Infinity
  – Chapter 22
Summary of Our Stroll Through Discrete Math

- Precise statements, proofs and logic.
- **INDUCTION.**
- Recursively defined structures and Induction. (Data structures; PL)
- Sums and asymptotics. (Algorithm analysis)
- Number theory. (Cryptography; probability; fun)
- Graphs. (Relationships/conflicts; resource allocation; routing; scheduling, . . .)
- Counting. (Enumeration and brute force algorithms)
- 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

- Comparing “sizes” of sets: countable.
  - Rationals are countable.
- Uncountable
  - Infinite binary strings.
- What does Infinity have to do with computing?
“Size” of a Set: Cardinality

• There’s a reason why small kids use fingers to count
  – They map their intuitive knowledge of 2-fingers to 2 of another object

• You have an equal number of fingers on each hand
  – You can map your left hand’s fingers to your right hand’s fingers

• Recall some types of such maps

1-1, but not onto. (injection, $A \rightarrow B$) $|A| \leq |B|$

onto; not 1-1 (surjection, $A \rightarrow B$) $|A| \geq |B|$

onto and 1-1 (bijection, $A \rightarrow B$) $|A| = |B|$

not a function
“Size” of a Set: Cardinality

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>![1-1, but not onto.](injection, $A \rightarrow B$)</td>
<td>![onto; not 1-1](surjection, $A \rightarrow B$)</td>
</tr>
<tr>
<td>$</td>
<td>A</td>
</tr>
</tbody>
</table>

- **Cardinality** $|A|$ (“size”), read “cardinality of $A$,” is the number of elements for finite sets
- In general, we can define the following relations between sets:

  $|A| \leq |B|$ iff there is an injection (1-to-1) from $A$ to $B$, i.e., $f: A \rightarrow B^{\text{INJ}}$

  $|A| > |B|$ iff there is no injection (1-to-1) from $A$ to $B$

  $|A| \geq |B|$ iff there is a surjection (onto) from $A$ to $B$, i.e., $f: A \rightarrow B^{\text{SUR}}$

  $|A| = |B|$ iff there is a bijection (1-1 and onto) from $A$ to $B$, i.e., $f: A \rightarrow B^{\text{BIJ}}$

  $|A| \leq |B|$ and $|B| \leq |A|$ $\rightarrow$ $|A| = |B|$ \quad \text{[Cantor-Bernstein Theorem]}
A Countable Set’s Cardinality is at most $|\mathbb{N}|$

- Suppose we have a finite set $A = \{a_1, \ldots, a_n\}$
  - Cardinality is $|A| = n$ if and only if there is a bijection from $A$ to $\{1, \ldots, n\}$
  - Can you come up with such a function?
    $$f(a_i) = i$$

- For infinite sets: the set $A$ is countable if $|A| \leq |\mathbb{N}|$.
  - Intuitively, $A$ is “smaller than” $\mathbb{N}$
  - Sometimes we say $A$ is at most countable to include both finite and infinite sets that are “smaller than” $\mathbb{N}$

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

- You cannot skip over any elements of $A$, but you might not use every element of $\mathbb{N}$
A Countable Set’s Cardinality is at most $|\mathbb{N}|$, cont’d

- To prove that a function $f: A \mapsto \mathbb{N}$ is an injection:
  - Assume $f$ is not an injection. (Proof by contradiction.)
  - This means there is a pair $x, y \in A$ for which $x \neq y$ and $f(x) = f(y)$
  - Use $f(x) = f(y)$ to prove that $x = y$, a contradiction. Hence, $f$ is an injection
All Finite Sets are Countable

• Suppose $A = \{3, 6, 8\}$
  
  – To show $|A| \leq |\mathbb{N}|$, we give an injection from $A$ to $\mathbb{N}$
  $\begin{align*}
  3 &\mapsto 1, \quad 6 \mapsto 23134, \quad 8 \mapsto 8
  \end{align*}$

• For an arbitrary set $A = \{a_1, \ldots, a_n\}$
  $\begin{align*}
  a_1 &\mapsto 1, \quad a_2 \mapsto 2, \ldots, \quad a_n \mapsto n
  \end{align*}$
Non-negative integers $\mathbb{N}_0 = \{0, 1, 2, \ldots \}$ are countable

- How can this be??
  - I know for a fact that $\mathbb{N}_0$ contains every element in $\mathbb{N}$, plus an extra 0
  - It’s clearly bigger!!

- Well, if they were finite sets, I would agree. But let’s recall the definition.

- To prove that $|\mathbb{N}_0| \leq |\mathbb{N}|$, we need an injection $f: \mathbb{N}_0 \rightarrow \mathbb{N}$
  - Ideas?
  - Let’s try $f(x) = x + 1$, $\forall x \in \mathbb{N}_0$

- **Proof.**
  - Assume $f$ is not an injection. So, there are $x \neq y$ in $\mathbb{N}_0$ with $f(x) = f(y)$:
    $$x + 1 = f(x) = f(y) = y + 1$$
  - But that means $x + 1 = y + 1$, i.e., $x = y$. Contradiction.

- Also, we know that $|\mathbb{N}| \leq |\mathbb{N}_0|$ since $\mathbb{N} \subseteq \mathbb{N}_0$

- By the Cantor-Bernstein Theorem, $\mathbb{N} = \mathbb{N}_0$

\[
\begin{array}{cccccccccc}
\mathbb{N}_0 & : & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \ldots \\
\mathbb{N} & : & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \ldots \\
\end{array}
\]
• Huh? The even numbers are exactly half of all natural numbers!!

\[ E = \{2, 4, 6, \ldots \}, \text{ so surely } |E| = \frac{1}{2} \mathbb{N}!! \]

• Turns out, not quite. Can you see a bijection?
  – The bijection \( f(x) = \frac{1}{2} x \) proves \(|E| = |\mathbb{N}|\)

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

• OK, fine, but all integers?? It has to be the case that \(|\mathbb{Z}| = 2|\mathbb{N}|!!\)
  – Is there a bijection? ☺
  – Recall the integers are \( \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots \} \)

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

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

• What does it mean for a set to be “listed”?  
  – You know the exact position of each element in the set  
  – Regardless of whether the set is finite or infinite

• For example:
  – \{3, 6, 8\} is a list (why?)  
    • (because it’s a finite set)  
  – \(E = \{2, 4, 6, \ldots\}\) is a list (why?)  
    • element \(i\) is just \(2i\)
  – What about \(\mathbb{Z}\)?  
    • Suppose I represent it as \{..., −3, −2, −1, 0, 1, 2, 3, ...\}  
      – Unclear what the indices are  
    • Suppose I represent it as \{0, −1, 1, −2, 2, ...\}  
      – Element 1 is 0, o.w. it is \(-i/2\) (if is even), \((i − 1)/2\) (if \(i\) is odd)
Every Countable Set Can Be “Listed”, cont’d

• Suppose I give you the following mapping between sets $A$ and $\mathbb{N}$

$$
\begin{align*}
A &: \quad \bullet \quad \star \quad \odot \quad \times \quad \circ \quad \diamond \quad \triangle \quad \square \quad \vdots \\
\mathbb{N} &: \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \quad 11 \quad 12 \quad 13 \quad 14 \quad 15 \quad 16 \quad 17 \quad 18 \quad 19 \quad 20 \quad \cdots
\end{align*}
$$

– How do I “list” $A$?
– Order elements according to their assigned value

• In general, a set can be “listed” if
  – Different elements are assigned to different list-positions.
  – We can determine the list-position of any element in the set.
Union of Two Countable Sets is Countable

• Consider two countable sets, $A$ and $B$
  – They are countable, so I can write $A = \{a_1, a_2, a_3, \ldots \}$ and $B = \{b_1, b_2, b_3, \ldots \}$

• Now, let’s look at the union
  \[ A \cup B = \{a_1, a_2, a_3, \ldots, b_1, b_2, b_3, \ldots \} \]
  – Hm, how do I show this is countable?
  – Can’t use “…” twice
  – How do I reorder terms?
  – Need to know the position of each $b_i$

• Here’s a better reordering:
  \[ A \cup B = \{a_1, b_1, a_2, b_2, a_3, b_3, \ldots \} \]
  – Now I know the position of each element
  – List-position of $a_i$ is $2i - 1$
  – List-position of $b_i$ is $2i$

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

- OK, this one is very surprising!
  - There are **infinitely** many rationals between every two integers!
  - The rationals are dense (there is a rational between any two rationals)!
  - Natural numbers are not!
  - Also, the set of rationals can be expressed as the product of integers and natural numbers:
    - \(|\mathbb{Q}| = |\mathbb{N}| \times |\mathbb{Z}|\), so of course \(|\mathbb{Q}| \gg |\mathbb{N}|\)??
- Well, let’s see...
Rationals are Countable: \(|\mathbb{Q}| = |\mathbb{N}|\), cont’d

### How do I “list” all rationals?

- I need a list that visits each rational \textit{exactly} once!
- I need to know each rational’s position \textit{exactly}

\[
\mathbb{Q} = \left\{ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ \frac{1}{1'} \ \frac{1}{2'} \ \frac{2}{2'} \ \frac{3}{3'} \ \frac{3}{3'} \ldots \right\}
\]

\(|\{\text{Rational Values}\}| \leq |\mathbb{Q}| \leq |\mathbb{N}|\)

### 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
  – How do I list them?
    • Start with the empty string (duh…)
    • Then list all strings of length 1, length 2, etc.

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

• I now know the exact position of every string!

• Exercise. 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 string’s numerical value:

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

  – Show:

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

• Wait a second… We keep seeing larger and larger sets that are countable!!

\( \mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathcal{B} \)

  – SURELY EVERYTHING IS COUNTABLE!?!
Infinite Binary Strings Are Uncountable!

• One of the most cool results in computational theory

• Cantor’s Diagonal Argument: Assume there is a list of all infinite binary strings

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

• We’ll now show that there exists a string that cannot be in that list!

• Look at the (red) diagonal string:
  \[ b = 0000100101 \cdot \]

• What’s so special about this string?
  – Let’s flip the bits
    \[ \bar{b} = 1111011010 \cdot \]
  – This string is not in the list!
  – Differs from each string \( b_i \) in position \( i \)
The Real Numbers are Uncountable

• Every real between 0 and 1 has an infinite binary representation and every infinite binary string evaluates to a real number

  \[ 0.0011111111111111 \cdots = \frac{1}{2^3} + \frac{1}{2^4} + \frac{1}{2^5} + \frac{1}{2^6} + \cdots = \frac{1}{4} \]

• This means

  \[ |\{\text{reals in [0,1]}\}| = |\{\text{infinite binary strings}\}| > |\mathbb{N}| \]

• Aha, found one!

• **Brain-breaking exercise (Continuum Hypothesis).** Prove that there is no set \( \mathcal{R} \) s.t.

  \[ |\{\text{reals in [0,1]}\}| > |\mathcal{R}| > |\mathbb{N}| \]
• Cantor took on the abstract beast Infinity. (1874)
• ~60 years later, Alan Turing asked the abstract question: What can we compute? (1936)
• For example, consider the set of binary functions \( f \) defined on \( \mathbb{N} \)

\[
\begin{array}{cccccccccccc}
n: & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots \\
f(n): & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & \cdots \\
\end{array}
\]

– Turns out the set of all such functions is uncountable
  • Corresponds to the set of all infinite binary strings
• Every program is a finite binary string. For example:

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

– This program corresponds to the finite binary string (ASCII code)

\[
0110100101101110011101000010110100001011101001001000100100111011
\]

• So, the number of programs is countable
  – But the number of functions is uncountable!
• There are many more functions than we can write/compute!
• There are MANY MANY functions that cannot be computed by programs!
• Are there interesting, useful functions that cannot be computed by programs?