

Preliminaries

This section revises some parts of Core A Probability, which are essential for this course, and lists some other mathematical facts to be used (without proof) in the following.

Probability space

We recall that a *sample space* Ω is a collection of all possible outcomes of a probabilistic experiment; an *event* is a collection of possible outcomes, ie., a subset of the sample space. We introduce the *impossible* event \emptyset and the *certain* event Ω ; also, if $A \subset \Omega$ and $B \subset \Omega$ are events, it is natural to consider other events such that $A \cup B$ (**A or B**), $A \cap B$ (**A and B**), $A^c \equiv \Omega \setminus A$ (**not A**), and $A \setminus B$ (**A but not B**).

Definition 0.1. Let \mathcal{A} be a collection of subsets of Ω . We shall call \mathcal{A} a field if it has the following properties:

1. $\emptyset \in \mathcal{A}$;
2. if $A_1, A_2 \in \mathcal{A}$, then $A_1 \cup A_2 \in \mathcal{A}$;
3. if $A \in \mathcal{A}$, then $A^c \in \mathcal{A}$.

Remark 0.1.1. Obviously, every field is closed w.r.t. taking finite unions or intersections.

Definition 0.2. Let \mathcal{F} be a collection of subsets of Ω . We shall call \mathcal{F} a σ -field if it has the following properties:

1. $\emptyset \in \mathcal{F}$;
2. if $A_1, A_2, \dots \in \mathcal{F}$, then $\bigcup_{k=1}^{\infty} A_k \in \mathcal{F}$;
3. if $A \in \mathcal{F}$, then $A^c \in \mathcal{F}$.

Remark 0.2.1. Obviously, property 2 above can be replaced by the equivalent condition $\bigcap_{k=1}^{\infty} A_k \in \mathcal{F}$.

Clearly, if Ω is fixed, the smallest σ -field in Ω is just $\{\emptyset, \Omega\}$ and the biggest σ -field consists of all subsets of Ω . We observe the following simple fact:

Exercise 0.3. Show that if \mathcal{F}_1 and \mathcal{F}_2 are σ -fields, then¹ $\mathcal{F}_1 \cap \mathcal{F}_2$ is a σ -field, but, in general, $\mathcal{F}_1 \cup \mathcal{F}_2$ is not a σ -field.

If A and B are events, we say that A and B are incompatible (or disjoint), if $A \cap B = \emptyset$.

Definition 0.4. Let Ω be a sample space, and \mathcal{F} be a σ -field of events in Ω . A probability distribution P on (Ω, \mathcal{F}) is a collection of numbers $P(A)$, $A \in \mathcal{F}$, possessing the following properties:

¹and, in fact, an intersection of arbitrary (even **uncountable!**) collection of σ -fields;

A1 for every event $A \in \mathcal{F}$, $P(A) \geq 0$;

A2 $P(\Omega) = 1$;

A3 for any pair of incompatible events A and B , $P(A \cup B) = P(A) + P(B)$;

A4 for any *countable* collection A_1, A_2, \dots of mutually incompatible² events,

$$P\left(\bigcup_{k=1}^{\infty} A_k\right) = \sum_{k=1}^{\infty} P(A_k).$$

Remark 0.4.1. Notice that the additivity axiom **A4** above does not extend to uncountable collections of incompatible events.

Remark 0.4.2. Obviously, property **A4** above and Definition 0.2 are non-trivial only in examples with infinitely many different events, ie., when the collection \mathcal{F} of all events (and, therefore, the sample space Ω) is infinite.

The following properties are immediate from the above axioms:

P1 for any pair of events A, B in Ω we have

$$P(B \setminus A) = P(B) - P(A \cap B), \quad P(A \cup B) = P(A) + P(B \setminus A);$$

in particular, $P(A^c) = 1 - P(A)$;

P2 if events A, B in Ω are such that $\emptyset \subseteq A \subseteq B \subseteq \Omega$, then

$$0 = P(\emptyset) \leq P(A) \leq P(B) \leq P(\Omega) = 1.$$

P3 if A_1, A_2, \dots, A_n are events in Ω , then $P(\cup_{k=1}^n A_k) \leq \sum_{k=1}^n P(A_k)$ with the inequality becoming an equality if these events are mutually incompatible;

Definition 0.5. A *probability space* is a triple (Ω, \mathcal{F}, P) , where Ω is a sample space, \mathcal{F} is a σ -field of events in Ω , and $P(\cdot)$ is a probability measure on (Ω, \mathcal{F}) .

In what follows we shall always assume that some probability space (Ω, \mathcal{F}, P) is fixed.

Conditional probability, independence

Definition 0.6. The *conditional probability* of event A given event B such that $P(B) > 0$, is

$$P(A|B) \stackrel{\text{def}}{=} \frac{P(A \cap B)}{P(B)}.$$

It is easy to see that if $E \in \mathcal{F}$ is any event with $P(E) > 0$, then $P(\cdot|E)$ is a probability measure on (Ω, \mathcal{F}) , ie., axioms **A1–A4** and properties **P1–P3** hold (just $P(\cdot)$ replace with $P(\cdot|E)$). We list some additional useful properties of conditional probabilities:

²ie., $A_k \cap A_j = \emptyset$ for all $k \neq j$;

P4 *multiplication rule* for probabilities: if A and B are events, then

$$P(A \cap B) = P(A) P(B | A) = P(B) P(A | B);$$

more generally, if A_1, \dots, A_n are arbitrary events in \mathcal{F} , then

$$P\left(\bigcap_{k=1}^n A_k\right) = P(A_1) \cdot \prod_{k=2}^n P\left(A_k \mid \bigcap_{j=1}^{k-1} A_j\right); \quad (0.1)$$

for example, $P(A \cap B \cap C) = P(A) P(B | A) P(C | A \cap B)$.

P5 *partition theorem or formula of total probability*: we say that events B_1, \dots, B_n form a **partition** of Ω if they are mutually incompatible (disjoint) and their union $\bigcup_{k=1}^n B_k$ is the entire space Ω . The partition theorem says that if B_1, \dots, B_n form a partition of Ω , then for any event A we have

$$P(A) = \sum_{k=1}^n P(B_k) \cdot P(A | B_k). \quad (0.2)$$

P6 *Bayes' theorem*: for any events A, B , we have

$$P(A | B) = \frac{P(A) P(B | A)}{P(B)};$$

in particular, if D is an event and C_1, \dots, C_n form a partition of Ω , then

$$P(C_k | D) = \frac{P(C_k) P(D | C_k)}{\sum_{k=1}^n P(C_k) P(D | C_k)}; \quad (0.3)$$

Exercise 0.7. Check carefully (ie., by induction) property **P4** above.

Then next definition is one of the most important in probability theory.

Definition 0.8. We say that events A and B are *independent* if

$$P(A \cap B) = P(A) P(B); \quad (0.4)$$

under (0.4), we have $P(A | B) = P(A)$, ie., event A is *independent of* B ; similarly, $P(B | A) = P(B)$, ie., event B is *independent of* A .

More generally,

Definition 0.9. A collection of events A_1, \dots, A_n is called (*mutually*) *independent*, if

$$P\left(\bigcap_{k=1}^n A_k\right) = \prod_{k=1}^n P(A_k). \quad (0.5)$$

It is immediate from (0.5) that every sub-collection of $\{A_1, \dots, A_n\}$ is also mutually independent.

Random variables

It is very common for the sample space Ω of possible outcomes to be a set of *real numbers*. Then the outcome to the “probabilistic experiment” is often called a *random variable* and denoted by a capital letter such as X . In this case the events are subsets $A \subseteq \mathbb{R}$ and it is usual to write $P(X \in A)$ instead of $P(A)$ and similarly $P(X = 1)$ for $P(\{1\})$, $P(1 < X < 5)$ for $P(A)$ where $A = (1, 5)$ and so on. The *probability distribution* of a r.v. X is the collection of probabilities $P(X \in A)$ for all intervals $A \subseteq \mathbb{R}$ (and other events that can be obtained from intervals via axioms **A1**–**A4**).

Let X be a random variable (so the sample space Ω is a subset of \mathbb{R}). We say that X is a *discrete r.v.* if in addition Ω is countable, i.e., if the possible values for X can be enumerated in a (possibly infinite) list. In this case the function $p(x) \stackrel{\text{def}}{=} P(X = x)$ (defined for all real x) is called the *probability mass function* of X and the corresponding probability distribution of X is defined via

$$P(X \in A) = \sum_{x \in A} P(X = x) = \sum_{x \in A} p(x).$$

If X takes possible values x_1, x_2, \dots , then, by axiom **A3**, $\sum_{k \geq 1} p(x_k) = 1$ and if x is NOT one of the possible values of X then $p(x) = 0$.

Similarly, a random variable X has a *continuous probability distribution* if there exists a non-negative function $f(x)$ on \mathbb{R} such that for any interval $(a, b) \subseteq \mathbb{R}$

$$P(a < X < b) = \int_a^b f(x) dx;$$

in particular, by axiom **A3**, we must have $\int_{-\infty}^{\infty} f(x) dx = 1$. The function $f(\cdot)$ is then called the *probability density function* (or *pdf*) of X .

In Core A Probability you saw a number of random variables with discrete (Bernoulli, binomial, geometric, Poisson) or continuous (uniform, exponential, normal) distribution.

Definition 0.10. For any random variable X , the *cumulative distribution function* (or *cdf*) of X is the function $F : \mathbb{R} \rightarrow [0, 1]$ that is given at all $x \in \mathbb{R}$ by

$$F(x) \stackrel{\text{def}}{=} P(X \leq x) = \begin{cases} \int_{-\infty}^x f(y) dy, & X \text{ a continuous r.v.}; \\ \sum_{x_k : x_k \leq x} p(x_k), & X \text{ a discrete r.v.}; \end{cases} \quad (0.6)$$

If, in addition, $f(x)$ is continuous function on some interval (a, b) then by the fundamental theorem of calculus, for all $x \in (a, b)$, $F'(x) = f(x)$; i.e., the cdf determines the pdf and vice versa. In fact, the cdf of a r.v. X always determines its probability distribution.

Remark 0.10.1. Suppose X is a random variable and h is some real-valued function defined for all real numbers. Then $h(X)$ is also a random variable, namely, the outcome to a new “experiment” obtained by running the old “experiment” to produce the r.v. X and then evaluating $h(X)$.

Joint distributions

It is essential for most useful applications of probability to have a theory which can handle many random variables simultaneously.

Definition 0.11. Let (X_1, \dots, X_n) be a *multivariate* random variable (or *random vector*). Its cumulative distribution function is

$$F_{X_1, \dots, X_n}(x_1, \dots, x_n) \stackrel{\text{def}}{=} \mathbf{P}(X_1 \leq x_1, \dots, X_n \leq x_n), \quad (0.7)$$

here and below we write $\{X_1 \leq x_1, \dots, X_n \leq x_n\} = \{X_1 \leq x_1\} \cap \dots \cap \{X_n \leq x_n\}$.

Bivariate variables: discrete case

Suppose (X, Y) is a bivariate r.v. and that X and Y are discrete r.v. taking possible values x_1, x_2, \dots and y_1, y_2, \dots respectively. Then the collection of probabilities

$$p(x_j, y_k) \equiv \mathbf{P}(X = x_j, Y = y_k), \quad k \geq 1, j \geq 1,$$

determines the *joint probability distribution* of (X, Y) . It is important to remember that given the joint distribution of X, Y we can recover the probability density function p_X (in this case it is called the *marginal probability distribution*) of X via

$$p_X(x_j) \equiv \mathbf{P}(X = x_j) = \sum_k \mathbf{P}(X = x_j, Y = y_k) = \sum_k p(x_j, y_k) \quad (0.8)$$

for any possible value x_j of X . Similarly, the marginal probability distribution of Y is given by

$$p_Y(y_k) = \sum_j \mathbf{P}(X = x_j, Y = y_k) = \sum_j p(x_j, y_k).$$

Conditional distribution and independence

For any discrete bivariate rv (X, Y) the *conditional distribution* of X given Y has probability mass function

$$p(x | y) \equiv \mathbf{P}(X = x | Y = y) = \frac{p(x, y)}{p_Y(y)}$$

for all y with $p_Y(y) > 0$. There is also a r.v. version of the partition theorem (0.2); it is often called the *law of total probability*: for any X -event A ,

$$\mathbf{P}(X \in A) = \sum_y \mathbf{P}(X \in A | Y = y) p_Y(y). \quad (0.9)$$

We say that X and Y are *independent* if for all x, y

$$p(x, y) = p_X(x) p_Y(y). \quad (0.10)$$

Alternatively, we have

Definition 0.12. Random variables X, Y are *independent* if for every X -event A and every Y -event B we have

$$P(X \in A, Y \in B) \equiv P((X, Y) \in A \times B) = P(X \in A) P(Y \in B). \quad (0.11)$$

The definitions (0.10), (0.11) can be easily extended to the case of any general multivariate distribution.

Let (X_1, \dots, X_n) be a random vector and $g : \mathbb{R}^n \rightarrow \mathbb{R}$ be a function. Then $g(X_1, \dots, X_n)$ is a random variable (obtained by the new “experiment” consisting of first carrying out the original experiment to determine the value of (X_1, \dots, X_n) and then applying the function g to this ordered n -tuple to obtain a real number $g(X_1, \dots, X_n)$).

Exercise 0.13. 1). Let (X, Y, Z) be a random vector with independent components; show that for any function $h : \mathbb{R}^2 \rightarrow \mathbb{R}$ the variables $h(X, Y)$ and Z are independent.

2). Let X_1, \dots, X_k and Y_1, \dots, Y_m be a collection of independent random variables. If the functions f and g are such that $f : \mathbb{R}^k \rightarrow \mathbb{R}$ and $g : \mathbb{R}^m \rightarrow \mathbb{R}$, show that the random variables $f(X_1, \dots, X_m)$ and $g(Y_1, \dots, Y_m)$ are independent.

Bivariate variables: continuous case

We will only consider the case where (X, Y) has a continuous joint pdf $f(x, y)$ defined for $(x, y) \in \mathbb{R}^2$. By analogy with the definition for discrete random variables,

$$P((X, Y) \in A) = \iint_A f(x, y) dx dy$$

for any integrable set A . In this case X and Y have the *marginal* pdfs

$$f_X(x) = \int_{-\infty}^{\infty} f(x, y) dy, \quad f_Y(y) = \int_{-\infty}^{\infty} f(x, y) dx$$

and for any interval (a, b) we have

$$P(a < X < b) \equiv \int_a^b \int_{-\infty}^{\infty} f(x, y) dx dy = \int_a^b f_X(x) dx.$$

We define the continuous conditional density of X given Y by

$$f(x|y) = \begin{cases} f(x, y)/f_Y(y), & \text{if } f_Y(y) > 0 \\ 0, & \text{if } f_Y(y) = 0. \end{cases}$$

Also, X and Y are *independent* if and only if $f(x, y) = f_X(x) f_Y(y)$ for every pair $(x, y) \in \mathbb{R}^2$.

Transformations $g(X, Y)$ in the continuous case are treated similarly to the discrete case.

Expectation

Definition 0.14. For any random variable X the *expected value* (or *mean*) of X is the number

$$\mathbf{E}(X) = \begin{cases} \sum_{x_k \in \Omega} x_k p(x_k), & X \text{ discrete with pmf } p; \\ \int_{-\infty}^{\infty} x f(x) dx, & X \text{ continuous with pdf } f. \end{cases} \quad (0.12)$$

The following generalisation of this definition is of great importance to the whole theory.

If X is a discrete rv and takes values in $\Omega = \{x_1, x_2, \dots\}$ with probabilities $p(x_k)$ and the transformed rv $g(X)$ takes values y_1, y_2, \dots with probabilities

$$q(y_m) \stackrel{\text{def}}{=} \mathbf{P}(X \in G_m) = \sum_{x \in G_m} p(x), \quad \text{where } G_m \stackrel{\text{def}}{=} \{x \in \Omega : g(x) = y_m\},$$

then the sets G_m form a partition of Ω and it follows that

$$\mathbf{E}(g(X)) = \sum_m y_m q(y_m) = \sum_m \sum_{x \in G_m} g(x) p(x) = \sum_{k=1}^{\infty} g(x_k) p(x_k).$$

Similarly, if X is continuous rv with pdf f , then

$$\mathbf{E}(g(X)) = \int_{-\infty}^{\infty} g(x) f(x) dx.$$

The most important properties of the expectation are:

E1 linearity: let f, g be real functions and let a, b be real numbers; then

$$\mathbf{E}(af(X) + bg(X)) = a\mathbf{E}(f(X)) + b\mathbf{E}(g(X)), \quad (0.13)$$

provided the corresponding expectations exist.

E2 monotonicity: if $h(x) \geq 0$ for all real x , then $\mathbf{E}(h(X)) \geq 0$; in other words, if the real functions f, g are such that $f(x) \leq g(x)$ for all real x , then

$$\mathbf{E}(f(X)) \leq \mathbf{E}(g(X)), \quad (0.14)$$

provided the corresponding expectations exist.

Recall three important special cases: the *variance* $\text{Var}(X)$ of a rv X , its *r-th moment* $\mathbf{E}(X^r)$, and its *moment generating function*, $M_X(t)$,

$$\text{Var}(X) \stackrel{\text{def}}{=} \mathbf{E}(X - \mathbf{E}(X))^2, \quad M_X(t) \stackrel{\text{def}}{=} \mathbf{E}(e^{tX}).$$

Exercise 0.15. Let X be a rv, and let $g : \mathbb{R} \rightarrow [0, \infty]$ be an increasing function such that $\mathbf{E}(g(X)) < \infty$. Show that for any real a , one has

$$P(X > a) \leq \frac{\mathbf{E}(g(X))}{g(a)}. \quad (0.15)$$

In particular, $P(X > a) \leq \mathbf{E}(\exp\{\lambda(X - a)\})$ for any real a and any $\lambda > 0$.

Notice that the Markov inequality and the Chebyshev inequality are special cases of (0.15).

Multivariate case

In the multivariate case, the expectation is defined similarly and has properties analogous to the considered above. Additionally, we mention two other properties:

E3 multivariate linearity: let (X_1, \dots, X_n) be a random vector, g_1, \dots, g_n be real functions, and a_1, \dots, a_n be real numbers. Then

$$\mathbb{E}\left(\sum_{k=1}^n a_k g_k(X_k)\right) = \sum_{k=1}^n a_k \mathbb{E}(g_k(X_k)). \quad (0.16)$$

E4 independence: if X_1, \dots, X_n are independent rv's, so that their joint pmf/pdf factorises,

$$p_{X_1, \dots, X_n}(x_1, \dots, x_n) = \prod_{k=1}^n p_{X_k}(x_k),$$

then for all real functions g_1, \dots, g_n one has

$$\mathbb{E}\left(\prod_{k=1}^n g_k(X_k)\right) = \prod_{k=1}^n \mathbb{E}(g_k(X_k)). \quad (0.17)$$

We say that the variables X and Y are *uncorrelated* if their covariance,

$$\text{Cov}(X, Y) \stackrel{\text{def}}{=} \mathbb{E}((X - \mathbb{E}(X))(Y - \mathbb{E}(Y))) \equiv \mathbb{E}(XY) - \mathbb{E}(X)\mathbb{E}(Y), \quad (0.18)$$

vanishes, $\text{Cov}(X, Y) = 0$. In particular, any pair of independent variables is uncorrelated.

By linearity property **E3**, the variance $\text{Var}(\sum_{k=1}^n X_k)$ of the sum of rv's X_1, \dots, X_n equals

$$\text{Var}\left(\sum_{k=1}^n X_k\right) = \sum_{k=1}^n \text{Var}(X_k) + 2 \sum_{k < l} \text{Cov}(X_k, X_l).$$

Thus, if the variables X_1, \dots, X_n are *pairwise uncorrelated* (in particular, independent), then

$$\text{Var}\left(\sum_{k=1}^n X_k\right) = \sum_{k=1}^n \text{Var}(X_k). \quad (0.19)$$

Conditional expectation

Let X be a discrete rv on a sample space Ω , and let $A \subseteq \Omega$ be an event. The *conditional expectation* of X given A is a number $\mathbb{E}(X | A)$ defined by

$$\mathbb{E}(X | A) = \sum_x x \mathbb{P}(X = x | A), \quad (0.20)$$

where the sum runs through all possible values of X .

In particular, we have the **partition theorem for expectation**: if events B_1, \dots, B_n form a partition of the sample space Ω , then

$$\mathbf{E}(X) = \sum_{k=1}^n \mathbf{E}(X | B_k) \mathbf{P}(B_k).$$

Using the definition (0.20), it is immediate to compute $\mathbf{E}(X | Y = y)$; we recall that then $\mathbf{E}(X | Y)$ is a random variable such that $\mathbf{E}(\mathbf{E}(X | Y)) = \mathbf{E}(X)$.

Limiting results

Theorem 0.16 (Law of Large Numbers). *Let X_1, \dots, X_n be iid (independent, identically distributed) rv's such that*

$$\mathbf{E}(X_k) \equiv \mu, \quad \text{Var}(X_k) = \sigma^2.$$

Denote $S_n \stackrel{\text{def}}{=} \sum_{k=1}^n X_k$. Then for any fixed $a > 0$

$$\mathbf{P}(|n^{-1}S_n - \mu| > a) \rightarrow 0 \tag{0.21}$$

as $n \rightarrow \infty$.

Theorem 0.17 (Central Limit Theorem). *Under the conditions of the previous theorem, denote*

$$S_n^* \stackrel{\text{def}}{=} \frac{S_n - n\mu}{\sqrt{\text{Var}(S_n)}} \equiv \frac{S_n - n\mu}{\sigma\sqrt{n}}.$$

Then, as $n \rightarrow \infty$, the distribution of S_n^ converges to that of the standard Gaussian random variable (ie., $\mathcal{N}(0, 1)$): for every fixed $a \in \mathbb{R}$,*

$$\mathbf{P}(S_n^* \leq a) \rightarrow \int_{-\infty}^a \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy. \tag{0.22}$$

Moment generating functions

As mentioned before, the *moment generating function* (or *mgf*) of a rv X is defined via

$$M_X(t) \stackrel{\text{def}}{=} \mathbf{E}(e^{tX}). \tag{0.23}$$

We finish by listing several useful properties of mgf's.

M1 For each positive integer r

$$\mathbf{E}(X^r) = \frac{d^r M_X}{dt^r}(0).$$

M2 [uniqueness] The mgf $M_X(t)$ of X uniquely determines the probability distribution of X , provided that $M_X(t)$ is finite in some neighbourhood of the origin.

M3 [linear transformation] If X has mgf $M_X(t)$, and $Y = aX + b$, then

$$M_Y(t) = e^{bt} M_X(at).$$

M4 [independence] Suppose that X_1, \dots, X_n are independent rv's and let $Y = \sum_{k=1}^n X_k$. Then

$$M_Y(t) = \prod_{k=1}^n M_{X_k}(t).$$

M5 [convergence] Suppose that Y_1, Y_2, \dots is an infinite sequence of rv's, and that Y is a further random variable. Suppose that $M_{Y_n}(t)$ is finite for $|t| < a$ for some positive a and that for all $t \in (-a, a)$

$$M_{Y_n}(t) \rightarrow M_Y(t) \quad \text{as } n \rightarrow \infty.$$

Then, as $n \rightarrow \infty$,

$$P(Y_n \leq c) \rightarrow P(Y \leq c).$$

for all real c such that $P(Y = c) = 0$.