E0 224 Computational Complexity Theory **Fall 2014**

Lecture 29: November 24

Lecturer: Chandan Saha *Scribe: Datta Krupa R, Sachin Kumar Srivastava, Mohd Aqil*

29.1 Abstract

1. Linearity testing. BLR [Blum, Luby, and Rubinfeld] test

Setup: Given a black box implementing some boolean function.
Task: We need to check if underlying function(say f) is linear. We are only allowed to query the box at points $x \in \{0,1\}^n$, whereby the box returns the value $f(x)$.

Objective: To complete the task using constantly many queries to the box (ensuring high probability of success)

(Recall) A function $f : \{0,1\}^n \to \{0,1\}$ is $(1-\epsilon)$-close to a linear function $g : \{0,1\}^n \to \{0,1\}$ if $Pr_{x \in \{0,1\}}\{f(x) = g(x)\} \geq 1 - \epsilon$

BLR test (one round)

1. Choose $x \in_R \{0,1\}^n, y \in_R \{0,1\}^n$ independently.
2. Let $z = x + y$. [addition is coordinatewise over F_2]
3. Query f at x, y, z check if $f(x) + f(y) = f(z)$
4. If equality holds then accept, else reject.

To capture the closeness between two functions, we use a nice notational switch. From here on, the underlying field is the field of reals.

Notational switch: $0 \to 1$ and $1 \to -1$
Now $f, g : \{1,-1\}^n \to \{1,-1\}$

We will identify a function $f : \{1,-1\}^n \to \mathbb{R}$, naturally with a 2^n-dimensional vector over $\mathbb{R}$. Let $f.g$ denote the "usual" dot product of f and g, when viewed as vectors in $\mathbb{R}^{2^n}$.

Let $f, g : \{1,-1\}^n \to \{1,-1\}$ Then,
$f.g$ = Number of coordinates where f and g agree - Number of coordinates f and g disagree.
$\Rightarrow f.g$ = Number of coordinates where f and g agree - (2^n - Number of coordinates where f and g agree)
$\Rightarrow f.g$ = 2*(Number of coordinates where f and g agree) - 2^n

Definition 29.1 (Inner product ($\langle f, g \rangle$)) *Let $f : \{1,-1\}^n \to R$, and $g : \{1,-1\}^n \to R$, then*
$\langle f, g \rangle = E_{x \in_R \{1,-1\}^n}[f(x)g(x)] = \frac{1}{2^n} f.g$

Fact: $\langle f,g\rangle$ defines an inner product space. i.e it satisfies axioms

1. $\langle f,g\rangle = \langle g,f\rangle$
2. $\langle \alpha f,g\rangle = \alpha\langle f,g\rangle$ where α is a scalar in R
3. $\langle h+f,g\rangle = \langle f,g\rangle + \langle h,g\rangle$
4. $\langle f,g+h\rangle = \langle f,g\rangle + \langle f,h\rangle$
5. $\langle f,f\rangle \geq 0$
6. $\langle f,f\rangle = 0 \Leftrightarrow f = 0$

The product $\langle f,g\rangle = \frac{1}{2^n} f.g$ captures the correlation between f and g.
Denote the 2^n Linear functions (after notational switch), by
$\chi_\phi \dots \chi_S \dots \chi_{[n]}$. where $\chi_S(x) = \prod_{i\in S} x_i$, where x_i denotes the i^{th} coordinate of x.

Lemma 29.2 *$\langle \chi_S, \chi_T\rangle = 1$ if $S = T$*
$\langle \chi_S, \chi_T\rangle = 0$ if $S \neq T$ where $S, T \subseteq [n]$

Corollary 29.3 *$\chi_\phi \dots \chi_{[n]}$ are linearly independent over R*

Corollary 29.4 *$\chi_\phi \dots \chi_{[n]}$ form an orthonormal basis for R^{2^n}*

Definition 29.5 (Fourier expansion) *From above corollary any vector $f : \{1,-1\}^n \to R$ has a unique representation of the form $f = \sum_{S\subseteq[n]} \alpha_S \chi_S$, where $\alpha_S \in R$. Such a representation is called the Fourier expansion of f.*

Remark: In a broader sense Fourier expansion, is representation of a vector over some other "interesting" basis.

Definition : Let $f = \sum_{S\subseteq[n]} \alpha_S \mathcal{X}_S$, the values $\{\alpha_S\}_{S\subseteq[n]}$ are the Fourier coefficients of f. We usually use the notation : $f = \sum_{S\subseteq[n]} \hat{f}(S).\mathcal{X}_S$, where $\hat{f}(S) = \alpha_S$.

Lemma : $< f,g > = \sum_{S\subseteq[n]} \hat{f}(S)\hat{g}(S)$, where $f,g : \{1,-1\}^n \to R$

Proof : $< f,g > = < \sum_S \hat{f}(S).\mathcal{X}_S, \sum_T \hat{g}(T).\mathcal{X}_T >$ (apply distributive law)

$= \sum_{S,T} \hat{f}(S).\hat{g}(T) < \mathcal{X}_S, \mathcal{X}_T >$

$= \sum_{S\subseteq[n]} \hat{f}(S).\hat{g}(S)$

Corollary 3 : $< f,f >= \sum_{S\subseteq[n]} \hat{f}(S)^2$

Corollary 4 : Let $f : \{1,-1\}^n \to \{1,-1\}$ Then $< f,f >= 1$, (by definition of inner product $\langle .,. \rangle$). Hence,

$\sum_{S\subseteq[n]} \hat{f}(S)^2 = 1$ (known as Parseval's equality)

BLR Test 2

It is an equivalent version of the actual BLR test after the notational switch. We will use this test for the sake of analysis.

1. Choose $x \in_R \{1,-1\}^n, y \in_R \{1,-1\}^n$ independently.
2. Let $z = x \circ y$, (where $x \circ y$ is the co-ordinate wise product).
3. Query f at x, y, z.
4. Check if $f(x).f(y) = f(z) \equiv f(x).f(y).f(z) = 1$ (as f takes $+1, -1$ values).
5. If $f(x).f(y).f(z) = 1$ then accept else reject.

We need to analyze the following quantity :

$$Pr_{x,y \in_R \{1,-1\}^n}\{f(x).f(y).f(x \circ y) = 1\}$$
$$= Pr\{ \text{ BLR test accepts } \}$$

Observation : Suppose $f, g : \{1,-1\}^n \to \{1,-1\}$, then

$$< f, g >= E_{x \in_R \{1,-1\}}[f(x).g(x)]$$
$$= \frac{1}{2^n}[\# \text{ of co-ordinates where } f,g \text{ agree - } \# \text{ of co-ordinates where } f,g \text{ disagree}]$$
$$= \frac{1}{2^n}[f.g]$$
$$= \text{fractions of co-ordinates where } f,g \text{ agree - fractions of co-ordinates where } f,g \text{ disagree}$$
$$= 2*(\text{fractions of co-ordinates where } f,g \text{ agree) - 1.}$$

Observation : Let $f : \{1,-1\}^n \to \mathbb{R}$ and let $f = \sum_{S \subseteq [n]} \hat{f}(S).\mathcal{X}_S$ be the Fourier expansion of f.

Then $< f, \mathcal{X}_S >= \hat{f}(S)$ for every $S \subseteq [n]$.

BLR Test Analysis

Outline : We will show that if $Pr\{\text{BLR test accepts}\}$ is high, then $\hat{f}(S)$ is high for some S.

$\Rightarrow < f, \mathcal{X}_S >$ is high

$\Rightarrow f$ is close to $\mathcal{X}_S$.

Theorem : If $Pr\{$ BLR test accepts $f\} \geq (1-\epsilon)$, then f is $(1-\epsilon)$ close to a linear function.

Proof : We define the following indicator variable :

$$e_{x,y} = \frac{1}{2} + \frac{1}{2}.f(x).f(y).f(z), \text{ where } z = x \circ y.$$

Observe that $e_{x,y} = 1$ if and only if BLR test accepts with x and y as the random vectors chosen in step 1.

Hence, $Pr_{x,y \in_R \{1,-1\}^n}\{$ BLR test accepts $f\}$

$$= Pr_{x,y \in_R \{1,-1\}^n}\{e_{xy} = 1\}$$
$$= E_{x,y}[e_{xy}]$$
$$= E_{x,y}\left[\frac{1}{2} + \frac{1}{2}.f(x).f(y).f(z)\right]$$
$$= \frac{1}{2} + \frac{1}{2}.E_{x,y}\left[f(x).f(y).f(z)\right] \quad \text{....(1).}$$

Analysing $E[f(x).f(y).f(x \circ y)]$

Let $f = \sum \hat{f}(S).\mathcal{X}_S$

$\Rightarrow\ f(x) = \sum_S \hat{f}(S).\mathcal{X}_S(x),$

$f(y) = \sum_T \hat{f}(T).\mathcal{X}_T(y)$, and

$f(x \circ y) = \sum_U \hat{f}(U).\mathcal{X}_U(x \circ y)$. Therefore,

$f(x).f(y).f(x \circ y) = \sum_{S,T,U} \hat{f}(S).\hat{f}(T).\hat{f}(U).\mathcal{X}_S(x).\mathcal{X}_T(y).\mathcal{X}_U(x \circ y)$

$\Rightarrow\ E_{x,y}[f(x).f(y).f(x \circ y)]$

$= \sum_{S,T,U} \hat{f}(S).\hat{f}(T).\hat{f}(U)E_{x,y}[\mathcal{X}_S(x).\mathcal{X}_T(y).\mathcal{X}_U(x \circ y)]$

We know that :

$\mathcal{X}_S(x) = \Pi_{i \in S} x_i$

$\mathcal{X}_T(y) = \Pi_{j \in T} y_j$

$\mathcal{X}_U(x \circ y) = \Pi_{k \in U} x_k y_k$

$\Rightarrow\ \mathcal{X}_S(x).\mathcal{X}_T(y).\mathcal{X}_U(x \circ y) = \Pi_{i \in S\Delta U} x_i \Pi_{j \in T\Delta U} y_j$

$\Rightarrow\ E_{x,y}\big[\mathcal{X}_S(x).\mathcal{X}_T(y).\mathcal{X}_U(x \circ y)\big] = E\big[\Pi_{i \in S\Delta U} x_i\big].E\big[\Pi_{j \in T\Delta U} y_j\big]$ (as x and y are chosen independently).

$\Rightarrow\ E_{x,y}\big[\mathcal{X}_S(x).\mathcal{X}_T(y).\mathcal{X}_U(x \circ y)\big] = \Pi_{i \in S\Delta U} E\big[x_i\big].\Pi_{j \in T\Delta U} E\big[y_j\big]$

$\Rightarrow\ E_{x,y}\big[\mathcal{X}_S(x).\mathcal{X}_T(y).\mathcal{X}_U(x \circ y)\big] = 0 \quad$ if $S\Delta U \neq \phi$ or $T\Delta U \neq \phi$

$\Rightarrow\ E_{x,y}[f(x).f(y).f(z)] = \sum_{S \subseteq [n]} \hat{f}(S)^3$

By the assumption made in the theorem statement :

$\frac{1}{2} + \frac{1}{2}\sum_{S \subseteq [n]} \hat{f}(S)^3 \geq (1 - \epsilon)$

$\Rightarrow \sum_{S \subseteq [n]} \hat{f}(S)^3 \geq (1 - 2\epsilon).$

Observe that $\sum_{S \subseteq [n]} \hat{f}(S)^3 \sum_{S \subseteq [n]} \hat{f}(S)^2.\hat{f}(S) \leq max_S\{\hat{f}(S)\}. \sum_{S \subseteq [n]} \hat{f}(S)^2$

Since, $\sum_{S \subseteq [n]} \hat{f}(S)^2 = 1$

$\sum_{S \subseteq [n]} \hat{f}(S)^2.\hat{f}(S) \leq max_S\{\hat{f}(S)\}$

$\Rightarrow$ there is fourier coefficient, say $\hat{f}(w)$, such that

$\hat{f}(w) \geq\ 1 - 2\epsilon$

$\Rightarrow < f, \mathcal{X}_w > \geq\ 1 - 2\epsilon$

$\Rightarrow\ 2$[fraction of co-ordinates where f and $\mathcal{X}_w$ agree]$-1 \geq\ 1 - 2\epsilon$

$\Rightarrow$ fraction of co-ordinates where f and $\mathcal{X}_w$ agree $\geq\ 1 - \epsilon$.

References

[AB09] Sanjeev Arora and Boaz Barak, 2009. *Computational Complexity: A Modern Approach*, Cambridge University Press.

[RD07] Lecture notes 2 and 3 from "Analysis of Boolean Functions" by Ryan O'Donnell `http://www.`

cs.cmu.edu/~odonnell/boolean-analysis/