Analysis of Boolean Functions

Foundations and Applications in TCS.

A Boolean function is a function $f: \{0,1\}^n \to \{0,1\}$.

It can model:

- Set systems in combinatorics

  $A \subseteq \{0,1\}^n \longrightarrow 1_A(x) = \begin{cases} 1 ; & x \in A \\ 0 ; & \text{otherwise.} \end{cases}$

- tests in cryptography / pseudorandomness

  we are trying to "fool".

- concepts and hypotheses in learning theory.
- Error correcting codes.
- Voting rules in social choice, e.g.,

  $x \in \{0,1\}^n$ represents the n votes on a binary decision and $f(x)$ represents the collective decision.

- Graph properties.

and more...

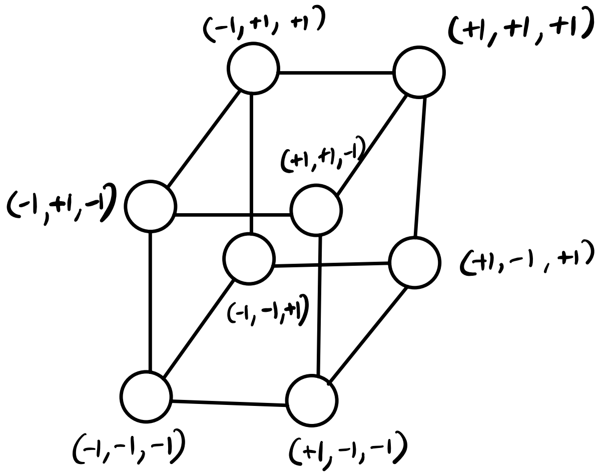
The Boolean Domain: We'll realize the Boolean domain $\{\text{True}, \text{False}\}$ as either $\{0,1\}$ or $\{+1,-1\}$

$b \longrightarrow (-1)^b$

$$\{\underset{F}{0}, \underset{T}{1}\} \qquad \{\underset{F}{+1}, \underset{T}{-1}\}$$

We'll be flexible, but will usually prefer the latter.

The Boolean Hypercube (the domain)



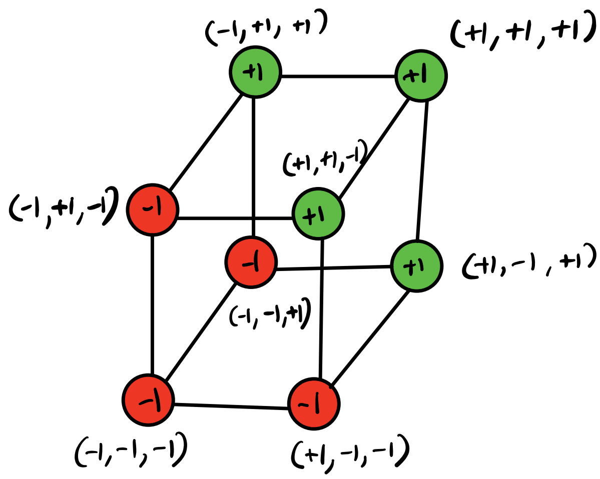
$x \sim y$

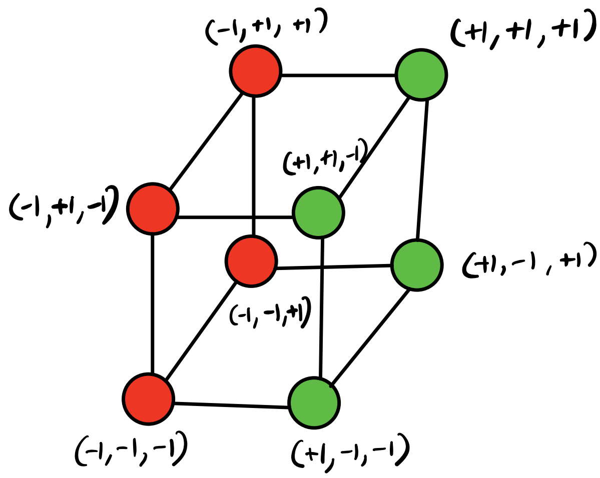
if they differ in exactly one coordinate.

Examples of Boolean Functions

green = +1

red = −1



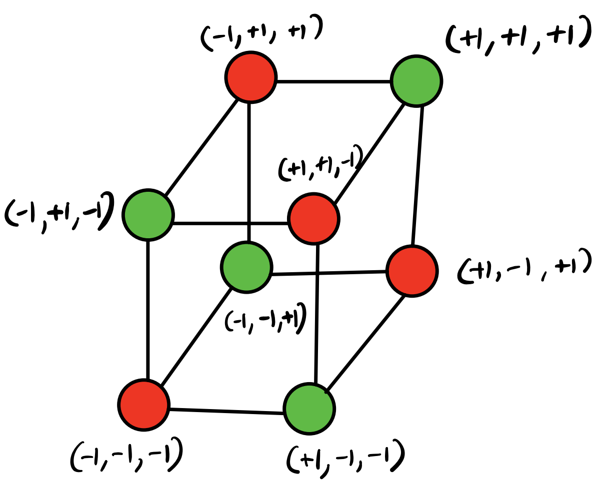


Majority vote

$$\mathrm{Maj}_3(x_1, x_2, x_3) = \begin{cases} +1 & x_1 + x_2 + x_3 > 0 \\ -1 & \text{otherwise} \end{cases}$$

Dictatorship

$$f(x_1, x_2, x_3) = x_1$$



Parity

$$\mathrm{Parity}_3(x_1, x_2, x_3) = x_1 \cdot x_2 \cdot x_3$$

The Fundamental Theorem of Boolean Functions:

Every Boolean function $f:\{\pm1\}^n \to \{\pm1\}$ can be uniquely represented as a multilinear polynomial over $\mathbb{R}$:

$$f(x) = \sum_{S\subseteq\{1,\dots,n\}} c_S \cdot \prod_{i\in S} x_i$$

where $c_S \in \mathbb{R}$

E.g. $\mathrm{Maj}_3(x_1,x_2,x_3) = \underset{\substack{\uparrow \\ \langle \mathrm{MAJ}_3,\, x_1\rangle}}{\tfrac{1}{2}} x_1 + \tfrac{1}{2}x_2 + \tfrac{1}{2}x_3 - \tfrac{1}{2}x_1x_2x_3$

First proof of Existence – Polynomial Interpolation

We construct the polynomial from the function truth-table by interpolation. Example: $\max_2(x_1,x_2)$

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

$$\begin{aligned}\max_2(x_1,x_2) = {} & \left(\tfrac{1-x_1}{2}\right)\left(\tfrac{1-x_2}{2}\right)\cdot(-1) \\ & + \left(\tfrac{1-x_1}{2}\right)\left(\tfrac{1+x_2}{2}\right)\cdot(+1) \\ & + \left(\tfrac{1+x_1}{2}\right)\left(\tfrac{1-x_2}{2}\right)\cdot(+1) \\ & + \left(\tfrac{1+x_1}{2}\right)\left(\tfrac{1+x_2}{2}\right)\cdot(+1). \\ = {} & \tfrac{1}{2} + \tfrac{1}{2}x_1 + \tfrac{1}{2}x_2 - \tfrac{1}{2}x_1x_2.\end{aligned}$$

More generally:

$$f(x) = \sum_{a \in \{\pm 1\}^n} f(a) \cdot \underbrace{\left(\frac{1+a_1x_1}{2}\right) \cdots \left(\frac{1+a_nx_n}{2}\right)}_{\text{indicates that } x=a}$$

Note: The proof works for any $f : \{\pm 1\}^n \to \mathbb{R}$.

The Fundamental Theorem of Boolean Functions:

Every ~~Boolean~~ function $f : \{\pm 1\}^n \to \mathbb{R}$ can be uniquely represented as a multilinear polynomial over $\mathbb{R}$:

$$f(x) = \sum_{S \subseteq \{1,\dots,n\}} \hat{f}(S) \cdot \underbrace{\chi_S(x)}_{\prod_{i \in S} x_i}$$

where $\hat{f}(S) \in \mathbb{R}$ is called the S-Fourier coef.

$\chi_S(x) = \prod_{i \in S} x_i$ is called the S-Fourier character.

Note: χ_S is also a Boolean Function

$$\chi_S : \{\pm 1\}^n \to \{\pm 1\} \qquad \chi_S(x_1,\dots,x_n) = \prod_{i \in S} x_i$$

Uniqueness: $V_n = \{f : \{\pm 1\}^n \to \mathbb{R}\}$ is a vector space of dimension 2^n.

The characters $\{\chi_S : S \subseteq [n]\}$ span V.

Since there are 2^n of them, they form a basis.

$\Rightarrow$ the Fourier repr is unique. $\blacksquare$

Second Proof of Fundamental Thm

Define the inner product of two functions $f, g : \{\pm 1\}^n \to \mathbb{R}$

as $$\langle f, g \rangle \triangleq \mathop{\mathbb{E}}_{x \in_R \{\pm 1\}^n} [f(x) \cdot g(x)]$$

Lemma: The characters $\{\chi_S : S \subseteq [n]\}$ form an orthonormal basis of V_n.

Proof. Let $S, T \subseteq [n]$ $\quad S \neq T$.

$$\begin{aligned}
\langle \chi_S, \chi_T \rangle &= \mathop{\mathbb{E}}_{x \in \{\pm 1\}^n} [\chi_S(x) \cdot \chi_T(x)] \\
&= \mathop{\mathbb{E}}_{x \in \{\pm 1\}^n} \Big[\prod_{i \in S} x_i \cdot \prod_{i \in T} x_i \Big] \\
&= \mathop{\mathbb{E}}_{x \in \{\pm 1\}^n} \Big[\prod_{i \in S \Delta T} x_i \cdot \cancel{\prod_{i \in S \cap T} x_i^2} \Big] \\
&= \prod_{i \in S \Delta T} \mathop{\mathbb{E}}_{x \in \{\pm 1\}^n} [x_i] \qquad \text{(since } x_1, \dots, x_n \text{ are independent)} \\
&= 0.
\end{aligned}$$

$$\langle \chi_S, \chi_S \rangle = 1.$$

So $\{\chi_S : S \subseteq [n]\}$ are orthonormal $\Rightarrow$ linearly independent. As there are 2^n of them $\Rightarrow$ they form a basis for V_n. $\blacksquare$

Inversion Formula: $\hat{f}(S) = \langle f, \chi_S \rangle$.

Proof:

$$\langle f, \chi_S \rangle = \Big\langle \sum_{T \subseteq [n]} \hat{f}(T)\chi_T, \chi_S \Big\rangle$$

$$= \sum_{T \subseteq [n]} \hat{f}(T) \langle \chi_T, \chi_S \rangle$$

$$= \hat{f}(S).$$

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

Proof:

$$\langle f, g \rangle = \Big\langle \sum_{S \subseteq [n]} \hat{f}(S)\chi_S, \sum_{T \subseteq [n]} \hat{g}(T)\chi_T \Big\rangle$$

$$= \sum_{S, T \subseteq [n]} \hat{f}(S)\hat{g}(T) \langle \chi_S, \chi_T \rangle$$

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

Parseval: $\mathbb{E}_{x \in \{\pm 1\}^n}[f(x)^2] = \langle f, f \rangle = \sum_{S \subseteq [n]} \hat{f}(S)^2$.

Fourier coefficients are an alternative repr of a Boolean function compared to truth-table.

They encode "global" properties, e.g.

$$\hat{f}(\phi) = \langle f, \chi_\phi \rangle = \mathbb{E}_{x \in_R \{\pm 1\}^n}[f(x) \cdot 1]$$

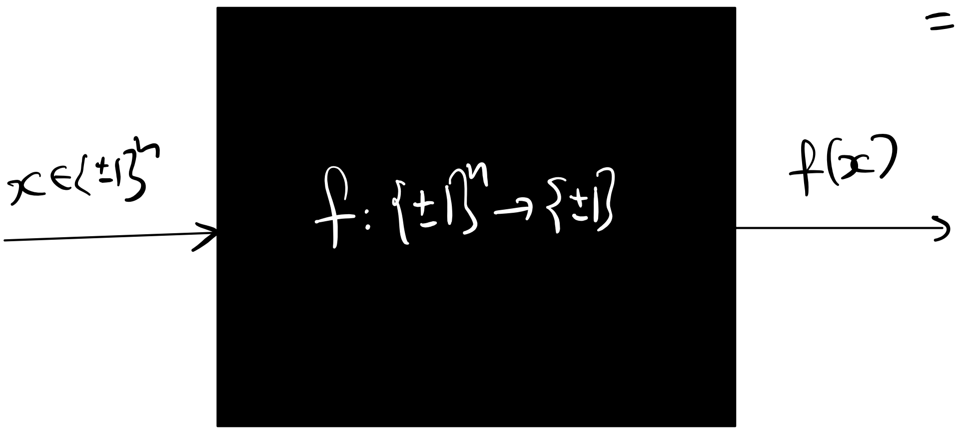
$$\mathrm{Var}[f] = \mathbb{E}_{x \in \{\pm 1\}^n}[f(x)^2] - \mathbb{E}_{x \in \{\pm 1\}^n}[f(x)]^2 = \sum_{\phi \neq S \subseteq [n]} \hat{f}(S)^2.$$

" $\langle f, x_i \rangle = \mathbb{E}_x[f(x) \cdot x_i]$

$$\hat{f}(\{i\}) = \frac{\mathbb{E}[f(x) \mid x_i = 1] - \mathbb{E}[f(x) \mid x_i = -1]}{2}.$$

Application: Linearity Testing

$$\chi_S(x)\cdot\chi_S(y) = \chi_S(x\cdot y)$$



Given Black-Box access to a Boolean function f, want to tell whether f is a character.

The Characters are multiplicative over $\{\pm 1\}$ $\iff$ linear over $\mathbb{Z}_2$.

Blum, Luby, Rubinfeld

[BLR]:
- Pick random $x, y \in_R \{\pm 1\}^n$ independently.
- check if $f(x)\cdot f(y) = f(x\cdot y)$.

Def'n: $f, g : \{\pm1\}^n \to \{\pm 1\}$. $\mathrm{dist}(f,g) = \Pr_{x\in\{\pm1\}^n}[f(x) \neq g(x)]$.

Thm: 1. If f is a character, then the BLR test always accepts.

2. If f is ε-far from all characters, then the BLR test rejects w.p. $\geq \varepsilon$.

Proof: (1) is clear. We prove (2).

Let $f: \{\pm 1\}^n \to \{\pm 1\}$

$$1-\varepsilon \le \Pr[\text{BLR accepts } f]$$

$$= \Pr_{x,y}[f(x)\cdot f(y) = f(x\cdot y)]$$

$$= \mathop{\mathbb{E}}_{x,y}\left[\frac{1+f(x)f(y)f(x\cdot y)}{2}\right]$$

By rearranging,

$$1-2\varepsilon \le \mathop{\mathbb{E}}_{x,y}[f(x)f(y)f(x\cdot y)]$$

$\chi_R(x)\cdot\chi_R(y)$

$\|$

$$= \mathop{\mathbb{E}}_{x,y}\left[\sum_{S\subseteq[n]}\hat{f}(S)\cdot\chi_S(x)\cdot\sum_{T\subseteq[n]}\hat{f}(T)\cdot\chi_T(y)\cdot\sum_{R\subseteq[n]}\hat{f}(R)\chi_R(x\cdot y)\right]$$

$$= \sum_{S,T,R\subseteq[n]}\hat{f}(S)\cdot\hat{f}(T)\cdot\hat{f}(R)\cdot\mathop{\mathbb{E}}_x[\underbrace{\chi_S(x)\chi_R(x)}]\mathop{\mathbb{E}}_y[\underbrace{\chi_T(y)\chi_R(y)}]$$

$$= \sum_{S\subseteq[n]}\hat{f}(S)^3$$

Parseval

$$\le \max_{S:S\subseteq[n]}\hat{f}(S)\cdot\left(\sum_{S\subseteq[n]}\hat{f}(S)^2\right) = \max_{S:S\subseteq[n]}\hat{f}(S)$$

So, there exists a character χ_S s.t. $1-2\varepsilon \le \langle f,\chi_S\rangle$.

$$1-2\varepsilon \le \langle f,\chi_S\rangle = \Pr_x[f(x)=\chi_S(x)] - \Pr_x[f(x)\ne\chi_S(x)]$$

$$= 1-2\cdot\Pr_x[f(x)\ne\chi_S(x)] = 1-2\cdot\mathrm{dist}(f,\chi_S)$$

Thus, $\mathrm{dist}(f,\chi_S)\le\varepsilon$. $\blacksquare$