When must one strengthen one's induction hypothesis?

Logic Colloquium 2017

Anders Lundstedt   Eric Johannesson

Department of Philosophy, Stockholm University

Stockholm August 2017

Introduction

The problem of giving a precise answer to the question

> "when must one strengthen one's induction hypothesis?"

is an instance of the general problem of making precise sense of imprecise things said or thought in mathematical practice. In our opinion this general problem is philosophically interesting.

Introduction

Some imprecise things said or thought in mathematical practice:

- The proof P is essentially different from proof P'.
- Homework problem: Prove fact F using method M.
- The fact F is stronger than the fact F'.
  - The induction hypothesis H is stronger than the induction hypothesis H'.
- One must prove a fact from a class of facts X in order to prove a fact Y.
  - If you do not strengthen your induction hypothesis when proving fact F by induction then you will get stuck when trying to prove the induction step.

A proof by strengthened induction hypothesis

Define $f : \mathbb{N} \to \mathbb{N}$ such that $f(n)$ is the sum of the first n odd natural numbers:

$$f(0) \coloneqq 0,$$
$$f(n+1) \coloneqq f(n) + 2n + 1.$$

That is, we have

$$\begin{aligned} f(0) &= 0, \\ f(1) &= 1, \\ f(2) &= 1 + 3, \\ f(3) &= 1 + 3 + 5, \\ f(4) &= 1 + 3 + 5 + 7, \\ &\vdots \end{aligned}$$

A proof by strengthened induction hypothesis

Fact

$f(n)$ is a perfect square for all n: for all natural numbers n there is a natural number m such that $f(n) = m^2$.

Let us try to prove this by "straightforward induction" (that is, "without strengthening the induction hypothesis"). Thus let us try to prove the following.

- Base case: $f(0)$ is a perfect square.
- Induction step: for all natural numbers n, if $f(n)$ is a perfect square then $f(n+1)$ is a perfect square.

A proof by strengthened induction hypothesis

Proof attempt of the induction step.

- Let n be any natural number.
- Induction hypothesis: there is a natural number k such that $f(n) = k^2$.
- We want to prove that $f(n+1) = m^2$ for some natural number m.
- We have

$$\begin{aligned} f(n+1) &= f(n) + 2n + 1 && \text{(by definition)} \\ &= k^2 + 2n + 1 && \text{(by induction hypothesis)} \end{aligned}$$

but $k^2 + 2n + 1$ is not a perfect square for arbitrary natural numbers k and n so we are "stuck". □

A proof by strengthened induction hypothesis

Let us try a different approach. Our fact follows immediately from the following "stronger" fact.

Fact

$f(n) = n^2$ for all natural numbers n.

Let us try to prove this by "straightforward induction", that is let us try to prove the following.

- Base case: $f(0) = 0^2$.
- Induction step: for all natural numbers n, if $f(n) = n^2$ then $f(n+1) = (n+1)^2$.

Proof of the base case.

$f(0) = 0 = 0^2$. □

A proof by strengthened induction hypothesis

Proof of the induction step.

- Let n be any natural number.
- Induction hypothesis: $f(n) = n^2$.
- We want to prove that $f(n+1) = (n+1)^2$.
- We have

$$\begin{aligned} f(n+1) &= f(n) + 2n + 1 && \text{(by definition)} \\ &= n^2 + 2n + 1 && \text{(by induction hypothesis)} \\ &= (n+1)^2. && \square \end{aligned}$$

Proof by strengthened induction hypothesis

Empirically, what we call proofs of $\forall x.\, \varphi(x)$ by "straightforward induction" are of the form

$$\dfrac{\begin{array}{c}\vdots \\ \varphi(0)\end{array} \qquad \begin{array}{c}\vdots \\ \forall x,\ \varphi(x) \rightarrow \varphi(x+1)\end{array}}{\forall x.\, \varphi(x)} \quad .$$

Empirically, what we call proofs of $\forall x.\, \varphi(x)$ by "induction with strengthened induction hypothesis" $\psi(x)$ are of the form

$$\begin{array}{c}\dfrac{\begin{array}{c}\vdots \\ \psi(0)\end{array} \qquad \begin{array}{c}\vdots \\ \forall x,\ \psi(x) \rightarrow \psi(x+1)\end{array}}{\forall x.\, \psi(x)} \\ \vdots \\ \forall x.\, \varphi(x)\end{array} \quad .$$

Proof by strengthened induction hypothesis

Suppose there is a proof of $\forall x.\, \varphi(x)$ of the "induction with strengthened induction hypothesis" form. Then there is a proof of $\forall x.\, \varphi(x)$ of the "straightforward induction" form:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \forall x.\, \varphi(x)\end{array}}{\varphi(0)} \qquad \begin{array}{c}\vdots\\ \forall x.\, \varphi(x)\\ \vdots\\ \forall x,\ \varphi(x) \to \varphi(x+1)\end{array}}{\forall x.\, \varphi(x)}\ .$$

Some definitions

Definition

- The *full (first-order) language of arithmetic*, notation $\mathcal{L}_{\mathsf{full}}$, is the first-order language that for each natural number n has
  - a constant symbol n,
  - a function symbol f of arity $n+1$ for each function $f : \mathbb{N}^{n+1} \to \mathbb{N}$,
  - a relation symbol P of arity n for each relation $P \subseteq \mathbb{N}^n$.
- The *minimal (first-order) language of arithmetic*, notation $\mathcal{L}_{\mathsf{min}}$, is the $\mathcal{L}_{\mathsf{full}}$-reduct with signature $\langle 0, 1, 2, \ldots, S, +, \cdot, < \rangle$.
- A first-order language L is a *(first-order) language of arithmetic* if and only if L is an $\mathcal{L}_{\mathsf{min}}$-expansion and an $\mathcal{L}_{\mathsf{full}}$-reduct.

Some definitions

Definition

Let L be a language of arithmetic.

- The *standard L-model* has domain $\mathbb{N}$ and each symbol interpreted as itself.
- The L-theory *true L-arithmetic* is the theory of the standard L-model.
- Any subset of true L-arithmetic is a *theory of L-arithmetic*.

Some definitions

Definition

Let L be a language of arithmetic and let $\varphi(x)$ be an L-formula with at most one free variable x. The *induction instance* for $\varphi(x)$ is the L-sentence

$$\mathrm{IND}(\varphi) :\equiv \varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(x+1)) \rightarrow \forall x.\, \varphi(x).$$

Our characterization

Definition

Let L be a language of arithmetic and let T be a theory of L-arithmetic. Let $\varphi(x)$ and $\psi(x)$ be L-formulas both with at most one free variable x. Say that ψ *witnesses that T proves $\forall x.\, \varphi(x)$ with and only with strengthened induction hypothesis* if and only if

$$
\begin{aligned}
&(1) \qquad & T, \mathrm{IND}(\varphi) &\nvdash \forall x.\, \varphi(x), \\
&(2) \qquad & T &\vdash \varphi(0), \\
&(3) \qquad & T &\vdash \psi(0), \\
&(4) \qquad & T &\vdash \forall x,\ \psi(x) \to \psi(x+1), \\
&(5) \qquad & T &\vdash \forall x.\, \psi(x) \to \forall x.\, \varphi(x).
\end{aligned}
$$

The theory PA^-

Let L^- be the $\mathcal{L}_{\min}$-reduct with signature $\langle 0, 1, +, \cdot, < \rangle$. ($L^-$ is the language of ordered rings, if you want.) We find it very reasonable that working mathematicians take the axioms of the L^--theory PA^-, *the theory of the non-negative parts of discretely ordered rings*[1], for granted. The axioms are:

- associativity of addition: $(x + y) + z = x + (y + z)$,
- associativity of multiplication: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
- commutativity of addition: $x + y = y + x$,
- commutativity of multiplication: $x \cdot y = y \cdot x$,
- distributivity of multiplication over addition: $x \cdot (y + z) = x \cdot y + x \cdot z$,
- (continues ...)

[1] As introduced in for example Richard Kaye's *Models of Peano Arithmetic* (1991).

The theory PA^-

The axioms of PA^-, continued:

- 0 is an additive identity: $x + 0 = 0$,
- 0 is a multiplicative zero: $x \cdot 0 = 0$,
- 1 is a multiplicative identity: $x \cdot 1 = x$,
- the order is irreflexive: $x \not< x$,
- the order is transitive: $x < y \wedge y < z \rightarrow x < z$,
- the order is total: $x < y \vee x = y \vee y < x$,
- addition respects the order: $x < y \rightarrow x + z < y + z$,
- multiplication respects the order:
  $0 < z \wedge x < y \rightarrow x \cdot z < y \cdot z$,
- smaller elements can be subtracted from larger elements:
  $x < y \rightarrow \exists z.\, x + z = y$,
- $0 < 1$,
- the order is discrete: $0 < x \rightarrow x = 1 \vee 1 < x$,
- 0 is the least element: $x = 0 \vee 0 < x$.

A weak but reasonable theory of arithmetic

Let T_{min} be the $\mathcal{L}_{\text{min}}$-expansion of PA^- with the missing axioms for constants, the successor function, addition, multiplication and the order:

- $S^n(0) = n$ for all natural numbers n,
- $S(x) \neq 0$,
- $S(x) = S(y) \to x = y$,
- $x \neq 0 \to \exists y.\, x = S(y)$,
- $x + S(y) = S(x + y)$,
- $x \cdot 0 = 0$,
- $x \cdot (y + 1) = x \cdot y + x$,
- $x < y \leftrightarrow \exists z,\ 0 \neq z \wedge x + z = y$.

(We have not given any thought to whether any of the above axioms are redundant.)

A proof that requires strengthened induction hypothesis

- Let $f\colon \mathbb{N} \to \mathbb{N}$ be the same function as before (so that $f(n)$ is the sum of the first n odd natural numbers).
- Let L be $\mathcal{L}_{\text{min}}$ expanded with the function symbol f.
- Let T be the L-theory of arithmetic we get by adding our defining equations for f to T_{min}, that is

$$T \coloneqq T_{\text{min}} \cup \{f(0) = 0,\ \forall x.\, f(x+1) = f(x) + 2x + 1\}.$$

- Let $\varphi(x)$ be the L-formula expressing that $f(x)$ is a perfect square and let $\psi(x)$ be the L-formula expressing that $f(x) = x^2$, that is

$$\varphi(x) :\equiv \exists y.\, f(x) = y \cdot y,$$
$$\psi(x) :\equiv f(x) = x \cdot x.$$

A proof that requires strengthened induction hypothesis

Fact

$T \vdash \forall x,\ \psi(x) \to \psi(x+1)$.

Proof sketch.

The proof given earlier can be easily formalized in T. □

A proof that requires strengthened induction hypothesis

Fact

ψ witnesses that T proves $\forall x. \varphi(x)$ with and only with strengthened induction hypothesis.

Proof sketch.

Condition (4) is the previous fact. Conditions (2), (3) and (5) are easy to show. It remains to show condition (1). For this we exhibit a T-model of $\mathrm{IND}(\varphi)$ which is not a model of $\forall x. \varphi(x)$, as follows. $\mathbb{Z}[X]^+$, the non-negative part of the ordered polynomial ring $\mathbb{Z}[X]$, is a model of PA^-. It easy to check that its obvious expansion to an $\mathcal{L}_{\mathrm{min}}$-structure is a model of T_{min}. By cleverly intepreting f on non-constant polynomials we get a T-model satisifying $\mathrm{IND}(\varphi)$ but not $\forall x. \varphi(x)$. □