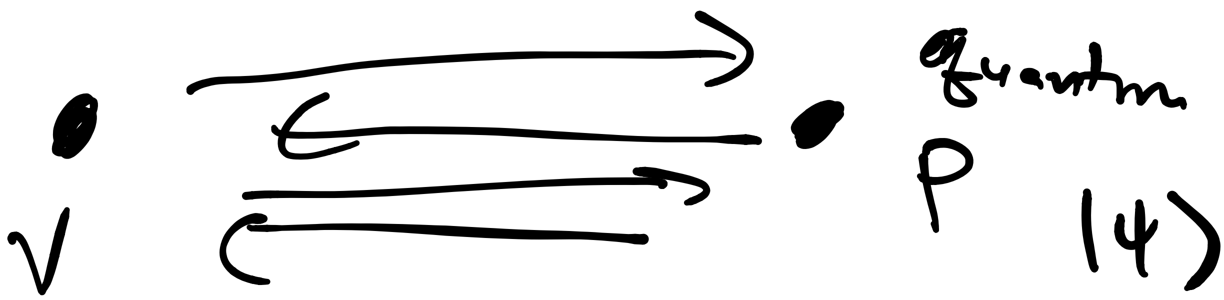
6.S979 Lecture 24

- Project due soon
- Volunteer to speak on Wednesday

Today: How do you verify that I computationally bounded prover is quantum?



Obs: P is indistinguishable from P' that classically simulates P (by brute force)

So computational assumption necessary

Q: What does it mean for P to be "quantum"?

A: Recall in CHSH / Magic square self-testing proofs, the key step was to show that provers have 2 incompatible measurements

$$A_0 A_1 \approx A_1 A_0$$

Say that P is "quantum" if it makes incompatible measurements

Technique due to Mahadev '18 (delegation of BQP)

Brakerski et al. '18

We'll start w/ baby protocol from Thomas Vidick

- - - - - - - - - - - - - -

Recall Simon's problem

$$f: \{0,1\}^n \longrightarrow \{0,1\}^n$$

2-to-1 function

$$f(x_0) = f(x_1) \text{ iff } x_0 = x_1 + s \mod 2, \quad s \in \{0,1\}^n$$

Q. alg. to find s:

$$\sum_{x \in \{0,1\}^n} |x\rangle |0^n\rangle$$

$$\xrightarrow{\text{query } f} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

$$\xrightarrow{\text{measure 2nd reg.}} \sum_{x : f(x) = y} |x\rangle |y\rangle$$

$$= \frac{1}{\sqrt{2}}\left(|x_0\rangle + |x_1\rangle\right)|y\rangle$$

$$= \frac{1}{\sqrt{2}}\underbrace{\left(|x_0\rangle + |x_0 + s\rangle\right)}_{\text{measure in } X \text{ basis}}|y\rangle$$

to get outcome

$d \in \{0,1\}^n$

<u>Claim:</u> $d \cdot s = 0 \mod 2$

<u>Ex:</u> $x_0 = 00$

$s = 10$

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)|y\rangle$$

$$|+\rangle|0\rangle \stackrel{?}{=} ||$$

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}$$

$$\frac{1}{\sqrt{2}}\left(\underset{00}{|++\rangle} + \underset{01}{|+-\rangle}\right)|y\rangle$$

$d \in \{00, 01\}$

Repeat to $d_1, \ldots, d_k$

$$d_1 \cdot s = 0$$
$$d_2 \cdot s = 0$$
$$\vdots$$
$$d_k \cdot s = 0$$

$\in \{0,1\}^n$

With $n-1$ linearly independent d's, can solve for s.

<u>Classically</u>: You need a lot of queries to distinguish 2-to-1 and 1-to-1 f (basically query till you find $x_0, x_1 \mapsto y$)

<u>However</u>: This holds for black box f. What about a concrete f?

Obs: If $f(x) = Ax$

$\ker(A) = \text{span}(s)$

But if I open the black box, a classical alg. can find s by Gaussian elimination

- - - - - - - - - - - - - - - -

Turning Simon's prob. into a protocol:

$$V \rightleftarrows P$$

1. V picks an f (pk, td) and sends it pk to P

2. P prepares $\sum_x |x\rangle |f(x)\rangle \to (|x_0\rangle + |x_1\rangle)|y\rangle$

If P demands clas return y

returns an image y of f.

3. With prob. 1/2 V either

- Asks P for a preimage
  P returns x
  V checks that $f(x) \stackrel{?}{=} y$

- Asks P for an "equation"
  P measures in the X basis to get d, returns
  V checks that $d \cdot (x_0 + x_1) = 0$

Properties of family $\mathcal{F}$

1) "Adaptive hard-core bit"
   Hard to find an x_0 and a $d \neq 0$ s.t. $d \cdot \underbrace{(x_0 + x_1)}_{s_{x_0}} = 0$

   (note s_{x_0} is not a fixed shift) (⇒ claw-free)

2) "Trapdoor"

Given f td, any y

can compute x_0, x_1 s.t. $f(x_0) = f(x_1) = y$

0) Can generate pk, td
public key

s.t. f_{pk} can be efficiently computed

2-to-1 "claw free"

Given pk, it is hard to find x_0, x_1, y s.t. $f_{pk}(x_0) = f_{pk}(x_1) = y$

3) $b : \{0,1\}^n \to \{0,1\}$

$y \leftarrow x_0$ $b(x_0) = 0$

$\nwarrow x_1$ $b(x_1) = 1$

Computable depending on pk.

Claim: • Suppose P succeeds in the protocol w/ $p = I$

- Prover's state at the end of step 2 is $|\psi\rangle$
- A: outcome $(-1)^{b(x)}$

  x is output of prover in step 3a.
- B: outcome $(-1)^{d \cdot (x_0 + x_1)}$

  d is output of prover in step 3b

Then A, B anticommute on $|\psi\rangle$

Specifically: $|\langle\psi|A_{+1} B A_{+1}|\psi\rangle + \langle\psi|A_{-1} B A_{-1}|\psi\rangle|$
$\leq$ negligible

$$A = \frac{I \pm A}{\sqrt{2}}$$

Pf idea: Suppose A, B are far from anticommuting. Then measure

A then B

$\downarrow$ gives you preimage

$\downarrow$ gives you a d

$\underbrace{}$

x_0, d s.t. $d(x_0 + x_1) = 0$

violates hardcore bit assumption

This shows that P is "quantum" "encoded" $|+\rangle$

$$\frac{1}{\sqrt{2}}(|x_0\rangle + |x_1\rangle)|y\rangle$$

What about "encoded"

$$\alpha|0\rangle + \beta|1\rangle$$

$$(\alpha|0\rangle|x_0\rangle + \beta|1\rangle|x_1\rangle)|y\rangle$$

- Suppose that $\forall y$

$$x_0 = (0, x_0')$$
$$x_1 = (1, x_1')$$

$b(x) =$ first bit of x

$$\alpha|0\rangle\sum_{x'}|x\rangle|0\rangle + \beta|1\rangle\sum_{x'}|x'\rangle|1\rangle$$

$$\xrightarrow{f} \sum_{x}(\alpha|0x\rangle|f(0x)\rangle + \beta|1x\rangle|f(1x)\rangle)$$

$$\xrightarrow{\text{measure image}} (\alpha|0x_0'\rangle + \beta|1x_1'\rangle)|y\rangle$$

Now the equation test doesn't quite make sense.

Mahadev protocol:

An extra ingredient
"extended claw-free function":
In addition to $\mathcal{F}$ of 2-to-1 functions
also have $\mathcal{G}$ of injective functions

- Given pk, can't tell whether
  it came from $\mathcal{G}$ or $\mathcal{F}$

Measurement protocol:

1) V generates pk, td
   either from $\mathcal{F}$ $(h=1)$
   or from $\mathcal{G}$ $(h=0)$
   w/ prob. $1/2$ each

   Send pk to P

2) P $\sum_x \left(\alpha|0x\rangle|f_{pk}(0x)\rangle + \beta|1x\rangle|f_{pk}(1x)\rangle\right)$

$\downarrow$ measures image

$h=0$ (injective)

$|bx\rangle|y\rangle$

$f_{pk}(bx)=y$

$h=1$ (2-to-1 function)

$\left(\alpha|0x_0\rangle+\beta|1x_1\rangle\right)|y\rangle$

P returns y

doesn't know which case it is in.