When must one use a non-analytic induction hypothesis?

Eric Johannesson* Anders Lundstedt†

April 2019

Definitions, results and proofs in mathematics are (almost) always precisely formulated. On the other hand, when mathematicians talk or think about definitions, results and proofs, their formulations are not always precise. For example, a mathematician might say that a certain proof uses this or that method, without being precise about what it means for a certain proof to use a certain method. Or a mathematician might say that a certain proof is a new proof of an already established result, without being precise about what it means for two proofs to be distinct from each other.

One category of imprecise statements made in mathematical practice are statements of the form "In order to prove X one must strengthen one's induction hypothesis". One will find such statements in textbooks, in the literature on inductive theorem proving, or simply as thoughts entertained by working mathematicians when they try to prove this or that result by induction.

Hetzl and Wong (2018) have made precise sense of "T proves $\forall x.\varphi(x)$ with and only with a non-analytic induction hypothesis" for theories T and sentences $\forall x.\varphi(x)$ of first-order arithmetic. They use the terminology "non-analytic", as opposed to "strengthened", because there need not be any sense in which an induction hypothesis $\psi(x)$ with which T proves $\forall x.\varphi(x)$ is stronger than $\varphi(x)$.

Define $f_1 : \mathbb{N} \to \mathbb{N}$ and $f_2 : \mathbb{N} \to \mathbb{Q}$ by $f_1(n) \coloneqq 1 + 3 + \cdots + (2n - 1)$ and $f_2(n) \coloneqq 1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{(n+1)^2}$, respectively. We consider the following two facts.

(F1) $f_1(n)$ is a perfect square for all n.

(F2) $f_2(n) < 2$ for all n.

If one tries to prove (F1) or (F2) by "straightforward induction" one gets "stuck" when trying to prove the induction step. In both cases an easy solution is to prove a "stronger" fact. (F1) follows from the "stronger" fact: (F1') $f_1(n) = n^2$ for all n. (F2) follows from the "stronger" fact: (F2') $f_2(n) < 2 - \frac{1}{n+1}$ for all n.

Using a slight reformulation of the notions introduced by Hetzl and Wong, we show that in a precise sense, in certain circumstances (F1) must be proved

*eric.johannesson@philosophy.su.se
†anders.lundstedt@philosophy.su.se

using a non-analytic induction hypothesis. We also present some results towards similarly settling whether (F2) must be proved using a non-analytic induction hypothesis.

The *minimal (first-order) language of arithmetic*, notation $\mathcal{L}_{\min}$, is the first-order language with signature $\langle 0, 1, +, \cdot, < \rangle$. A first-order language L is a *(first-order) language of arithmetic* if and only if L is an $\mathcal{L}_{\min}$-expansion.

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

Let L be a language of arithmetic and let T be an L-theory. 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 a non-analytic induction hypothesis* if and only if

(1) $T, \mathrm{IND}(\varphi) \nvdash \forall x.\varphi(x)$,

(2) $T \vdash \varphi(0)$,

(3) $T \vdash \psi(0)$,

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

(5) $T \vdash \forall x.\psi(x) \to \forall x.\varphi(x)$.

The $\mathcal{L}_{\min}$-theory PA^- is “the theory of the non-negative parts of discretely ordered commutative rings”. Kaye (1991) provides an axiomatization.

To make precise sense of (F1), we expand $\mathcal{L}_{\min}$ to a language L_1 by adding a unary function symbol f. We then define an L_1-theory T_1:

$$T_1 \coloneqq \mathrm{PA}^- \cup \{f(0) = 0, \forall x.f(x+1) = f(x) + 2 \cdot x + 1\}.$$

Next we define L_1-formulas $\varphi_1(x)$ and $\psi_1(x)$ such that $\forall x.\varphi_1(x)$ and $\forall x.\psi_1(x)$ correspond to (F1) and (F1’), respectively:

$$\varphi_1(x) :\equiv \exists y.f(x) = y \cdot y,$$
$$\psi_1(x) :\equiv f(x) = x \cdot x.$$

Fact. ψ_1 witnesses that T_1 proves $\forall x.\varphi_1(x)$ with and only with a non-analytic induction hypothesis.

Proof. We need to show (1)–(5) of the definition. (2)–(5) are easy. For (1) we construct an L_1-model satisfying T_1 and $\mathrm{IND}(\varphi_1)$ but not $\forall x.\varphi_1(x)$. $\mathbb{Z}[X]$—the ring of polynomials in the indeterminate X and with integer coefficients—is a discretely ordered commutative ring. Thus its non-negative part $\mathbb{Z}[X]^+$ (consisting of all polynomials with a non-negative leading term) is a model of PA^-. We expand $\mathbb{Z}[X]^+$ to an L_1-model M by interpreting the function symbol f on $\mathbb{Z}[X]^+$: We let f^M be the unique function such that $M \vDash T_1$ and such that $f^M(pX - 1) = pX^2$ for all polynomials $p > 0$ (the details of this construction are left to the reader). We then have $f^M(X) = X^2 + 2X - 1$ which is not a perfect square in M so $M \not\models \forall x.\varphi_1(x)$. Since $f^M(X-1) = X^2$ is a perfect square in M we then also have $M \not\models \varphi_1(X-1) \to \varphi_1(X)$ and thus we have $M \models \mathrm{IND}(\varphi_1)$. By construction we have $M \models T_1$ so we are done. QED

Since (F2) is a statement involving rationals, a little work is needed to phrase it as a statement in first-order arithmetic. Multiplying up the denominators and turning the ellipsis into a recursion, we arrive at the following. Let L_2 be $\mathcal{L}_{\min}$ expanded with the unary function symbols g and h. The L_2-theory T_2 and the L_2-formulas $\varphi_2(x)$ and $\psi_2(x)$ are defined by

$$\begin{aligned}
\mathrm{DEF}(g) &:\equiv g(0) = 1 \land \forall x. g(x+1) = (x+2)\cdot(x+2)\cdot g(x) + h(x),\\
\mathrm{DEF}(h) &:\equiv h(0) = 1 \land \forall x. h(x+1) = (x+2)\cdot(x+2)\cdot h(x),\\
T_2 &\coloneqq \mathrm{PA}^- \cup \{\mathrm{DEF}(g), \mathrm{DEF}(h)\},\\
\varphi_2(x) &:\equiv g(x) < 2\cdot h(x),\\
\psi_2(x) &:\equiv (x+1)\cdot g(x) + h(x) \leq 2\cdot(x+1)\cdot h(x).
\end{aligned}$$

To make sense of the above, note that for the unique functions $g, h : \mathbb{N} \to \mathbb{N}$ satisfying DEF(g) and DEF(h), respectively, we have $\frac{g}{h} = f_2$. $\forall x.\varphi_2(x)$ and $\forall x.\psi_2(x)$ then corresponds to (F2) and (F2'), respectively.

Conjecture. ψ_2 witnesses that T_2 proves $\forall x.\varphi_2(x)$ with and only with a non-analytic induction hypothesis.

To settle this conjecture we cannot use the same strategy—cleverly interpreting the new function symbols on $\mathbb{Z}[X]^+$—as in the proof above. In fact, for any $M \models T_2$ that is the non-negative part of a polynomial ring $R[X]$ we have $g^M(p) = h^M(p) = 0$ for non-constant polynomials p.[1]

For future work, we would of course like to settle the above conjecture. In the proof above we used (an expansion of) $\mathbb{Z}[X]^+$ as a countermodel. This means that the proof does not work if we add to T_1 any $\mathcal{L}_{\min}$-sentence that is true in the standard model but false in $\mathbb{Z}[X]^+$. One natural and simple such sentence is "all numbers are odd or even", that is $\sigma_1 :\equiv \forall x \exists y \colon x = y + y \lor x = y + y + 1$. Thus we would be interested to settle whether the above fact remains true when σ_1 is added to T_1. More generally, we would like to see significantly more general methods for settling such conjectures, as opposed to the method of hand-crafting countermodels for each particular case.

References

Kaye, Richard (1991). *Models of Peano Arithmetic*. Clarendon Press, Oxford.

Hetzl, Stefan and Tin Lok Wong (2018). "Some observations on the logical foundations of inductive theorem proving". *Logical Methods in Computer Science* 13.4, pp. 1–26.

[1] One way to see this is as follows. Let $\alpha = g$ or let $\alpha = h$. If $\alpha^M(p) \neq 0$ for a non-constant polynomial p then the degrees of the polynomials $\alpha^M(p), \alpha^M(p-1), \alpha^M(p-2), \ldots$ would form an infinitely descending chain of natural numbers. It does not help to let M be the non-negative part of a ring $R[X, X^{-1}]$ of Laurent polynomials either, for then if $M \models T_2$ and $\alpha^M(p) \neq 0$ for some non-constant polynomial p then for some natural number n, the degree of $\alpha^M(p-n)$ must be less than its order.