Lectures on Linearity Testing

Lecturer: Ronitt Rubinfield *Scribe: Yuchong Pan*

1 Linearity Testing

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 $x, y \in G$,

$$f(x) +_H f(y) =_H f(x +_G y).$$

For all $\varepsilon > 0$, f is said to be ε*-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
    if f(x) + f(y) ≠ f(x + y) then
        return "fail"
return "pass"
```

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

Observation 2. *Let G be a finite group. For all $a, y \in G$, $\mathbb{P}_{x \in G}[y = a + x] = 1/|G|$. In other words, if x is chosen uniformly from G, then $a + x$ is also uniformly distributed in G.*

Proof. Since only $x = y - a$ satisfies $y = a + x$, then $\mathbb{P}_{x \in G}[y = a + x] = \mathbb{P}_{x \in G}[x = y - a] = 1/|G|$. $\square$

2 Self-Correcting (Random Self-Reducibility)

Theorem 3. *Let G be a fintie group. Let $f : G \to G$ be a function such that there exists a linear function $g : G \to G$ and that $\mathbb{P}_{x \in G}[f(x) = g(x)] \geq 7/8$. Then for all $x \in G$, $g(x)$ can be computed with only $O(\log(1/\beta))$ calls to f (with at most β probability of error).*

Given input $x \in G$ and black box access to f, we define a *self corrector* in Algorithm 2.

Proposition 4. $\mathbb{P}[\mathit{output} = g(x)] \geq 1 - \beta$.

```
for i ← 1, ..., C · log(1/β) do
    pick y uniformly in G
    answer_i ← f(y) + f(x − y)
output the most common answer
```

Algorithm 2: A self corrector for a 1/8-linear function $f : G \to G$ on input x, where G is a finite group.

Proof. Let y be chosen uniformly in G. By Observation 2, $x - y$ is also uniformly distributed in G. Therefore,

$$\mathbb{P}[f(y) \neq g(y)] \leq \frac{1}{8}, \qquad \mathbb{P}[f(x-y) \neq g(x-y)] \leq \frac{1}{8}.$$

By the union bound,

$$\begin{aligned} \mathbb{P}[f(y) + f(x-y)] = g(x)] &= \mathbb{P}[f(y) + f(x-y)] = g(y) + g(x-y)] \\ &\geq \mathbb{P}[f(y) = g(y), f(x-y) = g(x-y)] \\ &\geq 1 - \left(\frac{1}{8} + \frac{1}{8}\right) = \frac{3}{4}. \end{aligned}$$

This implies that $\mathbb{P}[answer_i = g(x)] \geq 3/4$ for all i. The proof is hence complete. $\square$

3 Coppersmith's Example

Let $m \in \mathbb{N}$. Let $f : \mathbb{Z}_m \to \mathbb{Z}_m$ be defined by

$$f(x) = \begin{cases} 1, & \text{if } x \equiv 1 \pmod 3, \\ 0, & \text{if } x \equiv 0 \pmod 3, \\ -1, & \text{if } x \equiv 2 \pmod 3. \end{cases}$$

The graph of f is plotted in Figure 1.

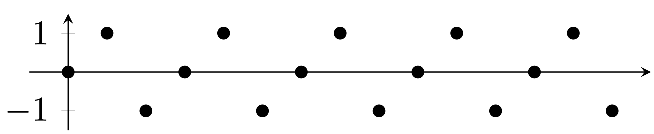

Figure 1: The graph of Coppersmith's example.

Note that the closest linear function $g : \mathbb{Z}_m \to \mathbb{Z}_m$ to f is given by $g(x) = 0$ for all $x \in \mathbb{Z}_m$, so f is 2/3-far from being linear. Note that f fails for $x, y \in \mathbb{Z}_m$ with $x \equiv y \equiv 1 \pmod 3$ or $x \equiv y \equiv 2 \pmod 3$, and passes for all other $x, y \in \mathbb{Z}_m$. Therefore, the *rejection probability of the linearity test* for f, denoted by δ_f, is given by

$$\delta_f = \mathop{\mathbb{P}}_{x,y \in \mathbb{Z}_m}[f(x) + f(y) \neq f(x+y)] = \frac{2}{9}.$$

Fortunately, 2/9 is the threshold; in other words, Coppersmith's example is the worst example. If $\delta_f < 2/9$ for some function $f : G \to G$ and finite group G, then f must be δ_f-close to being linear.

4 Fourier Analysis for Boolean Functions

The *n-dimensional Boolean hypercube* $\{0,1\}^n$ can be interpreted as having $n+1$ layers, where the i^{th} layer consists of n-bit Boolean strings with i ones for each $i \in \{0,\ldots,n\}$, and where two n-bit Boolean strings in consecutive layers are joined by an edge if they differ at exactly one bit. What are linear maps $\{0,1\}^n \to \{0,1\}$?

Definition 5. Given $x, y \in \{0,1\}^n$, the *inner product* of x and y is defined to be

$$x \cdot y = \sum_{i=1}^{n} x_i y_i \pmod 2.$$

Note that addition modulo 2 is the XOR operation. Linear functions on $\{0,1\}^n$ are of the form

$$L_a(x) = a \cdot x, \qquad \text{for fixed } a \in \{0,1\}^n,$$

or, alternatively,

$$L_A(x) = \sum_{i \in A} x_i \pmod 2, \qquad \text{for fixed } A \subset [n].$$

Therefore, there are exactly 2^n linear functions on $\{0,1\}^n$.

To simplify the presentation, we change the notation by letting $a \mapsto (-1)^a$ for $a \in \{0,1\}$ and by changing addition $a+b$ to multiplication $(-1)^a(-1)^b = (-1)^{a+b}$. Hence, the condition of linearity $f(a)+f(b) = f(a \oplus b)$ for all $a, b \in \{0,1\}^n$ is changed to $f(a) \cdot f(b) = f(a \odot b)$ for all $a, b \in \{1,-1\}^n$, where $(x_1,\ldots,x_n) \oplus (y_1,\ldots,y_n) = (x_1+y_1,\ldots,x_n+y_n)$ denotes the bitwise XOR (i.e., addition modulo 2) of two n-bit Boolean strings, and $(x_1,\ldots,x_n) \odot (y_1,\ldots,y_n) = (x_1 \cdot y_1,\ldots,x_n \cdot y_n)$ denotes the bitwise multiplication of two n-bit $\{1,-1\}$-valued strings. Moreover, linear functions on $\{1,-1\}^n$ are of the form

$$\chi_S(x) = \prod_{i \in S} x_i, \qquad \text{for fixed } S \subset [n].$$

Now, the linearity test accepts if and only if $f(x) \cdot f(y) = f(x \odot y)$. Then

$$f(x)f(y)f(x \odot y) = \begin{cases} 1, & \text{if the test accepts,} \\ -1, & \text{if the test rejects.} \end{cases}$$

Therefore, the indicator variable for the event that the test rejects is given by

$$\mathbb{1}_{f(x)\cdot f(y) \neq f(x \odot y)} = \frac{1 - f(x)f(y)f(x \odot y)}{2} = \begin{cases} 0, & \text{if the test accepts,} \\ 1, & \text{if the test rejects.} \end{cases}$$

This allows us to express the rejection probability in terms of the indicator variable:

$$\delta_f = \mathop{\mathbb{P}}_{x,y \in \{1,-1\}^n}[f(x) \cdot f(y) \neq f(x \odot y)] = \mathop{\mathbb{E}}_{x,y \in \{1,-1\}^n}\left[\frac{1 - f(x)f(y)f(x \odot y)}{2}\right].$$