AI 5030: PROBABILITY AND STOCHASTIC PROCESSES
HOMEWORK 1: SOLUTIONS

भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

1 Functions, Cardinality, Countability

1. Show that $2^{\mathbb{N}}$ is uncountable; here, $2^{\mathbb{N}}$ denotes the power set of $\mathbb{N}$.
Hint: Construct a bijection between $\{0,1\}^{\mathbb{N}}$ and $2^{\mathbb{N}}$, and use the fact from class that $\{0,1\}^{\mathbb{N}}$ is uncountable.

Solution: To show that $2^{\mathbb{N}}$ is uncountable, we first construct a bijection between $\{0,1\}^{\mathbb{N}}$ and $2^{\mathbb{N}}$.

The idea is to create a function which maps a binary string to a particular subset of the natural numbers. Intuitively, we store the positions at which the binary string has ones, and those and only those positions are part of the subset. For example:- $101\bar{0} = \{1,3\}$; here, $\bar{0}$ denotes a non-terminating string of zeros.

Consider the function $f : \{0,1\}^{\mathbb{N}} \to 2^{\mathbb{N}}$ defined by $f((a_n)_{n\in\mathbb{N}}) = \{n \in \mathbb{N} : a_n = 1\}$.

- *Injective:* Suppose $f((a_n)_{n\in\mathbb{N}}) = f((b_n)_{n\in\mathbb{N}})$. Then $\{n \in \mathbb{N} : a_n = 1\} = \{n \in \mathbb{N} : b_n = 1\}$, implying $a_n = b_n$ for all $n \in \mathbb{N}$. Thus, $(a_n)_{n\in\mathbb{N}} = (b_n)_{n\in\mathbb{N}}$.
- *Surjective:* For any subset $S \subseteq \mathbb{N}$, define $a_n = 1$ if $n \in S$ and $a_n = 0$ otherwise. Then $f((a_n)_{n\in\mathbb{N}}) = S$.

Thus, f is bijective. Because $\{0,1\}^{\mathbb{N}}$ is uncountable (proved in class), it follows that $2^{\mathbb{N}}$ is uncountable.

2. Show that $\mathbb{N}^2 := \mathbb{N} \times \mathbb{N} = \{(m,n) : m,n \in \mathbb{N}\}$ is countably infinite.
Using the principle of mathematical induction, show that $\mathbb{N}^d$ is countably infinite for each $d \in \mathbb{N}$.

Solution: We begin by constructing a bijection $f : \mathbb{N}^2 \to \mathbb{N}$ is bijective.

Consider the function
$$f(m,n) = \frac{(m+n-2)\times(m+n-1)}{2} + n, \quad m,n \in \mathbb{N}.$$

Injective:

To show that f as defined above is injective, suppose that $f(m,n) = f(p,q)$ for some $(m,n),(p,q) \in \mathbb{N}^2$. Assume that $(m,n) \neq (p,q)$, and without loss of generality, let $m+n < p+q$. Let $a := m+n-2$ and $d := (p+q-2) - (m+n-2)$. Clearly, $d \geq 1$. Also, we have

$$\begin{aligned} & f(m,n) = f(p,q) \\ \implies \ & \frac{a\times(a+1)}{2} + n = \frac{(a+d)\times(d+a+1)}{2} + q \\ \implies \ & n - q = ad + \frac{d\times(d+1)}{2} \\ \implies \ & n - q \geq a+1 \qquad\qquad (\because d \geq 1) \end{aligned} \tag{1}$$

The last line above implies that $n \geq q+a+1 = q+m+n-1 > n$, thereby contradicting the assumption that $f(m,n) = f(p,q)$. Therefore, it follows that $f(m,n) = f(p,q)$, which in turn implies $n = q$ and $m = p$, thereby proving that the function f is injective.

Surjective: Here, we need to show that $\forall y \in$ codomain of f, $\exists x \in$ domain of f such that $f(x) = y$. Below, we argue that $f^{-1}(y) = \{x\}$ for all $y \in$ codomain(f). Let $z = f(m,n) = \frac{(m+n-2)\times(m+n-1)}{2} + n$, and let

$$\begin{aligned} w &:= m+n-2, \\ t &:= \frac{w\times(w+1)}{2} \qquad\qquad (\therefore t \geq 0) \\ z &= t+n. \end{aligned}$$

Clearly, $w, t \geq 0$. The idea is to write each unique w as a function of unique z, then we can associate each z to unique m and n. Notice that $2t^2 = w \times (w+1) \Rightarrow w = \frac{-1+\sqrt{1+8t}}{2}$. and,

$$\begin{aligned} t &< z \\ t &\leq z - 1 && (\because n, z \in \mathbb{N}) \\ w &\leq \frac{-1 + \sqrt{1 + 8(z-1)}}{2} \end{aligned}$$

Then,

$$\begin{aligned} t \leq z - 1 &= t + n - 1 \\ &< t + m + n - 1 && (\because m \in \mathbb{N}) \\ &< \frac{w \times (w+1)}{2} + m + n - 1 \\ &< \frac{w \times (w+1)}{2} + w + 1 \\ 2(z-1) &< (w+1)^2 + (w+1) \\ (w+1) &> \frac{-1 + \sqrt{1 + 8(z-1)}}{2} \end{aligned}$$

Therefore, $w \leq \frac{-1+\sqrt{1+8(z-1)}}{2} < (w+1)$. Hence, $w = \lfloor \frac{-1+\sqrt{1+8(z-1)}}{2} \rfloor$. For $\forall z \in \mathbb{N}$, we get unique w and from that unique t, and then consequently unique m and n.
Thus, the above defined function $f : \mathbb{N}^2 \to \mathbb{N}$ is invertible and hence bijective. This establishes that $\mathbb{N}^2$ is countably infinite.

Assume, now, that $\mathbb{N}^d$ countably infinite, and therefore bijective with $\mathbb{N}$, for some finite $d \in \mathbb{N}$. Then,

$$\begin{aligned} |\mathbb{N}^{d+1}| &= |\mathbb{N}^d \times \mathbb{N}| \\ &= |\mathbb{N} \times \mathbb{N}| \\ &= |\mathbb{N}|. \end{aligned}$$

Thus, by using principle of mathematical induction, it follows that $\mathbb{N}^d$ is countably infinite for each $d \in \mathbb{N}$.

3. Show that $\mathbb{N}^{\mathbb{N}} := \underbrace{\mathbb{N} \times \mathbb{N} \times \cdots}_{\text{countably infinitely many cartesian products}}$ is uncountable. (Hint: Construct an injection from $\{0,1\}^{\mathbb{N}}$ to $\mathbb{N}^{\mathbb{N}}$.)

   Solution: We aim to show that $\mathbb{N}^{\mathbb{N}}$ is uncountable by constructing an injection from the uncountable set $\{0,1\}^{\mathbb{N}}$ to $\mathbb{N}^{\mathbb{N}}$.

   Define $f : \{0,1\}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$ by $f((a_n)_{n\in\mathbb{N}}) = (b_n)_{n\in\mathbb{N}}$, where

   $$b_n = \begin{cases} 2^n, & \text{if } a_n = 1, \\ 0, & \text{if } a_n = 0. \end{cases}$$

   - *Injective:* Suppose $f((a_n)_{n\in\mathbb{N}}) = f((c_n)_{n\in\mathbb{N}})$ and $f((c_n)_{n\in\mathbb{N}}) = (d_n)_{n\in\mathbb{N}}$. Then for all $n \in \mathbb{N}$, $b_n = d_n$, implying $a_n = c_n$. Thus, $(a_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}}$.
     Since f is injective and $\{0,1\}^{\mathbb{N}}$ is uncountable, it follows that $\mathbb{N}^{\mathbb{N}}$ is uncountable.

4. Show that for any set A (finite, countably infinite, or uncountable), $|2^A| > |A|$, where 2^A is the power set of A.
   Note: This result demonstrates that there are different levels of infinity. Thus, for instance,

   $$|\mathbb{N}| < |2^{\mathbb{N}}| = |\mathbb{R}| < |2^{\mathbb{R}}| < |2^{2^{\mathbb{R}}}| \cdots$$

   Solution: Clearly, $|2^A| \geq |A|$ (because the mapping $a \mapsto \{a\}$ for each $a \in A$ is an injection from A to 2^A). Suppose now that $|2^A| = |A|$. This implies that there exists a bijective function $f : A \to 2^A$. Consider the set $B = \{x \in A : x \notin f(x)\}$. Since f is surjective, there exists some $a \in A$ such that $f(a) = B$.

- If $a \in B$, then $a \notin f(a) = B$, a contradiction.
- If $a \notin B$, then $a \in f(a) = B$, a contradiction.

Therefore, no such surjection f exists, and we must have $|2^A| > |A|$. The idea used here is a common idea in mathematical logic. The Solution of the undecidability of the halting problem is an excellent example of this.

5. Fix a countable set A.

   (a) For any $n \in \mathbb{N}$, let B_n denote the collection of all possible n-tuples of the form $(a_1, a_2, \ldots, a_n)$, where $a_k \in A$ for each $k \in \{1, 2, \ldots, n\}$. Show that B_n is countable.
   Hence argue that $\bigcup_{n \in \mathbb{N}} B_n$ is countable.

   (b) A real number $x_0 \in \mathbb{R}$ is called *algebraic* if it is a root of a polynomial with integer coefficients. For example, $x_0 = \sqrt{2}$ is an algebraic number, as it is a root of the polynomial $x^2 - 2 = 0$ (whose coefficients are $1, -2$).
   Using the result in part (a) above, show that the set of all algebraic numbers is countable.
   Hint: Show that the there are only countably many polynomials with integer coefficients.

   Solution:

   (a) Notice that $B_n = A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ times}}$. If $|A| < \infty$, then $|B_n| = |A|^n < \infty$. If A is countably infinite, then following the lines of the proof of countability of $\mathbb{N}^d$ (Question 2), it follows that B_n is countably infinite. We have thus proved that B_n is countable for every $n \in \mathbb{N}$. Using the fact that a countable union of countable sets is countable, we may conclude that $\bigcup_{n \in \mathbb{N}} B_n$ is countable.

   (b) Notice that a polynomial f of degree $d \in \mathbb{N} \cup \{0\}$ with integer coefficients may be expressed as

   $$f(x) = a_0 + a_1\, x + a_2\, x^2 + \ldots + a_d\, x^d, \quad x \in \mathbb{R},$$

   where $a_i \in \mathbb{Z}$ for all $i \in \{1, \ldots, d\}$, $a_d \neq 0$. The above polynomial admits at most d real roots, and may be associated uniquely with the tuple $(a_0, \ldots, a_d) \in \mathbb{Z}^d$. Hence, it follows that the set of all polynomials with degree 0 is equivalent to the set $\mathbb{Z}$, the set of all polynomials of degree 1 is equivalent to $\mathbb{Z}^2$, the set of all polynomials of degree 2 is equivalent to $\mathbb{Z}^3$, and so on. Noting that $\mathbb{Z}^d$ is countably infinite for every $d \in \mathbb{N} \cup \{0\}$, it follows that

   $$\text{set of all polynomials with integer coefficients} \equiv \bigcup_{d=1}^{\infty} \mathbb{Z}^d.$$

   Using the fact that a countable union of countable sets is countable, we have that the set of all polynomials with integer coefficients is countably infinite.
   From this, it follows that the collection of all algebraic numbers is countably infinite.

6. Let $\mathscr{C}$ denote the collection of all finite length binary strings. Is $\mathscr{C}$ countable?

   Solution: Let C_n denote the collection of all binary strings of length n, for each $n \in \mathbb{N}$. Then, we have

   $$\mathscr{C} = \{0, 1, 00, 01, 10, 11, \ldots\} = \bigcup_{n=1}^{\infty} C_n.$$

   Noting that C_n is finite (hence countable) for each n, and using the fact that a countable union of countable sets is countable, we get that $\mathscr{C}$ is countable.