ON THE FOURIER ANALYSIS OF BOOLEAN FUNCTIONS AND THE LINAI-MANSOUR-NISAN THEOREM

EDWARD KIM

Abstract. We briefly summarize the basic tools of Fourier Analysis applied to the finite abelian group $\mathbb{Z}_2^n$. By viewing boolean functions $f : \{0,1\}^n \to \{0,1\}$ as square-integrable maps in the Hilbert space $L^2(\mathbb{Z}_2^n)$ under the uniform probability measure, we derive the Linai-Mansour-Nisan theorem concerning the tail of the Fourier spectrum of boolean functions in AC^0. Finally, we highlight some applications of the LMN theorem in the context of sensitivity and influence of functions in AC^0.

1. Fourier Analysis of Boolean Functions

1.1. **Characters.** We introduce some stepping stones defining the tools used in the Fourier Analysis of boolean functions. Many of these tools can be defined using techniques from Representation Theory, but for the sake of briefity, we will not delve into those concepts here in detail. Instead, we will provide remarks and snippets on relevant topics as needed along with references to the standard literature at the end of the section.

We first define some general concepts for any finite abelian group G. A group homomorphism from $\chi : G \to \mathbb{C}^*$ is called a *character* of G where $\mathbb{C}^* = \mathbb{C}/\{0\}$ is the multiplicative group of the complex numbers. We call the homomorphism $\chi_0 : G \to \mathbb{C}^*,\ \chi_0 = 1$ the *trivial character* of G. By definition, for $a, b \in G$,

$$\chi(a+b) = \chi(a)\chi(b) \tag{1.1}$$

for all characters χ.

Consider the set whose elements are the characters of G and whose binary operation is pointwise multiplication of complex-valued functions on G. This set is also an *abelian group* by the following theorem:

Theorem 1.1. *If G is a finite abelian group, then the characters of G form an abelian group under pointwise multiplication.*

Proof. We first show that if χ, ϕ are characters of G, then $\chi\phi$ is also a character of G. But this immediately follows from 1.1:

$$\chi\phi(a+b) = \chi(a)\chi(b)\phi(a)\phi(b) = [\chi(a)\phi(a)][\chi(b)\phi(b)] = \chi\phi(a)\chi\phi(b)$$

Hence, $\chi\phi$ is also a character of G. Furthermore, $\chi^{-1} = \frac{1}{\chi} = \overline{\chi}$ is also a character of G since

$$\chi^{-1}(a+b) = \frac{1}{\chi(a+b)} = \frac{1}{\chi(a)\chi(b)} = \frac{1}{\chi(a)}\frac{1}{\chi(b)} = \chi^{-1}(a)\chi^{-1}(b)$$

showing that the set has inverses. □

Remark 1.2. We abuse notation a bit and just note that χ^{-1} is not the inverse of the χ as a *map*. Rather, χ^{-1} will refer to the *group inverse* of character χ from hereon.

Denote this set as $\hat{G}$. The group $\hat{G}$ is known as the *character group* of G. It also will turn out that there is a bijective map between G and $\hat{G}$ such that the map is also a *group isomorphism*. We will prove this later on.

Let us now consider the simplest finite abelian group, $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$. It follows from basic properties of cyclic groups that the only characters of $\mathbb{Z}_n$ are:

$$\chi_j(x) = e^{2\pi ijx/n} \quad j \in [n],\ x \in \mathbb{Z}_n \tag{1.2}$$

We can decompose any finite abelian group G into a direct product of finite cyclic groups $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \cdots \times \mathbb{Z}_{n_k}$. If we decompose $x = \sum_{i\in[k]} x_i$ for $x \in G$, then the characters of G are defined as

$$\chi_a(x) = \prod_{i\in[k]} e^{2\pi i a_k x_k/n_k} \tag{1.3}$$

where x_i refers to the i^{th} index of x.

We see that every element $a \in G$ has an unique associated character χ_a. Furthermore

$$\chi_{a+b}(x) = \chi_a(x)\chi_b(x) \tag{1.4}$$

To define the Fourier transform, we must consider the Hilbert space $L_2(G)$ where G endowed with the uniform probability measure i.e the discrete measure mapping each subset $H \subseteq G$ to $\frac{|H|}{|G|}$. This yields the standard inner product for maps $f, g \in L_2(G)$:

$$\langle f, g\rangle = \frac{1}{|G|}\sum_{x\in G} f(x)\overline{g(x)} = \mathbb{E}_x f(x)\overline{g(x)} \tag{1.5}$$

Note that this induces the norm $||f||_2^2 = \langle f, f\rangle = \mathbb{E}_x|f(x)|^2$ on $L_2(G)$. It is simple to check that the characters of G indeed lie in $L_2(G)$. However, we can prove something stronger: the characters of G, χ_a form an *orthonormal basis* of $L_2(G)$. First, we prove a lemma:

Lemma 1.3. *Let χ be a non-trivial character of G. Then $\sum_{x\in G}\chi(x) = 0$*

Proof. Given any non-trivial character χ, the following holds for all $y \in G$:

$$\chi(y)\sum_{x\in G}\chi(x) = \sum_{x\in G}\chi(y+x) = \sum_{x\in G}\chi(x)$$

If $\sum_{x\in G}\chi(x) \neq 0$, then this would force $\chi(y) = 1$ for all $y \in G$. However, this would contradict the non-triviality of the χ. □

Theorem 1.4. *The characters $\chi \in \hat{G}$ form an orthonormal basis for $L_2(G)$*

Proof. We first note that $\langle\chi, \chi\rangle = \mathbb{E}_x|\chi(x)|^2 = 1$ since the image of character χ lies on the complex unit circle by the discussions above. Now given two non-trivial characters χ, ϕ

$$\langle\chi, \phi\rangle = \mathbb{E}_x\chi(x)\overline{\phi(x)} = \frac{1}{|G|}\sum_{x\in G}\chi\phi^{-1}(x) = 0$$

The last equality follows from Lemma 1.3 since $\chi\phi^{-1}$ must also be a non-trivial character if χ, ϕ are non-trivial characters. The case where one of the character is trivial also follows from the lemma. Finally, observe that $L_2(G)$ is $|G|$-dimensional as a vector space by considering the dual of G. We know that there are at least $|G|$-characters, showing that the characters span $L_2(G)$. However, from the lemma, the characters must also be pairwise orthgonal to each other. This yields that the characters of G form an *orthonormal basis* of

$L_2(G)$ and that there must be exactly $|G|$ characters in $\hat{G}$. Finally, by using 1.4, it follows that the map $a \mapsto \chi_a$ must be a group isomorphism, so $G \cong \hat{G}$. □

To finish, we restrict our attention to the finite abelian group $\mathbb{Z}_2^n$ as a natural group to define boolean functions $f : \{0,1\}^n \to \{0,1\}$. By the observations above, we conclude that our characters for $\mathbb{Z}_2^n$ are defined as:

$$\chi_a(x) = (-1)^{\sum_{i\in[n]} x_i a_i} = (-1)^{\sum_{i\in[n],\ a_i=1} x_i} \tag{1.6}$$

where x_i is the i^{th} bit of $x \in \{0,1\}^n$.

Notation 1.5. Instead of considering $x \in \{0,1\}^n$ as a bit-string, we would like to use the following notation: Let $S \subseteq [n]$ be such that $S_x = \{i \mid x_i = 1\}$. As there is a bijective correspondence between all such subsets S_x and $x \in \{0,1\}^n$, we will sometimes identify bit strings with their subset counterparts for notational convenience.

1.2. **The Fourier Transform.** We have shown above that the members of the character group $\hat{G}$ form an orthonormal basis of $L_2(G)$. This bestows us the power of decomposing any $f \in L_2(G)$ into its orthogonal counterparts. The restriction to the case where $G = \mathbb{Z}_2^n$ is what motivates us as any n-ary boolean function $f : \{0,1\}^n \to \{0,1\}$ must lie in $L_2(\mathbb{Z}_2^n)$. As before, we begin by considering the general case for any finite abelian group G

Let $\hat{f} : \hat{G} \to \mathbb{C}$ be the complex-valued function defined as:

$$\hat{f}(\chi_a) = \langle f, \chi_a \rangle,\ a \in G \tag{1.7}$$

We can iterate this for all characters to get a direct sum decomposition for any $f \in L_2(G)$ which we call the *Fourier Inversion Formula*

.

$$f = \sum_{a\in G} \hat{f}(\chi_a)\chi_a \tag{1.8}$$

It can be show that the map $f \mapsto \hat{f}$ is linear by the left-linearity of the inner product. This linear map is the *Fourier Transform on* G and (1.4) shows that the decomposition is unique. Thus the Fourier Transform is a linear isomorphism as $\hat{}: L_2(G) \to L_2(\hat{G})$. The complex value $\hat{f}(\chi_a)$ is called the *Fourier coefficient* associated to χ_a.

Notation 1.6. We will sometimes denote $\hat{f}(a)$ for $\hat{f}(\chi_a)$.

From the above definition, we directly calculate that

$$\hat{f}(0) = \langle f, \chi_0 \rangle = \mathbb{E}_x f(x) \tag{1.9}$$

A simple application of the Fourier Transform yields an useful identity which will be instrumental in our formulation of the Fourier tail of a boolean function.

Theorem 1.7. *(Parseval's Identity) Let $f \in L_2(G)$. Then*

$$||f||_2^2 = \sum_{a\in G} |\hat{f}(a)|^2$$

Proof.

$$||f||_2^2 = \langle f, f \rangle = \langle \sum_{a\in G} \hat{f}(a)\chi_a, \sum_{b\in G} \hat{f}(b)\chi_b \rangle = \sum_{a,b\in G} \hat{f}(a)\overline{\hat{f}(b)}\langle \chi_a, \chi_b \rangle = \sum_{a\in G} |\hat{f}(a)|^2$$

The last equality is just the orthonormality of the characters (1.4). □

By combining Parseval's Identity with the observation that $||\hat{f}||_2^2 = \langle \hat{f}, \hat{f} \rangle = \frac{1}{|G|} \sum_{a \in G} |\hat{f}(a)|^2$, we arrive at the *Plancheral Formula*

Theorem 1.8. *(Plancheral Formula)*

$$||\hat{f}||_2 = \sqrt{G}||f||_2$$

Example 1.9. *(Fourier coefficients for Parity)* Let $G = \mathbb{Z}_2^n$ and $f = \oplus_n$, the parity function on n bits. We wish to calculate the Fourier coefficients of f. We begin by calculating $\hat{f}(0^n)$ and $\hat{f}(1^n)$

$$\hat{f}(0^n) = \frac{1}{2^n} \sum_{x \in G} f(x) = \frac{2^{n-1}}{2^n} = \frac{1}{2} \tag{1.10}$$

$$\hat{f}(1^n) = \frac{1}{2^n} \sum_{x \in G} (-1)^{|x|} f(x) = \frac{-2^{n-1}}{2^n} = -\frac{1}{2} \tag{1.11}$$

Now for $a \neq 0^n, 1^n$, there must exist two indices i, j such that $a_i = 0$ and $a_j = 1$. Define e_i, e_j to be the n-bit strings such that all indices are set to zero except for the i^{th}, j^{th} places respectively. Note that:

$$\hat{f}(a) = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{\chi_a(x)} = \frac{1}{|G|} \sum_{x \in G} f(x + e_0 + e_1)\chi_a(x + e_0 + e_1)$$

since translating by $e_0 + e_1$ rearranges the lefthand sum. This yields the equality:

$$\hat{f}(a) = \frac{1}{2}\mathbb{E}_x[f(x)\chi_a(x) + f(x + e_0 + e_1)\chi_a(x + e_0 + e_1)]$$

As flipping bits at indices i, j does not change the parity for any $x \in \{0,1\}^n$, $f(x) = f(x+e_0+e_1)$. If $x_j = 1$, then adding e_j will flip the bit to $x_j = 0$. Recalling the definition of the character $\chi_a(x) = (-1)^{\sum_{i \in [n], a_i = 1}}$ shows that a factor of -1 disappears from the product since $a_j = 1$. Similarly, if initially $x_j = 0$, then the product gains a factor of -1. This proves that $\chi_a(x + e_0 + e_1) = -\chi_a(x)$ for all $x \in \{0,1\}^n$ which in turn proves that $\hat{f}(a) = 0$ for all such $a \neq 0^n, 1^n$. By Parseval's identity:

$$|| \oplus_n ||_2 = \frac{1}{\sqrt{2}}$$

Remark 1.10. *(Generalizations of Fourier Analysis)* The above properties on characters can be shown through techniques in Representation Theory. For instance, we know representations of finite groups are group homomorphisms into the group of linear automorphisms of a suitable complex vector space $\rho : G \to GL(\mathbb{C}^n)$. The *characters* of ρ are defined as $\chi(x) = Tr(\rho(x))$ where Tr is the trace operator. It turns out that the representations of finite abelian groups are one-dimensional i.e isomorphic to $\mathbb{C}$. Thus, $\rho(x)$ will just be multiplying $\mathbb{C}$ by some scalar $\lambda_x \in \mathbb{C}^*$. In this case, we can show that indeed for any $a, b \in G$ and χ any character of G:

$$\chi(a + b) = Tr(\rho(a + b)) = Tr(\rho(a) \circ \rho(b)) = \lambda_a \lambda_b = Tr(\rho(a))Tr(\rho(b)) = \chi(a)\chi(b)$$

Note that this relation does not hold for arbitrary finite groups. For more information on the Representation Theory of Finite Groups, see **??**.

Email address: ehkim@cs.unc.edu