Foundations and Frontiers of Probabilistic Proofs (Summer 2021)
Worksheet B.2: Linearity Testing
Date: 2021.07.28

Problem 1. (Affine function testing) A function $f\colon \mathbb{F}^n \to \mathbb{F}$ is *affine* if there exists a vector $a \in \mathbb{F}^n$ and constant $\beta \in \mathbb{F}$ such that $f(x) = \sum_{i\in[n]} a_i x_i + \beta$. Design and analyze a 4-query test for the set of affine functions. *Hint: reduce the problem to linearity testing, and rely on the BLR test for linear functions.*

Problem 2. (Self-correcting linear functions) Prove that linear functions can be self corrected. Namely, prove that there exists a probabilistic oracle algorithm A such that: if $f\colon \mathbb{F}^n \to \mathbb{F}$ is δ-close to a linear function $p(x_1,\ldots,x_n)$ (for $\delta < \frac{1}{2}(1-\frac{1}{|\mathbb{F}|})$) then for every $a \in \mathbb{F}^n$ it holds that $\Pr_r[A^f(a;r) = p(a)] \geq 1 - 2\delta$.

1. Prove that that distance between every two linear functions is $1-\frac{1}{|\mathbb{F}|}$. That is, if $p(x_1,\ldots,x_n)$ and $p'(x_1,\ldots,x_n)$ are two different linear functions, then $\Pr_{a\leftarrow\mathbb{F}^n}[p(a) = p'(a)] = \frac{1}{|\mathbb{F}|}$.
2. Prove that there is a single linear function $p(x_1,\ldots,x_n)$ that is δ-close to f, if $\delta < \frac{1}{2}\cdot(1-\frac{1}{|\mathbb{F}|})$.
3. Suggest a probabilistic oracle algorithm A (with small, constant, query complexity) that self-corrects f.
4. Prove the algorithm's correctness.

Problem 3. (Group-homomorphism testing) We study how the BLR test extends to testing if a function is close to a group homomorphism. Let G, H be two finite abelian groups, and let $f\colon G \to H$ be a function. Consider the following test: sample $x, y \in G$ at random and check that $f(x) + f(y) = f(x+y)$. Clearly, if f is a group homomorphism then the test accepts with probability 1.

1. Suppose that $f\colon G \to H$ is δ-far from the set of group homomorphisms from G to H. Prove that the test rejects f with probability at least $3\delta - 6\delta^2$. *Hint: compare to the homomorphism closest to f.*
2. The above bound is not useful when δ approaches $\frac{1}{2}$ or is larger than $\frac{1}{2}$. Prove that if the test rejects f with probability $\mu < \frac{1}{6}$ then f is 2μ-close to some homomorphism $h\colon G \to H$. (Note that the contrapositive of this statement addresses the flaw.) *Hint: use self-correction.*