Discrete Mathematics

Cardinality

Shin Hong

Oct 6, 2019

Cardinality

- The *cardinality* of a set A is equal to the cardinality of a set B, denoted $|A| = |B|$, if and only if there is a one-to-one correspondence (i.e., bijection) from A to B.

- If there is a one-to-one function from A to B but no bijection, the cardinality of A is less than or the cardinality of B and we write $|A| < |B|$.

Cardinality of Finite Sets

- A set S is finite with cardinality $n \in \mathbb{N}^0$ if there is a bijection from the subset of non-negative integers $\{0, 1, \ldots, n{-}1\}$ to S

Let's Think About Infinite Sets

1. A set S is an infinite set if one of its subsets is an infinite set
2. Every subset of a finite set is finite.
3. If $f : S \rightarrow T$ be an injection and S is infinite, T is infinite.
4. If S is an infinite set, the power set of S is infinite.
5. If S and T are infinite sets, $S \cup T$ is infinite.
6. If S is infinite and $T \neq \emptyset$, then $S \times T$ is infinite.
7. If S is infinite and $T \neq \emptyset$, the set of functions from T to S is infinite.

Cardinality of Infinte Set

- A set is *countable* when
  - the set is finite, or
  - the set has the same cardinality as the set of positive integers

- When an infinite set is countable (calling it *countably infinite*), its cardinality is denoted as $\aleph_0$ (i.e., aleph null)

- A set that is not countable is *uncountable*

Showing that a Set is Countable

- An infinite set is countable iff there is a way to list the elements in a sequence with indexes of positive integers
  - there must exist a function $f : N \to S = \{a_1, a_2, \ldots\}$ such that $a_1 = f(1)$, $a_2 = f(2), \ldots, a_n = f(n), \ldots$

- Ex. Show that the set of positive even integers E is countable

  Let $f(x) = 2x$. Then f is a bijection from $\mathbb{N}$ to E.

$$
\begin{array}{ccccccc}
1 & 2 & 3 & 4 & 5 & 6 & \ldots\ldots \\
\updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
2 & 4 & 6 & 8 & 10 & 12 & \ldots\ldots
\end{array}
$$

Showing that a Set is Countable

- Ex. Show that the set of integers $\mathbb{Z}$ is countable.

  $\mathbb{Z}$ can be listed as a sequence:

$$0, 1, -1, 2, -2, 3, -3, \cdots\cdots$$

This sequence can be defined by a bijection f from $\mathbb{N}$ to $\mathbb{Z}$:

- When n is even: $f(n) = n/2$
- When n is odd: $f(\mathrm{n}) = -(n-1)/2$

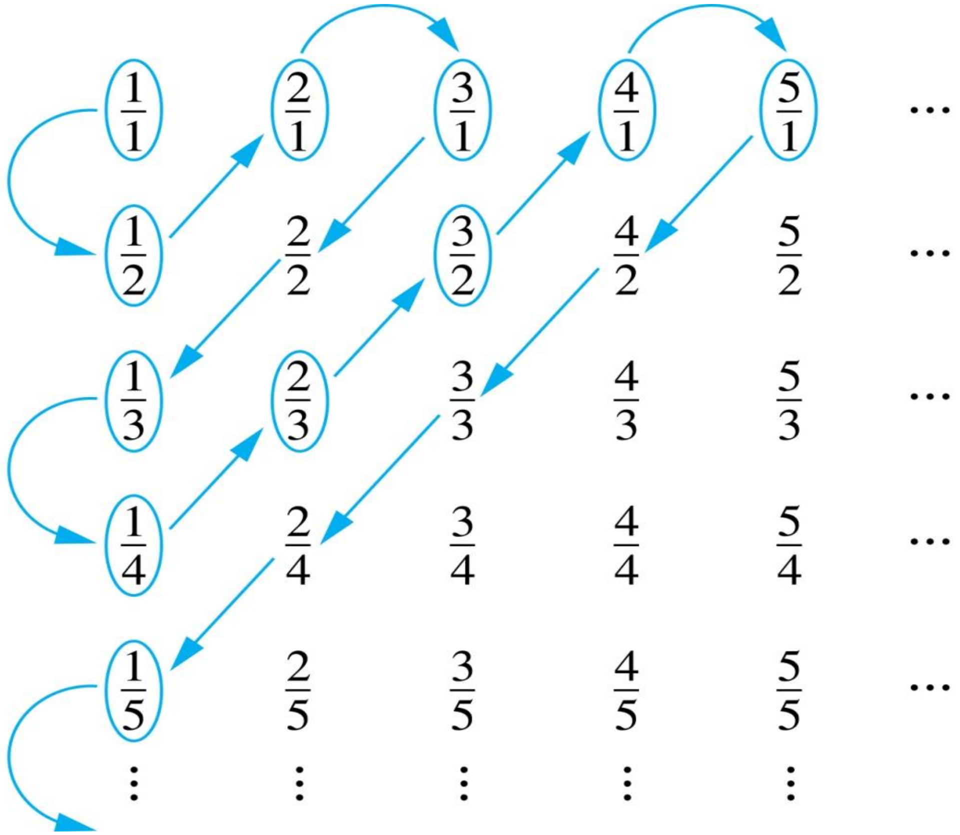
The Positive Rational Numbers are Countable

- Theorem. the set of all positive rational numbers is countable.

Constructing a sequence

List p/q with $p + q = 2$ first, and then list p/q with $p + q = 3$, and so on

1, ½, 2, 3, 1/3, 1/4, 2/3, ….



Enumeration

- An enumeration of a set S is a surjective function f from an initial segment of $\mathbb{N}$ to S.
  - f is a string where every element appears at least once
  - f is an enumeration without repetitions if f is bijective
  - f is an enumeration with repetitions if it is not injective
  - Example
    - $S = \{\alpha, \beta, \gamma, \delta\}$
    - $<\alpha, \gamma, \beta, \beta, \delta, \alpha>$ is an enumeration with repetition
    - $<\gamma, \alpha, \delta, \beta>$ is an enumeration without repetition

- A set S is countable iff there is an enumeration of S

Strings

- The set of strings over a finite alphabet A is countably infinite.
- Proof.
  - Show that the strings can be listed in a sequence:
    - All the strings of length 0 in alphabetical order.
    - Then all the strings of length 1 in lexicographic (as in a dictionary) order.
    - Then all the strings of length 2 in lexicographic order.
    - And so on.
  - This implies a bijection from $\mathbf{N}$ to S and hence it is countably infinite.

Every Java programs is a string, thus countable

The set of all Java programs is countable.

- Proof
  - Let *S* be the set of strings constructed from the characters which can appe ar in a Java program. Use the ordering from the previous example. Take each string in turn:
    - Feed the string into a Java compiler. (A Java compiler will determine if the input program is a syntactically correct Java program.)
    - If the compiler says YES, this is a syntactically correct Java program, we ad d the program to the list
    - We move on to the next string
  - In this way we construct an implied bijection from $\mathbb{N}$ to the set of Java progr ams. Hence, the set of Java programs is countable.

Uncountable Set

- Theorem. the set of real numbers $\mathbb{R}$ is uncountable.
- Proof (proof by contradiction)
  - Suppose that $\mathbb{R}$ is countable.
  - Then, the set of all real numbers in [0, 1) is countable, and the elements can be listed with positive integer indexes as follow

$$
\begin{aligned}
r_1 &= 0.d_{11}d_{12}d_{13}d_{14}\ \ldots \qquad d_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \\
r_2 &= 0.d_{21}d_{22}d_{23}d_{24}\ \ldots \\
r_3 &= 0.d_{31}d_{32}d_{33}d_{34}\ \ldots \\
r_4 &= 0.d_{41}d_{42}d_{43}d_{44}\ \ldots \\
&\vdots \\
r_i &= 0.\,d_{i1}\ d_{i2}\ \ldots d_{ii}\ \ldots
\end{aligned}
$$

  - There is a real number $r' = 0.\,d_1'\ d_2'\ d_3'\ \ldots d_i'\ \ldots$ such that
    - $d_i' = 4$ iff $d_{ii} \neq 4$
    - $d_i' = 5$ iff $d_{ii} = 4$
  - Then, $\forall i \in N\ (r' \neq r_i)$.
  - Consequently, this conclusion reaches to a contradiction.

Languages

- Let Σ be a finite alphabet and Σ^* the set of all strings over Σ. Then $\mathcal{P}(\Sigma^*)$ is uncountable.
- Proof using the Cantor's diagonalization
  - Let $<x_0, x_1, x_2, \ldots>$ be an enumeration of strings in Σ^* .
  - Suppose that $<A_0, A_1, \ldots>$ is an enumeration of $\mathcal{P}(\Sigma^*)$, s.t. A_i represents a subset of strings Σ^* as a bit vector
  - Think about $A' \in \mathcal{P}(\Sigma^*)$ such that $x_i \in A'$ iff $x_i \notin A_i$

	x_0	x_1	x_2	...
A_0	a_{00}	a_{01}	a_{02}	...
A_1	a_{10}	a_{11}	a_{12}	...
A_2	a_{20}	a_{21}	a_{22}	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Cardinalities of the Uncountable

- A set S is of cardinality c if there is a bijection from the set of real numbers in [0, 1] to S.
  - $\aleph_0 < c$
  - c.f. the set of real numbers in [0, 1] is called a continuum

- The continuum hypothesis claims that there exists no set A such that $\aleph_0 < |A| < c$
  - Note that, for an infinite set A, $\aleph_0 \leq |A|$

- For a set S, $|S| < |\mathcal{P}(S)|$.
  - $\aleph_0 = |N| < |\mathcal{P}(N)| < |\mathcal{P}(\mathcal{P}(N))| < \cdots$