**6.842 Randomness and Computation** March 14, 2022

# Lectures on Linearity Testing

*Lecturer: Ronitt Rubinfield* *Scribe: Yuchong Pan*

**Definition 1.** Let $G$ and $H$ be finite groups. Let $f : G \to H$. Then $f$ is said to be *linear* (i.e., is a *homomorphism*) if for all $x, y \in G$,

$$f(x) +_H f(y) = f\left(x +_G y\right).$$

For all $\varepsilon > 0$, $f$ is said to be $\varepsilon$-*linear* if there exists a linear function $g : G \to H$ such that $f$ and $g$ agree on at least $1 - \varepsilon$ fraction of inputs in $G$, i.e.,

$$\mathop{\mathbb{P}}_{x \in G}[f(x) = g(x)] \geq 1 - \varepsilon,$$

or equivalently,

$$\frac{|\{x \in G : f(x) = g(x)\}|}{|G|} \geq 1 - \varepsilon.$$

Algorithm 1 is a natural test for the linearity of a function $f : G \to H$, where $G$ and $H$ are finite groups.

```
repeat ? times
    pick random x, y ∈ G
    test f(x) + f(y) = f(x + y)
```

**Algorithm 1:** A natural test for the linearity of a function $f : G \to H$, where $G$ and $H$ are finite groups.