Foundations of Computer Security September 4, 2024
Massachusetts Institute of Technology 6.1600 Fall 2024
Srini Devadas, Yael Kalai Handout 2

Useful Facts and Definitions

1 The union bound

Let $B_1, \ldots, B_n$ be events in a common finite discrete sample space. Then the probability that *any one* of the bad events occurs is at most the sum of the probabilities of *each* bad event occurring. That is:

$$\Pr[B_1 \cup \cdots \cup B_n] \leq \Pr[B_1] + \cdots + \Pr[B_n].$$

The beautiful thing about the union bound is that it is extremely general—it applies whether the events are independent or not.

In cryptography, we use the union bound all of the time. One common application is to define "bad" events $B_1, \ldots, B_n$ and then to use the union bound to bound the probability that any of them occurs.

2 Linearity of expectation

For a discrete real-valued random variable X taking possible values $x_1, \ldots, x_n$, the expectation of X is defined as

$$\mathbb{E}\left[X\right] = \sum_{i=1}^{n} \Pr\left[X = x_i\right] \cdot x_i$$

The expectation is in some sense the "average" value of a random variable.

One extremely useful property of the expectation is that it is *linear*. That is, given random variables $X_1, ..., X_n$ and $X = \sum_{i=1}^{n} X_i$, we have

$$\mathbb{E}[X] = \mathbb{E}\left[\sum_{i=1}^{n} X_i\right] = \sum_{i=1}^{n} \mathbb{E}\left[X_i\right]$$

In words, the expected value of the sum of random variables is equal to the sum of the expected values. This is true whether or not the variables are independent.

3 A useful life fact

The following inequality is very handy when dealing with probabilities:

$$1 + x \leq e^x \qquad \text{for all } x \in \mathbb{R}.$$

When x is very close to 1, $1 + x \approx e^x$.
For example, say that you flip n coins that come up heads with probability ϵ, and you want to compute the probability that *at least one* comes up heads. This probability is one minus the probability that all n coins come up tails:

$$1 - (1 - \epsilon)^n \approx 1 - \exp(\epsilon n).$$

So if $\epsilon \gg 1/n$, you have a good chance of seeing a heads and when $\epsilon \ll 1/n$, you have a bad chance of seeing a heads.

4 Concentration inequalities

Concentration inequalities let us bound the probability that a random variable is much larger or smaller than its expectation. Many computer scientists live happy and successful lives knowing only the following two concentration inequalities. (Okay, you don't actually need to know any concentration inequalities to have a happy and successful life, but they can help!)

Markov's inequality. Let Y be a discrete random variable taking non-negative real values. Then for any $a > 0$,

$$\Pr[Y \geq a] \leq \frac{\mathbb{E}[Y]}{a}$$

A very convenient nice feature of this inequality is that it only depends on the expectation of the random variable.

Chernoff bounds. When you are dealing with independent random variables (e.g., many tosses of a fair coin, outputs of a random oracle on distinct inputs), we can get much stronger concentration bounds. In particular, the probability that the sum of independent 0/1 random variables is t times larger than its expectation is *exponentially small* in t. To be concrete, if you flip 10000 fair coins, it is extremely unlikely that you will see only 3 heads. Chernoff bounds capture this intuition formally.
Suppose $X_1, \ldots, X_n$ are *independent* random variables taking values in $\{0, 1\}$. Let X denote their sum and let $\mu = \mathbb{E}[X]$ denote the sum's expected value. Then for any $\beta > 0$,

- $\Pr[X > (1 + \beta)\mu] < e^{-\beta^2\mu/3}$, for $0 < \beta < 1$
- $\Pr[X > (1 + \beta)\mu] < e^{-\beta\mu/3}$, for $\beta > 1$
- $\Pr[X < (1 - \beta)\mu] < e^{-\beta^2\mu/2}$, for $0 < \beta < 1$

5 Binomial coefficient

The number of way to group n items into k groups is denoted $\binom{n}{k}$ and is pronounced "n choose k." These are called *binomial coefficients* because the coefficient of the monomial x^k in the expansion of $(1+x)^n$ is exactly $\binom{n}{k}$.
We will probably not need the following inequality for this course, but it may come in handy later in life:

$$\left(\frac{n}{k}\right)^k \le \binom{n}{k} \le \left(\frac{ne}{k}\right)^k,$$

where $e \approx 2.71\ldots$ is Euler's constant.