

## 1 Countability Basics

Note 11

- (a) Is  $f : \mathbb{N} \rightarrow \mathbb{N}$ , defined by  $f(n) = n^2$ , an injection (one-to-one)? Briefly justify.
- (b) Is  $f : \mathbb{R} \rightarrow \mathbb{R}$ , defined by  $f(x) = x^3 + 1$ , a surjection (onto)? Briefly justify.
- (c) The Bernstein-Schroder theorem states that, if there exist injective functions  $f : A \rightarrow B$  and  $g : B \rightarrow A$  between the sets  $A$  and  $B$ , then a bijection exists between  $A$  and  $B$ . Use this to demonstrate that  $(0, 1)$  and  $\mathbb{R}_+ = (0, \infty)$  have the same cardinality by defining appropriate injections.

### Solution:

- (a) Yes. One way to illustrate is by drawing the one-to-one mapping from  $n$  to  $n^2$ . More formally we can show that the preimage is unique by showing that  $m \neq n \implies f(m) \neq f(n)$ .

*Alternative 1:* Suppose  $m \neq n$ . Then without loss of generality let  $m > n$ . This implies that  $f(m) = m^2 > n^2 = f(n)$  and hence  $f(m) \neq f(n)$ .

*Alternative 2:* We'll do a proof by contraposition.  $f(m) = f(n) \implies m = n$ .

$$f(m) = f(n) \implies m^2 = n^2 \implies m^2 - n^2 = 0 \implies (m - n)(m + n) = 0 \implies m = \pm n$$

Since  $n$  can't be negative, we have an injection.

- (b) Yes. For any  $y \in \mathbb{R}$ , there exists a corresponding value  $x \in \mathbb{R}$  such that  $y = f(x)$ . To see this take  $x = \sqrt[3]{y-1}$ .
- (c) The injection from  $(0, 1)$  to  $(0, \infty)$  is trivial; consider the function  $f : (0, 1) \rightarrow (0, \infty)$  given by

$$f(x) = x.$$

It is easy to see that  $f$  is injective.

For the other way, consider the function  $g : (0, \infty) \rightarrow (0, 1)$  given by

$$g(x) = \frac{1}{x+1}.$$

To see that  $g$  is injective, suppose  $g(x) = g(y)$ . Then

$$\frac{1}{x+1} = \frac{1}{y+1} \implies x = y.$$

Hence  $g$  is injective. Thus we have an injective function from  $(0, 1)$  to  $(0, \infty)$  and an injective function from  $(0, \infty)$  to  $(0, 1)$ . By the Bernstein-Schroder theorem there exists a bijection from  $(0, 1)$  to  $(0, \infty)$  and hence they have the same cardinality.

## 2 Unprogrammable Programs

Note 12

Prove whether the programs described below can exist or not.

- (a) A program  $P(F, x, y)$  that returns true if the program  $F$  outputs  $y$  when given  $x$  as input (i.e.  $F(x) = y$ ) and false otherwise.
- (b) A program  $P$  that takes two programs  $F$  and  $G$  as arguments, and returns true if  $F$  and  $G$  halt on the same set of inputs (or false otherwise).

### Solution:

- (a)  $P$  cannot exist, for otherwise we could solve the halting problem:

```
def halt(F, x):  
    def Q(x):  
        F(x)  
        return 0  
    return P(Q, x, 0)
```

Halt defines a subroutine  $Q$  that first simulates  $F$  and then returns 0, that is  $Q(x)$  returns 0 if  $F(x)$  halts, and nothing otherwise. Knowing the output of  $P(F, x, 0)$  thus tells us whether  $F(x)$  halts or not.

- (b) We solve the halting problem once more:

```
def Halt(F, x):  
    def Q(y):  
        loop  
    def R(y):  
        if y == x:  
            F(x)  
        else:  
            loop  
    return not P(Q, R)
```

$Q$  is a subroutine that loops forever on all inputs.  $R$  is a subroutine that loops forever on every input except  $x$ , and runs  $F(x)$  on input  $x$  when handed  $x$  as an argument.

Knowing if  $Q$  and  $R$  halt on the same inputs boils down to knowing whether  $F$  halts on  $x$  (since that is the only case in which they could possibly differ). Thus, if  $P(Q, R)$  returns “True”, then we know they behave the same on all inputs and  $F$  must not halt on  $x$ , so we return `not P(Q, R)`.

### 3 Fixed Points

Note 12

Consider the problem of determining if a program  $P$  has any fixed points. Given any program  $P$ , a fixed point is an input  $x$  such that  $P(x)$  outputs  $x$ .

- (a) Prove that the problem of determining whether a program has a fixed point is uncomputable.
- (b) Consider the problem of outputting a fixed point of a program if it has one, and outputting "Null" otherwise. Prove that this problem is uncomputable.
- (c) Consider the problem of outputting a fixed point of a program  $F$  if the fixed point exists *and* is a natural number, and outputting "Null" otherwise. If an input is a natural number, then it has no leading zero before its most significant bit.

Show that if this problem can be solved, then the problem in part (b) can be solved. What does this say about the computability of this problem? (You may assume that the set of all possible inputs to a program is countable, as is the case on your computer.)

#### Solution:

- (a) We can prove this by reducing from the Halting Problem. Suppose we had some program `FixedPoint(F)` that solved the fixed-point problem. We can define `TestHalt(F, x)` as follows:

```
def TestHalt(F, x):  
    def F'(y):  
        F(x)  
        return y  
    return FixedPoint(F_prime)
```

If  $F(x)$  halts, we have that  $F'(y)$  will always just return  $y$ , so every input is a fixed point. On the other hand, if  $F(x)$  does not halt,  $F'$  won't return anything for any input  $y$ , so there can't be any fixed points. Thus, our definition of `TestHalt` must always work, which is a contradiction; this tells us that `FixedPoint` cannot exist.

- (b) If this problem is solvable then the problem in part (a) is solvable, as we can output "no" to whether  $F$  has a fixed point if the program in part (b) returns "Null" and "yes" otherwise.
- (c) The intuition is that there is a bijection between the set of all inputs and  $\mathbb{N}$  so we can reduce the problem in part (b) to this problem. In particular, since the set of all inputs is countably infinite, there exists a bijective function  $g$  that maps a natural number  $n$  to a unique input string  $g(n)$ . Also, we can extend the definition of  $g$  slightly so that  $g(\text{"Null"}) = \text{"Null"}$  so that it is still a bijection.

Consider the following program:

```
def FindFixedPoint(F):  
    def F'(n):
```

```

    if n not in N:
        error
    x = g(n)
    if F(x) = x:
        return n
    else:
        return n+1
return g(FindFixedPointInN(F'))

```

Since  $g$  is a bijection,  $g^{-1}$  exists, and if  $g(n) = x$ , then  $n = g^{-1}(x)$ . If there is some  $x$  such that  $F(x) = x$ , then  $n = g^{-1}(x)$  will be a fixed point for  $F'$ . Thus, if  $F$  has a fixed point,  $\text{FindFixedPointInN}(F')$  will return some  $n$  where  $g(n)$  is a fixed point for  $F$ .

On the other hand, if  $F(x) \neq x$  for every input  $x$ , then  $F'(n) = n + 1 \neq n$  for every  $n$ , which means  $F'$  will also not have a fixed point. Thus, our program solves the problem in part (b), which is already shown to be uncomputable. This means that this problem is also uncomputable.

## 4 Probability Warm-Up

Note 13

- Suppose that we have a bucket of 30 green balls and 70 orange balls. If we pick 15 balls uniformly out of the bucket, what is the probability of getting exactly  $k$  green balls (assuming  $0 \leq k \leq 15$ ) if the sampling is done **with** replacement, i.e. after we take a ball out the bucket we return the ball back to the bucket for the next round?
- Same as part (a), but the sampling is **without** replacement, i.e. after we take a ball out the bucket we **do not** return the ball back to the bucket.
- If we roll a regular, 6-sided die 5 times. What is the probability that at least one value is observed more than once?

### Solution:

- Let  $A$  be the event of getting exactly  $k$  green balls. Then treating all balls as distinguishable, we have a total of  $100^{15}$  possibilities to draw a sequence of 15 balls. In order for this sequence to have exactly  $k$  green balls, we need to first assign them one of  $\binom{15}{k}$  possible locations within the sequence. Once done so, we have  $30^k$  ways of actually choosing the green balls, and  $70^{15-k}$  possibilities for choosing the orange balls. Thus in total we arrive at

$$\mathbb{P}[A] = \frac{\binom{15}{k} \cdot 30^k \cdot 70^{15-k}}{100^{15}} = \binom{15}{k} \left(\frac{3}{10}\right)^k \left(\frac{7}{10}\right)^{15-k}.$$

- Using a similar approach, there are a total of  $100 \cdot 99 \cdots 86 = \frac{100!}{(100-15)!} = \frac{100!}{85!}$  ways to grab 15 balls.

We still want  $k$  green balls and  $15 - k$  orange balls, which we can select in

$$\begin{aligned} & \binom{15}{k} \cdot (30 \cdot 29 \cdots (30 - (k - 1))) \cdot (70 \cdot 69 \cdots (70 - (15 - k - 1))) \\ &= \binom{15}{k} \frac{30!}{(30 - k)!} \cdot \frac{70!}{(70 - (15 - k))!} \end{aligned}$$

ways. Here, we have  $\binom{15}{k}$  possible locations for the  $k$  green balls, and we use permutations rather than combinations to account for the fact that we are picking balls without replacement.

Since our sample space is uniform, the probability is thus

$$\mathbb{P}[A] = \frac{\binom{15}{k} \frac{30!}{(30 - k)!} \cdot \frac{70!}{(70 - (15 - k))!}}{\frac{100!}{(100 - 15)!}} = \frac{\binom{15}{k} \frac{30!}{(30 - k)!} \cdot \frac{70!}{(55 + k)!}}{\frac{100!}{85!}}.$$

*Alternative Solution:* Instead of considering a probability space where each ball is distinct, we can also consider a probability space where each ball is indistinguishable, and order does not matter. Intuitively, this is equivalent to the previous solution, since the numerator and denominator are accounting for order in the exact same way; considering the same situation without order and with indistinguishable balls is equivalent to dividing both the numerator and denominator by  $15!$  for the number of arrangements of the 15 balls we select.

With this in mind, we note that the size of the sample space is now  $\binom{100}{15}$ , since we are choosing 15 balls out of a total of 100. To find  $|A|$ , we need to be able to find out how many ways we can choose  $k$  green balls and  $15 - k$  orange balls. This means that we have  $|A| = \binom{30}{k} \binom{70}{15 - k}$ , since we must select  $k$  green balls out of 30 total, and  $15 - k$  orange balls out of 70 total.

Putting this together, we have

$$\mathbb{P}[A] = \frac{\binom{30}{k} \binom{70}{15 - k}}{\binom{100}{15}}.$$

- (c) Let  $B$  be the event that at least one value is observed more than once. We see that  $\mathbb{P}[B] = 1 - \mathbb{P}[\overline{B}]$ . So we need to find out the probability that the values of the 5 rolls are distinct. We see that  $\mathbb{P}[\overline{B}]$  is simply the number of ways to choose 5 numbers (order matters) divided by the sample space (which is  $6^5$ ). So

$$\mathbb{P}[\overline{B}] = \frac{6!}{6^5} = \frac{5!}{6^4}.$$

And

$$\mathbb{P}[B] = 1 - \frac{5!}{6^4}.$$

## 5 Five Up

### Note 13

Say you toss a coin five times, and record the outcomes. For the three questions below, you can assume that order matters in the outcome, and that the probability of heads is some  $p$  in  $0 < p < 1$ , but *not* that the coin is fair ( $p = 0.5$ ).

- (a) What is the size of the sample space,  $|\Omega|$ ?
- (b) How many elements of  $\Omega$  have exactly three heads?
- (c) How many elements of  $\Omega$  have three or more heads?

For the next three questions, you can assume that the coin is fair (i.e. heads comes up with  $p = 0.5$ , and tails otherwise).

- (d) What is the probability that you will observe the sequence HHHTT? What about HHHHT?
- (e) What is the probability of observing at least one head?
- (f) What is the probability you will observe more heads than tails?

For the final three questions, you can instead assume the coin is biased so that it comes up heads with probability  $p = \frac{2}{3}$ .

- (g) What is the probability of observing the outcome HHHTT? What about HHHHT?
- (h) What about the probability of at least one head?
- (i) What is the probability you will observe more heads than tails?

### **Solution:**

- (a) Since for each coin toss, we can have either heads or tails, we have  $2^5$  total possible outcomes.
- (b) Since we know that we have exactly 3 heads, what distinguishes the outcomes is at which point these heads occurred. There are 5 possible places for the heads to occur, and we need to choose 3 of them, giving us the following result:  $\binom{5}{3}$ .
- (c) We can use the same approach from part (b), but since we are asking for 3 or more, we need to consider the cases of exactly 4 heads, and exactly 5 heads as well. This gives us the result as:  $\binom{5}{3} + \binom{5}{4} + \binom{5}{5} = 16$ .

To see why the number is exactly half of the total number of outcomes, denote the set of outcomes that has 3 or more heads as  $A$ . If we flip over every coin in each outcome in set  $A$ , we get all the outcomes that have 2 or fewer heads. Denote the new set  $\bar{A}$ . Then we know that  $A$  and  $\bar{A}$  have the same size and they together cover the whole sample space. Therefore,  $|A| = |\bar{A}|$  and  $|A| + |\bar{A}| = 2^5$ , which gives  $|A| = 2^5/2$ .

- (d) Since each coin toss is an independent event, the probability of each of the coin tosses is  $\frac{1}{2}$  making the probability of this outcome  $\frac{1}{2^5}$ . This holds for both cases since both heads and tails have the same probability.

- (e) We will use the complementary event, which is the event of getting no heads. The probability of getting no heads is the probability of getting all tails. This event has a probability of  $\frac{1}{2^5}$  by a similar argument to the previous part. Since we are asking for the probability of getting at least one heads, our final result is:  $1 - \frac{1}{2^5}$ .
- (f) To have more heads than tails is to claim that we flip at least 3 heads. Since each outcome in this probability space is equally likely, we can divide the number of outcomes where there are 3 or more heads by the total number of outcomes to give us:  $\frac{\binom{5}{3} + \binom{5}{4} + \binom{5}{5}}{2^5} = \frac{1}{2}$

Alternatively, we see that for every sequence with more heads than tails we can create a corresponding sequence with more tails than heads by “flipping” the bits. For example, a sequence HTHHT which has more heads than tails corresponds to a flipped sequence THTTH which has more tails than heads. As a result, for every sequence with more heads there’s a sequence with more tails. Thus, the probability of having a sequence with more heads is  $1/2$ .

- (g) By using the same idea of independence we get for HHHTT:

$$\frac{2}{3} \times \frac{2}{3} \times \frac{2}{3} \times \frac{1}{3} \times \frac{1}{3} = \frac{2^3}{3^5}$$

For HHHHT, we get:

$$\frac{2}{3} \times \frac{2}{3} \times \frac{2}{3} \times \frac{2}{3} \times \frac{1}{3} = \frac{2^4}{3^5}$$

- (h) Similar to the unbiased case, we will first find the probability of the complement event, which is having no heads. The probability of this is  $\frac{1}{3^5}$ , which makes our final result  $1 - \frac{1}{3^5}$ .
- (i) In this case, since we are working in a nonuniform probability space (getting 4 heads and 3 heads don’t have the same probability), we need to separately consider the events with different numbers of heads to find our result. Thus for each  $3 \leq i \leq 5$ , we need to count the total number of outcomes with exactly  $i$  heads and multiply it by the probability of achieving any of those outcomes. This yields:

$$\begin{aligned} \mathbb{P}[\geq 3 \text{ Heads}] &= \binom{5}{3} \left(\frac{2}{3}\right)^3 \left(\frac{1}{3}\right)^2 + \binom{5}{4} \left(\frac{2}{3}\right)^4 \left(\frac{1}{3}\right)^1 + \binom{5}{5} \left(\frac{2}{3}\right)^5 \left(\frac{1}{3}\right)^0 \\ &= \binom{5}{3} \left(\frac{2}{3}\right)^3 \left(\frac{1}{3}\right)^2 + \binom{5}{4} \left(\frac{2}{3}\right)^4 \left(\frac{1}{3}\right)^1 + \binom{5}{5} \left(\frac{2}{3}\right)^5. \end{aligned}$$