1 Overview

- Projection PCP
  The verifier makes two queries to the proof, upon seeing the answer to the first query, there is at most one acceptable answer to the second query (projection).

- Parallel Repetition

We’ll call the probability a uniform test (random \((x, y), (x', y) \in E\)) is satisfied for the best \(a: X \rightarrow \Sigma_X\), the value:

\[
\text{val}(G) := \max_{a: X \rightarrow \Sigma_X} \Pr \left[ \pi_e(a(x)) = \pi_{e'}(a(x')) \neq \bot \right] \tag{1}
\]

**Theorem 1 (Projection PCP).** For any \(\varepsilon > 0\), it’s NP-hard given a label-cover instance \(G\) to distinguish between \(\text{val}(G) = 1\) and \(\text{val}(G) = \varepsilon\).

**Remark.** A nature definition of “\(G\)’s value” is

\[
\text{val}'(G) := \max_{a: X \rightarrow \Sigma_X, c: Y \rightarrow \Sigma_Y} \Pr \left[ \pi_e(a(x)) = c(y) \right] \tag{2}
\]

Another definition of “\(G\)’s value” is (3) in Theorem 3, let’s denote it by \(\text{val}''(G)\).

As \(\text{val}(G) = 1 \iff \text{val}'(G) = 1 \iff \text{val}''(G) = 1\), \(\text{val}(G) = \Theta(\text{val}(G''))\) (it’s not clear whether \(\text{val}(G) = \text{val}(G'')\)), The difference between \(\text{val}(G)\) in (1) and (3) doesn’t matters. The rest of this lecture would define \(\text{val}(G)\) as in (3).
Theorem 2. Convert any PCP to Label-cover problem lout the soundness error becomes a constant \( \approx 1 \). 
\[
\text{PCP}[O(\log n), O(1)] \subseteq \text{PCP}[O(\log n), 2]
\]

Strongest projection PCP we know reduces SAT on formula of size \( n \) to label cover problem on graphs of size \( n^{1+o(1)} \) poly\((\frac{1}{\varepsilon})\), alphabet size \( \exp(\frac{1}{\varepsilon}) \), such that

- Satisfiable formulas are mapped to \( G \) with \( \text{val}(G) = 1 \)
- Unsatisfiable formulas are mapped to \( G \) with \( \text{val}(G) \leq \varepsilon \)

There exists a trivial case where there exists \( e = (x, y), e' = (x', y) \in E \) such that the image of \( \pi_e \) and \( \pi_{e'} \) has no intersection, then a polynomial-time verifier could discover \( \text{val}(G) < 1 \).

Besides this trivial case, \( \text{val}(G) \geq \frac{1}{|\Sigma_X|^2} \) by considering a random proof. So better soundness must imply a blow up in alphabet size.

3 Parallel Repetition

3.1 Two-Prover One-Round Game

A 2-query projection PCP is correlated with a two-prover one-round label cover game.

Input: Label Cover problem

0. There are two provers cannot communicate with each other.
1. Verifier randomly chosen \( e = (x, y), e' = (x', y) \in E \)
2. Verifier sent \( x, x' \) to two provers resp. and receive answers \( a, a' \)
3. Verifier check whether \( \pi_e(a) = \pi_{e'}(a') \neq \bot \)

Theorem 3. The probability a verifier accept a two-prover one-round game with the optimal provers is

\[
\text{val}(G) := \max_{a,b:X \rightarrow \Sigma_X} \Pr_{(x,y),(x',y) \in E} \left[ \pi_e(a(x)) = \pi_{e'}(b(x')) \neq \bot \right]
\]

We want to transfer an instance in PCP game to projection PCP game such that

\[
G \mapsto G'
\]

\[
\text{val}(G) = 1 \implies \text{val}(G') = 1
\]

\[
\text{val}(G) \leq 0.999 \implies \text{val}(G') \leq \varepsilon
\]

3.2 Parallel Repetition

The naïve transfer is \( G \mapsto G^k \),

Input: Label Cover problem

0. There are two provers cannot communicate with each other.
1. Verifier randomly chosen \( e_i = (x_i, y_i), e'_i = (x'_i, y_i) \in E \) for \( i = 1, \ldots, k \)
2. Verifier sent \((x_1, \ldots, x_k), (x'_1, \ldots, x'_k)\) to two provers resp. and receive answers \((a_1, \ldots, a_k), (a'_1, \ldots, a'_k)\)
3. Verifier check whether \(\pi_e(a_i) = \pi_{e'}(a'_i) \neq \bot\) for all \(i = 1, \ldots, k\)

We know \(\text{val}(G^k) \geq \text{val}(G)^k\) as the provers could answer each queries independently. For sequentially repetition, the inequality is tight. One might hope \(\text{val}(G^k) \approx \text{val}(G)^k\). However, \(\text{val}(G^k)\) can be much higher than \(\text{val}(G)^k\). E.g. consider the “non-interactive agreement” game

- **Prover** \(A, B\) receive independent bit \(x, x' \in \{0, 1\}\) resp.
- **Both provers** report \((\text{player, bit})\)
- The task is to agree on a prover and correctly identify its bit

One could check that \(\text{val}(G) = \frac{1}{2}\), it’s surprising that \(\text{val}(G^2) = \frac{1}{2}\). One possible strategy: prover \(A\) report \((B, x_2), (A, x_2)\) given its input \((x_1, x_2)\) and prover \(B\) report \((B, x'_1), (A, x'_1)\) given its input \((x'_1, x'_2)\). Then prover succeeds if \(x'_1 = x_2\).

If this is the story, we could not prove strong PCP theorem. However, there exists a transfer \(G \mapsto G^*\) such that \(\text{val}(G) = \text{val}(G^*)\) and \(\text{val}((G^*)^k) \approx \text{val}(G^*)^k\)

### 3.3 $\delta$-Fortification $G \mapsto G^*$

**Theorem 4.** There is a transfer (“fortification”) \(G \mapsto G^*\) such that \(\text{val}((G^*)^k) \leq (\text{val}(G) + \varepsilon)^k + \varepsilon k\).

Suppose that the \(G\) verifier picks random \(e = (x, y), e' = (x', y) \in E\).

1. \(G^*\) verifier also picks random \(x_1, \ldots, x_k, x'_1, \ldots, x'_k \in X\).
2. Sends \((x_1, \ldots, x_s, x'_1, \ldots, x'_s)\) to first prover, receive \(a_1, \ldots, a_s\) the real query \(x\) is placed in a random index, \(s = \text{poly}\left(\frac{1}{\delta}\right)\)
3. Sends \((x'_1, \ldots, x'_s)\) to second prover, receive \(a'_1, \ldots, a'_s\)
4. Checks \(\pi_e(a) = \pi_{e'}(a') \neq \bot\)

**Lemma 5.** For any \(S, T \subseteq X^{s+1}\) such that \(|S|, |T| \geq \delta |X|^{s+1}\)

\(\text{val}(G^*_{S,T}) \leq \text{val}(G) + \delta\)

where \(G^*_{S,T}\) is \(G^*\) conditioned on \(x \in S, x' \in T\).

**Theorem 6.** When \(\delta < \frac{\varepsilon}{2|\Sigma_Y|}\),

\(\text{val}((G^*)^2) \leq \text{val}(G)(\text{val}(G) + \varepsilon) + \varepsilon\)

**Proof.** Let \(y_1, y_2, e_1 = (x_1, y_1), e_2 = (x_2, y_2), e'_1 = (x'_1, y'_1), e'_2 = (x'_2, y'_2)\) picked by verifier, \(a_1, a_2, a'_1, a'_2\) answers of provers.

Fix \(y_1, x_1, x'_1, \sigma \in \Sigma_Y\). Let

\[S = \{x_2 \mid \pi_{e_1}(a_1) = \sigma\} \quad T = \{x'_2 \mid \pi_{e'_1}(a'_1) = \sigma\}\]

The total contribution of all \((y_1, x_1, x'_1, \sigma)\) such that \(|S| \leq \delta |X|^{s+1}\) or \(|T| \leq \delta |X|^{s+1}\), is at most

\[2|\Sigma_Y| \cdot \delta \leq \varepsilon.\]

If \(|S|, |T| \geq \delta |X|^{s+1}\), by Lemma 5, \(\text{val}(G^*_{S,T}) \leq \text{val}(G) + \delta\). Therefore

\[\Pr[\text{verifier accept in } (G^*)^2] \leq \text{val}(G) \cdot \left(\text{val}(G) + \delta\right) + \varepsilon\]
References

