \text{w. prob. } 1-p. \end{cases}$

→ We played around with estimating a coin's bias in

Scratch!

Takeaways

Takeaways

- Getting p to within 10% $\approx$ getting 1 or 2 sigfigs
- Do 10 flips, 100 flips, 1000 flips....
  only the "last" batch really costs you...
  If you finally see "heads" on doing 10^6 flips,
  preceding 111,110 flips are just 11% more $\rightarrow$ negl.
- If $p \ll 10^{-6}$, probably WON'T see any heads
  till 10^6 flips
- OTOH: say you do $\frac{100}{p}$ flips...
  $$\Pr[\text{no heads}] = (1-p)^{100/p} \le (e^{-p})^{100/p}$$
  $$= e^{-100}$$
- Say, e.g., $p = 4.16 \times 10^{-9}$
  Say you do $n = 10^{11}$ flips.
  $E[\#\text{ heads}] = np = 416$
  Is it plausible we'll see 416 ± 42?
  $\rightarrow$ Binomial(n,p): Variance $= np(1-p) \sim np$
  std.dev. $= \sqrt{Var} = \sqrt{np}$
  in e.g.: $\sqrt{416} \approx 21$

In general: if you want stddev $\le$ 10% expec.

$$\sqrt{np} \le .1\, np$$
$$\Uparrow \quad 10 \le \sqrt{np}$$
$$100 \le np\ ,$$

$$\Uparrow \qquad \begin{aligned} &100 \le np \\ &n \geq 100/p. \end{aligned}$$

<u>SUMMARY</u>: With $O(1/p)$ coin flips, can estimate unknown coin's bias to $\pm 10\%$. (high confidence)

Exercise/homework: It's $O\left(\frac{(1/\varepsilon^2)}{p}\right)$ flips to estimate p to range $(1-\varepsilon)p \ldots (1+\varepsilon)p$.

Back to Grover's alg!

Recall: Starting from C_1 cooked up:

- Mystery Rotation ("combo" of 2 reflections)
- "starting state" $|u\rangle$ (unif. superpos.)

Starting here, doing MysteryRot a bunch of times, we <u>stay</u> in a certain 2-dim. subspace.

Mystery Rot was by θ:

$$\cos\theta = 1 - 2p \iff \theta \sim 2\sqrt{p}$$

if $p < \frac{1}{100}$, correct to w/i 0.1%

$$\Rightarrow p \sim \frac{\theta^2}{4}$$

Estimate θ:

$$\boxed{.96\theta \le \hat{\theta} \le 1.04\theta \quad (*)}$$

$$\Downarrow$$

$$\hat{p} = \frac{\hat{\theta}^2}{4}$$

$p = \frac{\theta}{4}$

$$.96^2 \frac{\theta^2}{4} \le \frac{\hat{\theta}^2}{4} \le 1.04^2 \frac{\theta^2}{4}$$

$$.91\, p \le \hat{p} \le 1.09 \cdot p$$

Suffices to estimate θ to w/i 4% to get p to w/i 10%.

Temporary Simplification:

Say MysteryRot_θ is just operating on 1 qubit in $\mathbb{R}^2$.

Q: How many times to use Rot_θ to estimate θ to 10%?

As we saw in Scratch:

$O(1/\theta)$ uses to get "1 sig fig" or $\pm 10\%$ accuracy

$\rightarrow$ Measure $\text{Rot}_\theta^k |0\rangle$ 100 times to see if you get a reasonable split of "0" & "1"

for $k = 1, 2, 4, 8, 10, 100 \ldots$

Remembering in Grover: $\theta_{grover} \sim 2\sqrt{p_c}$

$\therefore$ $\boxed{O\left(\frac{1}{\sqrt{p}}\right)}$ uses of Mystery Rot are enough to estimate p to 10%!

$\therefore$ $\boxed{O(\sqrt{p})}$ uses of Mystery are enough to estimate p to 10%!

Getting even more accuracy for θ.

let's measure it in fractions of 2π

E.g.: if $\theta \approx .\underbrace{000000000000}_{12\text{ zeroes}}4 \cdot 2\pi$

We'll need to repeat Rot_θ 10^{12} times to "get in ballpark"

E.g. inductively we've determined

$\theta \approx .00 \ldots 12\text{ zeroes} \ldots 047583(6?)(2??) \cdot 2\pi$

frankly not sure

super-sure

kinda sure

Let U = concat. of 10^{16} Rot_θ's.

Now U rotates by $4758.3(6?)(2??) \cdot 2\pi$.

equivalently $0.3(6?)(2??) \cdot 2\pi$

35%....37% of 2π

$130° \pm 4°$ $131.3° \pm .2°$

Apply $U|0\rangle$ 100 times

$\Pr[\text{measuring "0"}] = \cos(130° \pm 4°)^2$

$= 34\% \ldots 47\%$

With ~~100~~ $\boxed{O(1)}$ measurements can nail to 41.1% ± 1

can improve our confident

↳ can improve our confident

$.3\,(6?)(2??) \longrightarrow .36\,(0?)(8??)$

$\therefore$ U is rotating by $4758.3\boxed{6}(0?)(8??)$

$\therefore$ θ is $.000000000000475836(0?)(8??)$

Summary: With $O(10^{16})$ uses of Rot_θ,
get 17^{th} digit of accuracy in θ

$O(10^{17})$ uses
→ 18 digits

$\therefore$ with $O(10^{d})$ ← $O(1/\tau)$ uses of Rot_θ,
get $\hat{\theta}$ that's $\theta \pm 10^{-d}$ (with very high confidence)

↑ τ

Or: additive accuracy $\pm\tau$ on θ
with $O(1/\tau)$ uses of Mystery Rot_θ.

Observations

1. Getting θ to $\pm 10^{-16}$ requires 10^{16} repetitions of Mystery Rot.

What if we understood C well enough that we could build $(\text{Rot}_\theta)^{10^{16}}$ efficiently??!?!

Analogy: Compute $37^{10^{16}} \bmod 251$.

Analogy: Compute $37^{10^{16}} \bmod 251$.

Don't 10^{16} mults by 37.

$\rightsquigarrow O(16^2)$ operations

(2) Grover scenario: a bit harder than MysteryRot on 1 qubit.

"We "know" $|0\rangle$ but not "$|1\rangle$"."

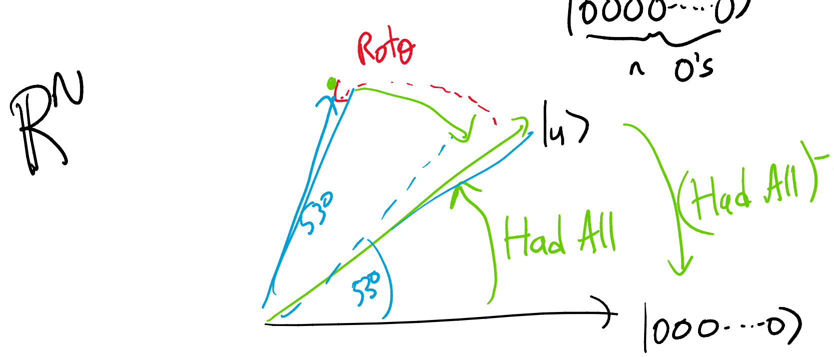
Property: We can make starting vector $|u\rangle$, unif. superpos easily.

We don't know another basis vector for 2-d subspace where all rotation.

Not a problem:

Algorithm can measure in <u>any</u> basis of $\mathbb{R}^N$ that includes $|u\rangle$.

Got this by doing Had All on $|\underbrace{0000\cdots0}_{n \text{ 0's}}\rangle$



$(\text{Had All})^{-1}$ Rotated vector is 53°

(Had A(1)) : Rotated vector is 53°
away from $|00\cdots0\rangle$

Standard measurement:
getting "00⋯0" : like measuring to $|0\rangle$ in $\mathbb{R}^2$
not-"00⋯0" : ~ $|1\rangle$ in $\mathbb{R}^2$.