Lecture 24

Lecturer: Ronitt Rubinfeld *Scribe: Ivaylo Riskov*

1 Recap

$$f : \{0,1\}^n \to \{0,1\}$$

$x < y$ if $\forall i, x_i \le y_i$

f is monotone if $\forall x \le y, f(x) \le f(y)$

We define a violating edge (x, y) such that $y = x \oplus e_i, x < y, f(x) > f(y)$. We can use the following tester: Pick $O\left(\frac{n}{\epsilon}\right)$ edges and reject if any violate.

Finally, we started the proof of the following theorem:

Theorem 1 *The above tester passes monotone functions and fails ϵ-far from monotone functions (must chnage f on at least ϵ fraction of the inputs) with probability at least $3/4$.*

2 Proof of Theorem

Claim 2 *If f is ϵ-far from monotone it has at least $\epsilon 2^n$ violating edges.*

Proof of claim: By contrapositive: assume f has less than $\epsilon 2^n$ violating edges.

Let $f^{(i)}$ be f after the i-th phase. That is, phase i fixes edges in i-th direction without ruining lower direction edges.

Inductive assumption: $f^{(i-1)}$ has no violating edges in directions $1 \ldots i-1$.

Definition 3 *Consider the following definitions:*

- $H_0 \leftarrow$ *nodes x such that $x_i = 0$*
- $H_1 \leftarrow$ *nodes x such that $x_i = 1$*
- $M_i \leftarrow$ *violating edges in i-th direction.*
- $U_1 \leftarrow$ *violating edges in H_0 having common endpoint with M_i*
- $U_2 \leftarrow$ *other violating edges in H_0*
- V_1, V_2 *same as U_1 and U_2, but for H_1*

From the above definition the set of violating edges in $f^{(i-1)}$ is $M_i \cup U_1 \cup U_2 \cup V_1 \cup V_2$.

Notes:

1. Edges in i-th direction, i.e. of the form $(x, x \oplus e_i)$, give perfect matching between H_0 and H_1.
2. Violating edges in M_i have 1 in H_0 and 0 in H_1.
3. Need to change 1 to 0 in H_0 or 0 to 1 in H_1.

If $|U_1| \le |V_1|$: modify $f^{(i-1)}$ to get $f^{(i)}$ by setting $f^i(y) = 1, \forall (x, y) \in M_i$.

This fixes all edges in M_i and V_1. All edges in U_1, U_2, and V_2 stay the same. However, this can create new violating edges. We will show that $|V_1|$ is at most the number of new violating edges, so in $f^{(i)}$ we fixed all edges in M_i and did not create more violating edges. We also need to show that no violations occured in directions $1, \ldots, i-1$. Note that only edges in H_1 can become violated.

Claim 4 *At most $|U_1|$ violating edge are created. (and therefore at most $|V_1|$ violating edges, because in this case $|U_1| \leq |V_1|$.*

Proof of claim: Let (x, y) be a violating edge in M_i and (y, z) be a non-violating edge in H_1 that became violating.

$$x = y \oplus e_i \quad z = y \oplus e_j = x \oplus e_i \oplus e_j$$

$f(x) = 1$ and $f(y)$ was 0, but is now 1. Consider the node $w = x \oplus e_j$ and so $z = w \oplus e_i$. However, $f(z)$ was not changed (we don't change nodes from 1 to 0) and so (w, z) must not have been in M_i, i.e. $(w, z) \notin M_i$. Therefore, $f(w) = 0$ which means that (x, w) is a violating edge. This gives a 1-to-1 mapping between new violating edges (y, z) to old violating edges in U_1 ■

The change of violating edges at i-th step is $-|M_i| - |V_1| + \#$ new violations. From the above claim, the number of new violations is at most $|U_1| \leq |V_1|$, so in total we got rid of at least M_i violating edges. Therefore after all n phases the total number of fixed violating edges is $|\bigcup M_i|$.

Note that no violations in previous directions are introduced. Suppose that $(z, y), z = y \oplus e_j, j < i$ is new violating in previous direction. Then $(x, w), w = x \oplus e_j, j < i$ was also violating, which contradicts the invariant for $f^{(i-1)}$.

■

3 Linearity testing

We now turn our attention to the problem of linearity testing.

Consider a mapping $f : G \to H$.

Definition 5 *f is "linear" or a "homomorphism" if*

$$\forall x, y \quad f(x) + f(y) = f(x + y)$$

.

Definition 6 *f is ϵ-linear if we can change it on at most ϵ fraction of the domain to make it linear.*

Let G be a finite group aand

$$\forall a, y \in G \quad Pr_{x \in G}[y = a + x] = \frac{1}{|G|}$$

Then if pick $x \in_R G$, $a + x$ if distributed uniformly in G.

3.1 Self-correcting

Given is f such that $\exists g, Pr_x[f(x) = g(x)] \geq 7/8$ and g is linear. In other words, g agrees with f on at least $7/8|G|$ of the inputs). The following algorithm computes $g(x)$:

For $i = 1 \ldots c \log 1/\beta$
  Pick $y \in_R G$
  $answer_i \leftarrow f(y) + f(x - y)$
Output: most common answer

Claim 7 *The probability that the above algorithm outputs $g(x)$ is at least $1 - \beta$.*

Proof $Pr[f(y) \neq g(y)] \leq 1/8$ and so $Pr[f(x-y) \neq g(x-y)] \leq 1/8$ by the observation that $x - y \in_R G$.

$$Pr[f(y) + f(x - y) \neq g(y) + g(x - y)] = Pr[f(y) + f(x - y) \neq g(x)] \leq 1/4$$

By Chernoff bounds we repeat and take the majority. ■

3.2 Testing Linearity

Consider the following algorithm:

Do $O(?)$ times:

Pick random x, y

If $f(x) + f(y) \neq f(x+y)$ fail and halt.

Example:

$$f(x) = \begin{cases} 1 & x \equiv 1 \bmod 3 \\ 0 & x \equiv 0 \bmod 3 \\ -1 & x \equiv -1 \bmod 3 \end{cases}$$

Note that f fails the test for $x \equiv y \equiv 1 \mathrm{mod} 3$ or $x \equiv y \equiv 2 \mod 3$, otherwise it passes.

The probability of failure is then: $\delta_f = Pr[f(x) + f(y) \neq f(x+y)] = 2/9$. But f is 2/3-far from linear.