EECS 1028 M: Discrete Mathematics for Engineers

Suprakash Datta
Office: LAS 3043

Course page: `http://www.eecs.yorku.ca/course/1028`
Also on Moodle

Cardinality Revisited

Sec 2.5

- A set is finite (has finite cardinality) if its cardinality is some (finite) integer n.

- Two sets A,B have the same cardinality iff there is a one-to-one correspondence from A to B

- E.g. alphabet (lower case), alphabet (upper case): $a \leftrightarrow A, \ldots z \leftrightarrow Z$.

Infinite sets

Questions:

- Why do we care?
- Cardinality of infinite sets
- Do all infinite sets have the same cardinality?

Need some machinery to reason about infinite sets

Countable sets

Definition: Is finite OR has the same cardinality as the positive integers.
E.g.

- The algorithm works for “any ”…
- Induction!

$\boxed{\text{Simplest type of infinite sets}}$

Why do we care?

Important Countable Sets

Fact (Will not prove): Any subset of a countable set is countable.

- The set of all binary strings
- The set of all Java programs!
- The set of all algorithms
- the set of all possible texts in the world

Countable Sets - Another Formulation

- A set S is infinite if there exists a surjective function $f : S \to \mathbb{N}$.
  "The set S has at least as many elements as $\mathbb{N}$."
- A set S is countable if there exists a surjective function
  $f : \mathbb{N} \to S$
  "The set S has no more elements than $\mathbb{N}$."
- A set S is countably infinite if there exists a bijective function
  $f : \mathbb{N} \to S$
  "The sets S and $\mathbb{N}$ are of equal size."

Countable Sets - Proofs

Proving a set to be countable involves (usually) constructing an explicit bijection with positive integers.

Will prove that

- The set of integers $\mathbb{Z}$ is countable
- The set of rationals $\mathbb{Q}$ is countable!
- The set of reals $\mathbb{R}$ is **not** countable!

$\mathbb{W} = \{0, 1, 2, \ldots\}$ is Countable

- We need to find a bijection between this sequence and $\mathbb{N}$
- Notice the pattern: $1 \leftrightarrow 0$, $2 \leftrightarrow 1$, $3 \leftrightarrow 2, \ldots$
- So the bijection is $f : \mathbb{N} \to \mathbb{W}$,

$$f(n) = n - 1$$

The Integers are Countable

- Write them as $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots\}$.
- Find a bijection between this sequence and $\mathbb{N}$
- Notice the pattern: $1 \leftrightarrow 0$,
  - $2 \leftrightarrow 1$
  - $4 \leftrightarrow 2$
  - $6 \leftrightarrow 3$
  - $\ldots$

  and
  - $3 \leftrightarrow -1$
  - $5 \leftrightarrow -2$
  - $7 \leftrightarrow -3, \ldots$

So the bijection is

$$\begin{aligned} f(n) &= n/2 \text{ if } n \text{ is even} \\ &= -(n-1)/2 \text{ otherwise} \end{aligned}$$

Other simple bijections

- Odd positive integers:
  $1 \to 1, 2 \to 3, 3 \to 5, 4 \to 7, \ldots$
  $f(n) = 2n - 1$

- Union of two countable sets A, B is countable:
  - Let $f : \mathbb{N} \to A, g : \mathbb{N} \to B$ be bijections
  - New bijection $h : \mathbb{N} \to A \cup B$

$$\begin{aligned} h(n) &= f(n/2) \text{ if } n \text{ is even} \\ &= g((n-1)/2) \text{ if } n \text{ is odd} \end{aligned}$$

The Set of all Binary Strings is Countable

Call this set B

- Define $f : B \to \mathbb{N}$ as follows. For any finite binary string b, $f(b) = ConvertToInt(1b)$
  That is, add a leading 1 to the string and interpret as as positive integer
- We can check that f is a bijection:
  - for any string we get a unique positive integer by adding a leading 1
  - for any natural number n we write it in binary and remove the most significant bit – this yields a valid binary string
- this proves that B is countable

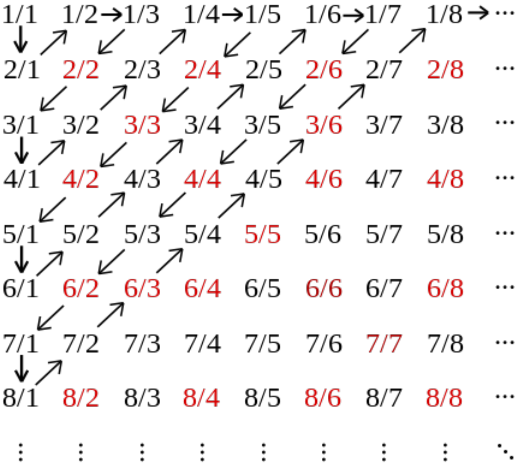
Consequences

- The set of all Java programs is countable: Convert each Java program to a binary string using ASCII representations. The set of Java programs is a subset of the set of binary strings
- The set of all algorithms: written in English (pseudo-code), same logic as that used for Java programs
- the set of all possible English texts in the world: Same reasoning as above

The Set of Rationals is Countable

- Show that $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable.
- Therefore $\mathbb{Q}^+ \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$ is countable
- To prove $\mathbb{Q}$ is countable, we use the technique used to construct a bijection from $\mathbb{Z}^+$ to $\mathbb{Z}$

$\mathbb{Z}^+ \times \mathbb{Z}^+$ is Countable



$\mathbb{Z}^+ \times \mathbb{Z}^+$ is Countable - Notes

- Why can we not count row-wise or column-wise?
- We can write down the ordering function explicitly
- Note that the ordering of $\mathbb{Q}$ is not in increasing order or decreasing order of value
- In proofs, you CANNOT assume that an ordering has to be in increasing or decreasing order
- So cannot use ideas like "between any two rational numbers x, y, there exists a rational number $0.5(x + y)$" to prove uncountability

$\mathbb{R}$ is not Countable

- Wrong proof strategy:
  - Suppose it is countable
  - Write them down in increasing order
  - Prove that there is a real number between any two successive reals.
- WHY is this incorrect? (Note that the above “proof” would show that the rationals are not countable!!)

$\mathbb{R}$ is not Countable - Steps

- Cantor diagonalization argument (1879)
- VERY powerful, important technique
- Proof by contradiction

Strategy:

- Assume countable
- look at all numbers in the interval $[0, 1)$
- list them in ANY order
- show that there is some number not listed

$[0, 1)$ is not Countable - Diagonalization proof

- Assume $[0, 1)$ is countable
- So there exists a bijection $F : \mathbb{N} \to \mathbb{R}$.
- So $F(1), F(2), \ldots$ are all infinite digit strings of the form $0.d_1d_2...$(padded with zeroes if required).
- Define the number (infinite string of digits) $Y = 0.y_1y_2...$ where

$$
\begin{aligned}
y_j &= F(i)_i + 1 \text{ if } F(i)_i < 8 \\
&= 7 \text{ if } F(i)_i \geq 8
\end{aligned}
$$

- Claim: $y \notin [0, 1)$
- Proof: if $y \in [0, 1)$, then $\exists j \in \mathbb{N}, y = F(j)$
  But $y, F(j)$ differs in the j^{th} digit by construction of y.

$[0, 1)$ is not Countable - Diagonalization proof - 2

$$0.\boxed{a_1}\, a_2\, a_3\, a_4\, a_5\, a_6\, a_7\, a_8\, a_9\, a_{10}\, a_{11}\ldots$$
$$0.b_1\,\boxed{b_2}\, b_3\, b_4\, b_5\, b_6\, b_7\, b_8\, b_9\, b_{10}\, b_{11}\ldots$$
$$0.c_1\, c_2\,\boxed{c_3}\, c_4\, c_5\, c_6\, c_7\, c_8\, c_9\, c_{10}\, c_{11}\ldots$$
$$0.d_1\, d_2\, d_3\,\boxed{d_4}\, d_5\, d_6\, d_7\, d_8\, d_9\, d_{10}\, d_{11}\ldots$$
$$0.e_1\, e_2\, e_3\, e_4\,\boxed{e_5}\, e_6\, e_7\, e_8\, e_9\, e_{10}\, e_{11}\ldots$$
$$0.f_1\, f_2\, f_3 f_4\, f_5\,\boxed{f_6}\, f_7\, f_8\, f_9 f_{10}\, f_{11}\ldots$$
$$\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots$$

new number not in list:

$$0.!a_1!b_2!c_3!d_4!e_5!f_6!g_7!h_8!i_9!j_{10}!k_{11}\ldots$$

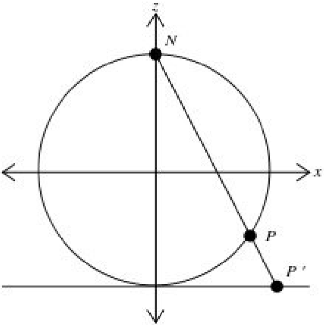
From https://skullsinthestars.com/2013/11/24/infinity-is-weird-whats-bigger-than-big/

$[0, 1)$ is not Countable - Notes

- Complication: many numbers in $[0, 1)$ have non-unique representations
- Q: Where does this proof fail on $\mathbb{N}$?
- Next: Inferring that $\mathbb{R}$ is not countable

$\mathbb{R}$ is not Countable

- Proof 1: Suppose $\mathbb{R}$ is countable. Then every subset of $\mathbb{R}$ is countable. Thus $[0, 1)$ is countable. This is a contradiction
- Proof 2: Show that the cardinality of $\mathbb{R}^{\geq 0}$ the same as that of $[0, 1)$. Define a bijection $f : \mathbb{R}^{\geq 0} \to [0, 1)$, by "wrapping" the interval $[0, 1)$ to the right half of the circle.



- $f(0) = (0, 0)$
- $f(P') = P$ in the picture
- $\lim_{x\to\infty} f(x) = N$ in the picture

$\mathcal{P}(\mathbb{N})$ is not Countable

- Again, assume this is countable. So there exists a listing $s_1, s_2, \ldots$ of its elements
- We use diagonalization shows that there will always be an element $x \in \mathcal{P}(\mathbb{N})$ that does not occur in the list $s_1, s_2, \ldots$
- The set $\mathcal{P}(\mathbb{N})$ contains all the subsets of $\mathbb{N}$. So, each subset $X \subseteq \mathbb{N}$ can be identified by an infinite string of bits $x_1 x_2 \ldots$ such that $x_j = 1$ iff $j \in X$.
- Aside: The above is a bijection between $\mathcal{P}(\mathbb{N})$ and the set of all infinite binary strings $\{0, 1\}^{\mathbb{N}}$

$\mathcal{P}(\mathbb{N})$ is not Countable - 2

$$
\begin{array}{ll}
s_1 & = 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,\ldots \\
s_2 & = 1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,\ldots \\
s_3 & = 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,\ldots \\
s_4 & = 1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,\ldots \\
s_5 & = 1\,1\,0\,1\,0\,1\,1\,0\,1\,0\,1\,\ldots \\
s_6 & = 0\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,\ldots \\
s_7 & = 1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,\ldots \\
s_8 & = 0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,\ldots \\
s_9 & = 1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,\ldots \\
s_{10} & = 1\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,\ldots \\
s_{11} & = 1\,1\,0\,1\,0\,1\,0\,0\,1\,0\,0\,\ldots \\
\vdots & \quad \vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\ddots
\end{array}
$$

$$
s = 1\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\,\ldots
$$

By Jochen Burghardt, CC BY-SA 3.0

`https://upload.wikimedia.org/wikipedia/commons/b/b7/Diagonal_argument_01_svg.svg`, via Wikimedia Commons

- We show that $s \notin \mathcal{P}(\mathbb{N})$
- By the same diagonalization argument as before, $\mathcal{P}(\mathbb{N})$ is not countable

$\mathcal{P}(\mathbb{N})$ is not Countable - Consequences

- Also, the power set of all binary strings is not countable: earlier we defined a bijection between the set of binary strings and $\mathbb{N}$; so there is a bijection between the power set of all binary strings and $\mathcal{P}(\mathbb{N})$

- Can be generalized from binary to any finite alphabet – this is used in later courses like EECS 2001: Introduction to the Theory of Computation

The Set of All Functions is not Countable

- There is a bijection from the set of all boolean functions with one integer input to the set of all subsets of $\mathbb{N}$
- We have seen that the set of all Java programs (or pseudocode, algorithms) is countable
- So there must exist problems for which there do not exist Java programs (or pseudocode, or algorithms), i.e., there are problems that are unsolvable!
- However, this does **not** tell us that any interesting problem is unsolvable

Other Infinities: A General Result

Theorem: There is no surjection from a set A to its power set $\mathcal{P}(A)$.
Proof:

- Suppose there exists a surjection $f : A \to \mathcal{P}(A)$
- Construct a set $B = \{x \in A | x \notin f(x)\}$
- $B \subseteq A$, so $B \in \mathcal{P}(A)$
- So $\exists y \in A, f(y) = B$
- Is $y \in B$?
  - Yes: So $y \in f(y) = B$, but then $y \notin f(y)$ by the definition of B
  - No: So $y \notin f(y) = B$, but then $y \in f(y)$ by the definition of B
- Contradiction

Other Infinities - 2

- So we can build a "bigger infinity" from a given infinite set
- We proved $\mathbb{R}, \mathcal{P}(\mathbb{N})$ and $\{0,1\}^{\mathbb{N}}$ uncountable. We showed that $\mathbb{R}$ has the same cardinality as $\mathcal{P}(\mathbb{N})$ and $\{0,1\}^{\mathbb{N}}$
- What if we take $\mathcal{P}(\mathbb{R})$?
  – Bigger set (different cardinality by the previous slide)
- Can we build bigger and bigger infinities this way?
  – Yes, by the previous slide
- Are there any other infinities?
  – Generalized Continuum Hypothesis: No

Questions

- Neither $\mathbb{R}$ nor $\mathbb{Z}$ have finite cardinalities, yet one set is countable, the other is not.
- The cardinality of $\mathbb{Z}$ is called $\aleph_0$ ("aleph null"), and that of $\mathbb{R}$ is called $\aleph_1$
- Q: Is there a set whose cardinality is "in-between"?
- Cantor's Continuum hypothesis: No.
- How do I know problem $\langle X \rangle$ in unsolvable?
  – EECS 2001, EECS 4111 and similar courses