Lecture Notes in Proof Theory

Work in progress

Graham E. Leigh

5th September 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* 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

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 theory — 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. These are the kind of questions that proof theory attempts to address.

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

Module I.

Two Calculi for Two Logics

2. Preliminaries

Set-theoretic notation. Let X be a set.

- $\mathscr{P}X$ is the power set of X.
- $X^{<\omega}$ denotes the set of finite sequences in X, namely the set of $(x_1, \ldots, x_n)$ for $n < \omega$ and $x_i \in X$.
- The cardinality of X is denoted $|X|$; except where stated otherwise, this will invariably be either a natural number (X is finite) or ω (meaning X is countably infinite).

2.1. The language of logic

The *logical symbols of propositional logic* are

$$\wedge \quad \vee \quad \rightarrow \quad \bot$$

collectively called the *(propositional) connectives*. To these one adds a collection $\mathscr{P}$ of *propositional variables* to obtain a *propositional language*.

The *logical symbols of (first-order) predicate logic* extends the propositional symbols by

- Quantifiers: $\forall$ and $\exists$.
- Bound variables: $v_0, v_1, \ldots$.
- Free variables: $a_0, a_1, \ldots$.

2.1 Definition
A *first-order language* extends the logical symbols by two sets of *non-logical* symbols:

- a set $\mathscr{F}$ of *function symbols*;
- a set $\mathscr{P}$ of *predicates*;

- a function $ar\colon \mathscr{F} \cup \mathscr{P} \to \mathbb{N}$ assigning each symbol a natural number called the *arity*.

The *propositional* fragment of a first-order language arises by dropping all function symbols and all predicates of non-zero arity. ⌟

A function symbol $f \in \mathscr{F}$ with arity $ar(f) = 0$ is called a *constant*; a predicate $P \in \mathscr{P}$ with arity 0 is a *propositional variable*. A symbol is *nullary*, *unary*, ..., *n-ary* if it has arity $0, 1, \ldots, n$, etc..

Terms and formulas are defined as expected but should adhere to the free/bound variable distinction.

2.2 Definition · Term
The *terms* are defined inductively as follows:

1. Every free variable is a term
2. Given terms $t_1, \ldots, t_n$ and an n-ary function symbol f, $f t_1 \cdots t_n$ is a term.

Adding bound variables into the mix creates the class of syntactic objects I call *pre-terms*:

1. Every variable (free or bound) is a pre-term.
2. Given pre-terms $t_1, \ldots, t_n$ and an n-ary function symbol f, $f t_1 \cdots t_n$ is a pre-term.

The variables occurring in a pre-term t are called the *active* (of the pre-term). In other words, a term is a pre-term in which only free variables are active. A (pre-)term with no active variables is *closed*. ⌟

With terms come formulas.

2.3 Definition · Atomic formula; prime formula
An expression $P t_1 \cdots t_n$ where P is an n-ary predicate and $t_1, \ldots, t_n$ are terms is called an *atomic formula*. The atomic formulas together with the symbol $\bot$ are, collectively, the *prime* formulas. ⌟

2.4 Definition · Pre-formula
The *pre-formulas*, and their active variables, are generated by the following clauses.

1. Given pre-terms $t_1, \ldots, t_n$ and n-ary predicate P, $Pt_1 \cdots t_n$ is a pre-formula. A variable is *active* in $Pt_1 \cdots t_n$ iff it is active in (at least) one of the t_i.
2. $\bot$ is a pre-formula with no active variables.
3. If F and G are pre-formulas, then so is $F \to G$, $F \wedge G$ and $F \vee G$. The active variables in each case is the union of active variables of each of F and G.
4. If F is a pre-formula and x a bound variable, then $\forall x F$ and $\exists x F$ are pre-formulas. The active variables of $\forall x F$ and $\exists x F$ are the active variables of F minus the variable x. ⌟

2.5 Definition · Formula
A *formula* is a pre-formula for which only free variables are active. A formula with *no* active variables is called *closed* or a *sentence*. ⌟

It is helpful in many cases to associate a numerical measure of *complexity* to (pre-)formulas. There are many choices. I take the following, which I call the *rank*.

2.6 Definition · Rank
The *rank* of a pre-formula F is denoted $|F|$ and determined by recursion on its generation:

- $|F| = 0$ if F is prime.
- $|F \wedge G| = |F \vee G| = |F \to G| = \max\{ |F|, |G| \}$.
- $|\forall x F| = |\exists x F| = |F|$. ⌟

2.7 Definition · Substitution
Let F be a pre-formula, a a free variable and t a pre-term. I write $F[t/a]$ for the pre-formula that results by substituting t for a in F. This is defined

recursively over terms and formulas:

$$\begin{aligned}
a_j[t/a_i] &= \begin{cases} t, & \text{if } i = j, \\ a_j, & \text{otherwise.} \end{cases} \\
v_j[t/a_i] &= v_j. \\
(St_1 \cdots t_n)[t/a_i] &= S(t_1[t/a_i]) \cdots (t_n[t/a_i]) \text{ for } S \in \mathscr{F} \cup \mathscr{P}. \\
\bot[t/a_i] &= \bot. \\
(F * G)[t/a_i] &= F[t/a_i] * G[t/a_i] \text{ for } * \in \{ \wedge, \vee, \to \}. \\
(QxF)[t/a_i] &= Qx\, F[t/a_i] \text{ for } Q \in \{ \forall, \exists \}.
\end{aligned}$$

Simultaneously substituting a sequence of terms $\vec{s} = s_0, \ldots, s_n$ for variables $\vec{c} = c_0, \ldots, c_n$ (where $c_i \neq c_j$ for all $i < j \leq n$) is defined in the expected way and denoted $F[\vec{s}/\vec{c}]$ or $F[s_0/c_0, \ldots, s_n/c_n]$. ⌟

2.8 Lemma
If F is a formula and t a term, $F[t/a]$ is a formula.

2.9 Convention · Meta-variables
Henceforth, I adopt the following naming conventions except where explicitly stated otherwise.

- lower case roman letters:
  - x, y, z (often with subscript, x_0, x_1, etc.) denote *bound* variables,
  - a, b, etc. denote *free* variables,
  - r, s and t range over terms (not pre-terms);
- upper case Roman letters F, G, A, B, etc. denote pre-formulas;
- upper case Greek letters Γ, Δ, etc. denote finite sets of formulas.

2.10 Convention · Denoting substitution
I will often introduce a formula along with a free variable, in the form of $F(a)$. This notation indicates that a is to be the focus of subsequent substitutions, whereby I write $F(t)$ in place $F[t/a]$.

Sometimes the free variable a is not mentioned explicitly. I may introduce a (pre-)formula as $F(x)$, subsequently writing $F(t)$. In this context,

$F(x)$ formally represents $G[x/a]$ for an appropriate choice of a (and G), whereby $F(t)$ means $G[t/a]$.

Finally, I introduce three formulaic abbreviations:

- $\top$ abbreviates the formula $\bot \to \bot$.
- $\neg F$ is shorthand for $F \to \bot$.
- $F \leftrightarrow G$ abbreviates $(F \to G) \wedge (G \to F)$.

2.2. Orders and trees

The various derivation calculi I present are all based on the mathematical notion of a tree. Recall that a relation $\leq$ on a set X is a *partial order* iff it is:

1. *Reflexive:* $x \leq x$ for all $x \in X$,
2. *Transitive:* if $x \leq y$ and $y \leq z$, then $x \leq z$,
3. *Anti-symmetric:* if $x \leq y$ and $y \leq x$ then $x = y$,

and is a *linear order* if, in addition, it is

4. *Linear:* for all $x, y \in X$, either $x \leq y$ or $y \leq x$.

Given a partial order $\leq$, I use $<$ to denote the derived *strict* suborder, defined by $x < y$ iff $x \leq y$ and $x \neq y$.

A *tree* is a non-empty set T, elements of which are called *vertices*, equipped with a partial order $\leq$ satisfying:

1. There exists a $\leq$-minimal vertex $* \in T$, called the *root*. Minimality of $*$ means that $* \leq v$ for all $v \in T$.
2. For every $v \in T$, the set $\{ u \in T \mid u \leq v \}$ of *predecessors* of u is finite and linearly ordered by $\leq$.

The following are straightforward consequences of the definition. Let $(T, \leq)$ be a tree and v a vertex.

2.11 Lemma
Every non-root vertex has a $\leq$-maximal predecessor. I.e., for every $v \neq *$ there is a unique $v_* < v$ such that $u < v$ iff $u \leq v_*$.

The vertex v_* in the above lemma is called the *immediate predecessor* of v, and I say that v is a *child* of v_*. The set of *children* of v is denoted

$$\mathrm{Child}_T(v) = \{\, u \in T \mid v = u_* \,\}.$$

A *leaf* is a vertex with no children. If the tree is clear from context I will omit its mention, writing, for instance, $\mathrm{Child}(v)$ for $\mathrm{Child}_T(v)$.

For the most part, I will only treat finite trees. In Module III, I present a sequent calculus whose derivations are, in general, infinitely branching trees, i.e., the set $\mathrm{Child}(v)$ can be infinite for some v. Such trees will still maintain another notion of finiteness in the sense of not containing any infinite branches, called *well-founded* trees.

2.12 Definition · Well-founded tree
Let $(T, \leq)$ be a tree. A *path* through T is a finite sequence $(v_i)_{i \leq k}$ such that $v_{i+1} \in \mathrm{Child}(v_i)$ for all $i < k$. An infinite sequence $(v_i)_{i \in \mathbb{N}}$ for which the prefix $(v_i)_{i \leq k}$ is a path for every k is called a *branch*.

A tree is *well-founded* iff it has no branches. ⌟

3. Natural deduction

I assume the reader is familiar with some deduction calculus/proof system for classical predicate logic. The precise calculus is not so important, so long as you understand the concept of a derivation system and the kind of object that can constitute a formal proof.

In these notes, I utilise two such calculi: *natural deduction* and *sequent calculi*. The latter will be introduced and covered in much detail, beginning in the next chapter. Natural deduction will also be given a formal definition. But I will gloss over some aspects that would be considered important in a first introduction, assuming that you either have seen the material before (for instance in the course *Logical Theory*) or can quickly relate the natural deduction calculus to the formal calculus you are most familiar with.

The various notions of *(formal) deduction/proof*, including those addressed in this work, have a common underlying structure. Namely, they are trees in which vertices are labelled by a certain kind of syntactic object — formulas in the case of natural deduction — and the relation between the label of a vertex and the label of its children corresponds to one of number of specified *rules of inference*.

An *inference over* X is a pair $(P, c) \in X^{<\omega} \times X$, where P is a finite sequence of objects — the *premises* — and c is a single deduction object, called the *conclusion*. For $P = (P_1, \ldots, P_n)$, I visualise the inference (P, C) as a rule

$$\frac{P_1 \quad \cdots \quad P_n}{C}$$

which *derives* the conclusion C from premises $P_1, \ldots, P_n$.

In natural deduction the set of formulas play the role of X and inferences relate finitely many premises (indeed, at most three) to a conclusion formula. In short, an inference in natural deduction is a pair (Γ, F) where

Γ is a finite sequence of formulas. Examples are

$$\frac{F}{F \vee G} \qquad \frac{F \quad G}{F \wedge G} \qquad \frac{F \to G \quad F}{G}$$

Abstractly then, an derivation calculus comprises two pieces of information:

- A set $\mathscr{O}$ of deduction *objects*;
- A set $\mathscr{I} \subseteq \mathscr{O}^{<\omega} \times \mathscr{O}$ of *inferences* or *rules*.

3.1 Definition · Derivation
A *derivation* in the calculus $(\mathscr{O}, \mathscr{I})$ is a tree $(T, \leq)$ together with a map $o\colon T \to \mathscr{O}$ assigning a deduction object to each vertex such that every vertex together with its children is an inference, i.e., for all v there exists an enumeration $v_1, \ldots, v_n$ of v's children such that

$$\big((o(v_1), \ldots, o(v_n)), o(v)\big) \in \mathscr{I}.$$

The deduction object labelling the root of T is called the *conclusion* of the derivation. ⌟

Observe that every vertex of a derivation must be the conclusion of an inference. In particular, objects labelling *leaves* must be derivable without premises. In some calculi zero-premise inferences correspond to *axioms* but in natural deduction they represent *assumptions* which other rule can 'mark' as *discharged* (or left *undischarged*) by certain inferences. Rules that 'discharge' assumptions are drawn as

$$\frac{\begin{array}{ccccc} & [a_1] & & & [a_n] \\ & \vdots & & & \vdots \\ b_0 & b_1 & \cdots & & b_n \end{array}}{c}$$

illustrating that there is an inference $\big((b_0, \ldots, b_n), c\big)$ deriving c from premises $b_0, \ldots, b_n$ and that in the subtree above b_i ($i > 0$) occurrences of an *assumption* a_i can be considered discharged.

Examples of assumption-discharging inferences in natural deduction are the introduction rule for implication and elimination rule for disjunction:

$$\dfrac{\begin{array}{c}[F]\\ \vdots\\ G\end{array}}{F \to G} \qquad \dfrac{F \vee G \quad \begin{array}{c}[F]\\ \vdots\\ H\end{array} \quad \cdots \quad \begin{array}{c}[G]\\ \vdots\\ H\end{array}}{H}$$

A final quirk of natural deduction is that some inferences are only applicable if the subderivation above them fulfils some condition. This is the case for two of the quantifier inferences:

$$\dfrac{F(a)}{\forall x F(x)} \qquad \dfrac{\exists x F(x) \quad \begin{array}{c}[F(a)]\\ \vdots\\ H\end{array}}{H}$$

which are associated a condition — the *eigenvariable* condition — that restrict their application to contexts in which the distinguished free variable a does not occur in any *undischarged* assumptions above the application of this rule.

It is these additional constraints on natural 'deductions' that explain the use of the term 'derivation' above rather than 'deduction' or 'proof'. Formally, some proof calculi are also equipped with a 'correctness condition' that identifies when a *derivation* is *well-formed* and can be considered a *deduction* or a *proof* in the calculus.

Before turning our full attention to natural deduction, I want the clarify the distinction between *inference* and *rule*. Above, I used the two terms almost interchangeably, as a specification of the premises and conclusions that can be used in derivations of a particular calculus. But when defining a system like natural deduction, we do not actually write down all the inferences. Rather, we present a set of schema or *rules* that generate the *inferences*. The *rule* called $\wedge$I, or $\wedge$-*introduction*, is the set of all inferences

$$\dfrac{F \quad G}{F \wedge G} \wedge\text{I}$$

where F and G range over formulas.

Thus, to fully specify a deduction calculus a third bit of information is sometimes (though not always) needed:

3.2 Definition · Calculus; deduction
A *calculus* is a triple $\mathsf{C} = (\mathscr{O}, \mathscr{R}, \mathscr{C})$ where

- $\mathscr{O}$ is a set of *deduction objects*;
- $\mathscr{R}$ is a set of *rules*, where a rule is a set of inference over $\mathscr{O}$;
- $\mathscr{C}$ is a *correctness condition* specifying which derivations in $\mathscr{O}$ and $\mathscr{R}$ are *deductions*. ⌟

I could, of course, have incorporated the correctness condition into the definition of derivation. Indeed, this is the approach that most texts in formal logic take. I write 'formal logic' and not 'proof theory' because the majority of textbooks in proof theory including the standard references (Negri and von Plato, 2001; Troelstra and Schwichtenberg, 2000; Schütte, 1950; Pohlers, 1989) are, understandably, more careful with the definition of proof.

The purpose of drawing attention to the correctness condition is to emphasise that *proofs* (in natural deduction) are not completely straightforward and, ultimately, isolating a deduction calculus with only trivial correctness conditions (finiteness say) will be extremely helpful.

Recall that only the deduction objects and rules are required for the definition of *derivation* I deliberately refrain from giving a formal definition of what constitutes a correctness condition as it is not particularly important.

3.1. Intuitionistic logic

In natural deduction, each logical connective and quantifier is associated two rules: an *introduction* rule and an *elimination* rule. In some cases, either category is further split into cases (such as $\wedge\mathsf{E}$ below).

I present each rule in turn. Unless otherwise stated, in all cases symbols F, G, a, t, etc. act as meta-variables ranging over all objects of the appropriate type, rather than denoting specific instances.

Assumption. A zero-premise rule for introducing assumptions (leaves of a derivation):

$$\frac{}{F}\,\mathsf{a}$$

As the assumption rule is the only zero-premise rule in natural deduction, mention of it will be suppressed.

Falsum. The connective $\bot$ has no introduction rule, but an elimination rule that permits the derivation of any formula from it.

$$\frac{\bot}{F}\,\bot\mathsf{E}$$

Conjunction. This connective is associated one introduction rule and two elimination rules:

$$\frac{F \quad G}{F \wedge G}\,\wedge\mathsf{I} \qquad \frac{F \wedge G}{F}\,\wedge\mathsf{E}_0 \qquad \frac{F \wedge G}{G}\,\wedge\mathsf{E}_1$$

Implication. An introduction rule (discharging an assumption) and one elimination rule

$$\frac{\begin{array}{c}[F]\\ \vdots \\ G\end{array}}{F \to G}\,\to\mathsf{I} \qquad \frac{F \to G \quad F}{G}\,\to\mathsf{E}$$

As explained above, the introduction rule allows the assumption F to be considered as discharged in the subderivation, indicated by the notation

$$\begin{array}{c}[F]\\ \vdots\end{array}$$

This information is not strictly part of the inference but is relevant for the notion of entailment in natural deduction, the relation of 'being derivable from assumptions'.

Disjunction. Two introduction rules and one elimination rule, the latter with discharged assumptions.

$$\frac{F}{F \vee G}\vee\mathsf{I}_0 \qquad \frac{G}{F \vee G}\vee\mathsf{I}_1 \qquad \frac{F \vee G \quad \begin{array}{c}[F]\\ \vdots \\ H\end{array} \quad \begin{array}{c}[G]\\ \vdots \\ H\end{array}}{H}\vee\mathsf{E}$$

Universal quantifier. An introduction and elimination rule. The introduction rules are separated according to the variable being 'discharged'. Application of the introduction rules are subject to the *eigenvariable condition* below.

$$\frac{F(a)}{\forall x F(x)}\forall\mathsf{I}_a \qquad \frac{\forall x F(x)}{F(t)}\forall\mathsf{E}$$

Recall that per convention 2.10, in the introduction rule $F(x)$ means $F[x/a]$. In particular, the variable a never occurs in the conclusion of $\forall\mathsf{I}_a$. In the elimination rule $\forall\mathsf{E}$, $\forall x F(x)$ and $F(t)$ mean $\forall x F[x/b]$ and $F[t/b]$ for some (unspecified) variable b.

Existential quantifier. To the universal quantifier as disjunction is to conjunction:

$$\frac{F(t)}{\exists x F(x)}\exists\mathsf{I} \qquad \frac{\exists x F(x) \quad \begin{array}{c}[F(a)]\\ \vdots \\ H\end{array}}{H}\exists\mathsf{E}_a$$

Applications of $\exists\mathsf{E}_a$ are also constrained by restricting where an eigenvariable condition:

Eigenvariable condition
The rules $\forall\mathsf{I}_a$ and $\exists\mathsf{E}_a$ are applicable only if a does not occur in the formula H nor in any assumption above this inference which is undischarged *after applying this rule.*

3.3 Example
The following is derivation in the above rules of $\exists x \neg F \to \neg\forall x F$. Notice that all assumptions are discharged (and that discharged assumptions are annotated

by the rule instance that discharged them):

$$\dfrac{\dfrac{[\exists x \neg F]^{\dagger} \qquad \dfrac{\dfrac{[\neg F(a)]^{\dagger\dagger} \qquad \dfrac{[\forall x F]^{\ddagger}}{F(a)}\,\forall\mathsf{E}}{\bot}\,\to\mathsf{E}}{\bot}\,\exists\mathsf{E}_a^{\dagger\dagger}}{\neg\forall x F}\,\to\mathsf{I}^{\ddagger}}{\exists x \neg F \to \neg\forall x F}\,\to\mathsf{I}^{\dagger}$$

The derivation above is well-formed: for the single inference to which the eigenvariable condition applies, $\exists\mathsf{E}_a$, the variable a does not occur in an undischarged assumption (except for the assumption $\neg F(a)$ which is discharged by this inference).

3.4 Definition · Natural deduction, N
Natural deduction is the calculus N over formulas comprising the aforementioned rules. A *deduction* is a finite derivation in N which fulfills the eigenvariable condition. ⌟

3.5 Definition · Entailment
The *entailment relation* is a relation $\vdash$ between a finite set of formulas and a formula defined as $\Gamma \vdash F$ iff that there exists a deduction in N with conclusion F such that every undischarged assumption of this derivation is an element of Γ.

A *validity* of N is any formula F such that $\varnothing \vdash F$ holds; also written as $\vdash F$. ⌟

As a direct consequence of the definition, I deduce

3.6 Lemma
If $\Gamma \vdash F$ and $\Delta \cup \{ F \} \vdash G$, then $\Gamma \cup \Delta \vdash G$

As $\Delta \cup \{ F \} \vdash F$ for all Δ and F, a special case of lemma 3.6 is

3.7 Lemma
$\Gamma \vdash F$ implies $\Gamma \cup \Delta \vdash F$ for all Δ.

3.8 Deduction theorem
For all F and G: $\Gamma \cup \{ F \} \vdash G$ iff $\Gamma \vdash F \to G$.

3.9 Lemma
If Γ *is a set of sentences and* $F(a)$ *any formula, then* $\Gamma \vdash F$ *iff* $\Gamma \vdash \forall x F(x)$.

3.1 Exercise
Prove 3.6–3.9.

3.2 Exercise
Express the correctness criterion for N as a property of paths. That is, specify the correctness condition $\mathscr{C}$ as a set of sequences of formulas and rules such that a derivation D is a deduction iff every path through D is contained in $\mathscr{C}$.

The set of validities of N determines a logic, known as intuitionistic logic.

3.10 Definition · Intuitionistic logic
I is the set of validities of N. I write $\mathsf{I} \vdash F$ iff $F \in \mathsf{I}$, iff $\varnothing \vdash F$ holds (in N). ⌟

3.2. Classical logic

In contrast to intuitionistic logic, classical logic is defined via semantics, specifically, Tarskian semantics. I will not recap the definition here; the reader can consult, for example, *Logical Theory*, ch. 4.

Classical logic can also be captured syntactically.

3.11 Definition · Classical natural deduction, Nc
The calculus Nc is the extension of N by the rule RAA:

$$\dfrac{\begin{array}{c}[\neg F]\\ \vdots \\ \bot\end{array}}{F}\,\mathsf{RAA}$$

with the same eigenvariable conditions applying to deductions.

The entailment relation for Nc is denoted $\vdash_{\mathsf{C}}$. That is, $\Gamma \vdash_{\mathsf{C}} F$ express the existence of a deduction according to Nc with conclusion F in which all undischarged assumptions are elements of Γ. ⌟

RAA stands for *reductio ad absurdum*. To avoid potential confusion, I use $\vdash_{\mathsf{I}}$ for the entailment

3.12 Theorem
The following are equivalent.

1. $\Gamma \vdash_{\mathsf{C}} F$.
2. $\Gamma \cup \{ \neg F \} \vdash_{\mathsf{C}} \bot$.
3. $\Gamma \cup \{ \neg\neg G \to G \mid G \in \Delta \} \vdash_{\mathsf{I}} F$ *for some set* Δ.
4. $\Gamma \cup \{ G \vee \neg G \mid G \in \Delta \} \vdash_{\mathsf{I}} F$ *for some set* Δ.

3.3 Exercise
Prove theorem 3.12.

4. The sequent calculus

Some content

4.1 Convention · The rule L→ in sequent calculi
The rule L⟶ in classical or intuitionistic contexts.

Negation translation magic (exercise)

5. Properties of the sequent calculus

Some content

Module II.

Cut elimination

6. Cut elimination

Here we present cut elimination for the calculi.

Cut rank, Inversion lemma and the like

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

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

6.1 Exercise
Prove that the rules R$\exists$ and L$\forall$ are not invertible in the above sense. That is, show the following two statements are *false*:

- If $\vdash_k^n \forall x F(x), \Gamma \Rightarrow \Delta, \forall x F(x)$ then $\vdash_k^n F(s), \Gamma \Rightarrow \Delta$ for some term s.
- If $\vdash_k^n \Gamma \Rightarrow \Delta, \exists x F(x)$ then $\vdash_k^n \Gamma \Rightarrow \Delta, F(s)$ for some term s.

For the classical sequent calculus two additional 'inversion' principles hold.

6.2 Second inversion lemma
In addition, classical predicate logic admits the inversions:

8. *If* C $\vdash_k^n \Gamma \Rightarrow \Delta, F \vee G$ *then* C $\vdash_k^n \Gamma \Rightarrow \Delta, F, G$.
9. *If* C $\vdash_k^n F \rightarrow G, \Gamma \Rightarrow \Delta$ *then* C $\vdash_k^n G, \Gamma \Rightarrow \Delta$ *and* C $\vdash_k^n \Gamma \Rightarrow \Delta, F$.

The intuitionistic sequent calculus supports just one part of the classical inversions.

6.3 Third inversion lemma
In addition to lemma 6.1, intuitionistic predicate logic admits the inversion

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

6.2 Exercise
Show that the 'missing' inversions for intuitionistic logic are false:

8′. If $\mathsf{I} \vdash^n_k \Gamma \Rightarrow F \vee G$ then either $\mathsf{I} \vdash^n_k \Gamma \Rightarrow F$ or $\mathsf{I} \vdash^n_k \Gamma \Rightarrow G$.

9′. If $\mathsf{I} \vdash^n_k F \to G, \Gamma \Rightarrow \Delta$ then $\mathsf{I} \vdash^n_k \Gamma \Rightarrow \Delta, F$.

6.1. Classical logic

For this section, I treat the classical sequent calculus C. Thus, $\vdash^n_k$ means $\mathsf{C} \vdash^n_k$ throughout.

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

Proof See lectures.

One case for reference. (Induction is on $m + n$.) Suppose $C = D \vee E$ and

1. $\vdash^m_k \Gamma \Rightarrow \Delta, C$
2. $\vdash^n_k C, \Sigma \Rightarrow \Lambda$

arise from

3. $\vdash^{m'}_k \Gamma \Rightarrow \Delta, C, D$
4. $\vdash^{n'}_k D, C, \Sigma \Rightarrow \Lambda$, and
5. $\vdash^{n''}_k E, C, \Sigma \Rightarrow \Lambda$

by the rules R∨ and L∨ respectively, where $m' < m$ and $n', n'' < n$. Figure 6.1 provides an illustration of the argument in this case. As $m' + n < m + n$, the induction hypothesis can be applied to the pair (3) and (2), yielding

6. $\vdash^{m'+n}_k \Gamma, \Sigma \Rightarrow \Delta, \Lambda, D$.

$$\dfrac{\dfrac{\vdash_k^{m'} \Gamma \Rightarrow \Delta, C, D \quad (3) \qquad \vdash_k^{n} C, \Sigma \Rightarrow \Lambda \quad (2)}{\vdash_k^{m'+n} \Gamma, \Sigma \Rightarrow \Delta, \Lambda, D}\,\text{IH} \qquad \dfrac{\vdash_k^{n'} D, C, \Sigma \Rightarrow \Lambda \quad (4)}{\vdash_k^{n'} D, \Sigma \Rightarrow \Lambda}\,\text{IL}}{\vdash_k^{m+n} \Gamma, \Sigma \Rightarrow \Delta, \Lambda}\,\text{cut}$$

Figure 6.1.: Illustration of the proof method in the reduction lemma for the case $C = D \vee E$. Numbering refers to the proof; IL = 'inversion lemma' and IH = 'induction hypothesis'.

I also apply the inversion lemma to (4), deducing

7. $\vdash_k^{n'} D, \Sigma \Rightarrow \Lambda$.

As $|D| < |C|$, it is possible to cut the final pair of sequents, resulting in

8. $\vdash_k^{h} \Gamma, \Sigma \Rightarrow \Delta, \Lambda$ for $h = \max\{ m' + n, n' \} + 1$.

As $h \leq m + n$, this case is complete. ⊣

6.5 Reduction theorem
If $\vdash_{k+1}^{m} \Gamma \Rightarrow \Delta$ *then* $\vdash_k^{2^m} \Gamma \Rightarrow \Delta$.

Proof In lectures. ⊣

Iterating the reduction lemma induces a cut-free proof. Define 2_k^n as $2_0^n = n$ and $2_{k+1}^n = 2^{2_k^n}$. The following result is due to Gerhard Gentzen and often referred to as *Genzten's Hauptsatz*.

6.6 Cut elimination theorem
Every sequent provable in classical predicate logic is provable without cut. In particular, if $\mathsf{C} \vdash_k^n \Gamma \Rightarrow \Delta$ *then* $\mathsf{C} \vdash_0^m \Gamma \Rightarrow \Delta$ *for some* $m \leq 2_k^n$.

Proof Induction on the cut rank. Recall, $\vdash_0$ is synonymous with 'cut-free provable'. ⊣

6.2. Intuitionistic logic

The rule of cut is also admissible in intuitionistic sequent calculus with essentially the same bounds. The failure of inversion creates some complications while the restriction to intuitionistic logic simplifies other cases.

6.7 Reduction lemma
Suppose $\mathsf{I} \vdash_k^m \Gamma \Rightarrow C$ *and* $\mathsf{I} \vdash_k^n C, \Sigma \Rightarrow \Lambda$. *If* $|C| = k$ *then* $\mathsf{I} \vdash_k^{(m+n).2} \Gamma, \Sigma \Rightarrow \Lambda$.

Proof See lectures. ⊣

6.8 Reduction theorem
If $\mathsf{I} \vdash_{k+1}^m \Gamma \Rightarrow \Delta$ *then* $\mathsf{I} \vdash_k^{4^m} \Gamma \Rightarrow \Delta$.

Proof In lectures. ⊣

Iterating the reduction lemma induces a cut-free proof. Define 4_k^n as $4_0^n = n$ and $4_{k+1}^n = 4^{4_k^n}$.

6.9 Cut elimination theorem
Every sequent provable in intuitionistic predicate logic is provable in the same calculus without cut. In particular, if $\mathsf{I} \vdash_k^n \Gamma \Rightarrow \Delta$ *then* $\mathsf{I} \vdash_0^m \Gamma \Rightarrow \Delta$ *for some* $m \leq 4_k^n$.

As a comparison, the reader can verify that $4_k^n \leq 2_{2k}^n$ for all n and k.

The next section looks more closely at the structure of cut-free proofs to derive a variety of structural results about classical and intuitionistic logic. Before that, I present a strengthening of the cut elimination bounds that can be achieved by a more careful proof of the reduction lemma. The proof of the following results are exercises.

6.3. Refining cut elimination

As formulated, the cut elimination theorem suggests that every logical connective contributes an exponential in the size of a proof. A careful examination of some cases show that many connectives can be dispensed 'cheaply', that is to say without inducing an exponential blow-up in proof height. As an example, consider the reduction lemma for a conjunction (classical or intuitionistic sequent calculus — they behave equally in this particular example):

1. $\vdash_k^m \Gamma \Rightarrow \Delta, D \wedge E$,
2. $\vdash_k^n D \wedge E, \Sigma \Rightarrow \Lambda$.

The reduction lemma states that if $k = |D \wedge E|$ then $\vdash_k^{m+n} \Gamma, \Sigma \Rightarrow \Delta, \Lambda$. However, the inversion lemma presents a different strategy to derive the same sequent. I 'invert' the sequents above to obtain

1. $\vdash_k^m \Gamma \Rightarrow \Delta, D$,
2. $\vdash_k^m \Gamma \Rightarrow \Delta, E$,
3. $\vdash_k^n D, E, \Sigma \Rightarrow \Lambda$,

and recombine as a sequence of two cuts of rank $< k$:

$$\dfrac{\vdash_k^m \Gamma \Rightarrow \Delta, D \qquad \dfrac{\vdash_k^m \Gamma \Rightarrow \Delta, E \qquad \vdash_k^n D, E, \Sigma \Rightarrow \Lambda}{\vdash_k^{\max\{m,n\}+1} D, \Gamma, \Sigma \Rightarrow \Delta, \Lambda}\,\mathsf{cut}}{\vdash_k^{\max\{m,n\}+2} \Gamma, \Sigma \Rightarrow \Delta, \Lambda}\,\mathsf{cut}$$

If $m, n > 1$ then $\max\{ m, n \} + 2 < m + n$.

The same trick can be applied to the other propositional connectives ($\vee$ and $\rightarrow$) for the classical sequent calculus:

6.3 Exercise
Using the method outlined above, state and prove an improved reduction lemma for *classical propositional* logic. Use your results to show that $\mathsf{CPL} \vdash_k^n \Gamma \Rightarrow \Delta$ implies $\mathsf{CPL} \vdash_0^h \Gamma \Rightarrow \Delta$ for $h = 2^{n.2^k}$.

As the quantifiers are not fully invertible ($\exists$ on the right or $\forall$ on the left) it is not possible to reduce quantified cuts via inversion alone. In that situation the bounds given by the standard reduction lemma become relevant.

6.4 Exercise
Generalise the previous exercise to deduce more efficient bounds on cut elimination for classical predicate logic.

The inversion technique works well enough for classical logic because the propositional connectives are invertible on both sides of the sequent arrow. This method cannot apply to intuitionistic logic, however, due to failure of some inversions. Still, there is another way to structure the reduction lemma that works smoothly for both logics. The idea is to use the sides of the sequent arrow as the control on complexity. In this way, the complexity of cut elimination can be ascribed to the case in which cut formulas 'switch' sides of the sequent arrow in reductions. To demonstrate this, I introduce a new complexity measure on formulas, called the implication depth, that counts the 'nesting' of implications. Let $|A|_*$ be the implication rank of A, defined by:

- $|A|_* = 0$ for A prime.
- $|QxA|_* = |A|_*$ for $Q \in \{\forall, \exists\}$.
- $|A \circ B|_* = \max\{\, |A|_*, |B|_* \,\}$ for $\circ \in \{\wedge, \vee\}$.
- $|A \to B|_* = \max\{\, |A|_* + 1, |B|_* \,\}$.

It will be necessary to restrict attention to the fragment without $\exists$ and $\vee$ as these add a level of complexity to the process that is beyond the scope of this course. I will also focus on intuitionistic logic; the reader can check that the statements below also apply just as well to classical logic.

6.10 Definition
Let $\vdash^n_q$ express derivability in the intuitionistic sequent calculus by a proof with height $\leq n$ in which all cut formulas have *implication rank* $< q$ and do not contain $\vee$ or $\exists$. ⌟

So the version of the cut rule used employed in $\vdash_*$ is

$$\frac{\vdash^n_q \Gamma \Rightarrow C \qquad \vdash^m_q C, \Lambda \Rightarrow B}{\vdash^h_q \Gamma, \Lambda \Rightarrow B}\,\mathsf{cut} \quad \text{for } |C|_* < q \text{ and } h > \max\{\, m, n \,\}.$$

The goal is to establish the following theorem.

6.11 Refined cut elimination theorem
If $\vdash^n_q \Gamma \Rightarrow A$ *then* $\vdash^m_0 \Gamma \Rightarrow A$ *for some* $m \leq 2^n_q$.

The reduction lemma that leads to the above result shifts the focus from reducing a single cut to reducing a batch of cuts as a single operation. Such a collection of cuts will have a specific form that can be expressed as a lifting of the standard two-premise cut rule to a multi-premise version, called the *multi-cut*:

$$\frac{\Gamma_0 \Rightarrow C_0 \qquad \cdots \qquad \Gamma_k \Rightarrow C_k \qquad C_0, \ldots, C_k, \Lambda \Rightarrow B}{\Gamma_0, \ldots, \Gamma_k, \Lambda \Rightarrow B}\,\mathsf{mcut}$$

The multi-cut has is origins in Gentzen's original proof of the *Haupsatz*

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma \Rightarrow A} \quad \dfrac{\vdots}{\Gamma \Rightarrow B}}{\Gamma \Rightarrow A \wedge B}\,\mathsf{R}\wedge \quad \dfrac{\dfrac{\vdots}{A, B, \Sigma \Rightarrow D}}{A \wedge B, \Sigma \Rightarrow D}\,\mathsf{L}\wedge}{\Gamma, \Sigma \Rightarrow D}\,\mathsf{cut}$$

reduces to

$$\dfrac{\dfrac{\vdots}{\Gamma \Rightarrow A} \quad \dfrac{\vdots}{\Gamma \Rightarrow B} \quad \dfrac{\vdots}{A, B, \Sigma \Rightarrow D}}{\Gamma, \Sigma \Rightarrow D}\,\mathsf{mcut}$$

Figure 6.2.: Reducing a binary cut on a conjunctive cut formula naturally induces *two* cuts which can be represented as a three-premise *multi-cut*. Cut formulas in the resultant multi-cut may have the same implication depth as in the first.

and can be viewed as abbreviating the sequence of binary cuts:

$$\dfrac{\dfrac{\Gamma_{k-1} \Rightarrow C_{k-1} \qquad \dfrac{\Gamma_k \Rightarrow C_k \quad C_0, \ldots, C_k, \Lambda \Rightarrow B}{C_0, \ldots, C_{k-1}, \Gamma_k, \Lambda \Rightarrow B}\,\mathsf{cut}}{\vdots}\,\mathsf{cut}}{\dfrac{\Gamma_0 \Rightarrow C_0 \qquad C_0, \Gamma_1, \ldots, \Gamma_k, \Lambda \Rightarrow B}{\Gamma_0, \ldots, \Gamma_k, \Lambda \Rightarrow B}\,\mathsf{cut}}\,\mathsf{cut}$$

The purpose of the multi-cut, however, is to hold together (in a single inference) the many individual cuts that are to be 'eliminated' at the once. A typical example of when the multi-cut rule is useful is in the reduction process attached to a binary cut with a conjunctive cut formula (see figure 6.2). If using the implication rank of formulas, cuts on the formulas A and B are considered as complex as on the conjunction $A \wedge B$ itself.

The reduction lemma for $\vdash\!\!\!*$ is the following:

6.12 Multi-cut reduction lemma
The following applies to I. *Suppose* $m_0, \ldots, m_k$, n *and* q *are such that*

- $\vdash\!\!\!*^{m}_{q}\ \Gamma_i \Rightarrow C_i$ *for each* $i \leq k$,

- $\vdash_{*q}^{n} C_0, \ldots, C_k, \Sigma \Rightarrow D$.

If $|C_i|_* = q$ *for all* $i \leq k$, *then* $\vdash_{*q}^{m+n} \Gamma_0, \ldots, \Gamma_k, \Sigma \Rightarrow D$.

In the special case of the standard 'two-premise' cut (where $k = 0$ above), the multi-cut reduction lemma states

If $\vdash_{*q}^{m} \Gamma \Rightarrow C$ and $\vdash_{*q}^{n} C, \Sigma \Rightarrow D$ where $|C|_* = q$, then $\vdash_{*q}^{m+n} \Gamma, \Sigma \Rightarrow D$.

The bound provided by the multi-cut reduction lemma is almost identical to the usual reduction lemma (which actually used the larger bound $(m + n).2$). But, crucially, the lemma claims that this bound is sufficient for reducing the *implication rank* of the cut, not merely the traditional rank.

6.5 Exercise
Prove the multi-cut reduction lemma. You will find the inversion lemma is needed to obtain the desired bound which you can assume holds for $\vdash_*$ with the same bounds.

6.6 Exercise
Using lemma 6.12 and any other observations to prove the refined cut elimination theorem (theorem 6.11).

6.7 Exercise
Using an appropriate negation translation of C into I, deduce a refined cut elimination theorem for classical logic.

6.8 Exercise
State and prove the above claims for the classical sequent calculus. How does you result compare with the indirect argument in exercise 6.7?

7. Consequences of cut elimination

Now we are getting somewhere

- Subformula and conservativity
- Interpolation theorem – Exercise.
- Harrop's theorem
- Herbrand's theorem

8. Predicate logic with equality

We haven't treated equality (yet).

8.1. Equality in natural deduction

$\mathsf{Nc}_{=}$ & $\mathsf{N}_{=}$.

8.2. Equality in sequent calculus

$\mathsf{IL}_{=}$ & $\mathsf{CL}_{=}$.

8.3. Cut elimination with equality

Hmm!

9. A game of cut

Shall we? Or should this be for inf PA?

Module III.

An Introduction to Ordinal Analysis

10. 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 *Logical Theory* for details.

10.1. Peano and Heyting arithmetic

10.1 Definition · Language of arithmetic
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 $\mathsf{Nc}_=$. Following a short examination of this theory I give an equivalent presentation as a sequent calculus extending $\mathsf{CL}_=$. The logics $\mathsf{Nc}_=$ and $\mathsf{CL}_=$ were introduced in chapter 8 (see also (Negri and von Plato, 2001, §6.5)).

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

10.2 Definition · Peano axioms
The Peano axioms of arithmetic are the following sentences.

- *Basic axioms:*

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

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

  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 schema of induction:*

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

10.3 Definition · Peano arithmetic
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, $\mathrm{PA} \vdash_{\mathsf{Nc}_=} A$ where PA is the set of Peano axioms. *Heyting arithmetic* (HA) is the corresponding *intuitionistic* theory, i.e., $\mathsf{HA} \vdash A$ expresses $\mathrm{PA} \vdash_{\mathsf{N}_=} A$. ⌟

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,

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

The following result is easy to prove.

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

Proof Exercise. ⊣

10.1 Exercise
Show the following are theorems of Heyting arithmetic.

1. $\forall x(\neg x = 0 \to \exists y(x = \mathsf{s}y))$.
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 *Logical Theory*, for example, for details.

10.5 Definition · Formula classes Δ_0, Π_1, Σ_1
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 $\mathsf{s}\cdots\mathsf{s}0$ are called *numerals*. The numeral evaluating to $n \in \mathbb{N}$ is denoted $\underline{n}$:

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

I state the representation theorem for primitive recursive relations.

10.6 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 $\mathscr{L}_A$ with at most the displayed variables free such that for all $n_1, \ldots, n_k \in \mathbb{N}$,

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

10.2. 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 more convenient definition is the following.

10.7 Definition · Peano arithmetic as a sequent calculus
$\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$ expresses that the sequent $\Gamma \Rightarrow \Delta$ has a derivation in the sequent calculus $\mathsf{CL}_=$ expanded by:

- Initial sequents $\Pi \Rightarrow \Sigma, A$ for A a basic Peano axiom.
- The *induction rule*:

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

  where a does not occur in the lower sequent. ⌟

The sequent calculus for Heyting arithmetic is the restriction to intuitionistic sequents where, recall, a sequent $\Gamma \Rightarrow \Delta$ is *intuitionistic* iff $|\Delta| = 1$.

10.8 Definition · Heyting arithmetic as a sequent calculus
$\mathsf{HA} \vdash \Gamma \Rightarrow \Delta$ expresses that $\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$ via a derivation using only intuitionistic sequents. ⌟

It is straightforward to see that PA, as a sequent calculus, is also closed under substitution where substitution is extended to sets of formulas pointwise: $\Gamma[A/P] \coloneqq \{ B[A/P] \mid B \in \Gamma \}$

10.9 Proposition
For every sequent $\Gamma \Rightarrow \Delta$ *and formula* $F(a)$*, if* $\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$ *then* $\mathsf{PA} \vdash \Gamma[F/P] \Rightarrow \Delta[F/P]$*. Likewise, if* $\mathsf{HA} \vdash \Gamma \Rightarrow A$ *then* $\mathsf{HA} \vdash \Gamma[F/P] \Rightarrow A[F/P]$.

Proof By induction on the derivation witnessing $\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$. If this is an initial sequent then $\Gamma[F/P] \Rightarrow \Delta[F/P]$ is also initial. Furthermore, for every inference

$$\frac{\Gamma_0 \Rightarrow \Delta_0 \quad \cdots \quad \Gamma_k \Rightarrow \Delta_k}{\Gamma \Rightarrow \Delta}$$

the result of substituting F for P in all premises and conclusion is an instance of the same inference rule. ⊣

An equivalent calculus can be given where substitution is given as an explicit rule of inference and the induction rule is restricted to the predicate P:

10.10 Definition
$\mathsf{PA}^* \vdash \Gamma \Rightarrow \Delta$ expresses that the sequent $\Gamma \Rightarrow \Delta$ has a derivation in the sequent calculus $\mathsf{CL}_=$ expanded by:

- Initial sequents $\Pi \Rightarrow \Sigma, A$ for A a basic Peano axiom.
- The *induction rule*:
$$\frac{Pa, \Pi \Rightarrow \Sigma, P(\mathsf{s}a)}{P\mathsf{0}, \Pi \Rightarrow \Sigma, \forall x Px}\,\mathsf{ir}_0$$
where a does not occur in the lower sequent.
- The *substitution rule* for every formula F:
$$\frac{\Gamma \Rightarrow \Delta}{\Gamma[F/P] \Rightarrow \Delta[F/P]}\,\mathsf{sub}$$
⌟

10.11 Proposition
For every sequent $\Gamma \Rightarrow \Delta$, $\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$ *iff* $\mathsf{PA}^* \vdash \Gamma \Rightarrow \Delta$.

Proof Proposition 10.9 provides the embedding of PA^* into PA. The converse direction requires replacing each instance of the (unrestricted)

induction rule by a combination of ir_0 and sub. Let $F' = \forall x(Px \leftrightarrow F(x))$. The next derivation witnesses derivability of the induction rule for F:

$$\dfrac{\dfrac{\dfrac{Pa, F' \Rightarrow F(a) \qquad F(a), \Pi \Rightarrow \Sigma, F(\mathsf{s}a)}{Pa, F', \Pi \Rightarrow \Sigma, F(\mathsf{s}a)}\,\mathsf{cut} \qquad F(\mathsf{s}a), F' \Rightarrow P(\mathsf{s}a)}{Pa, F', \Pi \Rightarrow \Sigma, P(\mathsf{s}a)}\,\mathsf{cut}}{P(\mathsf{0}), F', \Pi \Rightarrow \Sigma, \forall x P(x)}\,\mathsf{ir}_0$$ ⊣

10.12 Proposition
For every sentence A,

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 $F(a)$. Let $\Gamma = \{\, P(\mathsf{0}), \forall x(P(x) \to P(\mathsf{s}x)) \,\}$. By logic, a derivation of $P(a), \Gamma \Rightarrow P(\mathsf{s}a)$ is readily obtained which, followed by an application of the induction and substitution rules, and more logic completes the derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots \qquad \vdots}{P(a), \Gamma \Rightarrow P(a) \qquad P(\mathsf{s}a), \Gamma \Rightarrow P(\mathsf{s}a)}\,\mathsf{L}\to}{P(a) \to P(\mathsf{s}a), P(a), \Gamma \Rightarrow P(\mathsf{s}a)}\,\mathsf{L}\forall}{P(a), \Gamma \Rightarrow P(\mathsf{s}a)}\,\mathsf{ir}}{\Gamma \Rightarrow \forall x P(x)}}{F(\mathsf{0}), \forall x(F(x) \to F(\mathsf{s}x)) \Rightarrow \forall x F(x)}\,\mathsf{sub}}{\Rightarrow \forall x_1 \cdots \forall x_k \big(F(\mathsf{0}) \wedge \forall x(F(x) \to F(\mathsf{s}x)) \to \forall x F(x) \big)}\,\mathsf{L}\wedge, \mathsf{R}\to, \mathsf{R}\forall$$ ⊣

10.13 Proposition
If $\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$ *then* $\mathsf{PA} \vdash \Gamma[A/P] \Rightarrow \Delta[A/P]$.

Proof By definition. ⊣

10.2 Exercise
Complete the proof of proposition 10.12.

10.3. Fragments of arithmetic

There are important subtheories of Peano arithmetic that are worth introducing. I will begin with the theory of primitive recursion, called *primitive recursive arithmetic*, PRA. Primitive recursive arithmetic is, in essence, the equational theory of primitive recursive functions. For a recap on primitive recursive functions see, e.g. *Logical Theory*, ch 15. The theory is formulated in the extension of $\mathscr{L}_{\text{A}}$ by function symbols for all primitive recursive functions.

As the theories introduced this section will all be formulated over classical logic, I take the opportunity to the logical connectives are $\bot$, $\wedge$, $\to$ and $\forall$. Note, I am including implication rather than primitive negation as a matter of convenience.

The language of primitive recursive arithmetic, $\mathscr{L}_{\text{PRA}}$, contains a function symbol $\dot{h}$ (of arity n) for each primitive recursive function $h\colon \mathbb{N}^n \to \mathbb{N}$. *Primitive recursive arithmetic*, PRA, is the theory in classical logic whose non-logical axioms are the defining equations of each primitive recursive function.

10.14 Definition · Language of primitive recursive arithmetic
The symbols of $\mathscr{L}_{\text{PRA}}$ are generated as follows.

1. $P \in \mathscr{L}_{\text{PRA}}$ is a unary predicate symbol.
2. $\mathsf{s} \in \mathscr{L}_{\text{PRA}}$ (unary) and $\mathsf{0}_n \in \mathscr{L}_{\text{PRA}}$ (n-ary) for every n.
3. $\mathsf{p}_{n,k} \in \mathscr{L}_{\text{PRA}}$ (n-ary) for every n and $k < n$.
4. For each m-ary function symbol g and n-ary function symbols $\vec{h} = h_1, \dots, h_m$, an n-ary function symbol $\mathsf{c}_{g,\vec{h}} \in \mathscr{L}_{\text{PRA}}$.
5. For each n-ary function symbol g and $(n+2)$-ary function symbol h, an $(n+1)$-ary function symbol $\mathsf{r}_{f,g} \in \mathscr{L}_{\text{PRA}}$. ⌟

10.15 Definition · Primitive recursive arithmetic
PRA is the theory in classical logic axiomatised by the following sentences where $g, h, h_1, \dots, h_n$ range over primitive recursive function symbols of appropriate arity.

PR1 $\forall x \neg \mathsf{s}x = \mathsf{0}_0$.

PR2 $\forall x_1 \cdots x_n \, \mathsf{p}_{n,k}\vec{x} = x_{k+1}$.

PR3 $\forall x_1 \cdots x_n \, \mathsf{c}_{g,(h_1,\ldots,h_n)}\vec{x} = g(h_1\vec{x}) \cdots (h_n\vec{x})$.

PR4 For the function symbol $\mathsf{r}_{g,h}$, the axioms of primitive recursion:

$$\forall x_1 \cdots x_n \, \mathsf{r}_{g,h}\mathsf{0}\vec{x} = g\vec{x}$$
$$\forall y x_1 \cdots x_n \, \mathsf{r}_{g,h}(\mathsf{s}y)\vec{x} = hy(\mathsf{r}_{g,h}y\vec{x})\vec{x}.$$

PR5 The universal closure of $A(\mathsf{0}) \wedge \forall x(A(x) \to A(\mathsf{s}x)) \to \forall x A(x)$ for every quantifier-free formula A. ⌟

The reader can confirm that the axioms are well-formed (that each function symbol is associated the correct arity according to the definition).

I assume that $\mathscr{L}_{\text{PRA}}$ extends $\mathscr{L}_{\text{A}}$ in the sense that the symbols $\mathsf{0}$, s, $+$ and $\times$ name the corresponding function symbol in $\mathscr{L}_{\text{PRA}}$ and that $\mathscr{L}_{\text{PRA}}$ contains the unary predicate P. In the case of $+$, for example,

$$+ \coloneqq \mathsf{c}_{\hat{+},\mathsf{p}^2_1,\mathsf{p}^2_0} \text{ where } \hat{+} \coloneqq \mathsf{r}_{\mathsf{p}^1_0,\mathsf{s}_{3,1}} \text{ and } \mathsf{s}_{3,1} \coloneqq \mathsf{c}_{\mathsf{s},\mathsf{p}^2_1}$$

Checking the definition, the axioms express $\mathsf{s}_{3,1}$ as the ternary function that returns the successor of its middle argument (and ignores the other), $\hat{+}$ as addition defined by recursion on its *first* argument, and $+$ as $\hat{+}$ with the order of arguments exchanged. Although $\hat{+}$ clearly also *defines* addition on $\mathbb{N}$, it is only for $+$ that the basic Peano axioms are provable in from the PRA-axioms.

10.3 Exercise
Find a function symbol $\times$ in $\mathscr{L}_{\text{PRA}}$ such that the basic Peano axioms for the symbol are provable in PRA.

10.16 Lemma
The basic Peano axioms are provable in PRA.

Proof Only the second basic axiom, $\forall x \forall y(\mathsf{s}x = \mathsf{s}y \to x = y)$, is not obvious. For this, we consider the PRA-axioms for a particular instance of primitive recursion, the unary function $f = \mathsf{r}_{\mathsf{0},\mathsf{p}_{2,0}}$ that has associated axioms

$$f\mathsf{0} = \mathsf{0} \qquad f(\mathsf{s}a) = \mathsf{p}_{2,0}a(fa) \quad \text{and} \quad \mathsf{p}_{2,0}ab = a.$$

Reasoning informally in PRA: Assume $\mathsf{s}a = \mathsf{s}b$. Substitution of equal terms yields $a = \mathsf{p}_{2,0}a(fa) = f(\mathsf{s}a) = f(\mathsf{s}b) = \mathsf{p}_{2,0}b(fb) = b$. ⌟

10.17 Convention · Representating primitive recursive functions
For each primitive recursive function $h\colon \mathbb{N}^n \to \mathbb{N}$ is associated a canonical function symbol $\dot{h}$ in $\mathscr{L}_{\mathrm{PRA}}$ that expresses the construction h by the rules of primitive recursion.

As an example of the above convention, consider the exponentiation function $ex\colon n \mapsto 2^n$. There is a formula $E(a,b)$ in the language of arithmetic such that

1. $\mathsf{PA} \vdash \forall x \exists! y\, E(x,y)$.
2. $\mathsf{PA} \vdash E(\underline{n}, \underline{2^n})$ for every $n \in \mathbb{N}$.

Exponentiation base 2 is, however, clearly primitive recursive, so there exists a function symbol e in $\mathscr{L}_{\mathrm{PRA}}$ such that $\mathsf{PRA} \vdash \mathsf{e}\underline{n} = \underline{2^n}$ for each n. By the above convention, the function symbol e is denoted by writing $\dot{exp}$ or, more suggestively, as $\dot{2}^s$ in place of $\mathsf{e}s$.

10.18 Lemma
It is decidable whether $\mathbb{N} \vDash s = t$ holds for any two closed terms in $\mathscr{L}_{PRA}$.

Recall the implication rank introduced at the end of chapter 6, defined by counting the nesting depth on the negative side of implications:

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

10.19 Definition · The implication hierarchy
The ID_n formulas is the set of formulas of implication depth n. ⌟

To understand the definition, notice that the formula $\forall x \exists y \forall z F$ will have implication depth 2 if $|F|_* = 0$. Thus, Π^0_2 formulas in the usual sense correspond to implication depth 1.

10.20 Definition · Theories with restricted induction
For each n, PA_n denotes the theory in the language $\mathscr{L}_{\mathrm{PRA}}$ extending PRA by the axiom of induction for ID_n formulas. That is, PA_n extends PRA by the universal closure of

$$A(\mathsf{0}) \wedge \forall x(A(x) \to A(\mathsf{s}x)) \to \forall x A(x)$$

for every formula $A(a)$ satisfying $|A(a)|_* < n$. ⌟

Sequent calculi for fragments of arithmetic can be obtained by restricting the complexity of formulas in the substitution rule:

$$\frac{\Gamma \Rightarrow \Delta \qquad |A|_* \leq n}{\Gamma[A/P] \Rightarrow \Delta[A/P]}\,\mathsf{sub}_n$$

10.21 Definition · Sequent calculi for fragments of arithmetic
$\mathsf{PA}_n \vdash \Gamma \Rightarrow \Delta$ holds iff $\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$ via a derivation employing no more than 1 applications of the rule sub_1 (every path passes through at most one substitution and, in each case, the substituted formula is Π_n). ⌟

When induction is restricted, the cut rank can also be so.

10.22 Partial cut elimination theorem
Suppose $\mathsf{PA}_n \vdash \Gamma \Rightarrow \Delta$ *and* $n \geq 1$. *Then* $\mathsf{PA} \vdash \Gamma \Rightarrow \Delta$ *with a derivation in which all cut formulas have implication depth* $< n$.

Proof I omit the proof. ⊣

10.4 Exercise
Prove the base case of theorem 10.22: If $\mathsf{PA}_0 \vdash \Gamma \Rightarrow \Delta$ then there is derivation in which all cuts have implication depth 0.

10.4. Small proofs and big proofs

By proposition 10.12, 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, Boolos et al. (2007).

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 $r_1 = s_1, \ldots, r_k = s_k \Rightarrow t_1 = u_1, \ldots, t_l = u_l$ 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:

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

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

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

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

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).

10.23 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. ⊣

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

Proof Fix a formula $F(a)$ and as before let $\Gamma = \{ F(\mathsf{0}), \forall x(F(x) \to F(\mathsf{s}x)) \}$. 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 $F(\mathsf{0}), \Gamma \Rightarrow \Delta, F(\underline{n})$: for $n = 0, 1$ the claim is immediate. For $n = m + 1 > 1$ append the proof of the induction hypothesis by a single cut:

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

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

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

With the ω-rules replacing the traditional quantifier rules $\mathsf{R}\forall$ and $\mathsf{L}\exists$ 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.

10.25 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 PA$\omega \vdash \Gamma \Rightarrow \Delta$ 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.

10.26 Proposition
Every closed initial sequent of PA *is derivable in* PAω.

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 PAω 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 $\mathsf{R}\omega$. ⊣

10.6 Exercise
Complete the proof of proposition 10.26.

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

10.27 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* $\mathsf{HA}\omega$.

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

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 10.24 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*.

11. 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 Rathjen (2012).

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

- 01 $<$ 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 $\beta \leq \alpha$.
- 02 Every non-empty class of ordinals has a $<$-minimal element (necessarily unique by 01). That is, if $O \subseteq \mathbb{O}$ is non-empty there exists $\xi \in O$ such that $\xi \leq \alpha$ for all $\alpha \in O$.
- 03 For every set X and function $f : X \to \mathbb{O}$ 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 03. 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 $f : U \to V$ 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 $f[X]$.

11.2 Convention · Notating ordinals
Lowercase Greek letters α, β, etc. stand as metavariables for ordinals.

11.3 Lemma
Postulate 02 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 02, 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 01 and the principle of transfinite induction (I could also assume 03 but this is unnecessary). The aim is to establish 02. 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.

11.4 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 02 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 01. ⊣

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 11.4(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.

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

11.6 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 $\xi' \in O$).

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

11.1 Exercise
Prove lemma 11.5 to 11.7.

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.

11.1. 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 $\mathsf{id}\colon \mathbb{O} \to \mathbb{O}$ 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 $\{\,\omega, \omega', \ldots\,\}$ because $\mathbb{N}$ is a segment. Notice that order preserving functions on ordinals are always injective.

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

11.2 Exercise
Prove lemma 11.8.

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

11.9 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

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

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:

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

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 $f : O' \to Y$ 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.

11.10 Lemma
Let $f : \mathbb{O} \to \mathbb{O}$ 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 $O = \{\, f(\alpha), f(f(\alpha)), \ldots, f^n(\alpha), \ldots \,\}$ (arbitrary finite iterations of f on α). Let $\beta = \sup O$. Invoking continuity, $f(\beta) = \sup f[O] = \sup O = \beta$. Moreover, $\alpha \leq f(\alpha) \leq \beta$. ⊣

11.2. 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.

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

For $n < \omega$, define $\alpha.n$ as $\alpha.0 := 0$ and $\alpha.(n+1) := \alpha.n + \alpha$. ⌟

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

11.12 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* $\beta \leq \alpha + \beta$.

11.13 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 11.10.

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

Proof Lemma 11.10 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 11.13 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.

11.15 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 $\alpha \geq 1$). Many limit ordinals are not additive principal: If $\alpha \geq \omega$ then $\alpha + \omega \notin \text{AP}$ as $\alpha < \alpha + \omega$ but $\alpha + \alpha \not< \alpha + \omega$.

11.16 Lemma
The following are equivalent for all $\alpha > 1$:

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

Proof Fix $\alpha > 1$.

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 $\alpha > 1$ then $\alpha = \sup\{ \xi \mid \xi < \alpha \} \leq \sup\{ \xi + \xi \mid \xi < \alpha \}$.

2 ⇒ 3. By assumption α is a limit and for $\beta < \alpha$ it is the case that

$$\beta + \alpha = \sup\{ \beta + \xi \mid \xi < \alpha \} \leq \sup\{ \xi + \xi \mid \xi < \alpha \} \leq \alpha.$$

3 ⇒ 1. For every $\beta, \xi < \alpha$ it is the case that $\beta + \xi < \beta + \alpha = \alpha$. ⊣

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. First, I need

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

Proof Exercise. ⊣

11.18 Definition · Enumeration of the additive principal ordinals
$\omega^\alpha := E_{\mathrm{AP}}(\alpha)$. ⌟

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, $\omega.2$ $(= \omega + \omega)$, $\omega.3$ $(= \omega + \omega + \omega)$, $\ldots$, $\omega.n$ which is denoted ω^2.

As a consequence of part 3 of lemma 11.16, $\omega^\alpha + \omega^\beta = \omega^\beta$ iff $\alpha < \beta$. A corollary is the observation made earlier that $n + \omega = \omega$ which now follows from repeated applications of lemma 11.16: $(k + 1) + \omega = k + (\omega^0 + \omega^1) = k + \omega$.

Applying the new notation to lemma 11.16 yields

11.19 Lemma
For every $\alpha > 0$, $\omega^\alpha = \sup\{\, \omega^\xi.n \mid \xi < \alpha$ and $n < \omega \,\}$.

11.3 Exercise
Prove lemma 11.19.

The next observation has a number of important consequences.

11.20 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 11.10. 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 11.12(5); the rest use lemma 11.16(3)), also $\beta \leq \gamma$. Given that $\beta = \gamma$, uniqueness of the rest is immediate. ⊣

11.3. Normal forms and natural sum

Lemma 11.20 above provides the basis of a normal form representation of ordinals. This concept is introduced in the next definition.

11.21 Definition · Additive normal form
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.

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

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

Moreover, this decomposition is unique.

Proof The theorem is a simple generalisation of lemma 11.20. Let $\alpha =_{\text{NF}} \omega^{\alpha_0} + \xi_0$ by lemma 11.20. 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. ⊣

11.23 Definition · Cantor normal form
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 11.10 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.

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

11.25 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 $\alpha < \varepsilon_0$.

11.4 Exercise
Prove lemma 11.25.

11.5 Exercise
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 $\omega^\alpha.(\beta + 1) = \omega^\alpha.\beta + \omega^\alpha$.

11.6 Exercise
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 $\alpha \leq \varepsilon_0$.

11.7 Exercise
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 11.24 and deduce that the enumerating function is defined for all ordinals.

11.8 Exercise
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*

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

11.9 Exercise
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 Hessenberg (1906)). The Cantor normal theorem provides the means to achieve this.

11.26 Definition · Natural sum
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 $\alpha =_{\text{NF}} \omega^{\alpha_0}+\alpha_1$ and $\beta =_{\text{NF}} \omega^{\beta_0} + \beta_1$

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

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.

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

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

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).

11.28 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 $\alpha \# \gamma < \beta \# \gamma$.*

11.10 Exercise
Prove lemma 11.28.

11.11 Exercise
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 11.5.

12. Ordinal analysis of arithmetic

Ordinals will now be used to measure the *height* of ω-proofs. I begin by formalising the infinitary sequent calculi for arithmetic described at the end of chapter 10. Building on that definition, it will prove convenient to view Peano arithmetic as extending primitive recursive arithmetic.

12.1 Definition · Infinitary sequent calculus for arithmetic
$\mathsf{PA}\omega$ is the sequent calculus given by the following: Sequents comprise closed formulas in the language of primitive recursive arithmetic $\mathscr{L}_{\text{PRA}}$.

Initial sequents are *closed* sequents of the form

($\mathsf{L}\bot$) $\bot, \Gamma \Rightarrow \Delta$.

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

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

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

Inference rules are rules of C but restricted to closed sequents and with $\mathsf{R}\forall$ and $\mathsf{L}\exists$ 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. ⌟

It is important to note that the property of being an initial sequent of $\mathsf{PA}\omega$ is decidable. This is precisely because sequents do not contain free variables, whereby it is decidable whether an equation between primitive recursive terms is true (or not). Likewise, for each of the rules of $\mathsf{PA}\omega$: The property of being the n-th premise of a rule whose conclusion is $\Gamma \Rightarrow \Delta$ with specified principle formula is decidable.

12.2 Definition · Bounding infinitary derivations
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 $\mathsf{T} \vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta$, 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 $\mathsf{T} \vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta$ 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:

12.3 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 12.3 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.

12.4 Example
To be written.

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

12.1 Exercise
Assign ordinal bounds on the ω-proofs of $A, \Gamma \Rightarrow \Delta, A$ constructed in exercise 10.7.

Revisiting the Embedding lemma (lemma 10.27) it is possible provide ordinal bounds on the size of the resulting ω-proof. Let $\alpha.k = \underbrace{\alpha + \cdots + \alpha}_{k}$.

12.6 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* $\mathsf{HA}\omega$.

12.2 Exercise
Prove the refined embedding lemma following the schema of embedding lemma at the end of chapter 10.

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 13.2.

12.7 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

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

12.3 Exercise
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*.

12.9 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 $\vdash_k^\alpha \Gamma(s) \Rightarrow \Delta(s)$ 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.

12.10 Inversion lemma
The following hold for all parameters.

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

Proof I show cases 2 & 4.

2. By induction on α. Suppose $\vdash_k^\alpha s = t, \Gamma \Rightarrow \Delta$ 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) $\vdash_k^{\alpha_i} s = t, \Gamma_i \Rightarrow \Delta_i$ 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 $\mathsf{PA}\omega$ 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, $\vdash_k^\alpha \Gamma \Rightarrow \Delta$ holds as desired.

4. The argument is a direct generalisation of the finitary inversion lemma. Suppose $\vdash_k^\alpha \Gamma \Rightarrow \Delta, \forall x F(x)$. 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 $\vdash_k^\alpha \Gamma \Rightarrow \Delta, \forall x F(x)$ can be derived. The case of $\mathsf{R}\forall$ 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 $\vdash_k^\alpha \Gamma \Rightarrow \Delta, F(\underline{n})$ 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 $\mathbb{N} \vDash \underline{n} = s$. The substitution lemma then yields $\vdash_k^\alpha \Gamma \Rightarrow \Delta, F(s)$. ⊣

12.1. 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 $\alpha + \beta$.

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

There is a remarkable amount of flexibility proving 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 $\vdash_k^{\alpha\#\beta} \Gamma, \Sigma \Rightarrow \Delta, \Lambda$ 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 $\vdash_k^{\alpha\#\beta} \Gamma, \Sigma \Rightarrow \Delta, \Lambda$. 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 $\vdash_k^\beta C, \Sigma \Rightarrow \Lambda$. 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

$$\vdash_k^\gamma D(t), C, \Sigma \Rightarrow \Lambda.$$

The induction hypothesis yields

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

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

$C = D \rightarrow E$. 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 $\vdash_k^\beta C, \Sigma \Rightarrow \Lambda$, for which there exist $\gamma, \delta < \beta$ and $\Lambda = \Lambda_0 \cup \Lambda_1$ satisfying

1. $\vdash_k^\gamma C, \Sigma \Rightarrow \Lambda_0, D$.
2. $\vdash_k^\delta C, E, \Sigma \Rightarrow \Lambda_1$.

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

3. $\vdash_k^\alpha D, \Gamma \Rightarrow \Delta, E$.
4. $\vdash_k^\gamma \Sigma \Rightarrow \Lambda_0, D$.

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

Figure 12.1.: Illustration of the proof method in the reduction lemma for the case $C = D \to E$; IL = 'inversion lemma' and IH = 'induction hypothesis'.

5. $\vdash_k^\delta E, \Sigma \Rightarrow \Lambda_1$.

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

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

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

$$\vdash_k^{\alpha\#\beta} \Gamma, \Sigma \Rightarrow \Delta, \Lambda.$$

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. ⊣

12.4 Exercise
Complete the preceding proof.

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

12.6 Exercise
Give an alternative proof of lemma 12.11 using the proof strategy from the reduction lemma for C (lemma 6.4).

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

12.12 Reduction theorem for $\mathsf{PA}\omega$ theorem
If $\vdash_{k+1}^\alpha \Gamma \Rightarrow \Delta$ *then* $\vdash_k^{\omega^\alpha} \Gamma \Rightarrow \Delta$.

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

$$\vdash^{\omega^{\alpha_0} \# \omega^{\alpha_1}}_{k} \Gamma \Rightarrow \Delta$$

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 $f : \mathbb{O} \to \mathbb{O}$ such that $f(\alpha) \geq \sup\{\, f(\xi) \# f(\eta) \mid \xi, \eta < \alpha \,\}$. An obvious candidate is $f : \alpha \mapsto 2^{\alpha}$ (see exercise 11.6) and, indeed, lemma 12.11 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 11.9), 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 $\omega^{\alpha}_{0} := \alpha$ and $\omega^{\alpha}_{k+1} := \omega^{\omega^{\alpha}_{k}}$.

12.13 Cut elimination theorem
If $\vdash^{\alpha}_{k} \Gamma \Rightarrow \Delta$ *then* $\vdash^{\omega^{\alpha}_{k}}_{0} \Gamma \Rightarrow \Delta$.

Proof Consequence of theorem 12.12. ⊣

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

12.14 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 12.6) there is are n, k such that

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

Let $\alpha = \omega_k^{\omega.n}$. Then $\alpha < \varepsilon_0$ (by definition 11.24) and

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

by theorem 12.13. ⊣

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

12.15 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 12.15 can strengthen the result by clarifying what mathematical principles suffice to derive the consistency of arithmetic.

12.16 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 12.6) provides an explicit number $n < \omega$ such that

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

The existence of a cut-free proof of the empty sequent, along with the various results on which theorem 12.13 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. ⊣

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

Proof Exercise. ⊣

12.2. On fragments of Peano arithmetic

It is worth considering the cut elimination theorem in the context of fragments of arithmetic, namely the theories PA_n from section 10.3. Recall the convention that formulas in these calculi are expressed without $\vee$ or $\exists$.

Let $\mathsf{PA}\omega \vdash_q^\alpha \Gamma \Rightarrow \Delta$ denote derivability in PAω for such sequents in the usual way but with the cut referring to implication depth:

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

12.8 Exercise
Verify that the above version of PAω satisfies weakening, substitution and inversion lemmas with the same bounds

12.18 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* $\vdash^{\beta}_{k} C_0, \ldots, C_k, \Sigma \Rightarrow \Lambda$, *then*

$$(\dagger) \qquad \vdash^{\alpha+\beta}_{k} \Gamma_0, \ldots, \Gamma_n, \Sigma \Rightarrow \Delta_0, \ldots, \Delta_n, \Lambda.$$

Proof The overall structure of the proof will be recognisable as the strategy used in the proof of lemma 12.11. I proceed by induction on β. Suppose

1. $\vdash^{\alpha}_{k} \Gamma_i \Rightarrow \Delta_i, C_i$ and $|C_i|_* \leq k$ for each $i \leq n$, and
2. $\vdash^{\beta}_{k} C_0, \ldots, C_k, \Sigma \Rightarrow \Lambda$.

I refer to the C_i as the *cut* formulas and will henceforth write $\vec{C}$ in place of $\{ C_0, \ldots, C_k \}$. 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

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

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 $\mathbb{N} \vDash s = t$ 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. $\vdash^{\gamma}_{k} \vec{C}, F, \Sigma \Rightarrow \Lambda$.

Applying the inversion lemma to (‡) yields

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

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:

12.19 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 $\vdash^{2^\alpha}_{k} \Gamma \Rightarrow \Delta$. ⊣

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

12.21 Theorem
If $\mathsf{PA}_n \vdash \Gamma \Rightarrow \Delta$ *is closed, then* $\mathsf{PA}\omega \vdash^{\alpha}_{0} \Gamma \Rightarrow \Delta$ *for some* $\alpha < \omega_{n+1}$.

Proof sketch From $\mathsf{PA}_n \vdash A$ we deduce that $\mathsf{PA} \vdash \Rightarrow A$ with a proof in which all cut formulas have implication rank $< n$ (theorem 10.22). 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

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

13. Transfinite induction and proof-theoretic ordinals

The final chapter is devoted to proving the optimality of theorem 12.14/corollary 12.16. 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.

13.1. 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.

13.1 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. ⌟

13.2 Example
The following two orderings on natural numbers are well-orders. The third is well-founded but not a well-order.

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

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

13.3 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

$$|n|_\prec := \sup\{\, |m|_\prec + 1 \mid m \prec n \,\}$$
$$\|\prec\| := \sup\{\, |n|_\prec + 1 \mid n \in \mathbb{N} \,\}$$

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 $|\cdot|_\prec : \mathbb{N} \to \mathbb{O}$ 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 $\mathbb{O}$.

13.4 Example
I compute the order types of natural numbers in the three orderings from example 13.2. Note, for the standard ordering on $\mathbb{N}$,

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

The ordering $<_1$ satisfies

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

The ordering $<_2$ satisfies

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

The ordering $<_3$ satisfies

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

13.5 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 10.6) 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 $\forall x \prec a F(x)$ as an abbreviation for the formula $\forall x(x \prec a \wedge F(x))$.

13.6 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 $\{\, |n|_\prec \mid n \prec a \,\}$.

13.7 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

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

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

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

Unpacking theorem 13.8, 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.

13.9 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 $m, n \in \mathbb{N}$.

13.1 Exercise
Prove lemma 13.9. Hint: Utilise the Cantor normal form theorem and a (primitive recursive) bijection between $\mathbb{N}$ and finite sequences of $\mathbb{N}$.

13.2 Exercise
Prove the following generalisation of lemma 13.9: 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 13.9. The proof of theorem 13.8 relies on one lemma whose proof is rather time-consuming and will be omitted:

13.10 Lemma
There exists a ID_2*-formula* $F(a)$ *such that*

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

Although I won't present the formal proof, I will show how F is constructed and the argument proceeds informally. First, I describe the construction of F as an operation on classes of ordinals. Let $O \subseteq \mathbb{O}$ be an arbitrary class of ordinals (playing the role of the interpretation of P). I write $\beta \subseteq O$ as shorthand for $(\forall \xi < \beta)\xi \in O$. 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. Furthermore, $0 \in O'$ is equivalent to the statement that O is progressive: $\xi \subseteq O$ implies $\xi \in O$ for all ordinals ξ. I claim that O' is progressive iff O is progressive. The 'only if' direction follows from the previous observation (if O' is progressive then, in particular, $0 \in O'$ and so O is progressive). For the converse, suppose that O is progressive. I have already reasoned that $0 \in O'$, so suppose $\alpha > 0$ is such that $\alpha \subseteq O'$. To establish $\alpha \in O'$ I am required to show that whenever $\xi \subseteq O$ also $\xi + \omega^\alpha \subseteq O$. Suppose $\xi \subseteq O$ and let $\beta < \alpha$ be arbitrary. Vacuously, $\xi + \omega^\beta.0 \subseteq O$. Moreover, if $\xi + \omega^\beta.n \subseteq O$ then, as $\beta \in O'$, also $\xi + \omega^\beta.(n+1) \subseteq O$. Therefore, $\xi + \omega^\beta.n \subseteq O$ for all $n < \omega$ by induction. Given that $\beta < \alpha$ was arbitrary, I conclude that $\xi + \omega^\alpha \subseteq O$, as required.

The link with lemma 13.10 is that $\alpha \in O'$ implies $\omega^\alpha \in O$, so the desired formula F will be one that expresses O' under the interpretation that P expresses O:

$$F(a) \coloneqq \forall x \big((\forall y \prec x \, P y) \to (\forall y \prec x \oplus \dot{\omega}^a) \, P y \big).$$

Notice that F is

13.3 Exercise
Prove lemma 13.10. Following the

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 proposition it suffices to show that $\mathsf{PA} \vdash \mathsf{Prog}_{\prec} A \to \mathsf{Prog}_{\prec} A'$.

Lemma 13.10 provides a sufficient condition for deducing transfinite induction for the predicate P up to an ordinal α, namely, transfinite induction for F up to any ordinal β such that $\alpha \leq \omega^\beta$. The lemma readily generalises to the case P is any formula:

13.11 Proposition
For every formula $F(a)$ in the language of arithmetic, there exists a formula $F'(a)$ such that

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

Proof

13.2. Bounding provable transfinite induction

The goal of this section is the converse to theorem 13.8:

13.12 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 $n \in \mathbb{N}$,

$$(\dagger) \qquad \mathsf{PA}\omega \vdash_0^\alpha \mathsf{Prog}_\prec P \Rightarrow \forall x \prec \underline{n}\, Px.$$

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

$$(\ddagger) \qquad \mathsf{PA}\omega + (\prec) \vdash_0^\alpha \Rightarrow \forall x \prec \underline{n} Px.$$

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 $\mathbb{N} \vDash \underline{n} = s$. This notation presupposes that s is closed.

13.13 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 $\mathsf{PA}\omega + (\prec) \vdash_k^\alpha \Gamma \Rightarrow \Delta$ is given as in definition 12.2. ⌟

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 $\mathsf{PA}\omega$.

13.14 Lemma
If $\mathsf{PA}\omega \vdash_k^\alpha \Gamma \Rightarrow \Delta$ *then* $\mathsf{PA}\omega + (\prec) \vdash_k^\alpha \Gamma \Rightarrow \Delta$.

Proof Immediate. ⊣

13.15 Lemma
$\mathsf{PA}\omega + (\prec) \vdash_0^\omega \ \Rightarrow \mathsf{Prog}_\prec P$.

Proof Recall that $\mathsf{Prog}_\prec P = \forall x(\forall y(y \prec x \to Py) \to Px)$. Let k be the constant given by proposition 12.7 such that $\mathsf{PA}\omega \vdash_0^k \Rightarrow \underline{m} \prec \underline{n}$ 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 $m \prec n$:

$$\dfrac{\dfrac{\dfrac{}{\vdash_0^0 P\underline{m} \Rightarrow P\underline{m}}\mathsf{id} \qquad \begin{matrix}\vdots\\ \vdash_0^k \ \Rightarrow \underline{m} \prec \underline{n}\end{matrix}}{\vdash_0^{k+1} \underline{m} \prec \underline{n} \to P\underline{m} \Rightarrow P\underline{m}}\mathsf{L}{\to}}{\vdash_0^{k+2} \forall y \prec \underline{n}\, Py \Rightarrow P\underline{m}}\mathsf{L}\forall$$

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

$$\dfrac{\dfrac{\dfrac{\vdots}{\vdash_0^{k+2} \forall y \prec \underline{n}\, Py \Rightarrow P\underline{m} \text{ for all } m \prec n}\prec}{\vdash_0^{k+3} \forall y \prec \underline{n}\, Py \Rightarrow P\underline{n}}\mathsf{R}{\to}}{\dfrac{\vdash_0^{k+4} \Rightarrow (\forall y \prec \underline{n}\, Py) \to P\underline{n} \qquad \text{for every } n}{\vdash_0^{k+5} \Rightarrow \mathsf{Prog}_{\prec}P}\mathsf{R}{\forall}}$$

An application of bound weakening completes the proof. ⊣

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

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

Proof The embedding lemma for $\mathsf{PA}\omega$ (lemma 12.6) and inversions yields a $k < \omega$ such that for all $n \in \mathbb{N}$:

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

Lemma 13.15 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 $\alpha = |n|_{\prec}$.

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

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

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

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

$$\text{for every } \delta < \beta_n,\ \min\{\beta, \delta\} \leq \alpha + \gamma_\delta. \tag{13.1}$$

Consider two cases. First, suppose $\beta < \beta_n$. Choosing $\delta = \beta$ in (13.1) yields

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

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

$$\begin{aligned} \beta = \sup\{\delta + 1 \mid \delta < \beta\} &\leq \sup\{\alpha + \gamma_\delta + 1 \mid \delta < \beta\} && \text{by (13.1)} \\ &\leq \alpha + \sup\{\gamma_\delta + 1 \mid \delta < \beta\} && \text{continuity} \\ &\leq \alpha + \gamma. \end{aligned}$$

⊣

Proof of theorem 13.12 (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 13.16) 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 $\|\prec\| \leq \gamma{+}1 < \varepsilon_0$.⊣

13.3. 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.

13.18 Weakening lemma
If $\mathsf{PA}\omega{+}(\prec) \vdash_k^\alpha \Gamma \Rightarrow \Delta$ *and* $\Gamma' \Rightarrow \Delta'$ *is closed then* $\mathsf{PA}\omega{+}(\prec) \vdash_k^\alpha \Gamma', \Gamma \Rightarrow \Delta, \Delta'$.

13.19 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* $\mathbb{N} \vDash s = t$. *If* $\mathsf{PA}\omega + (\prec) \vdash_k^\alpha \Gamma(s) \Rightarrow \Delta(s)$ *then* $\mathsf{PA}\omega + (\prec) \vdash_k^\alpha \Gamma(t) \Rightarrow \Delta(t)$.

13.4 Exercise
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.

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

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 $\vdash_k^\alpha \Gamma \Rightarrow \Delta, C$ 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, $\vdash_k^\beta C, \Gamma \Rightarrow \Lambda$. 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 $\vdash_k^\alpha \Gamma \Rightarrow \Delta, \Lambda$. ⊣

13.5 Exercise
Complete the proof of the reduction lemma.

13.21 Cut elimination theorem
If $\mathsf{PA}\omega + (\prec) \vdash_k^\alpha \Gamma \Rightarrow \Delta$ *then* $\mathsf{PA}\omega + (\prec) \vdash_0^{\omega^\alpha_k} \Gamma \Rightarrow \Delta$.

Proof The proof proceeds precisely as before. ⊣

13.4. Characterisation of provable transfinite induction

Combining the results in this chapter:

13.22 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 13.8 and $\|\mathsf{PA}\| \leq \varepsilon_0$ by theorem 13.12. ⊣

13.23 Independence of transfinite induction corollary
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 12.21, but it needs to be refined.

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

Index of conventions

Bibliography

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

Georg Cantor. Beiträge zur begründung der transfiniten mengenlehre ii. *Mathematische Annalen*, 49(2):207–246, 1897. doi: 10.1007/BF01444205.

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. doi: 10.1016/S0049-237X(08)70827-9. English translation, "New Version of the Consistency Proof for Elementary Number Theory", in Gentzen (1969): 252–286.

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

Gerhard Hessenberg. *Grundbegriffe der Mengenlehre*. Göttingen, 1906.

Sara Negri and Jan von Plato. *Structural Proof Theory*. Cambridge University Press, 2001.

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

Wolfram Pohlers. *Proof Theory An Introduction*, volume 1407 of *Lecture Notes in Mathematics*. Springer, Berlin, Heidelberg, 1989. doi: 10.1007/978-3-540-46825-7.

Michael Rathjen. Proof theory. unpublished lecture notes, 2012.

Kurt Schütte. Beweistheoretische erfassung der unendlichen induktion in der zahlentheorie. *Mathematische Annalen*, 5(5):369–389, 1950. doi: 10.1007/BF01342849.

A. S. Troelstra and H. Schwichtenberg. *Basic Proof Theory*. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 2 edition, 2000.