6.893 Approximability of Optimization Problems	October 25, 1999

Lecture 12

Lecturer: Madhu Sudan — *Scribe: Sandeep Chatterjee*

In this lecture, we consider self-testing alogrithms and in particular, a self-tester for Hadamard Codes. We further discuss linearity testing and analysis as well as the Blum-Luby-Rubinfeld test for linearity.

1 Self-Testing Algorithms

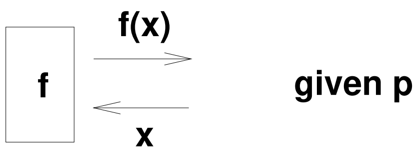
During the course of information transmission, there exists the potential for data corruption. Self-testing algorithms enable us to understand whether such corruption has occured.

Self-testing algorithms can be separated into two segments:

1) Linearity tests: Given an arbitrary string over a noisy channel, linearity tests allow us to understand whether the codeword is infact a codeword or if it has been corrupted. A linearity test is a quick tester for Hadamard Codes.

2) Low degree tests. Low degree tests are another segment of self-testing algorithms, which are useful for multivariate polynomial codes. We will discuss these tests in later lectures.

For a first cut at a self-testing algorithm, imagine that we have oracle access to both f and P. Now, we take a given P, choose an x at random and check whether $f(x) = P(x)$. This is shown below.



Unfortunately, we do not have an oracle for P. We need to devise a mechanism to feign oracle access to P. So, a suggestion would be to replace oracle access to P with $Self - Correct^f(x)$. Continuing from our earlier check:

$$f(x) = P(x)$$
$$f(x) = Self - Correct^f(x)$$

In this case, we choose an x at random, and check whether $f(x)$ equals $Self - Correct^f(x)$. Clearly, if f and P are equal, then self-correction works. If f and P are sufficiently close, self-correction also works. Only when f is far from all P does self-correction fail. We will revisit this at a later point in the lecture.

Now, let us expand this test for Hadamard codes. Recall the definition of our self-correcting algorithm for computing $f(x)$:

1. Choose $y \in \{0,1\}^m$ at random
2. Return $f(x+y) - f(y)$

Using this result, we would like to check:

$$f(x) = P(x)$$
$$f(x) = Self - Correct^f(x)$$
$$f(x) = f(x+y) - f(y)$$
$$f(x+y) = f(x) + f(y)$$

Next, we would like to generalize this for all finite abelian groups, G and H.

$$f : G \rightarrow H, \text{ where } G \text{ is in } \{0,1\}^n \text{ and } H \text{ is in } \{0,1\}.$$

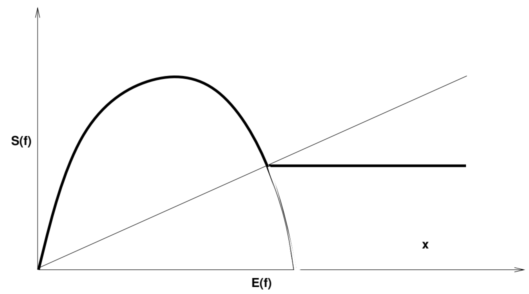
Continuing from our earlier result, we now pick $x, y \in G$ and check:

$$f(x+y) = f(x) + f(y)$$

Now that we have an intuitive feeling for self-testing, next we delve deeper. The first thing we would like to understand is how much error happened during transmission, and what our self-tester does in case of transmission error.

Let Linear $= \{\phi \mid \forall x, y; \phi(x+y) = \phi(x) + \phi(y)\}$
Let $Error(f) = \xi(f) = min_{\phi \in Linear} Pr_x[f(x) \neq \phi(x)]$.
Let $\delta(f) = Pr_{x,y \in G}[f(x) + f(y) \neq f(x+y)]$.

Intuitively, we would like to reject if $\xi(f)$ is large, and accept otherwise. Consider the point marked with an X in the graph below. This point shows high error, yet low rejection. Clearly, this is bad news. It is conceiveable to think that we would like some sort of a linear relationship between $\delta(f)$ and $\xi(f)$. Points below this line would be forbidden.



In fact, the true relationship is shown by the heavy line in the graph above. We will analyze a segment of this graph later.

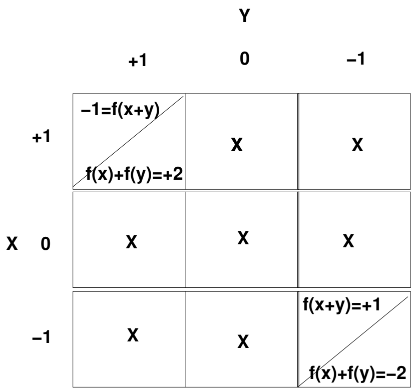
1.1 An Example

Let us first consider an example.

Let $G = H = Z_{3n}$

Define:
$f(x) = 0$ if $x = 0(mod3)$
$f(x) = 1$ if $x = 1(mod3)$
$f(x) = 3n - 1$ if $x = -1(mod3)$

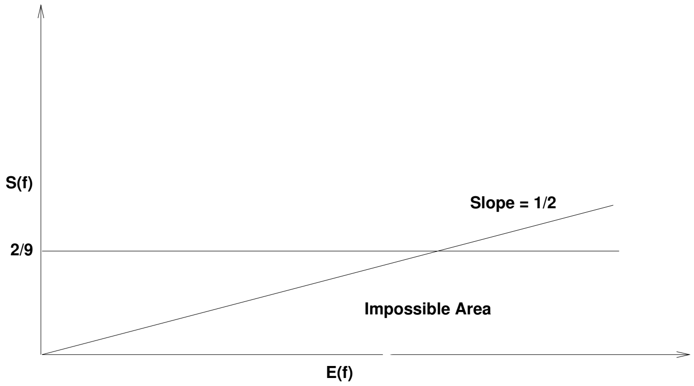
In the following table, we work out this example graphically. The X's in the table signify that $f(x+y) = f(x) + f(y)$, whereas the other boxes show the disequality. Using simple ratios, we find that with probability $\frac{2}{9}$ we reject, whereas with probability $\frac{7}{9}$ we accept. This is a function with $\delta(f) = \frac{2}{9}$ and $\xi(f) = \frac{2}{3}$.



Now, let's explore this further.

Claim: Suppose $\delta(f) < 2/9$. Then, there exists a $\phi \in Linear$ such that ϕ is 2δ-close to f. That is: $\xi(f) \leq 2\delta(f)$.

The figure below shows this pictorally.



Define: $\phi(x) = Majority_y(f(x+y) - f(y))$
This is our definition of the self-correction algorithm. This algorithm chooses the majority output of $self - correct^f(x)$ over all possible y's and returns it as its value. The two properties that we would like to show for this are:
1. ϕ is close to f; and,
2. ϕ is linear.

Proof of (1):

Let $BAD = \{x \mid f(x) \neq f(x+y) - f(y)$ for atleast half the y's$\}$.

Step 1a. It then follows that $x \notin BAD \Rightarrow \phi(x) = f(x)$
Step 1b. Now, we have to show that the cardinality of BAD or $\mid BAD \mid$ over the whole group, $\mid G \mid$ is small. That is, we want to show that $\frac{|BAD|}{|G|}$ is small.
For $x \in BAD$, $Pr_{y \in RND}$ [Test Fails] $\geq \frac{1}{2}$.
If $Pr[x \in BAD] > 2\delta$, then
$Pr[TestFails] > 2\delta\frac{1}{2} > \delta$. This is a contradiction. Thus, $Pr[x \in BAD] \leq 2\delta \Rightarrow Pr[\phi(x) \neq f(x)] \leq 2\delta$.

Proof of (2):

We must show that ϕ is linear.

We first show that $Pr_{y_1,y_2}[f(x+y_1)-f(y_1)=f(x+y2)-f(y2)]$ is overwhelming.
Re-arranging terms:

$Pr_{y_1,y_2}[f(x+y_1)+f(y_2)=f(x+y2)+f(y_1)] \geq$
$Pr_{y_1,y_2}[f(x+y_1+y_2)=f(x+y_1)+f(y_2)=f(x+y_2)+f(y_1)] \geq 1-2\delta \geq 1-2\delta \geq 1-\frac{4}{9} \geq \frac{5}{9}$.

Exercise: Consider a bucket with a variety of different colored balls. You must pick two balls with probability that they have the same color greater than $\frac{5}{9}$. It is left as an exercise to show that the most common color occurs at least $\frac{2}{3}$ of the time.

Using this result, $\forall x$, Pr y $[\phi(x) \neq f(x+y)-f(y)] < 1/3$

Now, consider $\forall x, z$. We want to show that: $\phi(x)+\phi(z)=\phi(x+z)$

For random y, we analyze each of these as follows:

$\phi(x)=f(y)-f(y-x)$, which, with probability $< \frac{1}{3}$ does not happen.
$\phi(z)=f(z+y)-f(y)$, which, with probability $< \frac{1}{3}$ does not happen.
$\phi(x+z)=f(z+y)-f(y-x)$, which, with probability $< \frac{1}{3}$ does not happen.

Using these results, we know that there must exist a y such that all of the above three actually hold. This proves linearity.

Combining steps 1 and 2, we have showed that for $\delta < \frac{2}{9}, \xi(f) \leq 2\delta(f)$.