25 Worksheet for Lecture 25 (Parallel Repetition)

Problem 25.1. In this problem, we will see that parallel repetition of PCPs might fail. Recall that an independent set S of a graph $G = (V, E)$ is a set of vertices such that for every $v_1, v_2 \in S$, $(v_1, v_2) \notin E$. Let the independent set language be

$$\text{IS} \coloneqq \{\, (G = (V, E), n) \mid G \text{ has an independent set of size } n \text{ and } n \geq 2 \,\} \quad .$$

Given a candidate list of n vertices, one can probabilistically check that it is an independent set of size n by verifying that a random pair of vertices in the list is distinct and non-adjacent. Formally, $\mathsf{PCP} \coloneqq (P, V)$ is a PCP for IS, where P and V are defined as follows.

- $P(G, n, S)$: Output $\pi \coloneqq S$.
- $V^{\pi}(G, n)$:
  1. Sample $i, j \in [n]$ such that $i < j$.
  2. Query π at i-th vertex first, j-th vertex second. Let v_i and v_j be the answers.
  3. Accept if and only if $v_i \neq v_j$ and $(v_i, v_j) \notin E$.

Let $t \in \mathbb{N}$ and V_t be the t-wise parallel repetition of V.

1. Show that PCP has perfect completeness and soundness error $\epsilon_{\mathsf{s}}(G, n) \leq 1 - 1/\binom{n}{2}$.
2. Show that the second query $(j_1, \ldots, j_t)$ of V_t doesn't contain 1, that is, for every $k \in [t]$, $j_k \neq 1$. *Hint: Recall that V_t works as follows.*
   - $V_t^{\Pi}(G, n)$:
     (a) *For $k \in [t]$, sample $i_k, j_k \in [n]$ such that $i_k < j_k$.*
     (b) *Query Π at $(i_1, \ldots, i_t)$-th vertex first, $(j_1, \ldots, j_t)$-th vertex second. Let $(v_{i_1}, \ldots, v_{i_t})$ and $(v_{j_1}, \ldots, v_{j_t})$ be the answers.*
     (c) *Accept if and only if for every $k \in [t]$, $v_{i_k} \neq v_{j_k}$ and $(v_{i_k}, v_{j_k}) \notin E$.*
3. Let $(G, n) \notin \text{IS}$ be such that G is not a complete graph. Using the previous item, show that there exists a malicious prover $\tilde{P}_t$ for t-wise parallel repetition of PCP outputting Π such that $V_t^{\Pi}(G, n)$ accepts Π with probability $1 - \left(\frac{n-1}{n}\right)^t$. *Hint: Construct Π such that $V_t^{\Pi}(G, n)$ accepts if and only if the first query $(i_1, \ldots, i_t)$ of V_t contains 1, that is, $i_k = 1$ for some $k \in [t]$.*
4. Deduce that $\lim_{t \to \infty} (\epsilon_{\mathsf{s}})_t(G, n) = 1$, where $(\epsilon_{\mathsf{s}})_t$ is the soundness of t-wise parallel repetition of PCP.
5. *Bonus:* Remember that consistent parallel repetition drives the error to 0. Discuss why $\tilde{P}_t$ doesn't cheat so well against the consistent parallel repetition verifier.

Problem 25.2. In this exercise, we investigate the relation between parallel repetition of PCPs and another proof system called MIPs.

For simplicity, we restrict ourselves to PCPs with a non-adaptive verifier and query complexity 2.

The MIP projection $\mathsf{MIP} \coloneqq ((\mathcal{P}_1, \mathcal{P}_2), \mathcal{V})$ of a PCP $\mathsf{PCP} \coloneqq (P, V)$ is the MIP where the interaction between $\mathcal{P}_1, \mathcal{P}_2, \mathcal{V}$ on an instance $\mathbb{x}$ and provers' joint randomness τ is defined as follows.

1. $\mathcal{V}$ samples verifier randomness $\rho \in \{0,1\}^{\mathsf{r}}$.
2. $\mathcal{V}$ computes the queries i, j of $V(\mathbb{x}; \rho)$ and sends i to $\mathcal{P}_1$, j to $\mathcal{P}_2$.
3. For $i \in [2]$, $\mathcal{P}_i$ computes $\pi \coloneqq P(\mathbb{x}; \tau)$.
4. $\mathcal{P}_1$ sends $a_1 \coloneqq \pi[i]$ to $\mathcal{V}$.
5. $\mathcal{P}_2$ sends $a_2 \coloneqq \pi[j]$ to $\mathcal{V}$.
6. $\mathcal{V}$ accepts if and only if $V(\mathbb{x}; \rho)$ given the oracle answers a_1, a_2.

Let $\mathsf{PCP} \coloneqq (P, V)$ be a PCP for a language $\mathcal{L}$ where V is non-adaptive. Let MIP be the MIP projection of PCP as defined above. Let β be the soundness error of MIP. For $t \in \mathbb{N}$, let $(\epsilon_{\mathsf{s}})_t$ the soundness of t-wise parallel repetition of PCP. Let $\mathbb{x} \notin \mathcal{L}$.

We will show that $\lim_{t\to\infty}(\epsilon_{\mathsf{s}})_t(\mathbb{x}) = 0$ if and only if $\beta(\mathbb{x}) < 1$.

1. Show that if $\beta(\mathbb{x}) < 1$, then $\lim_{t\to\infty}(\epsilon_{\mathsf{s}})_t = 0$:
   (a) Show that for every PCP, we have $\beta \geq \epsilon_{\mathsf{s}}$, where ϵ_{s} is the soundness error of the PCP, and β is the soundness error of the MIP projection of the PCP.
   (b) Observe that t-wise parallel repetition of MIP can be viewed as the MIP projection of t-wise parallel repetition of PCP. Deduce that $(\epsilon_{\mathsf{s}})_t \leq \beta_t$, β_t is the soundness of t-wise parallel repetition of MIP.
   (c) Use that parallel repetition drives the soundness error of non-adaptive MIPs to 0 to conclude that $\lim_{t\to\infty}(\epsilon_{\mathsf{s}})_t = 0$.
2. Show that if $\beta = 1$, then $\lim_{t\to\infty}(\epsilon_{\mathsf{s}})_t \geq 1/2^{\mathsf{r}}$:
   (a) For every $t \in \mathbb{N}$, show that there exists a malicious prover $\tilde{P}_t$ outputting Π such that $V_t^{\Pi}(\mathbb{x})$ accepts Π with probability at least $1/2^{\mathsf{r}}$. *Hint: Let $\tilde{P}_t$ fix a query pair (i, j) and set $\Pi[(i_1, \ldots, i_t)]$ using $\mathcal{P}_1$ or $\mathcal{P}_2$ depending on the value of i_1.*
3. *Bonus: Verify that the MIP projection of the PCP for* IS *in the previous question has soundness error* 1 *if the graph is not complete.*