Lecture 22: Few Applications

Close to the Uniform Distribution I

- We shall represent random variables over the sample space $\{0,1\}^n$ as real-valued functions over $\{0,1\}^n$
- Our objective in this part of the lecture is to obtain a technique to demonstrate "close-ness" to the uniform distribution
- Recall that the uniform distribution over the sample space $\{0,1\}^n$ is the constant function $\mathbb{U}$ such that $\mathbb{U}(x) = \frac{1}{N}$, for all $x \in \{0,1\}^n$. We had seen that the Fourier coefficients of this function is the delta function

$$\widehat{\mathbb{U}}(x) = \begin{cases} \frac{1}{N}, & \text{if } x = 0 \\ 0, & \text{otherwise.} \end{cases}$$

- Suppose $\mathbb{A}$ is a probability distribution over the same sample space $\{0,1\}^n$

Close to the Uniform Distribution II

- We are interested in measuring how close the distribution $\mathbb{A}$ is to the uniform distribution $\mathbb{U}$

Definition (Statistical Distance)

The *statistical distance* between two probability distributions $\mathbb{A}$ and $\mathbb{B}$ over the same discrete sample space Ω is represented by

$$\mathrm{SD}\left(\mathbb{A}, \mathbb{B}\right) := \frac{1}{2} \sum_{x \in \Omega} \left| \mathbb{A}(x) - \mathbb{B}(x) \right|$$

Intuitively, if $\mathrm{SD}\left(\mathbb{A}, \mathbb{B}\right)$ is small then the two distributions are close to each other.

Close to the Uniform Distribution III

- We can upper-bound the $\mathrm{SD}(\mathbb{A}, \mathbb{B})$ using their Fourier Coefficients

Lemma

$$\mathrm{SD}(\mathbb{A}, \mathbb{B}) \leqslant \frac{N}{2} \sqrt{\sum_{S \neq 0} \left(\widehat{\mathbb{A}}(S) - \widehat{\mathbb{B}}(S) \right)^2}$$

Proof Outline.

$$\begin{aligned}
2\mathrm{SD}(\mathbb{A},\mathbb{B}) &= \sum_{x\in\{0,1\}^n} \left|\mathbb{A}(x)-\mathbb{B}(x)\right|, && \text{By Definition}\\
&\leqslant \sqrt{N}\sqrt{\sum_{x\in\{0,1\}^n} \left(\mathbb{A}(x)-\mathbb{B}(x)\right)^2}, && \text{Cauchy-Schwarz}\\
&= N\sqrt{\frac{1}{N}\sum_{x\in\{0,1\}^n} (\mathbb{A}-\mathbb{B})(x)^2} && \\
&= N\sqrt{\sum_{S\in\{0,1\}^n} (\widehat{\mathbb{A}-\mathbb{B}})(S)^2}, && \text{Parseval's Identity}\\
&= N\sqrt{\sum_{S\neq 0} (\widehat{\mathbb{A}-\mathbb{B}})(S)^2}, && \widehat{\mathbb{A}}(0)=\widehat{\mathbb{B}}(0)=\frac{1}{N}\\
&= N\sqrt{\sum_{S\neq 0} \left(\widehat{\mathbb{A}(S)-\mathbb{B}}(S)\right)^2}, && \text{Linearity of Fourier}
\end{aligned}$$

- Intuitively, if two functions have Fourier coefficients that are close, then the functions are close as well
- In particular, we get the following corollary

Corollary

$$\mathrm{SD}\left(\mathbb{A}, \mathbb{U}\right) \leqslant \frac{N}{2}\sqrt{\sum_{S \neq 0} \widehat{\mathbb{A}}(S)^2}$$

- Small-bias distributions find a significant applications in derandomization techniques for algorithms

Definition (Small-Bias Distribution)

A distribution $\mathbb{A}$ has ε-bias if $\widehat{\mathbb{A}}(S) \leqslant \varepsilon/N$, for all $S \in \{0,1\}^n$ such that $S \neq 0$

- Think: State and prove that a random function $f\colon \{0,1\}^n \to \{+1,-1\}$ has a small bias with very high probability

- The XOR lemma states that if two distributions $\mathbb{A}$ and $\mathbb{B}$ are XORed, then the resultant distribution $\mathbb{A} \oplus \mathbb{B}$ is "very-small-bias" if both $\mathbb{A}$ and $\mathbb{B}$ were "small-biased"
- Note that $\mathbb{A} \oplus \mathbb{B}$ is the function $N(\mathbb{A} * \mathbb{B})$. So, we have $(\widehat{\mathbb{A} \oplus \mathbb{B}})(S) = N\widehat{\mathbb{A}}(S)\widehat{\mathbb{B}}(S)$.
- Suppose $\mathbb{A}$ is ε-biased and $\mathbb{B}$ is δ-biased. Then, the distribution $(\mathbb{A} \oplus \mathbb{B})$ is $(\varepsilon\delta)$-biased, because $N(\widehat{\mathbb{A} \oplus \mathbb{B}})(S) = \left(N\widehat{\mathbb{A}}(S)\right) \cdot \left(N\widehat{\mathbb{B}}(S)\right)$
- Let $k\mathbb{A}$ represent the distribution

$$\overbrace{\mathbb{A} \oplus \cdots \oplus \mathbb{A}}^{k\text{-times}}$$

- Note that if $\mathbb{A}$ is ε-biased then, inductively, we can show that the distribution $k\mathbb{A}$ is ε^k-biased

XOR Lemma II

- So, we can conclude that

$$\begin{aligned}
\mathrm{SD}\left(\mathbb{U}, k\mathbb{A}\right) &\leqslant \frac{N}{2}\sqrt{\sum_{S\neq 0} \widehat{(k\mathbb{A})}(S)^2} \\
&= \frac{1}{2}\sqrt{\sum_{S\neq 0} \left(N\widehat{(k\mathbb{A})}(S)\right)^2} \\
&\leqslant \frac{1}{2}\sqrt{\sum_{S\neq 0} \left(\varepsilon^k\right)^2} \\
&< \frac{\varepsilon^k\sqrt{N}}{2}
\end{aligned}$$

XOR Lemma III

- Using this above observation, we can conclude the following lemma

Lemma (XOR-Lemma)

If $\mathbb{A}$ is an ε-biased distribution and $k \geqslant \frac{(n/2)+\lg(1/2\delta)}{\lg(1/\varepsilon)}$, then we have $\mathrm{SD}\left(\mathbb{U}, k\mathbb{A}\right) \leqslant \delta$.

Extraction from any Min-Entropy Source via Masking with a Small-bias Distribution

Lemma

Let $\mathbb{S}$ be an ε-bias distribution and $\mathbb{M}$ be a min-entropy source with $\mathrm{H}_\infty(\mathbb{M}) \geqslant k$ over the sample space $\{0,1\}^n$. Then, we have $\mathrm{SD}\left(\mathbb{U}, \mathbb{S} \oplus \mathbb{M}\right) \leqslant \frac{\varepsilon}{2}\sqrt{\frac{N}{K}}$.

Proof Outline.

$$\begin{aligned}
\mathrm{SD}\left(\mathbb{U}, \mathbb{S} \oplus \mathbb{M}\right) &\leqslant \frac{N}{2}\sqrt{\sum_{S \neq 0} \widehat{(\mathbb{S} \oplus \mathbb{M})}(S)^2} = \frac{N}{2}\sqrt{\sum_{S \neq 0} N^2 \widehat{\mathbb{S}}(S)^2 \widehat{\mathbb{M}}(S)^2} \\
&\leqslant \frac{N}{2}\sqrt{\sum_{S \neq 0} \varepsilon^2 \widehat{\mathbb{M}}(S)^2} = \frac{N\varepsilon}{2}\sqrt{\sum_{S \neq 0} \widehat{\mathbb{M}}(S)^2} \\
&< \frac{N\varepsilon}{2}\sqrt{\frac{1}{NK}} = \frac{\varepsilon}{2}\sqrt{\frac{N}{K}}
\end{aligned}$$