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 \(U\) such that \(U(x) = \frac{1}{N}\), for all \(x \in \{0, 1\}^n\). We had seen that the Fourier coefficients of this function is the delta function

\[
\hat{U}(x) = \begin{cases} 
\frac{1}{N}, & \text{if } x = 0 \\
0, & \text{otherwise.}
\end{cases}
\]

- Suppose \(\mathbb{A}\) is a probability distribution over the same sample space \(\{0, 1\}^n\).
We are interested in measuring how close the distribution \( A \) is to the uniform distribution \( U \).

**Definition (Statistical Distance)**

The *statistical distance* between two probability distributions \( A \) and \( B \) over the same discrete sample space \( \Omega \) is represented by

\[
\text{SD}(A, B) := \frac{1}{2} \sum_{x \in \Omega} |A(x) - B(x)|
\]

Intuitively, if \( \text{SD}(A, B) \) is small then the two distributions are close to each other.
We can upper-bound the $\text{SD}(\mathbb{A}, \mathbb{B})$ using their Fourier Coefficients

**Lemma**

$$\text{SD}(\mathbb{A}, \mathbb{B}) \leq \frac{N}{2} \sqrt{\sum_{S \neq 0} \left( \hat{A}(S) - \hat{B}(S) \right)^2}$$
Proof Outline.

\[ 2SD(A, B) = \sum_{x \in \{0,1\}^n} |A(x) - B(x)|, \]  

By Definition

\[ \leq \sqrt{N} \sqrt{\sum_{x \in \{0,1\}^n} (A(x) - B(x))^2}, \]  

Cauchy-Schwarz

\[ = N \sqrt{\frac{1}{N} \sum_{x \in \{0,1\}^n} (A - B)(x)^2} \]  

Parseval’s Identity

\[ = N \sqrt{\sum_{S \in \{0,1\}^n} (\hat{A} - \hat{B})(S)^2}, \]  

\[ \hat{A}(0) = \hat{B}(0) = \frac{1}{N} \]

Linearity of Fourier

\[ = N \sqrt{\sum_{S \neq 0} (A(S) - B(S))^2}, \]  

\[ \]
Intuitively, if two functions have Fourier coefficients that are close, then the functions are close as well.

In particular, we get the following corollary:

\[ \text{SD}(\mathbb{A}, \mathbb{U}) \leq \frac{N}{2} \sqrt{\sum_{S \neq 0} \hat{A}(S)^2} \]
Small-bias distributions find a significant applications in derandomization techniques for algorithms

### Definition (Small-Bias Distribution)
A distribution $\mathbb{A}$ has $\varepsilon$-bias if $\hat{\mathbb{A}}(S) \leq \varepsilon/N$, for all $S \in \{0, 1\}^n$ such that $S \neq 0$

- Think: State and prove that a random function $f : \{0, 1\}^n \rightarrow \{+1, -1\}$ has a small bias with very high probability
The XOR lemma states that if two distributions $A$ and $B$ are XORed, then the resultant distribution $A \oplus B$ is “very-small-bias” if both $A$ and $B$ were “small-biased”.

Note that $A \oplus B$ is the function $N(A \ast B)$. So, we have $$(A \oplus B)(S) = N\hat{A}(S)\hat{B}(S).$$

Suppose $A$ is $\varepsilon$-biased and $B$ is $\delta$-biased. Then, the distribution $(A \oplus B)$ is $(\varepsilon\delta)$-biased, because $$N(A \oplus B)(S) = \left(N\hat{A}(S)\right) \cdot \left(N\hat{B}(S)\right).$$

Let $kA$ represent the distribution

$$\underbrace{A \oplus \cdots \oplus A}_{k\text{-times}}$$

Note that if $A$ is $\varepsilon$-biased then, inductively, we can show that the distribution $kA$ is $\varepsilon^k$-biased.
So, we can conclude that

\[
\text{SD}(\mathbb{U}, k\mathbb{A}) \leq \frac{N}{2} \sqrt{\sum_{S \neq 0} \left(\hat{k}\mathbb{A})(S)\right)^2}
\]

\[
= \frac{1}{2} \sqrt{\sum_{S \neq 0} \left(N(\hat{k}\mathbb{A})(S)\right)^2}
\]

\[
\leq \frac{1}{2} \sqrt{\sum_{S \neq 0} \left(\varepsilon^k\right)^2}
\]

\[
< \varepsilon^k \sqrt{N}
\]

\[
< \frac{\varepsilon^k \sqrt{N}}{2}
\]
Using this above observation, we can conclude the following lemma

Lemma (XOR-Lemma)

If $A$ is an $\varepsilon$-biased distribution and $k \geq \frac{(n/2)+\lg(1/2\delta)}{\lg(1/\varepsilon)}$, then we have $SD(U, kA) \leq \delta$. 
Lemma

Let $S$ be an $\varepsilon$-bias distribution and $M$ be a min-entropy source with $H_\infty(M) \geq k$ over the sample space $\{0, 1\}^n$. Then, we have

$$SD(U, S \oplus M) \leq \frac{\varepsilon}{2} \sqrt{\frac{N}{K}}.$$ 

Proof Outline.

$$SD(U, S \oplus M) \leq \frac{N}{2} \sqrt{\sum_{S \neq 0} (S \oplus \hat{M})(S)^2} = \frac{N}{2} \sqrt{\sum_{S \neq 0} N^2 \tilde{S}(S)^2 \hat{M}(S)^2}$$

$$\leq \frac{N}{2} \sqrt{\sum_{S \neq 0} \varepsilon^2 \hat{M}(S)^2} = \frac{N\varepsilon}{2} \sqrt{\sum_{S \neq 0} \hat{M}(S)^2}$$

$$\leq \frac{N\varepsilon}{2} \sqrt{\frac{1}{NK}} = \frac{\varepsilon}{2} \sqrt{\frac{N}{K}}.$$