



## 2.1 Counting

Remember that for a finite sample space  $S$  with equally likely outcomes, the probability of an event  $A$  is given by

$$P(A) = \frac{|A|}{|S|} = \frac{M}{N}$$

Thus, finding probability of  $A$  reduces to a **counting** problem in which we need to count how many elements are in  $A$  and  $S$ . In this section, we will discuss ways to count the number of elements in a set in an efficient manner. Counting is an area of its own and there are books on this subject alone. Here we provide a basic introduction to the material that is usually needed in probability. Almost everything that we need about counting is the result of the **multiplication principle**. We previously saw the multiplication principle when we were talking about Cartesian products. Here we look at it from a different perspective. Let us look at a simple example.

---

### Example 2.1

Suppose that I want to purchase a tablet computer. I can choose either a large or a small screen; a 64GB, 128GB, or 256GB storage capacity, and a black or white cover. How many different options do I have?

**Solution**

Here are the options:

1. L-64-B
2. L-64-W
3. L-128-B
4. L-128-W
5. L-256-B
6. L-256-W
7. S-64-B
8. S-64-W
9. S-128-B

- 10. S-128-W
- 11. S-256-B
- 12. S-256-W

Thus, there are 12 possible options. The multiplication principle states that we can simply multiply the number of options in each category (screen size, memory, color) to get the total number of possibilities, i.e., the answer is  $2 \times 3 \times 2 = 12$ .

---

Here is a formal statement of the multiplication principle.

**Multiplication Principle**

Suppose that we perform  $r$  experiments such that the  $k$ th experiment has  $n_k$  possible outcomes, for  $k = 1, 2, \dots, r$ . Then there are a total of  $n_1 \times n_2 \times n_3 \times \dots \times n_r$  possible outcomes for the sequence of  $r$  experiments.

---

**Example 2.2**

I need to choose a password for a computer account. The rule is that the password must consist of two lowercase letters (a to z) followed by one capital letter (A to Z) followed by four digits (0, 1,  $\dots$ , 9). For example, the following is a valid password

*ejT3018*

- Find the total number of possible passwords,  $N$ .
- A hacker has been able to write a program that randomly and independently generates  $10^8$  passwords according to the above rule. Note that the same password could be generated more than once. If one of the randomly chosen passwords matches my password, then he can access my account information. What is the probability that he is successful in accessing my account information?

**Solution**

To choose a password, I need to first choose a lowercase letter, then another lowercase letter, then one capital letter, and then 4 digits. There are 26 lowercase

letters, 26 capital letters, and 10 digits. Thus, by the multiplication principle, the total number of possible valid passwords is

$$N = 26 \times 26 \times 26 \times 10 \times 10 \times 10 \times 10 = 26^3 \times 10^4$$

Let  $G_i$  denote the event that the hacker's  $i$ th guess matches mine, for  $i = 1, 2, \dots, 10^8$ . The probability that the  $i$ th randomly chosen password matches mine is

$$P(G_i) = \frac{1}{N}$$

Now let  $p_{hack}$  be the probability that the hacker is successful, that is at least one of the randomly chosen passwords matches mine. Recall that "at least" means union:

$$p_{hack} = P\left(\bigcup_i G_i\right)$$

Note that the events  $G_i$  are independent since the guesses are independently generated, but they are not disjoint since multiple guesses could be correct if the hacker's program generates the same password. Therefore in this case it is easier to work with intersections than unions, so we will find the probability of the complement event first:

$$\begin{aligned} P\left(\bigcup_i G_i\right)^c &= P\left(\bigcap_i G_i^c\right) \\ &= \prod_{i=1}^N P(G_i^c) \quad (\text{by independence}) \\ &= \left(1 - \frac{1}{N}\right)^{10^8} \end{aligned}$$

Therefore,

$$\begin{aligned} p_{hack} &= 1 - \left(1 - \frac{1}{N}\right)^{10^8} \\ &= 1 - \left(1 - \frac{1}{26^3 \times 10^4}\right)^{10^8} \\ &= 0.4339 \end{aligned}$$

### Example 2.3

Let  $A$  be a set with  $|A| = n < \infty$ . How many distinct subsets does  $A$  have?

## Solution

Let's assume  $A = \{a_1, a_2, a_3, \dots, a_n\}$ . We can look at this problem in the following way. To choose a subset  $B$ , we perform the following experiment. First we decide whether or not  $a_1 \in B$  (two choices), then we decide whether or not  $a_2 \in B$  (two choices), then we decide whether or not  $a_3 \in B$  (two choices), ..., and finally we decide whether or not  $a_n \in B$  (two choices). By the multiplication principle, the total number of subsets is then given by  $2 \times 2 \times 2 \times \dots \times 2 = 2^n$ . To check our answer, let's assume  $A = \{1, 2\}$ . Then our formula states that there are 4 possible subsets. Indeed, the subsets are

1.  $\{\} = \emptyset$
  2.  $\{1\}$
  3.  $\{2\}$
  4.  $\{1, 2\}$
- 

Here, we would like to provide some general terminology for the counting problems that show up in probability to make sure that the language that we use is precise and clear.

- **Sampling:** sampling from a set means choosing an element from that set. We often **draw** a sample at random from a given set in which each element of the set has equal chance of being chosen.
- **With or without replacement:** usually we draw multiple samples from a set. If we put each object back after each draw, we call this **sampling with replacement**. In this case a single object can be possibly chosen multiple times. For example, if  $A = \{a_1, a_2, a_3, a_4\}$  and we pick 3 elements with replacement, a possible choice might be  $(a_3, a_1, a_3)$ . Thus "with replacement" means "repetition is allowed." On the other hand, if repetition is not allowed, we call it **sampling without replacement**.
- **Ordered or unordered:** If ordering matters (i.e.:  $a_1, a_2, a_3 \neq a_2, a_3, a_1$ ), this is called **ordered sampling**. Otherwise, it is called **unordered**.

Thus when we talk about sampling from sets, we can talk about four possibilities.

- ordered sampling with replacement
- ordered sampling without replacement

- unordered sampling without replacement
- unordered sampling with replacement

We will discuss each of these in detail and indeed will provide a formula for each. The formulas will be summarized at the end in [Table 2.1](#). Nevertheless, the best approach here is to understand how to derive these formulas. You do not actually need to memorize them if you understand the way they are obtained.

---