CS21201 Discrete Structures

Tutorial 7

Sizes of Sets

1. Let A be an infinite set.

(a) Prove that there exists a map $A \to A$ which is injective but not surjective.

Solution Pick any countable subset $B = \{b_1, b_2, b_3, \ldots\}$ of A. Define the map $f : A \to A$ as

$$f(a) = \begin{cases} b_{n+1} & \text{if } a = b_n, \\ a & \text{otherwise.} \end{cases}$$

(b) Prove that there exists a map $A \to A$ which is surjective but not injective.

Solution Let B be as in Part (a). Take the map $g : A \to A$ as

$$g(a) = \begin{cases} b_1 & \text{if } a = b_1, \\ b_{n-1} & \text{if } a = b_n \text{ for } n \geqslant 2, \\ a & \text{otherwise.} \end{cases}$$

2. Let A and B be uncountable sets with $A \subseteq B$. Prove or disprove: A and B are equinumerous.

Solution *False*. For example, take $B = 2^{\mathbb{R}}$, and $A = \{\{x\} \mid x \in \mathbb{R}\}$. By the power-set theorem, $|B| > |\mathbb{R}|$. Moreover, A is equinumerous with the uncountable set $\mathbb{R}$ via the bijective correspondence $\mathbb{R} \to A$ taking $x \mapsto \{x\}$.

3. Let A be an uncountable set and B a countably infinite subset of A. Prove/Disprove: A is equinumerous with $A - B$.

Solution *True*. Since $A - B \subseteq A$, we have $|A - B| \leqslant |A|$. We need to show that $|A| \leqslant |A - B|$, that is, there is an injective map $f : A \to A - B$. Since B is countable, we can write $B = \{b_1, b_2, b_3, \ldots\}$. If $A - B$ is finite (and so countable), then $A = (A - B) \cup B$ is countable too, so $A - B$ is infinite. This implies that we can find a countably infinite subset $C = \{c_1, c_2, c_3, \ldots\}$ of $A - B$. Now, define the map $f : A \to A - B$ as

$$f(a) = \begin{cases} c_{2n-1} & \text{if } a = c_n, \\ c_{2n} & \text{if } a = b_n, \\ a & \text{otherwise.} \end{cases}$$

It is an easy matter to show that f is a bijection (so an injection too).

4. Prove that the real interval $[0,1)$ is equinumerous with the unit square $[0,1) \times [0,1)$.

Solution The sets $\mathbb{F} = \mathbb{Q} \cap [0,1)$ and $\mathbb{F}^2$ are countable. Therefore $A = [0,1) - \mathbb{F}$ and $B = [0,1)^2 - \mathbb{F}^2$ are equinumerous with $[0,1)$ and $[0,1)^2$, respectively. Now, define that map $f : B \to A$ taking $(0.a_1a_2a_3\ldots, 0.b_1b_2b_3\ldots) \mapsto 0.a_1b_1a_2b_2a_3b_3\ldots$. Clearly, f is injective. Thus, $|B| \leqslant |A|$. The other inequality $|A| \leqslant |B|$ is simpler (map $0.c_1c_2c_3\ldots$ to $(0.c_1c_2c_3\ldots, 0.c_1c_2c_3\ldots)$).

5. Define a relation $\sim$ on $\mathbb{R}$ as $a \sim b$ if and only if $a - b \in \mathbb{Q}$.

(a) Prove that $\sim$ is an equivalence relation.

Solution Routine job.

(b) Is the set $\mathbb{R}/\sim$ of all equivalence classes of $\sim$ countable?

Solution *No*. $\mathbb{R}$ is the union of all equivalence classes of $\sim$. Each equivalence class $[x]$ is in bijective correspondence with $\mathbb{Q}$ via the map $r \mapsto x + r$, and so is countable. A countable union of countable sets is again countable.

6. Let $\mathbb{Z}[x]$ denote the set of all univariate polynomials with integer coefficients. Prove that $\mathbb{Z}[x]$ is countable.

Solution $\mathbb{Z}[x]$ is the countable union of $\{0\}$ and $\mathbb{Z}_d[x]$ for $d \in \mathbb{N}_0$, where $\mathbb{Z}_d[x]$ is the set of all univariate polynomials with integer coefficients and degree exactly equal to d. Such a polynomial can be written as $a_dx^d + a_{d-1}x^{d-1} + \cdots + a_2x^2 + a_1x + a_0$ with $a_i \in \mathbb{Z}$ and $a_d \neq 0$. Since each a_i has countably many possibilities, and there are only finitely many ($d+1$ to be precise) coefficients, each $\mathbb{Z}_d[x]$ is countable.

7. (a) A real or complex number a is called *algebraic* if $f(a) = 0$ for some non-zero $f(x) \in \mathbb{Z}[x]$. Let $\mathbb{A}$ denote the set of all algebraic numbers. Prove that $\mathbb{A}$ is countable.

Solution There are countably many polynomials in $\mathbb{Z}[x] - \{0\}$. Each such polynomial has only finitely many roots.

(b) Prove that there are uncountably many transcendental numbers.

Solution $\mathbb{R}$ is the disjoint union of $\mathbb{R} \cap \mathbb{A}$ and the set $\mathbb{T}$ of all (real) transcendental numbers. Since $\mathbb{A}$ is countable, so too is $\mathbb{R} \cap \mathbb{A}$. If $\mathbb{T}$ is countable, then $\mathbb{R}$ is countable too.

8. Let $\mathbb{Z}[x,y]$ be the set of all bivariate polynomials with integer coefficients.

(a) Prove that $\mathbb{Z}[x,y]$ is countable.

Solution Similar to the proof for $\mathbb{Z}[x]$.

(b) Let $\mathbb{V} = \{(a,b) \in \mathbb{C} \times \mathbb{C} \mid f(a,b) = 0 \text{ for some nonzero } f(x,y) \in \mathbb{Z}[x,y]\}$. Is $\mathbb{V}$ countable?

Solution *No.* The non-zero polynomial $x - y \in \mathbb{Z}[x,y]$ has a *root* (a,a) for all $a \in \mathbb{C}$. That is, $\mathbb{C} \times \mathbb{C} \subseteq \mathbb{V}$.

9. A set $S \subseteq \mathbb{R}$ is called *bounded* if S has both a lower bound and an upper bound in $\mathbb{R}$. Countable/Uncountable?

(a) The set of all bounded subsets of $\mathbb{Z}$.

Solution *Countable.* Let S be a bounded subset of $\mathbb{Z}$, Let $l \in \mathbb{R}$ be a lower bound of S, and $b \in \mathbb{R}$ an upper bound of S. But then S is a subset of the finite set $[\lceil l \rceil, \lfloor u \rfloor]$, and is itself finite. Now, use the facts that the two integer bounds can be chosen in only countably many ways, and the power set of a finite set is finite (and so countable).

(b) The set of all bounded subsets of $\mathbb{Q}$.

Solution *Uncountable.* Let $\mathbb{B}$ denote the set of all bounded subsets of $\mathbb{Q}$. Define a map $f : \mathbb{R} \to \mathbb{B}$ as follows. If x is rational, take $f(x) = \{x\}$. If x is irrational, let $a = \lfloor x \rfloor$. Then, $x - a$ is a proper fraction (in the interval $[0,1)$), and has an infinite decimal expansion of the form $0.d_1d_2d_3\ldots$. Define $f(x) = \{a, a + 0.d_1, a + 0.d_1d_2, a + 0.d_1d_2d_3, \ldots\}$, so $f(x)$ is bounded by a and x. It is an easy matter to argue that f is injective.

10. Provide a diagonalization argument to prove that the set of all infinite bit sequences is uncountable.

Solution Let S denote the set of all infinite bit sequences. Suppose that S is countable. Then, there exists a bijection $f : \mathbb{N} \to S$. We write $f(1), f(2), f(3), \ldots$ as follows.

$$\begin{aligned}
f(1) &= a_{11}, a_{12}, a_{13}, \ldots, a_{1n}, \ldots \\
f(2) &= a_{21}, a_{22}, a_{23}, \ldots, a_{2n}, \ldots \\
f(3) &= a_{31}, a_{32}, a_{33}, \ldots, a_{3n}, \ldots \\
&\vdots \\
f(n) &= a_{n1}, a_{n2}, a_{n3}, \ldots, a_{nn}, \ldots \\
&\vdots
\end{aligned}$$

Consider the sequence $s = a'_{11}, a'_{22}, a'_{33}, \ldots, a'_{nn}, \ldots$, where $'$ denotes bit complement. Then, $s \neq f(n)$ for all $n \in \mathbb{N}$. So f is not surjective, a contradiction.

11. Countable/Uncountable? Justify.

(a) The set F of all infinite bit sequences containing only a finite number of 0's.

Solution Countable. Let F_k denote the set of all infinite bit sequences containing exactly k 0's, where k is a fixed element of $\mathbb{N}_0$. We prove by induction on k that each F_k is countable.

[Basis] F_0 contains only one string $(111\ldots)$, and so is countable.

[Induction] Suppose that F_k is countable. Every element in F_{k+1} is of the form $1^u0\alpha$, where $u \in \mathbb{N}_0$, and $\alpha \in F_k$. That is, F_{k+1} is in bijection with $N_0 \times F_k$. But $\mathbb{N}_0$ is countable, and so also is F_k by the induction hypothesis. Therefore F_{k+1} is countable too.

Finally, note that $F = \bigcup_{k \geqslant 0} F_k$ is a union of countably many countable sets.

(b) The set I of all infinite bit sequences containing an infinite number of 0's.

Solution Uncountable. The set S of all infinite bit sequences is uncountable. If I is countable, $S = F \cup I$ would also be countable.

Direct proof: Define the injective map $S \to I$ as $a_1, a_2, a_3, \ldots \mapsto 0, a_1, 0, a_2, 0, a_3, 0, \ldots$.

12. Let M_0 be the set of all infinite bit sequences $a_1, a_2, a_3, \ldots$ such that for all $n \in \mathbb{N}$, the string $a_1 a_2 \ldots a_n$ contains more 0's than 1's. Define M_1 analogously (more 1's than 0's). Let N denote the set of all infinite bit sequences that are in neither M_0 nor M_1.

(a) Prove that M_0 is equinumerous with M_1.

Solution Consider the bijection $M_0 \to M_1$ taking $a_1, a_2, a_3, \ldots$ to $a'_1, a'_2, a'_3, \ldots$, where a'_n is the complement of the bit a_n.

(b) Prove that N is uncountable.

Solution Let S denote the set of all infinite bit sequences. S is uncountable. Consider the injective map $S \to N$ taking $a_1, a_2, a_3, \ldots$ to $0, 1, a_1, a_2, a_3, \ldots$.

(c) Prove/Disprove: M_0 and M_1 are uncountable.

Solution Uncountable. For example, consider the injective map $S \to M_0$ that takes the infinite sequence $a_1, a_2, a_3, a_4, \ldots$ to $0, 0, a_1, 0, a_2, 0, a_3, 0, a_4, \ldots$.

Additional Exercises

13. Let A, B be sets. Prove or disprove:

(a) If A is countable and $A \subseteq B$, then B is countable.
(b) If A is uncountable and $A \subseteq B$, then B is uncountable.
(c) If A and B are countable, then $A \cap B$ is countable.
(d) If A and B are uncountable, then $A \cap B$ is uncountable.

14. **(a)** Prove that the set of all finite subsets of $\mathbb{N}$ is countable.
(b) Conclude that the set of all infinite subsets of $\mathbb{N}$ is uncountable.

15. Let A be a finite set.

(a) Prove that the set of all functions $A \to \mathbb{N}$ is countable.
(b) Let $|A| \geqslant 2$. Prove that the set of all functions $\mathbb{N} \to A$ is uncountable.
(c) Let $|A| \geqslant 2$. Prove that the set of all functions $\mathbb{N} \to A$ is equinumerous with $\mathbb{R}$.

16. Provide explicit bijections between the following pairs of sets.

(a) The sets $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$.
(b) The set of rational numbers in the real interval $[0, 1)$ and the set $\mathbb{Q}$ of all rational numbers.
(c) The set of irrational numbers in the real interval $[0, 1)$ and the set of all irrational numbers.
(d) The real interval $[0, 1)$ and $\mathbb{R}$.
(e) The real interval $(0, 1)$ and $\mathbb{R}$.
(f) The real intervals $[0, 1)$ and $[a, b)$ for any $a, b \in \mathbb{R}$, $a < b$.
(g) The real intervals $[0, 1)$ and $(0, 1)$.
(h) The real intervals $[0, 1]$ and $(0, 1)$.

17. Let A, B be sets, where A is equinumerous with $\mathbb{R}$ and B is equinumerous with $\mathbb{N}$.

(a) Prove that $A \cup B$ is equinumerous with $\mathbb{R}$.
(b) Prove that the Cartesian product $A \times B$ is equinumerous with $\mathbb{R}$.

18. Prove that the set $\{a + ib \mid a, b \in \mathbb{Z}\}$ of Gaussian integers is countable.

19. **(a)** Prove that the set $\mathbb{Q}[[X]]$ of all power series with rational coefficients is uncountable.

(b) Prove that the set $\mathbb{Q}(X) = \{f(X)/g(X) \mid g(X) \neq 0\}$ of all rational functions with rational coefficients is countable.

(c) Conclude that $\mathbb{Q}[[X]]$ contains a power series which is not the power series expansion of any rational function in $\mathbb{Q}(X)$. Can you identify any such power series explicitly?

20. Prove that the union of two sets each equinumerous with $\mathbb{R}$ is again equinumerous with $\mathbb{R}$

21. Prove that the set of all permutations of $\mathbb{N}$ is not countable.

22. Let A be a set of size $\geqslant 2$ (A may be infinite). Modify the diagonalization proof to establish that there cannot exist a bijection between A and the set of all *non-empty* subsets of A.

23. Let $S = (s_1, s_2, s_3, \ldots)$ and $T = (t_1, t_2, t_3, \ldots)$ be two infinite bit sequences. We say that S and T have the *same tail* if there exists $N \in \mathbb{N}$ such that $s_n = t_n$ for all $n \geqslant N$. Prove that for any given sequence S, the set of sequences having the same tail as S is countable.

24. Let S be the set of all infinite bit sequences. The n-th element of a sequence $\alpha \in S$ is denoted by $\alpha(n)$ for $n \geqslant 0$. Prove the countability/uncountability of each of the following two subsets of S.

(a) $T_1 = \left\{\alpha \in S \mid \alpha(n) = 1 \text{ and } \alpha(n+1) = 0 \text{ for some } n \geqslant 0\right\}$.

(b) $T_2 = \left\{\alpha \in S \mid \alpha(n) = 1 \text{ and } \alpha(n+1) = 0 \text{ for no } n \geqslant 0\right\}$.

25. Let S be the set of all infinite bit sequences. Denote by A the set of all infinite bit sequences that contain two consecutive 0's (at least once). Also let B denote the set of all infinite bit sequences that do not contain consecutive 0's.

(a) Propose an injective map $S \to A$, and argue about the countability/uncountability of A.

(b) Prove whether B is countable or not.

** **26.** [*Cantor set*] Start with the real interval $I = [0, 1]$. Remove the open middle one-third $(\frac{1}{3}, \frac{2}{3})$ from $[0, 1]$. This leaves us with two closed intervals $[0, \frac{1}{3}]$ and $[\frac{2}{3}, 1]$. Remove the open middle one-thirds of these two intervals, that is, $(\frac{1}{9}, \frac{2}{9})$ and $(\frac{7}{9}, \frac{8}{9})$. The portion of I that remains now consists of the four closed intervals $[0, \frac{1}{9}]$, $[\frac{2}{9}, \frac{1}{3}]$, $[\frac{2}{3}, \frac{7}{9}]$, and $[\frac{8}{9}, 1]$. Again, remove the open middle one-thirds of these four intervals, leaving eight closed subintervals in I. Repeat this process infinitely often. Let C be the subset of I that remains after this infinite process. Prove that C is uncountable.

Note: The cantor set C is one of the first explicitly constructed examples of *fractal sets*.

** **27.** Repeat Cantor's process of the last exercise with the exception that you remove the closed middle one-thirds of the remaining intervals. That is, in the first step, you remove $[\frac{1}{3}, \frac{2}{3}]$, in the second step, you remove $[\frac{1}{9}, \frac{2}{9}]$ and $[\frac{7}{9}, \frac{8}{9}]$, and so on. Now, let D be the subset of $I = [0, 1]$, that remains after this infinite process. Evidently, D is a proper subset of C. Is D uncountable too?