Lecture 21: Min-Entropy Extraction via Small-bias Masking
Recall

- For a probability distribution $X$ over $\{0, 1\}^n$, we defined the bias of $X$ with respect to a linear test $S \in \{0, 1\}^n$ as follows

$$\operatorname{Bias}_X(S) = \mathbb{P}[S \cdot X = 0] - \mathbb{P}[S \cdot X = 1]$$

- The probability that two independent samples from $X$ and $Y$ turn out to be identical is defined as

$$\operatorname{Col}(X, Y) = \frac{1}{N} \sum_{S \in \{0, 1\}^n} \operatorname{Bias}_X(S) \operatorname{Bias}_Y(S)$$

- $X \oplus Y$ is a probability distribution over $\{0, 1\}^n$ such that $\mathbb{P}[X \oplus Y = z]$ is the probability that two samples according to $X$ and $Y$ add up to $z$

$$\operatorname{Bias}_{X \oplus Y} = \operatorname{Bias}_X \cdot \operatorname{Bias}_Y$$
The statistical distance between two probability distributions $X$ and $Y$ over the sample space $\{0, 1\}^n$ is

$$2SD(X, Y) = \sum_{x \in \{0, 1\}^n} |P[X = x] - P[Y = x]|$$

We showed that

$$2SD(X, Y) \leq \ell_2(Bias_X - Bias_Y)$$
Let $U$ represent the uniform distribution over the sample space $\{0, 1\}^n$

Note that, we have

$$\text{Bias}_U(S) = \begin{cases} 
1, & \text{if } S = 0 \\
0, & \text{if } S \neq 0 
\end{cases}$$

In fact, $\text{Bias}_X(0) = 1$ for all probability distributions $X$
Example 2

Let $U\langle v \rangle$, for $v \in \{0, 1\}^n$, represent the uniform distribution over the vector space spanned by $\{v\}$, i.e., the set $\{0, v\}$

Let $U\langle w \rangle$, for $w \in \{0, 1\}^n$, represent the uniform distribution over the vector space spanned by $\{w\}$, i.e., the set $\{0, w\}$

Prove: $U\langle v \rangle \oplus U\langle w \rangle = U\langle v, w \rangle$.
Here, $U\langle v, w \rangle$ represents the uniform distribution over the set spanned by $\{v, w\}$. If $v = w$, then $\langle v, w \rangle = \{0, v\}$; otherwise $\langle v, w \rangle = \{0, v, w, v + w\}$.

In general, for linearly independent vectors $v_1, v_2, \ldots, v_k \in \{0, 1\}^n$, we have

$$U\langle v_1, \ldots, v_k \rangle = U\langle v_1 \rangle \oplus \cdots \oplus U\langle v_k \rangle$$

So, we conclude that

$$\text{Bias}_{U\langle v_1, \ldots, v_k \rangle} = \text{Bias}_{U\langle v_1 \rangle} \cdots \text{Bias}_{U\langle v_k \rangle}$$
Example 2

- Prove: There exists a subset $T \subseteq \{0, 1\}^n$ of size $2^{n-1}$ such that $\text{Bias}_{\mathbb{U}_v}(S) = 1$ if $S \in T$; otherwise $\text{Bias}_{\mathbb{U}_v}(S) = 0$.
- Think: Which $S$ have $\text{Bias}_{\mathbb{U}_v} \oplus \mathbb{U}_w(S) = 0$?
Recall: Min-Entropy Sources

- Let $\mathbf{X}$ be a distribution over the sample space $\{0, 1\}^n$.
- We say that the distribution $\mathbf{X}$ has min-entropy at least $k$ if it satisfies the following condition. For any $x \in \{0, 1\}^n$, we have

$$\mathbb{P}[\mathbf{X} = x] \leq \frac{1}{2^k} =: \frac{1}{K}$$

This constraint is succinctly represented as $H_\infty(\mathbf{X}) \geq k$.

- Intuition: The probability of any element according to the distribution $\mathbf{X}$ is small. So, the outcome of $\mathbf{X}$ is “highly unpredictable.” Furthermore, $\mathbf{X}$ associates non-zero probability to at least $K$ elements in $\{0, 1\}^n$. 

We had seen that the collision probability of a high min-entropy distribution is low.

\[
\text{Col}(X, X) = \sum_{x \in \{0,1\}^n} \mathbb{P}[X = x]^2 \leq \sum_{x \in \{0,1\}^n} \mathbb{P}[X = x] \frac{1}{K} = \frac{1}{K}
\]

This implies that

\[
\sum_{S \in \{0,1\}^n} \text{Bias}_X(S)^2 \leq \frac{N}{K}
\]

Or, equivalently, we write

\[
\sum_{S \in \{0,1\}^n : S \neq 0} \text{Bias}_X(S)^2 \leq \frac{N}{K} - 1
\]
Recall: Min-Entropy Sources

Succinctly, we write

\[ \ell^*_2(\text{Bias}_x) \leq \sqrt{\frac{N}{K}} - 1 \]

Here \( \ell^*_2(f) \) is identical to the definition of \( \ell_2(f) \) except that it excludes \( f(0)^2 \) in the sum.
Let $\mathcal{Y}$ be a distribution over $\{0, 1\}^n$

We say that $\mathcal{Y}$ is a small-bias distribution if

$$\text{Bias}_{\mathcal{Y}}(S) \leq \varepsilon$$

for all $0 \neq S \in \{0, 1\}^n$

Prove: A random probability distribution is a small-bias distribution with very high probability
Let $X$ be a min-entropy source with $H_\infty(X) \geq k$.

Let $Y$ be a small bias distribution such that $\text{Bias}_Y(S) \leq \varepsilon$, for all $0 \neq S \in \{0, 1\}^n$.

We want to say that $X \oplus Y$ is very close to the uniform distribution $U$ over the sample space $\{0, 1\}^n$.

\[
\text{2SD (} X \oplus Y, U \text{)} \leq \ell_2(\text{Bias}_{X \oplus Y} - \text{Bias}_U)
= \ell^*(\text{Bias}_{X \oplus Y} - \text{Bias}_U)
= \ell^*_2(\text{Bias}_{X \oplus Y})
= \ell^*_2(\text{Bias}_X \text{Bias}_Y)
\leq \varepsilon \ell^*_2(\text{Bias}_X)
\leq \varepsilon \sqrt{\frac{N}{K} - 1}
\]