Notation

Algorithm

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

Experiment

To sample an element $x$ from a distribution $S$ we denote the experiment by $x \leftarrow S$. 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.

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

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

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

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 $\{y, z\}$ 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

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

1-1
• 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 $\Omega$. The expectation of $X$ is a number defined as follows.
  \[
  E[X] = \sum_{x \in \Omega} x Pr[X = x]
  \]
  The variance is given by,
  \[
  Var[X] = E[X^2] - (E[X])^2
  \]

• Let $X_1, X_2, \ldots, X_n$ be random variables. Then,
  \[
  E[X_1 + X_2 + \cdots + X_n] = E[X_1] + E[X_2] + \cdots + E[X_n]
  \]

• If $X$ and $Y$ are independent random variables, then
  \[
  E[XY] = E[X] \cdot E[Y]
  \]
  \[
  Var[X + Y] = Var[X] + Var[Y]
  \]

Markov’s Inequality

If $X$ is a positive random variable with expectation $E(X)$ and $a > 0$, then
\[
Pr[X \geq a] \leq \frac{E(X)}{a}
\]

Chebyshev’s Inequality

Let $X$ be a random variable with expectation $E(X)$ and variance $\sigma^2$, then for any $k > 0$,
\[
Pr[|X - E(X)| \geq k] \leq \frac{\sigma^2}{k^2}
\]

Chernoff’s inequality

Let $X_1, X_2, \ldots, X_n$ denote independent random variables, such that for all $i$, $E(X_i) = \mu$ and $|X_i| \leq 1$.
\[
Pr \left[ \left| \frac{\sum X_i}{n} - \mu \right| \geq \epsilon \right] \leq 2^{-\epsilon^2 n}
\]