CS 6815: Lecture 5

Instructor: Eshan Chattopadhyay Scribe: Drishti Wali

6^{th} September 2018

1 Introduction

Using the tools of Fourier Analysis which we developed last time, we will proceed to show how we can construct an ϵ-biased distribution which is almost k-wise independent but requires only $O(k + log(n))$ random bits compared to the lower bound of $k \times log(n)$ random bits for k-wise independent distributions. For this we would be requiring a result by Vazirani on comparing xor function based distributions to the uniform distribution.

2 Recap

Before constructing the ϵ-biased distributions, let us have a quick recap of the tools from Fourier Analysis we were building and would be needing in this lecture.
Group: In this lecture, $G = (\mathbb{F}_p^n, +)$ is a group over vectors of size n where each element comes from a field of size p with the addition operator as element-wise addition modulo p.
Characters: We defined non-trivial characters of the group G as

$$\chi_v(y) := \chi(\langle v, y\rangle) = \omega^{\sum_{i=1}^{n} v_i y_i}$$

for all $v \in \mathbb{F}_p^n$ and where $\omega = e^{\frac{2\pi\iota}{p}}$ is a non-primitive p^{th} root of unity.
Some general useful properties of these characters include:

Fact 2.1. *The characters are ortho-normal to one another*

$$\begin{aligned}\langle \chi_v, \chi_w\rangle &= \mathop{\mathbf{E}}_{x\sim\mathbb{F}_p^n}[\chi_v(x)\overline{\chi_w(x)}] \text{ (By the definition of inner product defined last time)}\\ &= \mathbb{1}_{v=w} \text{ (By using the fact that the sum of all powers of a non-primitive root of unity is 0)}\end{aligned}$$

Fact 2.2. *The set of characters form a basis for the set of functions $f : \mathbb{F}_p^n \to \mathbb{C}$*

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

where $\hat{f}(v) = \langle f, \chi_v\rangle = \mathop{\mathbb{E}}_{y\sim\mathbb{F}_p^n}[f(y)\chi_v(y)]$

Corollary 1. *Setting $p = 2$ then for all $v \in \mathbb{F}_2^n$;*

$$\chi_v(y) = (-1)^{\langle v,y\rangle} = (-1)^{\oplus y_T} = (-1)^{\sum_{i\in T} y_i} := \chi_T(y)$$

where $T = \{i \in [n] : v_i = 1\}$

3 ϵ - biased distributions

Let $\mathbf{D}$: $\mathbb{F}_2^n \to [0,1]$ be a distribution on $\mathbb{F}_2^n$.
By using Fact 2.2 we can write

$$\begin{aligned}
\mathbf{D}(x) &= \sum_{T\subseteq[n]} \hat{\mathbf{D}}(T)\chi_T(x) \\
&= \sum_{T\subseteq[n]} \mathop{\mathbb{E}}_{y\sim\mathbb{F}_2^n}[\mathbf{D}(y)\chi_T(y)]\chi_T(x) \\
&= \sum_{T\subseteq[n]} \frac{1}{2^n} \sum_{y\in\mathbb{F}_2^n} \mathbf{D}(y)\chi_T(y)\chi_T(x) \\
&= \sum_{T\subseteq[n]} \frac{1}{2^n} \mathop{\mathbf{E}}_{y\sim\mathbf{D}} \chi_T(y)\chi_T(x) \\
&= \sum_{T\subseteq[n]} \frac{1}{2^n} \mathop{\mathbf{E}}_{y\sim\mathbf{D}} (-1)^{\oplus y_T}\chi_T(x)
\end{aligned}$$

Definition 3.1 (ϵ-biased distribution)**.** *$\boldsymbol{D}: \mathbb{F}_2^n \to \mathbb{R}$ is an ϵ-biased distribution if $\forall\ T \subseteq [n]$, $T \neq \emptyset$*

$$|\hat{\boldsymbol{D}}(T)| \leq \frac{\epsilon}{2^n}$$

Now as

$$\hat{\mathbf{D}}(T) = \frac{1}{2^n} \mathop{\mathbb{E}}_{y\sim\mathbf{D}}[(-1)^{\oplus y_T}]$$

and

$$\hat{\mathbf{D}}(T) \leq \frac{\epsilon}{2^n} \Rightarrow |\mathop{\mathbb{E}}_{y\sim\mathbf{D}}[(-1)^{\oplus y_T}]| \leq \epsilon$$

Remark 3.2. *If $\boldsymbol{D}$ is an ϵ-biased distribution*

$$\frac{1}{2} - \epsilon \leq \mathop{Pr}_{y\sim\boldsymbol{D}}[\oplus y_T = 1] \leq \frac{1}{2} + \epsilon$$

3.1 Vazirani's XOR Lemma

Definition 3.3 (Statistical distance or Variational distance)**.** *Let $\boldsymbol{D}_1$, $\boldsymbol{D}_2$ be a distribution on Ω,*

$$|\boldsymbol{D}_1 - \boldsymbol{D}_2| = \frac{1}{2}\sum_{w\in\Omega}\left|\mathop{\mathbf{Pr}}_{y\sim\boldsymbol{D}_1}[y=w] - \mathop{\mathbf{Pr}}_{y\sim\boldsymbol{D}_2}[y=w]\right|$$

Lemma 3.4. *Let $\boldsymbol{D}$ be an ϵ-biased distribution on $\mathbb{F}_2^n$. Then,*

$$|\boldsymbol{D} - \boldsymbol{U}_n| \leq \epsilon \times 2^{n/2}$$

where $\boldsymbol{U}_n$ is the uniform distribution over n bits.

Proof: We know that

$$\hat{\mathbf{U}}(\emptyset) = \mathop{\mathbb{E}}_{x\sim\mathbb{F}_2^n}[\mathbf{U}(x)] = 2^{-n}$$

and

$$\hat{\mathbf{U}}(T) = \mathop{\mathbb{E}}_{x \sim \mathbb{F}_2^n}[\mathbf{U}(x)(-1)^{\oplus x_T}] = 0 \quad \text{for } T \subseteq [n],\, T \neq \emptyset$$

Consider $f : \mathbb{F}_2^n \to \mathbb{R}$; $f(x) = \mathbf{D}(x) - \mathbf{U}(x)$

$$\begin{aligned}
|\mathbf{D} - \mathbf{U}| &= \frac{1}{2}\|f\|_{l^1} && \text{(By construction)} \\
&\leq 2^{n/2}\|f\|_{l^2} && \text{(By Cauchy-Schwartz)} \\
&= 2^n\|f\|_{L^2} && \text{(By re-normalization)} \\
&= 2^n\|\hat{f}\|_{l^2} && \text{(By Parseval's identity)} \\
&\leq 2^n\|\hat{\mathbf{D}}\|_{l^2} && \text{(By the linearity of fourier coefficients)} \\
&\leq 2^n\sqrt{\frac{\epsilon^2}{2^n}} \leq 2^{n/2} \times \epsilon && \text{(By definition of } \epsilon\text{-biased distribution)}
\end{aligned}$$

4 δ-Almost k-wise independence

Now we will try to construct an almost k-wise independent distribution using an ϵ-biased distribution using much fewer bits.

Definition 4.1 (δ-almost k-wise distribution)**.** *A sequence of n bits $\boldsymbol{X} = (X_1, ..., X_n) \in \{0,1\}^n$ is a δ-almost k-wise distribution if $\forall T \subseteq [n]$, $|T| = k$*

$$|\boldsymbol{X}_T - \boldsymbol{U}_k| \leq \delta$$

where $\boldsymbol{X}_T = (X_{i_1}, ..., X_{i_k})$ for $T = i_1, .., i_k$

Theorem 2. *An $\delta \times 2^{k/2}$-biased distribution on $\{0,1\}^n$ $\boldsymbol{X}$ is also δ-almost k-wise independent*

Proof: Given that $\mathbf{X}$ is ϵ-biased we can use Vazirani's XOR lemma which gives us

$$|\mathbf{X}_T - \mathbf{U}_k| \leq \epsilon \times 2^{k/2}$$

Now if we pick $\epsilon \times 2^{k/2} \leq \delta \Rightarrow \epsilon \leq \delta \times 2^{-k/2}$ we would have a δ-almost k-wise independent distribution
The randomness required for an ϵ-biased distribution is $2\log(\frac{n}{\epsilon})$ bits and thus the total randomness used: $2\log n + 2\log(\frac{2^{k/2}}{\delta}) = 2\log n + k - 2\log\delta$

Remark 4.2. *We can have an δ-almost k-wise independent distribution using only $2log(n) + k - 2log(\delta)$ random bits as compared to $k/2 \times log(n+1)$ for exact k-wise independent distribution.*

The random bits required for a δ-almost k-wise independent distribution can be further reduced to $k\log\log(n)$