AI5030 / EE5817: PROBABILITY AND STOCHASTIC PROCESSES
HOMEWORK 01 - SOLUTIONS

FUNCTIONS, COUNTABLE SETS, UNCOUNTABLE SETS

Solutions Prepared By: Yashmitha Gogineni

1. **Cantor's pairing function and countability of finite cartesian products**

Let $\mathbb{W}$ denote the set of whole numbers, i.e., $\mathbb{W} = \mathbb{N} \cup \{0\}$. Consider the following depiction of the elements of the set $\mathbb{W} \times \mathbb{W}$ in which the rows are indexed by $m \in \mathbb{W}$, columns are indexed by $n \in \mathbb{W}$, and all pairs of whole numbers (m, n) with a constant value of $m + n$ have been colored identical (these pairs constitute the "diagonals" in the picture extending from bottom left to top right). For any $k \in \mathbb{W}$, let

$$D_k := \{(m, n) \in \mathbb{W} \times \mathbb{W} \,:\, m + n = k\}$$

denote the kth diagonal.

$$\begin{array}{ccccccccc}
(0,0) & (0,1) & (0,2) & (0,3) & (0,4) & (0,5) & (0,6) & (0,7) & \cdots \\
(1,0) & (1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) & (1,7) & \cdots \\
(2,0) & (2,1) & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) & (2,7) & \cdots \\
(3,0) & (3,1) & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) & (3,7) & \cdots \\
(4,0) & (4,1) & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) & (4,7) & \cdots \\
(5,0) & (5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) & (5,7) & \cdots \\
(6,0) & (6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6) & (6,7) & \cdots \\
(7,0) & (7,1) & (7,2) & (7,3) & (7,4) & (7,5) & (7,6) & (7,7) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

(a) If T_k denotes the number of pairs present on or to the left of the $(k-1)$th diagonal, show that $T_k = \frac{k(k+1)}{2}$.
Solution: For each diagonal D_j (with $j \geq 0$) the pairs are

$$D_j = \{(0, j), (1, j-1), \ldots, (j, 0)\},$$

so $|D_j| = j + 1$. The number of pairs on or to the left of the $(k-1)$th diagonal is therefore

$$T_k = \sum_{j=0}^{k-1} |D_j| = \sum_{j=0}^{k-1} (j+1) \overset{j+1=i}{=} \sum_{i=1}^{k} i = \frac{k(k+1)}{2},$$

as required.

(b) Let $(0, 0)$ be assigned index 0, $(1, 0)$ be assigned index 1, $(0, 1)$ be assigned index 2, $(2, 0)$ be assigned index 3, $(1, 1)$ be assigned index 4, and so on. Show that the index of (m, n) is given by $\frac{(m+n)(m+n+1)}{2} + n$.
Hint: Use the expression for T_k derived in part (a).

Solution: The diagonal containing (m, n) is the one with sum $s = m + n$. By part (a), there are $T_s = \dfrac{s(s+1)}{2}$ pairs strictly to the left of that diagonal (sth diagonal D_s) (same as saying that T_s pairs lie on or to the left of the $(s-1)$th diagonal D_{s-1}).
On the diagonal D_s we index pairs in order of increasing n (equivalently decreasing m): the first on that diagonal is $(s, 0)$ with offset 0, the second is $(s-1, 1)$ with offset 1, and in general (m, n) is the $n+1$-th element on D_s with offset n.
Hence, by adding this offset n to T_s, we get the index (starting from 0) of (m, n) as

$$T_s + n \overset{s=m+n}{=} \frac{(m+n)(m+n+1)}{2} + n,$$

proving the formula.

(c) Let $f : \mathbb{W} \times \mathbb{W} \to \mathbb{W}$ denote the index assignment function of part (b), i.e.,

$$f(m,n) = \frac{(m+n)(m+n+1)}{2} + n, \qquad (m,n) \in \mathbb{W} \times \mathbb{W}.$$

The function f as defined above is called *Cantor's pairing function*. Show that f is bijective, and conclude that $\mathbb{W} \times \mathbb{W}$ is countably infinite.

Injectivity. Let $(m,n), (m',n') \in \mathbb{W} \times \mathbb{W}$ and assume for contradiction that

$$f(m,n) = f(m',n'), \quad \text{but } (m,n) \neq (m',n')$$

Write $s = m+n$ and $s' = m'+n'$. Then from (1),

$$\frac{s(s+1)}{2} + n = \frac{s'(s'+1)}{2} + n'$$

Rearranging gives

$$\frac{s'(s'+1)}{2} - \frac{s(s+1)}{2} = n - n' \tag{1}$$

Case 1. Suppose $s < s'$. That is, $s' \geq s+1$. Then,

$$\frac{s'(s'+1)}{2} - \frac{s(s+1)}{2} = T_{s'} - T_s \;\geq\; T_{s+1} - T_s = s+1.$$

Thus the left-hand side of (1) satisfies

$$\text{LHS } \geq s+1 > s. \tag{2}$$

On the other hand, from $0 \leq n \leq s$ and $0 \leq n' \leq s'$, we have

$$n - n' \leq n \leq s,$$

so the right-hand side of (1) satisfies

$$\text{RHS } \leq s. \tag{3}$$

Combining (2) and (3), we obtain

$$\text{LHS} \geq s+1 > s \geq \text{RHS},$$

contradicting (1).

Case 2. If $s' < s$, the same argument (with the roles of s and s' reversed) leads to a contradiction.

Therefore, the only possibility is

$$s = s'.$$

Plugging this into (1) gives $n = n'$, and then $m = m'$. This contradicts the original assumption $(m,n) \neq (m',n')$. Therefore, if

$$f(m,n) = f(m',n') \quad \text{then, } (m,n) = (m',n')$$

Hence, f is injective.

Surjectivity. Constructive Proof.

Let $t \in \mathbb{W}$ be arbitrary. We will construct $(m,n) \in \mathbb{W} \times \mathbb{W}$ with $f(m,n) = t$ by repeatedly subtracting whole diagonals until the remainder fits the next diagonal.

Construction. Set $s := 0$ and $r := t$. While $r \geq s+1$ perform the update

$$r := r - (s+1), \qquad s := s+1.$$

When the process terminates we have $0 \leq r \leq s$. Define

$$n := r, \qquad m := s - n.$$

Verification. By construction $0 \le n \le s$, hence $m = s - n \ge 0$ and $(m, n) \in \mathbb{W} \times \mathbb{W}$. The amount subtracted during the loop equals

$$1 + 2 + \cdots + s = \frac{s(s+1)}{2},$$

and the final remainder equals $r = n$. Therefore

$$t = \frac{s(s+1)}{2} + n = f(m, n).$$

Thus the constructed pair (m, n) maps to t.

Termination and uniqueness. The loop must terminate because the running remainder r strictly decreases at each step (we subtract a positive integer at every iteration) and cannot stay $\ge s+1$ indefinitely. Uniqueness of the resulting s and n follows from the fact that for each t, the corresponding representation is always only one of the following, after determining s:

$$\left\{\frac{s(s+1)}{2} + 0,\ \frac{s(s+1)}{2} + 1,\ \ldots,\ \frac{s(s+1)}{2} + s\right\} \quad (s = 0, 1, 2, \ldots),$$

so there is exactly one representation of t as $\dfrac{s(s+1)}{2} + n$ with $0 \le n \le s$.

Example. Let $t = 25$.

- Start with $s = 0, r = 25$.
- Subtract 1: $r = 24, s = 1$.
- Subtract 2: $r = 22, s = 2$.
- Subtract 3: $r = 19, s = 3$.
- Subtract 4: $r = 15, s = 4$.
- Subtract 5: $r = 10, s = 5$.
- Subtract 6: $r = 4, s = 6$ and stop since $r = 4 < s + 1 = 7$.

We have $n = r = 4$ and $m = s - n = 6 - 4 = 2$. Check:

$$f(m, n) = \frac{(m+n)(m+n+1)}{2} + n = \frac{(2+4)(2+4+1)}{2} + 4 = \frac{6 \cdot 7}{2} + 4 = 21 + 4 = 25.$$

Hence $t = 25$ corresponds to the pair $(m, n) = (2, 4)$.
Since t was arbitrary, every $t \in \mathbb{W}$ has a preimage under f. Therefore f is surjective.

Note: Let A be a countable set (finite or countably infinite), and let F be a finite set. Then $A \cup F$ is finite if and only if A is finite. Likewise, $A \setminus F$ is finite if and only if A is finite.
Proof Sketch (Refer to Appendix for Proof):

- If A is finite set of size n, then $A \cup F$ has size $n + k$ (finite), and $A \setminus F$ has size at most n (finite).
- If A is countably infinite, let $f : \mathbb{N} \to A$ be a bijection.
  - For $A \cup F$, list the elements of F first, then continue with f shifted. This yields a bijection $\mathbb{N} \to A \cup F$.
  - For $A \setminus F$, skip the finitely many values of f that land in F, leaving a bijection $\mathbb{N} \to A \setminus F$.

Thus in both cases, the cardinality is unchanged.
Since, $\mathbb{W} = \mathbb{N} \cup \{0\}$ and $\mathbb{N}$ is countably infinite, $\mathbb{W}$ is countably infinite.
Combining injectivity and surjectivity, f is a bijection $\mathbb{W} \times \mathbb{W} \to \mathbb{W}$, so $\mathbb{W} \times \mathbb{W}$ is countably infinite.

(d) Using the principle of mathematical induction, show that $\mathbb{W} \underbrace{\times \cdots \times}_{d \text{ times}} \mathbb{W}$ is countably infinite for every $d \in \mathbb{N}$.

Solution: Proceed by induction on d.

Base case. For $d = 1$, $\mathbb{W}^1 = \mathbb{W}$ is countably infinite.

Inductive step. Assume $\mathbb{W}^d$ is countably infinite for some $d \geq 1$. Then

$$\mathbb{W}^{d+1} = \mathbb{W}^d \times \mathbb{W} = \bigcup_{w \in \mathbb{W}} \left(\mathbb{W}^d \times \{w\}\right).$$

For each fixed $w \in \mathbb{W}$, the set $\mathbb{W}^d \times \{w\}$ has the same cardinality as $\mathbb{W}^d$, since appending the coordinate w to each element of $\mathbb{W}^d$ gives a bijection between $\mathbb{W}^d$ and $\mathbb{W}^d \times \{w\}$. By the inductive hypothesis $\mathbb{W}^d$ is countable, hence each $\mathbb{W}^d \times \{w\}$ is countable.
$\mathbb{W}^{d+1}$ is a countable union of countable sets, and is therefore countable (proved in class). Moreover, as each $\mathbb{W}^d \times \{w\}$ is countably infinite, $\mathbb{W}^{d+1}$ is countably infinite. This completes the induction.

Alternative.
By the inductive hypothesis, there exists a bijection $\phi : \mathbb{W}^d \to \mathbb{W}$. Using the identity map id : $\mathbb{W} \to \mathbb{W}$ and Cantor's pairing function $f : \mathbb{W} \times \mathbb{W} \to \mathbb{W}$, we have

$$\mathbb{W}^{d+1} = \mathbb{W}^d \times \mathbb{W} \xrightarrow{\phi \times \mathrm{id}} \mathbb{W} \times \mathbb{W} \xrightarrow{f} \mathbb{W}.$$

Note: Proof of bijectivity of cartesian product of two bijections.
Injectivity. Suppose $(\varphi \times \psi)(a_1, c_1) = (\varphi \times \psi)(a_2, c_2)$. Then

$$(\varphi(a_1), \psi(c_1)) = (\varphi(a_2), \psi(c_2)).$$

By equality of ordered pairs we have $\varphi(a_1) = \varphi(a_2)$ and $\psi(c_1) = \psi(c_2)$. Since φ and ψ are injective, $a_1 = a_2$ and $c_1 = c_2$. Hence $(a_1, c_1) = (a_2, c_2)$ and $\varphi \times \psi$ is injective.
Surjectivity. Let $(b, d) \in B \times D$ be arbitrary. Since φ and ψ are surjective, there exist $a \in A$ and $c \in C$ with $\varphi(a) = b$ and $\psi(c) = d$. Then $(\varphi \times \psi)(a, c) = (b, d)$, so every element of $B \times D$ has a preimage. Thus $\varphi \times \psi$ is surjective.
Combining injectivity and surjectivity, $\varphi \times \psi$ is bijective.

Since $\phi \times$ id and f are both bijections, their composition is a bijection from $\mathbb{W}^{d+1}$ to $\mathbb{W}$(refer to Q3).
Hence $\mathbb{W}^{d+1}$ is countably infinite.

2. **Countably infinite cartesian products of countable sets is uncountable**

In this exercise, we will show that the countably infinite cartesian product of natural numbers, $\mathbb{N}^{\mathbb{N}} := \mathbb{N} \times \mathbb{N} \times \cdots$, is uncountable and has cardinality $\aleph_1$ (aleph$_1$).
For this exercise, we use the fact from class that $|\{0, 1\}^{\mathbb{N}}| = \aleph_1$.

(a) Construct an injective map from $\{0, 1\}^{\mathbb{N}}$ to $\mathbb{N}^{\mathbb{N}}$. Prove formally that the constructed map is an injection, and hence conclude that $|\mathbb{N}^{\mathbb{N}}| \geq \aleph_1$.
Solution: Let $b := b_1 b_2 b_3 \cdots$ denote an arbitrary element of $\{0, 1\}^{\mathbb{N}}$, so each $b_i \in \{0, 1\}$. Define a map $f : \{0, 1\}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$ by

$$f(b_1 b_2 b_3 \cdots) := c_1 c_2 c_3 \cdots, \qquad \text{where} \qquad c_i := \begin{cases} 1, & b_i = 1, \\ 2, & b_i = 0. \end{cases}$$

(Any fixed distinct naturals may be used in place of 1 and 2.)
For each binary sequence $b = b_1 b_2 \cdots$ we have $c_i \in \{1, 2\} \subset \mathbb{N}$, hence $(c_i)_{i \geq 1} \in \mathbb{N}^{\mathbb{N}}$. Thus f is well-defined.
Injectivity of f.
For the sake of contradiction, for some $b, b' \in \{0, 1\}^{\mathbb{N}}$, suppose $f(b_1 b_2 b_3 \cdots) = f(b_1' b_2' b_3' \cdots)$ and $b \neq b'$. Then the images(under f) are equal as sequences of natural numbers, so

$$(c_i)_{i \geq 1} = (c_i')_{i \geq 1},$$

hence, $c_i = c_i'$ for every $i \geq 1$. By the definition of the c_i this implies $b_i = b_i'$ for every i. Therefore $b_1 b_2 b_3 \cdots = b_1' b_2' b_3' \cdots$. This is a contradiction to our original assumption that $b \neq b'$. Hence, if $f(b_1 b_2 b_3 \cdots) = f(b_1' b_2' b_3' \cdots)$ then $b = b'$, proving that f is injective.

Since f is an injection from $\{0, 1\}^{\mathbb{N}}$ to $\mathbb{N}^{\mathbb{N}}$, we obtain the cardinality inequality

$$\left|\mathbb{N}^{\mathbb{N}}\right| \geq \left|\{0, 1\}^{\mathbb{N}}\right| = \aleph_1.$$

(b) Given a sequence of natural numbers $(a_1 a_2 a_3 \cdots) \in \mathbb{N}^{\mathbb{N}}$, consider the map

$$g : (a_1 a_2 a_3 \cdots) \mapsto \underbrace{1 \cdots 1}_{a_1} 0 \underbrace{1 \cdots 1}_{a_2} 0 \underbrace{1 \cdots 1}_{a_3} 0 \cdots$$

Show that the above map $g : \mathbb{N}^{\mathbb{N}} \to \{0,1\}^{\mathbb{N}}$ is injective, and hence conclude that $|\mathbb{N}^{\mathbb{N}}| \leq \aleph_1$.

Solution: With the map $g : \mathbb{N}^{\mathbb{N}} \to \{0,1\}^{\mathbb{N}}$ defined as above, to show that it is injective we can proceed by the standard proof by contradiction.

For some $a, a' \in \mathbb{N}^{\mathbb{N}}$ Let $x = g((a_i))$ and $y = g((a'_i))$ and assume for the sake of contradiction, $x = y$ but $a \neq a'$. We can decode x and y uniquely as follows: starting at the left, count the number of consecutive 1's before the first 0 — that count equals a_1. Skip the 0, then count the next run of 1's to obtain a_2, and so on. Because each a_i is finite, every run of 1's is finite and separated by a 0, so this procedure recovers the sequence (a_i) uniquely. Thus if $g((a_i)) = g((a'_i))$ then $(a_i) = (a'_i)$. This contradicts our original assumption that $(a_i) \neq (a'_i)$. Hence g is injective (one-one mapping).

Consequently,

$$|\mathbb{N}^{\mathbb{N}}| \leq |\{0,1\}^{\mathbb{N}}| = \aleph_1.$$

Combining with part (a) we obtain $|\mathbb{N}^{\mathbb{N}}| = \aleph_1$ (i.e. $\mathbb{N}^{\mathbb{N}}$ has the same cardinality as $\{0,1\}^{\mathbb{N}}$, denoted by $\aleph_1$).

3. **Suppose $f : \mathcal{X} \to \mathcal{Y}$ and $g : \mathcal{Y} \to \mathcal{Z}$ are bijective.**
Is $g \circ f : \mathcal{X} \to \mathcal{Z}$ bijective? Prove formally or give a counterexample.
Solution: Yes, the composition of bijections is a bijection.

To prove that $g \circ f$ is bijective, we need to show that it is both injective and surjective.

Injectivity For the sake of contradiction, let $x_1, x_2 \in \mathcal{X}$ such that $(g \circ f)(x_1) = (g \circ f)(x_2)$ and $x_1 \neq x_2$. By the definition of composition, this is equivalent to $g(f(x_1)) = g(f(x_2))$. Since g is injective, $f(x_1) = f(x_2)$. Since f is injective, $x_1 = x_2$. This contradicts our assumption that $x_1 \neq x_2$. Therefore, for any $x_1, x_2 \in \mathcal{X}$, if $(g \circ f)(x_1) = (g \circ f)(x_2)$, then $x_1 = x_2$.

Hence, $g \circ f$ is injective.

Surjectivity Let $z \in \mathcal{Z}$ be an arbitrary element. Since g is surjective, there exists an element $y \in \mathcal{Y}$ such that $g(y) = z$. Since f is surjective, there exists an element $x \in \mathcal{X}$ such that $f(x) = y$. By substituting y into the previous equation, we get $g(f(x)) = z$. By the definition of composition, this means $(g \circ f)(x) = z$. Therefore, for any $z \in \mathcal{Z}$, there exists an $x \in \mathcal{X}$ such that $(g \circ f)(x) = z$. Hence, $g \circ f$ is surjective.

Since $g \circ f$ is both injective and surjective, it is bijective.

4. **Show that the set $\mathscr{C} \subset \{0,1\}^{\mathbb{N}}$ of binary sequences with finitely many 1s is countably infinite.**
Solution: Let $\mathbb{W} = \mathbb{N} \cup \{0\}$. For each $k \in \mathbb{W}$ let $\mathscr{C}_k$ denote the set of infinite binary sequences (i.e. elements of $\{0,1\}^{\mathbb{N}}$) that contain exactly k entries equal to 1.

For fixed k, given $x \in \mathscr{C}_k$, let $0 \leq n_1 < n_2 < \cdots < n_k$ be the indices (indexing from 0) at which x has a 1. Define

$$\iota_k : \mathscr{C}_k \longrightarrow \mathbb{W}^k, \qquad \iota_k(x) := (n_1, n_2, \ldots, n_k).$$

This is well-defined because every element of $\mathscr{C}_k$ has exactly k ones, hence exactly k indices. The map ι_k is injective: if two sequences have the same k-tuple of positions then they are the same sequence. Since ι_k is an injection and $\mathbb{W}^k$ is countable (by the Cantor-pairing / induction argument already established in Q1), it follows that $\mathscr{C}_k$ is countable.

We have

$$\mathscr{C} = \bigcup_{k \in \mathbb{W}} \mathscr{C}_k,$$

a countable union of countable sets, so $\mathscr{C}$ is countable.

Finally, $\mathscr{C}_1$ (the sequences with exactly one 1) is countably infinite, since

$$n \longmapsto (\ldots, 0, 0, \underbrace{1}_{\text{position } n}, 0, 0, \ldots)$$

is a bijection $\mathbb{W} \hookrightarrow \mathscr{C}_1$ (proof left as exercise for the reader). This means $|\mathbb{W}| = |\mathscr{C}_1|$.Hence, $\mathscr{C}_1$ is countably infinite. As $\mathscr{C}_1 \subseteq \mathscr{C}$ and $\mathscr{C}$ is countable, it follows that $\mathscr{C}$ is countably infinite.

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.
Solution: Observe that

$$B_n = A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ times}}.$$

If $|A| < \infty$, then $|B_n| = |A|^n < \infty$ i.e is finite, hence, countable.

If A is countably infinite, then by the same reasoning used in the proof of the countability, by induction, of $\mathbb{W}^d$ (see Q1 part(d)), it follows that B_n = A^n, $n \in \mathbb{N}$ is countably infinite.

Thus, B_n is countable for every $n \in \mathbb{N}$. Since a countable union of countable sets is countable, it follows 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 rational 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 rational coefficients.
Solution: Notice that a polynomial f of degree $d \in \mathbb{N} \cup \{0\}$ with rational 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 $a_i \in \mathbb{Q}$ for all $i \in \{1, \ldots, d\}$, $a_d \neq 0$. The above polynomial admits at most d real roots, and can be associated uniquely with the tuple $(a_0, \ldots, a_d) \in \mathbb{Q}^{d+1}$. Hence, it follows that the set of all polynomials with degree 0 is equivalent to the set $\mathbb{Q}$, the set of all polynomials of degree 1 is equivalent to $\mathbb{Q}^2$, the set of all polynomials of degree 2 is equivalent to $\mathbb{Q}^3$, and so on. Noting that $\mathbb{Q}^{d+1}$ is countably infinite for every $d \in \mathbb{W}$ (again, can be proved on similar lines as in Q1 part(d)), it follows that

$$\text{set of all polynomials with rational coefficients} \equiv \bigcup_{d \in \mathbb{W}} \mathbb{Q}^{d+1} = \mathbb{P}\,(\text{say}).$$

Using the fact that a countable union of countable sets is countable, we conclude that the set of all polynomials with rational coefficients is countable.
Since each polynomial of degree d has only finitely many roots (at most d), the set of all algebraic numbers can be expressed as

$$\text{set of all algebraic numbers} = \bigcup_{p \in \mathbb{P}} R(p) = \mathbb{A}\,(\text{say}),$$

where $\mathbb{P}$ denotes the set of all polynomials with rational coefficients, and $R(p)$ denotes the set of roots of the polynomial p.
Because $\mathbb{P}$ is countable and each $R(p)$ is finite, $\mathbb{A}$ is a countable union of finite sets. Therefore, the set of all algebraic numbers is countable.

6. **Let $\mathscr{D}$ denote the collection of all finite-length binary strings**

(a) What is the cardinality of $\mathscr{D}$?
Solution: Let $\mathscr{D}_n$ be the set of all binary strings of length n. Then $|\mathscr{D}_n| = 2^n$. The set $\mathscr{D}$ is the union of all such sets for every non-negative integer n, i.e.,

$$\mathscr{D} = \bigcup_{n \in \mathbb{N}} \mathscr{D}_n.$$

Since each $\mathscr{D}_n$ is a finite set, $\mathscr{D}$ is a countable union of finite sets. Since, a countable union of countable sets is countable, $\mathscr{D}$ is countable. $\mathscr{D}$ is clearly infinite (as there exist strings of arbitrarily large finite length), therefore it is a countably infinite set. Thus, its cardinality is $\aleph_0$ (equivalently, cardinality of $\mathbb{N}$), i.e., $|\mathscr{D}| = \aleph_0$.

(b) How does $\mathscr{D}$ differ from $\{0,1\}^{\mathbb{N}}$? What are their cardinalities?
Solution: The sets $\mathscr{D}$ and $\{0,1\}^{\mathbb{N}}$ differ in the length of their elements.

- The elements of $\mathscr{D}$ are all finite-length binary strings.
- The elements of $\{0,1\}^{\mathbb{N}}$ are all infinite binary sequences.

The cardinalities are also distinct and as follows:

- $|\mathscr{D}| = \aleph_0$ (from part (a))
- $|\{0,1\}^{\mathbb{N}}| = \aleph_1$ (as demonstrated in class using Cantor's diagonal argument)

(c) Produce an example of an element of $\mathscr{D}$ that is not present in $\{0,1\}^{\mathbb{N}}$.
Solution: Any non-empty finite binary string is an element of $\mathscr{D}$ but not an element of $\{0,1\}^{\mathbb{N}}$. For instance, the string "1011" is in $\mathscr{D}$ because it has a finite length of 4. However, it cannot be in $\{0,1\}^{\mathbb{N}}$, as the elements of $\{0,1\}^{\mathbb{N}}$ are defined as infinite sequences.

Appendix

Claim. Let A be a countable set (finite or countably infinite), and let F be a finite set. Then, $A \cup F$ is finite if and only if A is finite. Likewise, $A \setminus F$ is finite if and only if A is finite.

Proof. We consider separately the two possibilities for the countable set A.

Case 1: A is finite. Suppose $|A| = n < \infty$ and $|F| = k < \infty$. Then $A \cup F$ is finite with $|A \cup F| \le n + k$ (indeed $|A \cup F| = n + k - |A \cap F|$), and $A \setminus F$ is finite with $|A \setminus F| \le n$ (indeed $|A \setminus F| = n - |A \cap F|$). Thus both $A \cup F$ and $A \setminus F$ are finite, so their cardinalities are in the same class (finite) as that of A. This establishes the claim in the finite case.

Case 2: A is countably infinite. Since A is countably infinite, there exists a bijection

$$f : \mathbb{N} \to A.$$

Write $F = \{x_1, \ldots, x_k\}$.

1. We first show that $A \cup F$ is countably infinite. Define $g : \mathbb{N} \to A \cup F$ by

$$g(n) = \begin{cases} x_{n+1}, & 0 \le n < k, \\ f(n-k), & n \ge k. \end{cases}$$

Injectivity. Suppose $g(n_1) = g(n_2)$ for $n_1, n_2 \in \mathbb{N}$. We consider cases.

- If $0 \le n_1 < n_2 < k$, then $g(n_i) = x_{n_i+1}$ for $i = 1, 2$. Since the x_j are distinct, $x_{n_1+1} = x_{n_2+1}$ implies $n_1 + 1 = n_2 + 1$, hence $n_1 = n_2$.
- If $n_1 < k \le n_2$, then $g(n_1) = x_{n_1+1}$ while $g(n_2) = f(n_2 - k) \in A$. WLOG, assume $F \cap A = \varnothing$; in this case the two values lie in disjoint parts of the construction, so equality is impossible. Thus this case cannot occur.
- If $k \le n_1 < n_2$, then $g(n_i) = f(n_i - k)$ for $i = 1, 2$. Since f is injective, $f(n_1 - k) = f(n_2 - k)$ implies $n_1 - k = n_2 - k$, hence $n_1 = n_2$.

In all cases $g(n_1) = g(n_2)$ forces $n_1 = n_2$, so g is injective.

Surjectivity. Let $y \in A \cup F$. If $y \in F$ then $y = x_j$ for some $1 \le j \le k$, and $y = g(j-1)$. If $y \in A$ then $y = f(m)$ for some $m \in \mathbb{N}$, and $y = g(m+k)$. Hence every element of $A \cup F$ is in the image of g, so g is surjective.

Therefore g is bijective, and $A \cup F$ is countably infinite.

2. We now show that $A \setminus F$ is countably infinite. Let

$$S := \{n \in \mathbb{N} : f(n) \notin F\}.$$

Since F is finite and f is a bijection, only finitely many n are excluded, so S is infinite. Enumerate S increasingly as $S = \{s_0 < s_1 < s_2 < \cdots\}$ and define

$$h(n) := f(s_n), \quad n \in \mathbb{N}.$$

Injectivity. Suppose $h(n_1) = h(n_2)$. Then $f(s_{n_1}) = f(s_{n_2})$. Since f is injective, $s_{n_1} = s_{n_2}$. But the enumeration (s_n) is strictly increasing, so $n_1 = n_2$. Hence h is injective.

Surjectivity. Let $y \in A \setminus F$. Since $y \in A$, there exists $m \in \mathbb{N}$ with $y = f(m)$. Because $y \notin F$, we have $m \in S$. Thus $m = s_j$ for some j, so $y = f(s_j) = h(j)$. Hence h is surjective onto $A \setminus F$.

Therefore h is bijective, and $A \setminus F$ is countably infinite.