Analysis

Let μ be the win prob on standard CHSH by these players on P_{ABE}.

If $\mu \approx \omega^* = \cos^2 \pi/8$, then rigidity tells us that Alice's answers a_t are close to uniform even w.r.t. Eve.

Crucially, A. & B. don't know if it's a test round or a gen. round. So their strategy must be fixed ahead of time and only depend on their current question.

Then passing the test can be analyzed by

let $X_t = [t \text{ is a test round}] \wedge [\text{CHSH won in round } t]$.

$$X = \sum_{t=1}^{n} X_t, \quad \text{then} \quad \mathbb{E}X = \mu p n.$$

We want to bound $\Pr[\mu \leq \omega^* - 2\eta \mid \text{not abort}]$

$$\Pr\left[\mu \le \omega^* - 2\eta \mid \text{not abort}\right]$$

$$= \Pr\left[\mu pn \le (\omega^* - 2\eta)pn \mid X \ge (\omega^* - \eta)pn\right]$$

$$\le \Pr\left[X - \mu pn \ge \eta pn\right]$$

$$= \Pr\left[X \ge \mathbb{E}X\left(1 + \frac{\eta}{\mu}\right)\right]$$ ↘ Chernoff

$$\le \exp\left(-\frac{\mu pn}{3} \cdot \frac{\eta^2}{\mu^2}\right)$$

$$= \exp\left(-\frac{p\eta^2 n}{3\mu}\right)$$

μ will end up being a constant so

$$\Pr\left[\mu \ge \omega^* - 2\eta \mid \text{not abort}\right] \ge 1 - 2^{-\Omega(p\eta^2 n)}.$$

By rigidity theorem strategy is $O(\sqrt{\eta})$ - close to ideal

so for suitable choice of constant ($\eta \sim 1/200$), then

$$H_{\min}(a_t \mid E) \geq 4/5.$$

Since $1-p \geq 1/2$ of the rounds are generation, get $\Omega(n)$ random coins with $H_{\min}(a_t \mid E) \geq 4/5$.

Can use randomness extraction to extract out $\Omega(n)$ near perfect bits.

Lastly, if δ is prob. of false certification, then $2^{-\Omega(pn)} \leq \delta$

so $p = \frac{1}{n} \log \frac{1}{\delta}$.

But wait how much randomness was spent?

Each round we flipped a coin with prob p. Costs $n \cdot \log 1/p$ coins.

That's too much.

Instead, let S be a random subset of size $2pn$ of $[2n]$.

Let $T = S \cap \{n\}$.

The claim is that the dist of T is very close to picking each round i.i.d.

But $\log \binom{2n}{2pn} \leq 2pn \log 1/p = 2 \log 1/\delta \left(\log n + \log 1/\delta \right)$.

So we have a procedure for converting

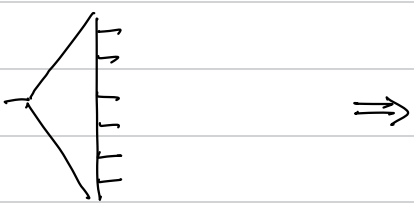
$O\left(\log 1/\delta \left(\log n + \log 1/\delta \right) \right)$ to $\Omega(n)$ randomness.

Caveats: state in lecture.

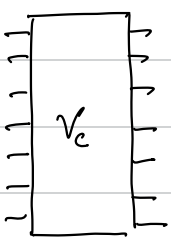
Quantum algs.

Next: 3-SAT on n variables, m clauses can be solved by a q. alg. with $O(m\sqrt{2^n})$ gates. (Grover's)

Precursor: classical comp. as a reversible ckt.



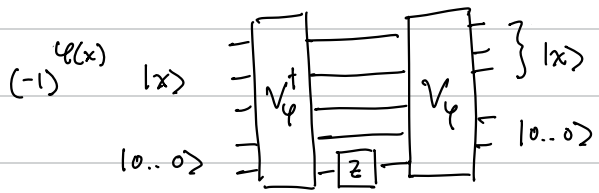
$C: \{0,1\}^n \to \{0,1\}$



$V_C: \{0,1\}^{n+|C|+1} \to \{0,1\}^{n+|C|+1}$.

For any 3-SAT formula φ, then $\exists$ a reversible ckt V which computes if y satisfies V.

V_φ has reversible implementation with $O(m)$ gates.



"Computing $\varphi(x)$ in the phase".

When the ancilla are set to 0, they are returned to 0 and so we can study algorithms that have access to P.

$$P : |x\rangle \longmapsto (-1)^{\varphi(x)} |x\rangle.$$

As we can implement P from elementary operations.

If φ is unsatisfiable $\varphi \equiv 0$ so $(-1)^{\varphi} = 1$.

Then, $U = \underline{\mathbb{1}}$.

If φ has exactly one solution z s.t. $\varphi(z) = 1$.

So, $$P|x\rangle = \begin{cases} -|x\rangle & \text{if } x = z \\ |x\rangle & \text{o.w.} \end{cases}$$

Equiv. $P = \mathbb{1} - 2|z\rangle\langle z|$

In general if $z_1, \ldots, z_k$ are the solutions, $P = \mathbb{1} - 2\left(\sum_{i=1}^{k} |z_i\rangle\langle z_i|\right)$.

Let's first come up with an alg. that works when there is a unique solution z. Generalize to multiple solutions as a problem set exercise.

Grover's algorithm:

We know $P_z = \mathbb{1} - 2|z\rangle\langle z|$ and we can implement P_z.

$-P_z$ is a reflection about the vector $|z\rangle$.

Build alg from 2 reflections: P_z and R.

$$R = 2|u\rangle\langle u| - \mathbb{1} \quad \text{where} \quad |u\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle.$$

$$H^{\otimes n} |0\rangle^{\otimes n} = |+\rangle^{\otimes n} = |u\rangle. \quad \text{So,}$$

$$R = H^{\otimes n} \left(2|0^n\rangle\langle 0^n| - \mathbb{1} \right) H^{\otimes n}.$$

$\mathbb{1} - 2|0^n\rangle\langle 0^n|$ is the phase unitary for the fn testing inequality with $|0^n\rangle$. So implementable.

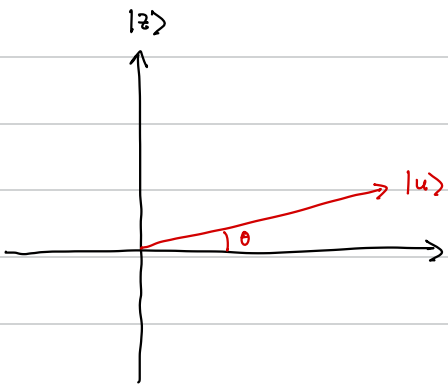
Algorithm (for choice of T):

Construct $(RP_z)^T |u\rangle$ and then measure in the standard basis.

There is a 2D subspace where all the action occurs.

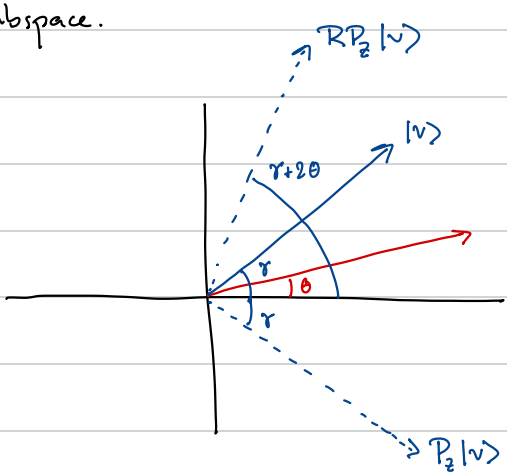
Consider the subspace spanned by $|z\rangle$ and $|u\rangle$. Both reflections preserve the subspace.

$$\langle z|u\rangle = \langle z|\left(\frac{1}{\sqrt{2^n}}\sum_x |x\rangle\right) = \frac{1}{\sqrt{2^n}}.$$



$$\theta = \arcsin\left(\frac{1}{\sqrt{2^n}}\right).$$

Lem $R \cdot P_z$ contributes a rotation by angle 2θ in this subspace.



So, $(RP_z)^T|u\rangle = |(2T+1)\theta\rangle$

Choose T s.t. $(2T+1)\arcsin\frac{1}{\sqrt{2^n}} \approx \pi/2$.

T must be integer! So state being measured is close to $|z\rangle$ but not exact.

Angle of final state is $\frac{\pi}{2} \pm 2\arcsin\left(\frac{1}{\sqrt{2^n}}\right) \leq \frac{\pi}{2} \pm \frac{2}{\sqrt{2^n}}$.

So, prob. that $|z\rangle$ is not measurement outcome $\leq 4/2^n$.

Furthermore $T = O(\sqrt{2^n})$.

Using that R can be implemented with $O(n)$ gates, P_z with $O(n)$ gates, this gives a

$$O(n\sqrt{2^n}) \text{ gate algorithm}$$

with success prob. $1 - 4/2^n$.