Lecture 16 — Grover's Geometry, & Approximate #SAT

Recall Grover's SAT alg.:

Given "code" C (AND/OR/NOT circuit), with n input bits, 1 output bit, say $C(x) = 1$ for some unique $x^* \in \{0,1\}^n$. Can find x^* in $\approx \sqrt{2^n}$ time.

[[We'll see a new geometric perspective on this alg., and also see how to do something stronger: for any C, approximate #x's such that $C(x)=1$.]]

e.g. use case: factoring RSA2048:

let $C(y,z)$ output 1 iff

$1 < y < z$ and $y \cdot z = \text{RSA2048}$.

[[Actually, we know special-purpose factoring algs a lot faster than $2^{n/2}$ time, but still interesting....]]

Alg: • Prepare "$|u\rangle$" $= \left.\begin{array}{c|l} \begin{bmatrix} +1 \\ +1 \\ +1 \\ \vdots \\ +1 \end{bmatrix} & \begin{array}{l} 00\cdots0 \\ 00\cdots1 \\ \\ \vdots \\ 11\cdots1 \end{array} \end{array}\right\} N = 2^n$

[[uniform superposition, unnormalized]]

[[Add & Diff all, starting from $|00\cdots0\rangle$]]

(i) If $C(x_1,\ldots,x_n)$ Then Minus $\longmapsto$ "$|v\rangle$" $:= \begin{array}{cl} \begin{bmatrix} +1 \\ \vdots \\ +1 \\ -1 \\ +1 \\ \vdots \\ +1 \end{bmatrix} & \begin{array}{l} \\ \\ \\ \leftarrow x^* \\ \\ \\ \\ \end{array} \end{array}$

(ii) Grover's "Reflection Across Mean" $\longmapsto \approx \begin{array}{cl} \begin{bmatrix} +1 \\ \vdots \\ +1 \\ +3 \\ +1 \\ \vdots \end{bmatrix} & \begin{array}{l} \\ \\ \\ \leftarrow x^* \\ \\ \\ \end{array} \end{array}$

Repeat $\approx \sqrt{N}$ times, $N = 2^n$.

Dream: get to "$|goal\rangle$" $= \begin{array}{cl} \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \sqrt{N} \\ 0 \\ \vdots \\ 0 \end{bmatrix} & \begin{array}{l} \\ \\ \\ \leftarrow x^* \\ \\ \\ \\ \end{array} \end{array}$

[[Then measuring reveals x^*.]]

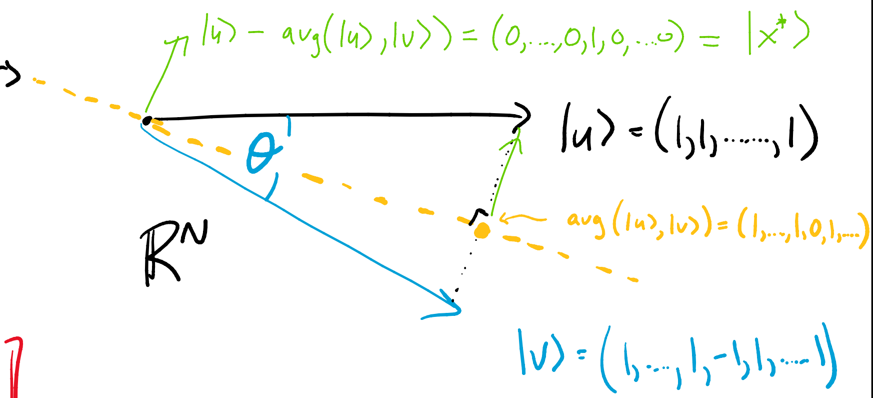
[[Recall that every unitary (quantum) operation (with real #'s) is an N-dimensional rotation/reflection.]]

(i) is a <u>reflection</u> [[do it twice in a row, get back to where you were]]

(ii) also a <u>reflection</u>

[Even though these operations are happening in N dims., let's still try to picture them....]

(i) reflects thru



[$|u\rangle$ & $|v\rangle$ are practically the same, so their angle θ is <u>very</u> small]

[the operation (i) $|u\rangle \mapsto |v\rangle$ is a reflection thru orange line; actually, thru the (hyper)plane perpendicular to $\nearrow = |x^*\rangle$ $|x^*\rangle$ gets reflected, everything else fixed.]

Q: What does (ii) reflect thru?

A: $|u\rangle = (1,\dots,1)$ is <u>only</u> unchanged direction:

$$\mu(1,\dots,1) + (\Delta_1, \Delta_2, \dots, \Delta_N) \longmapsto \mu(1,\dots,1) - (\Delta_1,\dots\dots,\Delta_N)$$

So it's reflection across $|u\rangle$.

<u>Obs</u>: If we start with a vector in this 2-d plane of $|u\rangle, |v\rangle$ [and we do, we start at $|u\rangle$], we stay in it!

Also: combo of 2 reflections is a <u>rotation</u>.

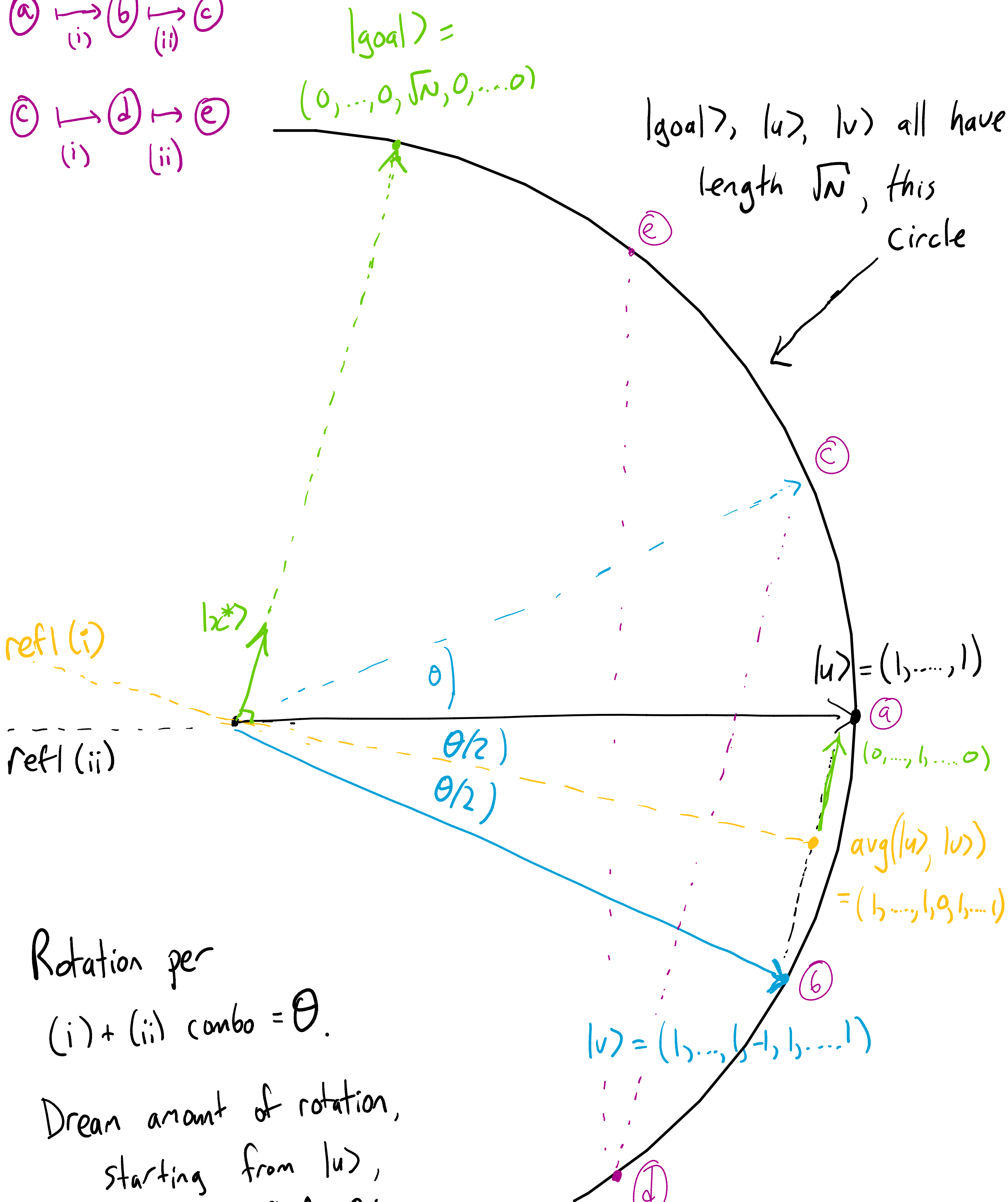
Alg's operation:

$a \xmapsto{(i)} b \xmapsto{(ii)} c$

$c \xmapsto{(i)} d \xmapsto{(ii)} e$

$\mathbb{R}^2 \subseteq \mathbb{R}^N$

$|goal\rangle$, $|u\rangle$, $|v\rangle$ all have length $\sqrt{N}$, this circle



Rotation per (i) + (ii) combo $= \theta$.

Dream amount of rotation, starting from $|u\rangle$, is $90° - \theta/2$.

Dream total rotation amount is $90° - \theta/2 \approx 90° = \pi/2$ radians.

[[θ is tiny]]

1 combo = θ rotation, where θ = angle of $|u\rangle, |v\rangle$.

Normalize to unit vectors $|\tilde{u}\rangle = \frac{|u\rangle}{\sqrt{N}}$, $|\tilde{v}\rangle = \frac{|v\rangle}{\sqrt{N}}$.

Then $\cos\theta = \langle\tilde{v}|\tilde{u}\rangle = \frac{1}{\sqrt{N}}\cdot\frac{1}{\sqrt{N}} [1\ 1\ \cdots\ -1\ 1 \cdots 1] \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$

[[inner product]]

$$= \frac{N-1-1}{N} = 1 - \frac{2}{N}.$$

[[super-tiny!]]

[[So how small is θ??]]

[[Trick...]] $\therefore (\cos\theta)^2 = \left(1-\frac{2}{N}\right)^2 = 1 - \frac{4}{N} + \cancel{\frac{4}{N^2}}$ super-duper tiny

$$\| $$

$1-(\sin\theta)^2$. $\therefore (\sin\theta)^2 = \frac{4}{N} \Rightarrow \sin\theta = \frac{2}{\sqrt{N}}$

But $\sin\theta \approx \theta$ for θ small! $\therefore \boxed{\theta \approx \frac{2}{\sqrt{N}}}$

$\therefore$ k combos $\Rightarrow k\cdot\frac{2}{\sqrt{N}}$ total rotation.

This is $\approx \frac{\pi}{2}$ (the dream) iff $\boxed{k \approx \frac{\pi}{4}\sqrt{N}}$

[[as promised, if you remember back to the sliding block 3B1B video stuff.]]

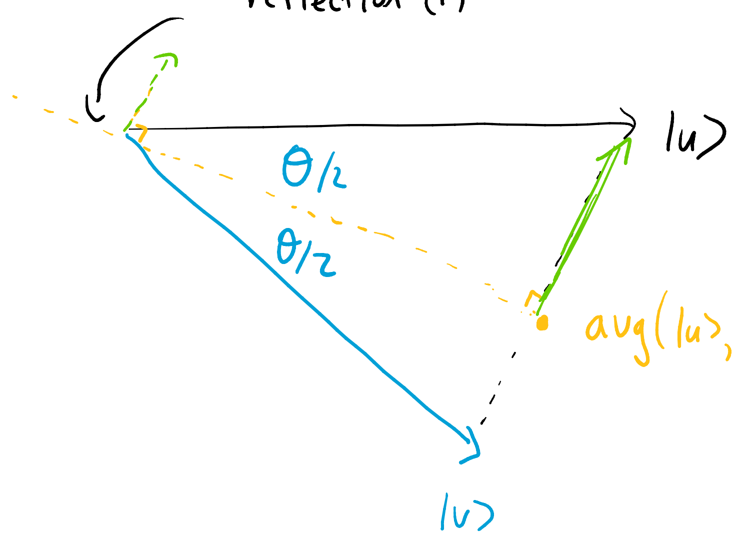
[[If you take $k = \lfloor \frac{\pi}{4}\sqrt{N} \rfloor$, get to w/i $\pm \frac{\text{small}}{\sqrt{N}}$ angle of $|\text{goal}\rangle$, hence readout is x^* w.prob. $1 - \frac{\text{small}}{\sqrt{N}}$.]]

[Now that we understand it so well, let's make extensions!]

Q: What if $C(x) = 1$ for exactly $\underline{2}$ values of x, say x_1^*, x_2^*. What changes?

$\underbrace{\text{"If } C(X_1,\dots,X_n) \text{ Then Minus"}}_{\text{reflection (i)}}$ now maps

$$|u\rangle = \begin{bmatrix} +1 \\ +1 \\ \vdots \\ \vdots \\ +1 \end{bmatrix} \longmapsto \begin{array}{c} \begin{bmatrix} +1\text{'s} \\ -1 \\ +1\text{'s} \\ -1 \\ +1\text{'s} \end{bmatrix} \end{array} \begin{array}{l} \\ \leftarrow x_1^* \\ \\ \leftarrow x_2^* \\ \\ \end{array} = \underline{\text{new}}\ |v\rangle$$



$$\text{avg}(|u\rangle, |v\rangle) = \begin{bmatrix} +1\text{'s} \\ 0 \\ +1\text{'s} \\ 0 \\ +1\text{'s} \end{bmatrix} \begin{array}{l} \\ \leftarrow x_1^* \\ \\ \leftarrow x_2^* \\ \\ \end{array}$$

$$\nearrow = |u\rangle - \text{avg}(|u\rangle,|v\rangle) = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \end{bmatrix} = |x_1^*\rangle + |x_2^*\rangle$$

One combo = rotation by new θ.

Dream rotation by $90° - \theta/2$ takes you to...

length-$\sqrt{N}$ vector in dir. of $\nearrow = |x_1^*\rangle + |x_2^*\rangle$,

namely $\sqrt{\frac{N}{2}}\left(|x_1^*\rangle + |x_2^*\rangle\right)$. $\leftarrow$ Measuring from here gives x_1^* or x_2^*, prob $\frac{1}{2}$ each.

So we'll get a random satisfying x after

$\approx \dfrac{\pi/2}{\text{new } \theta}$ combos. How much is new θ?

[Instead of working it out for 2, lets be a bit more general...]

Say C has $\underline{m}$ satisfying x's, $x_1^*, \ldots, x_m^*$.

$|v\rangle = (1, 1, \ldots -1, \ldots\ldots -1, \quad \ldots \qquad \ldots 1)$ with m -1's

$|u\rangle = (1, 1, \; - - - - - - - - - - \; 1)$

Unit length versions: $|\tilde{u}\rangle = \frac{1}{\sqrt{N}} |u\rangle, \quad |\tilde{v}\rangle = \frac{1}{\sqrt{N}} |v\rangle.$

$\cos\theta = \langle \tilde{v} | \tilde{u} \rangle = \frac{1}{N} \langle v | u \rangle = \frac{1}{N} (1 + 1 + \cdots -1 + \cdots\cdots 1)$ with m -1's

$= \frac{1}{N} (N - m \;\; - m)$

$\boxed{= 1 - \frac{2m}{N}}.$

(Side remark: if you didn't know m in advance, you could find (or approximate) m by (trying to) find (or approximate) θ.)

[This remark motivates a subject we will study a lot in the next lectures.... approximately finding θ given a mystery "Rotate by θ" operation....]

[[Anyway, assuming m satisfying x's for C, we got to....]] $\cos\theta = 1 - \frac{2m}{N}$

$$\Rightarrow \quad (\cos\theta)^2 = 1 - \frac{4m}{N} + \frac{4m^2}{N^2} \approx 1 - \frac{4m}{N} \quad \left(\text{assuming } \frac{m}{N} \text{ "small"}\right)$$

[[↑ the case of interest]]

$$(\sin\theta)^2 \approx \frac{4m}{N} \Rightarrow \sin\theta \approx 2\sqrt{\frac{m}{N}}$$

$$\Rightarrow \theta \approx 2\sqrt{\frac{m}{N}} \quad \left(\text{assuming } \frac{m}{N} \text{ "small"}\right)$$

$\therefore$ each Grover combo rotates you $\approx 2\sqrt{\frac{m}{N}}$ away from start state $|u\rangle$.

Knowing m, do $k \approx \frac{\pi}{4}\sqrt{\frac{N}{m}}$ combos, measure, get a random satisfying x^* [[pretty much; slight chance of wrongness due to $\approx$]]

E.g. say you knew $\frac{m}{N} \approx 0.01\%$ [[About $\frac{1}{10{,}000}$ frac. of x's satisfy x.]]

Classical probabilistic sampling $\Rightarrow \approx 10{,}000$ tries to find satisfying x.

Grover's method: $\approx \frac{\pi}{4}\sqrt{10{,}000} \approx 100$ uses of C.

[["Square-root speedup" again]]

[Back to "side remark".]

How would we know $m = \#\{x : C(x) = 1\}$?

[We wouldn't! When we first learned Grover, I had you assume $m = 1$. But in general, m could be anything!]

#SAT <u>problem</u>: Given C, determine m.

"SAT?": determine if $m = 0$ or $m \geq 1$.

[If you can do just the "SAT?" problem, you can also <u>find</u> satisfying inputs x efficiently... just do SAT? on $C(0, x_2, x_3, \ldots, x_n)$ & $C(1, x_2, x_3, \ldots, x_n)$ to see what a good first bit is, and repeat.]

<u>Recall</u>: Given "code" of C, can implement "Rot_θ" = "refl (i) then refl (ii)", which rotates $|u\rangle = (1, 1, \ldots, 1)$ by <u>mystery</u> angle θ in a <u>mystery</u> 2-dim plane containing $|u\rangle$.

$$\boxed{\cos\theta = 1 - \frac{2m}{N}} \implies \theta \approx 2\sqrt{\frac{m}{N}}$$ (assuming this is small)

<u>Goal</u>: Approximate θ, hence approximating m. (Approximate #SAT.)