Lecture 18 — Revolver Resolver

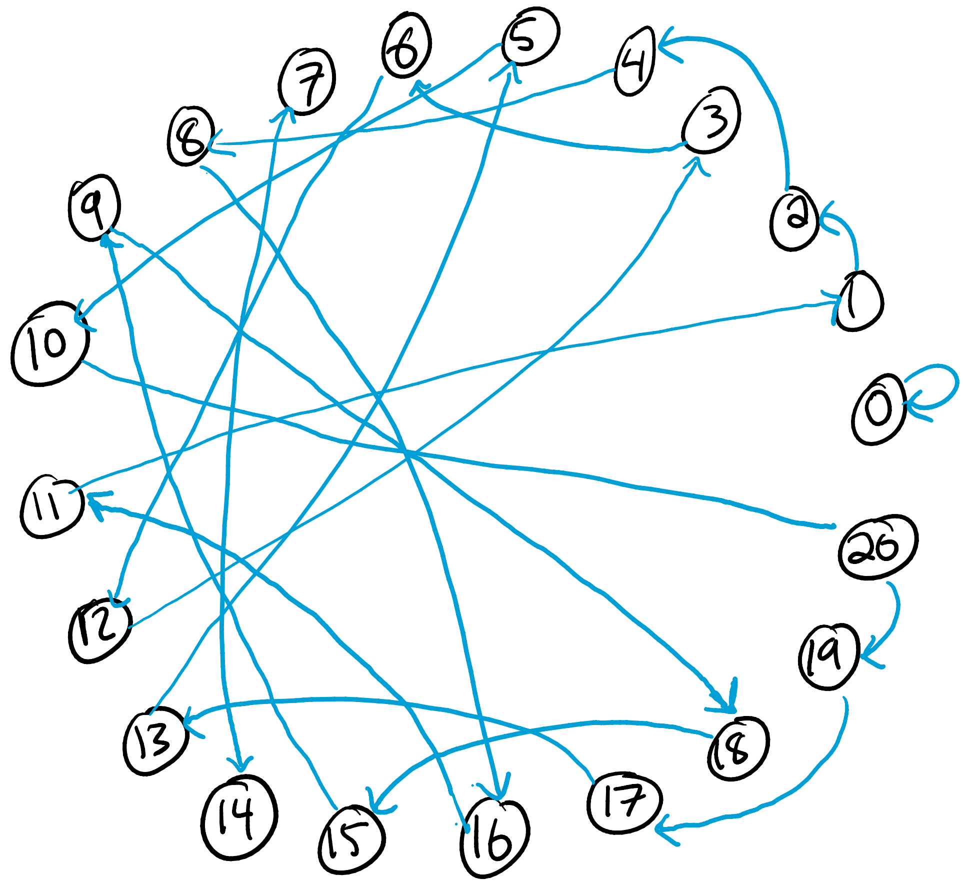
<u>Recall:</u> Given Rot_θ operating on 1 qubit, θ a mystery, can confidently get d digits of accuracy w/ $O(10^d)$ uses of Rot_θ and $O(d)$ measurements (checking for "0"s).

[Seems great — what more could you want? Well... a few more technical improvements as we'll see. E.g., as we saw when applying to Grover's alg., was important we could do this in an <u>unknown</u> 2-d plane, provided we could make a starting vector in this plane. Today we'll even discuss what if you don't know how to make that starting vector... After we make all technical improvements, we'll call the resulting quantum algorithm the...] Revolver Resolver.

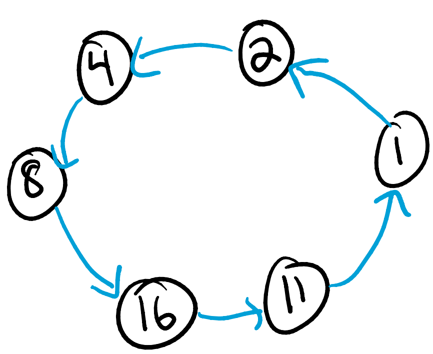
(Real name: "Quantum Phase Estimation")

[though Q.P.E. is about <u>complex</u> unitaries, eigenvectors/vals...]

[To keep you motivated to study technicalities, let me give a teaser of where we're headed: Factoring!]



[Here's the digraph of "multiplying by 2 mod 21". How long is the cycle that 1 is on? If you can figure that out, you can factor 21....]



[The adj. matrix of the graph kind of acts like "Rot_θ" for $\theta = (1/6)\cdot 2\pi$. If you discover $\theta \approx .166667 \cdot 2\pi$, you can probably figure cycle length 6....]

[But that's all "teaser" motivation. Back to technical improvements for Revolver Resolver....]

Grover setting:

- Can make "start vector" $|start\rangle \in \mathbb{R}^N$ [[unif. superpos n Grover case]]
  (= Had. All on $|00\ldots\ldots 0\rangle$)
- Can make (mystery) quantum oper. "U" on $\mathbb{R}^N$ [[combo of 2 refls. in Grover case]]
- Know repeating U from $|start\rangle$ rotates you in some (mystery) 2-d plane by some (mystery) angle θ.

[[As I said last time, since θ-estimation alg. only needs to measure angles between $|start\rangle$ & $U^k|start\rangle$ for various k, not knowing the 2-d plane isn't so bad; just need to be able to measure in a basis containing $|start\rangle$.

Now we make it even harder:]]

Suppose someone gives you $|start\rangle$, but you don't know what it is.

[[You don't know how to make any more copies...]]

[Seems hard! You can rotate $|start\rangle$ as many times as you want by applying U, but you then want to measure "against" $|start\rangle$; like, figure out the angle from $|start\rangle$. But how? You don't know $|start\rangle$; how to measure against it?]

"Idea": Given $|start\rangle$, go into an equal superpos. of rotatin it & not rotating it...
[Vaguely like getting two copies...]

<u>"Hadamard Test"</u>: Given N-dim U, and some qubits S in state $|start\rangle \in \mathbb{R}^N$....

1. Make qubit T
2. Add & Diff on T
3. "If T Then Do U on S"
   [aka "Controlled-U" with control bit T, target S]
4. Avg & Disp on T
5. Measure T

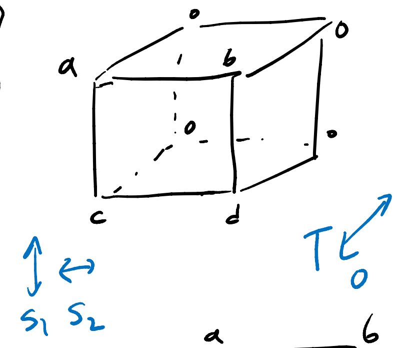
(Wait... we assumed we could do U, but does it mean you can do Controlled-U? We'll come back to this....)

[In normalized reality, steps 2 & 4 are both Hadamard.]

Analysis:

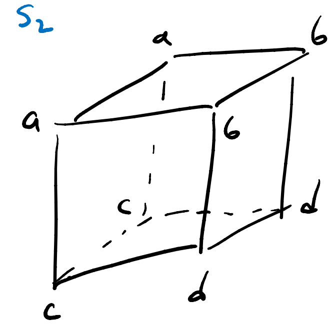
State after 1: $\underset{S}{|\text{start}\rangle} \otimes \underset{T}{|0\rangle}$

e.g. S is 2 qubits

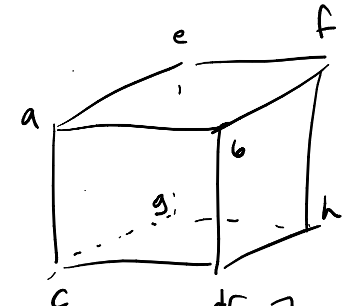


After 2: (unnormalized) $|\text{start}\rangle \otimes (|0\rangle + |1\rangle)$

$= \underset{|\nearrow\rangle}{|\text{start}\rangle \otimes |0\rangle} + \underset{|\nearrow\rangle}{|\text{start}\rangle \otimes |1\rangle}$



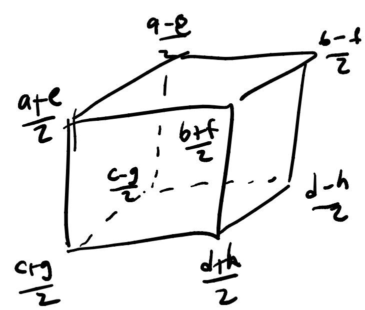
After 3: (controlled-U) $\underset{|\nearrow\rangle}{|\text{start}\rangle \otimes |0\rangle} + \underset{|\uparrow\rangle}{(U|\text{start}\rangle) \otimes |1\rangle}$



if $U\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} e \\ f \\ g \\ h \end{bmatrix}$

After 4: (avg & disp on T) $\left(\text{avg}\{|\text{start}\rangle, U|\text{start}\rangle\}\right) \otimes |0\rangle$

$+ \left(\text{disp}\{|\text{start}\rangle, U|\text{start}\rangle\}\right) \otimes |1\rangle$



$\text{Prob}[T=0] = \|\vec{\text{avg}}\|^2$

$= \left(\frac{a+e}{2}\right)^2 + \dots + \left(\frac{d+h}{2}\right)^2$

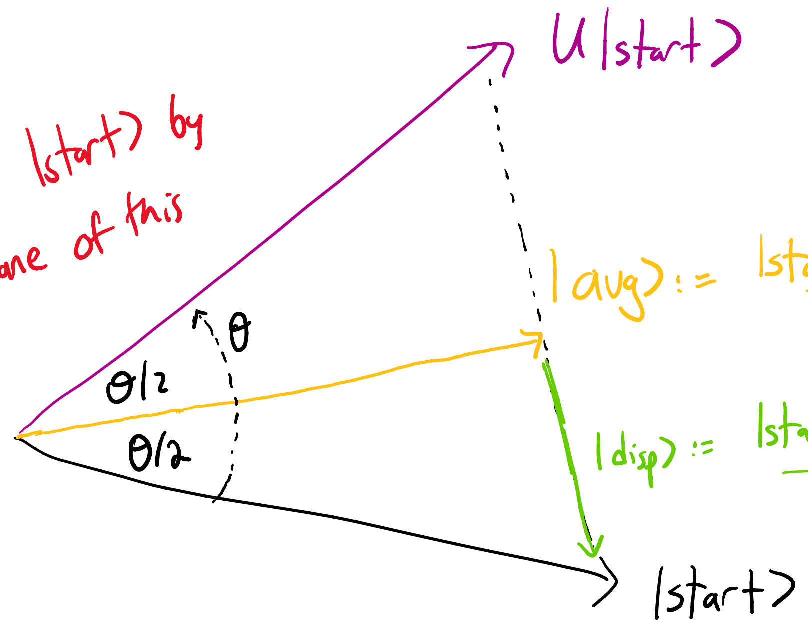
Step 5 Measurement:

next page . . .

$\text{Prob}[T=1] = \|\vec{\text{disp}}\|^2 = \left(\frac{a-e}{2}\right)^2 + \dots + \left(\frac{d-h}{2}\right)^2$

$\mathbb{R}^N$

[[U rotates |start⟩ by θ in plane of this page]]



$$|aug\rangle := \frac{|start\rangle + U|start\rangle}{2}$$

$$|disp\rangle := \frac{|start\rangle - U|start\rangle}{2}$$

State just before measuring T:

$$\underset{S}{|aug\rangle} \otimes \underset{T}{|0\rangle} + \underset{S}{|disp\rangle} \otimes \underset{T}{|1\rangle}$$

(normalized, since we did
1 Add & Diff,
1 Aug & Disp.)

$$\Pr[\text{T reads out to "0"}] = \| \, |aug\rangle \|^2 = \langle aug | aug \rangle = \left(\cos\frac{\theta}{2}\right)^2.$$

↳ and state of S collapses to $\dfrac{|aug\rangle}{\cos(\theta/2)}$

$$\Pr[\text{T reads out to "1"}] = \| \, |disp\rangle \|^2 = \langle disp | disp \rangle = \left(\sin\frac{\theta}{2}\right)^2$$

↳ and state of S collapses to $\dfrac{|disp\rangle}{\sin(\theta/2)}$

[[This is great!]]

<u>Good news 1</u>: $\Pr[T \text{ reads out } 0] = \left(\cos\frac{\theta}{2}\right)^2$

Had we been able to "measure against |start⟩" like we wanted, Pr[readout "start"] would be $(\cos\theta)^2$. More or less the same!

[[We can use this Hadamard Test to estimate $\theta/2$, then multiply estimate by 2, no worries.]]

<u>Good news 2</u>: Whether we read out T=0 or 1, state of S (unentangled with T) is either |avg⟩ or |disp⟩ (up to normalizing factors)

& BOTH OF THESE ARE IN THE 2-DIM PLANE U ROTATES |start⟩ IN.

$\therefore$ we can REUSE state of S as our "new |start⟩".

[[Recall we have to do lots of measurements and U-applications to estim θ well. So we need to keep doing Had Tests in this mystery 2d plane we started in. Luckily, we can keep reusing state of S. Don't care that |start⟩ has different orientation for each subtest.]]

"Controlled-U" / "If T Then Do U on S" issue.

We need to be able to do it.

If U is completely a black box, can't necessarily do it.

However... in all applications U is not a black box, we made its code ourselves [e.g., in Grover application, U is "If C Then Minus" which we built ourselves from C's code, plus Grover's refl. thru mean, which is a fixed alg.]

So then we can make it ourselves.

E.g.: we know...

U:

- Add 1 To S_1
- Add S_2 To S_3
- Had S_3
- Add S_1 AND S_5 To S_3

⋮

"If T Then U":

- Add T to S_1
- Add (T AND S_2) To S_3
- If T Then Had S_3

just some 2-qubit op; I hereby allow us all to use it

- Add (T & S_1 & S_5) To S_3

not a "base" instruction, but can implement in a couple of lines...

⋮

Summary: Revolver Resolver

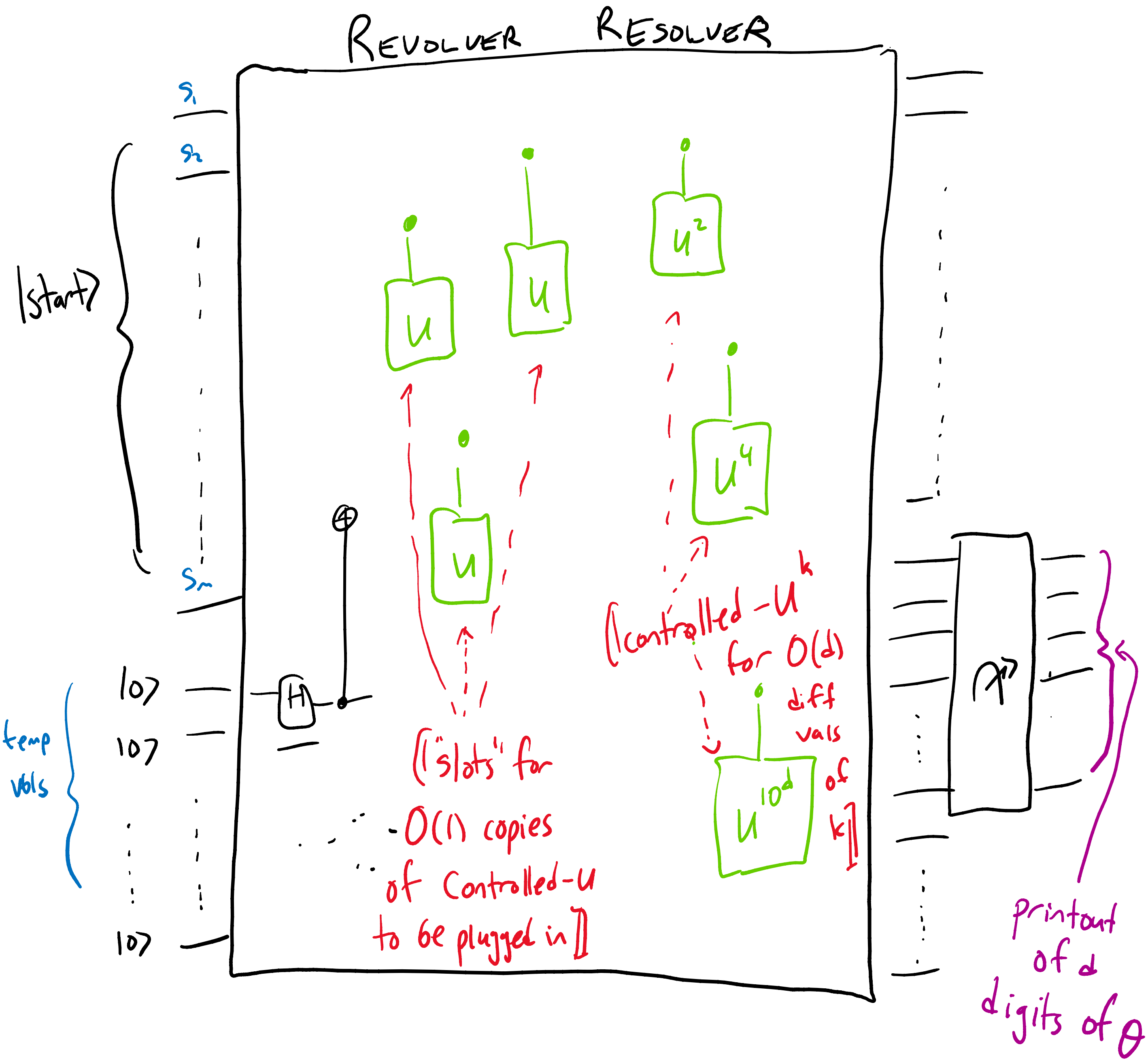
Input: • Controlled-U operating in $\mathbb{R}^N$
• $|start\rangle \in \mathbb{R}^N$ s.t. U rotates $|start\rangle$ within some 2-d plane by θ
• d

Output: θ to d digits of accuracy (with high confidence) using $O(d)$ measurements, $O(1)$ uses of Controlled-$U, U^2, U^4, U^8, \ldots, U^{2^k}$ such that $2^k \approx 10^d$.

[I was a bit sloppy in nailing down exact alg., but take my word for it, it suffices to use U in powers of powers-of-2, up until you're $O(\cdot)$ of the inverse-accuracy, 10^d.]

Remark: Alg. involves a lot of "intermediate measurements", mixture of classical/quantum ops, but as on homework, can put it in "standard form": all Makes at beginning, then only quantum ops, then all Measurement/Print at end.

[[Schematic of circuit for R.B. in standard form:]]



[[Remark: by being extra tidy, can ensure: a) no trash; b) state coming out of $s_1, \ldots, s_n$ qubits is <u>still</u> in 2-d plane that U rotates $|start\rangle$ in.]]

[[Pretty glorious, but why go to all this trouble?]]

1. For Factoring problem, our U will be such that we can implement U^{10^d} <u>super-efficiently</u>, in $O(d^2)$ time/gates, rather than 10^d.

2. We won't actually know any good "$|start\rangle$".

   But... we will know a <u>superposition</u> (linear combo) of good starts,

   $$|v\rangle = |start_1\rangle + |start_2\rangle + |start_3\rangle + \dots$$

   Will plug $|v\rangle$ into Revolver Resolver!

   And it will estimate associated rotation angles in superposition...!