Foundations and Frontiers of Probabilistic Proofs (Summer 2021)
Worksheet B.6: Exponential-Size PCPs
Date: 2021.08.03

In this worksheet we construct a linear PCP of *linear size* for a specific NP language.

The language R1CS($\mathbb{F}$) (rank-1 constraint satisfiability over the field $\mathbb{F}$) consists of all instances $\mathbb{x} = (A, B, C, v)$, where $A, B, C \in \mathbb{F}^{m \times n}$ are *coefficient matrices* and $v \in \mathbb{F}^{n'}$ for $n' \leq n$ is a *public input*, such that there exists a full assignment $z \in \mathbb{F}^n$ such that $Az \circ Bz = Cz$ and $z = (v, w)$ for some $w \in \mathbb{F}^{n-n'}$; here $\circ$ denotes the entry-wise product.

This condition represents a system of m equations: for each $i \in [m]$, the i-th equation is specified by the i-th rows of A, B, C and has the form $\langle A[i,*], z\rangle \cdot \langle B[i,*], z\rangle = \langle C[i,*], z\rangle$. In other words, each equation is a specific expression of degree 2 that involves three linear combinations, and so R1CS($\mathbb{F}$) can be viewed as a restriction of QESAT($\mathbb{F}$).

Problem 1. (LPCP for R1CS) Prove, following the steps below, that R1CS($\mathbb{F}$) has a linear PCP over $\mathbb{F}$ with the following parameters: soundness error $\epsilon = O(\frac{m}{|\mathbb{F}|})$, proof length $\mathsf{l} = O(n + m)$, query complexity $\mathsf{q} = 4$, and randomness complexity $\mathsf{r} = 1$ (1 random field element). Recall that a linear PCP π of length l answers a query $y \in \mathbb{F}^{\mathsf{l}}$ with the inner product $\langle y, \pi\rangle$.

1. Use arithmetization to reformulate the condition "$Az \circ Bz = Cz$" as a single univariate polynomial identity that involves the polynomial $\prod_{i \in H}(X - i)$ (for some domain H of size m) and the low-degree extensions of columns of A, B, C.
2. Describe a linear-length 4-query linear PCP (the proof format and LPCP verifier) for R1CS($\mathbb{F}$) that checks this polynomial identity at a random point, taking the public input v into account.
3. Prove the completeness and soundness of the linear PCP.

Problem 2. (R1CS is NP-complete) Prove that, for every finite field $\mathbb{F}$, R1CS($\mathbb{F}$) is NP-complete. *Hint: reduce from* CSAT *(satisfiable boolean circuits), and use v to enforce satisfiability.*