

THE CALCULUS OF COMPUTATION:
Decision Procedures with
Applications to Verification

by
Aaron Bradley
Zohar Manna

Springer 2007

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)

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

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

To prove $\forall x. F[x]$, 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 the conclusion
 $F[n+1]$ is T_{PA} -valid.

Example:

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

$$\blacktriangleright \forall x. x^0 = 1 \quad (E0)$$

$$\blacktriangleright \forall x, y. x^{y+1} = x^y \cdot x \quad (E1)$$

$$\blacktriangleright \forall x, z. \text{exp}_3(x, 0, z) = z \quad (P0)$$

$$\blacktriangleright \forall x, y, z. \text{exp}_3(x, y + 1, z) = \text{exp}_3(x, y, x \cdot z) \quad (P1)$$

Prove that

$$\boxed{\forall x, y. \text{exp}_3(x, y, 1) = x^y}$$

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:

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

OK since $\exp_3(x, 0, 1) = 1$ (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

$$\boxed{\forall x, y, z. \text{exp}_3(x, y, z) = x^y \cdot z}$$

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

$$\forall x, y. \text{exp}_3(x, y, 1) = x^y$$

Again, induction on y

$$\forall y \underbrace{[\forall x, z. \text{exp}_3(x, y, z) = x^y \cdot z]}_{F[y]}$$

Base case:

$$F[0] : \forall x, z. \text{exp}_3(x, 0, z) = x^0 \cdot z$$

OK since $\text{exp}_3(x, 0, z) = z$ (P0) and $x^0 = 1$ (E0).

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

Assume inductive hypothesis

$$F[n] : \forall x, z. \text{exp}_3(x, n, z) = x^n \cdot z \quad (\text{IH})$$

prove

$$F[n+1] : \forall x, z'. \text{exp}_3(x, n+1, z') = x^{n+1} \cdot z'$$

↑

$$\text{exp}_3(x, n+1, z') = \text{exp}_3(x, n, x \cdot z') \quad (\text{P1})$$

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

$$= x^{n+1} \cdot z' \quad (\text{E1})$$

Stepwise Induction (Lists T_{cons})

Axiom schema (induction)

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

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

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 list v ,
assume inductive hypothesis, i.e.,
 $F[v]$ is T_{cons} -valid,
then prove the conclusion
 $F[\text{cons}(u, v)]$ is T_{cons} -valid for arbitrary atom u .

Example

Theory T_{cons}^+ obtained from T_{cons} by adding the axioms for concatenating two lists, reverse a list, and decide if a list is flat (i.e., $\text{flat}(x)$ is \top iff every element of list x is an atom).

- ▶ $\forall \text{ atom } u. \forall v. \text{concat}(u, v) = \text{cons}(u, v)$ (C0)
- ▶ $\forall u, v, x. \text{concat}(\text{cons}(u, v), x) = \text{cons}(u, \text{concat}(v, x))$ (C1)
- ▶ $\forall \text{ atom } u. \text{rvs}(u) = u$ (R0)
- ▶ $\forall x, y. \text{rvs}(\text{concat}(x, y)) = \text{concat}(\text{rvs}(y), \text{rvs}(x))$ (R1)
- ▶ $\forall \text{ atom } u. \text{flat}(u)$ (F0)
- ▶ $\forall u, v. \text{flat}(\text{cons}(u, v)) \leftrightarrow \text{atom}(u) \wedge \text{flat}(v)$ (F1)

Prove

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

is T_{cons}^+ -valid.

Base case: For arbitrary atom u ,

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

by R0.

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

$$F[v] : flat(v) \rightarrow rvs(rvs(v)) = v \quad (IH)$$

Prove

$$F[cons(u, v)] : flat(cons(u, v)) \rightarrow rvs(rvs(cons(u, v))) = cons(u, v) \quad (*)$$

Case $\neg atom(u)$

$$flat(cons(u, v)) \Leftrightarrow atom(u) \wedge flat(v) \Leftrightarrow \perp$$

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

Case $atom(u)$

$$flat(cons(u, v)) \Leftrightarrow atom(u) \wedge flat(v) \Leftrightarrow flat(v)$$

by (F1).

$$rvs(rvs(cons(u, v))) = \dots = cons(u, v).$$

Complete Induction (Peano Arithmetic T_{PA})

Axiom schema (complete induction)

$$(\forall n. (\forall n'. n' < n \rightarrow F[n']) \rightarrow F[n]) \quad \dots \text{ inductive step}$$

$$\rightarrow \forall x. F[x] \quad \dots \text{ conclusion}$$

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

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

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 $quot(5, 3) = 1$ 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.

Proof of (1)

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

Consider an arbitrary natural number x .

Assume the inductive hypothesis

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

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

Let y be an arbitrary positive integer

Case $x < y$:

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

Case $\neg(x < y)$:

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

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

Well-founded Induction

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

$$s_1 \succ s_2 \succ s_3 \succ \dots$$

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

Examples:

- ▶ $<$ 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 not well-founded over the rationals.

$$1 > \frac{1}{2} > \frac{1}{3} > \frac{1}{4} > \dots$$

is an infinite decreasing sequence.

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

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 $<$.

Lexicographic Relation

Given pairs of sets and well-founded relations

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

Construct

$$S = S_1 \times \dots \times S_m$$

Define lexicographic relation \prec over S as

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

for $s_i, t_i \in S_i$.

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

Lexicographic well-founded induction principle

For theory T and well-founded lexicographic relation \prec ,

$$\left[\begin{array}{l} \forall n_1, \dots, n_m. \\ \left[\left[(\forall n'_1, \dots, n'_m. (n'_1, \dots, n'_m) \prec (n_1, \dots, n_m) \rightarrow F[n'_1, \dots, n'_m]) \right] \right. \\ \left. \rightarrow F[n_1, \dots, n_m] \right] \\ \rightarrow \forall x_1, \dots, x_m. F[x_1, \dots, x_m] \end{array} \right]$$

for Σ -formula $F[x_1, \dots, x_m]$ with free variables x_1, \dots, x_m , is T -valid.

Same as regular well-founded induction, just

$$n \Rightarrow \text{tuple } (n_1, \dots, n_m).$$

Example: Puzzle

Bag of red, yellow, and blue chips

If one chip remains in the bag – remove it

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.

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

Show

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

for each possible case. Since $<_3$ well-formed 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

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

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

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

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:

$$ack(0, 0) = 1$$

$$ack(1, 1) = 3$$

$$ack(2, 2) = 7$$

$$ack(3, 3) = 61$$

$$ack(4, 4) = 2^{2^{2^{2^{16}}}} - 3$$

Let $<_2$ be the lexicographic extension of $<$ to pairs of natural numbers.

$$(L0) \quad \forall y. \text{ack}(0, y) = y + 1$$

does not involve recursive call

$$(R0) \quad \forall x. \text{ack}(x + 1, 0) = \text{ack}(x, 1) \\ (x + 1, 0) >_2 (x, 1)$$

$$(S) \quad \forall x, y. \text{ack}(x + 1, y + 1) = \text{ack}(x, \text{ack}(x + 1, y)) \\ (x + 1, y + 1) >_2 (x + 1, y) \\ (x + 1, y + 1) >_2 (x, \text{ack}(x + 1, y))$$

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

Proof of property

Use well-founded induction over $<_2$ to prove

$$\forall x, y. \text{ack}(x, y) > y$$

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

Consider arbitrary natural numbers x, y .

Assume the inductive hypothesis

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

Show

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

Case $x = 0$:

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

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

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

Since

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

Then

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

Thus

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

Case $x > 0 \wedge y > 0$:

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

Since

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

Then

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

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

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

By (1)–(3), we have

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

Hence

$$\text{ack}(x, y) > (y-1) + 1 = y$$

Structural Induction

How do we prove properties about logical formulae themselves?

Structural induction principle

To prove a desired property of FOL formulae,

inductive step: Assume the inductive hypothesis, that for arbitrary FOL 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.

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:

$$F : \top \Rightarrow F' : \top$$

$$F : \perp \Rightarrow F' : \neg\top$$

$$F : P \Rightarrow F' : P \text{ for propositional variable } P$$

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 , \vee , \neg (and propositional variables).

$$F : \neg G \Rightarrow F' : \neg G'$$

$$F : G_1 \wedge G_2 \Rightarrow F' : \neg(\neg G'_1 \vee \neg G'_2)$$

$$F : G_1 \rightarrow G_2 \Rightarrow F' : \neg G'_1 \vee G'_2$$

$$F : G_1 \leftrightarrow G_2 \Rightarrow F' : \dots$$

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