# Computer Science 294 Lecture 1 Notes

Daniel Raban

January 17, 2023

## 1 Fourier Expansion of Boolean Functions

### 1.1 Boolean functions

**Definition 1.1.** A **boolean function** is a function $f : \{0,1\}^n \to \{0,1\}$.

We can think of this as representing what certain outputs are if we give a certain input to a system. For example,.a boolean function can represent the output of a circuit on certain inputs. In pseudoandomness, we can think of trying to fool this function with psudorandom bits. In social choice, we can think of this as a voting rule which turns individual votes into a joint decision of the group. We can encode a graph $G = (V, E)$ as a boolean string as a $\binom{|V|}{2}$-length string; then the function can specify all graphs with a certain property (e.g. connectedness).

In the boolean domain, we can think of true as 1 and false as 0. This encodes truth values via the finite field $\mathbb{F}_2$. We can also encode via $\mathbb{R}$ by mapping $1 \mapsto -1$ and $0 \mapsto 1$ (i.e. $b \mapsto (-1)^b$). In this case, we can think of a boolean function as $f : \{\pm 1\}^n \to \{\pm 1\}$.

**Example 1.1.** For $n = 3$, we can think of a boolean function as specifying $\pm 1$ on each of the vertices of a cube with vertices $(\pm 1, \pm 1, \pm 1)$.

### 1.2 Expressing boolean functions as polynomials

**Example 1.2.** The function $\max_2 : \{\pm 1\}^2 \to \{\pm 1\}$ is defined by

$$\begin{aligned} \max_2(-1,-1) &= -1 \\ \max_2(-1,1) &= 1 \\ \max_2(1,-1) &= 1 \\ \max_2(1,1) &= 1. \end{aligned}$$

We can also specify the values via a truth table:

| $x_1$ | $x_2$ | $\max_2(x_1, x_2)$ |
|---|---|---|
| $-1$ | $-1$ | $-1$ |
| $-1$ | $1$ | $1$ |
| $1$ | $-1$ | $1$ |
| $1$ | $1$ | $1$ |

We can also think of this function as a polynomial:

$$\max_2(x_1, x_2) = \frac{1}{2} + \frac{1}{2}x_1 + \frac{1}{2}x_2 - \frac{1}{2}x_1x_2$$

**Example 1.3.** Consider the majority vote function $\mathrm{MAJ}_3(x_1, x_2, x_3)$. This can be expressed by the polynomial

$$\mathrm{MAJ}_3(x_1, x_2, x_3) = \frac{1}{2}x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3 - \frac{1}{2}x_1x_2x_3.$$

We will now see how to generally encode boolean functions as polynomials.

**Theorem 1.1** (Fundamental theorem of boolean functions)**.** *Every boolean function* $f : \{0,1\}^n \to \{0,1\}$ *can be uniquely represented as a multilinear polynomial*

$$f(x_1, \ldots, x_n) = \sum_{S \subseteq \{1,\ldots,n\}} c_s \prod_{i \in S} x_i.$$

For notation, we will call $[n] = \{1, \ldots, \}$ $x^S = \prod_{i \in S} x_i$ and $c_s = \widehat{f}(S)$. To see how this works, let's look at a few examples.

**Example 1.4.** To encode $\max_2$ as a polynomial, we want to interpolate between the points we do know. One way to specify this is to add polynomials which evaluate to 0 on all but 1 point:

$$\begin{aligned}\max_2(x_1, x_2) = &\left(\frac{1+x_1}{2}\right)\left(\frac{1+x_2}{2}\right)\cdot(+1) + \left(\frac{1-x_1}{2}\right)\left(\frac{1+x_2}{2}\right)\cdot(+1) \\ &+ \left(\frac{1+x_1}{2}\right)\left(\frac{1-x_2}{2}\right)\cdot(+1) + \left(\frac{1-x_1}{2}\right)\left(\frac{1-x_2}{2}\right)\cdot(-1).\end{aligned}$$

**Example 1.5.** To encode $\mathrm{MAJ}_3$, we would use

$$\mathrm{MAJ}_3 = \left(\frac{1+x_1}{2}\right)\left(\frac{1+x_2}{2}\right)\left(\frac{1+x_3}{2}\right)\cdot(+1) + 7 \text{ other terms.}$$

*Proof.* We can always write

$$f(x) = \sum_{a \in \{\pm 1\}^n} f(a) \left(\frac{1 + a_1 x_1}{2}\right) \left(\frac{1 + a_2 x_2}{2}\right) \cdots \left(\frac{1 + a_n x_n}{2}\right).$$

For uniqueness, observe that we can think of the monomials (or **characters**) $\chi_S(x) := \prod_{i \in S} x_i$ as functions that only care about bits in the set $S$. If we think of $+1$ as true and $-1$ as false, $\chi_S(x)$ is the "x or" function of the bits in $S$. So what we are saying is that

$$f(x) = \sum_{S \subseteq [n]} \widehat{f}(S) \cdot \chi_S(x)$$

is a linear combination of the characters $\chi_S$. So we want to show that $\{\chi_S\}$ is a basis of $V$, the vector space of all functions $f : \{\pm 1\}^n \to \mathbb{R}$. We have shown that these character functions span $V$. We can think of the space $V$ as $\mathbb{R}^{2^n}$ be specifying the outputs on each input. This has dimension $2^n$, which is the same as the number of character functions we have. So this must be a basis, nd every vector is a unique linear combination of $\{\chi_S\}_{S \subseteq [n]}$. □

**Remark 1.1.** It doesn't matter that the range of $f$ is $\{\pm 1\}$. This procedure works the same if the function is real-valued, in general.

### 1.3 Fundamental theorem via inner products of characters

Now we will give another proof of this theorem.

**Definition 1.2.** The **inner product** of $f, g : \{\pm 1\}^n \to \mathbb{R}$ is

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

where we mean that $X$ is uniform on $\{\pm 1\}^n$.

Some sources will use a different normalization factor.
If $f, g : \{\pm 1\}^n \to \{\pm 1\}$, then

$$\begin{aligned} \langle f, g \rangle &= \mathbb{P}_{X \sim \{\pm 1\}^n}(f(X) = g(X)) - \mathbb{P}_{X \sim \{\pm 1\}^n}(f(X) \neq g(X)) \\ &= 1 - 2\mathbb{P}_{X \sim \{\pm 1\}^n}(f(X) = g(X)). \end{aligned}$$

We can think of $\mathbb{P}_{X \sim \{\pm 1\}^n}(f(X) = g(X))$ as a distance between two functions.

**Proposition 1.1.** *The characters are orthogonal to one another.*

**Lemma 1.1.**

$$\chi_S(x)\chi_T(s) = \chi_{S\triangle T}(x).$$

*Proof.*

$$\begin{aligned}\chi_S(x)\chi_T(s) &= \prod_{i\in S} x_i \prod_{j\in T} x_j \\ &= \prod_{i\in S\cap T} x_i^2 \cdot \prod_{j\in S\triangle T} x_j \\ &= \chi_{S\triangle T}(x).\end{aligned}$$

□

**Lemma 1.2.** *If $S \neq \varnothing$, $\mathbb{E}_{X\sim\{\pm1\}^n}[\chi_S(X)] = 0$.*

*Proof.*

$$\mathbb{E}_X[\chi_S(X)] = \mathbb{E}_{X\sim\{\pm1\}^n}\left[\prod_{i\in S} X_i\right]$$

Since the bits are independent,

$$\begin{aligned}&= \prod_{i\in S} \mathbb{E}[X_i] \\ &= 0.\end{aligned}$$

□

Now we can prove the proposition.

*Proof.* Using the two lemmas,

$$\langle \chi_S, \chi_T\rangle = \begin{cases} 1 & S = T \\ 0 & S \neq T, \end{cases}$$

where for $S \neq T$,

$$\langle \chi_S, \chi_T\rangle = \mathbb{E}[\chi_S(X)\chi_T(X)] = \mathbb{E}[\chi_{S\triangle T}(X)] = 0.$$

□

So we have furnished a more non-constructive proof of the fundamental theorem.

**Corollary 1.1.** *The characters $\chi_S$ form an orthonormal basis for the space $V = \{f : \{\pm1\}^n \to \mathbb{R}\}$.*

## 1.4 Fourier inversion formula, Plancherel's identity, and Parseval's identity

**Theorem 1.2** (Inversion formula)**.**

$$\widehat{f}(S) = \langle f, \chi_S \rangle.$$

*Proof.* We can replace $f$ by its **Fourier expansion**:

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

by the orthogonality of the character functions. □

This says that the coefficients capture the correlation of our function with all the character functions.

**Theorem 1.3** (Plancherel's identity)**.**

$$\langle f, g \rangle = \sum_{S \subseteq [n]} \widehat{f}(S)\widehat{g}(S).$$

*Proof.*

$$\begin{aligned}\langle f, g \rangle &= \left\langle \sum_S \widehat{f}(T)\chi_S, \sum_T \widehat{g}(T)\chi_T \right\rangle \\ &= \sum_{S,T} \widehat{f}(S)\widehat{g}(T)\langle \chi_S, \chi_T \rangle \\ &= \sum_S = \widehat{f}(S)\widehat{g}(S) \cdot 1.\end{aligned}$$

□

This says that the Fourier transform preserves the inner product. Here is the case where $f = g$.

**Theorem 1.4** (Parseval's identity)**.** *Let* $\|f\|_2^2 = \langle f, f \rangle = \sum_{S \subseteq [n]} \widehat{f}(S)^2$*, so that* $\|f\|_2 = \sqrt{\mathbb{E}_X[f(X)^2]}$*. If* $f$ *is boolean, then* $\|f\|_2 = 1$*.*

Next time, we will learn about property testing, where we can only test the output of $f : \mathbb{F}_2^n \to \mathbb{F}_2$. We will see how we can check if $f$ is linear.