

Lecture 4

Lecturer: Ronitt Rubinfeld

Scribe: Jacob Scott

1 Review

For Fourier analysis, we showed that all functions $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ can be represented as $f(x) = \sum_S \hat{f}(S) \chi_S(x)$. Here $\hat{f}(S) = \frac{1}{2^n} \sum f(x) \chi_S(x)$, and $\chi_S(x) = \prod_{i \in S} x_i$. From these definitions we state the following facts:

Fact 1 $\chi_S(x) \cdot \chi_T(x) = \chi_{S \Delta T}(x)$, where Δ is symmetric difference.

Fact 2 If $f = \chi_S(x)$, then $\hat{f}(S) = 1$, and $\forall T \neq S, \hat{f}(T) = 0$.

Fact 3 $\hat{f}(S) = 1 - 2 \text{dist}(f, \chi_S)$. Equivalently, $\text{dist}(f, \chi_S) = \frac{1 - \hat{f}(S)}{2}$.

We also restate the Boolean case of Parseval's Theorem:

Theorem 4 $1 = E[f(x)^2] = \sum_S \hat{f}(S)^2$

2 Dictator Functions

Last lecture we saw linear function testing in constant time, independent of the domain size of the function. Our tests passed all linear functions, and rejected all functions that were far from linear. It may have seemed like Fourier analysis was tailor made for handling linear functions, but this is not the case. Today, we will see how to apply it to testing dictator functions.

Definition 5 The *dictator functions* are $\chi_{\{1\}}, \chi_{\{2\}}$, and so on. That is, a function f is a dictator if and only if $f(x) = x_i$ for some i .

All dictator functions are linear and have degree one. We will relax the notation and refer to $\chi_{\{i\}}$ as χ_i . Dictator functions have applications to probabilistically checkable proofs (PCP), and better tests give better hardness of approximation results. Researchers in this area care about improving the constants involved.

2.1 Håstad's test

We will start with an analysis of Håstad's Test (the motivation for which will appear shortly). Given δ and queries to a blackbox function f , pick $x, y \in \{-1, 1\}^n$ uniformly at random. Also pick $w \in \{-1, 1\}^n$ randomly, but from a δ -biased distribution (e.g., $\Pr[w_i = -1] = \delta = 1 - \Pr[w_i = 1]$). Let $z = x \cdot y \cdot w$, and accept f if $f(x)f(y)f(z) = 1$, rejecting otherwise.

Theorem 6 $\Pr[\text{Håstad's Test accepts } f] = \frac{1}{2} + \frac{1}{2} \sum_S (1 - 2\delta)^{|S|} \hat{f}(S)^3$

Proof Let 1_H be an indicator random variable for the result of Håstad's test. Then, $E[1_H] = \frac{1}{2} + \frac{1}{2} E[f(x)f(y)f(z)] = \Pr[\text{Håstad's Test accepts } f]$. Then,

$$\begin{aligned} E[f(x)f(y)f(z)] &= E \left[\left(\sum_S \hat{f}(S) \chi_S(x) \right) \left(\sum_T \hat{f}(T) \chi_T(y) \right) \left(\sum_U \hat{f}(U) \chi_U(x \cdot y \cdot w) \right) \right] \\ &= \sum_S \sum_T \sum_U \hat{f}(S) \hat{f}(T) \hat{f}(U) E[\chi_S(x) \chi_T(y) \chi_U(x \cdot y \cdot w)] \end{aligned}$$

If we focus on $E[\chi_S(x)\chi_T(y)\chi_U(x \cdot y \cdot w)]$, we see that by Fact 1,

$$E[\chi_S(x)\chi_T(y)\chi_U(x \cdot y \cdot w)] = E[\chi_{S\Delta U}(x)\chi_{T\Delta U}(y)\chi_U(w)] = E[\chi_{S\Delta U}(x)]E[\chi_{T\Delta U}(y)]E[\chi_U(w)],$$

where the last equality follows because the values are now independent. Note that unless $S = T = U$, the product of these expectations is zero, because they are positive half the time and negative half the time (see Lecture 3). When $S = T = U$, $E[\chi_{S\Delta U}(x)]$ and $E[\chi_{T\Delta U}(y)]$ both equal 1, and $E[\chi_U(w)] = \prod_{i \in U} E[w_i] = (1 - 2\delta)^{|U|} = (1 - 2\delta)^{|S|}$.

Finally, we get that

$$E[f(x)f(y)f(z)] = \sum_S \sum_T \sum_U \hat{f}(S)\hat{f}(T)\hat{f}(U)E[\chi_S(x)\chi_T(y)\chi_U(x \cdot y \cdot w)] = \sum_S \hat{f}(S)^3(1 - 2\delta)^{|S|}.$$

■

2.2 Building a dictator tester

Our goal is to show that there exists a testing algorithm A with some (as yet unestablished) query complexity such that if f is a dictator, $Pr[A \text{ passes } f] \geq 1 - \beta$, and if f is ϵ -far from a dictator, $Pr[A \text{ rejects } f] \geq 1 - \beta$. We assume without loss of generality that $\epsilon < .01$.

We start from the following test. Run Håstad's test $O(\frac{1}{\epsilon^2} \log \frac{1}{\beta})$ times with $\delta = 3\epsilon/4$. Accept f if it passes Håstad's test $1 - .85\epsilon$ fraction of the time. If f is a dictator, then we know $f = \chi_S$ for some S with $|S| = 1$. Thus the probability that f passes Håstad's test is $\frac{1}{2} + \frac{1}{2}(1 - 2\delta) = 1 - \delta = 1 - 3\epsilon/4$. If f is ϵ -far from being a dictator or the function always equal 1, we will show that it passes with probability $\leq 1 - \epsilon$. This leaves an $\epsilon/4$ gap, which can be exploited by standard Chernoff bounds to get the $1 - \beta$ confidence that we desire (e.g., by setting our acceptance threshold to $1 - .85\epsilon$).

Lemma 7 *If f is ϵ -far from all dictator functions and the function $f(x) = 1$, then the probability that it passes Håstad's test is $\leq 1 - \epsilon$.*

Proof Suppose f is ϵ -far from all dictator functions and the function $f(x) = 1$, but $Pr[\text{Håstad's test passes } f] \geq 1 - \epsilon$. We then have (after some simple algebra) that

$$1 - 2\epsilon \leq \left(\sum_S \hat{f}(S)^2 \right) \cdot \left(\max_S (1 - 2\delta)^{|S|} \hat{f}(S) \right).$$

By Parseval's, this gives that $1 - 2\epsilon \leq \max_S (1 - 2\delta)^{|S|} \hat{f}(S)$. This implies that there exists S such that $\hat{f}(S) \geq 1 - 2\epsilon$, and by Fact 3, $\text{dist}(f, \chi_S) \leq \frac{1 - (1 - 2\epsilon)}{2} = \epsilon$. What remains is to show that $|S| \leq 1$, so that χ_S is either a dictator or the all ones function.

Note that by our choice of $\delta = 3\epsilon/4$, we have that $(1 - 2\delta)^{|S|} = (1 - 6\epsilon/4)^{|S|}$, which is $< 1 - 2\epsilon$ when $|S| > 1$. Thus the S that maximizes the above expression must have $|S| \leq 1$, so that χ_S is either a dictator or the all ones function. Hence, f is ϵ -close to one of the functions it should be far from. ■

How can we augment our test to ensure that functions ϵ -close to $f(x) = 1$ do not pass our test? Note that all dictator functions take on 0 half the time, and 1 half the time. One way would be to first run f on $O(\log \frac{1}{\beta})$ random inputs and reject it if more than $3/4$ fraction of the results are 1. By the Chernoff bound, this enables us to distinguish functions that are $1/6$ -close to $f(x) = 1$ from those that are $1/6$ -close to a dictator function.

3 Voting

Next, we consider at a high level how some of the techniques we have seen so far apply to fair voting schemes. First we present the **Condorcet method** for ranking three candidates. Given an election with n voters and three candidates, we would like a fair global ordering.

We are given three strings $S_1, S_2, S_3 \in \{-1, 1\}^n$. The i th bit of S_1 gives voter i 's preference of candidate A compared to candidate B (e.g. $S_1[i] = 1$ means voter i prefers candidate A to candidate B). Similarly, the i th bit of S_2 gives B compared to C and the i th bit of S_3 gives C compared to A .

Our goal is to produce an aggregate function $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ so that $(f(S_1), f(S_2), f(S_3))$ gives a global preference. We require that this preference is *rational*, by which we mean acyclic, which it is so long as the three preferences are not all equal (NAE). An aggregate function f is considered rational if for all S_1, S_2, S_3 , $(f(S_1), f(S_2), f(S_3))$ is NAE.

Theorem 8 (Arrow's Impossibility Theorem) *The only rational monotone aggregate functions are dictators.*¹

We can test whether or not a function f is rational aggregate by choosing $x, y, z \in \{-1, 1\}^n$ uniformly at random, and accepting if $(f(x), f(y), f(z))$ is NAE, and rejecting otherwise. The probability that a function f passes this test is

$$\frac{3}{4} - \frac{3}{4} \sum_S \left(\frac{-1}{3}\right)^{|S|} \hat{f}^2.$$

Dictators pass this test with probability 1, while constant functions always fail. Parity functions on two bits succeed with probability $\frac{2}{3}$. We can thus test if f is a dictator by testing if it is linear (see last lecture) and if it is a rational aggregate.

One thing to take away from this lecture is that in terms of what we have seen, the creativity lies more in constructing the test than doing the analysis, which tends to be boilerplate. Next lecture we go beyond testing and look at computational learning.

¹the only non-monotone rational aggregate functions are *anti-dictators*.