Lecture 2: August 28

Lecturer: Eshan Chattopadhyay *Scribe: Jiazhen Tan*

2.1 Pseudorandom Generators

To define a pseudorandom generator (PRG), we first fix a class of *distinguishers* or a class of tests, which we typically denote as $\mathcal{F}$. Informally, the PRG takes a short uniform string of length r bits to n bits, where $r < n$. For making the definition useful, we would require the PRG function should be "efficiently computable", where we make the notion of efficiency clear in later lectures.

Definition 2.1.1. *A family of tests* $\mathcal{F} = \bigcup_{n>0} \mathcal{F}_n$*, where* $\mathcal{F}_n$ *contains Boolean functions* $f : \{0,1\}^n \to \{0,1\}$ *that maps an* n*-bit string to a single bit.*

Notation: Let U_m be a uniform distribution on $\{0,1\}^n$.

We are now ready to formally define a PRG.

- The function $r : \mathbb{N} \to \mathbb{N}$ maps n to the seed length needed to generate a string of length n.
- The function $\epsilon : \mathbb{N} \to [0,1)$ is the error function.
- $\mathcal{G}_n : \{0,1\}^{r(n)} \to \{0,1\}^n$ is a function that maps $r(n)$ bit strings to n bit strings.
- $\mathcal{G} = (\mathcal{G}_n)_{n>0}$ is a collection of $\mathcal{G}_n$.

Definition 2.1.2. *Given an error function* ϵ*, we define* $\mathcal{G}$ *to be a PRG for* $\mathcal{F}$ *if* $\forall n \in \mathbb{N}, \forall f \in \mathcal{F}_n$,

$$\left|\mathbf{E}_{x\leftarrow U_n}[f(x)] - \mathbf{E}_{y\leftarrow U_{r(n)}}[f(G(y))]\right| < \epsilon(n)$$

An important application of PRGs is to derandomization, i.e, reducing the amount of randomness used in algorithms. In particular, a good enough PRG could altogether eliminate the need for using random bits.

Example 2.1.3. *Consider the class of polynomial time algorithms* $A : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *that takes an input string of length* n *and* n *bits of randomness to outputs a single bit.*

We assume that for all $z \in \{0,1\}^n$*, when the answer is supposed to be* `yes`*,*

$$\Pr_{x\leftarrow U_n}[A(z,x) = 1] \geq \frac{2}{3}$$

and when the answer is supposed to be `no`*,*

$$\Pr_{x\leftarrow U_n}[A(z,x) = 0] \geq \frac{2}{3}$$

Take $\mathcal{G} : \{0,1\}^{r(n)} \to \{0,1\}^n$ *such that*

$$\left|\mathbf{E}_{x\leftarrow U_n}[A(z,x)] - \mathbf{E}_{y\leftarrow U_{r(n)}}[A(z,G(y))]\right| < \frac{1}{10} = \epsilon(n)$$

Thus, if we iterate through all possible seeds y *and take the majority vote, this algorithm will deterministically give us the right answer. When* $r(n) = \log n$ *(resp.* $O(\log n)$*), The number of possible seeds is* $2^{r(n)} = n$ *(resp. polynomial in* n*). This gives an efficient way to eliminate randomness assuming that* $\mathcal{G}$ *is computable in polytime.*

2.1.1 Pairwise Independent Generator

A simple but particularly useful pseudorandom distribution is a pairwise independent string defined as follows.

Definition 2.1.4. *Let Σ be an alphabet. (For now, $\Sigma = \{0,1\}$ or the field $\mathbb{F}_q$)*
$X = (X_1, X_2, \cdots X_n) \in \Sigma^n$ where each X_i is a random variable on Σ, and for all pairs $i, j \in [n]$, such that $i \neq j$, X_i and X_j are independent. Then we call X a Pairwise Independent Distribution on Σ^n.

Example 2.1.5. *A simple example: Let $\Sigma = \{0,1\}$. $X = (X_1, X_2, X_3)$ is a distribution on $\{0,1\}^3$ where $X_3 = X_1 \oplus X_2$, the XOR of X_1 and X_2 is a pairwise independent distribution on 3 bits. In each column, each of the four combinations of the ftwo bits occurs with equal probability.*

$$X = \begin{array}{ccc} (X_1 & X_2 & X_3) \\ 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

We generalize the above example to give an efficient construction of a pairwise independent generator with seed length $O(\log n)$.

Construction 2.1.6 (Pairwise independent generator)**.** *Let $r = \lceil \log(n+1) \rceil$ and let $Y_1, Y_2, \ldots, Y_r$ be r uniform independent bits. For all nonempty subset S of $[n]$, we define*

$$X_S = \bigoplus_{i \in S} Y_i$$

Claim 2.1.7. *The random variable $X = (X_S)_{S \subseteq [n], S \neq \emptyset}$ is pairwise independent.*

Proof of Claim. Consider two nonempty subsets $A, B \subseteq [n]$.

- If A and B are disjoint,

$$\Pr[X_A = 1 | X_B = 1] = \Pr[X_A = 1] = \Pr[X_A = 1 | X_B = 0]$$

  The calculations for other cases are similar.

- If one is a subset of the other, with loss of generality $A \subseteq B$, then X_B, $X_{B \backslash A}$ are both uniform bits and $X_B = 1 | X_A = 1$ is equivalent to $X_{B \backslash A} = 0$

$$\Pr[X_B = 1 | X_A = 1] = \Pr[X_{B \backslash A} = 0] = \frac{1}{2} = \Pr[X_B = 1]$$

- If neither above is true about A and B, then taking set intersection and set difference won't give us nonempty sets.

$$X_A = X_{A \cap B} \oplus X_{A \backslash B}, \quad X_B = X_{A \cap B} \oplus X_{B \backslash A}$$

  where $A \backslash B$, $B \backslash A$, $A \cap B$ are disjoint. the first case says $X_{A \backslash B}, X_{B \backslash A}, X_{A \cap B}$ are independent.

$$\Pr[X_A = 1 | X_B = 1] = \Pr[X_{A \backslash B} \neq X_{A \cap B} | X_{B \backslash A} \neq X_{A \cap B} = \Pr[X_{A \backslash B} \neq X_{A \cap B}] = \frac{1}{2}$$

  So X_A and X_B are independent.

□

The following is an alternate construction of a pairwise independent distribution.

Construction 2.1.8. *Let $\mathbb{F}_q$ be a finite field of q elements. We sample a, b randomly from $\mathbb{F}_q$, and let $X_i = ai + b$ for all $i \in \mathbb{F}_q$.*

Claim 2.1.9. *Let $X = (X_1, X_2, \dots, X_q)$ where all X_i are defined as in 2.1.8. The X_i's are pairwise independent.*

Proof. For all pairs $i \neq j$, we can write $\begin{pmatrix} x_i \\ x_j \end{pmatrix} = M \begin{pmatrix} a \\ b \end{pmatrix}$ where $M = \begin{pmatrix} 1 & i \\ 1 & j \end{pmatrix}$ is invertible. Then, for arbitrary $m, n \in \mathbb{F}_q$,

$$\Pr\left[x_i = m, x_j = n\right] = \Pr\left[\begin{pmatrix} a \\ b \end{pmatrix} = M^{-1}\begin{pmatrix} m \\ n \end{pmatrix}\right] = \frac{1}{|\mathbb{F}_q|^2} = \Pr\left[x_i = m\right]\Pr\left[x_j = n\right]$$

□

2.1.2 Application: Error reduction in algorithms

Lemma 2.1.10. (Chebyshev's Inequality) *Let X be a random variable with mean μ, and variance σ. Then,*

$$\Pr\left[|X - \mu| > \epsilon\right] \leq \frac{\sigma}{\epsilon^2}.$$

Proof. If we apply Markov's Inequality to $(X - \mu)^2$, we get

$$\begin{aligned} \Pr\left[|X - \mu| > \epsilon\right] &= \Pr\left[(X - \mu)^2 > \epsilon^2\right] \\ &\leq \frac{\mathbf{E}[(X - \mu)^2]}{\epsilon^2} = \frac{\sigma}{\epsilon^2}. \end{aligned}$$

□

Claim 2.1.11. *Let X be the average of t pairwise independent on the interval $[0, 1]$. Then,*

$$\Pr\left[|X - \mu| > \epsilon\right] \leq \frac{1}{t\epsilon^2}$$

Proof. Given Chebyshev's Inequality, we only need to show $\mathrm{Var}[X] \leq 1/t$. Pairwise independence says that for $i \neq j$,

$$\mathbf{E}\left[(X_i - \mu)(X_j - \mu)\right] = \mathbf{E}[X_i - \mu]\mathbf{E}[X_j - \mu] = 0$$

$$\begin{aligned} \mathrm{Var}[X] = \mathbf{E}\left[(X - \mu)^2\right] &= \mathbf{E}\left[\left(\frac{\sum_{i=1}^t X_i}{t} - \mu\right)^2\right] \\ &= \frac{1}{t^2}\mathbf{E}\left[\left(\sum_{i=1}^t (X_i - \mu)\right)^2\right] \\ &= \frac{1}{t^2}\mathbf{E}\left[\sum_{i,j \in [t]} (X_i - \mu)(X_j - \mu)\right] = \frac{1}{t^2}\sum_{i,j \in [t]} \mathbf{E}\left[(X_i - \mu)(X_j - \mu)\right] \\ &= \frac{1}{t^2}\sum_{i \in [t]} \mathbf{E}\left[(X_i - \mu)^2\right] \qquad \text{(pairwise independence)} \\ &\leq \frac{1}{t^2}t = \frac{1}{t} \end{aligned}$$

□

The application to error reduction is now straightforward from the above lemma in the following way: Say A is a randomized algorithm that takes a random symbol from Σ. We repeat the randomized algorithm t times, using a pairwise independent distribution on Σ^t. The error analysis now follows by letting the random variable X_i indicate the probability of success of the i'th iteration of the algorithm.