Proof by strengthened induction hypothesis

Eric Johannesson and Anders Lundstedt

CLLAM seminar 2017-06-02

1 Introduction

Sometimes, in order to a prove an arithmetical fact $\forall x \varphi(x)$ by induction, straightforward induction "does not work" and instead one "must" use a "stronger" induction hypothesis $\psi(x)$ and prove $\forall x \psi(x)$, from which $\forall x \varphi(x)$ may be derived.

To give an example, suppose we want to prove that, for all natural numbers n, the sum of the first n odd numbers is a perfect square. Straightforward induction yields the following:

1. Base case: the sum of the first 0 odd numbers is 0, which is a perfect square.

2. Inductive step: if the sum of the first n odd numbers is a perfect square k^2, then the sum of the first $n+1$ odd numbers is $k^2 + 2n + 1$. But it is not true that $k^2 + 2n + 1$ is a perfect square for all k and n. So we are stuck.

Instead, we need to prove the following stronger result by induction: for all natural numbers n, the sum of the first n odd numbers is n^2. Straightforward induction yields the following:

1. Base case: the sum of the 0 first odd numbers is 0, which is 0^2.

2. Inductive step: if the sum of the first n odd numbers is n^2, then the sum of the first $n+1$ odd numbers is $n^2 + 2n + 1 = (n+1)^2$.

2 Formal characterization

Here's how *not* to characterize the situation: there are formulas $\varphi(x)$ and $\psi(x)$ such that

1. $PA \nvdash \varphi(0) \land \forall x(\varphi(x) \to \varphi(x'))$.
2. $PA \vdash \psi(0) \land \forall x(\psi(x) \to \psi(x'))$.
3. $PA \vdash \forall x\psi(x) \to \forall x\varphi(x)$.

This situation is impossible. 2 implies $PA \vdash \forall x\psi(x)$, which by 3 yields $PA \vdash \forall x\varphi(x)$, which by pure logic yields $PA \vdash \varphi(0) \land \forall x(\varphi(x) \to \varphi(x'))$, which contradicts 1.

Instead, the situation may perhaps be characterized as follows: starting from the axioms of Peano arithmetic minus the induction axioms, we successively prove more and more theorems using logic and the rule of induction:

$$\frac{\varphi(0) \qquad \forall x(\varphi(x) \to \varphi(x'))}{\forall x\varphi(x)}$$

Suppose that, at some stage in this process of mathematical inquiry, we have reached a theory T consisting of the axioms and hitherto proved theorems. Then, as we will show, the following situation may indeed arise:

1. $T \nvdash \varphi(0) \land \forall x(\varphi(x) \to \varphi(x'))$.
2. $T \vdash \psi(0) \land \forall x(\psi(x) \to \psi(x'))$.
3. $T \vdash \forall x\psi(x) \to \forall x\varphi(x)$.

This is equivalent to the following:

1. $T, \varphi(0) \land \forall x(\varphi(x) \to \varphi(x')) \to \forall x\varphi(x) \nvdash \forall x\varphi(x)$.
2. $T \vdash \psi(0) \land \forall x(\psi(x) \to \psi(x'))$.
3. $T \vdash \forall x\psi(x) \to \forall x\varphi(x)$.

3 A non-standard model

Consider the following non-standard model $\mathcal{M}$ of Robinson arithmetic. Let $A = \{..., a_{-2}, a_{-1}, a_0, a_1, a_2, ...\}$ be a countably infinite set disjoint from the natural numbers, and let the domain of the model be $\mathbb{N} \cup A$. Let the constant 0 be interpreted as the number 0, and extend the interpretation of the function symbols $', +, \cdot$ as follows:

1. $a'_z = a_{z+1}$ for $z \in \mathbb{Z}$.
2. $a_z + n = n + a_z = a_{z+n}$ for $z \in \mathbb{Z}$ and $n \in \mathbb{N}$.

3. $a_z + a_u = a_u + a_z = a_{z+u}$ for $z, u \in \mathbb{Z}$.

4. $a_z \cdot 0 = 0 \cdot a_z = 0$ for $z \in \mathbb{Z}$.

5. $a_z \cdot n = n \cdot a_z = a_{z \cdot n}$ for $z \in \mathbb{Z}$ and $n \in \mathbb{N} - \{0\}$.

6. $a_z \cdot a_u = a_u \cdot a_z = a_{z \cdot u}$ for $z, u \in \mathbb{Z}$.

It can easily be verified that this is also a model of what we may call *minimal arithmetic*, which is the theory you get by adding commutativity, associativity and distribution laws for addition and multiplications to the axioms of Robinson arithmetic.

In order to very that 1-3 above are possible, it will suffice to find true formulas $\varphi(x)$ and $\psi(x)$ (true in the sense of being satisfied by all natural numbers in the standard model as well as the non-standard model) with the following profile:

	...	a_{-2}	a_{-1}	a_0	a_1	a_2	...
$\varphi(x)$	...	0	0	1	0	0	...
$\psi(x)$	...	0	0	0	0	0	...

Then let T be the theory you get by adding $\psi(0) \wedge \forall x(\psi(x) \rightarrow \psi(x'))$ and $\forall x \psi(x) \rightarrow \forall x \varphi(x)$ to Robinson arithmetic. Since these sentences are true in our non-standard model, this is a model of T, verifying 1-3 above. For instance, let

$$\varphi(x) := \forall y \forall z(x \neq x \cdot x \wedge y + x = z + x \rightarrow y = z)$$
$$\psi(x) := \forall y \forall z(y + x = z + x \rightarrow y = z)$$

Then we actually have the following situation (with Q being Robinson arithmetic):

1. $Q \vdash \varphi(0)$.

2. $Q \nvdash \forall x(\varphi(x) \rightarrow \varphi(x'))$.

3. $Q \vdash \psi(0) \wedge \forall x(\psi(x) \rightarrow \psi(x'))$.

4. $\vdash \forall x(\psi(x) \rightarrow \varphi(x))$.

In this case, $\psi(x)$ is stronger than $\varphi(x)$ in the strongest possible sense.

4 Proof by different induction hypothesis?

As a matter of fact, the following situations are both possible:

1. $T \nvdash \varphi(0) \wedge \forall x(\varphi(x) \to \varphi(x')$.
2. $T \vdash \psi(0) \wedge \forall x(\psi(x) \to \psi(x'))$.
3. $T \vdash \forall x\psi(x) \leftrightarrow \forall x\varphi(x)$.
4. $T \nvdash \forall x(\psi(x) \to \varphi(x))$.
5. $T \nvdash \forall x(\varphi(x) \to \psi(x))$.

and

1. $T \nvdash \varphi(0) \wedge \forall x(\varphi(x) \to \varphi(x')$.
2. $T \vdash \psi(0) \wedge \forall x(\psi(x) \to \psi(x'))$.
3. $T \vdash \forall x\psi(x) \leftrightarrow \forall x\varphi(x)$.
4. $T \nvdash \forall x(\psi(x) \to \varphi(x))$.
5. $T \vdash \forall x(\varphi(x) \to \psi(x))$.

In the former case, it suffices to find true formulas $\varphi(x)$ and $\psi(x)$ with the following profile:

	...	a_{-2}	a_{-1}	a_0	a_1	a_2	...
$\varphi(x)$	...	1	1	1	0	0	...
$\psi(x)$	...	0	0	1	1	1	...

For instance, let

$$\varphi(x) := \forall y(x > y \to x^2 \neq y^2)$$
$$\psi(x) := \forall y(x < y \to x^2 \neq y^2)$$

Observe that $\vdash \forall x\varphi(x) \leftrightarrow \forall x\psi(x)$, by simple relabeling of variables. Thus, let $T = MA + \psi(0) \wedge \forall x(\psi(x) \to \psi(x'))$.

In the latter case, it suffices to find true formulas $\varphi(x)$ and $\psi(x)$ with the following profile:

	...	a_{-2}	a_{-1}	a_0	a_1	a_2	...
$\varphi(x)$	...	0	0	1	0	0	...
$\psi(x)$	...	0	0	1	1	1	...

For instance, let

$$\varphi(x) := \forall y(x \neq y \to x^2 \neq y^2)$$
$$\psi(x) := \forall y(x < y \to x^2 \neq y^2)$$

Observe that we have

$$\vdash \forall x(\varphi(x) \to \psi(x))$$

and

$$\forall x \forall y(x < y \lor x = y \lor y < x) \vdash \forall x \varphi(x) \leftrightarrow \forall x \psi(x)$$

and also

$$\mathcal{M} \vDash \forall x \forall y(x < y \lor x = y \lor y < x)$$

Thus, let $T = MA + \forall x \forall y(x < y \lor x = y \lor y < x) + \psi(0) \land \forall x(\psi(x) \to \psi(x'))$. We then have a case were one *must* use a different induction hypotheses, and *can* use one that is *weaker*.

5 The original example

Going back to our original example, let the function $f : \mathbb{N} \to \mathbb{N}$ be defined recursively as follows:

$$f(0) = 0$$
$$f(n+1) = f(n) + 2n + 1$$

What we want to show is that, for any natural number n, there's a natural number k such that $f(n) = k^2$. In order to that, we extend the language L_{PA} with a new 1-place function symbol $\mathtt{f}$, the intended interpretation of which is f, and add the following two axioms to our theory of minimal arithmetic:

$(A1)$ $\mathtt{f}(0) = 0$.

$(A2)$ $\forall x(\mathtt{f}(x') = \mathtt{f}(x) + (0'' \cdot x)')$.

Let $\varphi(x)$ be $\exists y(\mathtt{f}(x) = y \cdot y)$ and let $\psi(x)$ be $\mathtt{f}(x) = x \cdot x$. Clearly, $\vdash \forall x \psi(x) \to \forall x \varphi(x)$. To see that this may indeed a case where, in order to prove $\forall x \varphi(x)$ by induction, one needs to use the stronger induction hypothesis $\psi(x)$, extend the non-standard model $\mathcal{M}$ of minimal arithmetic introduced earlier with an interpretation $g : \mathbb{N} \cup A \to \mathbb{N} \cup A$ of $\mathtt{f}$, defined as follows:

1. $g(0) = 0$.
2. $g(n+1) = g(n) + 2 \cdot n + 1$ for $n \in \mathbb{N}$.

3. $g(a_0) = a_1$.

4. $g(a_{n+1}) = g(a_n) + 2 \cdot a_n + 1$ for $n \in \mathbb{N}$.

5. $g(a_{n-1}) = g(a_n) + 2 \cdot a_n + 1$ for $n \in \mathbb{Z} - (\mathbb{N} - \{0\})$.

The result $\mathcal{M}'$ is a model of $MA + A1 + A2$. Moreover, we have

$$\mathcal{M}' \not\models \forall x(\exists y(\mathtt{f}(x) = y \cdot y) \to \exists y(\mathtt{f}(x') = y \cdot y))$$

as witnessed by a_0 assigned to x, and

$$\mathcal{M}' \models \forall x(\mathtt{f}(x) = x' \cdot x' \to \mathtt{f}(x') = x'' \cdot x'')$$

since $g(a_n) > a_{(n+1)^2}$ for all $n \in \mathbb{Z}$. With $T = MA + A1 + A2$, we have

$$T \nvdash \forall x(\exists y(\mathtt{f}(x) = y \cdot y) \to \exists y(\mathtt{f}(x') = y \cdot y))$$

and

$$T \vdash \mathtt{f}(0) = 0 \cdot 0 \land \forall x(\mathtt{f}(x) = x \cdot x \to \mathtt{f}(x') = x' \cdot x')$$

as desired.