CS 6815: Lecture 4

Instructor: Eshan Chattopadhyay Scribe: Makis Arsenis and Ayush Sekhari

September 4, 2018

In this lecture, we will first see an algorithm to construct ϵ-biased spaces. Then we will take a detour to define characters for finite Abelian groups, and, using them define Fourier transformation for functions over $\mathbb{F}_p^n$. We will later give an introduction on how having small fourier coefficeints is related to $\epsilon-$biasedness, which will be continued over to the next lecture.

1 Construction of ε-biased spaces (continued from the last lecture)

We present an algorithm to construct n random variables in $\mathbb{F}_2$ which are ε-biased.

Procedure:
Let $r = \left\lceil \log_2 \left(\frac{n}{\varepsilon}\right) \right\rceil, q = 2^r \geq \frac{n}{\varepsilon}$.

(i) Pick random $y, z \in \mathbb{F}_q$.

(ii) For $i \in \{0, \dots, n-1\}$ set $X_i = \langle y^i, z \rangle \in \mathbb{F}_2$. [1]

Randomness used: $2 \left\lceil \log \left(\frac{n}{\varepsilon}\right) \right\rceil$.

Claim 1.1. *Consider n random variables $X = \{X_0, \dots, X_{n-1}\}$ constructed using the procedure above. Then X is an ε-biased space.*

Proof. For a random variable Z taking values in $\{0, 1\}$, let us define the function $\text{Bias}(Z)$ as the bias of the random variable Z, i.e.,

$$\text{Bias}(Z) = |\Pr[Z = 1] - \Pr[Z = 0]|$$

Additionally, for any set $S = \{s_1, \dots, s_t\} \subseteq [0, n-1], S \neq \emptyset$, define:

$$\bigoplus X_S = X_{s_1} \oplus \ldots \oplus X_{s_t}$$

Recalling that a set $X = \{X_0, \dots, X_{n-1}\}$ is said to be ϵ-biased, if for all sets $S \subseteq [n]$,

$$\text{Bias}\left(\bigoplus X_S\right) \leq \epsilon$$

We need to show that the set $X = \{X_0, \dots, X_{n-1}\}$ constructed using the procedure above forms an ϵ-biased space. Consider a set $S = \{s_1, \dots, s_t\} \subseteq [0, n-1], S \neq \emptyset$

[1]The notation $\langle a, b \rangle$ for $a, b \in \mathbb{F}_q$ means inner product with a, b viewed as vectors of the space $\mathbb{F}_2^r$, i.e. $\langle a, b \rangle = \sum_{i=1}^{r} a_i b_i \pmod 2$ where a_i, b_i are the i-th bits of a and, b respectively.

$$\bigoplus X_S = X_{s_1} \oplus \ldots \oplus X_{s_t} = \langle y^{s_1}, z\rangle + \ldots + \langle y^{s_t}, z\rangle = \langle y^{s_1} + \ldots + y^{s_t}, z\rangle^{2}$$

Let $P(y)$ be be the univariate polynomial over $\mathbb{F}_q$ defined by $P(y) = \sum_{i=1}^{t} y^{s_i}$. We can now rewrite the above as:

$$\bigoplus X_S = \langle P(y), z\rangle$$

Notice the following facts:

(i) If y is sampled from a distribution Y for which we are guaranteed that $P(y) \neq 0$ then:

$$\Pr_{y\sim Y, z\in F_2^r}[\langle P(y), z\rangle = 0] = \frac{1}{2}$$

(ii) Otherwise,

$$0 \leq \Pr_{y\sim F_q}[P(y) = 0] \leq \frac{\deg(P)}{q} \leq \frac{n-1}{q} < \varepsilon \tag{1}$$

The above follows using the *Schwartz-Zippel lemma* and the fact that P is a univariate polynomial over $\mathbb{F}_q$ of degree at most $n-1$.

Thus, we have:

$$\begin{aligned}\Pr\left[\bigoplus X_S = 0\right] &= \Pr[\langle P(y), z\rangle = 0 | P(y) \neq 0] \cdot \Pr[P(y) \neq 0] + 1 \cdot \Pr[P(y) = 0] \\ &= \frac{1}{2}(1 - \Pr[P(y) = 0]) + \Pr[P(y) = 0] \\ &= \frac{1}{2} + \frac{1}{2}\Pr[P(y) = 0]\end{aligned}$$

Using (1) with the above expression, we get:

$$\frac{1}{2} \leq \Pr\left[\bigoplus X_S = 0\right] \leq \frac{1}{2} + \frac{\varepsilon}{2}$$

and consequently,

$$\frac{1}{2} - \frac{\varepsilon}{2} \leq \Pr\left[\bigoplus X_S = 1\right] \leq \frac{1}{2}$$

□

And thus,

$$\begin{aligned}\mathrm{Bias}(\bigoplus X_S) &= \left|\Pr\left[\bigoplus X_S = 1\right] - \Pr\left[\bigoplus X_S = 0\right]\right| \\ &\leq \varepsilon\end{aligned}$$

We now take a detour and discuss Fourier Analysis on Finite Abelian groups which will be useful in constructing ϵ-biased spaces.

[2] Notice that in the last equality, the symbol $+$ on the left-hand side denotes addition over $\mathbb{F}_2$ whereas in the right-hand side denotes addition over $\mathbb{F}_q$.

2 Fourier Analysis on Finite Abelian Groups

Suggested Reading: Chapter 1 of the book "Analysis of Boolean Functions" by Ryan O' Donnel.

2.1 Characters of Finite Abelian Groups

Definition 2.1 (Group Homomorphism)**.** *A* group homomorphism $\chi : G_1 \to G_2$ *is a map between two groups* $(G_1, \cdot)$ *and* $(G_2, \circ)$ *such that the group operation is preserved, i.e.* $\forall x, y \in G_1$,

$$\chi(x \cdot y) = \chi(x) \circ \chi(y)$$

A consequence of the above definition is that: $\chi(1) = 1$ and $\chi(g^{-1}) = (\chi(g))^{-1}$ for all $g \in G_1$.

Example 2.2. *Let* $(G_1, \cdot) = (\mathbb{Z}, +), (G_2, \circ) = (\mathbb{Z}_m, +)$. *Then* $\chi(a) = (a \mod m)$ *is a group homomorphism from* $\mathbb{Z}$ *to* $\mathbb{Z}_m$.

From now on, we will be restricting ourselves to Finite Abelian Groups, and denote them by G. Aditionally, we will define S to be the set of unit norm complex numbers, i.e. $S := \{x \in \mathbb{C} : \ \|x\| = 1\}$ where $\mathbb{C}$ denotes complex numbers. We are ready to define characters of a group:

Definition 2.3. *(Character) A* character *of* G *is a homomorphism* $\chi : G \to S$.

Definition 2.4. *(Trivial Character) A character* $\chi : G \to S$ *is called "trivial" if* $\chi(g) = 1$, *for all* $g \in G$.

The following gives examples of characters for $G = (\mathbb{Z}_m, +)$.

Claim 2.5. *Let* $G = (\mathbb{Z}_m, +)$ *be a finite Abelian group. Also, let* ω *denote the* m^{th} *primitive root of unity (over* $\mathbb{C}$*), i.e.,* $\omega = e^{2\pi i/m}$ *where* $i^2 = -1$. *Then, the mapping* $\chi_j : G \mapsto S$ *defined by* $\chi_j(x) := \omega^{jx}$ *for all* $j \in [m]$, *is a group homomorphism from* G *to* S.

Proof. Let $x, y \in G$. Then:

$$\chi_j(x + y) = \omega^{j(x+y)} = \omega^{jx} \cdot \omega^{jy} = \chi_j(x) \cdot \chi_j(y)$$ [3]

Thus, X_j is a group homomorphism. □

We will now show that χ_j distinct for $j \in [m]$ and exhaustive.

Claim 2.6. $G = (\mathbb{Z}_m, +)$ *has exactly* m *characters. Additionally, the set* $\chi = \{\chi_j \mid j \in [m]\}$ *of characters as defined above has cardinality* m, *i.e.,* $|\chi| = m$, *and includes all the characters of* G.

Proof. Let us consider $\tilde{\chi}$ to be a character of G. Then the mapping $\tilde{\chi} : G \mapsto S$ is completely characterized by setting the value of $\tilde{\chi}(1)$, as:

$$\forall a \in [m], \quad \tilde{\chi}(a) = \tilde{\chi}(\underbrace{1 + 1 + \ldots + 1}_{a}) = (\tilde{\chi}(1))^a$$

Thus, the number of characters is equal to the number of ways to set $\tilde{\chi}(1)$. And, there are only m possible values to set $\chi(1)$ as $\chi(m) = (\chi(1))^m = 1$ implies $\chi(1)$ is an m^{th} root of unity.
Additionally, the set χ contains all of the characters $\tilde{\chi}$ characterized by setting $\tilde{\chi}$ to ω^j for some $j \in [m]$. All of them are distinct and $|\chi| = m$. Thus, χ is the complete set of characters of $\mathbb{Z}_m$. □

[3] Note that $(\cdot)$ in the RHS is on S.

Before proceeding, we also recall the *fundamental theorem of finite Abelian groups* which allows us to define characters for product groups,

Theorem 2.7 (Fundamendal Theorem of finite Abelian groups)**.** *A finite Abelian group is isomorphic to a direct product of cyclic groups of prime-power order, where the decomposition is unique up to the order in which the factors are written.*

The fundamental theorem allows one to look at $\mathbb{Z}_n$ as $\mathbb{Z}_{q_1} \times \mathbb{Z}_{q_1} \times \dots \mathbb{Z}_{q_r}$, where $q_1, \dots, q_r$ are powers of prime numbers and $\prod_{i=1}^{r} q_i = n$.

Claim 2.8. *Consider a finite Abelian group $G = G_1 \times G_2$. If $\chi_1 : G_1 \mapsto S$ is a character for G_1 and $\chi_2 : G_2 \mapsto S$ is a character for G_2 then $\chi : G \to \mathbb{C}$ defined as $\chi(g) = \chi_1(g_1) \cdot \chi_2(g_2)$, where $g \equiv (g_1, g_2)$, is a character for the direct product $G = G_1 \times G_2$.* [4]

We also define some more properties of characters-

Definition 2.9. *Let $f, g : G \to \mathbb{C}$ be characters of the finite Abelian group G* [5] *,*

(i) Inner Product:

$$\langle f, g \rangle = \mathop{\mathbb{E}}_{x \sim G}[f(x) \cdot \overline{g(x)}]$$

where $\overline{z}$ is defined as the complex conjugate of $z \in \mathbb{C}$.

(ii) l^p norm:

$$\|f\|_{l^p} = \left(\sum_{x \in G} |f(x)|^p \right)^{1/p}$$

where $|z|$ is defined as the absolute value of $z \in \mathbb{C}$.

(iii) L^p norm:

$$\|f\|_{L^p} = \left(\mathop{\mathbb{E}}_{x \sim G}[|f(x)|^p] \right)^{1/p}$$

Claim 2.10. *Let χ_1, χ_2 be two distinct characters of $\mathbb{Z}_m$. Then,*

(i) $\langle \chi_1, \chi_2 \rangle = 0$

(ii) $\langle \chi_1, \chi_1 \rangle = 1$

where $\langle \chi_1, \chi_2 \rangle$ is defined as in definition 2.9.

Proof. Without the loss of generality, let us assume that $\chi_1(x) = \omega^{jx}$ and $\chi_2(x) = \omega^{kx}$, for some $j, k < m$, then,

$$\langle \chi_1, \chi_2 \rangle = \mathbb{E}_{x \in \mathbb{Z}_m}[\omega^{jx}\omega^{-kx}] = \mathbb{E}_{x \in \mathbb{Z}_m}[\omega^{(j-k)x}] \tag{2}$$

(i) If $i \neq k$ then:

$$\begin{aligned} \langle \chi_1, \chi_2 \rangle = (2) &= \frac{1}{m} \sum_{x=1}^{m} \omega^{(j-k)x} \\ &= \frac{1}{m} \sum_{\alpha=1}^{m} \omega^{\alpha} \qquad \text{(since } \mathbb{Z}_m \text{ is a cyclic group)} \\ &= 0 \end{aligned}$$

[4] The operation $(\cdot)$ in the RHS is defined over S

[5] These definitions are more genereral and do not need f, g to be characters

(ii) If $i = k$ then:

$$
\begin{aligned}
\langle \chi_1, \chi_2 \rangle = (2) &= \frac{1}{m}\sum_{j=1}^{m} \omega^0 \\
&= \frac{1}{m}\sum_{j=1}^{m} 1 \\
&= 1
\end{aligned}
$$

□

Additive character of $\mathbb{F}_p^n$ (where p is a prime)
Consider the group $(\mathbb{F}_p^n, +)$ where $+$ means vector addition over $\mathbb{F}_p^n$, and let χ be a non-trivial character of $\mathbb{F}_p$.

Claim 2.11. *For $v \in \mathbb{F}_p^n$, define $\chi_v : \mathbb{F}_p^n \to S$ as $\chi_v(y) = \chi(\langle v, y\rangle)$ [6]. Then, for all $v \in \mathbb{F}_p^n$, χ_v is a character of $(\mathbb{F}_p^n, +)$.*

Proof. Let $x, y \in \mathbb{F}_p^n$:

$$\chi_v(x+y) = \chi(\langle v, x+y\rangle) = \chi(\langle v, x\rangle + \langle v, y\rangle) = \chi(\langle v, x\rangle) \cdot \chi(\langle v, y\rangle) = \chi_v(x) \cdot \chi_v(y)$$

Thus, for all $v \in \mathbb{F}_p^n$, χ_v is a character of $(\mathbb{F}_p^n, +)$. □

Claim 2.12. *Consider the set $\mathcal{X} = \{\overline{\chi_v} \mid v \in \mathbb{F}_p^n\}$ of the characters of $(\mathbb{F}_p^n, +)$ as defined above. Then $\mathcal{X}$ is a set of orthonormal functions.,*

Proof. We will show this in two parts as follows:

1. *For $v_1 \neq v_2 \in \mathbb{F}_p^n$, $\overline{\chi_{v_1}}$ and $\overline{\chi_{v_2}}$ are orthogonal, i.e., $\langle \overline{\chi_{v_1}},\ \overline{\chi_{v_2}} \rangle = 0$.*

   By definition, $\chi_v(x) = \chi(\langle x, v\rangle)$ and without loss of generality, let us assume that $\chi(z) = \omega^z$ for all $z \in \mathbb{F}_p$, where ω is a p^{th} root of unity. Thus,

$$
\begin{aligned}
\chi_{v_1}(x) &= \chi(\langle v_1, x\rangle) = \omega^{\langle v_1, x\rangle}, \text{ and,} \\
\chi_{v_2}(x) &= \chi(\langle v_2, x\rangle) = \omega^{\langle v_2, x\rangle}
\end{aligned}
$$

   Thus,

$$
\begin{aligned}
\langle \overline{\chi_{v_1}}, \overline{\chi_{v_2}} \rangle &= \mathbb{E}_{x \in \mathbb{F}_p^n}[\overline{\chi_{v_1}(x)} \cdot \overline{\overline{\chi_{v_2}(x)}}] \\
&= \mathbb{E}_{x \in \mathbb{F}_p^n}[\omega^{\langle -v_1, x\rangle} \cdot \omega^{\langle v_2, x\rangle}] \\
&= \mathbb{E}_{x \in \mathbb{F}_p^n}[\omega^{\langle v_2 - v_1, x\rangle}] \\
&= 0
\end{aligned}
$$

   where the last equality follows from the fact that the sum of all p^{th} roots of unity is 0, i.e., $\sum_{i=1}^{p} \omega^i = 0$.

[6] $\langle x, y\rangle = \sum_{i=1}^{n} x_i \cdot y_i$ for vectors $x, y \in \mathbb{F}_p^n$.

2. *For any* $v \in \mathbb{F}_p^n$, $\langle \overline{\chi_v},\ \overline{\chi_v} \rangle = 1$.

   Similar to the part-1, without loss of generality,

$$\chi_v(x) = \chi(\langle v, x \rangle) = \omega^{\langle v,x \rangle}, \text{ and,}$$

   Thus,

$$\begin{aligned}
\langle \overline{\chi_v},\ \overline{\chi_v} \rangle &= \mathbb{E}_{x \in \mathbb{F}_p^n}[\chi_v(x) \cdot \overline{\chi_v(x)}] \\
&= \mathbb{E}_{x \in \mathbb{F}_p^n}[\omega^{\langle v,x \rangle} \cdot \omega^{-\langle v,x \rangle}] \\
&= \mathbb{E}_{x \in \mathbb{F}_p^n}[\omega^{\langle v-v,x \rangle}] \\
&= \mathbb{E}_{x \in \mathbb{F}_p^n}[\omega^0] \\
&= 1
\end{aligned}$$

□

Thus, the set $\mathcal{X} = \{\overline{\chi_v} \mid v \in \mathbb{F}_p^n\}$ is orthonormal and has cardinality p^n, and correspondingly, forms an orthonormal basis to represent functions mapping $\mathbb{F}_p^n \mapsto \mathbb{F}_p$, as formalized in the following:

Claim 2.13. *Let* $\mathcal{V}$ *be the vector space of functions* $f : \mathbb{F}_p^n \to \mathbb{C}$. *Then the set* $\mathcal{X} = \{\overline{\chi_v} \mid v \in \mathbb{F}_p^n\}$ *forms an orthonormal basis for* $\mathcal{V}$.

In the next section, we will see exact decomposition of the given function in terms of its "*Fourier components*".

2.2 Fourier Analysis over $\mathbb{F}_p^n$

Theorem 2.14. *Given a function* $f : \mathbb{F}_p^n \to \mathbb{C}$. *Define* $\hat{f} : \mathbb{F}_p^n \to \mathbb{C}$ *as follows:*

$$\hat{f}(v) = \mathbb{E}_{s \sim \mathbb{F}_p^n}[f(x) \cdot \chi_v(x)] = \langle f, \overline{\chi_v} \rangle$$

Then, the function f *can be written in an alternate form using* $\hat{f}$ *as follows:*

$$f(x) = \sum_{v \in \mathbb{F}_p^n} \hat{f}(v) \cdot \overline{\chi_v(x)}$$

Proof. Using the claim 2.13, $\{\overline{\chi_v}\}_{v \in \mathbb{F}_n^p}$ is an orthonormal basis of $\mathcal{V}$. Thus, f can be expressed as:

$$f(x) = \sum_{v \in \mathbb{F}_p^n} C_v \cdot \overline{\chi_v(x)}$$

for some constants C_v, which can be calculated as follows:

$$\begin{aligned}
\langle f, \overline{\chi_v} \rangle &= \mathbb{E}_{x \sim \mathbb{F}_p^n}[f(x) \cdot \chi_v(x)] \\
&= \frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} \left(\sum_{u \in \mathbb{F}_p^n} C_u \cdot \overline{\chi_u(x)} \right) \cdot \chi_v(x) \\
&= \frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} C_v = C_v
\end{aligned}$$

where the last equality follows from the fact that $\langle \chi_u, \chi_v \rangle = 0$ for $u \neq v$ and is 1 otherwise. Thus,

$$f(x) = \sum_{v \in \mathbb{F}_p^n} \hat{f}(v) \cdot \overline{\chi_v(x)}$$

□

Note that the set $\mathcal{X}$ is fixed and known in advance. Thus, as shown above, f can be alternately represented using $\hat{f}$ or the vector $(\hat{f}(v) \mid v \in \mathbb{F}_p^n)$. This is called as the Fourier transform on the basis $\mathcal{X}$, and the constant $\hat{f}(v)$ is called as the Fourier coefficient for basis χ_v .

As we will see thoughout the course, looking at functions under the lens of "*Fourier transformation*", provides many computational benefits and simplicity. In the following theorem, we provide an identity to compute inner product of functions in terms using their "*Fourier coefficients*". The following theorem relates expectations in function space to dot product in the Fourier space.

Theorem 2.15 (Parseval's Theorem)**.** *Let function $f, g : \mathbb{F}_p^n \to \mathbb{C}$. Then:*

$$\mathbb{E}_{x \sim \mathbb{F}_p^n}[f(x) \cdot \overline{g(x)}] = \sum_{v \in \mathbb{F}_p^n} \hat{f}(v) \cdot \overline{\hat{g}(v)}$$

Proof.

$$\begin{aligned}
\mathbb{E}_{x \sim \mathbb{F}_p^n}[f(x) \cdot \overline{g(x)}] &= \langle f, g \rangle \\
&= \left\langle \sum_v \hat{f}(v) \cdot \overline{\chi_v}, \sum_w \hat{g}(w) \cdot \overline{\chi_v} \right\rangle \\
&= \sum_{v,w} \langle \hat{f}(v)\overline{\chi_v}, \hat{g}(w)\overline{\chi_w} \rangle \\
&= \sum_{v,w} \hat{f}(v) \cdot \overline{\hat{g}(w)} \langle \overline{\chi_v}, \overline{\chi_w} \rangle \\
&= \sum_v \hat{f}(v) \cdot \overline{\hat{g}(v)}
\end{aligned}$$

□

Corollary 2.16. *For a given function $f : \mathbb{F}_p^n \mapsto \mathbb{C}$,*

$$\|f\|_{L^2} = \|\hat{f}\|_{l^2}$$

3 ε-biased definition under the lens of Fourier Analysis

In this section, we will see how to construct $\varepsilon-$ biased distributions using Fourier coefficients.

Claim 3.1. *Let $D : \mathbb{F}_p^n \to \mathbb{R}$ be a distribution on $\mathbb{F}_p^n$. D is an ε-*biased distribution *on $\mathbb{F}_p^n$ if:*

$$\forall v \in \mathbb{F}_p^n, v \neq \vec{0} : |\hat{D}(v)| \leq \frac{\varepsilon}{p^n}$$

where $\hat{D}(v) = \frac{1}{p^n} \mathbb{E}_{x \in D}[\chi_v(x)]$.

continue in the next lecture...