6.5979 Lecture 25

$$\sum_x |x\rangle |f(x)\rangle$$

$$\downarrow$$

$$\big(|x_0\rangle + |x_1\rangle\big)|y\rangle$$

"encoded" $|+\rangle$

$$\downarrow \text{ X basis measurement}$$

$$d \cdot (x_0 + x_1) = 0$$

Modifications to f

1) For any y, preimages of y look like $(0, x_0)$
$(1, x_1)$

$b(x) =$ first bit of x

2) A family $\mathcal{G}$ of <u>injective</u>

s.t. given pk

can't distinguish $f_{pk} \in \mathcal{F}$

$\mathcal{G}$

- - - - - - - - -

P_{none} has $\alpha|0\rangle + \beta|1\rangle$

pk

$$\sum_x (\alpha|0x\rangle + \beta|1x\rangle)|0^n\rangle$$

$$\Big\downarrow \text{compute } f_{pk}$$

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

"encoding" of $\alpha|0\rangle + \beta|1\rangle$

P measure 3rd register to get y
returns to V

<u>Case 1:</u> $f_{pk} \in \mathcal{F}$

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

<u>Case 2:</u> $f_{pk} \in \mathcal{G}$

$$|b\, x\rangle|y\rangle$$

Once P has revealed y, it has "committed" to $\alpha|0\rangle + \beta|1\rangle$

Measurement phase:

V decides to run "test round" or a "Hadamard round"

Test round:

Ask for preimage, receive bx

Check that $f_{pk}(bx) = y$

Hadamard:

Prover measures the first reg. in X basis (Hadamard basis) to get b', d

(abort if $b', d = 0^n$)

- If $f_{pk} \in \mathcal{F}$ ("X measmnt")
  Record the measurement outcome
  as $(-1)^{b' + d\cdot(x_0 + x_1)}$

- If $f_{pk} \in \mathcal{G}$ ("Z measmnt")
  Ignore b', d
  Record measurement outcome
  as $(-1)^b$

(b, x) is preimage of y that V found using td

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

Claim: Suppose P succeeds w/ prob. 1 − negl.

Then $\exists$ a 1-qubit state ρ

s.t. $\mathrm{tr}[\sigma_Z \rho] \simeq \mathbb{E}$[outcome of Z-meas in patrol]

$\mathrm{tr}[\sigma_X \rho] \simeq \mathbb{E}$[outcome of X-meas in patrol]

for 1-qubit, $\simeq$

for n-qubits, computationally indistinguishable

Why?

- For Z measurements, 1-to-1 function forces collapse in Z basis

- Prover cannot tell whether an X-basis or Z-basis measurement is being performed

- Consider 2-to-1 case

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

By security of f, prover doesn't know x_0, x_1, can't alter the state

Also: X outcome $= (-1)^{b' + d(x_0 + x_1)}$

Prover only controls

To get X outcome $= +1$ w.h.p., guess b', d s.t. $b' + d(x_0 + x_1) = 0$

But you can't b/c of hardcore bit assumption

Using measurement protocol to verify BQP [Mahadev '18]

- First need multiqubit version

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

$$\longrightarrow \sum_{u, x_1, \dots x_n} \alpha_u \left(|u_1 x_1\rangle |f(u_1 x_1)\rangle\right) \left(|u_2 x_2\rangle |f(u_2 x_2)\rangle\right)$$

$$\vdots$$

$$\xleftarrow{y_1, \dots y_n}$$

$$\longrightarrow \sum_u \alpha_u \left(|u_i, x_{u_i, y_i}\rangle |y_i\rangle\right)$$

$$\vdots$$

Verifier can measure any tensor product of X, Z on

the qubits
without revealing to prover

2) History state

$\langle\psi| H_c |\psi\rangle \leq E_{\text{thresh}}$

$\Longrightarrow$ BQP computation c accepts whp.

$H_c = \sum X \otimes Z \otimes X \ldots$

- Tell prover to prepare $|\psi_c\rangle$ with low energy
- Run the n-qubit measurement protocol for many randomly chosen terms in H_c

Compute estimate for $\langle H_c \rangle$