COM S 6830 – Cryptography August 27, 2009

Handout 1: Notation and Probability

Instructor: Rafael Pass *Teaching Assistant: Dustin Tseng*

Notation

Algorithm

Let $\mathcal{A}$ denote an algorithm. We write $\mathcal{A}(\cdot)$ to denote an algorithm with one input and $\mathcal{A}(\cdot\,,\cdot)$ for two inputs. In general, the output of an algorithm can be considered as a probability distribution. So $\mathcal{A}(x)$ denotes a probability distribution. The algorithm is deterministic if the distribution is concentrated on a single element.

Experiment

To sample an element x from a distribution $\mathcal{S}$ we denote the experiment by $x \leftarrow \mathcal{S}$. If F is a finite set, then $x \leftarrow F$ is the experiment of sampling uniformly from the set F. To denote the ordered sequence in which the experiments happen we use semicolon.

$$(x \leftarrow \mathcal{S}; (y, z) \leftarrow \mathcal{A}(x))$$

Using this notation we can describe probability of events. If $p(\cdot\,,\cdot)$ denotes a predicate, then

$$\Pr[x \leftarrow \mathcal{S}; (y, z) \leftarrow \mathcal{A}(x) : p(y, z)]$$

is the probability that the predicate $p(y, z)$ is true after the ordered sequence of events $(x \leftarrow S; (y, z) \leftarrow A(x))$. The notation $\{x \leftarrow S; (y, z) \leftarrow A(x) : (y, z)\}$ denotes the probability distribution on $\{(y, z)\}$ generated by the ordered sequence of experiments $(x \leftarrow S; (y, z) \leftarrow A(x))$.

Probability

Basic Facts

- Events A and B are said to be *independent* if

$$\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$$

- Events $A_1, A_2, \ldots, A_n$ are said to be *pairwise independent* if for every i and every $j \neq i$, A_i and A_j are independent.
- *Union Bound:* Let $A_1, A_2, \ldots, A_n$ be events. Then,

$$\Pr[A_1 \cup A_2 \cup \ldots \cup A_n] \leq \Pr[A_1] + \Pr[A_2] + \ldots \Pr[A_n]$$

- Let X be a random variable with range Ω. The *expectation* of X is a number defined as follows.

$$\mathbb{E}[X] = \sum_{x \in \Omega} x \Pr[X = x]$$

  The *variance* is given by,

$$\mathrm{Var}[X] = \mathbb{E}[X^2] - (\mathbb{E}[X])^2$$

- Let $X_1, X_2, \ldots, X_n$ be random variables. Then,

$$\mathbb{E}[X_1 + X_2 + \cdots + X_n] = \mathbb{E}[X_1] + \mathbb{E}[X_2] + \cdots + \mathbb{E}[X_n]$$

- If X and Y are *independent random variables*, then

$$\begin{aligned} \mathbb{E}[XY] &= \mathbb{E}[X] \cdot \mathbb{E}[Y] \\ \mathrm{Var}[X + Y] &= \mathrm{Var}[X] + \mathrm{Var}[Y] \end{aligned}$$

Markov's Inequality

If X is a positive random variable with expectation $E(X)$ and $a > 0$, then

$$\Pr[X \geq a] \leq \frac{\mathbb{E}(X)}{a}$$

Chebyshev's Inequality

Let X be a random variable with expectation $E(X)$ and variance σ^2, then for any $k > 0$,

$$\Pr[|X - \mathbb{E}(X)| \geq k] \leq \frac{\sigma^2}{k^2}$$

Chernoff's inequality

Let $X_1, \ldots, X_n$ denote independent random variables with $|X_i| \leq 1$, and let $S = X_1 + \cdots + X_n$. Then

$$\Pr\left[\frac{1}{n}|S - \mathbb{E}[S]| \geq \varepsilon\right] \leq 2e^{-\frac{1}{2}\varepsilon^2 n} \in 2^{-O(\varepsilon^2 n)}$$