CSCI/MATH 2113 Discrete Structures

Appendix 3 Countable and Uncountable Sets

Alyssa Motas

April 12, 2021

Contents

1 Cardinality

Counting: Typical questions include:

- What is $|A|$?
- Is it the case that $|A| < |B|$?
- Is it the case that $|A| = |B|$?

For finite sets, we have

- Count $|A|$, say $|A| = n$.
- Count $|B|$, say $|B| = m$.
- Compare n and m.

What about for infinite sets? How do $|\mathbb{N}|$ and $|\mathbb{Z}|$ compare? What about $|\mathbb{N}|$ and $|\mathbb{R}|$?

1.1 Definition of bijection

For any nonempty sets A, B the function $f : A \to B$ is called a *one-to-one correspondence* if f is both one-to-one and onto.

1.2 Definition of same cardinality

If A, B are two nonempty sets, we say that A *has the same size, or cardinality*, as B and we write $A \sim B$, if there exists a one-to-one correspondence $f : A \to B$.

Example: $|\mathbb{N}| = |2\mathbb{N}| = \{n \in \mathbb{N} \mid n \text{ is even}\}$. To see this, consider the function $f : \mathbb{N} \to 2\mathbb{N}$. We have

- $f(n) = f(m) \Rightarrow 2n = 2m \Rightarrow n = m$, so f is injective.
- $x \in 2\mathbb{N} \Rightarrow x = 2y$ for $y \in \mathbb{N} \Rightarrow f(y) = x \Rightarrow f$ is surjective.

Another example is $|\mathbb{N}| = |3\mathbb{N}|$ since $g : \mathbb{N} \to 3\mathbb{N}$.

1.3 Properties of sets

Let A, B, C be sets. Then:

- $|A| = |A|$
- $|A| = |B| \Rightarrow |B| = |A|$
- $|A| = |B|$ and $|B| = |C| \Rightarrow |A| = |C|$.

Proof.

- $1_A : A \to A$ is bijective.
- If $|A| = |B|$, then $\exists f : A \to B$ bijection $\Rightarrow f$ is invertible $\Rightarrow f^{-1} : B \to A$ is invertible $\Rightarrow \exists g : B \to A$ bijective $\Rightarrow |B| = |A|$.
- $|A| = |B|$ and $|B| = |C|$

$$\begin{aligned}
&\Rightarrow \exists f : A \to B, \exists g : B \to C \text{ both bijective} \\
&\Rightarrow g \circ f : A \to C \text{ is bijective} \\
&\Rightarrow \exists h : A \to C \text{ bijective} \\
&\Rightarrow |A| = |C|.
\end{aligned}$$

□

1.4 Finite and infinite sets

Any set A is called a *finite* set if $A = \varnothing$ or if $|A| = |\{1, 2, 3, \ldots, n\}|$ for some $n \in \mathbb{Z}^+$. When $A = \varnothing$ we say that A has no elements and write $|A| = 0$. In the latter case, A is said to have n elements and we write $|A| = n$. When a set A is *not* finite, then it is called *infinite*.

Question: Is it the case that A, B infinite $\Rightarrow |A| = |B|$? Nope.

1.5 Countable

A set A is called *countable* (or *denumberable*) if (1) A is finite or (2) $|A| = |\mathbb{Z}^+|$.

Examples:

- $2\mathbb{N}$ and $3\mathbb{N}$ are countable.

- $\mathbb{Z}$ is countable. Define $f : \mathbb{N} \to \mathbb{Z}$ by

$$f(x) = \begin{cases} \dfrac{x}{2} & \text{if } x \text{ is even} \\ -\left(\dfrac{(x+1)}{2}\right) & \text{if } x \text{ is odd.} \end{cases}$$

  We show that f is injective: Suppose $f(x) = f(y)$.

  - If x and y are even, then

$$f(x) = \frac{x}{2} = \frac{y}{2} = f(y)$$

    so $x = y$.
  - If x and y are odd, then

$$f(x) = -\frac{x+1}{2} = -\frac{y+1}{2} = f(y)$$

    so $x = y$.
  - If x is odd and y is even, then

$$f(x) = -\frac{x+1}{2} = \frac{y}{2} = f(y) \Rightarrow y = -x - 1$$

    but $-x-1 < 0$ and $y \geq 0$ so this is a contradiction.

  Thus, f is an injection. Show that f is a surjection: for all $y \in \mathbb{Z}$ we have

  - If $y = 0$, then $f(1) = 0$
  - If $y > 0$, then $2y \in \mathbb{Z}^+$ and $f(2y) = \frac{2y}{2} = y$
  - If $y < 0$, then $-2y+1 \in \mathbb{Z}^+$ and $f(-2y+1) = -[(-2y+1)-1]/2 = -(-2y)/2 = y$.

  Therefore, f is a surjection and $|\mathbb{N}| = |\mathbb{Z}|$.

1.6 Finite and infinite sequence

For $n \in \mathbb{Z}^+$, a *finite sequence of n terms* is a function f whose domain is $\{1, 2, 3, \ldots, n\}$. Such a sequence is usually written as an *ordered* set $\{x_1, x_2, x_3, \ldots, x_n\}$, where $x_i = f(i)$ for all $1 \leq i \leq n$.
An *infinite sequence* is a function g having $\mathbb{Z}^+$ as ots dp,aom. This type of sequence is generally denoted by the *ordered* set $\{x_i\}_{i \in \mathbb{Z}^+}$ or $\{x_1, x_2, x_3, \ldots\}$, where $x_i = g(i)$ for all $i \in \mathbb{Z}^+$.

1.7 Sequence of distinct elements

If A is a nonempty countable set, then A can be written as a sequence of distinct elements.

1.8 Subset of an infinite countable set is countable

If S is a countable set and $A \subseteq S$, then A is countable.

Proof. When S is finite, this is clear. When S is infinite, then

- if A is finite, there is nothing to show.
- if A is infinite then we define a bijection from $\mathbb{N}$ to A.

Let $f : \mathbb{N} \to S$ be a bijection (which exists by assumption). Define $\overline{f} : \mathbb{N} \to A$

$$\overline{f}(0) = f(n_0) \text{ where } n_0 = \min\{n \in \mathbb{N} \mid f(n) \in A\}$$
$$\overline{f}(1) = f(n_1) \text{ where } n_1 = \min\{n \in \mathbb{N} \setminus \{n_0\} \mid f(n) \in A\}.$$

In general,

$$\overline{f}(k) = f(n_k) \text{ where } n_k = \min\{n \in \mathbb{N} \setminus \{n_{k-1}\} \mid f(n) \in A\}.$$

□

Corollary: If $\exists f : A \to \mathbb{N}$ injective then A is countable.

Proof. Then $f[A] \subseteq \mathbb{N}$ and $|A| = |f[A]|$. So, A is countable. □

1.9 Cantor's diagonal argument

The set $(0, 1] = \{x \mid x \in \mathbb{R} \text{ and } 0 < x \leq 1\}$ is not a countable set.

Proof. If $(0, 1]$ were countable, then we could write this set as a sequence of distinct terms: $(0, 1] = \{r_1, r_2, r_3, \dots\}$. To avoid two representations we agree to write real numbers in $(0, 1]$ such as 0.5 as $0.499\dots$ So, no element in $(0, 1]$ is represented by a decimal expansion that terminates. We have

$$\begin{aligned}
r_1 &= 0.a_{11}a_{12}a_{13}a_{14}\dots \\
r_2 &= 0.a_{21}a_{22}a_{23}a_{24}\dots \\
r_3 &= 0.a_{31}a_{32}a_{33}a_{34}\dots \\
&\vdots \\
r_n &= 0.a_{n1}a_{n2}a_{n3}a_{n4}\dots \\
&\vdots
\end{aligned}$$

where $a_{ij} \in \{0, 1, 2, 3, \dots, 8, 9\}$ for all $i, j \in \mathbb{Z}^+$.
Consider the real number $r = 0.b_1 b_2 b_3, \dots$, where for each $k \in \mathbb{Z}^+$,

$$b_k = \begin{cases} 3, & \text{if } a_{kk} \neq 3 \\ 7, & \text{if } a_{kk} = 3. \end{cases}$$

Then $r \in (0, 1)$, but for *every* $k \in \mathbb{Z}^+$, we have $r \neq r_k$. So, $r \notin \{r_1, r_2, r_3, \dots\}$. This contradicts our assumption that $(0, 1] = \{r_1, r_2, r_3, \dots\}$. $\square$

Corollary: $|(0, 1]| \neq |\mathbb{N}|$. In fact, $|(0, 1]| > |\mathbb{N}|$. When a set is not countable, it is termed *uncountable*. So, $(0, 1]$ is uncountable.

Corollary: The set $\mathbb{R}$ (of all real numbers) is an uncountable set.

Proof. If $\mathbb{R}$ were countable, then the subset $(0, 1]$ would be countable. $\square$

Remark: If $X \subseteq S$, then

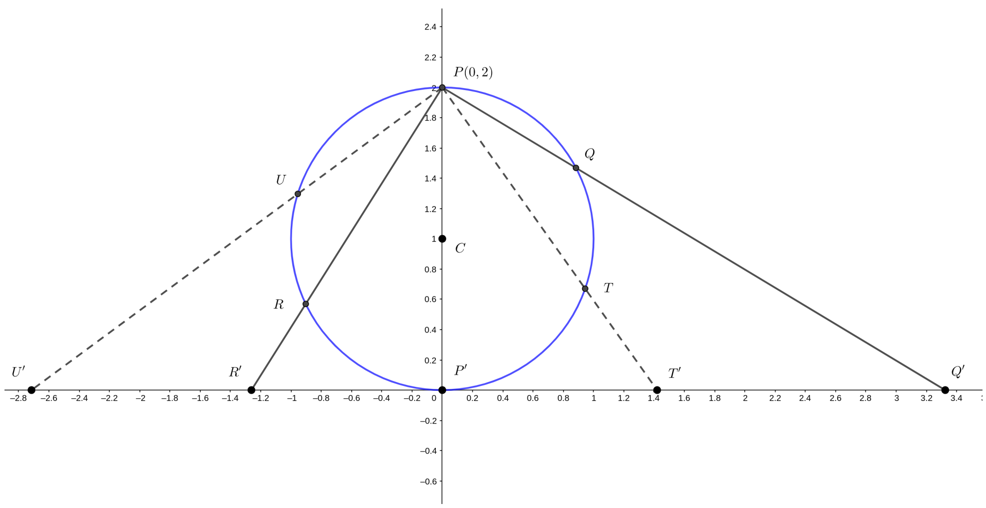
- if S is countable, then X is countable;
- if X is uncountable, then S is uncountable.

Examples:

- $\mathbb{N} \subseteq \mathbb{Q}$ and $\mathbb{Q} \subseteq \mathbb{R}$.
- $\mathbb{R} \subseteq \mathbb{C}$ so $\mathbb{C}$ is uncountable.
- $\mathbb{R} \subseteq \mathbb{R} \cup \{i\}$ so $\mathbb{R} \cup \{i\}$ is uncountable.

1.9.1 Example

Consider the points in the Cartesian plane on the unit circle $x^2+(y-1)^2 = 1$. How large is this set $S = \{(x, y) \mid x, y \in \mathbb{R} \text{ and } x^2 + (y-1)^2 = 1\}$? That is, is S countable or uncountable?
We have a unit circle centered at $C(0, 1)$. This circle is tangent to the real number line (or x-axis) at the point where $x = 0$. The point P, on the circumference, has coordinates $(0, 2)$.



This way, we obtain a one-to-one correspondence between the elements of S and the set $\mathbb{R}$. Hence $|S| = |\mathbb{R}|$, so S is another uncountable set.

1.10 Countable sets

- $\mathbb{N} \times \mathbb{N}$ is countable.

  Proof. Define the function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f(a, b) = 2^a 3^b$. The result will follow if we can show that f is one-to-one. For $(m, n), (u, v) \in \mathbb{N}\times\mathbb{N}$, $f(m, n) = f(u, v) \Rightarrow 2^m 3^n = 2^u 3^v \Rightarrow m = u, n = v$. Consequently, f is one-to-one and $\mathbb{N} \times \mathbb{N}$ is countable. $\square$

- $\mathbb{Z} \times \mathbb{Z}$ is countable.

  Proof. We know $\exists g : \mathbb{Z} \to \mathbb{N}$ bijective. Hence

$$g \times g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N} \times \mathbb{N}$$

is a bijection. But we have $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ bijective. Hence

$$g \circ (f \times f) : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$$

is a bijection. $\square$

- $\mathbb{Q}$ is countable.

  Proof. For $q \in \mathbb{Q}$, we have $q = \dfrac{n}{d}$ (reduced) $\Rightarrow (n, d) \in \mathbb{Z}^2$. $\square$

Remark: $\mathbb{Q}$ is dense in $\mathbb{R}$.

$$x, y \in \mathbb{R} \Rightarrow \exists q \in \mathbb{Q}, x \leq q \leq y.$$

$\mathbb{Q} \times \mathbb{Q}$ is dense in $\mathbb{R} \times \mathbb{R}$, and $\mathbb{R} \times \mathbb{R} \setminus \mathbb{Q} \times \mathbb{Q}$ is uncountable.

1.11 Powerset

If A is a set, then $|A| < |\mathcal{P}(A)|$.

Proof. True if $A = \varnothing$. If $A \neq \varnothing$, define

$$f : A \to \mathcal{P}(A).$$

f is an injection so $|A| \leq |\mathcal{P}(A)|$. Now suppose $g : A \to \mathcal{P}(A)$ is a surjection. Define

$$B = \{a \in A \mid a \notin g(a)\}.$$

Then $B \subseteq A$, so $B \in \mathcal{P}(A)$, so $\exists a \in A$ such that $g(a) = B$ (g surjective).

- if $a \in B$, then $a \notin g(a)$ so $a \notin B$.
- if $a \notin B$, then $a \notin g(a)$ so $a \in B$. (Contradiction)

$\square$

Corollary: $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots$