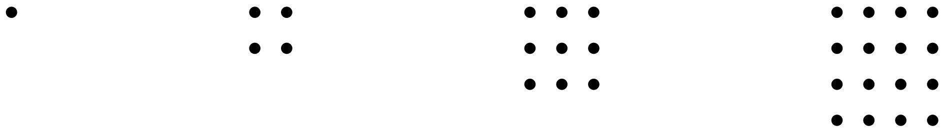
Chapter 7 outline:

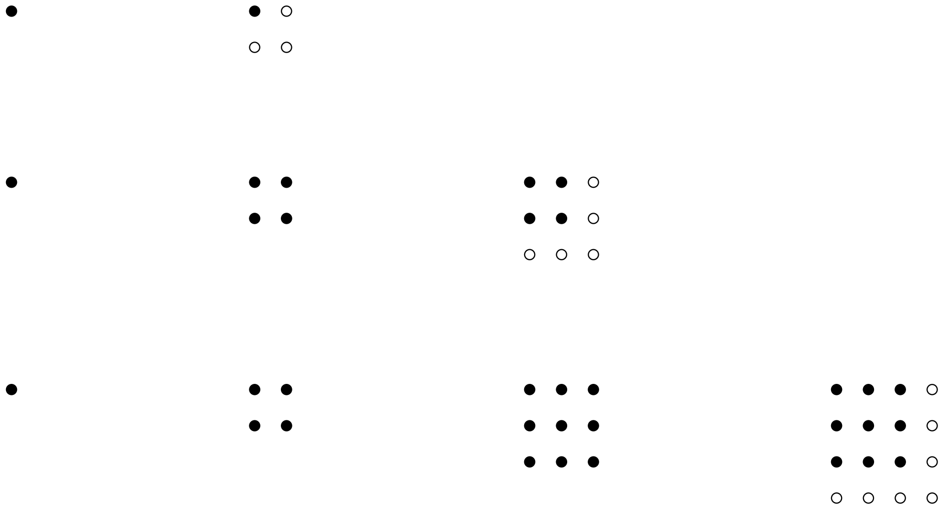
- Recursively-defined sets (last week Monday)
- Structural induction (Monday)
- Mathematical induction (**Today**)
- Non-recursive programs—loops (Friday)
- Loop invariant proofs (next week Monday)
- ~~A language processor~~ The Huffman encoding (next week Wednesday)

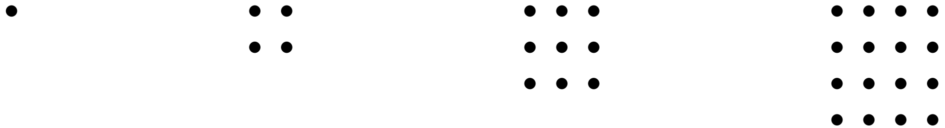
Last time we saw self-referential proofs for propositions quantified over recursively defined sets, **structural induction**.

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:

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

$$\sum_{i=1}^{5}(2i-1) = (2\cdot1-1)+(2\cdot2-1)+(2\cdot3-1)+(2\cdot4-1)+(2\cdot5-1) = 1+3+5+7+9$$

Recall the Peano definition of $\mathbb{W}$. Similarly for $\mathbb{N}$: $n \in \mathbb{N}$ if $n = 1$ or $n = x + 1$ for some $x \in \mathbb{N}$.

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

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

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*

$$\begin{array}{rcll}
\sum_{i=1}^{n}(2i-1) & = & 2n - 1 + \sum_{i=1}^{n-1}(2i-1) & \textit{by definition of summation} \\
& = & 2n - 1 + \sum_{i=1}^{x}(2i-1) & \textit{by substitution} \\
& = & 2n - 1 + x^2 & \textit{by the inductive hypothesis} \\
& = & 2n - 1 + (n-1)^2 & \textit{by substitution} \\
& = & 2n - 1 + n^2 - 2n + 1 & \textit{by algebra (FOIL)} \\
& = & n^2 & \textit{by algebra (cancellation)} \ \square
\end{array}$$

$$
\begin{array}{lrcccc}
4|0 & 0+1 & = & 1 & = & 5^0 \\
4|4 & 4+1 & = & 5 & = & 5^1 \\
4|24 & 24+1 & = & 25 & = & 5^2 \\
4|124 & 124+1 & = & 125 & = & 5^3 \\
4|624 & 624+1 & = & 625 & = & 5^4
\end{array}
$$

Conjecture: $\forall\ n \in \mathbb{W},\ 4|5^n - 1$

$\forall\ n \in \mathbb{W},\ 4 | 5^n - 1$

$\forall\ n \in \mathbb{W},\ 4|5^n - 1$

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 $n > 0$ 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,

$$
\begin{array}{rcll}
5^n - 1 & = & 5 \cdot 5^{n-1} - 1 & \text{by algebra, unless otherwise noted...} \\
& = & 5 \cdot (5^{n-1} - 1 + 1) - 1 & \\
& = & 5(4k + 1) - 1 & \text{by the inductive hypothesis} \\
& = & 5 \cdot 4 \cdot k + 5 - 1 & \\
& = & 5 \cdot 4 \cdot k + 4 & \\
& = & 4(5k + 1) &
\end{array}
$$

Hence $4|5^n - 1$ by definition of divides. □

$\forall\ n \in \mathbb{W},\ 4 | 5^n - 1$

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,

$$
\begin{aligned}
5^{n+1} - 1 &= 5 \cdot 5^n - 1 && \text{by algebra, unless otherwise noted...} \\
&= 5 \cdot (5^n - 1 + 1) - 1 \\
&= 5(4k + 1) - 1 && \text{by the inductive hypothesis} \\
&= 5 \cdot 4 \cdot k + 5 - 1 \\
&= 5 \cdot 4 \cdot k + 4 \\
&= 4(5k + 1)
\end{aligned}
$$

Hence $4 | 5^{n+1} - 1$ by definition of divides. □

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 $I(n)$

  $\vdots$

  $I(n+1)$

  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 $I(n-1)$

  $\vdots$

  $I(n)$

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

The *principle of mathematical induction* is

$$[I(0)\ \wedge\ \forall\ n \in \mathbb{W}, I(n) \rightarrow I(n+1)] \quad \rightarrow \quad [\forall\ n \in \mathbb{W}, I(n)]$$

$$\begin{aligned}
\sum_{i=1}^{1} i &= 1 &&= 1 &&= \tfrac{1\cdot 2}{2} \\
\sum_{i=1}^{2} i &= 1+2 &&= 3 &&= \tfrac{2\cdot 3}{2} \\
\sum_{i=1}^{3} i &= 1+2+3 &&= 6 &&= \tfrac{3\cdot 4}{2} \\
\sum_{i=1}^{4} i &= 1+2+3+4 &&= 10 &&= \tfrac{4\cdot 5}{2} \\
\sum_{i=1}^{5} i &= 1+2+3+4+5 &&= 15 &&= \tfrac{5\cdot 6}{2}
\end{aligned}$$

Ex 7.3.1. $\forall n \in \mathbb{N}, \quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Ex 7.3.1. $\forall n \in \mathbb{N}, \quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

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

$$
\begin{aligned}
\sum_{i=1}^{n+1} i &= n + 1 + \sum_{i=1}^{n} i && \text{by definition of summation} \\
&= n + 1 + \frac{n(n+1)}{2} && \text{by the inductive hypothesis} \\
&= \frac{2n+2+n^2+n}{2} && \text{by algebra} \\
&= \frac{n^2+3n+2}{2} && \text{``} \\
&= \frac{(n+1)(n+2)}{2} && \text{``} \qquad \square
\end{aligned}
$$

Observe:

$|A|$	$|\mathscr{P}(A)|$
$|\emptyset| = 0$	$|\{\emptyset\}| = 1$
$|\{a\}| = 1$	$|\{\emptyset, \{a\}\}| = 2$
$|\{a, b\}| = 2$	$|\{\emptyset, \{a\}, \{b\}, \{a, b\}\}| = 4$
$|\{a, b, c\}| = 3$	$|\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}s\}| = 8$

Conjecture: For any finite set A, $|\mathscr{P}(A)| = 2^{|A|}$.

Theorem 7.5. For all $n \in \mathbb{W}$, if A is a set such that $|A| = n$, then $|P(A)| = 2^n$.

Theorem 7.5. For all $n \in \mathbb{W}$, if A is a set such that $|A| = n$, then $|\mathscr{P}(A)| = 2^n$.

Proof. By induction on n.

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

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

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

$$
\begin{array}{rcll}
|\mathscr{P}(A - \{a\})| & = & |\{C \cup \{a\} \mid C \in \mathscr{P}(A - \{a\})\}| & \text{by Exercise 6.6.6} \\
|A - \{a\}| & = & |A| - |\{a\}| & \text{since } \{a\} \subseteq A\text{, and by Ex 7.3.6} \\
 & = & n + 1 - 1 & \text{by supposition} \\
 & = & n & \text{by arithmetic} \\
|\mathscr{P}(A - \{a\})| & = & 2^n & \text{by the inductive hypothesis} \\
|\mathscr{P}(A)| & = & |\mathscr{P}(A - \{a\})| & \\
 & & +|\{C \cup \{a\} \mid C \in \mathscr{P}(A - \{a\})\}| & \text{by Theorem 6.12} \\
 & = & 2^n + 2^n & \text{by substitution} \\
 & = & 2^{n+1} & \text{by algebra.}\square
\end{array}
$$

Iterated union (similar for intersection):

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

Ex 7.3.6. $\forall\ n \in \mathbb{N}, \overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A_i}$

Proof. *By induction on n.*

Base case. *Suppose $n = 1$. Then*

$$\overline{\bigcup_{i=1}^{1} A_i} = \overline{A_i} = \bigcap_{i=1}^{1} \overline{A_1}$$

Inductive case. *Suppose* $\overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A_i}$ *for some* $n \geq 1$*. Then*

$$
\begin{aligned}
\overline{\bigcup_{i=1}^{n+1} A_i} &= \overline{A_{n+1} \cup \bigcup_{i=1}^{n} A_i} && \textit{by definition of iterated union} \\
&= \overline{A_{n+1}} \cap \overline{\bigcup_{i=1}^{n} A_i} && \textit{by Ex 4.2.13 (DeMorgan's law of sets)} \\
&= \overline{A_{n+1}} \cap \bigcap_{i=1}^{n} \overline{A_i} && \textit{by the inductive hypothesis} \\
&= \bigcap_{i=1}^{n+1} \overline{A_i} && \textit{by the definition of iterated intersection}
\end{aligned}
$$

□

For next time:

Do Exercises 7.3.(2, 4, 7, 8)

Read 7.4