Lecture Notes in Proof Theory

Work in progress

Graham E. Leigh

19th February 2024

About this text

These lecture notes are written to accompany the course *Proof Theory* given to second semester students of the *Master in Logic* at the University of Gothenburg, Sweden. This means that I assume reader is comfortable with elementary formal logic including propositional and predicate (i.e., first-order) logic and natural deduction. The first half of the text *Logical Theory* [7] covers the assumed material and more. The latter half of this course deals with Peano arithmetic and incompleteness. Although designed to be self-contained, the reader will benefit from a having seen these two topics before (see, again, *Logical Theory*).

Contents

About this text iii

1. Lend me thy proof 1

Module I. Two Calculi for Two Logics 3

2. Natural Deduction (refresher) 5

3. The sequent calculus 7

4. Properties of the sequent calculus 9

Module II. Cut elimination 11

5. Cut elimination 13
   5.1. For classical logic 13
   5.2. For intuitionistic logic 14

6. Consequences of cut elimination 15

7. Predicate logic with equality 17
   7.1. Equality in natural deduction 17
   7.2. Equality in sequent calculus 17
   7.3. Cut elimination with equality 17

8. A game of cut and mouse 19

Module III. An Introduction to Ordinal Analysis **21**

9. Arithmetic and Sequent Calculi 23
   9.1. Peano and Heyting arithmetic 23
   9.2. Sequent calculi for arithmetic 26
   9.3. Small proofs and big proofs 28

10. An ordinal interlude 33
   10.1. Elementary Ordinal Functions 36
   10.2. Elementary Ordinal Arithmetic 37
   10.3. Normal forms and natural sum 40

11. Ordinal analysis of arithmetic 45
   11.1. Infinitary cut elimination 49
   11.2. Refining cut elimination arithmetic 54

12. Transfinite induction and proof-theoretic ordinals 59
   12.1. Provable transfinite induction 59
   12.2. Bounding provable transfinite induction 63
   12.3. Cut elimination, revisited 67
   12.4. Characterisation of provable transfinite induction 68

Bibliography 69

1. Lend me thy proof

What does a proof tell about a theorem beyond its truth? If the theorem states the existence of an object to what extent does the proof isolate the object in mind? The reader will be familiar with the classical logic and the method of 'proof by contradiction' — also known by the Latin phrase *reductio ad absurdum* — whereby an existential claim can be established by showing the negative *universal* claim to be contradictory. The mere statement of a theorem does not determine whether such method of proof is used or necessary. One proof of a theorem may directly construct a witness. Another may invoke only indirect reasoning but, perhaps, rely on fewer assumptions. A third proof might be too complex to determine; it might, for instance, appeal to lemmas whose proofs you do not have access to. And only a characterisation of the mathematical theories in which the theorem holds can answer the *real* question: Can the theorem be proved *only* by indirect methods?

With logic in mind, other questions also stand out. How *complex* is logic? For that matter, what does it mean to say that one logic — or even one *proof* — is more complex than another? Neither question can be given a definite answer, but we can get a handle on them by studying, comparing and manipulating proofs. In these lecture notes I will show, for example, that every classically valid formula can be given a proof in which only subformulas of the conclusion are used. Such a proof will not, in general, be the shortest such proof nor the most concise. But it is the *simplest* in one concrete sense: it does not reference any concepts more complex than the one being proved.

The reader will also be shown situations of the opposite kind: an example of a mathematical theorem admitting an elementary proof but for which every proof necessarily refers to concepts *more* complex than the conclusion. No doubt you will have encountered such cases before although you may not have realised at the time: the scenario is arithmetic and the theorem one of many examples whose proofs (in the language of arithmetic) necessitate a stronger induction invariant than the theorem itself.

On the topic of arithmetic, I assume you won't deny me the consistency of *Peano* arithmetic, the first-order theory axiomatised by the defining equations for functions of successor, addition and multiplication, plus the axiom schema of induction. One need only observe that each axiom is a true statement about the natural numbers, that is, that the structure of the natural numbers and its elementary functions forms a model of the Peano axioms. But the standard model of arithmetic is overkill for the purpose of consistency of the Peano axioms. Gödel's incompleteness theorem presents statements in the language of arithmetic that are true yet *not* provable from the Peano axioms. So what mathematical assumptions truly underpin the consistency of Peano arithmetic and, for that matter, other mathematical theories? And thinking of *different* theories, can the deductive *power* of a theory be measured, so that one theory can be directly compared to another?

This, in a nutshell, is *Proof Theory*: the mathematical theory of formal proofs and, by extension, the mathematical theory of mathematical proofs. And through the course of this text you, dear reader, will see for yourself the delights and delicacies that only a proof conceals. Together we will taste the sweetness of the topping, break through its smooth crust and sample the richness beneath.

But the proof of the pudding is in the eating. I hope you are hungry.

Module I.

Two Calculi for Two Logics

2. Natural Deduction (refresher)

Some content

3. The sequent calculus

Some content

Negation translation magic (exercise)

4. Properties of the sequent calculus

Some content

Module II.

Cut elimination

5. Cut elimination

Here we present cut elimination for the calculi.

Cut rank, Inversion lemma and the like

5.1 First inversion lemma *Let $\vdash$ denoted provability in either* C *or* I. *The following hold for all sequents and all n, k:*

1. *If* $\vdash^n_k \Gamma \Rightarrow \Delta, \bot$ *then* $\vdash^n_k \Gamma \Rightarrow \Delta$.
2. *If* $\vdash^n_k \Gamma \Rightarrow \Delta, F \wedge G$ *then* $\vdash^n_k \Gamma \Rightarrow \Delta, F$ *and* $\vdash^n_k \Gamma \Rightarrow \Delta, G$.
3. *If* $\vdash^n_k F \wedge G, \Gamma \Rightarrow \Delta$ *then* $\vdash^n_k F, G, \Gamma \Rightarrow \Delta$.
4. *If* $\vdash^n_k F \vee G, \Gamma \Rightarrow \Delta$ *then* $\vdash^n_k F, \Gamma \Rightarrow \Delta$ *and* $\vdash^n_k G, \Gamma \Rightarrow \Delta$.
5. *If* $\vdash^n_k \Gamma \Rightarrow \Delta, F \to G$ *then* $\vdash^n_k F, \Gamma \Rightarrow \Delta, G$.
6. *If* $\vdash^n_k \Gamma \Rightarrow \Delta, \forall x F(x)$ *then* $\vdash^n_k \Gamma \Rightarrow \Delta, F(s)$ *for every term s.*
7. *If* $\vdash^n_k \exists x F(x), \Gamma \Rightarrow \Delta$ *then* $\vdash^n_k F(s), \Gamma \Rightarrow \Delta$ *for every term s.*

5.2 Second inversion lemma

1. *If* $\mathsf{C} \vdash^n_k \Gamma \Rightarrow \Delta, F \vee G$ *then* $\mathsf{C} \vdash^n_k \Gamma \Rightarrow \Delta, F, G$.
2. *If* $\mathsf{C} \vdash^n_k F \to G, \Gamma \Rightarrow \Delta$ *then* $\mathsf{C} \vdash^n_k G, \Gamma \Rightarrow \Delta$ *and* $\mathsf{C} \vdash^n_k \Gamma \Rightarrow \Delta, F$.

5.3 Third inversion lemma *If* $\mathsf{I} \vdash^n_k F \to G, \Gamma \Rightarrow \Delta$ *then* $\mathsf{I} \vdash^n_k G, \Gamma \Rightarrow \Delta$.

5.1. For classical logic

5.4 Reduction lemma for C *Suppose* $\vdash^m_k \Gamma \Rightarrow \Delta, C$ *and* $\vdash^n_k C, \Sigma \Rightarrow \Lambda$. *If* $|C| = k$ *then* $\vdash^{m+n}_k \Gamma, \Sigma \Rightarrow D, \Lambda$.

Exercise 5.1 In this exercise you will prove a strengthening of the reduction lemma and, as a consequence, obtain more precise bounds on the cost of cut elimination in classical logic.

See Canvas assign 4.

5.2. For intuitionistic logic

6. Consequences of cut elimination

Now we are getting somewhere

Interpolation theorem – Exercise.
Harrop's theorem

7. Predicate logic with equality

We haven't treated equality (yet).

7.1. Equality in natural deduction

$\mathrm{Nc}_=$ & $\mathrm{Ni}_=$.

7.2. Equality in sequent calculus

$\mathrm{I}_=$ & $\mathrm{C}_=$.

7.3. Cut elimination with equality

Hmm!

8. A game of cut and mouse

Shall we? Or should this be for inf PA?

Module III.

An Introduction to Ordinal Analysis

9. Arithmetic and Sequent Calculi

As an application of proof theory beyond logic I will give an analysis of perhaps the most important formal theory in mathematics, the theory of Peano arithmetic. Among the results we present is a syntactic characterisation of the theorems of the theory, and a proof of its consistency which does not invoke any semantic considerations. A corollary of the analysis will be a characterisation of the non-finite mathematical assumptions required to establish the consistency of Peano arithmetic.

The proof I present has its origins in Gentzen's 1938 consistency proof but employs a simplification due to Kurt Schütte (1950) whereby arithmetic is treated as a fragment of infinitary logic and a corresponding infinitary notion of sequent calculus proof.

Elementary results about this theory covered in the pre-requisite course *Logical Theory* will be stated without proof; see corresponding chapters of [7] for details.

9.1. Peano and Heyting arithmetic

9.1 Definition The *language of arithmetic* is the first-order language $\mathscr{L}_{\mathrm{A}}$ comprising the following nonlogical symbols with associated arities:

1. function symbols: $\mathsf{0}^0$, s^1, $+^2$, $\times^2$.
2. predicates: P^1.

The theory of arithmetic is formulated over predicate logic *with equality*. I will first present theory with logic given by the classical natural deduction calculus with equality $\mathsf{Nc}_=$ before presenting an equivalent presentation based on the sequent calculus $\mathsf{C}_=$. Both logics were introduced in chapter 7; see also [6, §6.5].

Henceforth, *formula* will always refer to the language of arithmetic.

9.2 Definition The Peano axioms of arithmetic are the following sentences.

- *Basic axioms:*

  PA1. $\forall x \neg(0 = \mathsf{s}x)$

  PA2. $\forall x \forall y(\mathsf{s}x = \mathsf{s}y \rightarrow x = y)$

  PA3. $\forall x(x + 0 = x)$

  PA4. $\forall x \forall y(x + \mathsf{s}y = \mathsf{s}(x + y))$

  PA5. $\forall x(x \times 0 = 0)$

  PA6. $\forall x \forall y(x \times \mathsf{s}y = (x \times y) + x)$

- *Axiom scheme of induction:*

  PA7. The universal closure of $A(0) \wedge \forall x(A(x) \rightarrow A(\mathsf{s}x)) \rightarrow \forall x A(x)$ for every formula $A(a)$.

9.3 Definition *Peano arithmetic* (PA) is theory over classical predicate logic axiomatised by the Peano axioms. I will write $\mathsf{PA} \vdash A$ to express that A is a theorem of Peano arithmetic, that is, PA $\vdash_{\mathsf{Nc}_=} A$ where PA is the set of Peano axioms. *Heyting arithmetic* (HA) is the corresponding *intuitionistic* theory, i.e., $\mathsf{HA} \vdash A$ expresses PA $\vdash_{\mathsf{Ni}_=} A$.

The predicate P is auxiliary to the language of arithmetic in that it has no intended interpretation associated to it. It plays the role of a 'free' predicate as the next proposition demonstrates.

For a formulas A and $B(a)$ in the language of arithmetic, let $A[B/P]$ mark the result of replacing each occurrence of Ps in A by $B(s)$ for every term s. That is,

$$\begin{aligned}
(Ps)[B/P] &= B(s) \\
A[B/P] &= A \quad \text{for } A \text{ any other atomic formula} \\
(A_0 \rightarrow A_1)[B/P] &= (A_0[B/P] \rightarrow A_1[B/P]) \\
(\forall x A)[B/P] &= \forall x(A[B/P]) \\
&\text{etc}
\end{aligned}$$

The following result is easy to prove.

9.4 Proposition *If* $\mathsf{PA} \vdash A$ *then* $\mathsf{PA} \vdash A[B/P]$ *for every formula* $B(a)$. *Likewise for* HA.

Proof Exercise. ⊣

Exercise 9.1 Show the following are theorems of Heyting arithmetic.

1. $\forall x(\neg x = \mathsf{0} \to \exists y(x = \mathsf{s}y))$.
2. $\forall x \forall y(x + y = y + x)$.
3. $\forall x \forall y \forall z((x + y) + z = x + (y + z))$.
4. $\forall x \forall y(x \times y = y \times x)$.

As well as some basics of the theory of arithmetic, we recall the primitive recursive representation theorem. See [7], for example, for details.

9.5 Definition A formula is Δ_0 if it can be constructed from atomic formulas excluding P by the propositional connectives and bounded quantifiers. That is, the Δ_0 formulas forms the smallest collection of $\mathscr{L}_{\mathrm{A}}$-formulas satisfying:

1. all equations $s = t$ are Δ_0 formulas,
2. $\bot$ is a Δ_0 formula,
3. if F and G are Δ_0, then so is $F \to G$, $F \vee G$ and $F \wedge G$,
4. if $F(a)$ is Δ_0 and s is a term, then $\forall x < s\, F(x)$ and $\exists x < s\, F(x)$ are Δ_0, where these formulas are shorthands for $\forall x(x < s \to F(x))$ and $\exists x(x < s \wedge F(x))$ respectively.

A formula is Σ_1 (Π_1) if it has the form $\exists x F(x)$ (respectively $\forall x F(x)$) where $F(a)$ is Δ_0.

Notice that the bound variable x does not occur in the 'bounding' term s in the construction $\forall x < s\, F(x)$ above because terms do not contain bound variables.

Terms of the specific form $\mathsf{s} \cdots \mathsf{s0}$ are called *numerals*. The numeral evaluating to $n \in \mathbb{N}$ is denoted $\underline{n}$:

$$\underline{n} := \underbrace{\mathsf{s} \cdots \mathsf{s}}_{n} \mathsf{0}.$$

I state the representation theorem for primitive recursive relations.

9.6 Representation theorem *Let $R \subseteq \mathbb{N}^n$ be an k-ary relation on natural numbers. If R is primitive recursive there exists a Δ_0 formula $F_R(a_1, \ldots, a_k)$ of $\mathscr{L}_{\mathrm{A}}$ with at most the displayed variables free such that for all $n_1, \ldots, n_k \in \mathbb{N}$,*

$$\begin{aligned} \mathsf{PA} \vdash F_R(\underline{n}_1, \ldots, \underline{n}_k) \quad &\textit{iff} \quad (n_1, \ldots, n_k) \in R \\ \mathsf{PA} \vdash \neg F_R(\underline{n}_1, \ldots, \underline{n}_k) \quad &\textit{iff} \quad (n_1, \ldots, n_k) \notin R. \end{aligned}$$

There are important subtheories of Peano arithmetic that are worth introducing As I will cover only classical theories, I take the opportunity to remove some (classically) definable connectives. To be written.

Scope:

1. PRA.
2. $\mathsf{I}\Sigma_n$.

For the purpose of the following, the logical connectives are $\bot$, $\wedge$, $\rightarrow$ and $\forall$. Note, I am including implication rather than primitive negation as a matter of convenience.

9.7 Definition The Π_n^P formulas (the ^{P} expresses that the predicate P is permitted, in contrast to our earlier definition of Π_1) is the smallest set of formulas that contains

1. all prime formulas
2. $F \wedge G$ if $F, G \in \Pi_n^P$,
3. $\forall x F(x)$ if $F(a) \in \Pi_n^P$ and $n > 0$,
4. $F \rightarrow G$ if $F \in \Pi_{n-1}^P \cup \Pi_0^P$ and $G \in \Pi_n^P$.

9.2. Sequent calculi for arithmetic

There are different ways to formulate arithmetic in sequent calculi. One can incorporate all the axioms of arithmetic as initial sequents or treat each Peano axiom as contributing a rule of the calculus. A convenient definition is the following. $\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$ means that the sequent $\Gamma \Rightarrow \Delta$ has a derivation in the sequent calculus $\mathsf{C}_=$ expanded by:

- Initial sequents $\Pi \Rightarrow \Sigma, A$ for A a basic Peano axiom.

- The *induction rule*:

$$\frac{A(a), \Pi \Rightarrow \Sigma, A(\mathsf{s}a)}{A(0), \Pi \Rightarrow \Sigma, \forall x A(x)}\,\mathsf{ir}$$

 where a does not occur in the lower sequent.

The sequent calculus for Heyting arithmetic is the restriction to intuitionistic sequents. Recall, a sequent $\Gamma \Rightarrow \Delta$ is *intuitionistic* if $|\Delta| = 1$. Define $\mathsf{HA} \vdash \Gamma \Rightarrow \Delta$ as there exists a sequent calculus derivation witnessing $\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$ using only intuitionistic sequents.

9.8 Proposition

1. $\mathsf{PA} \vdash A$ *iff* $\mathsf{PA} \vdash\ \Rightarrow A$.
2. $\mathsf{HA} \vdash A$ *iff* $\mathsf{HA} \vdash\ \Rightarrow A$.

Proof I will show that every induction axiom admits a sequent calculus proof. The remainder of the proof is left as an exercise.

Fix a formula $F(a)$ and let $\Gamma = \{ F(0), \forall x(F(x) \rightarrow F(\mathsf{s}x)) \}$. By logic, a derivation of $F(a), \Gamma \Rightarrow F(\mathsf{s}a)$ is readily obtained. An application of the induction rule, followed by more logic completes the derivation:

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots\\ F(a), \Gamma \Rightarrow F(a)\end{array} \qquad \begin{array}{c}\vdots\\ F(\mathsf{s}a), \Gamma \Rightarrow F(\mathsf{s}a)\end{array}}{F(a) \rightarrow F(\mathsf{s}a), F(a), \Gamma \Rightarrow F(\mathsf{s}a)}\,\mathsf{L}{\rightarrow}}{F(a), \Gamma \Rightarrow F(\mathsf{s}a)}\,\mathsf{L}\forall}{\Gamma \Rightarrow \forall x F(x)}\,\mathsf{ir}$$

⊣

Exercise 9.2 Show that PA derives the same sequents as the calculus with induction axioms as initial sequents (along with the basic axioms) and no induction rule.

To be written.:

- SC for subtheories
- Partial CE

9.3. Small proofs and big proofs

By proposition 9.8, PA is consistent iff the empty sequent is not derivable. As with the sequent calculi from previous chapters, it is clear that there can be no cut-free derivation of the empty sequent, neither in PA nor HA. Thus, consistency of either theory would follow directly from a cut-elimination theorem for the above sequent calculi. There are sequents, however, that are provable but not *cut-free* provable. We will not present the argument here, which appeals to Gödel's incompleteness theorems; the finer details are beyond the scope of this book and can be found in, for example, [1].

Gentzen's observation was that every derivable *equational* sequent can be shown to have a cut-free derivation, where an equational sequent is one of the form $r_1 = s_1, \dots, r_k = s_k \Rightarrow t_1 = u_1, \dots, t_l = u_l$ wherein all terms are closed. As the empty sequent is an example of an equational sequent, consistency is an immediate corollary of the (partial) cut-elimination result.

Gentzen's argument is highly intricate and was greatly streamlined by Kurt Schütte (1950) who showed that full cut-elimination can be obtained by moving to a more relaxed notion of a sequent calculus derivation, termed 'ω-proofs', in which proofs are in general infinite objects. The basic idea is to replace the logical rules R$\forall$ and L$\exists$ each by a rule with infinitely many premises:

$$\frac{\Gamma \Rightarrow \Delta, A(0) \qquad \Gamma \Rightarrow \Delta, A(\underline{1}) \qquad \cdots \qquad \Gamma \Rightarrow \Delta, A(\underline{n}) \qquad \cdots}{\Gamma \Rightarrow \Delta, \forall x A(x)}\ \mathsf{R}\omega$$

$$\frac{A(0), \Gamma \Rightarrow \Delta \qquad A(\underline{1}), \Gamma \Rightarrow \Delta \qquad \cdots \qquad A(\underline{n}), \Gamma \Rightarrow \Delta \qquad \cdots}{\exists x A(x), \Gamma \Rightarrow \Delta}\ \mathsf{L}\omega$$

The rules Rω and Lω above are collectively called the ω-rules.

'Proof' in the sense of the sequent calculi of previous chapters meant 'finite tree labelled by sequents in agreement with the rules of the calculus'. A 'proof' that uses an ω-rule can never be finite as these rules have infinitely many premises. But the condition 'finite or infinite tree labelled by sequents in agreement with the rules of the calculus' is too liberal as it admits as 'proofs' trees with infinitely long branches, such as

$$\dfrac{\dfrac{\dfrac{\begin{matrix}\vdots \\ \Rightarrow \bot\end{matrix} \quad \dfrac{}{\bot \Rightarrow \bot}\,\mathsf{L}\bot}{\Rightarrow \bot}\,\mathsf{cut} \quad \dfrac{}{\bot \Rightarrow \bot}\,\mathsf{L}\bot}{\Rightarrow \bot}\,\mathsf{cut} \quad \dfrac{}{\bot \Rightarrow \bot}\,\mathsf{L}\bot}{\Rightarrow \bot}\,\mathsf{cut}$$

The answer is that, as in the finite case, there can be no infinite paths in an ω-proof but, unlike the finite case, the tree underlying an ω-proof may have infinitely wide branching. Such trees are called *well-founded*.

In sum, an *ω-proof* is a well-founded tree that is labelled by sequents in a way consistent with the rules of the sequent calculus (the ω- and non ω-rules).

9.9 Proposition

1. *There is an ω-proof of every sequent of the form $F, \Gamma \Rightarrow \Delta, F$*
2. *If there is an ω-proof of $\Gamma(a) \Rightarrow \Delta(a)$, then for every term s there is an ω-proof of $\Gamma(s) \Rightarrow \Delta(s)$.*

Proof Exercise. ⊣

9.10 Proposition *The induction rule can be simulated via ω-proofs.*

Proof Fix a formula $F(a)$ and as before let $\Gamma = \{ F(0), \forall x(F(x) \to F(\mathsf{s}x)) \}$. Suppose $F(a), \Gamma \Rightarrow \Delta, F(\mathsf{s}a)$ admits an ω-proof. As this is a premise to an induction rule the variable a does not occur in $\Gamma \cup \Delta$. By the previous proposition there is an ω-proof of the sequent $F(\underline{n}), \Gamma \Rightarrow \Delta, F(\underline{n+1})$ for each n. A sequence of cuts induces an ω-proof of $F(0), \Gamma \Rightarrow \Delta, F(\underline{n})$: for $n = 0, 1$ the claim is immediate. For $n = m + 1 > 1$ append the proof of the induction hypothesis by a single cut:

$$\dfrac{\begin{matrix}\vdots \\ F(\underline{0}), \Gamma \Rightarrow \Delta, F(\underline{m})\end{matrix} \qquad \begin{matrix}\vdots \\ F(\underline{m}), \Gamma \Rightarrow \Delta, F(\underline{n})\end{matrix}}{F(0), \Gamma \Rightarrow \Delta, F(\underline{n})}\,\mathsf{cut}$$

As $F(0), \Gamma \Rightarrow \Delta, F(\underline{n})$ is derivable for each n, an application of $\mathsf{R}\omega$ completes the (ω-)proof. ⊣

Exercise 9.3 Show that the induction axioms admit *cut-free* ω-proofs.

With the ω-rules replacing the traditional quantifier rules R$\forall$ and L$\exists$ it turns out that free variables can be completely eliminated from the sequent calculus, meaning that only closed sequents are derived. This convention serves to simplify much of the reasoning about ω-proofs. It is also possible to dispense with the logical rules for equality by adopting more liberal initial sequents.

The next definition introduces both conventions and settles the notion of ω-proof used hereon. Observe that it is decidable whether two closed terms s and t in the language of arithmetic evaluate to the same natural number. I will write $\mathbb{N} \vDash s = t$ if this is the case, and $\mathbb{N} \nvDash s = t$ otherwise.

9.11 Definition · PAω and HAω PAω is the sequent calculus given by the following:

- sequents comprise formulas in the language of arithmetic (with equality).
- Initial sequents are *closed* sequents of the form

  (L$\bot$) $\bot, \Gamma \Rightarrow \Delta$

  (id) $Ps, \Gamma \Rightarrow \Delta, Pt$ if $\mathbb{N} \vDash s = t$

  (R=) $\Gamma \Rightarrow \Delta, s = t$ if $\mathbb{N} \vDash s = t$

  (L=) $s = t, \Gamma \Rightarrow \Delta$ if $\mathbb{N} \nvDash s = t$
- Inference rules are rules of C but restricted to closed sequents and with R$\forall$ and L$\exists$ replaced by the two ω-rules:

$$(\mathsf{R}\omega)\ \frac{\Gamma \Rightarrow \Delta, F(\underline{n}) \text{ for every } n \in \mathbb{N}}{\Gamma \Rightarrow \Delta, \forall x F(x)}$$

$$(\mathsf{L}\omega)\ \frac{F(\underline{n}), \Gamma \Rightarrow \Delta \text{ for every } n \in \mathbb{N}}{\exists x F(x), \Gamma \Rightarrow \Delta}$$

Writing PAω $\vdash \Gamma \Rightarrow \Delta$ expresses that there is an ω-proof of $\Gamma \Rightarrow \Delta$ according to the above rules. In other words, there exists a well-founded tree labelled by sequents such that each leaf is an initial sequent and that each inner vertex together with its immediate successors in the tree forms a correct application of a rule of the calculus listed above.

HAω is the calculus above restricted to intuitionistic sequents.

With the sequent calculus formally defined, the realisation of finite PA-proofs as ω-proofs can resume. The first step is to give ω-proofs of the basic axioms of arithmetic.

9.12 Proposition *Every closed initial sequent of* PA *is derivable in* $\mathsf{PA}\omega$*.*

Proof Among the sequents to be shown derivable in PA are all initial sequents of C and the basic axioms of PA. I will treat the case of the basic axiom PA1, $\forall x(\neg 0 = \mathsf{s}x)$. Let $n \in \mathbb{N}$ be arbitrary. As the equation $0 = \mathsf{s}\underline{n}$ is false, $0 = \mathsf{s}\underline{n}, \Gamma \Rightarrow \Delta, \bot$ is an initial sequent of $\mathsf{PA}\omega$ for all closed Γ, Δ. Therefore $\mathsf{PA}\omega \vdash \Gamma \Rightarrow \Delta, \neg 0 = \mathsf{s}\underline{n}$ for every $n \in \mathbb{N}$ and $\mathsf{PA}\omega \vdash \Gamma \Rightarrow \Delta, \forall x(\neg 0 = \mathsf{s}x)$ by $\mathsf{R}\omega$. ⊣

Exercise 9.4 Complete the proof of proposition 9.12.

Exercise 9.5 Show that all closed sequents of the form $A, \Gamma \Rightarrow \Delta, A$ are provable in $\mathsf{PA}\omega$.

9.13 Embedding lemma *Suppose* $\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$ *and let* $\Gamma^* \Rightarrow \Delta^*$ *be any closed substitution instance of* $\Gamma \Rightarrow \Delta$ *(obtained by substituting closed terms for free variables). Then* $\mathsf{PA}\omega \vdash \Gamma \Rightarrow \Delta$*. Likewise, for Heyting arithmetic and* $\mathsf{HA}\omega$*.*

Exercise 9.6 Prove the embedding lemma. Do not forget the equality rules implicit in $\mathsf{C}_=$.

The next task is to analyse ω-proofs and establish a cut elimination theorem. Currently lacking, however, is some measure of the *complexity* of an ω-proof analogous (or, perhaps, generalising) the height of finite sequent calculus proofs. Although every path through an ω-proof is, by requirement, finite there are ω-proofs that admit paths of arbitrary (finite) length. The ω-proof described by the proof of proposition 9.10 is such an example. It comprises a single application of an ω-rule at the root with the premise for the numeral n being derived by a (finite) sequent proof of height at least n.

Thus the question comes down to how to associate a measure to ω-proofs such that strict subproofs (i.e., proofs of the premises of the root inference) can be recognised as being 'smaller' than the proof itself? The answer to this conundrum is in the title of this module: *ordinals*.

10. An ordinal interlude

To present the ordinals it is not necessary to have a set-theoretic definition of ordinals in mind (as, for example, arbitrary transitive sets). Indeed, there is no need to consider the question of by what ordinals *are* or from what they are *formed*. For a *theory* of ordinals all that is relevant are the order-theoretic properties satisfied by the ordinals and a selection of operations that can be defined on them. In short, ordinals are treated analogously to natural numbers: as a posited entity fulfilling specified criteria. The material of this chapter draws from lecture notes by Michael Rathjen [8].

10.1 Definition The *ordinals* is a class $\mathbb{O}$ equipped with a binary relation $<$ satisfying three postulates, where $\leq$ is the reflexive closure of $<$:

- O1. $<$ is a strict linear order on $\mathbb{O}$. That is, $<$ is irreflexive, transitive and linear, where linear means that for all $\alpha, \beta \in \mathbb{O}$ either $\alpha \leq \beta$ or $\beta \leq \alpha$.
- O2. Every non-empty class of ordinals has a $<$-minimal element (necessarily unique by O1). That is, if $O \subseteq \mathbb{O}$ is non-empty there exists $\xi \in O$ such that $\xi \leq \alpha$ for all $\alpha \in O$.
- O3. For every set X and function $f \colon X \to \mathbb{O}$ there exists $\xi \in \mathbb{O}$ such that $f(x) < \xi$ for every $x \in X$.

Set-theoretic concerns do matter in the language used to discuss ordinals. As, for example, the Burali-Forte paradox shows, it is inconsistent the Zermelo–Fraenkel (or Cantorian) conception of *set* in mind to consider that the collection of (all) ordinals forms a set. Hence use of term 'class' to refer to arbitrary collections of ordinals/objects and 'set' in specific case of O3. Familiarity with set theory is not necessary for the elementary theory of ordinals presented here. Indeed, it will suffice to replace every term ‘set’ in what follows by ‘countable set’ and ‘class’ by ‘countable or uncountable set’.

In the following, notation $\{ t \mid x \in X \}$ means the *class* of objects t as x ranges over the (class) X. Usually a function $f\colon U \to V$ between classes has been specified along with a (sub)class $X \subseteq U$ whence the notation $\{ f(x) \mid x \in X \}$ expresses the class of objects $f(x)$ for $x \in X$. This class will be written $f[X]$.

Convention 1 Lowercase Greek letters α, β, etc. stand as metavariables for ordinals. ⊣

10.2 Lemma *Postulate O2 is equivalent to the principle of transfinite induction. This is the statement that if O is progressive in the ordinals then $\mathbb{O} \subseteq O$, where O is progressive means that for all ordinals α, if $\beta \in O$ for every $\beta < \alpha$ then $\alpha \in O$.*

Proof Let O be progressive. Consider the class $C = \mathbb{O} \setminus O$ of ordinals not in O. If C is non-empty then, by O2, C contains a least ordinal, α say. As α is the least ordinal in C, every $\xi < \alpha$ is element of O. Progressiveness implies that $\alpha \in O$ contradicting that $\alpha \in C$. Hence, C is the empty class, so $\mathbb{O} \subseteq O$. For the converse claim, assume postulate O1 and the principle of transfinite induction (I could also assume O3 but this is unnecessary). The aim is to establish O2. Thus, let O be a non-empty class of ordinals and, for want of a contradiction, assume that O has no least element. As in the other direction, I consider the complement of O, the class $C = \mathbb{O} \setminus O$. Suppose α be any ordinal such that $\xi \in C$ for all $\xi < \alpha$. If $\alpha \in O$ then this is the least element of O. As O has no least element therefore $\alpha \in C$. So C is progressive and $C = \mathbb{O}$ by transfinite induction, contradicting the non-emptiness of O. ⊣

The next lemma provides the primary means to infer the existence of ordinals.

10.3 Lemma *Let O be a class of ordinals.*

1. *There exists a least upper bound of O. That is, an ordinal α such that $\xi \leq \alpha$ for all $\xi \in O$. This ξ is referred to as the* supremum *of O and denoted* $\sup O$.

2. *There exists a strict least upper bound of O, i.e., α such that $\xi < \alpha$ for all $\xi \in O$.*

In each case the proclaimed ordinal is unique.

Proof Begin with 1. Let O be given. Consider the class $O^{\geq}$ of all ordinals α such that $\xi \leq \alpha$ for *all* $\xi \in O$. The <-least element of $O^{\geq}$ (if such exists) is clearly the desired ordinal. But in order to apply postulate O2 to this class it is necessary to establish that $O^{\geq}$ is non-empty. For this I use the third postulate applied to identity function $\mathsf{id}\colon O \to \mathbb{O}\colon \xi \mapsto \xi$ (which is a function from O into $\mathbb{O}$). For 2, the same argument works with the class $O^{>}$ in place of $O^{\geq}$ where this is the class of ordinals *strictly* larger than all elements of O.

Uniqueness of each case is ensured by O1. ⊣

Henceforth, I will not make explicit reference to the postulates.

The least ordinal is denoted 0. This happens to be the supremum of the empty set: $0 := \sup \emptyset$. Given $\alpha \in \mathbb{O}$, the *successor* of α, in symbols α' or $\alpha + 1$, is the least ordinal greater than α, which exists (and is unique) by lemma 10.3(2) applied to the singleton set $\{ \alpha \}$. That is, α' is such that $\xi < \alpha'$ iff $\xi \leq \alpha$. The successor of 0 is denoted $1(= 0')$, its successor $2(= 0'')$, etc.

A *limit ordinal* is any non-zero ordinal λ such that $\eta' < \lambda$, for all $\eta < \lambda$. Define a function $f : \mathbb{N} \to \mathbb{O}$ by $f(0) = 0$ and $f(n+1) = f(n)'$. That is, $f(n)$ is the *ordinal* representing the natural n. The supremum of $\{ n \mid n \in \mathbb{N} \}$ is called ω, which is a limit by construction and, therefore, the least limit ordinal.

10.4 Lemma *Every non-zero ordinal is either a successor or a limit.*

10.5 Lemma *An ordinal λ is a limit iff $\lambda = \sup O$ for some non-empty set O closed under successor (meaning that $\xi \in O$ implies $\xi' \in O$).*

10.6 Lemma *Suppose O, O' are such that for every $\alpha \in O$ there exists $\beta \in O'$ such that $\alpha \leq \beta$. Then $\sup O \leq \sup O'$.*

Exercise 10.1 Prove lemma 10.4 to 10.6.

I will employ common set-theoretic abbreviations such as $\sup_{i \in I} \alpha_i$ for $\sup\{ \alpha_i \mid i \in I \}$ and $\sup_i \alpha_i$ for $\sup\{ \alpha_i \mid i < \omega \}$. I will also use λ as a metavariable for limit ordinals.

10.1. Elementary Ordinal Functions

A *segment* of $\mathbb{O}$ is any class O of ordinals which is closed downwards, i.e., if $\alpha < \beta \in O$ then $\alpha \in O$. If X and Y are segments then either $X \subseteq Y$ or $Y \subseteq X$; in either case $X \cap Y$ is a segment.

Let O be a segment. A function $f : O \to \mathbb{O}$ is said to be:

- *order preserving* if $\alpha < \beta$ implies $f(\alpha) < f(\beta)$ for all $\alpha, \beta \in O$.
- *continuous* if for all $U \subseteq O$, if $\sup U \in O$ then $f(\sup U) = \sup f[U]$.
- an *enumeration* (of $X \subseteq \mathbb{O}$) if f is order-preserving and $f[O] = X$.

The identity function $\mathsf{id} : \mathbb{O} \to \mathbb{O}$ is all of the above. In particular, it is an enumeration of $\mathbb{O}$. Let $f : \mathbb{N} \to \mathbb{O}$ be given by $f(0) = \omega$ and $f(n+1) = f(n)'$. This function is order preserving and continuous (the latter is trivial). It is also an enumeration of the set $\{ \omega, \omega', \dots \}$ because $\mathbb{N}$ is a segment. Notice that order preserving functions on ordinals are always injective.

10.7 Lemma *If O is a segment and f is order preserving then $\alpha \leq f(\alpha)$ for all $\alpha \in O$.*

Exercise 10.2 Prove lemma 10.7.

The main property of ordinal functions I need is the summarised by

10.8 Lemma *Every class of ordinals has a unique enumeration. The enumeration of $Y \subseteq \mathbb{O}$ will be denoted E_Y.*

Proof E_Y is determined as the inverse of a particular function $C_Y : Y \to \mathbb{O}$, called the *collapsing* function for Y, defined by

$$C_Y(\alpha) = \sup\{ C_Y(\xi) + 1 \mid \xi \in Y \text{ and } \xi < \alpha \}.$$

The collapsing function is clearly unique if it is well-defined. Moreover, C_Y This function is well-defined: Consider the class O of ordinals α for which the collapsing function on $Y_\alpha := Y \cap \{ \xi \mid \xi \leq \alpha \}$ exists. If $C_{Y_\xi} : Y_\xi \to \mathbb{O}$ is defined for each $\xi < \alpha$ I claim that $C : Y_\alpha \to \mathbb{O}$ defined by

$$\begin{aligned} C(\alpha) &= \sup\{ C_{Y_\xi}(\xi) + 1 \mid \xi < \alpha \text{ and } \xi \in Y \} \\ C(\xi) &= C_{Y_\xi}(\xi) \text{ for } \xi < \alpha \end{aligned}$$

is the collapsing function for Y_α. That this is the follows almost by definition. Indeed, all that is lacking is the observation that $C_{Y_\xi}(\beta) = C_{Y_\eta}(\beta)$ whenever $\beta \leq \xi < \eta$. So O is progressive and transfinite induction implies that class Y_α has a collapsing function C_{Y_α}. Now define C_Y as $\alpha \mapsto C_{Y_\alpha}(\alpha)$.

Clearly, C_Y is injective. Therefore the function admits a (right) inverse:

$$E_Y := C_Y^{-1} \colon C_Y[Y] \to Y$$

As $C_Y[Y]$ is (clearly) a segment, E_Y is an enumeration of Y.

As to uniqueness of E_Y, let $O = C_Y[Y]$ and suppose $f \colon O' \to Y$ is any enumeration of Y. In particular, O' is a segment. Transfinite induction implies that $f(\alpha) = E_Y(\alpha)$ for all $\alpha \in O \cap O'$. As both functions are injective and surjective into Y it follows that $O = O'$. ⊣

Two further properties of enumerations will be useful.

10.9 Lemma *Let $f \colon \mathbb{O} \to \mathbb{O}$ be continuous and order preserving (in particular, f is an enumeration of $f[\mathbb{O}]$). Then*

1. *For every $\alpha \geq f(0)$ there is a unique $\beta \leq \alpha$ such that $f(\beta) \leq \alpha < f(\beta+1)$.*
2. *For every α there is a unique $\beta \geq \alpha$ such that $\beta = f(\beta)$.*

Proof 1. Consider the set $O = \{\, \xi \mid f(\xi) \leq \alpha \,\}$ and let $\beta = \sup O$. Continuity yields

$$f(\beta) = \sup f[O] = \sup\{\, f(\xi) \mid f(\xi) \leq \alpha \,\} \leq \alpha$$

whereas $f(\beta + 1) > \alpha$ because $\beta + 1 \notin O$.

2. Fix α and define $O = \{\, f(\alpha), f(f(\alpha)), \dots, f^n(\alpha), \dots \}$ (arbitrary finite iterations of f on α). Let $\beta = \sup O$. Invoking continuity, $f(\beta) = \sup f[O] = \sup O = \beta$. Moreover, $\alpha \leq f(\alpha) \leq \beta$. ⊣

10.2. Elementary Ordinal Arithmetic

The basic operations of arithmetic can be extended to ordinals in a straightforward manner. Often these are defined by transfinite recursion, but the two operations we desire, addition and exponentiation base ω, can be expressed as enumeration functions. I start with addition.

10.10 Definition Let $\alpha^{\geq}$ be the class of ordinals $\geq \alpha$. *Ordinal addition*, $\alpha + \beta$, is defined as $\alpha + \beta \coloneqq E_{\alpha^{\geq}}(\beta)$. That is, $\alpha + \beta$ is defined as the β-th ordinal in the enumeration of the ordinals $\geq \alpha$.

The following are direct consequences of this definition and left to the reader.

10.11 Lemma *For all α, β and γ.*

1. $\alpha + 0 = \alpha$.
2. $\alpha + \beta' = (\alpha + \beta)'$.
3. *If β is a limit then $\alpha + \beta = \sup\{ \alpha + \xi \mid \xi < \beta \}$.*
4. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.
5. *$\alpha \leq \alpha + \beta$ and $\beta \leq \alpha + \beta$.*

10.12 Example $\alpha + \omega = \sup\{ \alpha + n \mid n \in \mathbb{N} \} = \sup\{ \alpha, \alpha', \alpha'', \dots \}$. *Thus $\alpha + \omega$ is the least limit ordinal strictly above α.*

In particular, $n + \omega = \omega$ for every $n < \omega$. As $1 + \omega = \omega < \omega + 1$ ordinal addition is not commutative.

As addition is associative (item 4 of the lemma above), I will omit brackets when stringing together applications of addition. So $\alpha + \beta + \gamma$ can refer to either $(\alpha + \beta) + \gamma$ or $\alpha + (\beta + \gamma)$.

The next lemma is a consequence of lemma 10.9.

10.13 Lemma *For every $\alpha \leq \beta$ there exists a unique ξ such that $\beta = \alpha + \xi$.*

Proof Lemma 10.9 implies a unique ξ such that $\alpha + \xi \leq \beta < \alpha + \xi'$. Since $\alpha + \xi' = (\alpha + \xi) + 1$ it follows that $\alpha + \xi = \beta$. ⊣

As example 10.12 demonstrates ω has the unusual property of being closed under addition: if $\xi, \eta < \omega$ then $\xi + \eta < \omega$. Ordinals satisfying this condition are called *additive principal* ordinals.

10.14 Definition A ordinal α is additive principal iff $\alpha > 0$ and $\xi + \eta < \alpha$ for all $\xi, \eta < \alpha$. The class of additive principal ordinals is denoted AP.

The least additive principal ordinal is 1; the next is clearly ω. Most ordinals are *not* additive principal. 1 is the only additive principal successor ordinal (because $\alpha + \alpha \geq \alpha'$ provided $\alpha \geq 1$). Even most limit ordinals not additive principal: If $\alpha \geq \omega$ then $\alpha + \omega \notin \mathrm{AP}$ as $\alpha < \alpha + \omega$ but $\alpha + \alpha \not< \alpha + \omega$.

10.15 Lemma *The enumeration function E_{AP} for additive principal ordinals is continuous and has domain $\mathbb{O}$.*

Proof Exercise. ⊣

Lemma 10.15 shows that the function enumerating the additive principal ordinals is defined on all ordinals, is order preserving and continuous.

10.16 Lemma *The following are equivalent for all $\alpha > 0$:*

1. *α is additive principal.*
2. $\alpha = 1$ *or* $\alpha = \sup\{\, \xi + \xi \mid \xi < \alpha \,\}$.
3. *for all $\beta < \alpha$, $\beta + \alpha = \alpha$.*

Proof 1 ⇒ 2. If α is additive principal then $\sup\{\, \xi + \xi \mid \xi < \alpha \,\} \leq \alpha$ by definition. Also, the additive principal ordinals except 1 are all limits, so if $\alpha \neq 1$ then $\alpha = \sup\{\, \xi \mid \xi < \alpha \,\} \leq \sup\{\, \xi + \xi \mid \xi < \alpha \,\}$.

2 ⇒ 3. For $\alpha = 1$ the claim is trivial. Otherwise, α is a limit and $\beta + \alpha \leq \sup\{\, \beta + \xi \mid \xi < \alpha \,\} \leq \sup\{\, \xi + \xi \mid \xi < \alpha \,\}$. As $\alpha = \sup\{\, \xi + \xi \mid \xi < \alpha \,\}$ the claim is established.

3 ⇒ 1. Straightforward. ⊣

As a consequence of part 3, $\omega^\alpha + \omega^\beta = \omega^\beta$ iff $\alpha < \beta$. A corollary is the observation made earlier, that $n + \omega = \omega$, which now follows from repeated applications of lemma 10.16: $\alpha' + \omega = \alpha + (\omega^0 + \omega^1) = \alpha + \omega^1$.

Additive principal ordinals are central to the theory of ordinals. As with addition, I will introduce more suggestive notation for the enumeration function for additive principal ordinals.

10.17 Definition $\omega^\alpha := E_{\mathrm{AP}}(\alpha)$.

By the definition $\omega^0 = 1$ and $\omega^1 = \omega$. The reader can confirm that next additive principal ordinal above ω is the supremum of ω, $\omega + \omega$, $\omega + \omega + \omega, \dots, \omega + \dots + \omega, \dots$ which is denoted ω^2.

10.18 Lemma *For every $\alpha > 0$ there exists unique β and $\xi < \alpha$ such that $\alpha = \omega^\beta + \xi$.*

Proof Let β be such that $\omega^\beta \leq \alpha < \omega^{\beta'}$ and ξ such that $\alpha = \omega^\beta + \xi$. Both ordinals are given by lemma 10.9. What remains is to show uniqueness of this choice. Thus, suppose $\alpha = \omega^\gamma + \eta$ for some γ and $\eta < \alpha$. The choice of β is clearly such that $\beta \geq \gamma$. As

$$\omega^\beta + \omega^{\gamma+1} \leq \alpha + \omega^{\gamma+1} \leq \omega^\gamma + \eta + \omega^{\gamma+1} = \omega^{\gamma+1}$$

(the first inequality uses lemma 10.11(5); the rest use lemma 10.16(3)), also $\beta \leq \gamma$. Given that $\beta = \gamma$, uniqueness of the rest is immediate. ⊣

10.3. Normal forms and natural sum

Lemma 10.18 above provides the basis of a normal form representation of ordinals. This concept is introduced in the next definition.

10.19 Definition I write $\alpha =_{\text{NF}} \omega^\beta + \gamma$ to express that (i) $\alpha = \omega^\beta + \gamma$ and (ii) $\gamma < \alpha$.

Cantor, in 1897, established an expanded version of this normal form decomposition.

10.20 Cantor normal form theorem *For every ordinal $\alpha > 0$ there exists n and ordinals $\alpha_n \leq \dots \leq \alpha_0$ such that*

$$\alpha = \omega^{\alpha_0} + \dots + \omega^{\alpha_n}.$$

Moreover, this decomposition is unique.

Proof The theorem is a simple generalisation of lemma 10.18. Let $\alpha =_{\text{NF}} \omega^{\alpha_0} + \xi_0$ by lemma 10.18. If $\xi_0 = 0$ the decomposition is complete. Otherwise, apply the lemma again to express $\xi_0 =_{\text{NF}} \omega^{\alpha_1} + \xi_1$, $\xi_1 =_{\text{NF}} \omega^{\alpha_2} + \xi_2$, etc. As $\alpha > \xi_0 > \xi_1 > \cdots$ is a strictly decreasing sequence or ordinals, necessarily $\xi_n = 0$ for some n. Thus, $\alpha = \omega^{\alpha_0} + \cdots + \omega^{\alpha_n}$. Furthermore, $\alpha_0 \geq \alpha_1 \geq \cdots \geq \alpha_n$ because $\omega^{\alpha_{i+1}} \leq \xi_i < \omega^{\alpha_i+1}$ for each i. Uniqueness is also a consequence of these normal forms. ⊣

10.21 Definition The normal form notation is extended in the following way. Writing $\alpha =_{\text{NF}} \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$ expresses that (i) $\alpha = \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$ and (ii) $\alpha \geq \alpha_1 \geq \cdots \geq \alpha_n$.

Lemma 10.9 showed that every continuous order preserving function on the ordinals has fixed points. I.e., for each such function f there are ordinals β such that $\beta = f(\beta)$. As the function $\xi \mapsto \omega^\xi$ (namely E_{AP}) is an example of such a function, there must exist ordinals α such that $\alpha = \omega^\alpha$. The proof of that lemma describes how to construct such an ordinal as the supremum of the sequence $0, 1, \omega, \omega^\omega, \ldots, \alpha, \omega^\alpha, \ldots$. This particular ordinal, conventionally denoted ε_0, will play a central role in the next chapter.

10.22 Definition $\varepsilon_0 \coloneqq \sup_i \omega_i$ where $\omega_0 = \omega$ and $\omega_{k+1} = \omega^{\omega_k}$.

10.23 Lemma *ε_0 is the least fixed point of the ordinal function $\alpha \mapsto \omega^\alpha$. That is, $\omega^{\varepsilon_0} = \varepsilon_0$ and $\alpha < \omega^\alpha$ for all $\alpha < \varepsilon_0$.*

Exercise 10.3 Prove lemma 10.23.

Exercise 10.4 Using the Cantor normal form theorem, define a multiplication operation where the first argument is restricted to additive principal ordinals: $\alpha, \beta \mapsto \omega^\alpha.\beta$. The function should be continuous in β and satisfy the recursive clauses: $\omega^\alpha.0 = 0$ and $\omega^\alpha.(\beta+1) = \omega^\alpha.\beta + \omega^\alpha$.

Exercise 10.5 Define a function $\alpha \mapsto 2^\alpha$ satisfying

$$\begin{aligned} 2^0 &= 1 \\ 2^{\alpha+1} &= 2^\alpha + 2^\alpha \\ 2^\lambda &= \sup\{\, 2^\xi \mid \xi < \lambda \,\} \end{aligned}$$

(You may find it useful to use the Cantor normal form theorem.) Show that this function is order preserving and continuous, and compute all fixed points of the function for ordinals $\alpha \leq \varepsilon_0$.

Exercise 10.6 Let $\alpha \mapsto \varepsilon_\alpha$ be the enumerating function of the ordinals η such that $\eta = \omega^\eta$. Express ε_α as a supremum of smaller ordinals as per definition 10.22 and deduce that the enumerating function is defined for all ordinals.

Exercise 10.7 Prove the Cantor normal form theorem in base 2: *For every ordinal $\alpha > 0$ there exists unique ordinals $\alpha_n \leq \cdots \leq \alpha_0 \leq \alpha$ such that*

$$\alpha = 2^{\alpha_0} + \cdots + 2^{\alpha_n}.$$

Exercise 10.8 What are the additive principal ordinals in base-2 normal form? Characterise the α such that $2^\alpha = \omega^\alpha$.

This brief foray into ordinals is concluded with another look at addition. Recall that addition on ordinals is not commutative: $1 + \omega \neq \omega + 1$ for example. It is possible to provide a natural notion of addition that *is* commutative. This is called the *natural sum* (sometimes *Hessenberg sum* after its originator Gerhard Hessenberg [5]). The Cantor normal theorem provides the means to achieve this.

10.24 Definition The natural sum of ordinals α and β, denoted $\alpha \# \beta$ is defined by recursion on the two ordinals. $0 \# \alpha = \alpha \# 0 := \alpha$ for all α. For non-zero $\alpha =_{\mathrm{NF}} \omega^{\alpha_0} + \alpha_1$ and $\beta =_{\mathrm{NF}} \omega^{\beta_0} + \beta_1$

$$\alpha \# \beta := \begin{cases} \omega^{\alpha_0} + (\alpha_1 \# \beta), & \text{if } \alpha_0 \geq \beta_0, \\ \omega^{\beta_0} + (\alpha \# \beta_1), & \text{if } \alpha_0 \leq \beta_0. \end{cases}$$

The operation of natural sum is well-defined as $\alpha_1 < \alpha$ and $\beta_1 < \beta$.

As an operation on the Cantor normal form, the natural sum has the following property.

10.25 Lemma *For $\alpha =_{\mathrm{NF}} \omega^{\alpha_1} + \cdots + \omega^{\alpha_m}$ and $\beta =_{\mathrm{NF}} \omega^{\beta_1} + \cdots + \omega^{\beta_n}$*

$$\alpha \# \beta := \omega^{\gamma_1} + \cdots + \omega^{\gamma_{m+n}}$$

where $\gamma_1 \geq \cdots \geq \gamma_{m+n}$ enumerate the ordinals $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ in descending order (with repetitions).

10.26 Lemma *The natural sum is commutative and strongly increasing in both arguments: For all α, β, γ,*

1. $\alpha \# \beta = \beta \# \alpha$*;*
2. $\alpha < \beta$ *implies* $\alpha \# \gamma < \beta \# \gamma$*.*

Exercise 10.9 Prove lemma 10.26.

Exercise 10.10 Using the Cantor normal form theorem define a commutative multiplication $\alpha.\beta$ operation on ordinals. It should satisfy the distribution law: $(\alpha \# \beta).\gamma = (\alpha.\gamma) \# (\beta.\gamma)$. Hint, start from the function in exercise 10.4.

11. Ordinal analysis of arithmetic

Ordinals will now be used to measure the *height* of ω-proofs. I begin by recalling the infinitary sequent calculi for arithmetic from the end of chapter 9.

11.1 Definition $\mathsf{PA}\omega$ is the sequent calculus given by the following:

- sequents comprise formulas in the language of arithmetic (with equality).
- Initial sequents are *closed* sequents of the form

(L$\bot$) $\bot, \Gamma \Rightarrow \Delta$

(id) $Ps, \Gamma \Rightarrow \Delta, Pt$ if $\mathbb{N} \vDash s = t$

(R=) $\Gamma \Rightarrow \Delta, s = t$ if $\mathbb{N} \vDash s = t$

(L=) $s = t, \Gamma \Rightarrow \Delta$ if $\mathbb{N} \nvDash s = t$

- Inference rules are rules of C but restricted to closed sequents and with R$\forall$ and L$\exists$ replaced by the two ω-rules:

$$(\mathsf{R}\omega)\ \frac{\Gamma \Rightarrow \Delta, F(\underline{n}) \text{ for every } n \in \mathbb{N}}{\Gamma \Rightarrow \Delta, \forall x F(x)}$$

$$(\mathsf{L}\omega)\ \frac{F(\underline{n}), \Gamma \Rightarrow \Delta \text{ for every } n \in \mathbb{N}}{\exists x F(x), \Gamma \Rightarrow \Delta}$$

$\mathsf{HA}\omega$ is the same calculus but restricted to intuitionistic sequents.

11.2 Definition Let T be $\mathsf{PA}\omega$, $\mathsf{HA}\omega$ or an extension of either calculus by rules that are at most ω-branching. The ternary relation $\mathsf{T} \vdash_k^\alpha \Gamma \Rightarrow \Delta$, between a sequent $\Gamma \Rightarrow \Delta$, an ordinal α and $k < \omega$, is defined by transfinite recursion on the rules of T:

1. If $\Gamma \Rightarrow \Delta$ is an initial sequent of T, then $\mathsf{T} \vdash_k^\alpha \Gamma \Rightarrow \Delta$ for all α and k;

2. For each inference $(*)$ of T except cut of the form
$$\frac{\{\,\Gamma_i \Rightarrow \Delta_i \mid i \in I\,\}}{\Gamma \Rightarrow \Delta}\,*$$
$\mathsf{T} \vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta$ holds if $\mathsf{T} \vdash^{\alpha_i}_{k} \Gamma_i \Rightarrow \Delta_i$ and $\alpha_i < \alpha$ for all $i \in I$;
3. If $\mathsf{T} \vdash^{\alpha_0}_{k} \Gamma \Rightarrow \Delta, C$ and $\mathsf{T} \vdash^{\alpha_1}_{k} C, \Gamma \Rightarrow \Sigma$ for $\alpha_0, \alpha_1 < \alpha$ and $|C| < k$, then $\mathsf{T} \vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta, \Sigma$.

Given $\mathsf{T} \vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta$ I will write that $\Gamma \Rightarrow \Delta$ is derivable (in T) with height $\leq \alpha$ and cut rank $\leq k$.

There is no requirement of minimality of α and k in the above definition. So the relation $\vdash^{\alpha}_{k}$ is monotone in α and k:

11.3 Lemma *If $\alpha \leq \beta$ and $k \leq l$ then $\mathsf{T} \vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta$ implies $\mathsf{T} \vdash^{\beta}_{l} \Gamma \Rightarrow \Delta$.*

Proof By transfinite induction on α. If $\Gamma \Rightarrow \Delta$ is an initial sequent, the result is immediate. Otherwise, there is an inference rule of T
$$\frac{\{\,\Gamma_i \Rightarrow \Delta_i \mid i \in I\,\}}{\Gamma \Rightarrow \Delta}\,*$$
and ordinals $\alpha_i < \alpha$ such that $\mathsf{T} \vdash^{\alpha_i}_{k} \Gamma_i \Rightarrow \Delta_i$ for each $i \in I$. The induction hypothesis implies that $\mathsf{T} \vdash^{\alpha_i}_{l} \Gamma_i \Rightarrow \Delta_i$ for each i, whereby $\mathsf{T} \vdash^{\beta}_{l} \Gamma \Rightarrow \Delta$ obtains. ⊣

Lemma 11.3 operates in the background of the majority of the results to follow. For that reason I will not make any explicit reference to the lemma.

11.4 Example *To be written.*

11.5 Lemma *If $\mathsf{HA}\omega \vdash^{\alpha}_{k} \Gamma \Rightarrow A$ then this fact can be observed by use of sequents of the form $\Sigma \Rightarrow B$ (i.e., exactly one formula on the right).*

Exercise 11.1 Assign ordinal bounds on the ω-proofs of $A, \Gamma \Rightarrow \Delta, A$ constructed in exercise 9.5.

Revisiting the Embedding lemma (lemma 9.13) it is possible provide ordinal bounds on the size of the resulting ω-proof. Let $\alpha.k = \underbrace{\alpha + \cdots + \alpha}_{k}$.

11.6 Refined embedding lemma *Suppose* $\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$ *and* $\Gamma \Rightarrow \Delta$ *is closed. Then there is* $n, k < \omega$ *such that* $\mathsf{PA}\omega \vdash_k^{\omega.n} \Gamma \Rightarrow \Delta$ *where* $\omega.n = \omega + \cdots + \omega$ *(*n *times). Likewise,* HA *into* $\mathsf{HA}\omega$*.*

Exercise 11.2 Prove the refined embedding lemma following the schema of embedding lemma at the end of chapter 9.

The next lemma hints at part of the usefulness of the ω-rule with the ability to isolate finitary reasoning from infinitary reasoning. The result will be useful in section 12.2.

11.7 Proposition *Let* $A(a_1, \ldots, a_k)$ *be a* Σ_1 *formula. There exists* $m < \omega$ *such that for all* $n_1, \ldots, n_k \in \mathbb{N}$*,*

$$\textit{if } \mathbb{N} \vDash A(\underline{n_1}, \ldots, \underline{n_k}) \textit{ then } \mathsf{HA}\omega \vdash_0^m \Rightarrow A(\underline{n_1}, \ldots, \underline{n_k}).$$

Proof By induction on the rank of A. ⊣

Henceforth, I will omit explicit mention of $\mathsf{PA}\omega$ and write $\vdash_k^\alpha \Gamma \Rightarrow \Delta$ to mean $\mathsf{PA}\omega \vdash_k^\alpha \Gamma \Rightarrow \Delta$. The following results are stated only for $\mathsf{PA}\omega$ but apply equally to $\mathsf{HA}\omega$ in the expected way. Admissibility of weakening becomes

11.8 Weakening Lemma *If* $\vdash_k^\alpha \Gamma \Rightarrow \Delta$ *and* $\Gamma' \Rightarrow \Delta'$ *is closed then* $\vdash_k^\alpha \Gamma', \Gamma \Rightarrow \Delta, \Delta'$*.*

Exercise 11.3 Prove the weakening lemma.

The substitution lemma for $\mathsf{PA}\omega$ takes a different formulation from previously. As sequents are closed, the correct formulation for ω-proofs is that provability depends on the *value* of terms, not their *form*.

11.9 Substitution Lemma *Let* $\Gamma(a) \Rightarrow \Delta(a)$ *be a sequent and* s *and* t *be closed terms such that* $\mathbb{N} \vDash s = t$*. If* $\vdash_k^\alpha \Gamma(s) \Rightarrow \Delta(s)$ *implies* $\vdash_k^\alpha \Gamma(t) \Rightarrow \Delta(t)$*.*

Proof Suppose $\vdash^\alpha_k \Gamma(s) \Rightarrow \Delta(s)$ and $\mathbb{N} \vDash s = t$. Let $\Gamma(a) \Rightarrow \Delta(a)$ be any sequent with at most a free. If $\Gamma(s) \Rightarrow \Delta(s)$ is initial then a case distinction on the different forms this sequent can take confirms that $\Gamma(s) \Rightarrow \Delta(s)$ is also initial provided $\mathbb{N} \vDash s = t$. The other case proceed by transfinite induction on α. ⊣

The final ingredient is the inversion lemma, the statement of which has the same form as before with two new cases treating equality.

11.10 Inversion lemma

1. *If* $\vdash^\alpha_k \Gamma \Rightarrow \Delta, \bot$ *then* $\vdash^\alpha_k \Gamma \Rightarrow \Delta$.
2. *If* $\vdash^\alpha_k s = t, \Gamma \Rightarrow \Delta$ *and* $\mathbb{N} \vDash s = t$ *then* $\vdash^\alpha_k \Gamma \Rightarrow \Delta$.
3. *If* $\vdash^\alpha_k \Gamma \Rightarrow \Delta, s = t$ *and* $\mathbb{N} \nvDash s = t$ *then* $\vdash^\alpha_k \Gamma \Rightarrow \Delta$.
4. *If* $\vdash^\alpha_k \Gamma \Rightarrow \Delta, \forall x F(x)$ *then* $\vdash^\alpha_k \Gamma \Rightarrow \Delta, F(s)$ *for every closed term* s.
5. *If* $\vdash^\alpha_k \exists x F(x), \Gamma \Rightarrow \Delta$ *then* $\vdash^\alpha_k F(s), \Gamma \Rightarrow \Delta$ *for every closed term* s.
6. *Analogous inversion principles for the rules* L∨, R∧, R→ *and* L→.

Proof I show cases 2 & 4.

2. By induction on α. Suppose $\vdash^\alpha_k s = t, \Gamma \Rightarrow \Delta$ and $\mathbb{N} \vDash s = t$. If $s = t, \Gamma \Rightarrow \Delta$ is initial then so is $\Gamma \Rightarrow \Delta$. The other cases are straightforward because the equation $s = t$ cannot be the principal formula of any rule. For if $s = t, \Gamma \Rightarrow \Delta$ is not initial, then there are sequents $\{ \Gamma_i \Rightarrow \Delta_i \mid i < \omega \}$ and ordinals $\{ \alpha_i \mid i < \omega \}$ such that

(a) $\vdash^{\alpha_i}_k s = t, \Gamma_i \Rightarrow \Delta_i$ for each $i < \omega$,

(b) $\alpha_i < \alpha$ for all i,

(c) $\{ \Gamma_i \Rightarrow \Delta_i \mid i < \omega \}$ enumerate all premises of an inference of PAω whose conclusion is $\Gamma \Rightarrow \Delta$.

In the case of unary or binary rules, $\Gamma_i = \Gamma_{i+1}$ and $\Delta_i = \Delta_{i+1}$ for all $i > 0$ or 1. But in the case of either of the two ω-rules, the sequents enumerate the infinitely many premises. By (a)–(c) and the induction hypothesis, $\vdash^\alpha_k \Gamma \Rightarrow \Delta$ holds as desired.

4. The argument is a direct generalisation of the finitary inversion lemma. Suppose $\vdash^\alpha_k \Gamma \Rightarrow \Delta, \forall x F(x)$. If this sequent is initial, then

so is $\Gamma \Rightarrow \Delta, F(s)$ for every closed term s. The rest of the argument proceeds, essentially, as above by a case distinction on the inferences through which $\vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta, \forall x F(x)$ can be derived. The case of R$\forall$ with $\forall x F(x)$ principal bears treatment. The premises of this inference can be assumed to have the form $\Gamma \Rightarrow \Delta, \forall x F(x), F(\underline{n})$. An application of the induction hypothesis (to each premise) yields $\vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta, F(\underline{n})$ for every n. If the desired closed term s is a numeral, this case is complete. Otherwise, let n be the value of s, i.e., $n \in \mathbb{N}$ is such that $\mathbb{N} \models \underline{n} = s$. The substitution lemma then yields $\vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta, F(s)$. ⊣

11.1. Infinitary cut elimination

I begin with the transfinite version of the reduction lemma. Recall, this is statement that borderline cuts can be simulated at the cost of increasing the depth of the proof by a controlled amount. In the finitary case the depth increase was, in the case of classical logic, $m + n$ where m and n bounded the depth of the two cut premises.

Lifting the statement of the reduction lemma to the transfinite realm is reasonably straightforward. Given premises of a borderline cut of height α and β respectively, the cut can be simulated by a height of $\alpha \# \beta$. The use of natural sum is crucial to the argument: the lifting of the finitary argument requires the resulting bound to be order-preserving in both arguments, a property we know fails for traditional ordinal sum $\alpha + \beta$.

11.11 Reduction lemma for PAω *Suppose* $\vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta, C$ *and* $\vdash^{\beta}_{k} C, \Sigma \Rightarrow \Lambda$. *If* $|C| \leq k$ *then* $\vdash^{\alpha\#\beta}_{k} \Gamma, \Sigma \Rightarrow \Delta, \Lambda$.

The reader may surprised to know that there is a great deal of flexibility in proofs of the reduction lemma, which I will demonstrate by presenting a slightly different strategy than we used for in the analysis of classical predicate logic.

Proof The proof branches into cases depending on the form of C. In each case I will establish $\vdash^{\alpha\#\beta}_{k} \Gamma, \Sigma \Rightarrow \Delta, \Lambda$ but the induction will proceed over either α or β (depending on the case) rather than on the sum $\alpha \# \beta$. If the principal connective of C is among $\{\bot, \forall, \wedge, \rightarrow\}$ I will refer to C as *locally negative* (cf. Canvas assignment no. 4). Otherwise, C will be *locally positive*.

Case I: C is atomic or locally negative. Here I proceed by induction on β and show that $\vdash^{\alpha\#\beta}_k \Gamma, \Sigma \Rightarrow \Delta, \Lambda$. I present two subcases:

$C = \forall x D(x)$. If $C, \Sigma \Rightarrow \Lambda$ is initial then $\Sigma \Rightarrow \Lambda$ is also initial and the claim holds by weakening. Otherwise, consider the rule that derives $\vdash^{\beta}_k C, \Sigma \Rightarrow \Lambda$. If the principal formula of the rule is *not* C then the induction hypothesis can be applied directly to its premises and the rule re-applied to derive the desired sequent with correct bounds. If, however, the rule is $\mathsf{L}\forall$ with C principal, the above argument does not work. But in this case there is $\gamma < \beta$ and term t such that

$$\vdash^{\gamma}_k D(t), C, \Sigma \Rightarrow \Lambda.$$

The induction hypothesis yields

$$\vdash^{\alpha\#\gamma}_k D(t), \Gamma, \Sigma \Rightarrow \Delta, \Lambda.$$

From the inversion lemma (part 4) I know also that $\vdash^{\alpha}_k \Gamma \Rightarrow \Delta, D(t)$. Since $|D(t)| < |C| = k$, an application of cut yields $\vdash^{\alpha\#\beta}_k \Gamma, \Sigma \Rightarrow \Delta, \Lambda$.

$C = D \rightarrow E$. I employ a similar argument as above but with a subtle difference in how the induction hypothesis is applied to account for the binary connectives. By the previous argument I can jump directly to the case that C is principal in the derivation of $\vdash^{\beta}_k C, \Sigma \Rightarrow \Lambda$, for which there exist $\gamma, \delta < \beta$ and $\Lambda = \Lambda_0 \cup \Lambda_1$ satisfying

1. $\vdash^{\gamma}_k C, \Sigma \Rightarrow \Lambda_0, D$.
2. $\vdash^{\delta}_k C, E, \Sigma \Rightarrow \Lambda_1$.

I start by applying the inversion lemma to my three hypotheses:

3. $\vdash^{\alpha}_k D, \Gamma \Rightarrow \Delta, E$.
4. $\vdash^{\gamma}_k \Sigma \Rightarrow \Lambda_0, D$.
5. $\vdash^{\delta}_k E, \Sigma \Rightarrow \Lambda_1$.

Then I apply the induction hypothesis between the sequents in 3 and 5 (using 'cut' formula E):

6. $\vdash^{\alpha\#\delta}_k D, \Gamma, \Sigma \Rightarrow \Delta, \Lambda_1$.

$$\dfrac{\dfrac{\vdash^{\gamma}_{k} C,\Sigma \Rightarrow \Lambda_0, D}{\vdash^{\gamma}_{k} \Sigma \Rightarrow \Lambda_0, D}\,\mathrm{IL} \qquad \dfrac{\dfrac{\vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta, C}{\vdash^{\alpha}_{k} D,\Gamma\Rightarrow\Delta,E}\,\mathrm{IL} \qquad \dfrac{\vdash^{\delta}_{k} C,E,\Sigma\Rightarrow\Lambda_1}{\vdash^{\delta}_{k} E,\Sigma\Rightarrow\Lambda_1}\,\mathrm{IL}}{\vdash^{\alpha\#\delta}_{k} D,\Gamma,\Sigma\Rightarrow\Delta,\Lambda_1}\,\mathrm{IH}}{\vdash^{\alpha\#\beta}_{k} \Gamma,\Sigma\Rightarrow\Delta,\Lambda}\,\mathsf{cut}$$

Figure 11.1.: Illustration of the proof method in the reduction lemma for the case $C = D \to E$; IL = 'inversion lemma' and IH = 'induction hypothesis'.

I can now combine 6 and 3 with a (standard) cut:

$$\vdash^{\alpha\#\beta}_{k} \Gamma, \Sigma \Rightarrow \Delta, \Lambda.$$

The conjunction subcase is left to the reader.

Case II: C is locally positive. This case is symmetric to the previous and left to the reader. ⊣

Exercise 11.4 Complete the preceding proof.

Exercise 11.5 Formulate and prove a reduction lemma for $\mathsf{HA}\omega$ following the proof scheme above.

Exercise 11.6 Give an alternative proof of lemma 11.11 using the proof strategy from the reduction lemma for C (lemma 5.4).

In the implication subcase of case II in the proof above, I used the induction hypothesis to simulate a cut on the formula E

11.12 Reduction theorem for $\mathsf{PA}\omega$ *If* $\vdash^{\alpha}_{k+1} \Gamma \Rightarrow \Delta$ *then* $\vdash^{\omega^\alpha}_{k} \Gamma \Rightarrow \Delta$.

Proof Induction on α. If $\Gamma \Rightarrow \Delta$ is initial, the claim holds trivially. So suppose $\vdash^{\alpha}_{k+1} \Gamma \Rightarrow \Delta$ is derived via a rule

$$\frac{\Gamma_i \Rightarrow \Delta_i \text{ for } i \in I}{\Gamma \Rightarrow \Delta}\,*$$

and for each i there is $\alpha_i < \alpha$ such that $\vdash^{\alpha_i}_{k+1} \Gamma_i \Rightarrow \Delta_i$. The induction hypothesis implies that $\vdash^{\omega^{\alpha_i}}_{k} \Gamma_i \Rightarrow \Delta_i$ for each i. So, if $*$ is not cut, then

$$\vdash^{\omega^\alpha}_{k} \Gamma \Rightarrow \Delta$$

obtains by re-applying the rule and observing that $\sup\{\, \omega^\eta \mid \eta < \alpha \,\} \leq \omega^\alpha$. Now suppose that the rule is cut, with cut formula C. If $|C| < k$ the same argument as above applies. Otherwise $|C| = k$ and the reduction lemma is applicable, yielding

$$\vdash_k^{\omega^{\alpha_0} \# \omega^{\alpha_1}} \Gamma \Rightarrow \Delta$$

Since $\omega^{\alpha_0} \# \omega^{\alpha_1} < \omega^\alpha$, the proof is complete. ⊣

The bound in the reduction theorem can be improved fairly easily. For the give proof strategy to work, it suffices to find an order-preserving function $f\colon \mathbb{O} \to \mathbb{O}$ such that $f(\alpha) \geq \sup\{\, f(\xi) \# f(\eta) \mid \xi, \eta < \alpha \,\}$. An obvious candidate is $f\colon \alpha \mapsto 2^\alpha$ (see exercise 10.5) and, indeed, lemma 11.11 can be strengthened by replacing ω^α with 2^α. Certainly, $2^\alpha \leq \omega^\alpha$ for all α, so working with this bound seems a significant improvement. But given that for every additive principal ordinal $\alpha \geq \omega^\omega$ in fact $2^\alpha = \omega^\alpha$ (cf. exercise 10.8), the distinction between exponentiation in the two bases does little in reducing the complexity of cut elimination.

In the next section I will present a strict refinement of the cut elimination theorem in which ordinal exponentiation is directly tied to the *quantifier* rank of the cut formula rather than the full rank.

Let $\omega_0^\alpha := \alpha$ and $\omega_{k+1}^\alpha := \omega^{\omega_k^\alpha}$.

11.13 Cut elimination theorem *If* $\vdash_k^\alpha \Gamma \Rightarrow \Delta$ *then* $\vdash_0^{\omega_k^\alpha} \Gamma \Rightarrow \Delta$.

Proof Consequence of theorem 11.12. ⊣

Exercise 11.7 Formulate and prove a corresponding reduction lemma and cut elimination theorem for $\mathsf{HA}\omega$.

11.14 Embedding theorem *If* $\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$ *and this a closed sequent, then there exists* $\alpha < \varepsilon_0$ *such that*

$$\mathsf{PA}\omega \vdash_0^\alpha \Gamma \Rightarrow \Delta.$$

In addition, α is effectively computable from the given PA*-proof.*

Proof Suppose $\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$. By the embedding lemma (lemma 11.6) there is are n, k such that

$$\mathsf{PA}\omega \vdash_k^{\omega \cdot n} \Gamma \Rightarrow \Delta.$$

Let $\alpha = \omega_k^{\omega \cdot n}$. Then $\alpha < \varepsilon_0$ (by definition 10.22) and

$$\mathsf{PA}\omega \vdash_0^{\alpha} \Gamma \Rightarrow \Delta$$

by theorem 11.13. ⊣

On the basis of cut elimination, a few observations can be already made.

11.15 Corollary PA *and, hence,* HA*, are consistent.*

Proof There can be no cut-free proof of the empty sequent. ⊣

An inspection of the various proofs leading up to corollary 11.15 can strengthen the result by clarifying what mathematical principles suffice to derive the consistency of arithmetic.

11.16 Corollary *Consistency of* PA *can be deduced using only finitary reasoning plus the principle of transfinite induction for ordinals* $\leq \varepsilon_0$.

By 'finitary reasoning' I mean the 'finite' mathematics that can be carried out using only finite objects (such as natural numbers) and primitive recursive functions. Examples include deciding whether one formula is a subformula of another, whether a given primitive recursive function enumerates the premises of an ω-rule (or Gödel codes of sequents) and what the concluding sequent is. It is beyond the scope of these lecture notes to attempt to make the statement more precise, but the following proof 'sketch' hopefully elucidates how this could be achieved and proven.

Proof sketch Suppose there is a finite PA-proof of the empty sequent. The embedding of PA in PAω (lemma 11.6) provides an explicit number $n < \omega$ such that

$$\mathsf{PA}\omega \vdash_n^{\omega \cdot n} \ \Rightarrow .$$

The existence of a cut-free proof of the empty sequent, along with the various results on which theorem 11.13 depends, can now be established by via finitary reasoning plus transfinite induction up to an ordinal strictly smaller than ε_0, for instance the ordinal ω_{n+2} suffices.

As there can be no cut-free proof of the empty sequent, there is no derivation of the empty sequent in PA. ⊣

11.17 Corollary *If Γ is a set of Π^0_1 sentences and Δ a set of Σ^0_1 sentences, then* $\mathsf{PA}\omega \vdash \Gamma \Rightarrow \Delta$ *iff there is a cut-free* $\mathsf{PA}\omega$ *derivation of finite height.*

Proof Exercise. ⊣

11.2. Refining cut elimination arithmetic

To be written. I will jump the gun somewhat.

The *negation rank* (*n-rank*) of a formula, $|F|_*$, counts the nesting depth on the negative side of implications:

$$|A|_* = 0 \quad (A \text{ prime}) \qquad |F \wedge G|_* = \max\{\, |F|_*, |G|_* \,\}$$
$$|\forall x F(x)|_* = |F(a)|_* \qquad |F \to G|_* = \max\{\, |F|_* + 1, |G|_* \,\}$$

Compare with the quantifier hierarchy for this language fragment. Since Π^P_0 is closed under negation, there is no a priori bound on the negation depth of formulas in Π^P_n.

11.18 Lemma *Every Π^P_n formula is equivalent, over weak arithmetic, to a formula with n-rank $n+1$.*

By *weak arithmetic*, I have in mind the theory known as Robinson's Q (see [7, ch. 18]) but primitive recursive arithmetic or, equivalently, the theory known as '$\mathsf{I}\Sigma_1$' suffices (cf. section 9.1).

Proof Using the full logical language, express $F \in \Pi^P_n$ in prefix normal form as

$$(\dagger) \qquad \forall \vec{x}_1 \exists \vec{x}_2 \cdots \exists \vec{x}_m G$$

where G is quantifier-free. We can choose $m \in \{ n, n+1 \}$ and G can be assumed to be Π^p_0 because over weak arithmetic a disjunction $E \vee F$ is provably equivalent to

$$\exists x \exists y (x + y = \mathsf{s0} \wedge (x = 0 \to E) \wedge (x = \mathsf{s0} \to F)).$$

and the leading existential quantifiers can be incorporated into the '$\exists \vec{x}_m$' sequence of quantifiers. It is now straightforward to witness (†) as an equivalent Π^p_m-formula whose negation rank is m. ⊣

A sequent is an expression $\Gamma \Rightarrow \Delta$ without free variables using the logical language isolated at the beginning of this section. Let $\vDash^{\alpha}_{*k} \Gamma \Rightarrow \Delta$ denote derivability in $\mathsf{PA}\omega$ for such sequents in the usual way but with a more liberal cut rule bounded by negation rank:

$$\dfrac{\vDash^{\alpha}_{*k} \Gamma \Rightarrow \Delta, C \qquad \vDash^{\beta}_{*k} C, \Sigma \Rightarrow \Lambda}{\vDash^{\gamma}_{*k} \Gamma, \Sigma \Rightarrow \Delta, \Lambda}\,\mathsf{cut} \quad \text{for } |C|_* < k \text{ and } \max\{ \alpha, \beta \} < \gamma.$$

I assume this variation of $\mathsf{PA}\omega$ satisfies weakening, substitution and inversion lemmas with the same bounds. Given a finite sequence $\vec{A} = (A_i)_{i \leq k}$ of formulas, I will write $\vec{A}, \Gamma \Rightarrow \Delta$ for $A_0, \dots, A_n, \Gamma \Rightarrow \Delta$.

11.19 Refined reduction lemma *Suppose* $\vDash^{\alpha}_{*k} \Gamma_i \Rightarrow \Delta_i, C_i$ *and* $|C_i|_* \leq k$ *for each* $i \leq n$. *If* $\vDash^{\beta}_{*k} \vec{C}, \Sigma \Rightarrow \Lambda$, *then*

(†) $$\vDash^{\alpha+\beta}_{*k} \Gamma_0, \dots, \Gamma_n, \Sigma \Rightarrow \Delta_0, \dots, \Delta_n, \Lambda.$$

Applications of the refined reduction lemma, however, will also be to simulate an ordinary two-premise cut rule. The significance of allowing multiple premises is hidden in the proof. The multi-premise 'cut' can be visualised as either a generalisation of the binary cut rule:

$$\dfrac{\Gamma_0 \Rightarrow \Delta_0, C_0 \qquad \cdots \qquad \Gamma_n \Rightarrow \Delta_n, C_n \qquad \vec{C}, \Sigma \Rightarrow \Lambda}{\Gamma_0, \dots, \Gamma_n, \Sigma \Rightarrow \Delta_0, \dots, \Delta_n, \Lambda}\, n\text{-}\mathsf{cut}$$

Or as sequence of binary cuts

$$\dfrac{\Gamma_n \Rightarrow \Delta_n, C_n \qquad \dfrac{\vdots}{C_n, \Gamma_0, \dots, \Gamma_{n-1}, \Sigma \Rightarrow \Delta_0, \dots, \Delta_{n-1}, \Lambda}}{\Gamma_0, \dots, \Gamma_n, \Sigma \Rightarrow \Delta_0, \dots, \Delta_n, \Lambda}\,\mathsf{cut}$$

where the elided part is

$$\dfrac{\Gamma_1 \Rightarrow \Delta_1, C_1 \qquad \dfrac{\Gamma_0 \Rightarrow \Delta_0, C_0 \qquad \vec{C}, \Sigma \Rightarrow \Lambda}{C_1, \dots, C_n, \Gamma_0, \Sigma \Rightarrow \Delta_0, \Lambda}\,\mathsf{cut}}{\vdots}\,\mathsf{cut}$$

The advantage of the former presentation is that the 'size' of the derivation does not depend on the order of the sequents. This allows the application of an induction hypothesis in cases that the binary cut view grows too large.

Proof The overall structure of the proof will be recognisable as the strategy used in the proof of lemma 11.11. I proceed by induction on β. Suppose

1. $\models^{\alpha}_{*k} \Gamma_i \Rightarrow \Delta_i, C_i$ and $|C_i|_* \leq k$ for each $i \leq n$, and
2. $\models^{\beta}_{*k} \vec{C}, \Sigma \Rightarrow \Lambda$.

I refer to $\vec{C}$ as the *cut* formulas. First, suppose no cut formula is principle in the final rule of assumption 2. If the sequent is initial, then $\Sigma \Rightarrow \Lambda$ is initial and (†) follows by weakening. Therefore, assume C_n is the principal formula in 2. There is a case distinction based on the form of C_n. The focus will therefore be on assumption 2 above and

$$(\ddagger) \qquad \models^{\alpha}_{*k} \Gamma_n \Rightarrow \Delta_n, C_n.$$

If $C_n = \bot$ or is a false equation then (†) results from applying the inversion lemma to (‡). If $C_n = Ps$, then $Pt \in \Lambda$ for some $\mathbb{N} \models s = t$ and (†) also follows from (‡) via substitution. The final case is that C_n is a true equation. But it is not possible for such an atomic formula to be principal in (†).

Moving on to the non-atomic case suppose, to begin, that $C_n = D \wedge E$. From 2 I obtain $\gamma < \beta$ and $F \in \{ D, E \}$ such that

3. $\models^{\gamma}_{*k} \vec{C}, F, \Sigma \Rightarrow \Lambda$.

Applying the inversion lemma to (‡) yields

4. $\models^{\alpha}_{*k} \Gamma_n \Rightarrow \Delta_n, F$.

Adding this final sequent to the list of hypotheses in 1 above, and using 3 in place of 2, I can apply the induction hypothesis (as $\gamma < \beta$), which derives (†).

The quantifier case, $C_n = \forall x D(x)$ is essentially the same argument. From principality of C_n and the inversion lemma I know

3′. $\vdash^{\gamma}_{*k} \vec{C}, D(s), \Sigma \Rightarrow \Lambda$ for some $\gamma < \beta$ and term s.

4′. $\vdash^{\alpha}_{*k} \Gamma_n \Rightarrow \Delta_n, D(s)$.

I can then deduce (†) from the induction hypothesis by adding 4′ to the list in 1 and 3′ in place of 2.

The final case is involves a different in the argument. Suppose $C_n = D \to E$. Hypothesis 2 and the inversion lemma yields three derivations to work from:

3″. $\vdash^{\gamma}_{*k} \vec{C}, E, \Sigma \Rightarrow \Lambda$,

4″. $\vdash^{\delta}_{*k} \vec{C}, \Sigma \Rightarrow \Lambda, D$,

5″. $\vdash^{\alpha}_{*k} D, \Gamma_n \Rightarrow \Delta_n, E$,

for $\gamma, \delta < \beta$. The first and third of these can be used with the induction hypothesis, obtaining as conclusion,

6″. $\vdash^{\alpha+\gamma}_{*k} D, \Gamma_0, \ldots, \Gamma_n, \Sigma \Rightarrow \Delta_0, \ldots, \Delta_n, \Lambda$.

To derive (†), I need to remove the formula D in 6″ I apply a cut against a second application of the induction hypothesis, this time using 4″ (and not expanding the list in 2):

7″. $\vdash^{\alpha+\delta}_{*k} \Gamma_0, \ldots, \Gamma_n, \Sigma \Rightarrow \Delta_0, \ldots, \Delta_n, \Lambda, D$.

As $|D|_* < k$ a standard cut can be used between sequents 4″ and 6″, the conclusion being (†). ⊣

As the focus is on better bounds on cut elimination, I will switch to base-2 exponentiation for the reduction theorem:

11.20 Refined reduction theorem *Suppose* $\vdash^{\alpha}_{*k+1} \Gamma \Rightarrow \Delta$. *Then* $\vdash^{2^\alpha}_{*k} \Gamma \Rightarrow \Delta$.

Proof This argument proceeds just as usual. Jumping to the main case, suppose $\vdash^{\alpha}_{*k+1} \Gamma \Rightarrow \Delta$ is derived via cut:

$$\vdash^{\beta}_{*k+1} \Gamma \Rightarrow \Delta, C \qquad \vdash^{\gamma}_{*k+1} C, \Sigma \Rightarrow \Lambda$$

where $\beta, \gamma < \alpha$ and $|C|_* \leq k$. The induction hypothesis yields

$$\vdash^{2^\beta}_{k} \Gamma \Rightarrow \Delta, C \qquad \vdash^{2^\gamma}_{k} C, \Sigma \Rightarrow \Lambda$$

and the refined reduction lemma implies $\vdash^{2^\alpha}_{*k} \Gamma \Rightarrow \Delta$. ⊣

11.21 Refined cut elimination *If* $\vDash^{\alpha}_{*k} \Gamma \Rightarrow \Delta$ *then* $\vDash^{\gamma}_{*0} \Gamma \Rightarrow \Delta$ *where* $\gamma = 2^{\alpha}_{k}$.

To be written.

11.22 Theorem *If* $\mathsf{I\Sigma}_n \vdash A$ *then* $\mathsf{PA}\omega \vdash^{\alpha}_{0} \Gamma \Rightarrow \Delta$ *for some* $\alpha < \omega_{n+1}$.

Proof sketch From $\mathsf{I\Sigma}_n \vdash A$ we deduce that $\mathsf{PA} \vdash \;\Rightarrow A$ with a proof in which all cuts have n-rank $\leq n$. The reason is that the induction rule is only applied to formulas with n-rank $\leq n$ and finitary cut elimination is available in PA to reduce the cut rank to formulas of the same n-rank as uses of induction. The embedding lemma of PA into $\mathsf{PA}\omega$ yields $\mathsf{PA}\omega \vDash^{\omega.k}_{*n} \;\Rightarrow A$, so $\mathsf{PA}\omega \vdash^{\gamma}_{0} \;\Rightarrow A$ where

$$\gamma = 2^{\omega.k}_{n}.$$

Recall that $2^{\omega.k} = \omega^k$, whence

$$\gamma \leq \omega^k_n < \omega_{n+1}. \qquad \dashv$$

12. Transfinite induction and proof-theoretic ordinals

The final chapter is devoted to proving the optimality of theorem 11.14/corollary 11.16. I will show how the principle of transfinite induction can be rendered in arithmetic and show that it is precisely the ordinal ε_0 that marks the boundary between the provable and unprovable instance of transfinite induction. It turns out that many interesting theories extending arithmetic (including set theories and theories of second-order arithmetic) can be characterised in such a way. The ordinal corresponding to 'provable instances of transfinite induction' is one of a number of ways in which ordinals can be used to describe, delineate and compare mathematical theories. *Ordinal analysis*, in a nutshell, is the isolation and comparison of such ordinal measures.

12.1. Provable transfinite induction

In the present section I will define precisely one way to assign an ordinal to a theory of arithmetic and show that under this measure the *proof-theoretic ordinal* of Peano arithmetic is at least ε_0. The following section will establish that this bound is optimal.

I begin by recalling some basic order-theory.

12.1 Definition Let $\prec$ be a relation on a non-empty set X. $\prec$ is:

- *well-founded* if there is no infinite $\prec$-descending sequence, namely no sequence $(x_i)_{i<\omega}$ such that $x_{i+1} \prec x_i$ for every i.
- a *well-order* if $\prec$ is linear and well-founded.

12.2 Example *The following two orderings on natural numbers are well-orders.*

The third is well-founded but not a well-order.

$$
\begin{aligned}
&m <_1 n \textit{ iff } 0 < m < n, \textit{ or } n = 0 \textit{ and } m \neq 0.\\
&m <_2 n \textit{ iff } \begin{cases} m < n, \textit{and both are even or both odd, or}\\ n \textit{ even and } m \textit{ odd.}\end{cases}\\
&m <_2 n \textit{ iff } m = 0 \textit{ and } n \neq 0.
\end{aligned}
$$

The proof of the next lemma is left as an exercise.

12.3 Lemma *A relation $\prec$ on a non-empty set X if a well-order iff every non-empty $Y \subseteq X$ has a $\prec$-least element.*

Let $\prec$ be a well-founded ordering of $\mathbb{N}$. I define

$$
\begin{aligned}
|n|_\prec &\coloneqq \sup\{\, |m|_\prec + 1 \mid m \prec n \,\}\\
\|{\prec}\| &\coloneqq \sup\{\, |n|_\prec + 1 \mid n \in \mathbb{N} \,\}
\end{aligned}
$$

Well-foundedness ensures the above notions are well-defined. I call $|n|_\prec$ the order-type of n in $\prec$, and $\|{\prec}\|$ the order-type of $\prec$. The function $|\cdot|_\prec \colon \mathbb{N} \to \mathbb{O}$ is order-preserving: $m \prec n$ implies $|m|_\prec < |n|_\prec$ and its range is a segment of $\mathbb{O}$. If $\prec$ is a well-order then the function is also injective, whence $|\cdot|_\prec$ is an order-preserving enumeration of $\mathbb{N}$ in $\mathbb{O}$.

12.4 Example *I compute the order types of natural numbers in the three orderings from example 12.2. Note, for the standard ordering on $\mathbb{N}$,*

$$
\begin{aligned}
|n|_< &= n \quad \textit{for every } n\\
\|{<}\| &= \sup\{\, n + 1 \mid n \in \mathbb{N} \,\} = \omega.
\end{aligned}
$$

The ordering $<_1$ satisfies

$$
\begin{gathered}
|n+1|_{<_1} = n \quad \textit{and} \quad |0|_{<_1} = \omega\\
\|{<_1}\| = \omega + 1.
\end{gathered}
$$

The ordering $<_2$ satisfies

$$
\begin{aligned}
|2n|_{<_2} &= n\\
|2n+1|_{<_2} &= \omega + n\\
\|{<_2}\| &= \omega + \omega.
\end{aligned}
$$

The ordering $<_3$ satisfies

$$\begin{aligned} |0|_{<_3} &= 0 \\ |n|_{<_3} &= 1 \ \textit{for all } n > 0 \\ \|{<_3}\| &= 2. \end{aligned}$$

12.5 Lemma *If $\prec$ is a well-founded relation on $\mathbb{N}$ then for every $\alpha < \|{\prec}\|$ there exists $n \in \mathbb{N}$ such that $|n|_\prec = \alpha$. If $\prec$ is a well-ordering then n is unique.*

For $\prec$ a primitive recursive relation on $\mathbb{N}$ the representation theorem for arithmetic (theorem 9.6) presents a Δ_0 formula $F_\prec(a, b)$ in the language of arithmetic (without the predicate P) such that for all $n, m \in \mathbb{N}$,

$$\mathsf{PA} \vdash F_\prec(\underline{m}, \underline{n}) \text{ iff } m \prec n.$$

In what follows, I will write $a \prec b$ for the formula $F_\prec(a, b)$, and use $\forall x \prec aF(x)$ as an abbreviation for the formula $\forall x(x \prec a \land F(x))$.

12.6 Definition For each primitive recursive ordering $\prec$ and formula $A(x)$ define formulas:

$$\begin{aligned} \mathsf{Prog}_\prec A &:= \forall x(\forall y \prec x\, A(y) \to A(x)) \\ \mathsf{TI}_\prec(A, a) &:= \mathsf{Prog}_\prec A \to \forall y \prec a\, A(y) \\ \mathsf{TI}_\prec(A) &:= \forall x\, \mathsf{TI}_\prec(A, x) \end{aligned}$$

If $\prec$ is a well-order, the formula $\mathsf{Prog}_\prec A$ expresses progressiveness of the set of ordinals $|n|_\prec$ such that $\mathbb{N} \vDash A(\underline{n})$. In the case $\prec\ =\ <$ is the standard ordering on $\mathbb{N}$, this is the same as $A(x)$ being *inductive*. As a result, $\mathsf{TI}_\prec(A, a)$ states the principle of transfinite induction for this set restricted to the segment of ordinals $\{\, |n|_\prec \mid n \prec a \,\}$.

12.7 Definition Let T be a theory in the language $\mathscr{L}_\mathrm{A}$. The *proof theoretic ordinal* of T is the ordinal $\|\mathsf{T}\|$ defined by

$$\|\mathsf{T}\| = \sup\{\, \|{\prec}\| \mid \prec \text{ is a pr. rec., well-founded and } \mathsf{T} \vdash \mathsf{TI}_\prec(P) \,\}$$

The goal of this section is a lower bound on the proof-theoretic ordinal of Peano and Heyting arithmetic:

12.8 Theorem $\|\mathsf{PA}\| \geq \|\mathsf{HA}\| \geq \varepsilon_0$.

Unpacking theorem 12.8, it states that there exists a sequence of well-founded relations $\{ \prec_i \}_i$ such that $\sup_i \|\prec_i\| = \varepsilon_0$ and $\mathsf{HA} \vdash \mathsf{TI}_{\prec_i}(P)$ for each i. A sequence of well-founded relations is not, strictly speaking, necessary as a single well-ordering can be defined of order-type ε_0 and for which transfinite induction can be proven for each proper initial segment. I leave the proof of the next lemma as an exercise.

12.9 Lemma *There exists a primitive recursive well-ordering of $\mathbb{N}$ of order-type ε_0 and primitive recursive functions $\oplus$ and $\dot\omega$ representing addition and exponentiation respectively in the sense that $\oplus\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and $\dot\omega\colon \mathbb{N} \to \mathbb{N}$ satisfy*

$$|m \oplus n|_\prec = |m|_\prec \,\#\, |n|_\prec \qquad \textit{and} \qquad |\dot\omega(m)|_\prec = \omega^{|m|_\prec}$$

for all $m, n \in \mathbb{N}$.

Exercise 12.1 Prove lemma 12.9. Hint: Utilise the Cantor normal form theorem and a (primitive recursive) bijection between $\mathbb{N}$ and finite sequences of $\mathbb{N}$.

Exercise 12.2 Prove the following generalisation of lemma 12.9: Given a primitive recursive well-ordering of order-type α construct a primitive recursive ordering of $\mathbb{N}$ of order-type ε_α.

In the following $\prec$ denotes the primitive recursive well-ordering of order type ε_0 given by lemma 12.9. The proof of theorem 12.8 relies on one lemma whose proof is rather time-consuming and will be omitted:

12.10 Lemma *For every formula $A(a)$ in the language of arithmetic, there exists a formula $A'(a)$ such that*

$$\mathsf{PA} \vdash \forall x\big(\mathsf{TI}_\prec(A', x) \to \mathsf{TI}_\prec(A, \dot\omega^x)\big).$$

Although I won't present the proof, it will be useful to know how A' is constructed from A. First, I present the construction as an operation on sets of ordinals. I write $\beta \subseteq O$ as shorthand for $(\forall \xi < \beta)\xi \in O$. Given $O \subseteq \mathbb{O}$, define O' as the class

$$O' = \{ \alpha \mid \forall \xi(\xi \subseteq O \text{ implies } \xi + \omega^\alpha \subseteq O) \}.$$

It is not difficult to see that O' is a segment and $\alpha \in O'$ implies $\omega^\alpha \in O$, from which $\omega^{\alpha+1} \subseteq O$ quickly follows. Expressing the operation in the language of arithmetic provides the formula A' in lemma 12.10:

$$A'(a) := \forall x(\forall y \prec x\, A(y) \to \forall y \prec x \oplus \dot{\omega}^a\, A(y)).$$

The above remarks concerning the properties of O and O' can be shown in PA to hold for A and A'. Thus, to prove the lemma it suffices to show that $\mathsf{PA} \vdash \mathsf{Prog}_\prec A \to \mathsf{Prog}_\prec A'$, which involves similar argumentation.

12.2. Bounding provable transfinite induction

The goal of this section is the converse to theorem 12.8:

12.11 Theorem $\|\mathsf{PA}\| \leq \varepsilon_0$.

The proof strategy is as follows. I fix an arbitrary primitive recursive well-ordering $\prec$ and suppose that $\mathsf{TI}_\prec(P)$ is provable in PA. The embedding theorem for $\mathsf{PA}\omega$ provides an ordinal $\alpha < \varepsilon_0$ and a cut-free proof of $\mathsf{TI}_\prec(P)$ bounded above by α. Applying the inversion lemma yields, for every $n \in \mathbb{N}$,

$$(\dagger) \qquad \mathsf{PA}\omega \vdash^\alpha_0 \mathsf{Prog}_\prec P \Rightarrow \forall x \prec \underline{n}\, Px.$$

I want to infer from (†) that $|n|_\prec < \varepsilon_0$ for every n. In fact, it will be the case that (†) holds only if $|n|_\prec \leq \alpha$.

To that aim I will utilise an extension of $\mathsf{PA}\omega$, called $\mathsf{PA}\omega + (\prec)$, such that (†) implies

$$(\ddagger) \qquad \mathsf{PA}\omega + (\prec) \vdash^\alpha_0 \Rightarrow \forall x \prec \underline{n} Px.$$

The transfer from (†) to (‡) will depend on a cut elimination theorem for $\mathsf{PA}\omega + (\prec)$. An analysis of cut-free provability in $\mathsf{PA}\omega + (\prec)$ will lead me from (‡) quite directly to $|n|_\prec \leq \alpha$ for all n, i.e., $\|\prec\| \leq \alpha < \varepsilon_0$.

I begin by introducing the extension of $\mathsf{PA}\omega$ used in (‡). Henceforth, let $\prec$ be a fixed primitive recursive well-ordering on $\mathbb{N}$. For the sake of simplifying notation, I will write $s^\mathbb{N}$ for the value of s in the standard model, i.e., the n such that $\mathbb{N} \models \underline{n} = s$. This notation presupposes that s is closed.

12.12 Definition The rule ($\prec$) comprises all instances of the inference

$$\frac{\Gamma \Rightarrow \Delta, P\underline{n} \quad \text{for every } n \prec s^{\mathbb{N}}}{\Gamma \Rightarrow \Delta, Ps}\prec$$

The infinitary sequent calculus $\mathsf{PA}\omega + (\prec)$ extends the axioms and rules of $\mathsf{PA}\omega$ by the inference ($\prec$) above. The relation $\mathsf{PA}\omega + (\prec) \vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta$ is given as in definition 11.2.

In general, the rule ($\prec$) will have infinitely many premises like the ω-rules. For instance, if there is an element m with order-type ω, and $M = \{ n \in \mathbb{N} \mid n \prec m \}$ then one instance of the rule is

$$\frac{\Gamma \Rightarrow P\underline{n} \text{ for all } n \in M}{\Gamma \Rightarrow P\underline{m}}\prec$$

The next three lemmas provide the motivation for this extension of $\mathsf{PA}\omega$.

12.13 Lemma *If* $\mathsf{PA}\omega \vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta$ *then* $\mathsf{PA}\omega + (\prec) \vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta$.

Proof Immediate. ⊣

12.14 Lemma $\mathsf{PA}\omega + (\prec) \vdash^{\omega}_{0} \Rightarrow \mathsf{Prog}_{\prec}P$.

Proof Recall that $\mathsf{Prog}_{\prec}P = \forall x(\forall y(y \prec x \rightarrow Py) \rightarrow Px)$. Let k be the constant given by proposition 11.7 such that $\mathsf{PA}\omega \vdash^{k}_{0} \Rightarrow \underline{m} \prec \underline{n}$ for all $m \prec n$. For every $n \in \mathbb{N}$ I obtain the following derivation in $\mathsf{PA}\omega$ (with implicit application of weakening) for all $m, n \in \mathbb{N}$ satisfying $m \prec n$:

$$\dfrac{\dfrac{\dfrac{}{\vdash^{0}_{0} P\underline{m} \Rightarrow P\underline{m}}\,\mathsf{id} \qquad \begin{array}{c}\vdots\\ \vdash^{k}_{0} \Rightarrow \underline{m} \prec \underline{n}\end{array}}{\vdash^{k+1}_{0} \underline{m} \prec \underline{n} \rightarrow P\underline{m} \Rightarrow P\underline{m}}\,\mathsf{L}{\rightarrow}}{\vdash^{k+2}_{0} \forall y \prec \underline{n}\, Py \Rightarrow P\underline{m}}\,\mathsf{L}\forall$$

Continuing the derivation in $\mathsf{PA}\omega + (\prec)$:

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots\\ \vdash^{k+2}_{0} \forall y \prec \underline{n}\, Py \Rightarrow P\underline{m} \text{ for all } m \prec n\end{array}}{\vdash^{k+3}_{0} \forall y \prec \underline{n}\, Py \Rightarrow P\underline{n}}\prec}{\vdash^{k+4}_{0} \Rightarrow (\forall y \prec \underline{n}\, Py) \rightarrow P\underline{n}}\,\mathsf{R}{\rightarrow} \qquad \text{for every } n}{\vdash^{k+5}_{0} \Rightarrow \mathsf{Prog}_{\prec}P}\,\mathsf{R}\forall$$

An application of bound weakening completes the proof. ⊣

12.15 Refined embedding lemma *If* $\mathsf{PA} \vdash \mathsf{TI}_{\prec}(P)$ *then there exists* $k < \omega$ *such that for all* $n \in \mathbb{N}$*,*

$$\mathsf{PA}\omega + (\prec) \vdash_k^{\omega^2} \; \Rightarrow \forall y \prec \underline{n}\, P y.$$

Proof The embedding lemma for $\mathsf{PA}\omega$ (lemma 11.6) and inversions yields a $k < \omega$ such that for all $n \in \mathbb{N}$:

$$\mathsf{PA}\omega \vdash_k^{\omega . k} \mathsf{Prog}_{\prec} P \Rightarrow \forall y \prec \underline{n}\, P y$$

Lemma 12.14 and a pair of cuts completes the argument. ⊣

Paired with cut elimination for $\mathsf{PA}\omega + (\prec)$, treated in the next section, the lemma above yields (‡). Under the assumption of cut elimination (with the same bounds as $\mathsf{PA}\omega$), just one lemma stands before an optimal upper bound on the proof-theoretic strength of PA. This is the lemma below.

Since $\prec$ is a fixed well-ordering, for $\alpha < \|\prec\|$ I will write $\overline{\alpha}$ for the numeral $\underline{n}$ such that $\alpha = |n|_{\prec}$.

12.16 Bounding lemma *Let* $\alpha_1, \dots, \alpha_m, \beta_0, \dots, \beta_n < \|\prec\|$*. If*

$$\mathsf{PA}\omega + (\prec) \vdash_0^{\gamma} P\overline{\alpha_1}, \dots, P\overline{\alpha_m} \Rightarrow P\overline{\beta_0}, \dots, P\overline{\beta_n}$$

then $\min\{ \beta_0, \dots, \beta_n \} \leq \max\{ \alpha_1, \dots, \alpha_m \} + \gamma$.

Proof Induction on γ. If $P\overline{\alpha_1}, \dots, P\overline{\alpha_m} \Rightarrow P\overline{\beta_0}, \dots, P\overline{\beta_n}$ is initial, then $\alpha_i = \beta_j$ for some i and j and the claim holds vacuously. If, however, the sequent is not initial then, as the derivation is cut-free, the final rule applied must be an instance of $(\prec)$. I can assume, without loss of generality, that the principal formula is $P\overline{\beta_n}$, i.e., that the inference applied is

$$\frac{P\overline{\alpha_1}, \dots, P\overline{\alpha_m} \Rightarrow P\overline{\beta_0}, \dots, P\overline{\beta_n}, P\overline{\delta} \quad \text{for all } \delta < \beta_n}{P\overline{\alpha_1}, \dots, P\overline{\alpha_m} \Rightarrow P\overline{\beta_0}, \dots, P\overline{\beta_n}} \prec$$

For each $\delta < \beta_n$ the corresponding premise has a cut-free derivation of height $< \gamma$. That is, for every $\delta < \beta_n$ there exists $\gamma_\delta < \gamma$ such that

$$\mathsf{PA}\omega + (\prec) \vdash_0^{\gamma_\delta} P\overline{\alpha_1}, \dots, P\overline{\alpha_m} \Rightarrow P\overline{\beta_0}, \dots, P\overline{\beta_n}, P\overline{\delta}.$$

Let $\beta = \min\{\beta_0, \dots, \beta_n\}$ and $\alpha = \max\{\alpha_1, \dots, \alpha_m\}$. The induction hypothesis implies that

$$\text{for every } \delta < \beta_n,\ \min\{\beta, \delta\} \leq \alpha + \gamma_\delta. \tag{12.1}$$

Consider two cases. First, suppose $\beta < \beta_n$. Choosing $\delta = \beta$ in (12.1) yields

$$\beta \leq \alpha + \gamma_\beta < \alpha + \gamma,$$

whereby the claim holds as desired. Otherwise, $\beta = \beta_n$, and

$$\begin{aligned} \beta = \sup\{\delta + 1 \mid \delta < \beta\} &\leq \sup\{\alpha + \gamma_\delta + 1 \mid \delta < \beta\} && \text{by (12.1)} \\ &\leq \alpha + \sup\{\gamma_\delta + 1 \mid \delta < \beta\} && \text{continuity} \\ &\leq \alpha + \gamma. \end{aligned}$$

⊣

Proof of theorem 12.11 (assuming cut elmination) Let $\prec$ be any primitive recursive well-order of $\mathbb{N}$ and suppose $\mathsf{PA} \vdash \mathsf{TI}_\prec(P)$. Let $\alpha = \|\prec\|$. The refined embedding lemma (lemma 12.15) provides a finite k such that for all $n \in \mathbb{N}$

$$\mathsf{PA}\omega + (\prec) \vdash_k^{\omega^2} \Rightarrow \forall y \prec \underline{n}\, Py.$$

In particular, for every $\beta < \alpha$,

$$\mathsf{PA}\omega + (\prec) \vdash_k^{\omega^2} \Rightarrow P\overline{\beta}.$$

Cut elimination for $\mathsf{PA}\omega + (\prec)$ provides an ordinal $\gamma < \varepsilon_0$ such that (see next section) for every $\beta < \alpha$

$$\mathsf{PA}\omega + (\prec) \vdash_0^{\gamma} \Rightarrow P\overline{\beta}.$$

The bounding lemma ensures that $\beta \leq \gamma$, meaning that $\|\prec\| \leq \gamma + 1 < \varepsilon_0$. ⊣

12.3. Cut elimination, revisited

What remains is to confirm cut elimination for the extended calculus $\mathsf{PA}\omega + (\prec)$. The reader can confirm that weakening and substitution remain admissible in this extension.

12.17 Weakening Lemma *If* $\mathsf{PA}\omega + (\prec) \vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta$ *and* $\Gamma' \Rightarrow \Delta'$ *is closed then* $\mathsf{PA}\omega + (\prec) \vdash^{\alpha}_{k} \Gamma', \Gamma \Rightarrow \Delta, \Delta'$.

12.18 Substitution Lemma *Let* $\Gamma(a) \Rightarrow \Delta(a)$ *be a sequent with a the only free variable, and let s and t be closed terms such that* $\mathbb{N} \models s = t$. *If* $\mathsf{PA}\omega + (\prec) \vdash^{\alpha}_{k} \Gamma(s) \Rightarrow \Delta(s)$ *then* $\mathsf{PA}\omega + (\prec) \vdash^{\alpha}_{k} \Gamma(t) \Rightarrow \Delta(t)$.

Exercise 12.3 Prove the weakening and substitution lemmas for $\mathsf{PA}\omega + (\prec)$.

Precisely the same formulation of the reduction lemma also holds, but here there are some notable changes to the proof. I present only the 'simple' version of this result and leave the quantifier-relevant form for the reader.

12.19 Reduction lemma *Suppose* $\mathsf{PA}\omega + (\prec) \vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta, C$ *and* $\mathsf{PA}\omega + (\prec) \vdash^{\beta}_{k} C, \Gamma \Rightarrow \Lambda$. *If* $|C| = k$ *then* $\mathsf{PA}\omega + (\prec) \vdash^{\alpha\#\beta}_{k} \Gamma \Rightarrow \Delta, \Lambda$.

Proof Like the inferences of $\mathsf{PA}\omega$, the rule $(\prec)$ has the property of just one principal formula, namely

$$\frac{\Gamma_i \Rightarrow \Delta_i \text{ for } i \in I}{\Gamma \Rightarrow \Delta}$$

is an instance iff there is $F \in \Delta$ such that

$$\frac{\Sigma, \Gamma_i \Rightarrow \Delta_i, \Lambda \text{ for } i \in I}{\Sigma \Rightarrow \Lambda, F}$$

is an instance for all Σ and Λ.

As such, the new rule does not affect the part of the argument where C is not principal in one of the assumptions. So it suffices to treat the case in which $C = Ps$ for some s and is principal in both assumptions. But if Ps is principal in the proof $\vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta, C$ then inference deriving this sequent is either initial (whence $Pt \in \Gamma$ for $\mathbb{N} \vDash s = t$) or the conclusion of $(\prec)$. In the latter case, however, it is not clear how to use the premises of the rule against the second assumption. Fortunately, though, it is not necessary because we are assuming that C is principal in the second hypothesis, $\vdash^{\beta}_{k} C, \Gamma \Rightarrow \Lambda$. For this to be the case, $C, \Gamma \Rightarrow \Lambda$ must be an initial sequent, meaning that $Pt \in \Lambda$ such that $\mathbb{N} \vDash s = t$. The substitution lemma applied to the *first* hypothesis, shows derivability of $\vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta, \Lambda$. ⊣

Exercise 12.4 Complete the proof of the reduction lemma.

Exercise 12.5 Formulate and prove a quantifier-relevant formulation of the reduction lemma for $\mathsf{PA}\omega + (\prec)$ following the schema of **??**.

12.20 Cut elimination *If* $\mathsf{PA}\omega + (\prec) \vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta$ *then* $\mathsf{PA}\omega + (\prec) \vdash^{\omega^{\alpha}_{k}}_{0} \Gamma \Rightarrow \Delta$.

Proof The proof proceeds precisely as before. ⊣

12.4. Characterisation of provable transfinite induction

Combining the results in this chapter:

12.21 Proof-theoretic characterisation theorem *The proof-theoretic ordinal of Peano and Heyting arithmetic is* ε_0.

Proof As $\varepsilon_0 \leq \|\mathsf{HA}\| \leq \|\mathsf{PA}\|$ by theorem 12.8 and $\|\mathsf{PA}\| \leq \varepsilon_0$ by theorem 12.11. ⊣

12.22 Independence of transfinite induction *There is a primitive recursive well-ordering* $\prec$ *on* $\mathbb{N}$ *and a formula* A *in the language of arithmetic such that* $\mathsf{PA} \nvdash \mathsf{TI}_{\prec}(A)$.

The following will be a consequence of theorem 11.22, but it needs to be refined.

12.23 Theorem *The proof-theoretic ordinal of* $\mathsf{I}\Sigma_n$ *for* $n > 0$ *is* ω_{n+1}.

Bibliography

[1] G S Boolos, J P Burgess, and R C Jeffrey. *Computability and Logic*. Cambridge University Press, 5th ed edition, 2007.

[2] Georg Cantor. Beiträge zur begründung der transfiniten mengenlehre ii. *Mathematische Annalen*, 49(2):207–246, 1897.

[3] Gehard Gentzen. Neue fassung des widerspruchsfreiheitsbeweises für die reine zahlentheorie. In *Forschungen zur Logik und zur Grundlegung der exacten Wissenschaften*, volume Neue Folge 4, pages 19–44. Hirzel, Leipzig, 1938. English translation, "New Version of the Consistency Proof for Elementary Number Theory", in [4]: 252–286.

[4] Gehard Gentzen. *The Collected Papers of Gerhard Gentzen*, volume 55 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, Amsterdam, 1969.

[5] Gerhard Hessenberg. *Grundbegriffe der Mengenlehre*. Göttingen, 1906.

[6] Sara Negri, Jan von Plato, and Aarne Ranta. *Structural Proof Theory*. Cambridge University Press, 2001.

[7] Open Logic Contributers and Logic Group at GU. *Logial Theory*. University of Gothenburg, 2024.

[8] Michael Rathjen. Proof theory. unpublished lecture notes, 2012.

[9] Kurt Schütte. Beweistheoretische erfassung der unendlichen induktion in der zahlentheorie. *Mathematische Annalen*, 5(5):369–389, 1950.