IIT Kanpur

Lecture 1: Introduction

Scribe: Anindya Ganguly   Lecture: Rajat Mittal

October 22, 2021

1 Domain of a Boolean Functions

Domain of a Boolean functions is either $\{-1,1\}^n$ or $\{0,1\}^n$. Till the date, we had visualized this as a Boolean hypercube. However, we do not thought it as an algebraic structure like group or field.

Definition of $\mathbb{F}_2$*:* $\mathbb{F}_2 = \{0,1\} \mod 2$ operation under addition and multiplication.

Definition of $\mathbb{F}_2^n$*:* It is a n-bit binary string. Note that, it is not a finite field. Since $\mathbb{F}_2^n$ does not form an integral domain. However this forms a vector space. In this vector space constant are only 0, and 1.

The number of elements of $\mathbb{F}_2^n$-vector space is 2^n and bases vectors are the standard bases vector. Dot product of any two vectors $x = (x_i)_{i=1}^n$; $x = (x_i)_{i=1}^n$ is defined as $\sum_{i=1}^n x_i y_i \mod 2$

2 Subspaces in $\mathbb{F}_2^n$

Every subset of $\mathbb{F}_2^n$ is not a subspace. For example, consider $\{00\cdots0,\ 10\cdots0,\ 00\cdots1\}$. See some two non-identity element does not belongs to the set. The subset follows the axioms of subspace are known as subspace of $\mathbb{F}_2^n$. Trivially, $\{(000\cdots0)\}$ is a zero dimension subspace. See, $S' = \{(000\cdots0), \alpha\}$ is a dimension one subspace having two elements, where α is any n-bit binary string. In the similar fashion we may conclude that a k-dimension has 2^k elements. Since any vector v in this subspace can be written as $\alpha = \Sigma_{i=1}^n \alpha_i v_i$; where $(v_i)_{i=1}^n$ are basis vectors and α_i's are scalar. For details one may visit [2].

3 Orthogonal Complement

Let A be a subspace of $\mathbb{F}_2^n$. Then orthogonal complement of A is denoted by $A^\perp$ and defined as set of all vectors for which dot product will vanish. Mathematically we can express it as

$$A^\perp = \{\gamma \in \mathbb{F}_2^n \ : \ \gamma \cdot x \ \ \forall x \in A\}$$

It can be easily establish that $A^\perp$ is a subspace of $\mathbb{F}_2^n$. To prove the statement take any two vectors α, β from $A^\perp$. Then $(c\alpha + \beta) \cdot x = c\alpha \cdot x + \beta \cdot x = 0$. This shows that $c\alpha + \beta \in A^\perp$.

Assume that, dimension of the subspace A is k, then dimension of $A^\perp$ is $n-k$. Therefore, $A^\perp$ has 2^{n-k} elements. So the mathematical formula for dimension of $A^\perp$= dimension of vector space − dimension of subspace A.Right now we are interested in $(A^\perp)^\perp$. Surprisingly, $(A^\perp)^\perp = A$.

Proof:

* $A \subseteq (A^\perp)^\perp$: Let $w \in A$, then $< w, v >= 0 \ \forall v \in A^\perp$. Hence $w \in (A^\perp)^\perp$.

* To complete the proof we use $\dim A + \dim A^{\perp} = n$. It is enough to show that $\dim A = \dim\ (A^{\perp})^{\perp}$.

$$\dim\ (A^{\perp})^{\perp} = n - \dim A^{\perp} = n - (n - \dim A) = \dim A$$

Hence we have establish the fact.

Subcube of $\mathbb{F}_2^n$

This concept is coming from our intuition of hypercube.

Definition: Set of inputs where certain co-ordinates are fixed. For example, $\{000, 100\}$ is a subcube of $\mathbb{F}_2^n$. See here we are assign $x_2 = 0;\ x_3 = 0$. Now if we fix k-variables out of n, then size of subcube is 2^{n-k}. Set of the inputs in decision tree is a good example for subcube.

Next genuine question comes in our mind is *Is every subcube is a subspace?* The answer is no. Also, a subspace need not be a subcube. For example take $\{00\cdots0,\ 11\cdots1\}$. Clearly it is a subspace, but it is not a subcube. Because it can not possible to set any subset of variable such that only two elements get a subspace.

Affine Subspace

The only subspace of $\mathbb{R}^2$ are line passing through the origin. However, any line passing parallel to these also a kind of subspace. This can be thought as translation of subspaces. Such subspaces are known as *affine subspaces*. Therefore, the mathematical definition for an affine subsapce A is

$$A = H + a = \{x + a\ :\ x \in H\}$$

where H is a known subspace and a is the translation. Note that, affine subspace are not in general forms a

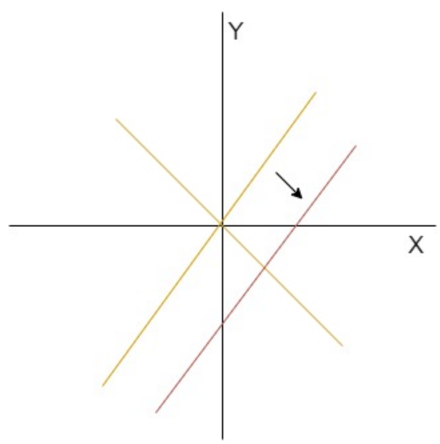

Figure 1: Affine Subspace (red line)

subspace. However subcube is an affine subspace. Now we give an example which is an affine subspace but not a subspace and not a subcube. Consider the subspace $H = \{00\cdots0,\ 11\cdots1\}$ along with the translation $a = 1010\cdots01$. Then,

$$H + a = \{101010\cdots01,\ 010101\cdots0\}.$$

This $H + a$ does not form a subspace and also does not form a subcube. The relation between affine subspace, subcube and subspace reflects on the diagram.

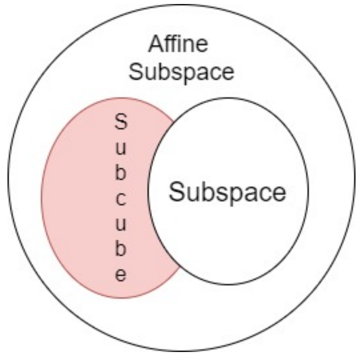

Figure 2: Relation between subcube subspace and affine subspace

Parities

Now we define paritie in different way.

$$\chi_S(x) = \Pi_{i \in S}\ x_i$$

Let say γ be the indicator of the subset S. Take an example: $n = 5$, and $S = \{x_1, x_2, x_3\}$ then $\gamma = 11010$ is the indicator variable. It is obvious to index the Fourier characters $\chi_S : \mathbb{F}_2^n \rightarrow \ \{-1, 1\}$ not by subsets $S \subseteq [n]$ but by their 0-1 indicator vectors $v \in \mathbb{F}_2^n$; hence

$$\chi_\gamma(x) = (-1)^{\gamma \cdot x},$$

where the dot product is performed in $\mathbb{F}_2^n$. We are looking to the value of $\chi_\beta \chi_\gamma$; where S_β, and S_γ are subsets corresponding to β and γ. Then

$$\chi_\beta \chi_\gamma = \chi_{\beta+\gamma} \quad \forall \beta,\ \gamma$$

where $S_{\beta \Delta \gamma}$ is the set corresponding to $\beta + \gamma$.

We know that the characters form a group under multiplication, this group isomorphic to the group $\mathbb{F}_2^n$ under multiplication. To avoid confusion let define this group as $\widehat{\mathbb{F}_2^n}$. Next write the Fourier expression of $f : \mathbb{F}_2^n \rightarrow \ \mathbb{R}$ as:

$$f(x) = \sum_{\gamma \in \widehat{\mathbb{F}_2^n}} \hat{f}(\gamma) \chi_\gamma(x).$$

The Fourier transform of f is visualized as a $\hat{f} : \widehat{\mathbb{F}_2^n} \rightarrow \mathbb{R}$. It is possible to measure its complexity with 2-norms.

$$\hat{\|} f \hat{\|}_2 = \|\hat{f}\|_2^2 = \sum_{\gamma \in \widehat{\mathbb{F}_2^n}} (\hat{f}(\gamma))^2.$$

It is the Parseval's identity. Now we focused on $\hat{\|} f \hat{\|}_1$.

$$\hat{\|} f \hat{\|}_1 = \sum_{\gamma}\ |\hat{f}(\gamma)|.$$

Clearly this value is always greater than or equal to 1. Question is how big it will or can we bound it using some inequality. Take a help from Cauchy-Schwarz inequality

$$\sum_{\gamma} |\hat{f}(\gamma)| \geq \sqrt{2^n}$$

Indicator function for a subspace

Recall our subspace A of $\mathbb{F}_2^n$. Now indicator function for a subspace is $\mathbf{1}_A : \mathbb{F}_2^n \to \{0,1\}$ and it is defined as

$$\mathbf{1}_A \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases} \tag{1}$$

Remark: Since $A = (A^{\perp})^{\perp}$, so $x \in A$ iff $\gamma \cdot x \quad \forall x \in A^{\perp}$.

Fourier expression for the indicator function $\mathbf{1}_A$ is expressed as

$$\mathbf{1}_A = \frac{1}{2^k} \sum_{\gamma \in A^{\perp}} x_{\gamma},$$

where k is the dimension of $A^{\perp}$, that is the co-dimension of A.

Aim is to establish this expression correctly represent $\mathbf{1}_A$. That is if $x \in A$, then $\mathbf{1}_A = 1$ otherwise $\mathbf{1}_A = 0$.

$$1 \in A \Rightarrow \ \chi_{\gamma}(x) = (-1)^{\gamma \cdot x} = 1 \text{ (because } \gamma \cdot x = 0 \ \ \forall \gamma \text{)}$$

$$\chi_{\gamma}(x) = 1 \ \ \forall \gamma \in A^{\perp}$$

$$\Rightarrow \mathbf{1}_A = \frac{1}{2^k} \cdot 2^k = 1$$

Now $x \notin A \ \Rightarrow$ there exist $\gamma \in A^{\perp}$ such that $\gamma \cdot x = 1$

$$A^{\perp} = \cup_y \ (y, y+\gamma)$$

$$\mathbf{1}_A(x) = \ \frac{1}{2^k} \sum_{\gamma \in A^{\perp}} \chi_{\gamma} = \ \frac{1}{2^k} \left[\sum_y \chi_y(x) + \sum_y \chi_{y+\gamma}(x) \right]$$

$$= \frac{1}{2^k} \left[(-1)^{y \cdot x} + (-1)^{y \cdot x + x \cdot \gamma} \right] = 0$$

Hence the result.

Acknowledgement Thanks to the [1].

References

[1] O'Donnell, Ryan. Analysis of boolean functions. Cambridge University Press, 2014.

[2] Strang, Gilbert, et al. Introduction to linear algebra. Vol. 3. Wellesley, MA: Wellesley-Cambridge Press, 1993.