Fourier Analysis of Boolean Functions

John Augustine (IIT Madras)

Krishna Palem (RICE University)

Source:
These slides are based on source material (including notation, concepts, and presentation approach) from *Analysis of Boolean Functions* by *Ryan O'Donnell* (Published 2014 by Cambridge University Press).

Acknowledgement: We thank Ashutosh Ingole (IIT Madras) for collaboration that resulted in these slides.

Topics in this Lecture

1. Introduction to boolean Functions
   - 1.a Hamming Cube
2. Fourier Expansion of boolean Functions
   - 2.a Multilinear Polynomials and Fourier Expansion
   - 2.b Parity Functions
3. Parity Functions as the Orthonormal Basis for Fourier Expansion

Introduction to Boolean Functions

A Broad Perspective of Computation

- Input is encoded as a sequence of bits.
- Output: some function of the input bits.
  - Often an integer or a real number. E.g., computing mean.
  - Sometimes, even just a bit: E.g., Is the input graph connected?
- Our focus on boolean functions is based on this perspective.

General Definition of Boolean Functions

$$f: \{0,1\}^n \rightarrow \mathbb{R}$$

- A boolean function maps n length binary vectors to $\mathbb{R}$.
- An alternative representation of "bits" is $\{-1, +1\}$.
- An important special case is

$$f: \{-1, +1\}^n \rightarrow \{-1, +1\}$$

Example of Boolean Function

- Example: Consider a boolean function max_2, which returns maximum of 2 input bits,

$$max_2 : \{-1, +1\}^2 \rightarrow \{-1, +1\}$$

- There are four different possible input strings for boolean function max_2. Outputs for these input strings are shown below.

$$max_2(+1, +1) = +1$$
$$max_2(-1, +1) = +1$$
$$max_2(+1, -1) = +1$$
$$max_2(-1, -1) = -1$$

Vector Representation of Boolean Functions

- Let $f: \{-1, +1\}^n \rightarrow \mathbb{R}$ be an arbitrary boolean function.
- Consider the 2^n distinct input bit strings in a *fixed or chosen* order.
- Arranging the corresponding output values (in the chosen order) as a column vector gives a vector representation of boolean function f.

Example:
Consider the order of 2-bit inputs:
$(\{+1, +1\}, \{-1, +1\},$
$\{+1, -1\}, \{-1, -1\})$

The vector representation of max_2 is

$$\begin{bmatrix} +1 \\ +1 \\ +1 \\ -1 \end{bmatrix}$$

Towards the Standard Basis

- Let $\mathbf{V}$ be the vector space of all boolean functions.
- For any boolean function in this space, there are total 2^n possible input strings.
- Take one such boolean function from $\mathbf{V}$ which outputs 1 for the first string, and for the remaining $2^n - 1$ of the input strings it outputs 0.
- Take another boolean function which behaves the same way for the second input string……

Standard Basis (contd.)

- Similarly, we can find all 2^n such boolean functions, which output 1 only for one particular input string i, $1 \leq i \leq 2^n$ and 0 for remaining $2^n - 1$.
- Notice that the vectors representing these 2^n boolean functions forms a Basis.
  - Using vectors from this basis, we can generate any other vector in $\mathbf{V}$.
  - Verify!
- This particular basis is called *standard basis*.

Inner Product of Two Functions

- Being a vector space, we now wish to define a suitable inner product, denoted by "$\langle \cdot, \cdot \rangle$".
- Recall that the usual inner product on a pair of functions f and g would correspond to

$$\langle f, g \rangle = \sum_{x \in \{-1,+1\}^n} f(x) g(x) .$$

- For our purposes, it is more convenient to scale this by a factor of $\frac{1}{2^n}$ making it an average rather than a sum.

Inner Product of Two Functions (contd.)

- So formally, we define an *inner product*, on a pair of boolean functions $f, g: \{-1, +1\}^n \to \mathbb{R}$ by

$$\langle f, g \rangle = \frac{1}{2^n} \sum_{x \in \{-1,+1\}^n} f(x) g(x) .$$

- This is equivalent to saying that inner product is the expected value of the product of f and g when the input string is drawn uniformly at random.

$$\langle f, g \rangle = E_{x \sim \{-1,+1\}^n}[f(x) g(x)]$$

- Here $x \sim \{-1, +1\}^n$ means x is chosen uniformly at random from $\{-1, +1\}^n$

Fourier Expansion of Boolean Functions

Multilinear Polynomials

- A *multilinear polynomial* is a polynomial that is linear in each of its variables.
- The degree of a multilinear polynomial is the maximum number of distinct variables occurring in it.
- Example: A simple example of multilinear polynomial is

$$ax_1 + bx_2 + cx_1x_2 + d.$$

- In the above example, a, b, c and d are constants, x_1 and x_2 are variables.
- $ax_1^2 + bx_2 + cx_1x_2 + d$ is not a multilinear polynomial, because the polynomial is not linear in x_1.

Fourier Expansion

- The Fourier expansion of a boolean function is its representation as a real valued multilinear polynomial.
- Example: Recall the boolean function max_2, which returns maximum of 2 bits,

$$max_2(+1,+1) = +1,$$
$$max_2(-1,+1) = +1,$$
$$max_2(+1,-1) = +1,$$
$$max_2(-1,-1) = -1.$$

- What can be a multilinear polynomial for max_2?

Fourier Expansion (contd.)

- The multilinear polynomial for max_2 is given below,

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

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

Fourier Expansion (contd.)

- Another example of boolean function is maj_3 which returns the majority of 3 input bits.

$$maj_3 : \{-1, +1\}^3 \rightarrow \{-1, +1\}$$

- Can you determine its multilinear polynomial ?

Fourier Expansion (contd.)

- The multilinear polynomial for boolean function maj_3 is given below,

$$maj_3(x_1, x_2, x_3) = \frac{1}{2}x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3 - \frac{1}{2}x_1x_2x_3$$

- How can we determine a Fourier Expansion for any given boolean function ?

Determining Multilinear Polynomials

- Useful Definition: The *indicator polynomial* for each input bit string $a = (a_1, \ldots, a_n) \in \{-1, +1\}^n$, denoted by $1_{\{a\}}(x)$, takes value 1 when $x = a$ and value 0 when $x \neq a$.

- Thus, we can "construct" f as follows.

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

Determining Multilinear Polynomials (contd.)

- Let us first focus our efforts in constructing $1_{\{a\}}(x)$. We do this in two steps.
  1. For each index i, we want a monomial m_i in x_i that evaluates to 1 iff $a_i = x_i$. Otherwise, m_i = 0.

     Attempt 1: $m_i = a_i x_i$. Why does this fail? How to fix it?

     Attempt 2: $m_i = (1 + a_i x_i)/2$. Verify that it works using the fact that the values of x_i are +1 or -1.
  2. With m_i indicating if $a_i = x_i$, we can now compose them to get:

$$1_{\{a\}}(x) = m_1 \times m_2 \times \cdots \times m_n.$$

$1_{\{a\}}(x) = 0$ if at least one $m_i = 0$ for $1 \leq i \leq n$ and

$1_{\{a\}}(x) = 1$ otherwise.

Determining Multilinear Polynomials (contd.)

- For each input bit string a we can represent the indicator polynomial $1_{\{a\}}(x)$ as follows,

$$1_{\{a\}}(x) = \left(\frac{1 + a_1 x_1}{2}\right)\left(\frac{1 + a_2 x_2}{2}\right)\ldots\ldots\left(\frac{1 + a_n x_n}{2}\right)$$

- Recall that, $x = (x_1 \ldots\ldots\ldots x_n)$ and $x_i \in \{-1, +1\}$.
- How can we now construct the multilinear polynomial for boolean function max_2 ?

Determining Multilinear Polynomials (contd.)

- In the previous equation, for boolean function max_2, there are total four distinct possible input sequences.
- Hence, there are four distinct indicator polynomials corresponding to these input sequences.
- Taking summation of each indicator polynomial multiplied by its function value gives the desired multilinear polynomial.

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

Function value

Indicator polynomial

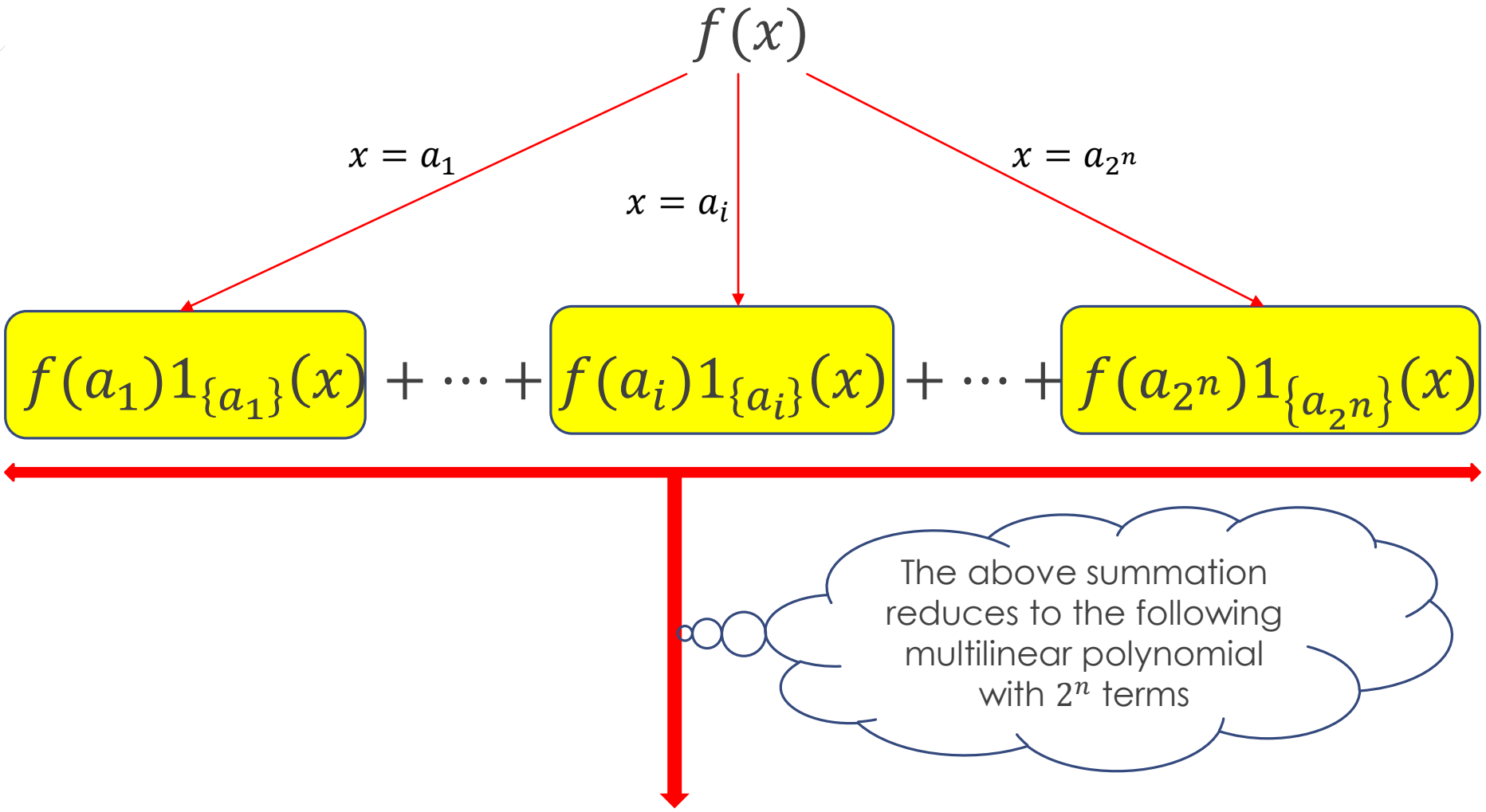
Determining Multilinear Polynomials and hence the Fourier Expansion

- For boolean function max_2, considering indicator polynomial for each input bit string a
  - Using the form $f(x) = \sum_{a \in \{-1,1\}^n} f(a) 1_{\{a\}}(x)$, we get the following equation.

(Note: in this slide, we will use "1" to represent "+1")

$$max_2(x) = \left\{ \begin{array}{ll} & 1\left(\frac{1+x_1}{2}\right)\left(\frac{1+x_2}{2}\right) \\ + & 1\left(\frac{1-x_1}{2}\right)\left(\frac{1+x_2}{2}\right) \\ + & 1\left(\frac{1+x_1}{2}\right)\left(\frac{1-x_2}{2}\right) \\ + & (-1)\left(\frac{1-x_1}{2}\right)\left(\frac{1-x_2}{2}\right) \end{array} \right\} = \frac{1}{2} + \frac{1}{2}x_1 + \frac{1}{2}x_2 - \frac{1}{2}x_1x_2$$

Extending our Methods to any Boolean Function



Towards an Alternative Basis using Fourier Expansion

- The total number of terms in general expansion of multilinear polynomial on previous slide is 2^n, which is same as the dimension of the vector space of boolean functions.
- Notice that the variables in each term of the expansion are themselves boolean functions, called monomials.
- We will see shortly that any boolean function can be represented as a unique linear combination of monomials.
- Finally, we will show that these monomials form a basis for the vector space of all boolean functions, that is different from the standard basis we have seen earlier.

Additional Useful Definition: Monomials of Multilinear Polynomials

- Consider $S \subseteq [1,2,\cdots,n]$
  - then the monomial corresponding to S is written as

$$x^S = \prod_{i \in S} x_i \quad (with\ x^{\phi} = 1\ by\ convention, x_i \in \{-1, +1\})$$

here, x_i is the i^{th} bit in the input string.

- Note that there can be 2^n possible monomials, one corresponding to each set S.
- Our goal is to express multilinear polynomials as sums of 2^n monomial terms one for each $S \subseteq [1,2,\cdots,n]$.
- For every such monomial term in a multilinear polynomial, we will denote its coefficient by $\hat{f}(S)$.

Theorem 1

Theorem: We can express any boolean function $f:\{-1,+1\}^n \to \mathbb{R}$ *uniquely* as a multilinear polynomial,

$$f(x) = \sum_{S \subseteq [1 \cdots n]} \hat{f}(S) x^S$$

Justified shortly

- The above expression is called the Fourier expansion of boolean function f.
- $\hat{f}(S)$ are Fourier coefficients.
  - In general, the values of $\hat{f}(S)$ are real.
- Collectively, the Fourier coefficients are called the Fourier spectrum of f.

Theorem 1 (contd.)

- For boolean function max_2, the multilinear polynomial is

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

- Therefore the Fourier coefficients are

$$\widehat{max_2}(\phi) = \frac{1}{2}$$

$$\widehat{max_2}(\{1\}) = \frac{1}{2}$$

$$\widehat{max_2}(\{2\}) = \frac{1}{2}$$

$$\widehat{max_2}(\{1,2\}) = -\frac{1}{2}$$

Interpreting x^S as Parity Functions

- Notice that x^S is itself a boolean function.
- x^S is the logical parity or exclusive-or(XOR) of the bits corresponding to the indices in S, which we will refer to as the parity function.

$$x^S = \prod_{x_i \in S} x_i$$

- Hence the Fourier expansion

$$f(x) = \sum_{S \subseteq [1 \cdots n]} \hat{f}(S) x^S \qquad ..(1)$$

is a linear combination of parity functions.

Example: max_2. Consider a fixed order of input (+1,+1),(-1,+1),(+1,-1) and (-1,-1).For max_2, we have four parity functions $x^{\phi}, x^{\{1\}}, x^{\{2\}}$ and $x^{\{1,2\}}$. Each one of them can be represented as a vector, e.g.

$$x^{\{1,2\}} = \begin{bmatrix} +1 \\ -1 \\ -1 \\ +1 \end{bmatrix}.$$

Parity Functions as the Orthonormal Basis for Fourier Expansion

Basis for Fourier Expansion or Fourier Basis

- We will now see how parity functions form a basis.
  - We will call this a Fourier Basis.
- What are some interesting properties of this basis?

Parity Functions as the Orthonormal Basis for Fourier Expansion

- The Fourier expansion in $eq.(1)(slide\ no.30)$, shows that every boolean function in $\mathbf{V}$ is a linear combination of the parity functions.
  - Parity functions are a spanning set for the vector space of all boolean functions.
- Since the number of parity functions is

$$2^n = \dim(\mathbf{V})$$

we can deduce that they are in fact a linearly independent basis for $\mathbf{V}$.

Parity Functions as the Orthonormal Basis for Fourier Expansion (contd.)

- The previous argument justifies the uniqueness of the Fourier expansion stated in Theorem 1.
  - Follows from the linear independence of parity functions and the cardinality of parity functions is equal to the dimension of $\mathbf{V}$.
- Now that we know parity functions form a basis, and any boolean function can be represented as the linear combination of parity functions, we can actually replace boolean functions by there respective vector representations and then same fact holds for the vectors too.
- We will verify this with our favorite boolean function max_2.

Example: Boolean function max_2

- Example: boolean function max_2 has four(2^2) parity functions, $x^{\phi}, x^{\{1\}}, x^{\{2\}}$ and $x^{\{1,2\}}$.
  - Each parity function can be represented as a vector in $\mathbf{V}$. For this purpose, we will consider a fixed order of input strings, $(+1,+1), (-1,+1), (+1,-1)$ and $(-1,-1)$.

$$\begin{array}{lcccc} input\ strings & x^{\phi} & x^{\{1\}} & x^{\{2\}} & x^{\{1,2\}} \\ (+1,+1) \rightarrow & +1 & +1 & +1 & +1 \\ (-1,+1) \rightarrow & +1 & -1 & +1 & -1 \\ (+1,-1) \rightarrow & +1 & +1 & -1 & -1 \\ (-1,-1) \rightarrow & +1 & -1 & -1 & +1 \end{array}$$

- Recall: the vector representation of max_2 is $\begin{bmatrix} +1 \\ +1 \\ +1 \\ -1 \end{bmatrix}$

Example: Boolean function max_2

- Recall that the multilinear polynomial of max_2 is

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

- This is equivalent to

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

- Using vector notations, we have

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