1 Introduction

Fact 1 $SZK \subseteq AM \cap c_0AM$. The right hand side is unlikely to contain $NP$.

In this lecture we will propose an interactive proof system for the 3-coloring graph problem (which we know to be $NP$-complete), and we will begin the proof that shows that our interactive proof system is computational zero-knowledge. So we will try to show $NP \subseteq CZK$ - (note that given Fact 1, here we have to relax statistical zero knowledge to computational zero knowledge).

2 IP System for 3-Coloring

Recall that 3-Coloring is defined as the language of graphs

$$\{G \mid \exists \text{3-coloring } \alpha : [n] \rightarrow [3] \text{ of } G\}$$

Now we present our proposed IP construction for the 3-Coloring problem. We have a prover-verifier pair $(P_{3\text{COL}}, V_{3\text{COL}})$. We also have a computationally hiding, statistically binding commitment scheme $(\tilde{S}, \tilde{R})$. The IP proceeds as follows:

1. $P_{3\text{COL}}$ finds the 3-Coloring $\alpha$ for $G$.
2. $P_{3\text{COL}}$ samples a permutation $\pi$ on $[3]$ (the set of colors).
3. $P_{3\text{COL}}$ computes the new 3-Coloring $\beta = \pi \circ \alpha$.
4. $P_{3\text{COL}}$ samples keys $sk_1, sk_2, \ldots sk_n$.
5. $P_{3\text{COL}}$ computes the commitment message $c_i = \tilde{S}(1^k, sk_i, \beta(i))$ for each $i$.
6. $P_{3\text{COL}}$ sends $\vec{c} = [c_1, c_2, \ldots c_n]$ to $V_{3\text{COL}}$.
7. $V_{3\text{COL}}$ samples an edge $(u, v) \leftarrow E$.
8. $V_{3\text{COL}}$ sends $(u, v)$ to $P_{3\text{COL}}$.
9. $P_{3\text{COL}}$ returns $sk_u, sk_v$ to $V_{3\text{COL}}$.
10. $V_{3\text{COL}}$ computes $\chi_u = \tilde{R}(1^k, sk_u, c_u)$, and $\chi_v = \tilde{R}(1^k, sk_v, c_v)$.
11. $V_{3\text{COL}}$ checks whether $\chi_u \neq \chi_v$, and $\chi_u, \chi_v \in [3]$.

This IP construction is complete and sound, with acceptance probability $\leq 1 - \frac{1}{|E|}$. 

20-1
Theorem 2 \((P_{3\text{COL}},V_{3\text{COL}})\) is CZK (assuming that \((\tilde{S}, \tilde{R})\) is secure).

Here we present a partial proof of the Theorem, to be completed in the next lecture.

We construct a simulator \(S\) with black box access to some verifier \(V^*\). For some \(G \in 3\text{COL}\), the steps for computing \(S^{V^*}(G)\) are as follows:

1. Sample a random tape \(r_{V^*}\) for \(V^*\).
2. Sample a random coloring \(\gamma : [n] \rightarrow [3]\).
3. Sample keys \(sk_1, \ldots, sk_n\).
4. Compute \(c_i = \tilde{S}(1^k, sk_i, \gamma(i))\) for each \(i\).
5. Obtain \((u, v)\) from sending the commitment vector \(\vec{c}\) to \(V^*(G, r_{V^*})\).
6. If \(\gamma(u) = \gamma(v)\), go back to step 1.
7. Output \((r_{V^*}, \vec{c}, (u, v), (sk_u, sk_v))\).

We will now analyze this simulator. Suppose by way of contradiction that there exists probabilistic polynomial time distinguisher \(D\) that distinguishes \(S^{V^*}(G)\) from \(\text{VIEW}_{V^*}((P_{3\text{COL}}, V^*)\langle G \rangle)\) with probability \(\delta(k)\).

Let \(E_{(u^*, v^*)}\) denote the event \(V^*\) outputs \((u^*, v^*)\).

Now, by averaging, there exists \((u^*, v^*) \in E\) such that

\[
\left| \Pr[D(S^{V^*}(G)) = 1 \land E_{(u^*, v^*)}] - \Pr[D(\text{VIEW}_{V^*}((P_{3\text{COL}}, V^*)\langle G \rangle)) = 1 \land E_{(u^*, v^*)}] \right| \geq \frac{\delta(k)}{|E|}
\]

Now given this \(D\), we can construct an attacker \(A\) that attacks \((\tilde{S}, \tilde{R})\).

To compute \(A_{(G, \alpha)}((d_{a,i})_{a \in [3], i \in [n]})\) given a graph \(G\), a 3-Coloring \(\alpha\), the attacker attacks the decommitment message \(d\) in the following steps:

1. Pick a random permutation \(\pi : [3] \rightarrow [3]\).
2. Sample \(sk_{u^*}, sk_{v^*}\).
3. Construct the commitment vector

\[
c_i = \begin{cases} 
\tilde{S}(1^k, sk_i, \pi(\alpha(i))) & \text{if } (i = u^*) \lor (i = v^*) \\
\ d_{\pi(\alpha(i))} & \text{otherwise}
\end{cases}
\]

4. Give \(\vec{c}\) to \(V^*(G)\), obtain \((u, v)\).
5. If \((u, v) \neq (u^*, v^*)\), output 0.
6. Output \(D(\vec{c}, (u^*, v^*), (sk_{u^*}, sk_{v^*}))\).

The idea here is that \(d\) can either be a commitment to the string with the pattern "123123123..." repeated \(n\) times, in which case it corresponds to \(D(\text{VIEW}_{V^*})\), or it is a commitment to \(3n\) i.i.d. random samples from \([3]\), in which case it corresponds to \(D(S^{V^*})\).
Lemma 3

\[ Pr[A(123\text{-}\text{challenge}) = 1] = Pr[D(\text{VIEW}_V) = 1 \land \mathcal{E}_{(u^*, v^*)}] \]

Lemma 4

\[ \left| Pr[A(\text{random challenge}) = 1] - Pr[D(S^{V'}) = 1 \land \mathcal{E}_{(u^*, v^*)}] \right| \leq \frac{\delta(k)}{2|E|} \]

We want to show that

\[ |Pr[A(123\text{-}\text{challenge}) = 1] - Pr[A(\text{random challenge}) = 1]| \]

is non negligible. Using the triangle equality (\(|x - y| \geq ||x| - |y||\)) and the above two lemmas, we can reformulate the statement above as

\[ \left| Pr[D(\text{VIEW}_{V'}) = 1 \land \mathcal{E}_{(u^*, v^*)}] - Pr[D(S^{V'}) = 1 \land \mathcal{E}_{(u^*, v^*)}] \right| \leq \frac{\delta(k)}{2|E|} \]

Proof of Lemma 4: Given \( \gamma : [n] \to [3] \), define \( q_\gamma \) to be the probability that \( Q_\gamma \) outputs 1, where \( Q_\gamma(1^k) \) is computed as follows:

1. Sample \( sk_1, \ldots, sk_n \).
2. Compute \( c_i = \tilde{S}(1^k, sk_i, \gamma(i)) \).
3. Send \( \vec{c} \) to \( V^*(G) \) to obtain \((u, v)\).
4. Output 1 iff \((u, v) = (u^*, v^*), \gamma(u^*) = \gamma(v^*) \), and \( D(\vec{c}, (u^*, v^*), (sk_{u^*}, sk_{v^*})) = 1 \).

Now we can rewrite

\[ Pr[A(\text{random challenge}) = 1] = \sum_{\gamma} \frac{q_\gamma}{3^3} \]

Now we want to rewrite

\[ Pr[D(S^{V'}) = 1 \land \mathcal{E}_{(u^*, v^*)}] \]

First we see that, for a particular transcript \( tr \),

\[ Pr[S^{V'} \text{ outputs } tr] = \sum_{i=1}^{\infty} Pr[S^{V'} \text{ outputs } tr \text{ at round } i] \]

\[ = \sum_{i} Pr[S^{V'} \text{ outputs } tr \text{ at round } 1] Pr[i-1 \text{ retries}] \]

\[ = \frac{1}{Pr[\text{do not retry}]} Pr[S^{V'} \text{ outputs } tr \text{ at round } 1] \]

Here the last step is obtained by convergence of geometric series. This allows us to rewrite

\[ Pr[D(S^{V'}) = 1 \land \mathcal{E}_{(u^*, v^*)}] = \sum_{tr \text{ with } (u^*, v^*)} \frac{1}{Pr[\text{do not retry}]} Pr[S^{V'} \text{ outputs } tr \text{ at round } 1] Pr[D(tr) = 1] \]

\[ = \frac{1}{Pr[\text{do not retry}]} \sum_{\gamma | \gamma(u^*) \neq \gamma(v^*)} \frac{1}{3^n} q_\gamma \]

\[ \square \]

20-3