Exercise 3 – Due 19.1.2006

Purpose

Gain better understanding of PCPs of proximity for codes. Show non-triviality of the Raz Parallel Repetition Theorem.

Definitions

- Let Pair-Binary-RS be the following pair language. The explicit input is a triple $(\mathbb{F}_{2^k}, S, d)$, where S is a $\mathbb{F}_2$-linear sub-space of $\mathbb{F}_{2^k}$ of size $n = |S|$. The implicit input is a function $p : S \to \mathbb{F}_{2^k}$. A pair $((\mathbb{F}_{2^k}, S, d), p)$ is in the language iff $p \in \mathrm{RS}(F, S, d)$.

- Let Pair-Binary-$\mathrm{RS}_{1/8}$ be the restriction of Pair-Binary-RS to explicit inputs of the form $(\mathbb{F}_{2^k}, S, d = |S|/8)$.

- Recall the definition of a code tester and a locally testable code (see Section 2.1.2 in lecture notes). We use the notation there. Let $\delta_0 \in (0, 1)$ be a *proximity parameter* and $s \in (0, 1)$ be a *soundness constant*. A family of codes $\mathcal{C} = \{C_k \mid k \in \mathbb{N}^+\}$ is called a *weak* $(t(k), r(k), q(k), s, \delta_0)$-LTC if it has an $(t(k), r(k), q(k))$-local-tester T, with the following weaker notion of soundness:

  - **Weak soundness** If $\Delta^*(w, C_k) \geq \delta_0$ then $\mathbf{Pr}_R\big[T^w\big[1^k; R\big] = \mathsf{accept}\big] \leq 1 - s$

Questions

1. Recall in class we stated (and sketched a proof of) the following claim:

$$\textsc{Pair-Binary-RS}_{1/8} \in \mathbf{PCPP}\left(\begin{array}{ll} \mathsf{length} & = \ell(n) = n\mathrm{poly}(\log(n)) \\ \mathsf{randomness} & = r(n) = \log(\ell(n)) + \mathcal{O}(1) \\ \mathsf{query} & = q(n) = \mathcal{O}(1) \\ \mathsf{time} & = t(n) = n^{\mathcal{O}(1)} \\ \mathsf{completeness} & = 1 \\ \mathsf{soundness} & = s(\delta, n) = \delta/\mathrm{poly}(\log(n)) \end{array}\right),$$

   Using this claim, show the same holds for arbitrary degree (with essentially the same parameters). In other words, prove:

$$\textsc{Pair-Binary-RS} \in \mathbf{PCPP}\left(\begin{array}{ll} \mathsf{length} & = \mathcal{O}(\ell(n)) \\ \mathsf{randomness} & = r(n) + \mathcal{O}(1) \\ \mathsf{query} & = \mathcal{O}(q(n)) \\ \mathsf{time} & = \mathcal{O}(t(n)) \\ \mathsf{completeness} & = 1 \\ \mathsf{soundness} & = \min\{\delta/2, s(\delta/16, n)\} \end{array}\right).$$

2. Let $\mathcal{C} = \{C_k \mid k \in \mathbb{N}^+\}$ be a family of $[n(k), k, d(k)]_{F_k}$ linear codes (over alphabet F_k, not neccessarily of size k). Let

$$\mathrm{Pair}{-}\mathcal{C} = \Big\{(1^k, w) : w \in \mathrm{Image}(C_k)\Big\}.$$

   Suppose

$$\mathrm{Pair}{-}\mathcal{C} \in \mathbf{PCPP}\left(\begin{array}{ll} \mathsf{length} & = \ell(k) \\ \mathsf{randomness} & = r(k) \\ \mathsf{query} & = q(k) \\ \mathsf{time} & = t(k) \\ \mathsf{completeness} & = 1 \\ \mathsf{soundness} & = s(\delta, k) \end{array}\right),$$

   and $\delta > 0 \Rightarrow s(\delta, k) > 0$ for all k. Prove: For every $\delta_0, \epsilon \in (0,1)$ there exists a family $\mathcal{C}' = \{C'_k \mid k \in \mathbb{N}^+\}$ which is a weak $\big(t'(k), r'(k), q'(k), \frac{1}{2}, \delta_0\big)$-LTC. Furthermore, the distance of C'_k is at least $(1-\epsilon)$ time the distance of C_k. What is the blocklength of C'_k? What is the query complexity? Taking $\mathcal{C} = \textsc{Pair-Binary-RS}$, what parameters for a weak LTC do we get?

3. Consider the following two player, one round, game. Verifier chooses uniformly and independently $q_0, q_1 \in \{0,1\}$ and sends q_0 to P_0 and q_1 to P_1. Prover P_i responds with two bits, denoted a_i, b_i. Verifier accepts iff $a_0 = a_1$ and $b_0 = b_1$ and $b_{a_1} = q_{a_1}$.

   - Prove an upper bound on the success probability of the game.
   - Prove a lower bound that matches the upper bound from the previous question, on the success probability of the two-fold parallel repetition of the game.