CS 6817: Special Topics in Complexity Theory **Spring 2025**

Lecture 2: Jan 23, 2025

Lecturer: Eshan Chattopadhyay *Scribe: Max Tromanhauser*

1 The Fundamental Theorem

Continuing from last lecture, we look to prove the following fundamental theorem.

Theorem 1.1. *Let $f : \{-1,1\}^n \to \mathbb{R}$ be a Boolean function. Then there exists a unique, real, multilinear polynomial $p(x)$ such that $p(x) = f(x)$ for all $x \in \{-1,1\}^n$.*

In the previous lecture, we defined the Fourier transform of $f(x)$ to be the polynomial

$$p(x) = \sum_{S \subseteq [n]} c_s x^S$$

where $x^S = \prod_{i \in S} x_i$. The coefficient c_s is called the *Sth Fourier coefficient of f* and is also denoted $\hat{f}(S)$ where $\hat{f} : 2^{[n]} \to \mathbb{R}$. We have already established $p(x)$ to be real and multilinear, but we still must show that it is unique.

Towards that end, we defined a vector space $V = \{f : \{-1,1\}^n \to \mathbb{R}\}$ with inner product $\langle f, g \rangle = \mathbb{E}_x[f(x)g(x)]$ and ℓ_2-norm $||f||_2 = \sqrt{\langle f, f \rangle}$. This definition satisfies the three requirements of an inner product:

1. It is trivially **symmetric** by the commutativity of multiplication.

2. It is **positive-definite** — i.e., if $\langle f, f \rangle = 0$ then $f : \{-1,1\}^n \to 0$. By definition of expectation, if $\mathbb{E}_x[f(x)^2] = 0$ then $\frac{1}{2^n} \sum_x f(x)^2 = 0$ and so $f(x) = 0$ for all $x \in \{-1,1\}^n$.

3. It is **linear in the first argument** as for all $f, g, h \in V$, we can show $\langle f+g, h \rangle = \langle f, h \rangle + \langle g, h \rangle$ by the linearity of expectation,

$$\begin{aligned}
\langle f + g, h \rangle &= \mathop{\mathbb{E}}_{x \in \{-1,1\}^n} [(f(x) + g(x)) \cdot h(x)] \\
&= \mathop{\mathbb{E}}_{x \in \{-1,1\}^n} [(f(x)h(x) + g(x)h(x))] \\
&= \mathop{\mathbb{E}}_{x \in \{-1,1\}^n} [(f(x)h(x)] + \mathop{\mathbb{E}}_{x \in \{-1,1\}^n} [g(x)h(x))] \\
&= \langle f, h \rangle + \langle g, h \rangle
\end{aligned}$$

Claim 1.2. *Let $\chi_S(x) = x^S$, then $\{\chi_S\}_{S \subseteq [n]}$ forms an orthonormal basis of V.*

Note that this claim will directly show the uniqueness for Theorem 1.1 since any function is then expressed as a *unique* linear combination of x^S terms. Thus, $p(x)$ must be unique.

Proof.

1. Because χ_S is Boolean valued, $\chi_S(x)^2 = 1$ for all $x \in \{-1,1\}^n$. Therefore, all χ_S are normal as $||\chi_S(x)||_2 = \sqrt{\langle \chi_S, \chi_S \rangle} = \sqrt{\mathbb{E}_x[\chi_S(x)^2]} = 1$.

2. For all $S, T \subseteq [n]$ and $S \neq T$, we want to show $\langle \chi_S, \chi_T \rangle = 0$. Let $S \triangle T$ be the symmetric difference between these subsets and note that $S \triangle T \neq \emptyset$ because $S \neq T$.

$$\begin{aligned}\langle \chi_S, \chi_T \rangle &= \mathop{\mathbb{E}}_{x \in \{-1,1\}^n} [\chi_S(x) \cdot \chi_T(x)] \\ &= \mathop{\mathbb{E}}_{x \in \{-1,1\}^n} [\chi_{S \cap T}(x)^2 \cdot \chi_{S \triangle T}(x)] \\ &= \mathop{\mathbb{E}}_{x \in \{-1,1\}^n} [\chi_{S \triangle T}(x)] = 0\end{aligned}$$

As before, $\chi_{S \cap T}(x)^2 = 1$ because it is a Boolean valued function. Similarly, $\mathbb{E}_x[\chi_{S \triangle T}(x)] = 0$ as $S \triangle T \neq \emptyset$ and so $\chi_{S \triangle T}(x)$ is a parity function.

3. Because $\dim_{\mathbb{R}}(V) = 2^n$ and $\{\chi_S\}_{S \subseteq [n]}$ is a set of 2^n normal, orthogonal vectors in V, then it must be an orthonormal basis for V. □

2 Useful Fourier analytic formulas

As we've established, any Boolean function $f(x)$ can be expressed as $f(x) = \sum_{S \subseteq [n]} \hat{f}(S) \chi_S(x)$. Now we will make several observations that follow from this.

Observation 2.1. $\hat{f}(S) = \langle f, \chi_S \rangle$.

This follows from the linearity of expectation:

$$\begin{aligned}\langle f, \chi_S \rangle &= \left\langle \sum_{T \subseteq [n]} \hat{f}(T) \chi_S(x), \chi_S \right\rangle \\ &= \sum_{T \subseteq [n]} \hat{f}(T) \langle \chi_T(x), \chi_S(x) \rangle \\ &= \hat{f}(S)\end{aligned}$$

The final equality follows from the orthogonality of the basis $\{\chi_S\}$ — i.e., that all terms $\langle \chi_T, \chi_S \rangle = 0$ if $S \neq T$. With this fact, we can see that

$$\hat{f}(S) = \langle f, \chi_S \rangle = \mathop{\mathbb{E}}_{x \in \{-1,1\}^n} [f(x) \chi_S(x)]$$

This is the *inverse Fourier transform* and will be useful throughout the course.

Observation 2.2. *If f is Boolean valued, then $\hat{f}(S) = \Pr_x[f(x) = \chi_S(x)] - \Pr_x[f(x) \neq \chi_S(x)]$.*

This directly follows from the definition of expectation. Because both functions output $\{-1, 1\}$, then $f(x)\chi_S(x) = 1$ if $f(x) = \chi_S(x)$ and $f(x)\chi_S(x) = -1$ otherwise. Thus,

$$\begin{aligned}\mathop{\mathbb{E}}_{x \in \{-1,1\}^n} [f(x)\chi_S(x)] &= \frac{1}{2^n} \sum_{x \in \{-1,1\}^n} f(x)\chi_S(x) \\ &= \frac{1}{2^n} \left(\sum_{x\,:\, f(x) = \chi_S(x)} 1 \right) + \frac{1}{2^n} \left(\sum_{x\,:\, f(x) \neq \chi_S(x)} -1 \right) \\ &= \Pr_{x \in \{-1,1\}^n} [f(x) = \chi_S] - \Pr_{x \in \{-1,1\}^n} [f(x) \neq \chi_S]\end{aligned}$$

Observation 2.3. $\mathbb{E}_x[f(x)] = \hat{f}(\emptyset)$.

This is derived by using the linearity of expectation and noting that $\mathbb{E}_x[\chi_S(x)] = 0$ for any $S \neq \emptyset$.

$$\begin{aligned}
\mathop{\mathbb{E}}_{x\in\{-1,1\}^n}[f(x)] &= \mathop{\mathbb{E}}_{x\in\{-1,1\}^n}\left[\sum_{S\subseteq[n]} \hat{f}(S)\chi_S(x)\right] \\
&= \sum_{S\subseteq[n]} \hat{f}(S) \mathop{\mathbb{E}}_{x\in\{-1,1\}^n}[\chi_S(x)] \\
&= \mathop{\mathbb{E}}_{x\in\{-1,1\}^n}[\hat{f}(\emptyset)\chi_\emptyset(x)] \\
&= \hat{f}(\emptyset)
\end{aligned}$$

The final equality comes from the choice that $\chi_\emptyset(x) = 1$ for all $x \in \{-1,1\}^n$.

Observation 2.4 (Parseval's Identity)**.** $\mathbb{E}_x[f(x)^2] = \langle f, f\rangle = \sum_{S\subseteq[n]} \hat{f}(S)^2$.

This is a direct result of the linearity of the inner product and the orthogonality of the $\{\chi_S\}$ basis.

$$\begin{aligned}
\langle f, f\rangle &= \left\langle \sum_{S\subseteq[n]} \hat{f}(S)\chi_S(x), \sum_{T\subseteq[n]} \hat{f}(T)\chi_T(x) \right\rangle \\
&= \sum_{S,T\subseteq[n]} \hat{f}(S)\hat{f}(T)\langle \chi_S(x), \chi_T(x)\rangle \\
&= \sum_{S\subseteq[n]} \hat{f}(S)^2
\end{aligned}$$

Observation 2.5. $\mathrm{Var}[f(x)] = \sum_{S\subseteq[n], S\neq\emptyset} \hat{f}(S)^2$.

This follows directly from the combination of Observations 2.3 and 2.4.

$$\begin{aligned}
\mathrm{Var}_{x\in\{-1,1\}^n}[f(x)] &= \mathop{\mathbb{E}}_{x\in\{-1,1\}^n}[f(x)^2] - \mathop{\mathbb{E}}_{x\in\{-1,1\}^n}[f(x)]^2 \\
&= \sum_{S\subseteq[n]} \hat{f}(S)^2 - \hat{f}(\emptyset)^2 \\
&= \sum_{S\subseteq[n], S\neq\emptyset} \hat{f}(S)^2
\end{aligned}$$

Observation 2.6 (Plancheral Theorem)**.** $\mathbb{E}_x[f(x)g(x)] = \langle f, g\rangle = \sum_{S\subseteq[n]} \hat{f}(S)\hat{g}(S)$.

This follows exactly the same derivation as Observation 2.4 substituting $\hat{f}(T)$ with $\hat{g}(T)$.

Observation 2.7. *If f is Boolean valued, then $\sum_{S\subseteq[n]} \hat{f}(S)^2 = 1$.*

This is a direct corollary to Observation 2.4, as a Boolean valued f has $\mathbb{E}_x[f(x)^2] = 1$.

3 Property Testing

A property tester is an algorithm with black box access to a function which decides whether that function exhibits some property. Properties are defined as be a collection of functions.

We begin by defining a distance measure for Boolean functions and properties, then provide a formal definition for a tester.

Definition 3.1. *Given $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$, we define their distance to be*

$$\mathrm{dist}(f,g) = \Pr_{x \xleftarrow{\$} \mathbb{F}_2^n}[f(x) \neq g(x)].$$

Given property $P \subseteq \{f : \mathbb{F}_2^n \to \mathbb{F}_2\}$, we define a function's distance to that property to be

$$\mathrm{dist}(f,P) = \min_{g \in P} \mathrm{dist}(f,g).$$

Definition 3.2. *A randomized algorithm $\mathcal{A}$ is an (r, λ)-*tester *for property P if, for all $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $\mathcal{A}^f$ makes at most r queries and*

1. *If $f \in P$, then $\Pr[\mathcal{A}^f \text{ accepts}] = 1$*
2. *If $f \notin P$, then $\Pr[\mathcal{A}^f \text{ rejects}] \geq \lambda \cdot \mathrm{dist}(f,P)$*

where the probabilities are over the randomness of $\mathcal{A}$.

3.1 Linearity Testing

Now we turn to a specific property and a tester for it. Given black box access to some Boolean function, we would like to make a small (constant) number of queries to determine if the function is linear. That is to say, it belongs to the property

$$\mathsf{LIN} = \{f : \mathbb{F}_2^n \to \mathbb{F}_2 \mid \forall x, y \in \mathbb{F}_2^n,\ f(x+y) = f(x) + f(y)\}$$

Our tester for LIN is from Blum, Luby, Rubinfeld '90 and so is called the *BLR Test.* To test for linearity, simply sample two random elements $x, y \xleftarrow{\$} \mathbb{F}_2^n$ and accept if and only if $f(x) + f(y) = f(x+y)$.

Theorem 3.3. *The BLR test is a (3, 1)-tester for* LIN.

We will prove the above theorem in next class.