CS 120/CSCI E-177: Introduction to Cryptography

Salil Vadhan and Alon Rosen Sept. 21, 2006

Lecture Notes 2:

Review of Probability

Recommended Reading.

- Cormen, Leiserson, Rivest, Stein. *Introduction to Algorithms* (2nd ed), Appendix C & Ch. 5.
- Goldreich, §1.2.

1 Review of Probability

1.1 Probability spaces

A *probability space* is a finite or countable set S together with a function $\Pr : S \to [0,1]$ such that $\sum_{x \in S} \Pr[x] = 1$. In this course, the probability space will not always be specified explicitly. Consider the following example:

- Alice flips 100 fair coins $A \in \{0,1\}^{100}$.
- Bob flips 100 fair coins $B \in \{0,1\}^{100}$.
- Carol chooses with probability 3/4 Alice's coin tosses ($C = A$), with probability 1/4 Bob's coin tosses ($C = B$).
- Eve gets $E = A \oplus B$ (bitwise XOR).

Here, the underlying probability space is $S = \{0,1\}^{100} \times \{0,1\}^{100} \times \{a, b\}$. For any triplet (x, y, z),

$$\Pr[(x, y, z)] =$$

The source of the randomness is all the coin tosses of the involved parties or the random choices made.

An *event* is a subset of the probability space. The probability of an event T is defined to be $\Pr[T] \stackrel{\text{def}}{=} \sum_{x \in T} \Pr[x]$, but often can be computed more directly.

Example:

1.2 Random variables

Random variables are functions, not necessarily real-valued, on the probability space. In our example, we can consider the following random variables:

- A, Alice's coin tosses (which is just the first coordinate for an element of the probability space)
- Z_A, the number of zeroes obtained by Alice

- $Z_A + Z_B$, the number of zeroes obtained by Alice and Bob together

The random variables X and Y are said to be *independent* if :

$$\forall x, y,\ \Pr[X = x \ \&\ Y = y] = \Pr[X = x] \cdot \Pr[Y = y].$$

Examples:

Random variables $X_1, \ldots, X_k$ are *independent* if

$$\forall x_1, \ldots, x_k,\ \Pr[X_1 = x_1 \ \& X_2 = x_2 \ \& \cdots \&\ X_k = x_k] = \Pr[X_1 = x_1] \cdot \Pr[X_2 = x_2] \cdots \Pr[X_k = x_k].$$

Not the same as pairwise independence!
Example:

1.3 Expectation of a random variable

The *expectation* of a real-valued random variable X is defined as: $\mathrm{E}[X] = \sum_x \Pr[X = x] \cdot x$. We have the property of linearity:

$$\mathrm{E}[X + Y] = \mathrm{E}[X] + \mathrm{E}[Y]$$

$$\mathrm{E}[cX] = c \cdot \mathrm{E}[X] \text{ for any constant c}$$

Note that $\mathrm{E}[XY] = \mathrm{E}[X] \cdot \mathrm{E}[Y]$ if X and Y are independent, *but not in general.*
Examples:

- $\mathrm{E}[Z_A]$
- $\mathrm{E}[Z_A^2]$

1.4 Markov's inequality

If X is a non-negative real-valued random variable, we have:

$$\Pr[X \geq t] \leq \frac{\mathrm{E}[X]}{t}$$

If X has a small expectation, we have a bound on how often the random variable can get large.
Example:

1.5 Chernoff Bound

This is a form of the Law of Large Numbers, which says that the average of random variables over many independent trials will be close to the expectation (with high probability).

Let $X_1, \ldots, X_n$ be independent $[0,1]$-valued random variables, with $\Pr[X_i = 1] = \mu$ for all i. The *Chernoff Bound* states that

$$\Pr\left[\frac{1}{n}\sum_{i=1}^{n} X_i > \mu + \varepsilon\right] \leq e^{-2\varepsilon^2 n}$$

and

$$\Pr\left[\frac{1}{n}\sum_{i=1}^{n} X_i < \mu - \varepsilon\right] \leq e^{-2\varepsilon^2 n}.$$

Example:

1.6 Conditioning

Let E and F be events. We define the probability of E occurring given that F occurs as:

$$\Pr[E|F] = \frac{\Pr[E \cap F]}{\Pr[F]}$$

Bayes' Law states that:

$$\Pr[E|F] = \frac{\Pr[F|E] \cdot \Pr[E]}{\Pr[F]}$$

Example: