CS 6817: Special Topics in Complexity Theory	Spring 2025

Lecture 1: Jan 21, 2025

Lecturer: Eshan Chattopadhyay *Scribe: Liam Packer*

1 Introduction, Basic Notions

Definition 1.1. *A Boolean function is a real-valued function from the hypercube $\{0,1\}^n$, or $\{-1,1\}^n$, to $\mathbb{R}$.*

The choice between $\{-1,1\}^n$ and $\{0,1\}^n$ seems arbitrary. But we'll see later that $\{-1,1\}^n$ is more convenient. We will connect Theorem 1.8 to the usual Fourier expansions of functions $f : \mathbb{R}^d \to \mathbb{R}$, but for this we need to endow the hypercube with a *group* operation, and then look at the *characters* of that group (to be seen later). For $\{-1,1\}^n$ we can use component-wise multiplication as the group operation, while for $\{0,1\}^n$ we can use component-wise addition (mod 2).

In the end, the two sets are related by a simple transformation: for each component of a point $x \in \{0,1\}^n$, send $0 \mapsto 1$ and $1 \mapsto -1$. One representation of this map is

$$x \mapsto (-1)^x,$$

to be interpreted compontent-wise. Another representation is

$$x \mapsto 2x - 1.$$

This mapping is linear and easily invertible which is convenient. Either way, we have a (linear) bijective correspondence between $\{-1,1\}^n$ and $\{0,1\}^n$.

Remark 1.2. *Occasionally we'll refer to the components x_i of a point $x \in \{-1,1\}^n$ as bits.*

Example 1.3. *The `AND` function, which takes $x \in \{-1,1\}^n$ and returns -1 if $x_i = -1$ for all bits x_i, and returns 1 otherwise. Explicitly,*

$$\texttt{AND}(x) = 1 - 2\prod_{i=1}^{n} \frac{1 - x_i}{2}.$$

As a sanity check: if $x_i = 1$ for any i, then the product above is 0 and so $\texttt{And}(x) = 1$. If $x_i = -1$ for all bits, then the product above is 1, meaning $\texttt{And}(x) = -1$.

Example 1.4. *The `PARITY` function, which takes $x \in \{-1,1\}^n$ and returns -1 if there are an odd number of bits wizth $x_i = -1$. Explicitly,*

$$\texttt{PARITY}(x) = \prod_{i=1}^{n} x_i$$

We can also consider Boolean functions as elements of a vector space. To see this, first consider a finite dimensional vector space V spanned by basis elements $\{e_i\}_{i=1}^n$. Then for any $v \in V$ we can write $v = \sum_i e_i v_i$. From here we can consider v as a function $v : \{1, \cdots, n\} \to \mathbb{R}$ where $v(i) = v_i$.

We can run the above argument backwards to say that the Boolean functions $f : \{-1,1\}^n \to \mathbb{R}$ are elements of a 2^n dimensional vector space V. But what's a good basis? And is there still a "natural" inner product to use, like $a \cdot b = \sum_i a_i b_i$ in $\mathbb{R}^n$?

Definition 1.5. *A real multilinear polynomial $p : \mathbb{R}^n \to \mathbb{R}$ is of the form:*

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

where $x^S = \prod_{i \in S} x_i$, $C_S \in \mathbb{R}$, $[n] = \{1, \cdots, n\}$ and $x^\emptyset = 1$.

Remark 1.6. *These polynomials are really affine-linear in each of its components. (check that $p(x_1, \cdots, \lambda x_k, \cdots, x_{2^n}) \neq \lambda p(x)$ by considering something like $p(x_1, x_2) = 1 + x_1 + x_1 x_2$).*

Theorem 1.7. *The monomials x^S form a basis for Boolean functions. In other words, for any $f : \{-1, 1\}^n \to \mathbb{R}$, there exists a unique multilinear polynomial p such that*

$$f(x) = p(x) \quad \text{for all } x \in \{-1, 1\}^n.$$

Proof. We will proceed in two steps. First, we'll show there exists a polynomial p that agrees with f on the hypercube. Then, we show it's unique.

To start with, since the domain of f is discrete, we can decompose f into a linear combination its possible values,

$$f(x) = \sum_{a \in \{-1,1\}^n} f(a) 1_{x=a}(x).$$

If we can show that $1_{x=a}(x)$ can be written as a finite linear combination of monomials, then we've completed the first step. Taking a hint from the `And` function in example 1.3, we can write

$$1_{x=a}(x) = \prod_{i=1}^{n} \frac{1 + a_i x_i}{2}.$$

Indeed, if $a_i \neq x_i$, then $a_i x_i = -1$ and the product is 0. If $a_i = x_i$ for all i , then $a_i x_i = 1$ for all i and the product is 1. Therefore

$$f(x) = \sum_{a \in \{-1,1\}^n} f(a) \prod_{i=1}^{n} \frac{1 + a_i x_i}{2} = \sum_{S \subseteq [n]} C_S x^S,$$

for some $C_S \in \mathbb{R}$. This last equality is valid since any term of the sum involves only monomials in x_i; therefore we may group terms with common monomial terms $\prod_{i \in S} x_i$.

For uniqueness, we will show that x^S are orthonormal with respect to an inner product. Clearly the size of $\{x^S\}_{S \subseteq [n]}$ is 2^n, so orthogonality will imply its a basis. We'll use the inner product

$$\langle f, g \rangle = \frac{1}{2^n} \sum_{x \in \{-1,1\}^n} f(x) g(x) = \mathbb{E}[f(X) g(X)]$$

where X is a uniform random variable over the hypercube (check: the inner product axioms). Choosing $f(x) = x^S$ and $g(x) = x^T$ for two subsets $S, T \subseteq [n]$, we have

$$\mathbb{E}[X^S X^T] = \frac{1}{2^n} \sum_{x \in \{-1,1\}^n} x^S x^T.$$

We can put $x^S x^T$ into the form x^U where $U \subseteq [n]$ is a related subset,

$$x^S x^T = \prod_{i \in S} x_i \prod_{j \in T} x_j = \prod_{i \in S \cup T \setminus (S \cap T)} x_i.$$

To check the last equality, if $i \in S \cap T$, then x_i appears twice in the product and $x_i^2 = 1$, so the components in the intersection $S \cap T$ can be excluded from the product. So,

$$\mathbb{E}[X^S X^T] = \frac{1}{2^n} \sum_{x \in \{-1,1\}^n} x^U.$$

Suppose first that $U \neq \emptyset$. Then we can find some $k \in U$, and

$$\sum_{x \in \{-1,1\}^n} x^U = \sum_{x : x_k = 1} x^U + \sum_{y : y_k = 1} y^U = 0$$

The last equality follows by 1. $x^U = -y^U$ where y is equal to x but with the k^{th} bit flipped, and 2. bit flipping is a bijection so the sizes of the sums are the same.

If instead $U = \emptyset$, then the above reduces to 1. Altogether this means x^S and x^T are orthogonal, and $\{x^S\}_{S \subseteq [n]}$ is a basis for the Boolean functions, so any representation

$$f(x) = \sum_S C_S x^S$$

is unique. □

Definition 1.8. *The coefficients C_S appearing in the unique polynomial $p(x)$ are the Fourier coefficients of f,*

$$\hat{f}(S) = C_S,$$

In this notation, the theorem reads: for any Boolean function $f : \{-1,1\}^n \to \mathbb{R}$,

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S) x^S$$