The Calculus of Computation
Zohar Manna
Spring 2009

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)

$F[0] \wedge$ ... base case
$(\forall n.\ F[n] \rightarrow F[n+1])$ ... inductive step
$\rightarrow \forall x.\ F[x]$ ... conclusion

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

To prove $\forall x.\ F[x]$, the conclusion, i.e.,

$\quad$ $F[x]$ 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.,
  $\quad$ $F[n]$ is T_{PA}-valid,
  then prove
  $\quad$ $F[n+1]$ 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*: $F[0] : 0 = \frac{0 \cdot 1}{2}$
- *Inductive step*: Assume $F[n] : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$, (IH) show

$$
\begin{aligned}
F[n+1] \quad &: \quad 1 + 2 + \cdots + n + (n+1) \\
&= \frac{n(n+1)}{2} + (n+1) \qquad\qquad by \ (IH) \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2}
\end{aligned}
$$

Therefore,

$$\forall n \in \mathbb{N}. \ 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

<u>Example:</u>

Theory T_{PA}^+ obtained from T_{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 $x^y.z$)

Prove that

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

is T_{PA}^+-valid.

First attempt:

$$\forall y \; [\underbrace{\forall x. \; exp_3(x, y, 1) = x^y}_{F[y]}]$$

We chose induction on y. Why?

Base case:

   $F[0] : \; \forall x. \; exp_3(x, 0, 1) = x^0$

   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

   $F[n + 1] : \forall x. \; exp_3(x, n + 1, 1) = x^{n+1}$

   from the inductive hypothesis

   $F[n] : \forall x. \; exp_3(x, n, 1) = x^n$

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

$$\forall y\ \underbrace{[\forall x, z.\ exp_3(x, y, z) = x^y \cdot z]}_{F[y]}$$

Base case:

$$F[0]:\ \forall x, z.\ exp_3(x, 0, z) = x^0 \cdot z$$

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
$$F[n] : \forall x, z.\ exp_3(x, n, z) = x^n \cdot z \qquad \text{(IH)}$$

prove
$$F[n+1] : \forall x', z'.\ exp_3(x', n+1, z') = x'^{n+1} \cdot z'$$
$$\uparrow \text{note}$$

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

$$
\begin{aligned}
exp_3(x', n+1, z') &= exp_3(x', n, x' \cdot z') && \text{(P1)} \\
&= x'^n \cdot (x' \cdot z') && \text{IH } F[n]; x \mapsto x', z \mapsto x' \cdot z' \\
&= x'^{n+1} \cdot z' && \text{(E1)}
\end{aligned}
$$

Stepwise Induction (Lists T_{cons})

Axiom schema (induction)

$(\forall$ atom $u.\ F[u]) \wedge$ ... base case
$(\forall u, v.\ F[v] \rightarrow F[cons(u, v)])$ ... inductive step
$\rightarrow \forall x.\ F[x]$ ... conclusion

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

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

To prove $\forall x.\ F[x]$, i.e.,

     $F[x]$ is T_{cons}-valid for all lists x,

it suffices to show

▶ base case: prove $F[u]$ is T_{cons}-valid for arbitrary atom u.

▶ inductive step: For arbitrary lists u, v,
     assume inductive hypothesis, i.e.,
        $F[v]$ is T_{cons}-valid,
     then prove
        $F[cons(u, v)]$ is T_{cons}-valid.

Example: Theory T_{cons}^+ I

T_{cons} with axioms

Concatenating two lists

- $\forall$ atom u. $\forall v. concat(u, v) = cons(u, v)$ (C0)
- $\forall u, v, x.\ concat(\mathrm{cons}(u, v), x) = \mathrm{cons}(u, concat(v, x))$ (C1)

Example: Theory T_{cons}^{+} II

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

$$
\begin{aligned}
& concat(cons(a, cons(b, c)), d) \\
= \ & cons(a, concat(cons(b, c), d)) && (C1) \\
= \ & cons(a, cons(b, concat(c, d))) && (C1) \\
= \ & cons(a, cons(b, cons(c, d))) && (C0)
\end{aligned}
$$

$$
\begin{aligned}
& concat(cons(cons(a, b), c), d) \\
= \ & cons(cons(a, b), concat(c, d)) && (C1) \\
= \ & cons(cons(a, b), cons(c, d)) && (C0)
\end{aligned}
$$

Example: Theory T_{cons}^{+} III

Reversing a list

- ▶ $\forall$ atom u. $rvs(u) = u$ (R0)
- ▶ $\forall x, y$. $rvs(concat(x, y)) = concat(rvs(y), rvs(x))$ (R1)

Example: for atoms a, b, c,

$$
\begin{aligned}
& rvs(cons(a, cons(b, c)) \\
= \ & rvs(concat(a, concat(b, c))) && (C0) \\
= \ & concat(rvs(concat(b, c)), rvs(a)) && (R1) \\
= \ & concat(concat(rvs(c), rvs(b)), rvs(a)) && (R1) \\
= \ & concat(concat(c, b), a) && (R0) \\
= \ & concat(cons(c, b), a) && (C0) \\
= \ & cons(c, concat(b, a)) && (C1) \\
= \ & cons(c, cons(b, a)) && (C0)
\end{aligned}
$$

Example: Theory T_{cons}^+ IV

Deciding if a list is flat;

i.e., $flat(x)$ is true iff every element of list x is an atom.

- ▶ $\forall$ atom u. $flat(u)$ (F0)
- ▶ $\forall u, v.$ $flat(cons(u, v)) \leftrightarrow atom(u) \wedge flat(v)$ (F1)

Example: for atoms a, b, c,

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

Prove

$$\forall x. \underbrace{flat(x) \;\rightarrow\; rvs(rvs(x)) = x}_{F[x]}$$

is T^+_{cons}-valid.

<u>Base case</u>: For arbitrary atom u,

$$F[u] : flat(u) \;\rightarrow\; rvs(rvs(u)) = u$$

by $F0$ and $R0$.

<u>Inductive step</u>: For arbitrary lists u, v, assume the inductive hypothesis

$$F[v] : flat(v) \;\rightarrow\; rvs(rvs(v)) = v \qquad \text{(IH)}$$

and prove

$$F[\text{cons}(u, v)] \;:\; \text{flat}(\text{cons}(u, v)) \;\rightarrow$$
$$rvs(rvs(\text{cons}(u, v))) = \text{cons}(u, v) \qquad (*)$$

Case $\neg\text{atom}(u)$

$$\text{flat}(\text{cons}(u, v)) \;\Leftrightarrow\; \text{atom}(u) \wedge \text{flat}(v) \;\Leftrightarrow\; \bot$$

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

Case $\text{atom}(u)$

$$\text{flat}(\text{cons}(u, v)) \;\Leftrightarrow\; \text{atom}(u) \wedge \text{flat}(v) \;\Leftrightarrow\; \text{flat}(v)$$

by (F1). Now, show

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

Missing steps:

$$
\begin{aligned}
&\quad rvs(rvs(\text{cons}(u, v))) \\
&= \ rvs(rvs(concat(u, v))) &&\text{(C0)} \\
&= \ rvs(concat(rvs(v), rvs(u))) &&\text{(R1)} \\
&= \ concat(rvs(rvs(u)), rvs(rvs(v))) &&\text{(R1)} \\
&= \ concat(u, rvs(rvs(v))) &&\text{(R0)} \\
&= \ concat(u, v) &&\text{(IH), since } flat(v) \\
&= \ \text{cons}(u, v) &&\text{(C0)}
\end{aligned}
$$

Complete Induction (Peano Arithmetic T_{PA})

Axiom schema (complete induction)

$$(\forall n.\ (\underbrace{\forall n'.\ n' < n\ \rightarrow\ F[n']}_{IH})\ \rightarrow\ F[n]) \qquad \ldots \text{ inductive step}$$

$$\rightarrow\ \forall x.\ F[x] \qquad\qquad\qquad \ldots \text{ conclusion}$$

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

To prove $\forall x.\ F[x]$, the conclusion i.e.,

$\quad F[x]$ 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.,

  $\quad F[n']$ is T_{PA}-valid for every $n' \in \mathbb{N}$ such that $n' < n$,

  then prove

  $\quad F[n]$ is T_{PA}-valid.

Is base case missing?

No. Base case is implicit in the structure of complete induction.

Note:

- ▶ Complete induction is theoretically equivalent in power to stepwise induction.
- ▶ Complete induction sometimes yields more concise proofs.

Example: Integer division $\quad quot(5,3) = 1$ and $rem(5,3) = 2$

Theory T_{PA}^* obtained from T_{PA} by adding the axioms:

- ▶ $\forall x, y.\ x < y\ \rightarrow\ quot(x,y) = 0$ (Q0)
- ▶ $\forall x, y.\ y > 0\ \rightarrow\ quot(x+y,y) = quot(x,y) + 1$ (Q1)
- ▶ $\forall x, y.\ x < y\ \rightarrow\ rem(x,y) = x$ (R0)
- ▶ $\forall x, y.\ y > 0\ \rightarrow\ rem(x+y,y) = rem(x,y)$ (R1)

Prove

(1) $\forall x, y.\ y > 0\ \rightarrow\ rem(x,y) < y$

(2) $\forall x, y.\ y > 0\ \rightarrow\ x = y \cdot quot(x,y) + rem(x,y)$

Best proved by complete induction.

<u>Proof of (1)</u>

$$\forall x. \underbrace{\forall y. \; y > 0 \; \rightarrow \; rem(x, y) < y}_{F[x]}$$

<u>Consider</u> an arbitrary natural number x.

<u>Assume</u> the inductive hypothesis

$$\forall x'. \; x' < x \; \rightarrow \; \underbrace{\forall y'. \; y' > 0 \; \rightarrow \; rem(x', y') < y'}_{F[x']} \tag{IH}$$

<u>Prove</u> $F[x] : \forall y. \; y > 0 \; \rightarrow \; rem(x, y) < y$.

Let y be an arbitrary positive integer

<u>Case $x < y$:</u>

$$
\begin{aligned}
rem(x, y) \;\; &= \;\; x \qquad \text{by (R0)} \\
&< \;\; y \qquad \text{case}
\end{aligned}
$$

Case $\neg(x < y)$:

Then there is natural number n, $n < x$ s.t. $x = n + y$

$$
\begin{array}{rlll}
rem(x, y) & = & rem(n + y, y) & x = n + y \\
& = & rem(n, y) & \text{(R1)} \\
& < & y & \text{IH } (x' \mapsto n, y' \mapsto y) \\
& & & \text{since } n < x \text{ and } y > 0
\end{array}
$$

Well-founded Induction I

A binary predicate $\prec$ over a set S is a <u>well-founded relation</u> iff there does not exist an infinite decreasing sequence

$$s_1 \succ s_2 \succ s_3 \succ \cdots \text{ where } s_i \in S$$

<u>Note</u>: where $s \prec t$ iff $t \succ s$

<u>Examples</u>:

- $<$ is well-founded over the natural numbers.
  Any sequence of natural numbers decreasing according to $<$ is finite:

  $$1023 > 39 > 30 > 29 > 8 > 3 > 0.$$

- $<$ is <u>not</u> 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 II

- $<$ is not well-founded over the integers:

$$7200 > \ldots > 217 > \ldots > 0 > \ldots > -17 > \ldots$$

- The strict sublist relation $\prec_c$ is well-founded over the set of all lists.

- The relation

$$F \prec G \text{ iff } F \text{ is a strict subformula of } G$$

is well-founded over the set of formulae.

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 Σ-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 $<$.

<u>Lexicographic Relation</u>

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

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

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

Define <u>lexicographic relation</u> $\prec$ over S as

$$\underbrace{(s_1, \ldots, s_m)}_{s} \prec \underbrace{(t_1, \ldots, t_m)}_{t} \Leftrightarrow \bigvee_{i=1}^{m} \left(s_i \prec_i t_i \wedge \bigwedge_{j=1}^{i-1} s_j = t_j \right)$$

for $s_i, t_i \in S_i$.

• If $(S_1, \prec_1), \ldots, (S_m, \prec_m)$ are well-founded, so is $(S, \prec)$.
<u>Example</u>: $S = \{A, \cdots, Z\}$, $m = 3$, $CAT \prec DOG$, $DOG \prec DRY$,
$\overline{DOG \prec DOT}$.

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 $\prec$,

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

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

Same as regular well-founded induction, just

$$n \ \Rightarrow \ \text{tuple } \bar{n} = (n_1, \ldots, n_m) \quad x \ \Rightarrow \ \text{tuple } \bar{x} = (x_1, \ldots, x_m)$$
$$n' \ \Rightarrow \ \text{tuple } \bar{n}' = (n'_1, \ldots, n'_m)$$

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

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

▶ Well-founded lexicographic relation $<_3$ for such triples, e.g.

$$(11, 13, 3) \not<_3 (11, 9, 104) \qquad (11, 9, 104) <_3 (11, 13, 3)$$

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

Show

$$(y', b', r') <_3 (y, b, r)$$

for each possible case. Since $<_3$ well-founded relation
$\Rightarrow$ only finite decreasing sequences $\Rightarrow$ process must terminate

1. If one of the two removed chips is red –
   do not put any chips in the bag

$$\left.\begin{array}{c} (y-1, b, r-1) \\ (y, b-1, r-1) \\ (y, b, r-2) \end{array}\right\} <_3 (y, b, r)$$

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

$$(y-1, b+5, r) <_3 (y, b, r)$$

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

$$\left.\begin{array}{c} (y-1, b-1, r+10) \\ (y, b-2, r+10) \end{array}\right\} <_3 (y, b, r)$$

Example: Ackermann function

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

Ackermann axioms:

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

Ackermann function grows quickly:

$ack(0, 0) = 1$
$ack(1, 1) = 3$
$ack(2, 2) = 7$ $ack(4, 4) = 2^{2^{2^{2^{16}}}} - 3$
$ack(3, 3) = 61$

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 $T_{\mathbb{N}}^{ack}$ valid.

Consider arbitrary natural numbers x, y.
Assume the inductive hypothesis

$$\forall x', y'.\ \underbrace{(x', y') <_2 (x, y) \ \rightarrow\ \underbrace{ack(x', y') > y'}_{F[x', y']}}$$ (IH)

Show

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

Case $x = 0$:

$$ack(0, y) = y + 1 > y \qquad \text{by (L0)}$$

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

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

Since

$\qquad (\underbrace{x - 1}_{x'}, \underbrace{1}_{y'}) <_2 (x, y)$

Then

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

Thus

$\qquad ack(x, 0) = ack(x - 1, 1) > 1 > 0$

<u>Case $x > 0 \wedge y > 0$:</u>

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

Since

$$(\underbrace{x - 1}_{x'}, \underbrace{ack(x, y - 1)}_{y'}) <_2 (x, y)$$

Then

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

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

Furthermore, since

$$(\underbrace{x}_{x'}, \underbrace{y-1}_{y'}) <_2 (x, y)$$

then

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

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 $\top$, $\vee$, $\neg$ (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

<u>Inductive step</u>:
Assume as the <u>inductive hypothesis</u> that G, G_1, G_2 are equivalent to G', G_1', G_2' constructed only from $\top$, $\lor$, $\neg$ (and propositional variables).

$$
\begin{aligned}
F : \neg G &\Rightarrow F' : \neg G' \\
F : G_1 \lor G_2 &\Rightarrow F' : G_1' \lor G_2' \\
F : G_1 \land G_2 &\Rightarrow F' : \neg(\neg G_1' \lor \neg G_2') \\
F : G_1 \rightarrow G_2 &\Rightarrow F' : \neg G_1' \lor G_2' \\
F : G_1 \leftrightarrow G_2 &\Rightarrow (G_1' \rightarrow G_2') \land (G_2' \rightarrow G_1') \Rightarrow F' : \ldots
\end{aligned}
$$

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