CS1231S: Discrete Structures

Tutorial #8: Cardinality and Revision

(Week 10: 21 – 25 October 2024)

Answers

---

1. In lecture example #3, we showed that $\mathbb{Z}$ is countable by defining a bijection $f: \mathbb{Z}^+ \to \mathbb{Z}$ as follows:

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even;} \\ -\dfrac{n-1}{2} & \text{if } n \text{ is odd.} \end{cases}$$

The above is based on the definition $\aleph_0 = |\mathbb{Z}^+|$. Suppose we adopt the definition $\aleph_0 = |\mathbb{N}|$ instead, define a bijection $g: \mathbb{N} \to \mathbb{Z}$ using a single-line formula to show that $\mathbb{Z}$ is countable.

Answer:

One such bijection (there could be others) $g: \mathbb{N} \to \mathbb{Z}$ is:

$$g(n) = (-1)^n \left\lfloor \frac{n+1}{2} \right\rfloor$$

Proof:

Note that (-1) to an even power is 1, and (-1) to an odd power is -1.

1. **(Injectivity)**
   - 1.1. Let $g(a), g(b) \in \mathbb{Z}$ and $g(a) = g(b)$.
   - 1.2. Then $g(a)$ and $g(b)$ must both be non-negative or both negative.
   - 1.3. Case 1: $g(a)$ and $g(b)$ are both non-negative.
     - 1.3.1. Then a and b must be even.
     - 1.3.2. Then $(-1)^a \left\lfloor \frac{a+1}{2} \right\rfloor = (-1)^b \left\lfloor \frac{b+1}{2} \right\rfloor \Rightarrow \left\lfloor \frac{a+1}{2} \right\rfloor = \left\lfloor \frac{b+1}{2} \right\rfloor \Rightarrow \frac{a}{2} = \frac{b}{2} \Rightarrow a = b.$
   - 1.4. Case 2: $g(a)$ and $g(b)$ are both negative.
     - 1.4.1. Then a and b must be odd.
     - 1.4.2. Then $(-1)^a \left\lfloor \frac{a+1}{2} \right\rfloor = (-1)^b \left\lfloor \frac{b+1}{2} \right\rfloor \Rightarrow -\left\lfloor \frac{a+1}{2} \right\rfloor = -\left\lfloor \frac{b+1}{2} \right\rfloor \Rightarrow \frac{a+1}{2} = \frac{b+1}{2} \Rightarrow a = b.$
   - 1.5. In all cases, $a = b$.
   - 1.6. Therefore g is injective.

2. **(Surjectivity)**
   - 2.1. Let $m \in \mathbb{Z}$. Then m is non-negative or negative.
   - 2.2. Case 1: m is non-negative.
     - 2.2.1. Let $n = 2m$.
     - 2.2.2. Then $n \in \mathbb{N}$ and $g(n) = (-1)^{2m} \left\lfloor \frac{2m+1}{2} \right\rfloor = \frac{2m}{2} = m.$
   - 2.3. Case 1: m is negative.
     - 2.3.1. Let $n = -2m - 1$.
     - 2.3.2. Then $n \in \mathbb{N}$ and $g(n) = (-1)^{-2m-1} \left\lfloor \frac{(-2m-1)+1}{2} \right\rfloor = -\frac{-2m}{2} = m.$
   - 2.4. In all cases, there exists $n \in \mathbb{N}$ such that $g(n) = m$.
   - 2.5. Therefore g is surjective.

3. Therefore g is a bijection from $\mathbb{N}$ to $\mathbb{Z}$.

2. Let B be a countably infinite set and C a finite set. Show that $B \cup C$ is countable

(a) by using the sequence argument;

(b) by defining a bijection $g: \mathbb{N} \to B \cup C$.

Lemma 9.2
An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \cdots$ in which every element of B appears.

Answers:

(a) 1. Apply Lemma 9.2 to obtain a sequence $b_0, b_1, b_2, \cdots$ in which every element of B appears.
2. Suppose $|C| = n \in \mathbb{N}$. We may write $C = \{c_0, c_1, c_2, \cdots, c_{n-1}\}$.
3. Then $c_0, c_1, c_2, \cdots, c_{n-1}, b_0, b_1, b_2, \cdots$ is a sequence in which every element of $B \cup C$ appears.
4. So $B \cup C$ is countable by Lemma 9.2.

(b) 1. As B is a countably infinite set, we have a bijection $f: \mathbb{N} \to B$.
2. Let $C' = C \setminus B = \{c_0, c_1, c_2, \cdots, c_{k-1}\}$ where $c_0, c_1, c_2, \cdots, c_{k-1}$ are all distinct.
3. Define a function $g: \mathbb{N} \to B \cup C$ such that

$$g(x) = \begin{cases} c_x & \text{if } x < k; \\ f(x-k) & \text{otherwise.} \end{cases}$$

4. **(Injectivity)**
   4.1. Let $x_1, x_2 \in \mathbb{N}$ such that $g(x_1) = g(x_2)$.
   4.2. Case 1: $x_1, x_2 \geq k$.
      4.2.1. $f(x_1 - k) = g(x_1) = g(x_2) = f(x_2 - k)$.
      4.2.2. $x_1 - k = x_2 - k$ (by injectivity of f) and so $x_1 = x_2$.
   4.3. Case 2: $x_1, x_2 < k$.
      4.3.1. $c_{x_1} = g(x_1) = g(x_2) = c_{x_2}$.
      4.3.2. $x_1 = x_2$ (since $c_0, c_1, \dots, c_{k-1}$ are all distinct).
   4.4. Case 3: exactly one of x_1, x_2 is less than k.
      4.4.1. WLOG, assume $x_1 < k \leq x_2$.
      4.4.2. $g(x_1) = c_{x_1} \in C' = C \setminus B$. In particular, $g(x_1) \notin B$ (by def of set difference).
      4.4.3. $g(x_1) = g(x_2) = f(x_2 - k) \in B$.
      4.4.4. Contradiction, hence this case will never happen.
   4.5. In all possible cases, we have $x_1 = x_2$.
   4.6. Therefore g is injective.
5. **(Surjectivity)**
   5.1. Let $y \in B \cup C$.
   5.2. Case 1: $y \in B$.
      5.2.1. There exists some $z \in \mathbb{N}$ such that $y = f(z)$ (by surjectivity of f).
      5.2.2. Let $x = z + k \in \mathbb{N}$.
      5.2.3. Then, $x \geq k$ and so $g(x) = g(z+k) = f(z) = y$ (by definition of g).
   5.3. Case 2: $y \notin B$.
      5.3.1. Then, $y \in C \setminus B = C'$.
      5.3.2. There exists some $x \in \mathbb{N}$ with $x < k$ such that $y = c_x$ (by definition of $c_0, c_1, \dots, c_{k-1}$).
      5.3.3. Then, $g(x) = c_x = y$ (by definition of g).
   5.4. In all cases, there exists some $x \in \mathbb{N}$ such that $g(x) = y$.
   5.5. Therefore g is surjective.
6. Therefore g is a bijection from $\mathbb{N}$ to $B \cup C$.

Note: You can see that the sequence argument "shields off" a lot of details.

3. Recall the definition of $\bigcup_{i=m}^{n} A_i$ in Tutorial 3.

(a) Consider this claim:

"Suppose $A_1, A_2, \cdots$ are finite sets. Then $\bigcup_{i=1}^{n} A_i$ is finite for any $n \geq 2$."

The above statement is true. However, consider the following "proof":

"We will prove by induction on n. Since A_1 and A_2 are finite, then $A_1 \cup A_2$ is finite, so the claim is true for $n = 2$. Now suppose the claim is true for $n = k$, so $\bigcup_{i=1}^{k} A_i$ is finite. Let $A_{k+1} = \emptyset$. Then $\bigcup_{i=1}^{k+1} A_i = (\bigcup_{i=1}^{k} A_i) \cup A_{k+1} = \bigcup_{i=1}^{k} A_i$ which is finite by the induction hypothesis, so the claim is true for $n = k + 1$. Therefore, the claim is true for all $n \geq 2$."

What is wrong with this "proof"?

(b) Disprove the following: "Suppose $A_1, A_2, \cdots$ are finite sets. Then $\bigcup_{k=1}^{\infty} A_k$ is finite."
[The point here is: induction takes you to any finite n, but <u>not</u> to infinity.]

Answers:

(a) There is an implicit universal quantification on $A_1, A_2, \cdots$, i.e. we have to prove the claim is true for all possible $A_1, A_2, \cdots$, so we cannot just consider the special case $A_{k+1} = \emptyset$.

(b) Let $A_i = \{i\}$ for all $i \geq 1$. Then $\bigcup_{i=1}^{\infty} A_i = \mathbb{Z}^+$, which is infinite.

4. Suppose $A_1, A_2, A_3, \cdots$ are countable sets.

(a) Prove, by induction, that $\bigcup_{i=1}^{n} A_i$ is countable for any $n \in \mathbb{Z}^+$.

(b) Does (a) prove that $\bigcup_{i=1}^{\infty} A_i$ is countable?

Answers:

(a) $\bigcup_{i=1}^{n} A_i$ is countable.

> **Lemma 9.4**
> Let A and B be countably infinite sets. Then $A \cup B$ is countable.

Proof:

1. Let $P(n)$ means "$\bigcup_{i=1}^{n} A_i$ is countable".
2. **Basis step:** $\bigcup_{i=1}^{1} A_i = A_1$ is countable, so $P(1)$ is true.
3. **Inductive step:** Suppose $P(k)$ is true.
   3.1. $\bigcup_{i=1}^{k+1} A_i = (\bigcup_{i=1}^{k} A_i) \cup A_{k+1}$.
   3.3. Case 1: Both $\bigcup_{i=1}^{k} A_i$ and A_{k+1} are finite.
      3.3.1 Then, $\left(\bigcup_{i=1}^{k} A_i\right) \cup A_{k+1}$ is finite, and hence countable.
   3.4. Case 2: Exactly one of $\bigcup_{i=1}^{k} A_i$ and A_{k+1} is finite.
      3.4.1 Then, $\left(\bigcup_{i=1}^{k} A_i\right) \cup A_{k+1}$ is countable (by Q2).
   3.5. Case 3: Neither $\bigcup_{i=1}^{k} A_i$ nor A_{k+1} is finite.
      3.5.1 Then, $\left(\bigcup_{i=1}^{k} A_i\right) \cup A_{k+1}$ is countable (by Lemma 9.4).
   3.6. Hence $P(k + 1)$ is true.
4. Therefore $\bigcup_{i=1}^{n} A_i$ is countable for any $n \in \mathbb{Z}^+$ by MI.

(b) No. Question 3(b) shows that a proof that $\bigcup_{i=1}^{n} A_i$ is finite for every $n \geq 2$ does not imply $\bigcup_{i=1}^{\infty} A_i$ is finite. Similarly here, a proof that $\bigcup_{i=1}^{n} A_i$ is countable for every $n \geq 1$ does not imply that $\bigcup_{i=1}^{\infty} A_i$ is countable.

Note that $\bigcup_{i=1}^{\infty} A_i$ is indeed countable, just that it cannot be proved using the approach in part (a). We will prove it in the next question.

5. Let S_i be a countably infinite set for each $i \in \mathbb{Z}^+$. Prove that $\bigcup_{i\in\mathbb{Z}^+} S_i$ is countable.
[Hint: Use this theorem covered in class: $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable.]

Lemma 9.2
An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \cdots$ in which every element of B appears.

Answer:

1. Note that $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable.
2. Hence there is a bijection $f: \mathbb{Z}^+ \to \mathbb{Z}^+ \times \mathbb{Z}^+$.
3. For each $i \in \mathbb{Z}^+$, since S_i is countable, apply Lemma 9.2 to find a sequence $b_{i,1}, b_{i,2}, b_{i,3}, \cdots$ in which every element of S_i appears.
4. Define a sequence $c_1, c_2, c_3, \cdots$ by setting each $c_k = b_{i,j}$, where $(i, j) = f(k)$.
5. In view of Lemma 9.2, it suffices to show that every element of $\bigcup_{i\in\mathbb{Z}^+} S_i$ appears in the sequence $c_1, c_2, c_3, \cdots$.
   - 5.1. Take $x \in \bigcup_{i\in\mathbb{Z}^+} S_i$.
   - 5.2. The definition of $\bigcup_{i\in\mathbb{Z}^+} S_i$ gives $i \in \mathbb{Z}^+$ such that $x \in S_i$.
   - 5.3. So line 3 tell us that x appears in the sequence $b_{i,1}, b_{i,2}, b_{i,3}, \cdots$.
   - 5.4. Let $j \in \mathbb{Z}^+$ such that $x = b_{i,j}$.
   - 5.5. From the surjectivity of f, we obtain $k \in \mathbb{Z}^+$ such that $f(k) = (i, j)$.
   - 5.6. Then $x = b_{i,j} = c_k$ by the definition of c_k.

6. Let X be a (not necessarily countable) infinite set and Y be a finite set.
Define a bijection $X \cup Y \to X$.

Proposition 9.3
Every infinite set has a countably infinite subset.

Answer:

1. Use Proposition 9.3 to find a countably infinite subset $X_0 \subseteq X$.
2. Let $Y_0 = Y \setminus X$, so that Y_0 is finite.
3. Then $X_0 \cup Y_0$ is countable by question 2.
4. Hence $|X_0 \cup Y_0| = |\mathbb{Z}^+| = |X_0|$ by the definition of countably infinite sets.
5. Hence there is a bijection $f: X_0 \cup Y_0 \to X_0$.
6. Define $g: X \cup Y \to X$ as follows: for each $z \in X \cup Y$,

$$g(z) = \begin{cases} f(z), & \text{if } z \in X_0 \cup Y_0; \\ z, & \text{otherwise.} \end{cases}$$

7. g is the required bijection.

7. Let A be a countably infinite set. Prove that $\mathcal{P}(A)$ is uncountable. ($\mathcal{P}(A)$ is the power set of A.)
Answer:

Sketch: We prove by contradiction. Assuming that $\mathcal{P}(A)$ is countable, we provide a sequence of elements of $\mathcal{P}(A)$. Then we produce an element of $\mathcal{P}(A)$ that does not appear in the sequence that claims to contain all elements of $\wp(A)$.

1. Suppose not, that is, $\mathcal{P}(A)$ is countable.
2. $\mathcal{P}(A)$ is infinite as A is infinite and $\{a\} \in \mathcal{P}(A)$ for every $a \in A$.
3. By Proposition 9.1, there is a sequence $a_0, a_1, a_2, \cdots \in A$ in which every element of A appears exactly once.
4. By Proposition 9.1, there is a sequence $B_0, B_1, B_2, \cdots \in \mathcal{P}(A)$ in which every element of $\mathcal{P}(A)$ appears exactly once.
5. Now, define $B = \{a_i : a_i \notin B_i\}$.
6. Note that $B \in \mathcal{P}(A)$ since $a_0, a_1, a_2, \cdots \in A$.
7. To show $B \neq B_i$ for all $i \in \mathbb{N}$.
    - 7.1. Let $i \in \mathbb{N}$.
    - 7.2. Case 1: If $a_i \notin B_i$, then $a_i \in B$ by the definition of B.
    - 7.3. Case 2: If $a_i \in B_i$, then $a_i \notin B$ by the definition of B (as every element a_i of A appears exactly once in the sequence $a_0, a_1, a_2, \cdots$, so no $a_i = a_j$ if $i \neq j$.)
    - 7.4. In all cases, $B \neq B_i$.
8. Since B is not in the sequence $B_0, B_1, B_2, \cdots \in \mathcal{P}(A)$, this contradicts the claim that $\mathcal{P}(A)$ is countable.
9. Therefore, $\mathcal{P}(A)$ is uncountable.

> **Proposition 9.1**
> An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \cdots \in B$ in which every element of B appears exactly once.

8. [AY2022/23 Semester 1 Exam]
Given the following statements on any finite set A,

(i) If R is a reflexive relation on A, then $|A| \leq |R|$.

(ii) If R is a symmetric relation on A, then $|A| \leq |R|$.

(iii) If R is a transitive relation on A, then $|A| \leq |R|$.

Prove or disprove each of the statements.

Answers:

(i) True.

1. Let A be a finite set and R a reflexive relation on A.
2. Define a function $f: A \to R$ by setting, for $x \in A, f(x) = (x, x)$.
3. $(F1)$ 3.1. Let $x \in A$.
   3.2. $x\ R\ x$ (by the definition of reflexivity).
   3.3. Hence, we have $\big(x, (x, x)\big) \in f$ (by the definition of f).
4. $(F2)$ 4.1. Let $x \in A$ and $y_1, y_2 \in R$ such that $(x, y_1) \in f$ and $(x, y_2) \in f$.
   4.2. Then $y_1 = (x, x) = y_2$ (by the definition of f).
5. From lines 3 and 4, f is well defined.
6. (f is injective)
   6.1. Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$.
   6.2. Then $(x_1, x_1) = (x_2, x_2)$ (by the definition of f).
   6.3. Hence $x_1 = x_2$ (by equality of ordered pairs).
   6.4. Therefore f is injective.
7. Since $f: A \to R$ is an injective function, $|A| \leq |R|$ (by the Pigeonhole Principle).

(ii) and (iii): False

Let R be an empty relation on a non-empty set A.
Then R is vacuously symmetric and transitive, but $|A| > 0 = |\emptyset|$.

Function. A function $f: X \to Y$ is a relation satisfying:
(F1) $\forall x \in X\ \exists y \in Y\ (x, y) \in f$.
(F2) $\forall x \in X\ \forall y_1, y_2 \in Y\ \Big(\big((x, y_1) \in f \wedge (x, y_2) \in f\big) \to y_1 = y_2\Big)$

Injection. A function $f: X \to Y$ is injective iff $\forall x_1, x_2 \in X\ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$.

Pigeonhole Principle (Lecture 9 slide 6)
Let A and B be finite sets. If there is an injection $f: A \to B$, then $|A| \leq |B|$.

9. [AY2022/23 Semester 2 Exam]
The Fibonacci sequence F_n is defined for $n \in \mathbb{N}$ as follows:

$$F_0 = 0, \quad F_1 = 1, \quad \text{and} \quad F_n = F_{n-1} + F_{n-2} \text{ for } n > 1.$$

Prove by Mathematical Induction the following statement:

$$\boldsymbol{Even(F_n) \Leftrightarrow Even(F_{n+3}), \forall n \in \mathbb{N}.}$$

The predicate $Even(x)$ is true when the integer x is even and false otherwise. You may use the following fact in your proof:

Fact 1: $Even(x+y) \Leftrightarrow \big(Even(x) \Leftrightarrow Even(y)\big)$

***Answer**:* Proof by Strong Induction

1. For each $n \in \mathbb{N}$, let $P(n) \equiv \big(Even(F_n) \Leftrightarrow Even(F_{n+3})\big)$.
2. **(Basis step)**
   2.1. $F_2 = F_1 + F_0 = 1 + 0 = 1$; $F_3 = F_2 + F_1 = 1 + 1 = 2$; $F_4 = F_3 + F_2 = 2 + 1 = 3$ (by definition of Fibonacci sequence)
   2.2. $P(0) \equiv (Even(F_0) \Leftrightarrow Even(F_3)) \equiv (Even(0) \Leftrightarrow Even(2))$ is true.
   2.3. $P(1) \equiv (Even(F_1) \Leftrightarrow Even(F_4)) \equiv (Even(1) \Leftrightarrow Even(3))$ is true.
3. **(Inductive step)**
   3.1. Inductive hypothesis: Let $k \in \mathbb{N}$ such that $P(0) \wedge P(1) \wedge \ldots \wedge P(k)$ is true.
   3.2. Case 1: $k = 0$.
      3.2.1. $P(1) \equiv (Even(F_1) \Leftrightarrow Even(F_4)) \equiv (Even(1) \Leftrightarrow Even(3))$ is true (by step 2.1).
   3.3. Case 2: $k \geq 1$.
      3.3.1. $Even(F_{k+1}) \Leftrightarrow Even(F_k + F_{k-1})$ (by definition of Fibonacci sequence)
      3.3.2. $\Leftrightarrow \big(Even(F_k) \Leftrightarrow Even(F_{k-1})\big)$ (by Fact 1)
      3.3.3. $\Leftrightarrow \big(Even(F_{k+3}) \Leftrightarrow Even(F_{k+2})\big)$ (by IH: $P(k)$ and $P(k-1)$ are true)
      3.3.4. $\Leftrightarrow Even(F_{k+3} + F_{k+2})$ (by Fact 1)
      3.3.5. $\Leftrightarrow Even(F_{k+4})$ (by definition of Fibonacci sequence)
   3.4. Thus $P(k+1)$ is true.
4. Therefore, $\forall\, n \in \mathbb{N}\; P(n)$ is true by Strong Mathematical Induction.

10. [AY2022/23 Semester 2 Exam]

(a) Let $\sim$ be an equivalence relation on X and let $g : X \to Y$ be a function such that

$$g(a) = g(b) \Leftrightarrow a \sim b \quad \forall a, b \in X.$$

Prove or disprove the following statement:

The following function f is well-defined:

$f : X/\sim \to Y$ given by the formula $f([x]) = g(x)\ \forall x \in X$.

(b) If the function f in part (a) above is well-defined, prove or disprove whether function f is injective or not injective.

If the function f in part (a) above is not well-defined, would changing the function g in part (a) to

$$g(a) = g(b) \Leftrightarrow a \nsim b \quad \forall a, b \in X.$$ (Note: $\nsim$ is the negation of $\sim$.)

make the function f in part (a) well-defined? Prove or disprove.

(c) Given the following bijections f and g on the set $A = \{1,2,3,4\}$,

$$f = \{(1,2), (2,4), (3,1), (4,3)\};$$
$$g = \{(1,4), (2,1), (3,2), (4,3)\}.$$

Find the order of f, g and $(f^{-1} \circ g)$.

Lemma Rel.1 Equivalence Classes
Let $\sim$ be an equivalence relation on a set A. The following are equivalent for all $x, y \in A$.
(i) $x \sim y$; (ii) $[x] = [y]$; (iii) $[x] \cap [y] \neq \emptyset$.

Answers:

(a)

1. Given $f([x]) = g(x)\ \forall x \in X$.
2. Let $[x] \in X/\sim$ be an arbitrary equivalence class of $\sim$ for some $x \in X$.
3. Since g is a function, this shows the existence of an image of $[x]$ (i.e. $g(x)$) under f.
4. (Next, to show that the image of $[x]$ under f is unique)
   Suppose $f([x]) = g(x)$ and $f([x']) = g(x')$ are such that $[x] = [x']$.
5. Since $[x] = [x']$, we have $x \sim x'$ (by Lemma Rel.1 Equivalence Classes)
6. Hence $g(x) = g(x')$ (by definition of g)
7. Hence the image of $[x]$ is unique.
8. Since the image of $[x]$ exists and is unique for every $[x] \in X/\sim$, the function f is well-defined.

(b)

1. Suppose $f([x]) = f([x'])$.
2. Then $g(x) = g(x')$ (by definition of f)
3. Then $x \sim x'$ (by definition of g)
4. Then $[x] = [x']$ (by Lemma Rel.1 Equivalence Classes)
5. Hence f is injective (by definition of injection)

Injection. A function $f: X \to Y$ is injective iff $\forall x_1, x_2 \in X\ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$.

(c)

Order of f = 4; order of g = 4; order of $(f^{-1} \circ g)$ = 3.

The ***order*** of a a bijection $f: A \to A$ is the smallest $n \in \mathbb{Z}^+$ such that

$$\underbrace{f \circ f \circ \cdots \circ f}_{n\text{-many } f\text{'s}} = id_A.$$