Foundations of Computer Science
Lecture 22

Infinity

Size versus Cardinality: Comparing “Sizes”
Countable: Sets Which Are Not “Larger” Than N
Is There A Set “Larger” Than N? Cantor’s Diagonal Argument
Infinity and Computing
Our Short Stroll Through Discrete Math

1. Precise statements, proofs and logic.

2. **INDUCTION.**

3. Recursively defined structures and Induction. (Data structures; PL)

4. Sums and asymptotics. (Algorithm analysis)

5. Number theory. (Cryptography; probability; fun)

6. Graphs. (Relationships/conflicts; resource allocation; routing; scheduling, . . .)

7. Counting. (Enumeration and brute force algorithms)

8. Probability. (Real world algorithms involve randomness/uncertainty)
   - Inputs arrive in a random order;
   - Randomized algorithms (primality testing, machine learning, routing, conflict resolution . . .)
   - Expected value is a summary of what happens. Variance tells you how good the summary is.
Today: Infinity

   - Rationals are countable.

2. Uncountable
   - Infinite binary strings.

3. What does Infinity have to do with computing?
“Size” of a Set: Cardinality

You have 5 fingers on each hand.

You must know how to count.

You have an equal number of fingers on each hand.

All you need is a correspondence.

Cardinality $|A|$ (“size”), read “cardinality of $A$,” is the number of elements for finite sets

- $|A| \leq |B|$ iff there is an injection (1-to-1) from $A$ to $B$, i.e., $f : A \overset{\text{inj}}{\rightarrow} B$.
- $|A| > |B|$ iff there is no injection from $A$ to $B$.
- $|A| \geq |B|$ iff there is a surjection (onto) from $A$ to $B$, i.e., $f : A \overset{\text{sur}}{\rightarrow} B$.
- $|A| = |B|$ iff there is a bijection (1-to-1 and onto) from $A$ to $B$, i.e., $f : A \overset{\text{bij}}{\rightarrow} B$.

$|A| \leq |B| \ \text{AND} \ |B| \leq |A| \ \rightarrow \ |A| = |B|$. \ \text{(Cantor-Bernstein Theorem)}
A Countable Set’s Cardinality Is At Most $\lvert \mathbb{N} \rvert$

Finite sets: $\lvert A \rvert = n$ if and only if there is a bijection from $A$ to $\{1, \ldots, n\}$.

Infinite sets: The set $A$ is countable if $\lvert A \rvert \leq \lvert \mathbb{N} \rvert$. $A$ is “smaller than” $\mathbb{N}$.

To show that $A$ is countable you must find a 1-to-1 mapping from $A$ to $\mathbb{N}$.

```
A : 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 ...
```

```
\mathbb{N} : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 ...
```

You cannot skip over any elements of $A$, but you might not use every element of $\mathbb{N}$.

To prove that a function $f : A \mapsto \mathbb{N}$ is an injection:

1: Assume $f$ is not an injection. (Proof by contradiction.)
2: This means there is a pair $x, y \in A$ for which $x \neq y$ and $f(x) = f(y)$.
3: Use $f(x) = f(y)$ to prove that $x = y$, a contradiction. Hence, $f$ is an injection.
All Finite Sets are Countable

$A = \{3, 6, 8\}$. To show $|A| \leq \mathbb{N}$, we give an injection from $A$ to $\mathbb{N}$,

$3 \mapsto 1 \quad 6 \mapsto 2 \quad 8 \mapsto 3$.

For an arbitrary finite set $A = \{a_1, a_2, \ldots, a_n\}$, $\mathbb{N}$,

$a_1 \mapsto 1 \quad a_2 \mapsto 2 \quad a_3 \mapsto 3 \quad \cdots \quad a_n \mapsto n.$
Non-negative integers $\mathbb{N}_0 = \{0, 1, 2, \ldots \}$ are countable

How can this be? $\mathbb{N}_0$ contains every element in $\mathbb{N}$ plus 0?

To prove $|\mathbb{N}_0| \leq |\mathbb{N}|$, we give an injection $f : \mathbb{N}_0 \xrightarrow{\text{inj}} \mathbb{N}$,

$$f(x) = x + 1, \text{ for } x \in \mathbb{N}_0.$$  

*Proof.* Assume $f$ is not an injection. So, there are $x \neq y$ in $\mathbb{N}_0$ with $f(x) = f(y)$:

$$x + 1 = f(x) = f(y) = y + 1.$$  

That is $x + 1 = y + 1$ or $x = y$, which contradicts $x \neq y$. 

Also, $|\mathbb{N}| \leq |\mathbb{N}_0|$ because $\mathbb{N} \subseteq \mathbb{N}_0 \rightarrow |\mathbb{N}_0| = |\mathbb{N}|$. (Cantor-Bernstein)
Positive Even Numbers and Integers are Countable

\[ E = \{2, 4, 6, \ldots\}. \text{ Surely } |E| = \frac{1}{2}|\mathbb{N}|? \]

The bijection \( f(x) = \frac{1}{2}x \) proves \( |E| = |\mathbb{N}| \)

\[
\begin{array}{ccccccccccccc}
E : & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & 18 & 20 & \cdots \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \cdots \\
\mathbb{N} : & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots \\
\end{array}
\]

\[ \mathbb{Z} = \{0, \pm1, \pm2, \ldots\}. \text{ } |\mathbb{Z}| = |\mathbb{N}|. \]

\[
\begin{array}{cccccccccccc}
0 & -1 & -2 & -3 & -4 & -5 & -6 & -7 & -8 & -9 & -10 \cdots \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \cdots \\
\mathbb{N} : & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \cdots \\
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots \\
\end{array}
\]

**Exercise.** What is a mathematical formula for the bijection?
Every Countable Set Can Be “Listed”

\{3, 6, 8\} is a list. \(E = \{2, 4, 6, \ldots\}\) is a list. What about \(\mathbb{Z}\)?

\[\cdots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \cdots\] ← not a list

\[0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \cdots\] ← list

\(A:\)

\[\circ \quad \bullet \quad \diamondsuit \quad \times \quad + \quad \cdot \quad \ast \quad \heartsuit \quad \odot \quad \bullet \quad \circ \quad \cdots\]

\(N:\)

\[1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \quad 11 \quad 12 \quad 13 \quad 14 \quad 15 \quad 16 \quad 17 \quad 18 \quad 19 \quad 20 \quad \cdots\]

\(A:\)

\[\bullet \quad \heartsuit \quad + \quad \square \quad \circ \quad \diamondsuit \quad \times \quad \ast \quad \heartsuit \quad \odot \quad \bullet \quad \circ \quad \cdots\]

\(N:\)

\[1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \quad 11 \quad 12 \quad 13 \quad 14 \quad 15 \quad 16 \quad 17 \quad 18 \quad 19 \quad 20 \quad \cdots\]

\(\mathbb{N}_0:\) \ \{0, 1, 2, 3, 4, 5, \ldots\} \quad \(E:\) \ \{2, 4, 6, 8, 10, \ldots\} \quad \(\mathbb{Z}:\) \ \{0, +1, -1, +2, -2, +3, -3, +4, -4, \ldots\}

1. Different elements are assigned to different list-positions.
2. Can determine the list-position of \textit{any} element in the set. For \(\mathbb{Z}\),

\[
\text{list position of } z = \begin{cases} 
2z & z > 0; \\
2|z| + 1 & z \leq 0;
\end{cases}
\]
Union of Two Countable Sets is Countable

A and B are countable, so they can be listed.

\[ A = \{a_1, a_2, a_3, a_4, a_5, \ldots \} \quad B = \{b_1, b_2, b_3, b_4, b_5, \ldots \}. \]

Here is a list for \( A \cup B \)

\[ A \cup B = \{a_1, a_2, a_3, a_4, a_5, \ldots, b_1, b_2, b_3, b_4, b_5, \ldots \}. \]

What is the list-position of \( b_1 \)? Cannot use “…” twice.

\[ A \cup B = \{a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4, a_5, b_5, \ldots \}. \]

list-position of \( a_i \) is \( 2i - 1 \);
list-position of \( b_i \) is \( 2i \).

**Pop Quiz.** Get a list of \( \mathbb{Z} \) with \( A = \{0, -1, -2, -3, \ldots \} \) and \( B = \{1, 2, 3, \ldots \} \) using union.
Rationals are Countable: $|\mathbb{Q}| = |\mathbb{N}|$

This is surprising because between any two rationals there is another (not true for $\mathbb{N}$).

<table>
<thead>
<tr>
<th>$\mathbb{Q}$</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>+1</td>
</tr>
</tbody>
</table>

Intuition suggests $|\mathbb{Q}| = |\mathbb{N}| \times |\mathbb{Z}| \gg |\mathbb{N}|$. ☹️

$\mathbb{Q} = \left\{ \frac{0}{1}, \frac{1}{1}, \frac{1}{2}, \frac{0}{2}, \frac{0}{3}, \frac{-1}{3}, \frac{1}{3}, \frac{-1}{2}, \frac{-1}{1}, \frac{2}{1}, \frac{2}{2}, \frac{2}{3}, \frac{2}{4}, \frac{-1}{4}, \frac{1}{4}, \frac{0}{4}, \frac{0}{5}, \cdots \right\}$

$|\{\text{Rational Values}\}| \leq |\mathbb{Q}| \leq |\mathbb{N}|$.

**Exercise.** What is a mathematical formula for the list-position of $z/n \in \mathbb{Q}$?
Programs are Countable

Programs are finite binary strings. We show that all finite binary strings $\mathcal{B}$ are countable.

$$\mathcal{B} = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, 0000, \ldots \}$$

Pop Quiz. What is the list-position of 0110?

Exercise. For the $(k+1)$-bit string $b = b_k b_{k-1} \cdots b_1 b_0$, define the strings numerical value:

$$\text{value}(b) = b_0 \cdot 2^0 + b_1 \cdot 2^1 + \cdots + b_{k-1} \cdot 2^{k-1} + b_k \cdot 2^k.$$  

Show:

$$\text{list-position of } b = 2^{\text{length}(b)} + \text{value}(b).$$

$\mathbb{N}_0, E, \mathbb{Z}, \mathbb{Q}, \mathcal{B}$ are countable, \ldots Is Everything Countable?
Cantor’s Diagonal Argument: Assume there is a list of all infinite binary strings.

\[
\begin{align*}
    b_1: & \quad 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \cdots \\
    b_2: & \quad 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \cdots \\
    b_3: & \quad 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \cdots \\
    b_4: & \quad 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \cdots \\
    b_5: & \quad 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \cdots \\
    b_6: & \quad 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \cdots \\
    b_7: & \quad 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \cdots \\
    b_8: & \quad 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \cdots \\
    b_9: & \quad 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \cdots \\
    b_{10}: & \quad 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \cdots \\
    \vdots & \quad \\
\end{align*}
\]

Consider the “diagonal string”

\[ b = 0000100101 \cdots \]

Flip the bits,

\[ \bar{b} = 1111011010 \cdots \]

\(\bar{b}\) is not in the list (differs in the \(i\)th position from \(b_i\)), a contradiction.

Reals are Uncountable

Every real has an infinite binary representation and every infinite binary string evaluates to a real number.

\[ \text{e.g.} \quad 0.001111111111111111111 \cdots = \frac{1}{2^3} + \frac{1}{2^4} + \frac{1}{2^5} + \frac{1}{2^6} + \frac{1}{2^7} + \cdots = \frac{1}{2}. \]

That is \(|\{\text{reals in } [0, 1]\}| = |\{\text{infinite binary strings}\}| > |\mathbb{N}|.\]
Cantor took on the abstract beast Infinity. (1874)

~ 60 years later, Alan Turing asked the abstract question: What can we compute? (1936)

Every binary function $f$ on $\mathbb{N}$ corresponds to an infinite binary string $f(1)f(2)f(3)\cdots$,

<table>
<thead>
<tr>
<th>$n$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>\cdots</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f(n)$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>\cdots</td>
</tr>
</tbody>
</table>

Every program is a finite binary string. For example,

```c
int main(); // a program that does nothing
```

is the finite binary string (ASCII code)

```
011010010110111001110100001011011010110001011010010110111000101010000010100100111011
```

Programs $\leftarrow$ Countable
Functions $\leftarrow$ Uncountable $\rightarrow$ |{functions on $\mathbb{N}$}| $\gg$ |{programs}|

There are MANY MANY functions that cannot be computed by programs! Are there interesting, useful functions that cannot be computed by programs?