Probability

Derek Li

Contents

1 Review

1.1 Set

Definition 1.1 (Power Set)**.** For a given set Ω, the power set is the set of all of its subsets

$$\mathcal{P}(\Omega) = \{A | A \subset \Omega\}.$$

The power set is closed w.r.t. all the usual set-theoretic operations.

Definition 1.2 (Arbitrary Unions)**.** Let $\omega \in \Omega, A_n \subset \Omega, n \in \mathbb{N}$.

$$\omega \in \bigcup_{n=1}^{\infty} A_n \text{ iff } \exists n \text{ s.t. } \omega \in A_n$$

Definition 1.3 (Arbitrary Intersections)**.** Let $\omega \in \Omega, A_n \subset \Omega, n \in \mathbb{N}$.

$$\omega \in \bigcap_{n=1}^{\infty} A_n \text{ iff } \forall n, \omega \in A_n.$$

Hence, we have

$$P(\omega \in A_n, \exists n) = P\left(\omega \in \bigcup_{n=1}^{\infty} A_n\right) \text{ and } P(\omega \in A_n, \forall n) = P\left(\omega \in \bigcap_{n=1}^{\infty} A_n\right).$$

Definition 1.4 (Infinitely Often)**.** Let $\omega \in \Omega, A_n \subset \Omega, n, N \in \mathbb{N}$.

$$\omega \in \bigcap_{N=1}^{\infty} \bigcup_{n=N}^{\infty} A_n \text{ iff } \forall N, \exists n \geqslant N \text{ s.t. } \omega \in \bigcup_{n=N}^{\infty} A_n.$$

1.2 Number Systems and Euclidean Space

With the notation of set, one way to consider whole number could be:
$0 = \varnothing, 1 = \{\varnothing\}, 2 = \{0, 1\}, \cdots$, and thus

$$\begin{aligned} n + 1 &= n \cup \{n\} \\ &= \{0, 1, \cdots, n-1\} \cup \{n\} \\ &= \{0, 1, \cdots, n\}. \end{aligned}$$

We can also define number systems with set:

$$\mathbb{N} = \{1, 2, \cdots\}, \mathbb{W} = \mathbb{N} \cup \{0\}, \mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}, \mathbb{Q} = \left\{\frac{n}{m}\middle| n \in \mathbb{Z}, m \in \mathbb{N}\right\},$$
$$\mathbb{R} = \left\{x = \lim_{n\to\infty} r_n \middle| r_n \in \mathbb{Q}, n \in \mathbb{N}\right\}, \mathbb{C} = \{z = x + iy | x, y \in \mathbb{R}\}.$$

In multi-variable calculus, we define

$$\mathbb{R}^n = \{\mathbf{x} | x_i \in \mathbb{R}.i = 1, \cdots, n\},$$

where $\mathbf{x} = (x_i, i = 1, \cdots, n)$ and

$$\mathbb{R}^\infty = \{\mathbf{x} = (x_i, i = 1, 2, \cdots) | x_i \in \mathbb{R}, i \in \mathbb{N}\}.$$

1.3 Functions

Before we define a function, we look at the product $A \times B$ of any two sets A and B, which is defined as the set of all ordered pairs that may be formed of the elements of the first set A, with the second set B :

$$A \times B = \{(a, b) | a \in A, b \in B\}.$$

Definition 1.5 (Ordered Pairs)**.** An ordered pair is $(a, b) = \{\{a\}, \{a, b\}\}$.

Definition 1.6 (Function)**.** A function f with domain A and range B, denoted by $f : A \to B$, is any $f \subset A \times B$ s.t. $\forall a \in A, \exists! b \in B$ with $(a, b) \in f$.

From the definition, b is uniquely determined by a and we may write $b = f(a)$.

The collection of all functions from a particular domain A to a certain B is denoted by

$$B^A = \{f \subset A \times B | f : A \to B\}.$$

1.4 Inverse Image

Definition 1.7 (Inverse Image)**.** For any function say $X : \Omega \to \mathcal{X}$, the inverse image of any $A \subset \mathcal{X}$ is defined as

$$X^{-1}(A) := \{\omega \in \Omega | X(\omega) \in A\}.$$

1.5 Indicator Functions and Indicator Map

Definition 1.8 (Indicator Function)**.** For any $A \subset \Omega$, we define $I_A \in 2^\Omega$ by

$$I_A(\omega) := \begin{cases} 1, & \omega \in A \\ 0, & \omega \notin A \end{cases}.$$

Indicator function defines a bijective correspondence between subsets of Ω and their indicator functions, that is referred to as the indicator map

$$\begin{aligned} I : \mathcal{P}(\Omega) &\overset{\cong}{\to} 2^\Omega \\ A &\mapsto I_A. \end{aligned}$$

Theorem 1.1. The indicator map is bijective.

Proof. We want to show the indicator map is both injective and surjective.

(Injection) Let $I_A = I_B$, then $I_A(\omega) = I_B(\omega), \forall \omega$.

We have

$$\omega \in A \Leftrightarrow I_A(\omega) = 1 = I_B(\omega) \Leftrightarrow \omega \in B,$$

i.e., $A = B$.

(Surjection) Want to show $\forall f \in 2^\Omega, \exists A \in \mathcal{P}(\Omega)$ s.t. $I(A) = I_A = f$.

Take any $f \in 2^\Omega$ and let $A = \{\omega | f(\omega) = 1\}$. We have

$$\omega \in A \Leftrightarrow \begin{cases} f(\omega) = 1 \\ I_A(\omega) = 1 \end{cases} \Rightarrow f(\omega) = I_A(\omega), \forall \omega.$$

Hence, $f = I_A$. □

From the proof, we also have

$$A = f^{-1}(1) = I_A^{-1}(1).$$

Note that

$$I_{\bigcap_{n=1}^\infty A_n}(\omega) = \inf_{n=1}^{\infty} I_{A_n}(\omega) \text{ and } I_{\bigcup_{n=1}^\infty A_n}(\omega) = \sup_{n=1}^{\infty} I_{A_n}(\omega).$$

Also,

$$\sum_{n=1}^{\infty} I_{A_n}(\omega) \in \mathbb{W} \cup \{\infty\}.$$

1.6 Series

Recall that when $|a| < 1$,

$$\sum_{i=0}^{\infty} a^i := \lim_{n\to\infty} \sum_{i=0}^{n} a^i = \lim_{n\to\infty} \frac{1-a^{n+1}}{1-a} = \frac{1}{1-a}.$$

2 Random Variables

Definition 2.1 (Finite Discrete Uniform Distribution)**.** $U \sim \text{unif}(\Omega)$ with ${}^{\#}\Omega < {}^{\#}\mathbb{N}$ iff

$$P(U = \omega) = \frac{1}{\Omega} \Leftrightarrow P(U \in A) = \frac{{}^{\#}A}{{}^{\#}\Omega}.$$

Example 2.1. $U \sim \text{unif}\{1, \cdots, n\}$ iff $P(U = i) = \frac{1}{n}, i = 1, \cdots, n$.

Note. $-U \sim \text{unif}\{-n, \cdots, -1\}$ and $n + 1 - U \sim \text{unif}\{1, \cdots, n\}$. Hence we say $n + 1 - U \overset{\text{d}}{=} U$ and thus

$$n + 1 - \mathbb{E}[U] = \mathbb{E}[U] \Rightarrow \mathbb{E}[U] = \frac{n+1}{2} = \frac{1 + \cdots + n}{n}.$$

Here is another way to express $Z \sim \text{unif}\{0, 1, \cdots, p - 1\}$.

Definition 2.2. $Z \sim \text{unif}(p)$, where $p = \{0, 1, \cdots, p - 1\}$, iff

$$P(Z = i) = \frac{1}{p}, \forall i \in p.$$

Definition 2.3 (Uniform Distribution)**.** $U \sim \text{unif}[0, 1]$ iff

$$P(U \leqslant u) = u, \forall 0 \leqslant u \leqslant 1.$$

2.1 Distribution Functions in General

Theorem 2.1 (Sequential Continuity)**.** $A_n \to A \Rightarrow P(A_n) \to P(A)$.

2.2 Fundamental Theorem of Applied Probability

For any $p \in \mathbb{N}$ with $p \geqslant 2$ we define the p-adic series

$$U = \sum_{i=1}^{\infty} Z_i p^{-i}.$$

Example 2.2. $Z : z_{11}, z_{12}, \cdots, z_{1n}, \cdots; z_{21}, z_{22}, \cdots, z_{2n}$ and
$U = .z_{11}z_{12}z_{13}\cdots, .z_{21}z_{22}z_{23}\cdots$.

If $Z \sim \text{unif}(10)$, then $.z_1z_2\cdots z_n\cdots = \sum_{i=1}^{\infty} z_i 10^{-i}$.

Lemma 2.1. Let $\dot{p}^{\infty} = \{\mathbf{z} = (z_i, i \in \mathbb{N}) | z_i \in p, i \in \mathbb{N}, z_i < p-1 \text{ io}(i)\}$. Then $u = \sum\limits_{i=1}^{\infty} z_i p^{-i}$ defines a bijective function $\Phi : \dot{p}^{\infty} \xrightarrow{\cong} [0,1)$.

Note. The range cannot include 1, because it is not allowed to end in $p-1$ repeated and

$$\sum_{i=1}^{\infty} p^{-i}(p-1) = \frac{p-1}{p} \sum_{i=0}^{\infty} p^{-i} = \frac{p-1}{p} = 1.$$

Proof. We know $0 \leqslant u < \frac{p-1}{p} \sum_{i=0}^{\infty} p^{-i} = 1$.

Besides,

$$u = \sum_{i=1}^{\infty} z_i p^{-i}$$
$$\Leftrightarrow 0 \leqslant u - \sum_{i=1}^{n} z_i p^{-i} = \sum_{i=n+1}^{\infty} z_i p^{-i} < \sum_{i=n+1}^{\infty} p^{-i}(p-1) = p^{-(n+1)} \frac{p-1}{1-1/p} = p^{-n}.$$
$$\Leftrightarrow z_n p^{-n} \leqslant u - \sum_{i=1}^{n-1} z_i p^{-i} < p^{-n} + z_n p^{-n} = (z_n+1)p^{-n}.$$
$$\Leftrightarrow z_n \leqslant p^n \left(u - \sum_{i=1}^{n-1} z_i p^{-i} \right) < z_n + 1.$$

Recall that $[x] = m$ iff $m \leqslant x < m+1$ uniquely determines m as the greatest integer less than or equal to x. Therefore,

$$z_n = \left[p^n \left(u - \sum_{i=1}^{n-1} z_i p^{-i} \right) \right], n \geqslant 2,$$

and $z_1 = [pu]$. □

Lemma 2.2. For $u = \sum\limits_{i=1}^{\infty} z_i p^{-i}, \mathbf{z} \in \dot{p}^{\infty}$, we have

$$z_1 = b_1, \cdots, z_n = b_n \Leftrightarrow u \in \left[\sum_{i=1}^{n} b_i p^{-i}, \sum_{i=1}^{n} b_i p^{-i} + p^{-n} \right).$$

Theorem 2.2 (Fundamental Theorem of Applied Probability)**.** For $U = \sum_{i=1}^{\infty} Z_i p^{-i}, p \geqslant 2$, we have

$$U \sim \text{unif}[0,1] \Leftrightarrow Z_i \overset{\text{i.i.d.}}{\sim} \text{unif}(p).$$