Yosef Goren

December 24, 2022

1 MIP vs PCP

1.1

1.2

Let V_p be a PCP prover with perfect completness, soundness error $\frac{1}{2}$ and q queries.
Define a $2 - message$, MIP protocol as follows:

- V_m (Verifier):
  - Given x, ask V_p for it's queries on x. Denote these $Q := \{Q_i \mid i \in [q]\}$
  - $\forall i \in [q]$ ask P_i for response to Q_i. Denote $R := \{R_i \mid i \in [q]\}$.
  - Return R to V_p.
- P_i (Prover i):
  - Given an input x, and a query Q_i, if $x \in L$, there exists a PCP proof to convince V_p, denote it H.
  - Use Q_i as index in H (as a bolean array), and return $R_i := H[Q_i]$.
- Completness:
  If $x \in L$, then P_i will all return the correct awnser to the query in H (the PCP proof), thus the awnser to V_p's query will be as if it has queried itself like in the original PCP protocol; thus due to the soundness of the PCP protocol, V_m will accept x.
- Soundness: Assume $\exists P_1^*, P_2^*, ..., P_q^*$ s.t.

  $$\Pr_{r \xleftarrow{\$}}[(V, P_1^*, ..., P_q^*)(x) = 1] \geq \frac{1}{2}$$

  From here we can construct

2 Tensor Codes

2.1 A Characterization

- $$(C_1 \otimes C_2)(A) = C_1(C_2A^T)^T = C_1(AC_2^T) = (C_1A)C_2^T = (C_2(C_1A)^T)^T$$