CS 40: Computational Complexity

Sair Shaikh

November 9, 2025

Problem 30. Prove that for every constant q, we have

$$\mathrm{PCP}_{s:1}[r, q] \subseteq \mathrm{PCP}_{1-(1-s)/q:1}[r + \lceil \log q \rceil, 2]_{\{0,1\}^q}.$$

Solution. Let $\Sigma = \{0,1\}^q$. Let $A \in \mathrm{PCP}_{s:1}[r, q]$, and let V be the associated verifier.

For each random string r, V makes q queries to π to recieve q binary answers. We wish to replace this with one super-query receiving a member of a larger alphabet Σ. Towards this goal, let $i_{1,u}, \cdots, i_{q,u}$ be the indices that V would query given a proof string π when run with randomness u. We can construct a table $T \in \Sigma^*$ from a proof string π with $T[u] = (\pi(i_{1,u}), \cdots, \pi(i_{q,u}))$. Provided the table is filled honestly, a verifier V' run with randomness u can query $T[u]$ once and recieve the same information as V, and thus enact the same protocol.

However, a table may be filled dishonestly, i.e. not come from encoding a proof string as described above. To check for this, we additionally encode π in Σ^* by appending $q-1$ 0s to each character, and then check one random bit of $T[u]$ against this π. Then, given any proof of this format, (T, π) (concatenated as strings), the verifier V' follows the following protocol:

1. Use the first r bits of randomness, u, to query $T[u]$.
2. Use u to determine the original query locations of V. Use the last $\lceil \log q \rceil$ bits of randomness to pick an index $j \in [1, \cdots, q]$. Query $\pi(i_{j,u})$. These steps are non-adaptive as we can always pre-compute and then query.
3. Simulate V's verification process on $T[u]$, reject if V would have rejected.
4. Check $T[u][j]$ against the extra bit $\pi(i_{j,u})$ to check $T[u]$ for consistency against π. Reject if different, otherwise accept.

We claim that this protocol shows that $A \in \mathrm{PCP}_{1-(1-s)/q:1}[r + \lceil \log q \rceil, 2]_{\{0,1\}^q}$. The claim on the alphabet, query complexity, randomness complexity, as well as probabilistic polynomial runtime are clear. Thus, we only need to verify the completeness and the soundness.

First, assume $x \in A$. Then there exists a proof π^* that makes V accept x with certainity. Using π^*, we can construct T^* "honestly" as described above. Then, V' run on (T^*, π^*) passes Step 3 with certainity, as it recieves the same responses as V and enacts the same computation. Moreover, since T^* is constructed to be consistent with π^*, Step 4 passes with certainity. Thus, this protocol has completeness 1 when deciding A.

Now consider $x \notin A$. Let (T, π) be an arbitrary proof string. We claim that V' rejects x with probability $\geq \frac{1-s}{q}$. Observe that V rejects x with probability $\geq 1 - s$. Let $R \subseteq \{0,1\}^r$ be the set of values for the randomness that make V reject (with proof string π). Then $\mathbf{Pr}[u \in R] \geq 1 - s$ by definition. We claim that if $u \in R$, then V' rejects x (using randomness u for the first r bits) with probability $\geq \frac{1}{q}$. We condition on whether $T[u]$ is consistent with the corresponding values in π.

1. If $T[u]$ is consistent with π, then V' recieves the same responses as V would (run with randomness u and proof π). As $u \in R$, V would reject, thus V' would reject in Step 3 with certainity.
2. If $T[u]$ is not consistent with π, then there is at least 1 place where it is inconsistent. Thus, the probability of picking j that leads to Step 4 rejecting is $\geq \frac{1}{q}$. Thus, the probability of rejecting is Step 3 or Step 4 is $\geq \frac{1}{q}$.

Thus, we have shown that:

$$\mathbf{Pr}[V'(x, u, T, \pi) = 0 | u \in R] \geq \frac{1}{q}$$

Then, we can use the law of total probability and the bounds computed before to compute:

$$\begin{aligned}\mathbf{Pr}[V'(x, u, T, \pi) = 0] &\geq \mathbf{Pr}[V'(x, u, T, \pi) = 0 | u \in R] \, \mathbf{Pr}[u \in R] \\ &\geq \left(\frac{1}{q}\right)(1 - s) = \left(\frac{1 - s}{q}\right)\end{aligned}$$

Thus, the soundness error is as claimed:

$$\mathbf{Pr}[V'(x, u, T, \pi) = 1] \leq 1 - \left(\frac{1 - s}{q}\right)$$

Thus, we have shown $A \in \mathrm{PCP}_{1-(1-s)/q:1}[r + \lceil \log q \rceil, 2]_{\{0,1\}^q}$.