Chapter 6 roadmap:
▶ Recursive definitions and types (Monday)
▶ Structural induction (Wednesday)
▶ Mathematical induction (Today)
▶ Loop invariant proofs (next week Monday and Wednesday)

Last time we saw self-referential proofs for propositions quantified over recursively defined sets, structural induction.

Today we see self-referential proofs for propositions quantified over the natural numbers and whole numbers.
▶ Opening examples and observations
▶ General form of mathematical induction
▶ Comments on the term induction
▶ Other examples, including on sets
Conjecture:

\[ \forall n \in \mathbb{N}, \sum_{i=1}^{n} (2i - 1) = n^2 \]

\[ \sum_{i=1}^{5} (2i - 1) = (2 \cdot 1 - 1) + (2 \cdot 2 - 1) + (2 \cdot 3 - 1) + (2 \cdot 4 - 1) + (2 \cdot 5 - 1) = 1 + 3 + 5 + 7 + 9 \]

Recall the Peano definition of \( \mathbb{W} \). Similarly for \( \mathbb{N} \): \( n \in \mathbb{N} \) if \( n = 1 \) or \( n = x + 1 \) for some \( x \in \mathbb{N} \).
∀ \ n \in \mathbb{N}, \sum_{i=1}^{n}(2i - 1) = n^2

Proof.
Suppose \ n \in \mathbb{N}. Then either \ n = 1 \ or \ there \ exists \ n \in \mathbb{N} such that \ n = x + 1.

Base case. Suppose \ n = 1. Then \ \sum_{i=1}^{1}(2i - 1) = 2 - 1 = 1 = 1^2.

Inductive case. Suppose \ n = x + 1 such that \ x \in \mathbb{N} and \ \sum_{i=1}^{x}(2i - 1) = x^2.

Then \ \sum_{i=1}^{n}(2i - 1) = 2n - 1 + \sum_{i=1}^{n-1}(2i - 1)
by definition of summation
= 2n - 1 + \sum_{i=1}^{x}(2i - 1)
by substitution
= 2n - 1 + x^2
by the inductive hypothesis
= 2n - 1 + (n - 1)^2
by substitution
= 2n - 1 + n^2 - 2n + 1
by algebra (FOIL)
= n^2
by algebra (cancellation)
∀ \( n \in \mathbb{N} \), \( \sum_{i=1}^{n}(2i - 1) = n^2 \)

**Proof.** Suppose \( n \in \mathbb{N} \). Then either \( n = 1 \) or there exists \( n \in \mathbb{N} \) such that \( n = x + 1 \).

**Base case.** Suppose \( n = 1 \). Then

\[
\sum_{i=1}^{n}(2i - 1) = 2 - 1 = 1 = 1^2
\]

**Inductive case.** Suppose \( n = x + 1 \) such that \( x \in \mathbb{N} \) and \( \sum_{i=1}^{x}(2i - 1) = x^2 \). Then

\[
\sum_{i=1}^{n}(2i - 1) = 2n - 1 + \sum_{i=1}^{n-1}(2i - 1) \quad \text{by definition of summation}
\]

\[
= 2n - 1 + \sum_{i=1}^{x}(2i - 1) \quad \text{by substitution}
\]

\[
= 2n - 1 + x^2 \quad \text{by the inductive hypothesis}
\]

\[
= 2n - 1 + (n - 1)^2 \quad \text{by substitution}
\]

\[
= 2n - 1 + n^2 - 2n + 1 \quad \text{by algebra (FOIL)}
\]

\[
= n^2 \quad \text{by algebra (cancellation)} \quad \square
\]
\[
\begin{align*}
4 \mid 0 & \quad 0 + 1 = 1 = 5^0 \\
4 \mid 4 & \quad 4 + 1 = 5 = 5^1 \\
4 \mid 24 & \quad 24 + 1 = 25 = 5^2 \\
4 \mid 124 & \quad 124 + 1 = 125 = 5^3 \\
4 \mid 624 & \quad 624 + 1 = 625 = 5^4
\end{align*}
\]

Conjecture: \( \forall \ n \in \mathbb{W}, \ 4 \mid 5^n - 1 \)
\[ \forall n \in \mathbb{W}, \ 4 \mid 5^n - 1 \]
∀ \( n \in \mathbb{W} \), \( 4|5^n - 1 \)

**Proof.** By induction on \( n \).

**Base case.** Suppose \( n = 0 \). Then \( 5^0 - 1 = 1 - 1 = 0 = 4 \cdot 0 \). Hence \( 4|5^0 - 1 \) by the definition of divides.

**Inductive case.** Suppose \( n > 0 \) and \( 4|5^{n-1} - 1 \). Then, by definition of divides, there exists \( k \in \mathbb{W} \) such that \( 5^{n-1} - 1 = 4k \). Moreover,

\[
5^n - 1 = 5 \cdot 5^{n-1} - 1
\]

by algebra, unless otherwise noted. . .

\[
= 5 \cdot (5^{n-1} - 1 + 1) - 1
\]

\[
= 5(4k + 1) - 1
\]

by the inductive hypothesis

\[
= 5 \cdot 4 \cdot k + 5 - 1
\]

\[
= 5 \cdot 4 \cdot k + 4
\]

\[
= 4(5k + 1)
\]

Hence \( 4|5^n - 1 \) by definition of divides. \( \square \)
\[ \forall n \in \mathbb{W}, \ 4|5^n - 1 \]

**Proof.** By induction on \( n \).

**Base case.** Suppose \( n = 0 \). Then \( 5^0 - 1 = 1 - 1 = 0 = 4 \cdot 0 \). Hence \( 4|5^0 - 1 \) by the definition of divides.

**Inductive case.** Suppose \( 4|5^n - 1 \) for some \( n \geq 0 \). Then, by definition of divides, there exists \( k \in \mathbb{W} \) such that \( 5^n - 1 = 4k \). Moreover,

\[
5^{n+1} - 1 = 5 \cdot 5^n - 1 \quad \text{by algebra, unless otherwise noted.}\ldots
= 5 \cdot (5^n - 1 + 1) - 1
= 5(4k + 1) - 1 \quad \text{by the inductive hypothesis}
= 5 \cdot 4 \cdot k + 5 - 1
= 5 \cdot 4 \cdot k + 4
= 4(5k + 1)
\]

Hence \( 4|5^{n+1} - 1 \) by definition of divides. \( \square \)
To prove $\forall \ n \in \mathbb{W}, I(n)$,

- Show $I(0)$

- Show $\forall \ n \in \mathbb{W}, I(n) \rightarrow I(n+1)$, that is
  
  Suppose $n \geq 0$ such that $I(n)$
  
  $I(n+1)$
  
  Alternately, show $\forall n \in \mathbb{W}$ such that $n > 0$, $I(n-1) \rightarrow I(n)$, that is
  
  Suppose $n \geq 0$ such that $I(n-1)$
  
  $I(n)$

- Conclude $\forall \ n \in \mathbb{W}, I(n)$

The principle of mathematical induction is

$$[I(0) \land \forall \ n \in \mathbb{W}, I(n) \rightarrow I(n+1)] \rightarrow [\forall \ n \in \mathbb{W}, I(n)]$$
\[
\begin{align*}
\sum_{i=1}^{1} i &= 1 &= 1 &= \frac{1 \cdot 2}{2} \\
\sum_{i=1}^{2} i &= 1 + 2 &= 3 &= \frac{2 \cdot 3}{2} \\
\sum_{i=1}^{3} i &= 1 + 2 + 3 &= 6 &= \frac{3 \cdot 4}{2} \\
\sum_{i=1}^{4} i &= 1 + 2 + 3 + 4 &= 10 &= \frac{4 \cdot 5}{2} \\
\sum_{i=1}^{5} i &= 1 + 2 + 3 + 4 + 5 &= 15 &= \frac{5 \cdot 6}{2}
\end{align*}
\]
Ex 6.5.1. \( \forall n \in \mathbb{N}, \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \).
Ex 6.5.1. \( \forall n \in \mathbb{N}, \quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2}. \)

**Proof.** By induction on \( n \).

**Base case.** Suppose \( n = 1 \). Then \( \sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2} \).

**Inductive case.** Suppose that for some \( n \geq 1, \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \). Then

\[
\sum_{i=1}^{n+1} i = n + 1 + \sum_{i=1}^{n} i \quad \text{by definition of summation}
\]

\[
= n + 1 + \frac{n(n+1)}{2} \quad \text{by the inductive hypothesis}
\]

\[
= \frac{2n+2+n^2+n}{2} \quad \text{by algebra}
\]

\[
= \frac{n^2+3n+2}{2}
\]

\[
= \frac{(n+1)(n+2)}{2}
\]  

□
Observe:

| $|A|$ | $|\mathcal{P}(A)|$ |
|---|---|
| $|\emptyset| = 0$ | $|\{\emptyset\}| = 1$ |
| $|\{a\}| = 1$ | $|\{\emptyset, \{a\}\}| = 2$ |
| $|\{a, b\}| = 2$ | $|\{\emptyset, \{a\}, \{b\}, \{a, b\}\}| = 4$ |
| $|\{a, b, c\}| = 3$ | $|\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}| = 8$ |
Conjecture: For any finite set $A$, $|\mathcal{P}(A)| = 2^{|A|}$.

**Theorem 6.5.** For all $n \in \mathbb{W}$, if $A$ is a set such that $|A| = n$, then $|P(A)| = 2^n$. 
Theorem 6.5. For all \( n \in \mathbb{W} \), if \( A \) is a set such that \( |A| = n \), then \( |\mathcal{P}(A)| = 2^n \).

Proof. By induction on \( n \).

Base case. Suppose \( n = 0 \). Then \( A = \emptyset \), and \( |\mathcal{P}(A)| = |\{\emptyset\}| = 1 = 2^0 \).

Inductive case. Suppose for some \( n \geq 0 \), if \( A \) is a set such that \( |A| = n \), then \( |\mathcal{P}(A)| = 2^n \). Suppose further than \( A \) is a set such that \( |A| = n + 1 \).

Since \( |A| > 0 \), let \( a \in A \). By Corollary 4.12, \( \mathcal{P}(A - \{a\}) \) and \( \{C \cup \{a\} \mid C \in \mathcal{P}(A - \{a\})\} \) make a partition of \( \mathcal{P}(A) \). Then

\[
|\mathcal{P}(A - \{a\})| = |\{C \cup \{a\} \mid C \in \mathcal{P}(A - \{a\})\}| \quad \text{by Exercise 7.9.6}
\]
\[
|A - \{a\}| = |A| - |\{a\}| \quad \text{since } \{a\} \subseteq A, \text{ and by Ex 7.9.1}
\]
\[
= n + 1 - 1 \quad \text{by supposition}
\]
\[
= n \quad \text{by arithmetic}
\]
\[
|\mathcal{P}(A - \{a\})| = 2^n \quad \text{by the inductive hypothesis}
\]
\[
|\mathcal{P}(A)| = |\mathcal{P}(A - \{a\})| + |\{C \cup \{a\} \mid C \in \mathcal{P}(A - \{a\})\}| \quad \text{by Theorem 7.12}
\]
\[
= 2^n + 2^n \quad \text{by substitution}
\]
\[
= 2^{n+1} \quad \text{by algebra.} \Box
\]
Iterated union (similar for intersection):

\[ \bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n \]

**Ex 6.6.1.** \( \forall n \in \mathbb{N} \), \( \bigcup_{i=1}^{n} A_i = \bigcap_{i=1}^{n} A_i \)

**Proof.** *By induction on* \( n \).

**Base case.** Suppose \( n = 1 \). Then

\[ \bigcup_{i=1}^{1} A_i = A_1 = \bigcap_{i=1}^{1} A_1 \]
Inductive case. Suppose \( \bigcup_{i=1}^{n} A_i = \bigcap_{i=1}^{n} A_i \) for some \( n \geq 1 \). Then

\[
\bigcup_{i=1}^{n+1} A_i = A_{n+1} \cup \bigcup_{i=1}^{n} A_i \quad \text{by definition of iterated union}
\]

\[
= \overline{A_{n+1}} \cap \bigcup_{i=1}^{n} A_i \quad \text{by Ex 4.3.13 (DeMorgan’s law of sets)}
\]

\[
= \overline{A_{n+1}} \cap \bigcap_{i=1}^{n} \overline{A_i} \quad \text{by the inductive hypothesis}
\]

\[
= \bigcap_{i=1}^{n+1} \overline{A_i} \quad \text{by the definition of iterated intersection}
\]
For next time:
    Pg 273: 6.5.(2 & 4)
    Pg 278: 6.6.(2 & 3)

Read 6.9 carefully
Skim 6.10

Take quiz (by Wednesday)