Chapter 4: Induction

Induction

- Stepwise induction (for $T_{PA}$, $T_{cons}$)

- Complete induction (for $T_{PA}$, $T_{cons}$)
  Theoretically equivalent in power to stepwise induction, but sometimes produces more concise proof

- Well-founded induction
  Generalized complete induction

- Structural induction
  Over logical formulae

Stepwise Induction (Peano Arithmetic $T_{PA}$)

Axiom schema (induction)

$F[0] \land (\forall n. F[n] \rightarrow F[n+1])$ \hspace{1cm} ... base case
$\rightarrow \forall x. F[x]$ \hspace{1cm} ... inductive step

for $\Sigma_{PA}$-formulae $F[x]$ with one free variable $x$.

To prove $\forall x. F[x]$, the conclusion, i.e.,
$F[x]$ is $T_{PA}$-valid for all $x \in \mathbb{N}$,
it suffices to show

- base case: prove $F[0]$ is $T_{PA}$-valid.
- inductive step: For arbitrary $n \in \mathbb{N}$,
  assume inductive hypothesis, i.e.,
  $F[n]$ is $T_{PA}$-valid,
  then prove $F[n+1]$ is $T_{PA}$-valid.

Example

Prove:

$$F[n] : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

for all $n \in \mathbb{N}$.

- Base case: $F[0] : 0 = \frac{0(0+1)}{2}$
- Inductive step: Assume $F[n] : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$, (IH) show

$$F[n+1] : 1 + 2 + \cdots + n + (n+1)$$

$$= \frac{n(n+1)}{2} + (n+1)$$

$$= \frac{n(n+1) + 2(n+1)}{2}$$

by (IH)

$$= \frac{(n+1)(n+2)}{2}$$

Therefore,

$$\forall n \in \mathbb{N}. 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$
Example: Theory $T_{\mathit{PA}}^+$ obtained from $T_{\mathit{PA}}$ by adding the axioms:

- $\forall x. x^0 = 1$ (E0)
- $\forall x, y. x^{y+1} = x^y \cdot x$ (E1)
- $\forall x, z. \exp_3(x, 0, z) = z$ (P0)
- $\forall x, y, z. \exp_3(x, y + 1, z) = \exp_3(x, y, x \cdot z)$ (P1)

$(\exp_3(x, y, z)$ stands for $x^y \cdot z)$

Prove that

$$\forall x, y. \exp_3(x, y, 1) = x^y$$

is $T_{\mathit{PA}}^+$-valid.

First attempt: $\forall y \left[ \forall x. \exp_3(x, y, 1) = x^y \right]$ $F[y]$

We chose induction on $y$. Why?

Base case: $\forall x. \exp_3(x, 0, 1) = x^0$

For arbitrary $x \in \mathbb{N}$, $\exp_3(x, 0, 1) = 1$ (P0) and $x^0 = 1$ (E0).

Inductive step: Failure.

For arbitrary $n \in \mathbb{N}$, we cannot deduce $\forall x. \exp_3(x, n + 1, 1) = x^{n+1}$

from the inductive hypothesis $\forall x. \exp_3(x, n, 1) = x^n$

Second attempt: Strengthening

Strengthened property

$$\forall x, y, z. \exp_3(x, y, z) = x^y \cdot z$$

Implies the desired property (choose $z = 1$)

$$\forall x, y. \exp_3(x, y, 1) = x^y$$

Proof of strengthened property:

Again, induction on $y$

$$\forall y \left[ \forall x, z. \exp_3(x, y, z) = x^y \cdot z \right]$$ $F[y]$

Base case:

$$\forall x, z. \exp_3(x, 0, z) = x^0 \cdot z$$

For arbitrary $x, z \in \mathbb{N}$, $\exp_3(x, 0, z) = z$ (P0) and $x^0 = 1$ (E0).

Inductive step: For arbitrary $n \in \mathbb{N}$

Assume inductive hypothesis $\forall x. \exp_3(x, n, z) = x^n \cdot z$ (IH)

prove

$$\forall x', z'. \exp_3(x', n + 1, z') = x'^{n+1} \cdot z'$$

$\uparrow$note

Consider arbitrary $x', z' \in \mathbb{N}$:

$\exp_3(x', n + 1, z') = \exp_3(x', n, x' \cdot z')$ (P1)

$$= x'^n \cdot (x' \cdot z')$$ $\text{IH } F[n]; x \mapsto x', z \mapsto x' \cdot z'$

$$= x'^{n+1} \cdot z'$$ (E1)
Stepwise Induction (Lists $T_{\text{cons}}$)

Axiom schema (induction)

$$(\forall \text{atom } u. F[u]) \land (\forall u, v. F[v] \rightarrow F[\text{cons}(u, v)])$$

... base case

... inductive step

$\rightarrow \forall x. F[x]$ ... conclusion

for $\Sigma_{\text{cons}}$-formulae $F[x]$ with one free variable $x$.

Note: $\forall$ atom $u. F[u]$ stands for $\forall u. (\text{atom}(u) \rightarrow F[u])$.

To prove $\forall x. F[x]$, i.e., $F[x]$ is $T_{\text{cons}}$-valid for all lists $x$,

it suffices to show

- **base case**: prove $F[u]$ is $T_{\text{cons}}$-valid for arbitrary atom $u$.
- **inductive step**: For arbitrary lists $u, v$,

  assume inductive hypothesis, i.e., $F[v]$ is $T_{\text{cons}}$-valid,

  then prove

  $F[\text{cons}(u, v)]$ is $T_{\text{cons}}$-valid.

---

Example: Theory $T_{\text{cons}}^+$ I

$T_{\text{cons}}$ with axioms

**Concatenating two lists**

$\triangleright \forall$ atom $u. \forall v. \text{cons}(u, v) = \text{cons}(u, v)$ (C0)

$\triangleright \forall u, v, x. \text{cons}(\text{cons}(u, v), x) = \text{cons}(u, \text{cons}(v, x))$ (C1)

---

Example: Theory $T_{\text{cons}}^+$ II

Example: for atoms $a, b, c, d$,

$$\text{cons}(\text{cons}(a, \text{cons}(b, c)), d)$$

$= \text{cons}(a, \text{cons}(\text{cons}(b, c), d))$ (C1)

$= \text{cons}(a, \text{cons}(b, \text{cons}(c, d)))$ (C1)

$= \text{cons}(a, \text{cons}(b, \text{cons}(c, d)))$ (C0)

---

Example: Theory $T_{\text{cons}}^+$ III

**Reversing a list**

$\triangleright \forall$ atom $u. \text{rvs}(u) = u$ (R0)

$\triangleright \forall x, y. \text{rvs}(\text{cons}(x, y)) = \text{cons}(\text{rvs}(y), \text{rvs}(x))$ (R1)

Example: for atoms $a, b, c$,

$$\text{rvs}(\text{cons}(a, \text{cons}(b, c)))$$

$= \text{rvs}(\text{cons}(\text{cons}(a, \text{cons}(b, c))))$ (C0)

$= \text{cons}(\text{rvs}(\text{cons}(b, c)), \text{rvs}(a))$ (R1)

$= \text{cons}(\text{cons}(\text{rvs}(c), \text{rvs}(b)), \text{rvs}(a))$ (R1)

$= \text{cons}(\text{cons}(c, b), a)$ (R0)

$= \text{cons}(\text{cons}(c, b), a)$ (C0)

$= \text{cons}(c, \text{cons}(b, a))$ (C1)

$= \text{cons}(c, \text{cons}(b, a))$ (C0)
Example: Theory $T^+_\text{cons} IV$

Deciding if a list is flat;
i.e., $\text{flat}(x)$ is true iff every element of list $x$ is an atom.

- $\forall$ atom $u$. $\text{flat}(u)$  \hspace{1cm} (F0)
- $\forall u, v$. $\text{flat}(\text{cons}(u, v)) \iff \text{atom}(u) \land \text{flat}(v)$  \hspace{1cm} (F1)

Example: for atoms $a$, $b$, $c$,

$$\text{flat}(\text{cons}(a, \text{cons}(b, c))) = \text{true}$$
$$\text{flat}(\text{cons}(\text{cons}(a, b), c)) = \text{false}$$

and prove

$$F[\text{cons}(u, v)] : \text{flat}(\text{cons}(u, v)) \rightarrow$$
$$\text{rvs}(\text{rvs}(\text{cons}(u, v))) = \text{cons}(u, v) \hspace{1cm} (\ast)$$

Case $\neg$atom($u$)

$$\text{flat}(\text{cons}(u, v)) \iff \text{atom}(u) \land \text{flat}(v) \iff \bot$$

by (F1). ($\ast$) holds since its antecedent is $\bot$.

Case atom($u$)

$$\text{flat}(\text{cons}(u, v)) \iff \text{atom}(u) \land \text{flat}(v) \iff \text{flat}(v)$$

by (F1). Now, show

$$\text{rvs}(\text{rvs}(\text{cons}(u, v))) = \cdots = \text{cons}(u, v).$$

Prove

$$\forall x. \text{flat}(x) \rightarrow \text{rvs}(\text{rvs}(x)) = x$$

is $T^+_\text{cons}$-valid.

Base case: For arbitrary atom $u$,

$$F[u] : \text{flat}(u) \rightarrow \text{rvs}(\text{rvs}(u)) = u$$

by $F0$ and $R0$.

Inductive step: For arbitrary lists $u, v$, assume the inductive
hypothesis

$$F[v] : \text{flat}(v) \rightarrow \text{rvs}(\text{rvs}(v)) = v \hspace{1cm} (\text{IH})$$

Missing steps:

$$\text{rvs}(\text{rvs}(\text{cons}(u, v)))$$
$$= \text{rvs}(\text{rvs}(\text{concat}(u, v))) \hspace{1cm} (C0)$$
$$= \text{rvs}(\text{concat}(\text{rvs}(v), \text{rvs}(u))) \hspace{1cm} (R1)$$
$$= \text{concat}(\text{rvs}(\text{rvs}(u)), \text{rvs}(\text{rvs}(v))) \hspace{1cm} (R1)$$
$$= \text{concat}(u, \text{rvs}(\text{rvs}(v))) \hspace{1cm} (R0)$$
$$= \text{concat}(u, v) \hspace{1cm} (\text{IH}, \text{since} \ \text{flat}(v))$$
$$= \text{cons}(u, v) \hspace{1cm} (C0)$$
Complete Induction (Peano Arithmetic $T_{PA}$)

**Axiom schema (complete induction)**

\[(\forall n. (\forall n'. n' < n \rightarrow F[n']) \rightarrow F[n])\]  
... inductive step

\[
\Rightarrow (\forall n. F[n])^{IH}
\]
... conclusion

for $\Sigma_{PA}$-formulae $F[x]$ with one free variable $x$.

To prove $\forall x. F[x]$, the conclusion i.e.,  $F[x]$ is $T_{PA}$-valid for all $x \in \mathbb{N}$, it suffices to show

- inductive step: For arbitrary $n \in \mathbb{N}$, assume inductive hypothesis, i.e.,  $F[n']$ is $T_{PA}$-valid for every $n' \in \mathbb{N}$ such that $n' < n$, then prove $F[n]$ is $T_{PA}$-valid.

**Proof of (1)**

$\forall x. \forall y. y > 0 \rightarrow \text{rem}(x, y) < y$

Consider an arbitrary natural number $x$.
Assume the inductive hypothesis

$\forall x'. x' < x \rightarrow \forall y'. y' > 0 \rightarrow \text{rem}(x', y') < y' \quad \text{(IH)}$

Prove $F[x]: \forall y. y > 0 \rightarrow \text{rem}(x, y) < y$.

Let $y$ be an arbitrary positive integer

Case $x < y$:

$\text{rem}(x, y) = x \quad \text{by (R0)}$

$< y \quad \text{case}$
Well-founded Induction I
A binary predicate $\prec$ over a set $S$ is a well-founded relation iff there does not exist an infinite decreasing sequence $s_1 \succ s_2 \succ s_3 \succ \cdots$ where $s_i \in S$.

Note: where $s \prec t$ iff $t \succ s$.

Examples:
- $\prec$ is well-founded over the natural numbers.
  Any sequence of natural numbers decreasing according to $\prec$ is finite:
  $1023 > 39 > 30 > 29 > 8 > 3 > 0$.
- $\prec$ is not well-founded over the rationals in $[0, 1]$.
  $1 > \frac{1}{2} > \frac{1}{3} > \frac{1}{4} > \cdots$ is an infinite decreasing sequence.

Well-founded Induction Principle
For theory $T$ and well-founded relation $\prec$,
the axiom schema (well-founded induction)

$$\forall n. (\forall n'. n' \prec n \rightarrow F[n']) \rightarrow F[n] \rightarrow \forall x. F[x]$$

for $\Sigma$-formulae $F[x]$ with one free variable $x$.

To prove $\forall x. F[x]$, i.e., $F[x]$ is $T$-valid for every $x$,
it suffices to show
- inductive step: For arbitrary $n$,
  assume inductive hypothesis, i.e.,
  $F[n']$ is $T$-valid for every $n'$, such that $n' \prec n$.
  then prove $F[n]$ is $T$-valid.

Complete induction in $T_{PA}$ is a specific instance of well-founded induction, where the well-founded relation $\prec$ is $\prec$.

Well-founded Induction II
- $\prec$ is not well-founded over the integers:
  $7200 > \cdots > 217 > \cdots > 0 > \cdots > -17 > \cdots$
- The strict sublist relation $\prec_c$ is well-founded over the set of all lists.
- The relation $F \prec G$ iff $F$ is a strict subformula of $G$.
  is well-founded over the set of formulae.

Lexicographic Relation
Given pairs $(S_i, \prec_i)$ of sets $S_i$ and well-founded relations $\prec_i$

$$(S_1, \prec_1), \ldots, (S_m, \prec_m)$$

Construct

$$S = S_1 \times \cdots \times S_m;$$

i.e., the set of $m$-tuples $(s_1, \ldots, s_m)$ where each $s_i \in S_i$.

Define lexicographic relation $\prec$ over $S$ as

$$\left(\begin{array}{c} s \\ t \end{array}\right) \prec \left(\begin{array}{c} t_1, \ldots, t_m \\ t \end{array}\right) \iff \bigvee_{i=1}^{m} \left( s_i \prec_i t_i \land \bigwedge_{j=1}^{i-1} s_j = t_j \right)$$

for $s_i, t_i \in S_i$.

- If $(S_1, \prec_1), \ldots, (S_m, \prec_m)$ are well-founded, so is $(S, \prec)$.

Example: $S = \{A, \ldots, Z\}$, $m = 3$, $CAT \prec DOG$, $DOG \prec DRY$, $DOG \prec DOT$. 
Example: For the set $\mathbb{N}^3$ of triples of natural numbers with the lexicographic relation $\prec$,

$$(5, 2, 17) \prec (5, 4, 3)$$

Lexicographic well-founded induction principle
For theory $T$ and well-founded lexicographic relation $\prec$,

$$\left( \forall \bar{n}. \left( \forall \bar{n}'. \bar{n} \prec \bar{n}' \rightarrow F[\bar{n}'] \right) \rightarrow F[\bar{n}] \right) \rightarrow \forall \bar{x}. F[\bar{x}]$$

for $\Sigma_T$-formula $F[\bar{x}]$ with free variables $\bar{x}$, is $T$-valid.

Same as regular well-founded induction, just

$n \Rightarrow$ tuple $\bar{n} = (n_1, \ldots, n_m)$ $x \Rightarrow$ tuple $\bar{x} = (x_1, \ldots, x_m)$

$n' \Rightarrow$ tuple $\bar{n}' = (n'_1, \ldots, n'_m)$

Example: Puzzle
Bag of red, yellow, and blue chips
If one chip remains in the bag – remove it (empty bag – the process terminates)
Otherwise, remove two chips at random:

1. If one of the two is red – don't put any chips in the bag

2. If both are yellow – put one yellow and five blue chips

3. If one of the two is blue and the other not red – put ten red chips

Does this process terminate?

Proof: Consider

$\Rightarrow$ Set $S : \mathbb{N}^3$ of triples of natural numbers and

► Well-founded lexicographic relation $\prec_3$ for such triples, e.g.

$$(11, 13, 3) \not\prec_3 (11, 9, 104) (11, 9, 104) \prec_3 (11, 13, 3)$$

Let $y, b, r$ be the yellow, blue, and red chips in the bag before a move.
Let $y', b', r'$ be the yellow, blue, and red chips in the bag after a move.

Show

$$(y', b', r') \prec_3 (y, b, r)$$

for each possible case. Since $\prec_3$ well-founded relation

$\Rightarrow$ only finite decreasing sequences $\Rightarrow$ process must terminate
Example: Ackermann function

Theory $T_{ack}^N$ is the theory of Presburger arithmetic $T_N$ (for natural numbers) augmented with

Ackermann axioms:

- $\forall y. \ ack(0, y) = y + 1 \quad (L0)$
- $\forall x. \ ack(x + 1, 0) = \ack(x, 1) \quad (R0)$
- $\forall x, y. \ ack(x + 1, y + 1) = \ack(x, \ack(x + 1, y)) \quad (S)$

Ackermann function grows quickly:

- $\ack(0, 0) = 1$
- $\ack(1, 1) = 3$
- $\ack(2, 2) = 7$
- $\ack(3, 3) = 61$
- $\ack(4, 4) = 2^{2^{2^{2^2}}} - 3$

Proof of termination

Let $<^2$ be the lexicographic extension of $<$ to pairs of natural numbers.

(L0) $\forall y. \ack(0, y) = y + 1$
does not involve recursive call

(R0) $\forall x. \ack(x + 1, 0) = \ack(x, 1)$
$(x + 1, 0) >^2 (x, 1)$

(S) $\forall x, y. \ack(x + 1, y + 1) = \ack(x, \ack(x + 1, y))$
$(x + 1, y + 1) >^2 (x + 1, y)$
$(x + 1, y + 1) >^2 (x, \ack(x + 1, y))$

No infinite recursive calls $\Rightarrow$ the recursive computation of $\ack(x, y)$ terminates for all pairs of natural numbers.

Proof of property

Use well-founded induction over $<^2$ to prove

$\forall x, y. \ ack(x, y) > y$

is $T_{ack}^N$ valid.

Consider arbitrary natural numbers $x, y$.

Assume the inductive hypothesis

$\forall x', y'. \ (x', y') <^2 (x, y) \Rightarrow \ack(x', y') > y' \quad (IH)$

Show

$F[x, y] : \ack(x, y) > y$.

Case $x = 0$:

$\ack(0, y) = y + 1 > y \quad$ by (L0)

Case $x > 0 \land y = 0$:

$\ack(x, 0) = \ack(x - 1, 1) \quad$ by (R0)

Since

$(x - 1, 1) <^2 (x, y)$

Then

$\ack(x - 1, 1) > 1 \quad$ by (IH) $(x' \mapsto x - 1, y' \mapsto 1)$

Thus

$\ack(x, 0) = \ack(x - 1, 1) > 1 > 0$
Case $x > 0 \land y > 0$:

$$ack(x, y) = ack(x - 1, ack(x, y - 1)) \text{ by } (S) \quad (1)$$

Since

$$\left(\frac{x - 1, ack(x, y - 1)}{x', y'}\right) < (x, y)$$

Then

$$ack(x - 1, ack(x, y - 1)) > ack(x, y - 1) \quad (2)$$

by (IH) ($x' \mapsto x - 1, y' \mapsto ack(x, y - 1)$).

Furthermore, since

$$\left(\frac{x', y - 1}{x, y'}\right) < (x, y)$$

then

$$ack(x, y - 1) > y - 1 \quad (3)$$

By (1)–(3), we have

$$ack(x, y) \overset{(1)}{=} ack(x - 1, ack(x, y - 1)) \overset{(2)}{>} ack(x, y - 1) \overset{(3)}{>} y - 1$$

Hence

$$ack(x, y) > (y - 1) + 1 = y$$

### Structural Induction

How do we prove properties about logical formulae themselves?

**Structural induction principle**

To prove a desired property of formulae,

- **inductive step**: Assume the inductive hypothesis, that for arbitrary formula $F$, the desired property holds for every strict subformula $G$ of $F$.
- Then prove that $F$ has the property.

Since atoms do not have strict subformulae, they are treated as base cases.

**Note**: “strict subformula relation" is well-founded

### Example: Prove that

Every propositional formula $F$ is equivalent to a propositional formula $F'$ constructed with only $\top, \lor, \neg$ (and propositional variables)

**Base cases:**

- $F : \top \Rightarrow F' : \top$
- $F : \bot \Rightarrow F' : \neg \top$
- $F : P \Rightarrow F' : P$ for propositional variable $P$
Inductive step:
Assume as the inductive hypothesis that \( G, G_1, G_2 \) are equivalent to \( G', G'_1, G'_2 \) constructed only from \( \top, \lor, \neg \) (and propositional variables).

\[
\begin{align*}
F : \neg G & \quad \Rightarrow \quad F' : \neg G' \\
F : G_1 \lor G_2 & \quad \Rightarrow \quad F' : G'_1 \lor G'_2 \\
F : G_1 \land G_2 & \quad \Rightarrow \quad F' : \neg (\neg G'_1 \lor \neg G'_2) \\
F : G_1 \rightarrow G_2 & \quad \Rightarrow \quad F' : \neg G'_1 \lor G'_2 \\
F : G_1 \leftrightarrow G_2 & \quad \Rightarrow \quad (G'_1 \rightarrow G'_2) \land (G'_2 \rightarrow G'_1) \Rightarrow F' : \ldots
\end{align*}
\]

Each \( F' \) is equivalent to \( F \) and is constructed only by \( \top, \lor, \neg \) by the inductive hypothesis.