Lecture 19

2 APR 2014

With the error reduction technique from before, there are two undesirable aspects:

1) we need many copies of the quantum proof or witness
2) the quantum proof is damaged

Remarkably, there is a way around both of these problems due to an approach by Marriott & Watrous detailed in arXiv: cs/0506068.

To motivate this approach, consider a QMA proof system w/ perfect completeness, so that for all $x \in A_{yes}$, $\exists$ a state $|\psi\rangle$ such that $\Pr\{\text{accept}(x, \psi)\} = 1$ & $\forall x \in A_{no}$ + $|\psi\rangle$, $\Pr\{\text{accept}(x, \psi)\} \leq 1/3$

Let $\Pi_1 = |1\rangle\langle 1| \otimes I_{p(n)+n-1}$

"projection onto the accepting subspace"

$\Pi_0 = |0\rangle\langle 0| \otimes I_{p(n)+n-1}$

"projection onto the rejecting subspace"

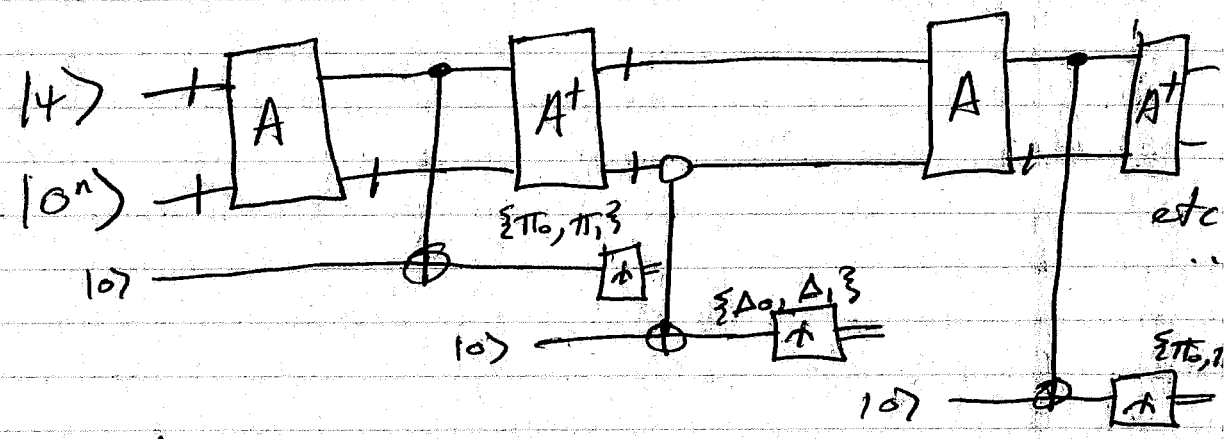
$\Delta_1 = I_{p(n)} \otimes |0^n\rangle\langle 0^n|$

"projection onto the valid input subspace"

$\Delta_0 = I_{p(n)+n} - \Delta_1$

"projection onto the invalid input subspace"

Consider the following circuit



idea is apply A, measure $\{\Pi_0, \Pi_1\}$, apply $A^\dagger$, measure $\{\Delta_0, \Delta_1\}$, repeat...

In the case of a YES instance, (assuming perfect completeness), we always get "1" as the measurement outcome. This is b/c the 1st measurement accepts w/ probability 1 + also, this measurement does not disturb the state at all. Then ~~when~~ the 2nd measurement will give 1 always, etc.

On the other hand, for a NO instance, the 1st measurement is successful only w/ $pr \leq \xi \cdot \xi \leq 1/3$, implying that the witness state is potentially damaged. Further measurements then do not succeed perfectly, the probability of accepting will fall off exponentially w/ the # of repetitions.

Now, QMA w/ perfect completeness is not known to be equal to QMA, so we need a different procedure to reduce error for QMA proof systems w/o perfect completeness.

For this purpose, we will use the same quantum procedure w/ a different classical post-processing.

We know that the maximum acceptance probability of the proof system is

$$\max_{|\psi\rangle} \left\| \Pi_1 A |\psi\rangle |0^n\rangle \right\|_2^2$$

$$= \max_{|\psi\rangle} \left\| \Pi_1 A \Delta_1 |\psi\rangle |0^n\rangle \right\|_2^2$$

$$= \max_{|\psi\rangle} \langle \psi | \langle 0 | \Delta_1 A^\dagger \Pi_1 A \Delta_1 |\psi\rangle |0^n\rangle$$

$$= \max_{|\phi\rangle} \langle \phi | \Delta_1 A^\dagger \Pi_1 A \Delta_1 |\phi\rangle$$

$$= \left\| \Delta_1 A^\dagger \Pi_1 A \Delta_1 \right\|_\infty \equiv p$$

So the best strategy of the prover is to supply $|\phi\rangle = |\psi\rangle |0^n\rangle$.

We want to figure out the form of the post-measurement states after every measurement.

So after 1st iteration, the states will be

$$|\gamma_0\rangle \equiv \frac{\Pi_0 A \Delta_1 |\phi\rangle}{\sqrt{1-p}}$$

$$|\gamma_1\rangle \equiv \frac{\Pi_1 A \Delta_1 |\phi\rangle}{\sqrt{p}}$$

We know that $\langle\gamma_1|\gamma_0\rangle = 0$ b/c $\Pi_0 \Pi_1 = 0$

Furthermore

$$\langle\gamma_1|\gamma_1\rangle = \frac{1}{p}\langle\phi| \Delta_1 A^\dagger \Pi_1 A \Delta_1 |\phi\rangle$$

$$= \frac{p}{p}\langle\phi|\phi\rangle \quad (|\phi\rangle \text{ is an eigenvector of } \Delta_1 A^\dagger \Pi_1 A \Delta_1 \text{ w/ eigenval. } p)$$

$$= 1$$

so $|\gamma_1\rangle$ is a unit vector

Also

$$\langle \gamma_0 | \gamma_0 \rangle = \langle \phi | \Delta_1 A^\dagger \Pi_0 A \Delta_1 | \phi \rangle / (1-p)$$

$$= \langle \phi | \Delta_1 A^\dagger (I - \Pi_1) A \Delta_1 | \phi \rangle \Big/ (1-p)$$

$$= \frac{1-p}{1-p} \langle \phi | \phi \rangle$$

$$= 1$$

so $|\gamma_0\rangle$ is also a unit vector

$\Rightarrow$ $\{|\gamma_0\rangle, |\gamma_1\rangle\}$ is an O.N. basis

The next step of the procedure is to apply $A^\dagger$ after applying A & measuring $\{\Pi_0, \Pi_1\}$, so we want to know the form of

$$A^\dagger |\gamma_0\rangle \quad \& \quad A^\dagger |\gamma_1\rangle$$

We will return to this question after a little development

Let $|\delta_1\rangle = \dfrac{\Delta_1 A^+ \pi_1 |\gamma_1\rangle}{\sqrt{p}}$

$|\delta_0\rangle = \dfrac{\Delta_0 A^+ \pi_1 |\gamma_1\rangle}{\sqrt{1-p}}$

Then $\langle\delta_1|\delta_0\rangle = 0$ b/c $\Delta_1 \Delta_0 = 0$

Also, $|\delta_1\rangle = |\phi\rangle$ b/c

$$|\delta_1\rangle = \frac{\Delta_1 A^+ \pi_1 |\gamma_1\rangle}{\sqrt{p}}$$

$$= \left(\frac{\Delta_1 A^+ \pi_1}{\sqrt{p}}\right)\left(\frac{\pi_1 A \Delta_1}{\sqrt{p}}\right)|\phi\rangle$$

$$= \frac{1}{p}\,\Delta_1 A^+ \pi_1 A \Delta_1 |\phi\rangle$$

$$= \frac{p}{p}|\phi\rangle = |\phi\rangle$$ (b/c $|\phi\rangle$ is an eigenvector of $\Delta_1 A^+ \pi_1 A \Delta_1$)

Furthermore, $|\gamma_1\rangle$ is an eigenvector of $\pi_1 A \Delta_1 A^+ \pi_1$ w/ eigenval. p b/c

$$\pi_1 A \Delta_1 A^+ \pi_1 |\gamma_1\rangle = \pi_1 A \Delta_1 A^+ \pi_1 \left(\frac{\pi_1 A \Delta_1 |\phi\rangle}{\sqrt{p}}\right)$$

$$= \pi_1 A \Delta_1 \frac{p}{\sqrt{p}}|\phi\rangle$$

$$= p\left(\frac{\Pi_1 A \Delta_1 |\phi\rangle}{\sqrt{p}}\right) = p\,|\gamma_1\rangle$$

All of this implies that

$$\langle \delta_1|\delta_1\rangle = \frac{1}{p}\langle \gamma_1|\,\Pi_1 A \Delta_1 A^\dagger \Pi_1\,|\gamma_1\rangle$$

$$= \frac{p}{p}\langle \gamma_1|\gamma_1\rangle$$

$$= 1$$

$\therefore\ |\delta_1\rangle$ is a unit vector

By similar reasoning

$$\langle \delta_0|\delta_0\rangle = \frac{1}{1-p}\langle \gamma_1|\,\Pi_1 A \Delta_0 A^\dagger \Pi_1\,|\gamma_1\rangle$$

$$= \frac{1}{1-p}\langle \gamma_1|\,\Pi_1 A (I-\Delta_1) A^\dagger \Pi_1\,|\gamma_1\rangle$$

$$= \frac{1-p}{1-p}\langle \gamma_1|\gamma_1\rangle = 1$$

so $|\delta_0\rangle$ is a unit vector

$\Rightarrow$ $\{|\delta_0\rangle, |\delta_1\rangle\}$ is an O.N. basis

So if we get $|\gamma_1\rangle$ after the first measurement, apply $A^\dagger$, followed by a measurement of $\{\Delta_0, \Delta_1\}$ we get post-measurement states $|\delta_0\rangle$ & $|\delta_1\rangle$

Now if we get $|\delta_1\rangle$ & apply A, what is the form of $A|\delta_1\rangle$?

Consider that

$$A|\delta_1\rangle = (\Pi_0 + \Pi_1) A |\delta_1\rangle$$

$$= \Pi_0 A |\delta_1\rangle + \Pi_1 A |\delta_1\rangle$$

$$= \Pi_0 A \frac{\Delta_1 A^\dagger \Pi_1}{\sqrt{p}} |\gamma_1\rangle +$$

$$\Pi_1 A \frac{\Delta_1 A^\dagger \Pi_1}{\sqrt{p}} |\gamma_1\rangle$$

$$= \Pi_0 A \frac{\Delta_1 A^\dagger \Pi_1 A \Delta_1}{\sqrt{p}\cdot\sqrt{p}} |\phi\rangle$$

$$+ \frac{p}{\sqrt{p}} |\gamma_1\rangle$$

$$= \Pi_0 A |\phi\rangle + \sqrt{p}\,|\gamma_1\rangle$$

$$= \sqrt{1-p}\,|\gamma_0\rangle + \sqrt{p}\,|\gamma_1\rangle$$

Since $\{|\delta_0\rangle, |\delta_1\rangle\}$ is an O.N. basis & A is unitary, $A|\delta_0\rangle$ has the form

$$A|\delta_0\rangle = -\sqrt{p}\,|\gamma_0\rangle + \sqrt{1-p}\,|\gamma_1\rangle$$

So this is

$$A|\delta_1\rangle = \sqrt{1-p}\,|\gamma_0\rangle + \sqrt{p}\,|\gamma_1\rangle$$

$$A|\delta_0\rangle = -\sqrt{p}\,|\gamma_0\rangle + \sqrt{1-p}\,|\gamma_1\rangle$$

Applying A^+ to this gives

$$|\delta_1\rangle = \sqrt{1-p}\,A^+|\gamma_0\rangle + \sqrt{p}\,A^+|\gamma_1\rangle$$

$$|\delta_0\rangle = -\sqrt{p}\,A^+|\gamma_0\rangle + \sqrt{1-p}\,A^+|\gamma_1\rangle$$

Multiply 2nd by $\sqrt{1-p}$ + 1st by $\sqrt{p}$

$$\sqrt{1-p}\,|\delta_0\rangle = -\sqrt{p(1-p)}\,A^+|\gamma_0\rangle + (1-p)A^+|\gamma_1\rangle$$

$$\sqrt{p}\,|\delta_1\rangle = \sqrt{p(1-p)}\,A^+|\gamma_0\rangle + pA^+|\gamma_1\rangle$$

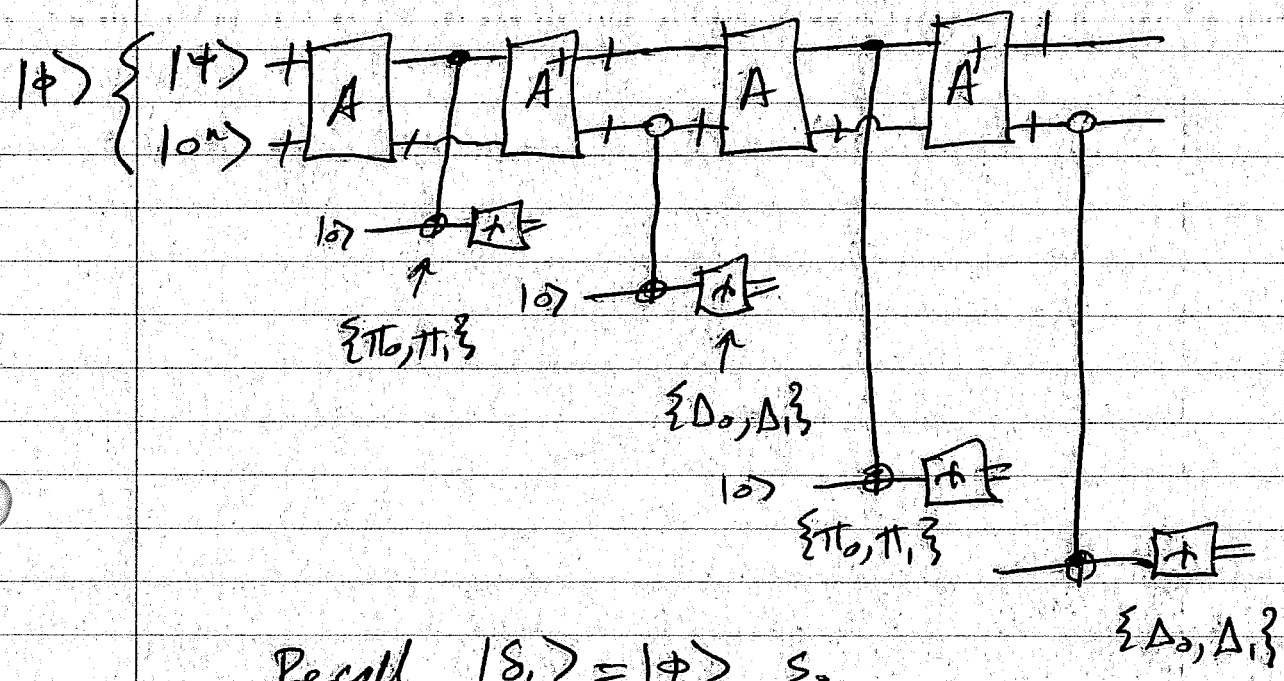
Add them to And that

$$A^+|\gamma_1\rangle = \sqrt{1-p}\,|\delta_0\rangle + \sqrt{p}\,|\delta_1\rangle$$

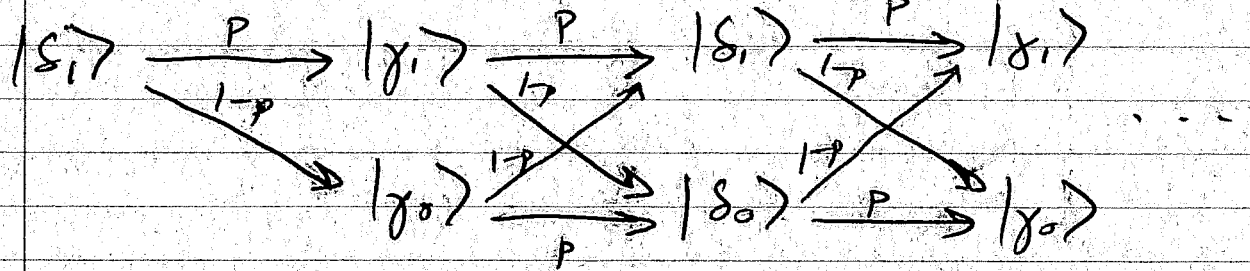
&

$$A^+|\gamma_0\rangle = -\sqrt{p}\,|\delta_0\rangle + \sqrt{1-p}\,|\delta_1\rangle$$

Now, from these equations we can say what happens from the following circuit:



Recall $|\delta_1\rangle = |\phi\rangle$, s.



~~So the probability of any~~

Idea is to keep track of each transition, i.e., whether one measurement outcome is different from the previous.

Let y_i denote the outcome of the i^{th} measurement, w/ $y_0 = 1$ since we start w/ $|\xi_1\rangle$ as the initial state

Then set

$$z_i = \begin{cases} 1 & \text{if } y_i = y_{i-1} \\ 0 & \text{if } y_i \neq y_{i-1} \end{cases}$$

The probability for any particular sequence is

$$z^N = (z_1, \ldots, z_N)$$

$$p^{w(z^N)} (1-p)^{N - w(z^N)}$$

where w counts the number of ones.

Then we compute

$$\frac{1}{N} \sum_{i=1}^{N} z_i$$ & accept if this is larger than $\frac{a+b}{2}$

We know that $p \geq a$ in the case of a YES instance, while $a - \left(\frac{a+b}{2}\right) = \frac{a-b}{2} = \frac{1}{2q(n)}$

So using Chernoff bound as before,
& setting $N = 8q^2(n)\, r(n)$

for $r \in$ poly

the probability of acceptance is
larger than $1 - 2^{-r(n)}$

Also, as a bonus, observe that
we get the witness back after
about $O(\frac{1}{p^2})$ repetitions
of the procedure.

For the case of a NO instance,
we need to use the fact that

$\forall |\psi\rangle$ $\Pr\{\text{accept}(x, \psi)\} \leq b(n)$

& any $|\psi\rangle$ can be written in
the eigenbasis of $\Delta_1 A^\dagger \Pi_1 A \Delta_1$
& a fact from linear algebra known
as Jordan's lemma & Chernoff bound
to conclude that

$\Pr\{\text{accept}\} \leq 2^{-r(n)}$

& $\frac{a+b}{2} \geq b$

$\frac{a+b}{2} - b = \frac{a-b}{2}$