Foundations and Frontiers of Probabilistic Proofs (July 2023)
Worksheet 7: Linearity Testing
Date: July 20, 2023

Problem 1. (Basics of linear codes) Let $C: \mathbb{F}^k \to \mathbb{F}^n$ be a *linear* code (i.e., $C(x) + C(y) = C(x + y)$ and $C(\alpha x) = \alpha C(x)$ for every $x, y \in \mathbb{F}^k$ and $\alpha \in \mathbb{F}$).

1. Prove that the (relative) distance of C is $\delta = \frac{\min_{x \neq 0} |C(x)|}{n}$, where $|y| = |\{ i \in [n] : y_i \neq 0 \}|$ is the *Hamming weight* of y.

   What can you say about the cardinality of (the image of) C if $\delta > 0$? What about when $\delta = 0$?

2. Show that there exists $G \in \mathbb{F}^{n \times k}$ such that $C(x) = G \cdot x$ for every $x \in \mathbb{F}^k$. (In other words, C is the image of the *generator matrix* G.)

3. Show that there exists $H \in \mathbb{F}^{(n-k) \times n}$ such that $C(x) \cdot H^{\intercal} = 0$ for every $x \in \mathbb{F}^k$. (In other words, C is the kernel of the *parity-check matrix* H.)

4. Give an example of a code with $k = 2$ and $n = 3$ (over the finite field of your choice). Compute its relative distance and show that the generator and parity-check matrices are not unique by exhibiting G_1, G_2, H_1, H_2 satisfying items 2 and 3 with $G_1 \neq G_2$ and $H_1 \neq H_2$.

Problem 2. (Hadamard code) The code $\mathrm{Had}: \mathbb{F}^k \to \mathbb{F}^{|\mathbb{F}|^k}$ is defined as $\mathrm{Had}(x) := (\langle x, y \rangle)_{y \in \mathbb{F}^k}$ (i.e., the encoding of x is the linear function $\mathrm{Had}(x): \mathbb{F}^k \to \mathbb{F}$ where $\mathrm{Had}(x)(y) = \langle x, y \rangle$). Show that Had has relative distance $1 - 1/|\mathbb{F}|$. (Despite its exponential block length, this code has important features that will be useful in this course: *local testability* and *local decodability*.)

Problem 3. (Affine function testing) A function $f: \mathbb{F}^n \to \mathbb{F}$ 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 4. (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 $f: \mathbb{F}^n \to \mathbb{F}$ 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 5. (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 $f: G \to H$ 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 $f: G \to H$ 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 $h: G \to H$. (Note that the contrapositive of this statement addresses the flaw.) *Hint: use self-correction.*