

---

Thomas H. Cormen  
Charles E. Leiserson  
Ronald L. Rivest  
Clifford Stein

---

**Introduction to Algorithms**  
*Second Edition*

The MIT Press  
Cambridge, Massachusetts London, England

McGraw-Hill Book Company  
Boston Burr Ridge, IL Dubuque, IA Madison, WI  
St. Louis Montréal Toronto

**C.1-15** ★

Show that for any integer  $n \geq 0$ ,

$$\sum_{k=0}^n \binom{n}{k} k = n2^{n-1}. \quad (\text{C.11})$$

## Probability

Probability is an essential tool for the design and analysis of probabilistic and randomized algorithms. This section reviews basic probability theory.

We define probability in terms of a *sample space*  $S$ , which is a set whose elements are called *elementary events*. Each elementary event can be viewed as a possible outcome of an experiment. For the experiment of flipping two distinguishable coins, we can view the sample space as consisting of the set of all possible 2-strings over  $\{H, T\}$ :

$$S = \{HH, HT, TH, TT\}.$$

An *event* is a subset<sup>1</sup> of the sample space  $S$ . For example, in the experiment of flipping two coins, the event of obtaining one head and one tail is  $\{HT, TH\}$ . The event  $S$  is called the *certain event*, and the event  $\emptyset$  is called the *null event*. We say that two events  $A$  and  $B$  are *mutually exclusive* if  $A \cap B = \emptyset$ . We sometimes treat an elementary event  $s \in S$  as the event  $\{s\}$ . By definition, all elementary events are mutually exclusive.

### Axioms of probability

A *probability distribution*  $\Pr\{\}$  on a sample space  $S$  is a mapping from events of  $S$  to real numbers such that the following *probability axioms* are satisfied:

1.  $\Pr\{A\} \geq 0$  for any event  $A$ .
2.  $\Pr\{S\} = 1$ .

<sup>1</sup>For a general probability distribution, there may be some subsets of the sample space  $S$  that are not considered to be events. This situation usually arises when the sample space is uncountably infinite. The main requirement is that the set of events of a sample space be closed under the operations of taking the complement of an event, forming the union of a finite or countable number of events, and taking the intersection of a finite or countable number of events. Most of the probability distributions we shall see are over finite or countable sample spaces, and we shall generally consider all subsets of a sample space to be events. A notable exception is the continuous uniform probability distribution, which will be presented shortly.

3.  $\Pr\{A \cup B\} = \Pr\{A\} + \Pr\{B\}$  for any two mutually exclusive events  $A$  and  $B$ . More generally, for any (finite or countably infinite) sequence of events  $A_1, A_2, \dots$  that are pairwise mutually exclusive,

$$\Pr\left\{\bigcup_i A_i\right\} = \sum_i \Pr\{A_i\}.$$

We call  $\Pr\{A\}$  the **probability** of the event  $A$ . We note here that axiom 2 is a normalization requirement: there is really nothing fundamental about choosing 1 as the probability of the certain event, except that it is natural and convenient.

Several results follow immediately from these axioms and basic set theory (see Section B.1). The null event  $\emptyset$  has probability  $\Pr\{\emptyset\} = 0$ . If  $A \subseteq B$ , then  $\Pr\{A\} \leq \Pr\{B\}$ . Using  $\bar{A}$  to denote the event  $S - A$  (the **complement** of  $A$ ), we have  $\Pr\{\bar{A}\} = 1 - \Pr\{A\}$ . For any two events  $A$  and  $B$ ,

$$\Pr\{A \cup B\} = \Pr\{A\} + \Pr\{B\} - \Pr\{A \cap B\} \tag{C.12}$$

$$\leq \Pr\{A\} + \Pr\{B\}. \tag{C.13}$$

In our coin-flipping example, suppose that each of the four elementary events has probability  $1/4$ . Then the probability of getting at least one head is

$$\begin{aligned} \Pr\{\text{HH, HT, TH}\} &= \Pr\{\text{HH}\} + \Pr\{\text{HT}\} + \Pr\{\text{TH}\} \\ &= 3/4. \end{aligned}$$

Alternatively, since the probability of getting strictly less than one head is  $\Pr\{\text{TT}\} = 1/4$ , the probability of getting at least one head is  $1 - 1/4 = 3/4$ .

### Discrete probability distributions

A probability distribution is **discrete** if it is defined over a finite or countably infinite sample space. Let  $S$  be the sample space. Then for any event  $A$ ,

$$\Pr\{A\} = \sum_{s \in A} \Pr\{s\},$$

since elementary events, specifically those in  $A$ , are mutually exclusive. If  $S$  is finite and every elementary event  $s \in S$  has probability

$$\Pr\{s\} = 1/|S|,$$

then we have the **uniform probability distribution** on  $S$ . In such a case the experiment is often described as "picking an element of  $S$  at random."

As an example, consider the process of flipping a **fair coin**, one for which the probability of obtaining a head is the same as the probability of obtaining a tail, that

defined on the sample space  $S = \{H, T\}^n$ , a set of size  $2^n$ . Each elementary event in  $S$  can be represented as a string of length  $n$  over  $\{H, T\}$ , and each occurs with probability  $1/2^n$ . The event

$A = \{\text{exactly } k \text{ heads and exactly } n - k \text{ tails occur}\}$

is a subset of  $S$  of size  $|A| = \binom{n}{k}$ , since there are  $\binom{n}{k}$  strings of length  $n$  over  $\{H, T\}$  that contain exactly  $k$  H's. The probability of event  $A$  is thus  $\Pr\{A\} = \binom{n}{k}/2^n$ .

### Continuous uniform probability distribution

The continuous uniform probability distribution is an example of a probability distribution in which not all subsets of the sample space are considered to be events. The continuous uniform probability distribution is defined over a closed interval  $[a, b]$  of the reals, where  $a < b$ . Intuitively, we want each point in the interval  $[a, b]$  to be "equally likely." There is an uncountable number of points, however, so if we give all points the same finite, positive probability, we cannot simultaneously satisfy axioms 2 and 3. For this reason, we would like to associate a probability only with *some* of the subsets of  $S$  in such a way that the axioms are satisfied for these events.

For any closed interval  $[c, d]$ , where  $a \leq c \leq d \leq b$ , the **continuous uniform probability distribution** defines the probability of the event  $[c, d]$  to be

$$\Pr\{[c, d]\} = \frac{d - c}{b - a}.$$

Note that for any point  $x = [x, x]$ , the probability of  $x$  is 0. If we remove the endpoints of an interval  $[c, d]$ , we obtain the open interval  $(c, d)$ . Since  $[c, d] = [c, c] \cup (c, d) \cup [d, d]$ , axiom 3 gives us  $\Pr\{[c, d]\} = \Pr\{(c, d)\}$ . Generally, the set of events for the continuous uniform probability distribution is any subset of the sample space  $[a, b]$  that can be obtained by a finite or countable union of open and closed intervals.

### Conditional probability and independence

Sometimes we have some prior partial knowledge about the outcome of an experiment. For example, suppose that a friend has flipped two fair coins and has told you that at least one of the coins showed a head. What is the probability that both coins are heads? The information given eliminates the possibility of two tails. The three remaining elementary events are equally likely, so we infer that each occurs with probability  $1/3$ . Since only one of these elementary events shows two heads, the answer to our question is  $1/3$ .

Conditional probability formalizes the notion of having prior partial knowledge of the outcome of an experiment. The **conditional probability** of an event  $A$  given that another event  $B$  occurs is defined to be

$$\Pr\{A \mid B\} = \frac{\Pr\{A \cap B\}}{\Pr\{B\}} \quad (\text{C.14})$$

whenever  $\Pr\{B\} \neq 0$ . (We read “ $\Pr\{A \mid B\}$ ” as “the probability of  $A$  given  $B$ .”) Intuitively, since we are given that event  $B$  occurs, the event that  $A$  also occurs is  $A \cap B$ . That is,  $A \cap B$  is the set of outcomes in which both  $A$  and  $B$  occur. Since the outcome is one of the elementary events in  $B$ , we normalize the probabilities of all the elementary events in  $B$  by dividing them by  $\Pr\{B\}$ , so that they sum to 1. The conditional probability of  $A$  given  $B$  is, therefore, the ratio of the probability of event  $A \cap B$  to the probability of event  $B$ . In the example above,  $A$  is the event that both coins are heads, and  $B$  is the event that at least one coin is a head. Thus,  $\Pr\{A \mid B\} = (1/4)/(3/4) = 1/3$ .

Two events are **independent** if

$$\Pr\{A \cap B\} = \Pr\{A\} \Pr\{B\} , \quad (\text{C.15})$$

which is equivalent, if  $\Pr\{B\} \neq 0$ , to the condition

$$\Pr\{A \mid B\} = \Pr\{A\} .$$

For example, suppose that two fair coins are flipped and that the outcomes are independent. Then the probability of two heads is  $(1/2)(1/2) = 1/4$ . Now suppose that one event is that the first coin comes up heads and the other event is that the coins come up differently. Each of these events occurs with probability  $1/2$ , and the probability that both events occur is  $1/4$ ; thus, according to the definition of independence, the events are independent—even though one might think that both events depend on the first coin. Finally, suppose that the coins are welded together so that they both fall heads or both fall tails and that the two possibilities are equally likely. Then the probability that each coin comes up heads is  $1/2$ , but the probability that they both come up heads is  $1/2 \neq (1/2)(1/2)$ . Consequently, the event that one comes up heads and the event that the other comes up heads are not independent.

A collection  $A_1, A_2, \dots, A_n$  of events is said to be **pairwise independent** if

$$\Pr\{A_i \cap A_j\} = \Pr\{A_i\} \Pr\{A_j\}$$

for all  $1 \leq i < j \leq n$ . We say that the events of the collection are (**mutually independent**) if every  $k$ -subset  $A_{i_1}, A_{i_2}, \dots, A_{i_k}$  of the collection, where  $2 \leq k \leq n$  and  $1 \leq i_1 < i_2 < \dots < i_k \leq n$ , satisfies

$$\Pr\{A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}\} = \Pr\{A_{i_1}\} \Pr\{A_{i_2}\} \dots \Pr\{A_{i_k}\} .$$

For example, suppose we flip two fair coins. Let  $A_1$  be the event that the first coin is heads, let  $A_2$  be the event that the second coin is heads, and let  $A_3$  be the event that the two coins are different. We have

$$\begin{aligned}\Pr\{A_1\} &= 1/2 . \\ \Pr\{A_2\} &= 1/2 . \\ \Pr\{A_3\} &= 1/2 . \\ \Pr\{A_1 \cap A_2\} &= 1/4 . \\ \Pr\{A_1 \cap A_3\} &= 1/4 . \\ \Pr\{A_2 \cap A_3\} &= 1/4 . \\ \Pr\{A_1 \cap A_2 \cap A_3\} &= 0 .\end{aligned}$$

Since for  $1 \leq i < j \leq 3$ , we have  $\Pr\{A_i \cap A_j\} = \Pr\{A_i\} \Pr\{A_j\} = 1/4$ , the events  $A_1$ ,  $A_2$ , and  $A_3$  are pairwise independent. The events are not mutually independent, however, because  $\Pr\{A_1 \cap A_2 \cap A_3\} = 0$  and  $\Pr\{A_1\} \Pr\{A_2\} \Pr\{A_3\} = 1/8 \neq 0$ .

### Bayes's theorem

From the definition of conditional probability (C.14) and the commutative law  $A \cap B = B \cap A$ , it follows that for two events  $A$  and  $B$ , each with nonzero probability,

$$\begin{aligned}\Pr\{A \cap B\} &= \Pr\{B\} \Pr\{A | B\} \\ &= \Pr\{A\} \Pr\{B | A\} .\end{aligned}\tag{C.16}$$

Solving for  $\Pr\{A | B\}$ , we obtain

$$\Pr\{A | B\} = \frac{\Pr\{A\} \Pr\{B | A\}}{\Pr\{B\}} ,\tag{C.17}$$

which is known as **Bayes's theorem**. The denominator  $\Pr\{B\}$  is a normalizing constant that we can reexpress as follows. Since  $B = (B \cap A) \cup (B \cap \bar{A})$  and  $B \cap A$  and  $B \cap \bar{A}$  are mutually exclusive events,

$$\begin{aligned}\Pr\{B\} &= \Pr\{B \cap A\} + \Pr\{B \cap \bar{A}\} \\ &= \Pr\{A\} \Pr\{B | A\} + \Pr\{\bar{A}\} \Pr\{B | \bar{A}\} .\end{aligned}$$

Substituting into equation (C.17), we obtain an equivalent form of Bayes's theorem:

$$\Pr\{A | B\} = \frac{\Pr\{A\} \Pr\{B | A\}}{\Pr\{A\} \Pr\{B | A\} + \Pr\{\bar{A}\} \Pr\{B | \bar{A}\}} .$$

Bayes's theorem can simplify the computing of conditional probabilities. For example, suppose that we have a fair coin and a biased coin that always comes up heads. We run an experiment consisting of three independent events: one of the two coins is chosen at random, the coin is flipped once, and then it is flipped again. Suppose that the chosen coin comes up heads both times. What is the probability that it is biased?

We solve this problem using Bayes's theorem. Let  $A$  be the event that the biased coin is chosen, and let  $B$  be the event that the coin comes up heads both times. We wish to determine  $\Pr\{A | B\}$ . We have  $\Pr\{A\} = 1/2$ ,  $\Pr\{B | A\} = 1$ ,  $\Pr\{\bar{A}\} = 1/2$ , and  $\Pr\{B | \bar{A}\} = 1/4$ ; hence,

$$\begin{aligned}\Pr\{A | B\} &= \frac{(1/2) \cdot 1}{(1/2) \cdot 1 + (1/2) \cdot (1/4)} \\ &= 4/5.\end{aligned}$$

### Exercises

#### C.2-1

Prove **Boole's inequality**: For any finite or countably infinite sequence of events  $A_1, A_2, \dots$ ,

$$\Pr\{A_1 \cup A_2 \cup \dots\} \leq \Pr\{A_1\} + \Pr\{A_2\} + \dots \quad (\text{C.18})$$

#### C.2-2

Professor Rosencrantz flips a fair coin once. Professor Guildenstern flips a fair coin twice. What is the probability that Professor Rosencrantz obtains more heads than Professor Guildenstern?

#### C.2-3

A deck of 10 cards, each bearing a distinct number from 1 to 10, is shuffled to mix the cards thoroughly. Three cards are removed one at a time from the deck. What is the probability that the three cards are selected in sorted (increasing) order?

#### C.2-4 \*

Describe a procedure that takes as input two integers  $a$  and  $b$  such that  $0 < a < b$  and, using fair coin flips, produces as output heads with probability  $a/b$  and tails with probability  $(b - a)/b$ . Give a bound on the expected number of coin flips, which should be  $O(1)$ . (*Hint*: Represent  $a/b$  in binary.)

#### C.2-5

Prove that

$$\Pr\{A | B\} + \Pr\{\bar{A} | B\} = 1.$$

**C.2-6**

Prove that for any collection of events  $A_1, A_2, \dots, A_n$ ,

$$\Pr\{A_1 \cap A_2 \cap \dots \cap A_n\} = \Pr\{A_1\} \cdot \Pr\{A_2 \mid A_1\} \cdot \Pr\{A_3 \mid A_1 \cap A_2\} \cdots \Pr\{A_n \mid A_1 \cap A_2 \cap \dots \cap A_{n-1}\}.$$

**C.2-7** ★

Show how to construct a set of  $n$  events that are pairwise independent but such that no subset of  $k > 2$  of them is mutually independent.

**C.2-8** ★

Two events  $A$  and  $B$  are *conditionally independent*, given  $C$ , if

$$\Pr\{A \cap B \mid C\} = \Pr\{A \mid C\} \cdot \Pr\{B \mid C\}.$$

Give a simple but nontrivial example of two events that are not independent but are conditionally independent given a third event.

**C.2-9** ★

You are a contestant in a game show in which a prize is hidden behind one of three curtains. You will win the prize if you select the correct curtain. After you have picked one curtain but before the curtain is lifted, the emcee lifts one of the other curtains, knowing that it will reveal an empty stage, and asks if you would like to switch from your current selection to the remaining curtain. How would your chances change if you switch?

**C.2-10** ★

A prison warden has randomly picked one prisoner among three to go free. The other two will be executed. The guard knows which one will go free but is forbidden to give any prisoner information regarding his status. Let us call the prisoners  $X, Y$ , and  $Z$ . Prisoner  $X$  asks the guard privately which of  $Y$  or  $Z$  will be executed, arguing that since he already knows that at least one of them must die, the guard won't be revealing any information about his own status. The guard tells  $X$  that  $Y$  is to be executed. Prisoner  $X$  feels happier now, since he figures that either he or prisoner  $Z$  will go free, which means that his probability of going free is now  $1/2$ . Is he right, or are his chances still  $1/3$ ? Explain.

---

### C.3 Discrete random variables

A (*discrete*) *random variable*  $X$  is a function from a finite or countably infinite sample space  $S$  to the real numbers. It associates a real number with each possible



outcome of an experiment, which allows us to work with the probability distribution induced on the resulting set of numbers. Random variables can also be defined for uncountably infinite sample spaces, but they raise technical issues that are unnecessary to address for our purposes. Henceforth, we shall assume that random variables are discrete.

For a random variable  $X$  and a real number  $x$ , we define the event  $X = x$  to be  $\{s \in S : X(s) = x\}$ ; thus,

$$\Pr\{X = x\} = \sum_{s \in S: X(s)=x} \Pr\{s\}.$$

The function

$$f(x) = \Pr\{X = x\}$$

is the **probability density function** of the random variable  $X$ . From the probability axioms,  $\Pr\{X = x\} \geq 0$  and  $\sum_x \Pr\{X = x\} = 1$ .

As an example, consider the experiment of rolling a pair of ordinary, 6-sided dice. There are 36 possible elementary events in the sample space. We assume that the probability distribution is uniform, so that each elementary event  $s \in S$  is equally likely:  $\Pr\{s\} = 1/36$ . Define the random variable  $X$  to be the *maximum* of the two values showing on the dice. We have  $\Pr\{X = 3\} = 5/36$ , since  $X$  assigns a value of 3 to 5 of the 36 possible elementary events, namely, (1, 3), (2, 3), (3, 3), (3, 2), and (3, 1).

It is common for several random variables to be defined on the same sample space. If  $X$  and  $Y$  are random variables, the function

$$f(x, y) = \Pr\{X = x \text{ and } Y = y\}$$

is the **joint probability density function** of  $X$  and  $Y$ . For a fixed value  $y$ ,

$$\Pr\{Y = y\} = \sum_x \Pr\{X = x \text{ and } Y = y\},$$

and similarly, for a fixed value  $x$ ,

$$\Pr\{X = x\} = \sum_y \Pr\{X = x \text{ and } Y = y\}.$$

Using the definition (C.14) of conditional probability, we have

$$\Pr\{X = x \mid Y = y\} = \frac{\Pr\{X = x \text{ and } Y = y\}}{\Pr\{Y = y\}}.$$

We define two random variables  $X$  and  $Y$  to be **independent** if for all  $x$  and  $y$ , the events  $X = x$  and  $Y = y$  are independent or, equivalently, if for all  $x$  and  $y$ , we have  $\Pr\{X = x \text{ and } Y = y\} = \Pr\{X = x\} \Pr\{Y = y\}$ .

Given a set of random variables defined over the same sample space, one can define new random variables as sums, products, or other functions of the original variables.

### Expected value of a random variable

The simplest and most useful summary of the distribution of a random variable is the “average” of the values it takes on. The *expected value* (or, synonymously, *expectation* or *mean*) of a discrete random variable  $X$  is

$$E[X] = \sum_x x \Pr\{X = x\} , \quad (\text{C.19})$$

which is well defined if the sum is finite or converges absolutely. Sometimes the expectation of  $X$  is denoted by  $\mu_X$  or, when the random variable is apparent from context, simply by  $\mu$ .

Consider a game in which you flip two fair coins. You earn \$3 for each head but lose \$2 for each tail. The expected value of the random variable  $X$  representing your earnings is

$$\begin{aligned} E[X] &= 6 \cdot \Pr\{2 \text{ H's}\} + 1 \cdot \Pr\{1 \text{ H, 1 T}\} - 4 \cdot \Pr\{2 \text{ T's}\} \\ &= 6(1/4) + 1(1/2) - 4(1/4) \\ &= 1 . \end{aligned}$$

The expectation of the sum of two random variables is the sum of their expectations, that is,

$$E[X + Y] = E[X] + E[Y] , \quad (\text{C.20})$$

whenever  $E[X]$  and  $E[Y]$  are defined. We call this property *linearity of expectation*, and it holds even if  $X$  and  $Y$  are not independent. It also extends to finite and absolutely convergent summations of expectations. Linearity of expectation is the key property that enables us to perform probabilistic analyses by using indicator random variables (see Section 5.2).

If  $X$  is any random variable, any function  $g(x)$  defines a new random variable  $g(X)$ . If the expectation of  $g(X)$  is defined, then

$$E[g(X)] = \sum_x g(x) \Pr\{X = x\} .$$

Letting  $g(x) = ax$ , we have for any constant  $a$ ,

$$E[aX] = aE[X] . \quad (\text{C.21})$$

Consequently, expectations are linear: for any two random variables  $X$  and  $Y$  and any constant  $a$ ,

$$E[aX + Y] = aE[X] + E[Y] . \quad (\text{C.22})$$

When two random variables  $X$  and  $Y$  are independent and each has a defined expectation,

$$E[XY] = \sum_x \sum_y xy \Pr\{X = x \text{ and } Y = y\}$$

$$\begin{aligned}
 &= \sum_x \sum_y xy \Pr\{X = x\} \Pr\{Y = y\} \\
 &= \left( \sum_x x \Pr\{X = x\} \right) \left( \sum_y y \Pr\{Y = y\} \right) \\
 &= E[X]E[Y] .
 \end{aligned}$$

In general, when  $n$  random variables  $X_1, X_2, \dots, X_n$  are mutually independent,

$$E[X_1 X_2 \cdots X_n] = E[X_1] E[X_2] \cdots E[X_n] . \tag{C.23}$$

When a random variable  $X$  takes on values from the set of natural numbers  $\mathbf{N} = \{0, 1, 2, \dots\}$ , there is a nice formula for its expectation:

$$\begin{aligned}
 E[X] &= \sum_{i=0}^{\infty} i \Pr\{X = i\} \\
 &= \sum_{i=0}^{\infty} i (\Pr\{X \geq i\} - \Pr\{X \geq i + 1\}) \\
 &= \sum_{i=1}^{\infty} \Pr\{X \geq i\} ,
 \end{aligned} \tag{C.24}$$

since each term  $\Pr\{X \geq i\}$  is added in  $i$  times and subtracted out  $i - 1$  times (except  $\Pr\{X \geq 0\}$ , which is added in 0 times and not subtracted out at all).

When we apply a convex function  $f(x)$  to a random variable  $X$ , *Jensen's inequality* gives us

$$E[f(X)] \geq f(E[X]) , \tag{C.25}$$

provided that the expectations exist and are finite. (A function  $f(x)$  is *convex* if for all  $x$  and  $y$  and for all  $0 \leq \lambda \leq 1$ , we have  $f(\lambda x + (1 - \lambda)y) \leq \lambda f(x) + (1 - \lambda)f(y)$ .)

### Variance and standard deviation

The expected value of a random variable does not tell us how “spread out” the variable’s values are. For example, if we have random variables  $X$  and  $Y$  for which  $\Pr\{X = 1/4\} = \Pr\{X = 3/4\} = 1/2$  and  $\Pr\{Y = 0\} = \Pr\{Y = 1\} = 1/2$ , then both  $E[X]$  and  $E[Y]$  are  $1/2$ , yet the actual values taken on by  $Y$  are farther from the mean than the actual values taken on by  $X$ .

The notion of variance mathematically expresses how far from the mean a random variable’s values are likely to be. The *variance* of a random variable  $X$  with mean  $E[X]$  is

$$\begin{aligned}
\text{Var}[X] &= E[(X - E[X])^2] \\
&= E[X^2 - 2XE[X] + E^2[X]] \\
&= E[X^2] - 2E[XE[X]] + E^2[X] \\
&= E[X^2] - 2E^2[X] + E^2[X] \\
&= E[X^2] - E^2[X] .
\end{aligned}
\tag{C.26}$$

The justification for the equalities  $E[E^2[X]] = E^2[X]$  and  $E[XE[X]] = E^2[X]$  is that  $E[X]$  is not a random variable but simply a real number, which means that equation (C.21) applies (with  $a = E[X]$ ). Equation (C.26) can be rewritten to obtain an expression for the expectation of the square of a random variable:

$$E[X^2] = \text{Var}[X] + E^2[X] . \tag{C.27}$$

The variance of a random variable  $X$  and the variance of  $aX$  are related (see Exercise C.3-10):

$$\text{Var}[aX] = a^2 \text{Var}[X] .$$

When  $X$  and  $Y$  are independent random variables,

$$\text{Var}[X + Y] = \text{Var}[X] + \text{Var}[Y] .$$

In general, if  $n$  random variables  $X_1, X_2, \dots, X_n$  are pairwise independent, then

$$\text{Var}\left[\sum_{i=1}^n X_i\right] = \sum_{i=1}^n \text{Var}[X_i] . \tag{C.28}$$

The **standard deviation** of a random variable  $X$  is the positive square root of the variance of  $X$ . The standard deviation of a random variable  $X$  is sometimes denoted  $\sigma_X$  or simply  $\sigma$  when the random variable  $X$  is understood from context. With this notation, the variance of  $X$  is denoted  $\sigma^2$ .

## Exercises

### C.3-1

Two ordinary, 6-sided dice are rolled. What is the expectation of the sum of the two values showing? What is the expectation of the maximum of the two values showing?

### C.3-2

An array  $A[1..n]$  contains  $n$  distinct numbers that are randomly ordered, with each permutation of the  $n$  numbers being equally likely. What is the expectation of the index of the maximum element in the array? What is the expectation of the index of the minimum element in the array?

**C.3-3**

A carnival game consists of three dice in a cage. A player can bet a dollar on any of the numbers 1 through 6. The cage is shaken, and the payoff is as follows. If the player's number doesn't appear on any of the dice, he loses his dollar. Otherwise, if his number appears on exactly  $k$  of the three dice, for  $k = 1, 2, 3$ , he keeps his dollar and wins  $k$  more dollars. What is his expected gain from playing the carnival game once?

**C.3-4**

Argue that if  $X$  and  $Y$  are nonnegative random variables, then

$$E[\max(X, Y)] \leq E[X] + E[Y] .$$

**C.3-5** ★

Let  $X$  and  $Y$  be independent random variables. Prove that  $f(X)$  and  $g(Y)$  are independent for any choice of functions  $f$  and  $g$ .

**C.3-6** ★

Let  $X$  be a nonnegative random variable, and suppose that  $E[X]$  is well defined. Prove **Markov's inequality**:

$$\Pr\{X \geq t\} \leq E[X]/t \tag{C.29}$$

for all  $t > 0$ .

**C.3-7** ★

Let  $S$  be a sample space, and let  $X$  and  $X'$  be random variables such that  $X(s) \geq X'(s)$  for all  $s \in S$ . Prove that for any real constant  $t$ ,

$$\Pr\{X \geq t\} \geq \Pr\{X' \geq t\} .$$

**C.3-8**

Which is larger: the expectation of the square of a random variable, or the square of its expectation?

**C.3-9**

Show that for any random variable  $X$  that takes on only the values 0 and 1, we have  $\text{Var}[X] = E[X]E[1 - X]$ .

**C.3-10**

Prove that  $\text{Var}[aX] = a^2\text{Var}[X]$  from the definition (C.26) of variance.