Ordinal analysis of arithmetic; provable and unprovable instances of transfinite induction

Master Class Logic, Utrecht, 2006–2007, S. A. Terwijn

The following notes are meant as a supplement to Schwichtenberg [6].

Preliminaries on ordinals

- Ordinals are order types of well-orders. For a set-theoretic definition see e.g. Kunen [4]. For example ω is the order type of $(\mathbb{N}, \leq)$. Every ordinal is either 0, a successor (i.e. of the form $\alpha + 1$), or a limit.

- Ordinal arithmetic.

  $\alpha + \beta$ is the order type of $\{(0, \xi) : \xi < \alpha\} \cup \{(1, \eta) : \eta < \beta\}$ with the lexicographic order: $(i, \xi) < (j, \eta)$ if and only if $i < j$ or $i = j$ and $\xi < \eta$.

  $\alpha \cdot \beta$ is α laid out β times, i.e. the order type of $\beta \times \alpha$ with the lexicographic order. One can visualize this as β with every $\xi < \beta$ replaced by a copy of α.

  α^β is $\alpha \cdot \alpha \cdot \alpha \cdot \ldots$ (β times).

- The above operations on ordinals can be recursively defined as follows:

$$\begin{cases} \alpha + 0 = \alpha \\ \alpha + (\beta + 1) = (\alpha + \beta) + 1 \\ \alpha + \lambda = \sup\{\alpha + \xi : \xi < \lambda\} \quad \text{for } \lambda \text{ a limit.} \end{cases}$$

$$\begin{cases} \alpha \cdot 0 = 0 \\ \alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha \\ \alpha \cdot \lambda = \sup\{\alpha \cdot \xi : \xi < \lambda\} \quad \text{for } \lambda \text{ a limit.} \end{cases}$$

$$\begin{cases} \alpha^0 = 1 \\ \alpha^{\beta+1} = \alpha^\beta \cdot \alpha \\ \alpha^\lambda = \sup\{\alpha^\xi : \xi < \lambda\} \quad \text{for } \lambda \text{ a limit.} \end{cases}$$

- Note that $+$ is not commutative: $1 + \omega = \omega \neq \omega + 1$. Also $\cdot$ is not commutative: $\omega \cdot 2 = \omega + \omega \neq \omega = 2 \cdot \omega$.

- Ordinal exponentiation should not be confused with *cardinal* exponentiation: For ordinals we have $2^\omega = \sup\{2^n : n < \omega\} = \omega$, whereas for cardinals we have $2^\omega > \omega$ by Cantor's theorem.

- For an arbitrary ordinal α we define

$$\begin{aligned} \omega_0 &= 1 & \alpha_1 &= \alpha \\ \omega_{n+1} &= \omega^{\omega_n} & \alpha_{n+1} &= \omega^{\alpha_n} \\ \varepsilon_0 &= \sup\{\omega_n : n \in \omega\} & \varepsilon(\alpha) &= \sup\{\alpha_n : n \in \omega\} \end{aligned}$$

Note that $\varepsilon_0 = \varepsilon(0) = \omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}} = \min\{\xi : \omega^\xi = \xi\}$. The ordinals below ε_0 can be built up from 0 using successor, +, and the function ω^α. The build-up is unique if one uses the *Cantor normal form*:

Theorem For every ordinal $\alpha > 0$ there are unique $\alpha_1 \geq \ldots \geq \alpha_n$ such that $\alpha = \omega^{\alpha_1} + \ldots + \omega^{\alpha_n}$.

Proof. Uniqueness. Suppose that

$$\omega^{\alpha_1} + \ldots + \omega^{\alpha_n} = \omega^{\beta_1} + \ldots + \omega^{\beta_m}. \tag{1}$$

Let i be minimal such that $\alpha_i \neq \beta_i$. If such i does not exist and $n \neq m$ then clearly (1) cannot hold, so $n = m$ in this case and we have uniqueness. If i exists, without loss of generality $\alpha_i > \beta_i$. But then

$$\omega^{\alpha_i} \geq \omega^{\beta_i+1} = \omega^{\beta_i} \cdot \omega = \sup\{\omega^{\beta_i} \cdot n : n \in \omega\} > \omega^{\beta_i} \cdot n$$

for every n. Hence $\omega^{\alpha_i} > \omega^{\beta_i} + \ldots + \omega^{\beta_m}$, contradicting (1).

Existence. We prove by induction on β that every α with $0 < \alpha < \omega^\beta$ has a Cantor normal form.

$\beta = 0$. Since $\omega^0 = 1$ there is nothing to prove.

$\beta + 1$. We have $\omega^{\beta+1} = \omega^\beta \cdot \omega = \sup\{\omega^{\beta_i} \cdot n : n \in \omega\}$. By the induction hypothesis, every $\alpha < \omega^\beta$ has a Cantor normal form. We prove by induction on n that every $0 < \alpha < \omega^\beta \cdot n$ has a Cantor normal form. The base case $n = 1$ holds by induction hypothesis. Induction step $n+1$: Suppose $\alpha < \omega^\beta(n+1) = \omega^\beta \cdot n + \omega^\beta$. If $\alpha < \omega^\beta \cdot n$ we are done by induction hypothesis. Otherwise $\omega^\beta \cdot n \leq \alpha < \omega^\beta \cdot n + \omega^\beta$. But then $\alpha = \omega^\beta \cdot n + \xi$ for some $\xi < \omega^\beta$. By induction hypothesis ξ has a Cantor normal form $\omega^{\xi_1} + \ldots + \omega^{\xi_m}$. By $\xi < \omega^\beta$ all the exponents ξ_i have $\xi_i < \beta$, so it follows that α also has a Cantor normal form.

β a limit. In this case $\omega^\beta = \sup\{\omega^\gamma : \gamma < \beta\}$. If $\alpha < \omega^\beta$ then there is $\gamma < \beta$ such that $\alpha < \omega^\gamma$, so by induction hypothesis α has a Cantor normal form. □

- For $\alpha = \omega^{\alpha_1} + \ldots + \omega^{\alpha_n}$ and $\beta = \omega^{\beta_1} + \ldots + \omega^{\beta_m}$ in Cantor normal form, the *natural (or Hessenberg) sum* is defined as $\alpha \# \beta = \omega^{\gamma_1} + \ldots + \omega^{\gamma_{n+m}}$, where the γ_k are a permutation of the α_i and β_j such that $\gamma_1 \geq \ldots \geq \gamma_{n+m}$. The sum $\#$ is strictly monotone in both arguments, whereas the ordinary sum $+$ is not. This property is needed for the induction proof of the Reduction Lemma, [6, p882].

- Using the build-up of the ordinals $\alpha < \varepsilon_0$ we can code them by natural numbers $\ulcorner\alpha\urcorner < \omega$ as follows.
  $\ulcorner 0 \urcorner = 0$
  $\ulcorner\alpha\urcorner = \langle 1, \ulcorner\alpha_1\urcorner, \ldots, \ulcorner\alpha_n\urcorner\rangle$ if $\alpha = \omega^{\alpha_1} + \ldots + \omega^{\alpha_n}$.

  Note that the coding $\ulcorner\cdot\urcorner : \varepsilon_0 \longrightarrow \omega$ is not a bijection, but we will not really need that. In any case, we could easily have devised a bijective coding had we wished it.

- Define the well-order $\prec$ on (a subset of) ω by $n \prec m$ if there are $\alpha < \beta < \varepsilon_0$ such that $\ulcorner\alpha\urcorner = n$ and $\ulcorner\beta\urcorner = m$.

- The relation $\prec$ is primitive recursive since it can be defined using bounded quantification. We can also define an inverse function $o : \omega \longrightarrow \varepsilon_0$ (defined on all numbers of the form $\ulcorner\alpha\urcorner$) such that $o(\ulcorner\alpha\urcorner) = \alpha$ and $\ulcorner o(n)\urcorner = n$. Now the following functions are primitive recursive:[1]

  $\lambda n, m.\, \ulcorner o(n) + o(m)\urcorner$,

  $\lambda n, k.\, \ulcorner o(n) \cdot k\urcorner$,

  $\lambda n.\, \ulcorner \omega^{o(n)}\urcorner$.

  Thus we can discuss these operations on ε_0 within the language of arithmetic.

- Tree representations of ordinals. With every well-founded tree T (i.e. a tree without infinite branches) one can associate an ordinal by defining for every node σ, $\mathrm{ord}(\sigma) = 0$ if σ is a leaf, and

  $$\mathrm{ord}(\sigma) = \sup\big\{\mathrm{ord}(\tau) + 1 : \tau \text{ predecessor of } \sigma\big\}$$

  otherwise. This is to be taken as a definition by recursion on the well-founded partial order T, starting at the leaves. If σ is the root of T, the ordinal associated with T is $\mathrm{ord}(\sigma)$. We will denote this ordinal by $\mathrm{ord}(T)$. Tree representations of ordinals are also important in other parts of logic, e.g. for the Kleene-Suslin theorem stating that $\mathbf{\Delta}^1_1$ equals the Borel sets in descriptive set theory.

[1] Strictly speaking this is not correct since the function o is not total, but it has a primitive recursive extension.

Transfinite induction

- Let PA be *arithmetic*: It has axioms for 0, S, $+$, $\cdot$, $=$, and induction:

$$\varphi(0) \wedge \forall n\big(\varphi(n) \to \varphi(S(n))\big) \to \forall n \varphi(n).$$

  N.B. In Schwichtenberg [6], PA is called Z. This is the same as what is called PA in the syllabus (p47).

- We extend PA by allowing set variables, but no set quantification. Since there are no axioms for set variables, this is a conservative extension, which is again denoted by PA.

- For every $i \in \omega$, the term $S^i 0$ in PA is denoted by $\bar{\imath}$.

- Since the order $\prec$ is primitive recursive we can define the following arithmetical formulas:

$$\begin{aligned} n \subseteq X &\equiv \forall m\big(m \prec n \to m \in X\big) \\ \mathrm{Prog}(X) &\equiv \forall n\big(n \subseteq X \to n \in X\big) \\ \mathrm{TI}_{\prec\alpha}(X) &\equiv \mathrm{Prog}(X) \to \forall n \prec \ulcorner \alpha \urcorner (n \in X), \text{ where } \alpha < \varepsilon_0 \\ \mathrm{TI}_{\prec}(X) &\equiv \mathrm{Prog}(X) \to \forall n (n \in X) \end{aligned}$$

  Thus $\mathrm{TI}_{\prec}(X)$ formalizes transfinite induction along the well-order $\prec$.

- **Theorem** (Gentzen [1]) $\mathrm{PA} \vdash \mathrm{TI}_{\prec\alpha}(X)$ for every $\alpha < \varepsilon_0$.

  Proof. Since the sequence ω_n is cofinal in ε_0 it suffices to prove that $\mathrm{PA} \vdash \mathrm{TI}_{\prec\omega_n}(X)$ for all n.

  In the following we argue *in* PA. Above we already showed that in PA we can discuss operations such as addition on the ordinals below ε_0 by using a primitive recursive coding.

  For any formula $A(x)$ with free variable x define

$$A^+(x) = \forall y\big(\forall z \prec y\ A(z) \to \forall z \prec y + \omega^x\ A(z)\big).$$

  We write $\mathrm{Prog}(A)$ for $\mathrm{Prog}(\{x : A(x)\})$.

  Lemma 1. For any A it holds that $\mathrm{Prog}(A) \to \mathrm{Prog}(A^+)$.

To prove the lemma, suppose that $\mathrm{Prog}(A)$. For a proof of $\mathrm{Prog}(A^+)$ suppose that

$$\forall y \prec x \; A^+(y). \tag{2}$$

From this we want to prove $A^+(x)$. So suppose further

$$\forall z \prec y \; A(z) \quad \text{and} \tag{3}$$
$$z \prec y + \omega^x. \tag{4}$$

We have to prove that $A(z)$.

Case $x = 0$. In this case $z \prec y + 1$, hence $z \preccurlyeq y$. If $z \prec y$ then $A(z)$ by (3), and if $z = y$ then by (3) and $\mathrm{Prog}(A)$ also $A(z)$.

Case $x > 0$. By $z \prec y + \omega^x$ there are $v \prec x$ and $n \in \omega$ such that $z \prec y + \omega^v \cdot n$. (See the exercises. This is provable *in* PA.) Now perform ordinary induction on n to prove $\forall z \prec y + \omega^v \cdot n \; A(z)$.

$n = 0$. This is (3).

$n + 1$. Since $v \prec x$ we have $A^+(v)$ by (2), and in particular

$$\forall z \prec y + \omega^v \cdot n \; A(z) \;\to\; \forall z \prec y + \omega^v \cdot (n+1) \; A(z).$$

By the induction hypothesis we have $\forall z \prec y + \omega^v \cdot n \; A(z)$, so it follows that $\forall z \prec y + \omega^v \cdot (n+1) \; A(z)$. This concludes the case $x > 0$, and the proof of Lemma 1.

To finish the proof of the theorem, we prove by ordinary induction on n that for any formula A,

$$\mathrm{Prog}(A) \to \forall x \prec \omega_n \; A(x).$$

$n = 0$. We have $\omega_0 = 1$ so if $x \prec \omega_0$ then $x = 0$. Since $\forall y \prec 0 \; A(y)$ holds vacuously, with $\mathrm{Prog}(A)$ we obtain $A(0)$.

$n + 1$. Suppose $\mathrm{Prog}(A)$. By Lemma 1 then also $\mathrm{Prog}(A^+)$. Now apply the induction hypothesis to the formula $A^+(x)$ to obtain $\forall x \prec \omega_n \; A^+(x)$. By $\mathrm{Prog}(A^+)$ we obtain from this

$$A^+(\omega_n) \equiv \forall y \big(\forall z \prec y \; A(z) \to \forall z \prec y + \omega^{\omega_n} \; A(z)\big).$$

Taking $y = 0$ we obtain $\forall z \prec \omega_{n+1} \; A(z)$.[2] □

- **Theorem** (Gentzen [1]) $\mathrm{PA} \nvdash \mathrm{TI}_{\prec}(X)$.

  (Cf. Schwichtenberg [6, 3.6.3].)

[2] Note that in the induction step we obtain $\forall z \prec \omega_{n+1} \; A(z)$ by applying the induction hypothesis to the more complicated formula A^+ !

- The following shows precisely how much induction one needs to prove consistency. RP is the following *reflection principle*:

  $$\mathrm{Der}(x, y) \equiv x \text{ codes a PA-proof of } \varphi \text{ with } y = \ulcorner\varphi\urcorner.$$

  $$\mathrm{RP} \equiv \exists x \mathrm{Der}(x, \ulcorner\varphi\urcorner) \rightarrow \varphi$$

  The predicate $\mathrm{Der}(x, y)$ can be defined primitive recursively. The laws governing the provability predicate were completely determined in the seminal paper by Solovay [7].

  Note that RP implies the consistency of PA: take $\varphi = \perp$.

  Theorem (Kreisel and Lévy [3]) $\mathrm{PA} \vdash \mathrm{RP} \leftrightarrow \mathrm{TI}_{\prec}(X)$.

  (Cf. Schwichtenberg [6, 5.2].)

- It should be stressed that the above results about transfinite induction below ε_0 strongly depend on the natural well-order $\prec$. To weaken the claim that the ordinal ε_0 measures the strength of PA we quote the following result of Kreisel. The formula $\mathrm{TI}_{\lhd}(X)$ is defined precisely as $\mathrm{TI}_{\prec}(X)$, using $\lhd$ instead of $\prec$.

  Theorem (Kreisel [2]) There is a primitive recursive definition $\lhd$ of the standard order on ω such that $\mathrm{PA} \nvdash \mathrm{TI}_{\lhd}(X)$.

  A proof of this and related results can be found in [8].

- Another use of cut elimination is the classification of the provably computable functions of PA as the class of ε_0-recursive functions, cf. Schwichtenberg [6], section 4.

References

[1] Gerhard Gentzen, *Beweisbarkeit und Unbeweisbarkeit von Anfangsfällen der transfiniten Induktion in der reinen Zahlentheorie*, Mathematische Annalen 119 (1943) 140–161.

[2] Georg Kreisel, *Notes concerning the elements of proof theory*, course notes, UCLA, 1967–1968.

[3] Georg Kreisel and Azriel Lévy, *Reflection principles and their use for establishing the complexity of axiomatic systems*, Z. Math. Logik Grundlagen Math. 14 (1968) 97–142.

[4] Kenneth Kunen, *Set theory: An introduction to independence proofs*, North-Holland, 1983.

[5] Wolfram Pohlers, *Proof theory*, Lecture Notes in Mathematics 1407, Springer, 1989.

[6] Helmut Schwichtenberg, *Proof theory: Some applications of cut-elimination*, Chapter D2 in Handbook of Mathematical Logic, North-Holland, 1977.

[7] Robert M. Solovay, *Provability interpretations of modal logic*, Israel Journal of Mathematics 25 (1976) 287–304.

[8] Anne S. Troelstra and Helmut Schwichtenberg, *Basic proof theory*, Cambridge University Press, 1996.