CHAPTER 3

INTRODUCTION TO THE THEORY OF PROOFS

In order to study *proofs* as mathematical objects, it is necessary to introduce deductive systems which are richer and model better the intuitive proofs we give in mathematics than the Hilbert system of Part A. Our (limited) aim in this Part is to formulate and establish in outline a central result of Gentzen, which in addition to its foundational significance also has a large number of applications.

3A. The Gentzen Systems

The main difference between the Hilbert proof system and the Gentzen systems **G** and **GI** is in the *proofs*, which Gentzen endows with a rich, combinatorial structure that facilitates their mathematical study. It will also be convenient, however, to enlarge the language $\mathbb{FOL}(\tau)$ with a sequence of **propositional variables**

$$\mathsf{p}_1, \mathsf{p}_1, \dots ,$$

so that the Propositional Calculus is naturally embedded in $\mathbb{FOL}(\tau)$, for any signature τ. So the formulas of $\mathbb{FOL}(\tau)$ are now defined by the recursion

$$\begin{aligned} \chi :\equiv p \mid s = t \mid R(t_1, \dots , t_n) \quad &(\text{the } \textit{prime formulas}) \\ \mid \neg(\phi) \mid (\phi) \to (\psi) \mid (\phi)\ \&\ (\psi) \mid (\phi) \vee (\psi) \mid \forall v\phi \mid \exists v\phi & \end{aligned}$$

where p is any propositional variable; and in the semantics of the system, we admit assignments which in addition to their values on individual variables also assign a truth value $\pi(p)$ (either 1 or 0) to every propositional variable p.

We should also note that the identity symbol is treated like any other relation constant by the Gentzen systems, i.e., we do not postulate the Axioms for Identity and we will need to include them among the hypotheses when they are relevant.

Definition 3A.1. A **sequent** (in a fixed signature τ) is an expression

$$\phi_1, \dots, \phi_n \Rightarrow \psi_1, \dots, \psi_m$$

where $\phi_1, \dots, \phi_n, \psi_1, \dots, \psi_m$ are τ-formulas. We view the formulas on the left and the right as comprising **multisets**, i.e., we identify sequences which differ only in the order in which they list their terms. The empty multisets are allowed, so that the simplest sequent is just $\Rightarrow$. The next simplest ones are of the form $\Rightarrow \phi$ and $\phi \Rightarrow$.

Definition 3A.2. The axioms and rules of inference of the **classical Gentzen system G** and the **intuitionistic system GI** are listed in Table 1; the only difference between the two systems is that in **GI** we only allow sequents which have at most one formula on the right, they look like

$$A \Rightarrow \phi \text{ or } A \Rightarrow$$

There is one axiom (scheme), the sequent $\phi \Rightarrow \phi$, for each formula ϕ; one **introduction rule** (on the left) and one **elimination rule** (on the right) for each logical construct; a similar pair of **thinning** (T) and **contraction** (C) introduction and elimination rules; and the **Cut Rule** at the end—which may be viewed as an elimination rule but plays a very special role. In all rules where an extended formula $\phi(v)$ and a substitution instance $\phi(t)$ or $\phi(x)$ of that formula occur, we assume that the term t or the variable x is free for v in $\phi(v)$, and there is an additional **Restriction** in the $\forall$-introduction and $\exists$-elimination rules which is listed in the Table.

3A.3. Terminology. We classify the rules of **G** and **GI** into three categories, as follows:

1. The **structural rules** T (Thinning) and C (Contraction).
2. The **Cut**.
3. The **logical rules**, two for each logical construct, which are again subdivided into **propositional** and **quantifier** rules in the obvious way.

Each rule has one or two **premises**, the sequents above the line, and a **conclusion**, the sequent below the line; a single sequent axiom is its own conclusion and has no premises.

The formulas in A, B are the **side formulas** of a rule. The remaining zero, one or two formulas in the premises are the **principal formulas** of the rule, and the remaining formulas in the conclusion are the **new formulas** of the rule. Notice that an axiom has no side formulas, no principal formulas and two new (identical) formulas; a Cut has two principal formulas and no new formulas; and every other rule has exactly one new formula.

Each new formula in a rule is associated with zero, one or two formulas in the premises, which are its **parents**; the new formula is an "orphan" in an axiom and in the thinning rule T. We also associate each side formula in the conclusion of a rule with exactly one parent in one of the premises, from which is was copied.

The Gentzen Systems **G**, **GI**

Axiom Scheme $\phi \Rightarrow \phi$

$\rightarrow$	$\dfrac{A,\, \phi \Rightarrow B,\, \psi}{A \Rightarrow B,\, \phi \rightarrow \psi}$	$\dfrac{A_1 \Rightarrow B_1,\, \phi \quad A_2,\, \psi \Rightarrow B_2}{A_1,\, A_2,\, \phi \rightarrow \psi \Rightarrow B_1,\, B_2}$
$\&$	$\dfrac{A \Rightarrow B,\, \phi \quad A \Rightarrow B,\, \psi}{A \Rightarrow B,\, \phi \,\&\, \psi}$	$\dfrac{\phi,\, A \Rightarrow B}{\phi \,\&\, \psi,\, A \Rightarrow B} \quad \dfrac{\psi,\, A \Rightarrow B}{\phi \,\&\, \psi,\, A \Rightarrow B}$
$\vee$	$\dfrac{A \Rightarrow B,\, \phi}{A \Rightarrow B,\, \phi \vee \psi} \quad \dfrac{A \Rightarrow B,\, \psi}{A \Rightarrow B,\, \phi \vee \psi}$	$\dfrac{A,\, \phi \Rightarrow B \quad A,\, \psi \Rightarrow B}{A,\, \phi \vee \psi \Rightarrow B}$
$\neg$	$\dfrac{A,\, \phi \Rightarrow B}{A, \Rightarrow B,\, \neg\phi}$	$\dfrac{A \Rightarrow B,\, \phi}{A,\, \neg\phi \Rightarrow B}$
$\forall$	$\dfrac{A \Rightarrow B,\, \phi(v)}{A \Rightarrow B,\, \forall x\phi(x)}$ (**Restr**)	$\dfrac{A,\, \phi(t) \Rightarrow B}{A,\, \forall x\phi(x) \Rightarrow B}$
$\exists$	$\dfrac{A \Rightarrow B,\, \phi(t)}{A \Rightarrow B,\, \exists x\phi(x)}$	$\dfrac{A,\, \phi(v) \Rightarrow B}{A,\, \exists x\phi(x) \Rightarrow B}$ (**Restr**)
T	$\dfrac{A \Rightarrow B}{A \Rightarrow B,\, \phi}$	$\dfrac{A \Rightarrow B}{A,\, \phi \Rightarrow B}$
C	$\dfrac{A \Rightarrow B,\, \phi,\, \phi}{A \Rightarrow B,\, \phi}$	$\dfrac{A,\, \phi,\, \phi \Rightarrow B}{A,\, \phi \Rightarrow B}$

$$\text{Cut} \qquad \frac{A_1 \Rightarrow B_1,\, \chi, \qquad \chi,\, A_2 \Rightarrow B_2}{A_1,\, A_2 \Rightarrow B_1,\, B_2}$$

(1) A, B are multisets of formulas in $\mathbb{FOL}(\tau)$.
(2) For the Intuitionistic system **GI**, at most one formula is allowed on the right.
(3) **Restr** : the **active variable** v is not free in A, B.
(4) The formulas in A, B are the *side formulas* of an inference.
(5) The formulas ϕ, ψ above the line are the *principal formulas* of the inference. (One or two; none in the axiom.)
(6) There is an obvious *new formula* below the line in each inference, except for Cut.
(7) Each new and each side formula in the conclusion of each rule is associated with zero, one or two parent formulas in the premises.

Table 1. The Gentzen systems.

Definition 3A.4 (Proofs)**.** The set of Gentzen **proofs** of depth $\leq d$ and the **endsequent** of each proof are defined together by the following recursion on the natural number $d \geq 1$.

1. For each formula ϕ, the pair $(\emptyset, \phi \Rightarrow \phi)$ is a proof of depth ≤ 1 and endsequent $\phi \Rightarrow \phi$. We picture it in **tree form** by:

$$\frac{}{\phi \Rightarrow \phi}$$

2. If Π is a proof of depth $\leq d$ and endsequent α and

$$\frac{\alpha}{\beta}$$

is a one-premise inference rule, then the pair (Π, β) is a proof of depth $\leq (d+1)$ and endsequent β. We picture (Π, β) in tree form by:

$$\frac{\Pi}{\beta}.$$

3. If Π_1, Π_2 are proofs of depth $\leq d$ and respective endsequents α_1, α_2, and if

$$\frac{\alpha_1 \qquad \alpha_2}{\beta}$$

is a two-premise inference rule, then the pair $((\Pi_1, \Pi_2), \beta)$ is a proof of depth $\leq (d+1)$. We picture $((\Pi_1, \Pi_2), \beta)$ in tree form by:

$$\frac{\Pi_1 \qquad \Pi_2}{\beta}$$

A **proof** Π in **G** of **GI** is a proof of depth d, for some d, and it is a proof of its endsequent; it is a **propositional proof** if none of the four rules about the quantifiers are used in it. We denote the relevant relations by

$$\mathbf{G} \vdash A \Rightarrow B,\ \mathbf{G} \vdash_{\text{prop}} A \Rightarrow B,\ \mathbf{GI} \vdash A \Rightarrow B,\ \text{or}\ \mathbf{GI} \vdash_{\text{prop}} A \Rightarrow B$$

accordingly.

We let $\mathbf{G}_{\text{prop}}$ and $\mathbf{GI}_{\text{prop}}$ be the restricted systems in which only formulas for the Propositional Calculus 1K.1 and only propositional rules are allowed.

Proposition 3A.5 (Parsing for Gentzen proofs)**.** *Each proof* Π *satisfies exactly one of the following three conditions.*

1. $\Pi = (\emptyset, \beta)$*, where* β *is an axiom.*
2. $\Pi = (\Sigma, \beta)$*, where* Σ *is a proof of smaller depth and endsequent some* α*, and there is a one premise rule* $\dfrac{\alpha}{\beta}$*.*

3. $\Pi = ((\Sigma_1, \Sigma_2), \beta)$, *where* Σ_1, Σ_2 *are proofs of smaller depth and respective endsequents* α_1, α_2, *and there is a two premise rule* $\dfrac{\alpha_1 \quad \alpha_2}{\beta}$.

In all cases, a proof is a pair and the second member of that pair is its endsequent.

Proofs in the Gentzen systems are displayed in tree form, as in the following examples which prove in **G** three of the propositional axioms of the Hilbert system:

$$\dfrac{\dfrac{\dfrac{\chi \Rightarrow \chi}{\Rightarrow \chi, \neg\chi}\,(\Rightarrow \neg)}{\neg\neg\chi \Rightarrow \chi}\,(\neg \Rightarrow)}{\Rightarrow \neg\neg\chi \to \chi}\,(\Rightarrow\to) \qquad \dfrac{\dfrac{\dfrac{\phi \Rightarrow \phi}{\phi, \psi \Rightarrow \phi}\,(T)}{\phi \Rightarrow \psi \to \phi}\,(\Rightarrow\to)}{\Rightarrow \phi \to (\psi \to \phi)}\,(\Rightarrow\to)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\phi \Rightarrow \phi}{\phi, \psi \Rightarrow \phi}\,(T) \qquad \dfrac{\psi \Rightarrow \psi}{\phi, \psi \Rightarrow \psi}\,(T)}{\phi, \psi \Rightarrow \phi \;\&\; \psi}\,(\Rightarrow \&)}{\phi \Rightarrow \psi \to (\phi \;\&\; \psi)}\,(\Rightarrow\to)}{\Rightarrow \phi \to (\psi \to (\phi \;\&\; \psi))}\,(\Rightarrow\to)$$

Notice that the first of these proofs is in **G**, while the last two are in **GI**.

In the next example of a **GI**-proof of another of the Hilbert propositional axioms we do not label the rules, but we put in boxes the principal formulas for each application:

$$\dfrac{\dfrac{\dfrac{\phi \Rightarrow \boxed{\phi} \qquad \dfrac{\phi \Rightarrow \boxed{\phi} \qquad \dfrac{\psi \Rightarrow \boxed{\psi} \qquad \boxed{\chi} \Rightarrow \chi}{\psi, \boxed{\psi \to \chi} \Rightarrow \chi}}{\phi, \boxed{\psi}, \phi \to (\psi \to \chi) \Rightarrow \chi}}{\boxed{\phi}, \phi \to \psi, \phi \to (\psi \to \chi) \Rightarrow \boxed{\chi}}}{\dfrac{\phi \to \psi, \boxed{\phi \to (\psi \to \chi)} \Rightarrow \boxed{\phi \to \chi}}{\boxed{\phi \to \psi} \Rightarrow \boxed{\phi \to (\psi \to \chi) \to (\phi \to \chi)}}}}{\Rightarrow (\phi \to \psi) \to ((\phi \to (\psi \to \chi)) \to (\phi \to \chi))}$$

The form of the rules of inference in the Gentzen systems makes it much easier to discover proofs in them rather than in the Hilbert system. Consider,

for example, the following, which can be constructed step-by-step starting with the last sequent (which is what we want to show) and trying out the most plausible inference which gives it:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\phi \Rightarrow \phi}{\forall v\phi \Rightarrow \phi}(\forall \Rightarrow)}{\forall v\phi \Rightarrow \exists u\phi}(\Rightarrow \exists)}{\exists u\forall v\phi \Rightarrow \exists u\phi}(\exists \Rightarrow,\ u \text{ not free on the right})}{\exists u\forall v\phi \Rightarrow \forall v\exists u\phi}(\Rightarrow \forall,\ v \text{ not free on the left})}{\Rightarrow \exists u\forall v\phi \to \forall v\exists u\phi}(\Rightarrow\to)$$

In fact these guesses are unique in this example, except for Thinnings, Contractions and Cuts, an it is quite common that the most difficult proofs to construct are those which required T's and C's—especially as we will show that Cuts are not necessary.

Theorem 3A.6 (Strong semantic soundness of **G**)**.** *Suppose*

$$\mathbf{G} \vdash \phi_1, \dots, \phi_n \Rightarrow \psi_1, \dots, \psi_m,$$

and **A** *is any structure (of the fixed signature): then for every assignment* π *into* **A***,*

$$\text{if } \mathbf{A}, \pi \models \phi \ \& \ \dots \ \& \ \phi_n, \text{ then } \mathbf{A}, \pi \models \psi \vee \dots \vee \psi_m.$$

Here the empty conjunction is interpreted by 1 and the empty disjunction is interpreted by 0.

Theorem 3A.7 (Proof-theoretic soundness of **G**)**.** *If* $\mathbf{G} \vdash A \Rightarrow B$*, then* $A \vdash \vee B$ *in the Hilbert system, by a deduction in which no free variable of* A *is quantified and the Identity Axioms* (5) – (17) *are not used.*

Theorem 3A.8 (Proof-theoretic completeness of **G**)**.** *If* $A \vdash \phi$ *in the Hilbert system by a deduction in which no free variable of* A *is quantified and the Identity Axioms* (5) – (17) *are not used, then* $\mathbf{G} \vdash A \Rightarrow \phi$*.*

These three theorems are all proved by direct (and simple, if a bit cumbersome) inductions on the given proofs.

3A.9. Remark. The condition in Theorem 3A.8 is necessary, because (for example)

$$R(x) \vdash \forall x R(x) \tag{66}$$

but the sequent

$$R(x) \Rightarrow \forall x R(x)$$

is not provable in **G**, because of the strong Soundness Theorem 3A.6. The Hilbert system satisfies the following weaker Soundness Theorem, which does not contradict the deduction (67): *if* $A \vdash \phi$ *and every assignment* π *into* $\mathbf{A}$ *satisfies* A*, then every assignment* π *into* $\mathbf{A}$ *satisfies* ϕ*.* (We have stated the Soundness Theorem for the Hilbert system in **4.3** only for sets of sentences as hypotheses, but to prove it we needed to show this stronger statement.)

Theorem 3A.10 (Semantic Completeness of **G**)**.** *Suppose* $\psi, \phi_1, \ldots, \phi_n$ *are* τ*-formulas such that for every* τ*-structure* $\mathbf{A}$ *and every assignment* π *into* $\mathbf{A}$*,*

$$\text{if } \mathbf{A}, \pi \models \phi_1 \ \& \ \cdots \ \& \ \phi_n, \text{ then } \mathbf{A}, \pi \models \psi;$$

it follows that

$$\mathbf{G} \vdash \mathrm{IA}, \phi_1, \ldots, \phi_n \Rightarrow \psi,$$

where IA *are the* (finitely many) *identity axioms for the relation and function symbols which occur in* $\psi, \phi_1, \ldots, \phi_n$*.*

Proof This follows easily from Theorem 3A.8 and the Completeness Theorem for the Hilbert system. ⊣

3A.11. The intuitionistic Gentzen system GI. The system **GI** is a formalization of L. E. J. Brouwer's *intuitionistic logic*, the logical foundation of constructive mathematics. This was developed near the beginning of the 20th century. It was Gentzen's ingenious idea that constructive logic can be captured simply by restricting the number of formulas on the right of a sequent. About constructive mathematics, we will say a little more later on; for now, we just use **GI** as a tool to understand the combinatorial methods of analyzing formal proofs that pervade proof theory.

Problems for Section 3A

Problem 3A.1. Prove Theorem 3A.10, the (strong) Semantic Completeness of **G**.

3B. Cut-free proofs

Cut is the only **G**-rule which "loses the justification" for the truth of its conclusion, just as Modus Ponens (which is a simple version of it) does in the Hilbert system. As a result, *Cut-free* Gentzen proofs (which do not use the Cut) have important special properties.

Proposition 3B.1. *If one of the logical symbols* $\neg$, $\&$, $\vee$, $\rightarrow$, $\forall$ *or* $\exists$ *does not occur in the endsequent of a Cut-free proof* Π*, then that logical symbol does not occur at all in* Π*, and hence neither of the rules involving that logical symbol are applied in* Π*.*

Definition 3B.2. The **subformulas** of a formula of $\mathbb{FOL}(\tau)$ are defined by the following recursion.

1. If $\chi \equiv p, \chi \equiv R(t_1, \dots, t_n)$ or $\chi \equiv s = t$ is prime, then χ is the only subformula of itself.
2. If χ is a propositional combination of ϕ and ψ, then the subformulas of χ are χ itself, and all the subformulas of ϕ and ψ.
3. If $\chi \equiv \exists x \phi(x)$ or $\chi \equiv \forall x \phi(x)$, then the subformulas of χ are χ and all subformulas of substitution instances $\phi(t)$, where t is an arbitrary term, free for x in $\phi(x)$. (Here t may be a variable, since variables are terms, and in particular $\phi(x)$ is a subformula of χ.)

For example, the subformulas of $\exists x R(x, y)$ are all $R(t, y)$, and there are infinitely many of them; if a formula has only finitely many subformulas, then it is propositional.

Theorem 3B.3 (Subformula Property)**.** *If* Π *is a* **Cut-free proof** *with endsequent* α*, then every formula which occurs in* Π *is a subformula of some formula in* α*.*

Corollary 3B.4. *If a constant* c*, a relation symbol* R *or a function symbol* f *does not occur in the endsequent of a Cut-free proof* Π*, then* c*,* R *or* f *does not occur at all in* Π*.*

Problems for Section 3B

Problem 3B.1. Suppose Π is a Cut-free proof in **G** of a sequent $\Rightarrow \phi$, where ϕ is in prenex form and has n quantifiers; prove that every formula in Π is prenex with at most n quantifiers.

Problem 3B.2. Suppose Π is a Cut-free proof in **G** with endsequent $A \Rightarrow B$, in which there are no applications of the (four) logical rules that involve the symbols $\neg$ and $\rightarrow$. Prove that every formula ϕ which occurs on the left of some sequent in Π is a subformula of some formula in A; and every formula ψ which occurs on the right of some sequent in Π is a subformula of some formula in B.

Problem 3B.3. Suppose Π is a Cut-free proof in **G** of a sequent $\Rightarrow \phi$, where ϕ is in prenex form and has n quantifiers; prove that every formula in Π is prenex with at most n quantifiers.

3C. Cut Elimination

We outline here (with few details) a proof of the following, fundamental theorem of Gentzen, to the effect that up to alphabetic changes in bound variables, every provable sequent has a Cut-free proof:

Theorem 3C.1 (Cut Elimination Theorem, Gentzen's Hauptsatz)**.** *From a proof in* **G** *or* **GI** *of a sequent* α *in which no variable occurs both free and bound, we can construct a pure variable, Cut-free proof of* α *in the same system.*

Pure variable proofs will be defined below in Definition 3C.8.

This is the basic result of Proof Theory, and it has a host of important consequences in all parts of logic (and some parts of classical mathematics as well).

3C.2. The Mix rule. This is a strengthening of the Cut rule, which allows us to Cut simultaneously all occurrences of the Cut formula:

$$\frac{A_1 \Rightarrow B_1 \qquad A_2 \Rightarrow B_2}{A_1,\, A_2 \setminus \{\chi\} \Rightarrow B_1 \setminus \{\chi\},\, B_2} \text{ assuming that } \chi \in A_2 \cap B_1.$$

For a multiset D, by $D \setminus \{\chi\}$ we mean the result of removing all occurrences of χ from D.

By $\mathbf{G}^m$ and $\mathbf{GI}^m$ we understand the systems in which the Cut Rule has been replaced by the Mix Rule.

Lemma 3C.3. *If we replace the Cut Rule by the Mix Rule, we get exactly the same provable sequents, both for* **G** *and for* **GI***.*

In fact*: every proof* Π *of* **G** *or* **GI** *can be converted into a proof* Π^m *in* $\mathbf{G}^m$ *or* $\mathbf{GI}^m$ *respectively, in which exactly the same logical rules are used—i.e., by replacing the Cuts by Mixes and* (possibly) *introducing some applications of structural rules; and vice versa.*

From now on by "proof" we will mean "proof in $\mathbf{G}^m$ or $\mathbf{GI}^m$", unless otherwise stated.

Definition 3C.4. To each (occurrence of a) sequent α in a proof Π, we assign **the part of the proof above** α by the following recursion.

1. If α is the endsequent of a proof Π, then the part of Π above α is the entire Π.
2. If $\Pi = (\Sigma, \beta)$ is a proof and α occurs in Σ, then the part of Π above α is the part of Σ above α. (Here Σ is a proof, by the Parsing Lemma for proofs.)

3. If $\Pi = ((\Sigma_1, \Sigma_2), \beta)$ is a proof and α occurs in Σ_1, then the part of Π above α is the part of Σ_1 above α; and if α occurs in Σ_2, then the part of Π above α is the part of Σ_2 above α. (Again Σ_1, Σ_2 are proofs here.)

Lemma 3C.5. *If α occurs in a proof Π, then the part of Π above α is a proof with endsequent α.*

The proof of Mix Elimination for propositional proofs is substantially easier than the proof for the full systems, especially as *all propositional proofs have the pure variable property.* We give this first.

Theorem 3C.6 (Main Propositional Lemma)**.** *Suppose we are given a propositional proof*

$$\dfrac{\dfrac{\Pi_1}{A_1 \Rightarrow B_1} \qquad \dfrac{\Pi_2}{A_2 \Rightarrow B_2}}{A_1,\, A_2 \setminus \{\chi\} \Rightarrow B_1 \setminus \{\chi\},\, B_2}$$

in $\mathbf{G}^m$ or $\mathbf{GI}^m$ which has exactly one Mix as its last inference; we can then construct a Mix-free, propositional proof of the endsequent

$$A_1,\, A_2 \setminus \{\chi\} \Rightarrow B_1 \setminus \{\chi\},\, B_2 \tag{67}$$

which uses the same logical rules.

Equivalently: *given any propositional, Mix-free proofs of*

$$A_1 \Rightarrow B_1 \quad \textit{and} \quad A_2 \Rightarrow B_2$$

such that a formula χ occurs in both B_1 and A_2, we can construct a propositional, Mix-free proof of (68) *which uses the same logical rules.*

Outline of the proof. We define the *left Mix rank* to be the number of consecutive sequents in the proof which ends with $A_1 \Rightarrow B_1$ starting from the last one and going up, in which χ occurs on the right; so this is at least 1. The *right Mix rank* is defined similarly, and the *rank* of the Mix is their sum. *The minimum Mix rank is* 2. The *grade* of the Mix is the number of logical symbols in the Mix formula χ.

The proof is *by induction on the grade.* Both in the basis (when χ is a prime formula) and in the induction step, we will need an *induction on the rank*, so that the proof really is by *double induction.*

Lemma 1. If the Mix formula χ occurs in A_1 or in B_2, then we can eliminate the Mix using Thinnings and Contractions.

Lemma 2. If the left Mix rank is 1 *and the last left inference is by a T or a C, then the Mix can be eliminated; similarly if the right Mix rank is* 1 *and the*

last right inference is a C or a T. (Actually the last left inference cannot be a C if the left Mix rank is 1.)

Main part of the proof. We now consider cases on what the last left inference and the last right inference is, and we may assume that the Main Lemma holds for all cases of smaller grade, and for all cases of the same grade but smaller rank. The cases where one of the ranks is > 1 are treated first, and are messy but fairly easy. The main part of the proof is in the consideration of the four cases (one for each propositional connective) where the rank is exactly 2, so that χ is introduced by the last inference on both sides: in these cases we use the induction hypothesis on the grade, reducing the problem to cases of smaller grade (but possibly larger rank). ⊣

Proof of Theorem 3C.1 for propositional proofs is by induction on the number of Mixes in the given proof, with the basis given by Lemma 3C.6; in the Inductive Step, we simply apply the same Lemma to an *uppermost Mix*, one such the part of the proof above its conclusion has no more Mixes. ⊣

The proof of the Hauptsatz for the full (classical and intuitionistic) systems is complicated by the extra hypothesis on free-and-bound occurrences of the same variable, which is necessary because of the following example whose proof we will leave for the problems:

Proposition 3C.7. *The sequent* $\forall x \forall y R(x,y) \Rightarrow R(y,y)$ *is provable in* **GI**, *but it is not provable without a Cut* (even in the stronger system **G**).

To deal with this problem, we need to introduce a "global" restriction on proofs, as follows.

3C.8. Definition. A **pure variable proof** (in any of the four Gentzen systems we have introduced) is a proof Π with the following two properties.

1. No variable occurs both free and bound in Π.
2. If v is the active variable in an application of one of the two rules which have a restriction,

$$\frac{A \Rightarrow B, \phi(v)}{A \Rightarrow B, \forall x \phi(x)} \qquad \text{or} \qquad \frac{A, \phi(v) \Rightarrow B}{A, \exists x \phi(x) \Rightarrow B},$$

then v occurs only in the part of the proof above the premise of this application.

Lemma 3C.9. *In a pure variable proof, a variable* v *can be used at most once in an application of the* $\Rightarrow \forall$ *or the* $\exists \Rightarrow$ *rules.*

Proposition 3C.10 (Pure Variable Lemma)**.** *If α is a sequent in which no variable occurs both free and bound, then from every proof of α we can construct a pure variable proof of α, employing only replacement of some variables by fresh variables.*

With this result at hand, we can establish an appropriate version of Lemma 3C.6 which applies to the full systems:

Theorem 3C.11 (Main Lemma)**.** *Suppose we are given a pure variable proof*

$$\dfrac{\dfrac{\Pi_1}{A_1 \Rightarrow B_1} \qquad \dfrac{\Pi_2}{A_2 \Rightarrow B_2}}{A_1,\, A_2 \setminus \{\chi\} \Rightarrow B_1 \setminus \{\chi\},\, B_2}$$

in $\mathbf{G}^m$ or $\mathbf{GI}^m$ which has exactly one Mix as its last inference; we can then construct a Mix-free, pure variable proof of the endsequent

$$A_1,\, A_2 \setminus \{\chi\} \Rightarrow B_1 \setminus \{\chi\},\, B_2 \tag{68}$$

which uses the same logical rules.

Equivalently: *from any given, pure variable, Mix-free proofs of*

$$A_1 \Rightarrow B_1 \quad \textit{and} \quad A_2 \Rightarrow B_2$$

such that a formula χ occurs in both B_1 and A_2 and no free variable of one of them occurs bound in the other, we can construct a pure variable, Mix-free proof of (69) *which uses the same logical rules.*

The proof of this is an extension of the proof of Lemma 3C.6 which requires the consideration of two, additional cases in the induction step with rank 2—quite simple, as it happens, because the quantifier rules have only one premise.

Outline of proof of Theorem 3C.1. It is enough to prove the theorem for pure variable proofs in the system with Mix instead of Cut; and we do this by induction on the number of Mixes in the given, pure variable proof, using the Main Lemma 3C.11. ⊣

Problems for Section 3C

Problem 3C.1. Construct a Cut-free **GI** proof of

$$(\phi \to \psi) \to ((\phi \to \neg\psi) \to \neg\phi)$$

Problem 3C.2. Construct a Cut-free **GI** proof of

$$(\phi \to \chi) \to ((\psi \to \chi) \to ((\phi \vee \psi) \to \chi))$$

Problem 3C.3. Construct a Cut-free **G** proof of *Peirce's Law*,

$$(((p \to q) \to p) \to p)$$

Problem 3C.4. Construct a proof in **GI** of the sequent

$$\forall x \forall y) R(x, y) \;\Rightarrow\; R(y, y).$$

3D. The Extended Hauptsatz

For sequents of formulas in prenex form, the Gentzen Hauptsatz provides a particularly simple and useful form.

3D.1. Normal proofs. A proof Π in **G** is **normal** if it is a pure variable, Cut-free proof and a **midsequent** $A^* \Rightarrow B^*$ occurs in it with the following properties.

1. Every formula which occurs above the midsequent $A^* \Rightarrow B^*$ is quantifier free.
2. The only rules applied below the midsequent are quantifier rules or Contractions.

Notice that by the first of these properties, *no quantifier rules are applied in a normal proof above the midsequent*—only propositional and structural rule applications. So a normal proof looks like

$$\begin{array}{c} \Pi \\ \hline A^* \Rightarrow B^* \\ \vdots \\ A \Rightarrow B \end{array}$$

where Π is a propositional proof and in the "linear trunk" which follows the provable, quantifier-free sequent only one-premise Contractions and quantifier inferences occur.

Theorem 3D.2 (The Extended Hauptsatz)**.** *If $A \Rightarrow B$ is a sequent of prenex formulas in which no variable occurs both free and bound, and if $A \Rightarrow B$ is provable in* **G***, then there exists a normal proof of $A \Rightarrow B$.*

Outline of proof. This is a constructive argument, which produces the desired normal proof of $A \Rightarrow B$ from any given proof of it.

Step 1. By the Cut Elimination Theorem we get a new proof, which is Cut-free and pure variable.

Step 2. We replace all Axioms and all Thinnings by Axioms and Thinnings on prime (and hence quantifier free) formulas (without destroying the Cut-free, pure variable property).

The *order* of a quantifier rule application in the proof is the number of Thinnings and propositional inferences below it, down to the endsequent, and the *order of the proof* is the sum of the orders of all quantifier rule applications in the proof. If the order of the proof is 0, then there is no quantifier rule application above a Thinning or a propositional rule application, and then the proof (easily) is normal.

Proof is by induction on the order of the given proof. We begin by noticing that if the order is > 0, then there must exist some quantifier rule application *immediately above* a Thinning or a propositional rule application; we choose one such, and alter the proof to one with a smaller order and the same endsequent. The heart of the proof is the consideration of cases on *what these two inferences immediately above each other are*, the top one a quantifier rule application and the bottom one a propositional rule application or a T. It is crucial to use the fact that all the formulas in the endsequent are prenex, and hence (by the subformula property) all the formulas which occur in the proof are prenex; this eliminates a great number of inference pairs. $\dashv$

This proof of the Extended Hauptsatz uses the *permutability of inferences property* of the Gentzen systems, which has many other applications.

Theorem 3D.3 (Herbrand's Theorem)**.** *If a prenex formula*

$$\theta \equiv (Q_1 x_1) \cdots (Q_n x_n) \phi(x_1, \ldots, x_n)$$

is provable in $\mathbb{FOL}$ *without the Axioms of Identity* (15) – (17) *, then there exists a quantifier free tautology of the form*

$$\phi^* \equiv \phi_1 \vee \cdots \vee \phi_n$$

such that:

(1) *Each* ϕ_i *is a substitution instance of the matrix* $\phi(x_1, \ldots, x_n)$ *of* θ*, and*
(2) θ *can be proved from* ϕ^* *by the use of the following four Herbrand rules of inferences which apply to disjunctions of formulas:*

$$\frac{\psi_1(t) \vee \cdots \vee \psi_n}{\exists x \psi(x) \vee \cdots \chi \cdots \vee \psi_n}\ (\exists) \qquad \frac{\psi_1 \vee \cdots \chi_1 \vee \chi_2 \cdots \vee \psi_n}{\psi \vee \cdots \chi_2 \vee \chi_1 \cdots \vee \psi_n}\ (I)$$

$$\frac{\psi_1 \vee \cdots \chi \vee \chi \vee \psi_n}{\psi_1 \vee \cdots \chi \cdots \vee \psi_n}\ (C) \qquad \frac{\psi_1(v) \vee \cdots \vee \psi_n}{\forall x \psi(x) \vee \cdots \vee \psi_n}\ (\forall)\ (\textbf{Restr})$$

(**Restr**)**:** *The variable* v *does not occur free in the conclusion.*

3D.4. Remarks. The Herbrand rules obviously correspond to the Gentzen quantifier rules and Contraction, together with the Interchange rule which we do not need for multiset sequents; and the restriction on the $\forall$-rule is the same, the variable v must not be free in the conclusion. A provable disjunction which satisfies the conclusion of the theorem is called a *Herbrand expansion* of θ; by extension, we often refer to the midsequent of a Gentzen normal proof as a Herbrand expansion of the endsequent.

There is an obvious version of the theorem for implications of the form

$$\theta_1 \to \theta_2$$

with both θ_1, θ_2 prenex.

Problems for Section 3D

Problem 3D.1. Suppose Π is a Cut-free proof in $\mathbf{G}$ with endsequent $A \Rightarrow B$, in which there are no applications of the (four) logical rules that involve the symbols $\neg$ and $\to$. Prove that every formula ϕ which occurs on the left of some sequent in Π is a subformula of some formula in A; and every formula ψ which occurs on the right of some sequent in Π is a subformula of some formula in B.

3E. The propositional Gentzen systems

The Semantic Completeness Theorem 3A.10 combined with the Hauptsatz imply easily the following result, where *propositional tautologies* were defined in the brief Section 1K.1.

Theorem 3E.1 (Completeness of $\mathbf{G}_{\text{prop}}$)**.** *A propositional formula ϕ is a tautology if and only if there is a Cut-free proof in $\mathbf{G}_{\text{prop}}$ of the sequent $\Rightarrow \phi$.*

This, however, is an unnecessarily complex proof: we should not need either the Completeness Theorem for $\mathbb{FOL}$ or the full Hauptsatz to establish a basically simple fact. We outline here a more direct proof of this result, and we incidentally collect some basic facts about the Propositional Calculus which we have (somehow) avoided to discuss before now.

3E.2. Truth tables. Suppose ϕ is a propositional formula with n distinct propositional variables. There are 2^n n-tuples of 0's and 1's, and so the truth values of ϕ under all possible assignments of truth values to its variables can be pictured in a table with n columns and 2^n lines (rows), one for each assignment of truth values to the variables. For example, in the case of the formula $\phi \equiv$

$\neg p$ & q which has two variables (and including a column for the subformula $\neg p$ which is used in the computation):

p	q	$\neg p$	$\neg p$ & q
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	0

Consider also the following truth table, which specifies succinctly the *truth-value* (or *bit*) *function* which is defined by the primitive, propositional connectives:

p	q	$\neg p$	p & q	$p \vee q$	$p \to q$
0	0	1	0	0	1
0	1	1	0	1	1
1	0	0	0	1	0
1	1	0	1	1	1

A propositional formula ϕ is a tautology if it only has 1s in the column of its truth table which catalogues its value.

OUTLINE OF KALMAR'S PROOF OF THEOREM 3E.1. Fix a list of distinct propositional variables $p_1, \ldots, p_n$, and for each assignment π, let

$$\pi p_i \equiv \begin{cases} p_i, & \text{if } \pi(p_i) = 1, \\ \neg p_i, & \text{if } \pi(p_i) = 0. \end{cases}$$

Set

$$\text{Line}_\pi(\vec{p}) = \text{Line}_\pi \equiv \pi p_1, \pi p_1, \ldots, \pi p_n. \tag{69}$$

As a multiset, Line_π expresses formally the hypotheses on the propositional variables in the line corresponding to π in the truth table of any formula in which only the letters $p_1, \ldots, p_n$ occur.

Step 1. If only the letters $p_1, \ldots, p_n$ occur in ϕ, then for every π,

$$\text{if value}(\phi, \pi) = 1, \text{ then } \mathbf{G}_{\text{prop}} \vdash \text{Line}_\pi \Rightarrow \phi,$$
$$\text{if value}(\phi, \pi) = 0, \text{ then } \mathbf{G}_{\text{prop}} \vdash \text{Line}_\pi \Rightarrow \neg\phi.$$

This is proved by an induction on ϕ which is routine, but necessarily messy, since it must use every inference rule of $\mathbf{G}_{\text{prop}}$.

For each assignment π to $p_1, \ldots, p_n$ and each $i \leq n$, let

$$L_i(\pi) = \pi p_{i+1}, \pi p_{i+2}, \ldots, \pi p_n,$$

so that

$$L_0(\pi) \equiv \text{Line}(\pi), \quad L_n(\pi) = \emptyset,$$
$$\text{and for every } i < n, L_i(\pi) \equiv \pi p_i, L_{i+1}(\pi).$$

Step 2. If only the letters $p_1, \ldots, p_n$ occur in ϕ and ϕ is a propositional tautology, then for every $i \leq n$ and for every assignment π,

$$L_i(\pi) \Rightarrow \phi$$

is provable in $\mathbf{G}_{\text{prop}}$.

This is proved by induction on $i \leq n$, simultaneously for all assignments, and the Basis Case is Step 1, while the last Case $i = n$ gives the required result. For the inductive step, the Induction Hypothesis applied to the two assignments

$$\pi\{p_i := 1\}, \quad \pi\{p_i := 0\}$$

gives us proofs of

$$p_i, L_{i+1}(\pi) \Rightarrow \phi \text{ and } \neg p_i, L_{i+1}(\pi) \Rightarrow \phi,$$

since ϕ is a tautology; and from these two proofs we easily get a proof of $L_{i+1}(\pi) \Rightarrow \phi$ in $\mathbf{G}_{\text{prop}}$, which uses a Cut. The proof is completed by appealing to the propositional case of the Hauptsatz 3C.1. ⊣

Proposition 3E.3. *For every valid, quantifier-free τ-formula ϕ with n, distinct prime subformulas $\phi_1, \ldots, \phi_n$ and no occurrence of the identity symbol $=$, there is a propositional tautology ψ with n distinct propositional variables such that*

$$\phi \equiv \psi\{p_1 :\equiv \phi_1, \ldots, p_n :\equiv \phi_n\}.$$

Problems for Section 3E

Problem 3E.1. Prove each of the following sequents in **G**, if possible in **GI**.

1. $\neg(\phi \ \& \ \psi) \Rightarrow \neg\phi \vee \neg\psi$.
2. $\neg\phi \vee \neg\psi \Rightarrow \neg(\phi \ \& \ \psi)$.
3. $\Rightarrow \phi \vee \neg\phi$.
4. $\neg\neg\neg\phi \Rightarrow \neg\phi$.

Problem 3E.2. Prove each of the following sequents in **G**, if possible in **GI**.

1. $\exists x R(x) \Rightarrow \neg\forall x \neg R(x)$.
2. $\neg\forall x \neg R(x) \Rightarrow \exists x R(x)$.

3. $\neg\exists x\forall y)R(x,y) \Rightarrow \forall x\exists y\neg R(x,y)$.
4. $\neg\exists x\forall y)R(x,y) \Rightarrow \forall x\neg\forall y)R(x,y)$.

Problem 3E.3. Assume the Cut Elimination Theorem for *gentzeni* and prove that

$$\text{if } \mathbf{GI} \vdash \Rightarrow \phi \vee \psi, \text{ then } \mathbf{GI} \vdash \Rightarrow \phi \text{ or } \mathbf{GI} \vdash \Rightarrow \psi.$$

Problem 3E.4. Prove that the sequent in Problem 3C.4 does not have a Cut-free proof in **G**.

Problem 3E.5. Assume the Cut Elimination Theorem for **GI** and prove that the sequent

$$\neg\neg R(x) \Rightarrow R(x)$$

in not provable in the intuitionistic system **GI**.

Problem 3E.6. Assume the Cut Elimination Theorem for **GI** and prove all the assertions of unprovability in **GI** that you made in Problems 3E.1 and 3E.2.

Problem 3E.7. Prove Proposition 3E.3—that every valid, quantifier-free formula can be obtained by replacing each propositional variable in some tautology by a quantifier-free formula.

Problem 3E.8. Suppose $R(i,j)$ is a relation defined for $i,j \leq n$, choose a double sequence of propositional variables $\{p_{ij}\}_{i,j\leq n}$, and consider the assignment

$$\pi(p_{ij}) = \begin{cases} 1, & \text{if } R(i,j), \\ 0, & \text{otherwise.} \end{cases}$$

The variables $\{p_{ij}\}$ can be used to express various properties about the relation R, for example

$$R \text{ is symmetric} \iff \pi \models \bigwedge\!\!\!\bigwedge_{i,j\leq n} [p_{ij} \leftrightarrow p_{ji}].$$

Find similar formulas which express the following properties of R:

(a) R is the graph of a function.
(b) R is the graph of a one-to-one function.
(c) R is the graph of a surjection—a function from $\{0,\ldots,n\}$ onto $\{0,\ldots,n\}$.

3F. Craig Interpolation and Beth definability (via proofs)

The midsequent of a normal proof in **G** is a valid, quantifier-free formula, and so (by Proposition 3E.3), it can be obtained from a propositional tautology by replacing the propositional variables by prime formulas. This fact can be used to derive several interesting results about $\mathbb{FOL}$ from their propositional versions, which are generally much easier to establish. We illustrate the process here with two, basic results about first order definability.

Theorem 3F.1 (The Propositional Interpolation Theorem)**.** *Suppose*

$$\phi(\vec{p},\vec{q}) \to \psi(\vec{p},\vec{r})$$

is a propositional tautology, where we have indicated all the (distinct) letters which may occur in the formulas, and there is at least one p_i; then there exists a formula $\chi(\vec{p})$ in which none of the q's or r's occur, such that

$$\phi(\vec{p},\vec{q}) \to \chi(\vec{p}), \quad \chi(\vec{p}) \to \psi(\vec{p},\vec{r})$$

are both tautologies.

For an example: if the given tautology is

$$p \ \& \ q \to p \vee r,$$

we can take $\chi \equiv p$, with which both $p \ \& \ q \to p$ and $p \to p \vee r$ are tautologies. In fact this is the interpolant which will come out of the general proof in this case.

Outline of proof. If no assignment π satisfies ϕ, we can then take

$$\chi(\vec{p}) \equiv p_i \ \& \ \neg p_i$$

with the assumed p_i which occurs in both ϕ and ψ. So we may assume that at least one assignment satisfies ϕ.

Generalizing the definition of lines in (70) and making explicit the implied conjunction, we set for each assignment π,

$$L(\pi,\vec{p}) \equiv \bigwedge\!\!\bigwedge \mathrm{Line}_\pi(\vec{p}) \equiv \pi p_1 \ \& \ \pi p_2 \ \& \ \cdots \ \& \ \pi p_n.$$

Notice that, immediately from the definition,

$$\mathrm{value}(L(\pi,\vec{p}),\pi) = 1.$$

We now take $\chi(\vec{p})$ to be the disjunction of these conjunctions over all assignments π which satisfy ϕ:

$$\chi(\vec{p}) \equiv \bigvee\!\!\bigvee \{L(\pi,\vec{p}) \mid \mathrm{value}(\phi,\pi) = 1\}.$$

Clearly, $\phi \to \chi(\vec{p})$ is a tautology, because if $\text{value}(\pi, \phi) = 1$, then $L(\pi, \vec{p})$ is one of the disjuncts of $\chi(\vec{p})$ and π satisfies it. For the second claim, suppose towards a contradiction that there is a π such that

$$\text{value}(\chi(\vec{p}), \pi) = 1, \quad \text{and} \quad \text{value}(\psi, \pi) = 0;$$

now the definition of $\chi(\vec{p})$ implies that $\text{value}(\phi, \pi) = 1$, and so $\text{value}(\psi, \pi) = 1$ by the hypothesis, which is a contradiction. ⊣

Theorem 3F.2 (The Craig Interpolation Theorem)**.** *Suppose*

$$\phi(\vec{Q}) \to \psi(\vec{R}) \tag{70}$$

is valid, where the formulas $\phi(\vec{Q})$ and $\psi(\vec{R})$ may have symbols from some signature τ in addition to the (fresh, distinct) symbols exhibited. From a proof of (71)*, we can construct a formula χ in $\mathbb{FOL}(\tau)$ and proofs of the implications*

$$\phi(\vec{Q}) \to \chi, \quad \chi \to \psi(\vec{R}).$$

Outline of the proof. The argument involves some unavoidable detail, primarily to deal with the identity symbol $=$ about which the Gentzen system knows nothing.

We start with the construction of prenex formulas $\phi'(\vec{Q})$ and $\psi'(\vec{R})$ such that the equivalences

$$\phi(\vec{Q}) \leftrightarrow \phi'(\vec{Q}), \quad \psi(\vec{R}) \leftrightarrow \psi'(\vec{R})$$

are valid and no variable occurs both free and bound in the (assumed valid) implication

$$\phi'(\vec{Q}) \to \psi'(\vec{R}).$$

By Theorem 3A.10 (the Semantic Completeness of **G**),

$$\mathbf{G} \vdash \text{IA}(\tau), \text{IA}(\vec{Q}), \text{IA}(\vec{R}) \Rightarrow \phi'(\vec{Q}) \to \psi'(\vec{R}),$$

where $\text{IA}(\tau), \text{IA}(\vec{Q}), \text{IA}(\vec{R})$ are the identity axioms for the relation and function symbols which occur in τ, $\phi'(\vec{Q})$ and $\psi'(\vec{R})$ (in prenex form); and then, easily,

$$\mathbf{G} \vdash \text{IA}(\tau), \text{IA}(\vec{Q}), \phi'(\vec{Q}) \Rightarrow (\text{IA}(\vec{R}) \to \psi'(\vec{R})). \tag{71}$$

We now replace the identity symbol $=$ by a fresh, binary relation symbol E, i.e., we replace each prime formula of the form $t = s$ by $E(t, s)$, to obtain formulas

$$\text{IA}(E, \tau), \text{IA}(E, \vec{Q}), \phi'(E, \vec{Q}), \text{IA}(E, \vec{R}), \psi'(E, \vec{R});$$

and since the proof in **G** which establishes (72) does not use any special properties of the identity symbol, if we replace $=$ by E in it, we get

$$\mathbf{G} \vdash \mathrm{IA}(E,\tau), \mathrm{IA}(E,\vec{Q}), \phi'(E,\vec{Q}) \Rightarrow (\mathrm{IA}(E,\vec{R}) \to \psi'(E,\vec{R})).$$

We now apply the Extended Hauptsatz to get a normal proof Π of this sequent. The midsequent

$$A^* \Rightarrow B^*$$

of Π is a valid, quantifier-free sequent with no occurrence of $=$, and so (easily, by Proposition 3E.3), there is a valid propositional sequent

$$A^{**} \Rightarrow B^{**}$$

from which $A^* \Rightarrow B^*$ can be obtained by replacing its propositional variables with prime formulas. Moreover, prime formulas which involve symbols in $\vec{Q}$ occur only in A^{**}, and prime formulas which involve symbols in $\vec{Q}$ occur only in B^{**}, and so by the Propositional Interpolation Theorem 3F.1, there is a (τ, E)-formula χ^{**} such that

$$\mathbf{G} \vdash A^{**} \Rightarrow \chi^{**}; \qquad \mathbf{G} \vdash \chi^{**} \Rightarrow B^{**}.$$

If we now replace back E by $=$, we get a τ-formula χ^* such that

$$\mathbf{G} \vdash A^* \Rightarrow \chi^*, \qquad \mathbf{G} \vdash \chi^* \Rightarrow B^*. \tag{72}$$

This completes the preparation or the proof. In the main argument, *we apply to each of these two sequents* (essentially) *the same sequence of quantifier rule applications and contractions which are used to get* $\mathrm{IA}(E,\vec{Q}), \phi'(E,\vec{Q}) \Rightarrow (\mathrm{IA}(E,\vec{R}) \to \psi'(E,\vec{R}))$ from $A^* \Rightarrow B^*$, to obtain in the end a new τ-formula χ and and proofs of the required

$$\mathbf{G} \vdash \mathrm{IA}(\tau), \mathrm{IA}(\vec{Q}) \;\&\; \phi(\vec{Q}) \Rightarrow \chi, \quad \mathbf{G} \vdash \chi \Rightarrow (\mathrm{IA}(\vec{R}) \to \psi(\vec{R})). \qquad \dashv$$

Theorem 3F.3 (The Beth Definability Theorem)**.** *Suppose $\phi(R)$ is a sentence in $\mathbb{FOL}(\tau \cup \{R\})$, where the n-ary relation symbol R is not in the signature τ, and the sentence*

$$\phi(R) \;\&\; \phi(S) \to (\forall \vec{x})[R(\vec{x}) \leftrightarrow S(\vec{x})]$$

is provable (or equivalently valid). From any proof of it we can construct a $\chi(\vec{x})$ in $\mathbb{FOL}(\tau)$ such that

$$\phi(R) \to (\forall \vec{x})[R(\vec{x}) \leftrightarrow \chi(\vec{x})]$$

is provable.

The Beth Theorem says that *implicit first order definability* coincides with *explicit first order definability*. In addition to their obvious foundational significance, both of these results are among the most basic of Model Theory, with many applications.

3G. The Hilbert program

The discovery of paradoxes in set theory (especially the Russell Paradox) in the beginning of the 20th century created a "foundational crisis" in mathematics which was not completely resolved until the middle 1930s. There were essentially three main responses to it:

(1) *Axiomatic set theory*. Introduced by Zermelo in 1908 in direct response to the paradoxes, this led rapidly to substantial mathematical developments, and eventually to a new notion of *grounded set* which replaced Cantor's intuitive approach and, in a sense, "justified the axioms": in any case, no contradictions have been discovered in *Zermelo-Fraenkel set theory* since its formalization was complete in the 1930s. Working "within ZFC" is now the standard, "mathematical" approach to the foundations of mathematics.

(2) *Constructive mathematics* (intuitionism), advocated primarily by Brouwer. This rejected set theory and classical logic as "meaningless", and attempted to reconstruct a new kind of mathematics on constructive principles. It did not succeed in replacing classical mathematics as the language of science, but it has influenced deeply the philosophy of mathematics.

(3) *Formalism*, introduced by Hilbert, who formulated the *Hilbert program*, a sequence of mathematical conjectures whose proof would solve the problem posed by the paradoxes. The basic elements of the Hilbert Program (vastly oversimplified) are as follows:

Step 1. Formulate mathematics (or a substantial part of it) as a *formal, axiomatic theory* T, so it can be studied as a mathematical object using standard, combinatorial techniques.

Our modern conception of formal, first-order logic, with its precisely defined terms, formulas, proofs, etc., was developed as part of this first step of the Hilbert Program—it had never been so rigorously formulated before.

Step 2. Prove that T is *complete*: i.e., for each sentence θ of T,

$$\text{either } T \vdash \theta \quad \text{or} \quad T \vdash \neg\theta.$$

Step 3. Prove that T is consistent, i.e., there is not sentence θ such that

$$T \vdash \theta \text{ and } T \vdash \neg\theta.$$

Basic methodological principle: the proofs in the last two steps must be *finitistic*, i.e., (roughly) constructive, utterly convincing combinatorial arguments about finite objects, such as natural numbers, symbols, strings of symbols and the like. There is no attempt to define rigorously the pre-mathematical notion of *finitistic proof*: it is assumed that we can recognize a finitistic argument—and be convinced by it—when we see it.

The basic idea is that if Steps 1 – 3 can be achieved, then *truth* can be replaced in mathematics by *proof*, so that metaphysical questions (like *what is a set*) are simply by-passed.

Hilbert and his school worked on this program as mathematicians do, trying first to complete it for weak theories T and hoping to develop methods of proof which would eventually apply to number theory, analysis and even set theory. They had some success, and we will examine two representative results in Sections 3H and 3J. But Gödel's fundamental discoveries in the 1930s established conclusively that the Hilbert Program cannot go too far. They will be our main concern.

It should be emphasized that the notions and methods introduced as part of the Hilbert Program have had an extremely important role in the development of modern, mathematical logic, and even Gödel's work depends on them: in fact, Gödel proved his fundamental results in response to questions which arose (explicitly or implicitly) in the Hilbert Program.

3H. The finitistic consistency of Robinson's Q

Robinson's Q was defined in 2G.1. We introduce its *Skolemized version* Q_s, which has an additional (unary) function symbol Pd and for axioms (in full) the universal closures of the following formulas:

1. $\neg[S(x) = 0]$.
2. $S(x) = S(y) \to x = y$.
3. $x + 0 = x,\ x + S(y) = S(x + y)$.
4. $x \cdot 0 = 0,\ x \cdot (Sy) = x \cdot y + x$.
5. $\mathrm{Pd}(0) = 0$.
6. $\mathrm{Pd}(S(x)) = x$.
7. $x = 0 \vee x = S(\mathrm{Pd}(x))$.
8. $x = x\ \&\ (x = y \to y = x)\ \&\ [(x = y\ \&\ y = z) \to x = z]$.

9. $x = y \to [S(x) = S(y)\ \&\ \mathrm{Pd}(x) = \mathrm{Pd}(y)]$.
10. $(x = y\ \&\ u = v) \to [x + u = y + v\ \&\ x \cdot u = y \cdot v$.

Aside from the explicit inclusion of the relevant Axioms of Identity, the basic difference between Q and Q_s is that all the axioms of Q_s are universal sentences, while the characteristic axiom

$$\forall x[x = 0 \vee (\exists y)[x = S(y)]]$$

of Q has an existential quantifier in it. Axiom 7 of Q_s is the "Skolemized version" of the Robinson axiom; in this case we can obviously see that the "Skolem function" $\mathrm{Pd}(x)$ is the predecessor function

$$\mathrm{Pd}(x) = \begin{cases} 0, & \text{if } x = 0, \\ x - 1, & \text{otherwise.} \end{cases} \tag{73}$$

However, this *Skolemization* which eliminates existential quantifiers by introducing new function symbols can be done in arbitrary sentences, and in each case we can prove the analog of the following, simple fact:

Lemma 3H.1. *We can prove in* $\mathbf{G}$ *the sequent*

$$\forall x[x = 0 \vee x = S(\mathrm{Pd}((x)))] \Rightarrow \forall x[x = 0 \vee (\exists y)[x = S(y)]],$$

and so for any sentence θ*,*

$$\textit{if } \mathbf{G} \vdash \mathsf{Q} \Rightarrow \theta, \textit{ then } \mathbf{G} \vdash \mathsf{Q}_s \Rightarrow \theta.$$

It follows that if Q_s *is consistent, then so is* Q*.*

Theorem 3H.2. *Robinson's theory* Q *is* (finitistically) *consistent.*

OUTLINE OF PROOF. We assume, towards a contradiction that (with $1 = S(0)$), $\mathsf{Q}_s \vdash 0 = 1$, so that there is a proof in $\mathbf{G}$ of the sequent

$$\mathsf{Q}_s \Rightarrow 0 = 1;$$

and since all the axioms on Q_s are prenex, by the Extended Hauptsatz, there is a normal proof of this sequent. Consider the midsequent of such a normal proof: it is of the form

$$\theta_1, \dots, \theta_n \Rightarrow 0 = 1$$

where each θ_i is a substitution instance of the *matrix* of one of the axioms of Q_s, something like

$$Sx + S(u \cdot Sx) = S(Sx + (u \cdot Sx))$$

in the case of Axiom 3. Now *replace by* 0 *all the (free) variables which occur in the part of the proof above the midsequent*, so that in the example the midsequent becomes the equation

$$S0 + S(0 \cdot S0) = S(S0 + (0 \cdot S0)).$$

The (propositional) proof above the midsequent remains a proof, and it establishes the sequent

$$\theta_1^*, \ldots, \theta_n^* \Rightarrow 0 = 1$$

where each θ_i^* is a *numerical identity*. But these numerical identities are all true with the standard interpretation of the symbols $0, S, +, \mathrm{Pd}, \cdot$; and so we cannot have a proof by logic alone which leads from them to the obviously false identity $0 = 1$. ⊣

DISCUSSION: In some sense, all we have done is to say that we have a model of Q_s, and hence the theory must be consistent. The "finitistic" justification for the proof is that (1), the model is *constructive*—its universe is the set $\mathbb{N}$ of natural numbers, we can compute all the values of the functions $S, \mathrm{Pd}, +, \cdot$ involved, and we can verify numerical equations among them; and (2), we only need to understand and accept finitely many numerical instances of universal sentences, which we can verify "by hand". In other words, all we need to believe about the natural numbers is that we can define $Sx, \mathrm{Pd}(x), x+y$ and $x \cdot y$ on some initial segment of $\mathbb{N}$ (comprising the specific numbers which occur in the assumed contradictory midsequent) so that their basic, numerically verifiable identities are true. The Extended Hauptsatz is used precisely to replace a general understanding of "truth in $(\mathbb{N}, 0, S, +, \cdot)$" for arbitrary sentences with quantifiers by this limited understanding of "numerical truth".

3I. Primitive recursive functions

We introduce here and establish the basic properties of the *primitive recursive* functions and relations on $\mathbb{N}$, which have numerous applications in many parts of logic.

3I.1. We will use the following specific functions on $\mathbb{N}$:

1. The successor, $S(x) = x + 1$.
2. The n-ary constants, $C_q^n(\vec{x}) = q$.
3. The projections, $P_i^n(x_1, \ldots, x_n) = x_i$, $(1 \leq i \leq n)$. Notice that $P_1^1(x) = id(x)$ is the identity.

Definition 3I.2. A function $f : \mathbb{N}^n \to \mathbb{N}$ is defined by **composition** from given functions h, $g_1, \ldots, g_m$, if for all $\vec{x} \in \mathbb{N}^n$,

$$f(\vec{x}) = h(g_1(\vec{x}), \ldots, g_m(\vec{x})).$$

Here f and all the g_i are n-ary and h is m-ary. Example:

$$f(x) = x + x = +(id(x), id(x)) = 2x$$

is a composition of addition with the identity (taken twice). The function

$$S_1^2(x, y) = S(P_1^2(x, y)) = x + 1$$

is the binary function which adds 1 to its first argument.

A function f is defined by **primitive recursion** from h, g, if for all $y, \vec{x} \in \mathbb{N}^n$,

$$f(0, \vec{x}) = g(\vec{x}),$$
$$f(y + 1, \vec{x}) = h(f(y, \vec{x}), y, \vec{x}).$$

Here f is $n+1$-ary, g is n-ary and h is $n+2$-ary. We also include (by convention) the degenerate case where g is just a number and a unary function is being defined:

$$f(0) = q,$$
$$f(y + 1) = h(f(y), y).$$

Examples: if

$$f(0, x) = id(x) = x, \quad f(y + 1, x) = S_1^2(f(y, x), y),$$

then (by an easy induction on y),

$$f(y, x) = y + x.$$

Definition 3I.3. The class of **primitive recursive functions** is the smallest set of functions (of all arities) on $\mathbb{N}$ which contains the successor S, the constants C_q^n, and the projections P_i^n, and which is closed under composition and primitive recursion.

A relation $R \subseteq \mathbb{N}^k$ is **primitive recursive** if its characteristic function is, where

$$\chi_R(\vec{x}) = \begin{cases} 1, & \text{if } R(\vec{x}), \\ 0, & \text{otherwise.} \end{cases}$$

Proposition 3I.4. (1) *If* $\mathbf{A} = (\mathbb{N}, f_0, \ldots, f_k)$ *where* $f_0, \ldots, f_k$ *are primitive recursive and* f *is* $\mathbf{A}$*-explicit, then* f *is primitive recursive.*

(2) *Primitive recursive functions and relations are arithmetical.*

PROOF is easy, using Theorems 1D.2 (the closure properties of $\mathcal{E}(\mathbf{A})$) and 1E.2. ⊣

3I.5. A **primitive recursive derivation** is a sequence of functions

$$f_0, f_1, \dots, f_k,$$

where each f_i is S, a constant C_q^n or a projection P_i^n, or is defined by composition or primitive recursion from functions before it in the sequence.

Lemma 3I.6. *A function is primitive recursive if and only of it occurs in some primitive recursive derivation.*

Lemma 3I.7. *The following functions are primitive recursive.*

1. $x + y$.
2. $x \cdot y$.
3. $x! = 1 \cdot 2 \cdot 3 \cdots x$, *with* $0! = 1$.
4. $\mathrm{pd}(x) = x - 1$, *with* $pd(0) = 0$.
5. $x \dot{-} y = \max(0, x - y)$.
6. $\min(x, y)$.
7. $\min(x_1, \dots, x_n)$.
8. $\max(x, y)$.
9. $\max(x_1, \dots, x_n)$.
10. $\max(x_1, \dots, x_n)$.
11. $\mathrm{bit}(x) = \begin{cases} 0, & \text{if } x = 0, \\ 1, & \text{if } x > 0. \end{cases}$
12. $\overline{\mathrm{bit}}(x) = 1 \dot{-} \mathrm{bit}(x)$.

Lemma 3I.8. *If h is primitive recursive, then so are f and g where:*

(1) $f(x, \vec{y}) = \sum_{i<x} h(i, \vec{y})$, $(= 0$ when $x = 0)$.

(2) $g(x, \vec{y}) = \prod_{i<x} h(i, \vec{y})$, $(= 1$ when $x = 0)$.

PROOF is left for Problem 4A.1. ⊣

Lemma 3I.9 (Closure properties of primitive recursive relations)**.** (1) *The identity relation $x = y$ is primitive recursive.*

(2) *The negation of a primitive recursive relation is primitive recursive; and the conjunction of primitive recursive relations is primitive recursive.* (So the class of primitive recursive relations is closed under all propositional logic operations.)

(3) *If $P(i, \vec{y})$ is primitive recursive, then so are the relations defined from it by bounded quantification:*

$$Q(x, \vec{y}) \iff_{\text{df}} (\exists i < x) P(i, \vec{y}),$$
$$R(x, \vec{y}) \iff_{\text{df}} (\forall i < x) P(i, \vec{y}).$$

(4) *If P and $f_1, \dots, f_k$ are primitive recursive, then so is the relation*

$$R(\vec{x}) \iff_{\text{df}} P(f_1(\vec{x}), \dots, f_k(\vec{x})).$$

(5) *If R is primitive recursive, then so is the function*

$$f(x, \vec{y}) = (\mu i < x) R(i, \vec{y});$$

here μi is read "the least i", and if there is no $i < x$ which satisfies $R(i, \vec{y})$, then $f(x, \vec{y}) = x$.

Lemma 3I.10. *The following functions and relations are primitive recursive.*

(1) $\text{quot}(x, y)$ = the (integer) quotient of x by y, *set* $= 0$ *if* $y = 0$.
(2) $\text{rem}(x, y)$ = the remainder of the division of x by y, set $= x$ if $y = 0$.
(3) $\text{Prime}(x) \iff x > 1$ & x has no divisors other than 1 and itself.
(4) $p(i) = p_i$ = the i'th prime number.

For $y > 0$, the integer quotient $q = \text{quot}(x, y)$ and remainder $r = \text{rem}(x, y)$ are the unique natural numbers which satisfy

$$x = yq + r, \quad 0 \leq r < y.$$

Next we introduce a coding of tuples from $\mathbb{N}$ which is more convenient than the one we defined using the β-function in Section 1E.

3I.11. Definition. A **coding** of a set X in the set C is any injective (one-to-one) function $\pi : X \rightarrowtail C$.

With each coding $\langle\ \rangle : \mathbb{N}^* \rightarrowtail \mathbb{N}$ of the finite sequences of numbers into the numbers, we associate the following functions and relations:

1. $\langle x_1, \dots, x_n \rangle_n = \langle x_1, \dots, x_n \rangle$, the n-ary function (for each fixed n) which codes n-tuples, for very n including $n = 0$: so $\langle \epsilon \rangle$ is some fixed number, the code of the empty tuple. (In using this notation, we never write the n.)
2. $\text{Seq}(w) \iff_{\text{df}} (\exists x_0, \dots, x_{n-1})[w = \langle x_0, \dots, x_{n-1} \rangle]$, the *sequence coding relation.*
3. $\text{lh}(w) = n$, if $w = \langle x_0, \dots, x_{n-1} \rangle$, the *length function* (=0 if w is not a sequence number).
4. $\text{proj}(w, i) = (w)_i = x_i$, if $w = \langle x_0, \dots, x_{n-1} \rangle$ and $i < n$, the *projection function* (=0 if w is not a sequence number or $i \geq \text{lh}(w)$).

5. $\text{append}(u,t) = \langle x_0,\dots,x_{n-1},t\rangle$ if $u = \langle x_0,\dots,x_{n-1}\rangle$, $= 0$ otherwise.

A sequence coding on the set $\mathbb{N}$ of numbers is **primitive recursive** if these associated functions and relations are all primitive recursive.

The *restriction* of a sequence code u to its first i elements is defined by the primitive recursion

$$u\restriction 0 = \langle\epsilon\rangle, \quad u\restriction(i+1) = \text{append}(u\restriction i, (u)_i), \tag{74}$$

so that

$$\langle u_0,\dots,u_{n-1}\rangle\restriction i = \langle u_o,\dots,u_{i-1}\rangle \quad (i<n).$$

Using the appending function, we can also define by primitive recursion the *concatenation* of codes of sequences, setting

$$\begin{aligned} f(0,u,v) &= u,\\ f(i+1,u,v) &= \text{append}(f(i,u,v),(v)_i),\\ u*v &= f(\text{lh}(v),u,v). \end{aligned} \tag{75}$$

It follows easily that when u,v are sequence codes, then $u*v$ codes their concatenation.

Lemma 3I.12. *The following function on $\mathbb{N}^*$ is a primitive recursive coding:*

$$\begin{aligned} \langle\epsilon\rangle &= 1 \quad \text{(the code of the empty tuple is 1)}\\ \langle x_0,\dots,x_n\rangle &= p_0^{x_0+1}\cdot p_1^{x_1+1}\cdots p_n^{x_n+1} \quad (n\geq 0). \end{aligned}$$

It satisfies the following additional properties for all $x_0,\dots,x_{n-1}$ and all sequence codes u,v,w:

$$\begin{aligned} x_i &< \langle x_0,\dots,x_{n-1}\rangle, \quad (i<n),\\ &\text{if } v,u*w\neq 1, \text{ then } v<u*v*w. \end{aligned}$$

This is the *standard* or *prime power coding* of tuples from $\mathbb{N}$.

Lemma 3I.13 (Complete Primitive Recursion)**.** *Suppose g is primitive recursive, $\langle\ \rangle$ is a primitive recursive coding of tuples and the function f satisfies the identity*

$$f(x) = g(x,\langle f(0),\dots,f(x-1)\rangle);$$

it follows that f is primitive recursive.

Similarly with parameters, when

$$f(x,\vec{y}) = g(x,\vec{y},\langle f(0,\vec{y}),\dots,f(x-1,\vec{y})\rangle).$$

Proof. The function

$$\overline{f}(x) = \langle f(0), \dots, f(x-1)\rangle$$

satisfies the identities

$$\begin{aligned}\overline{f}(0) &= \langle\epsilon\rangle,\\ \overline{f}(x+1) &= \overline{f}(x) * \langle g(x, \overline{f}(x))\rangle,\end{aligned}$$

so that it is primitive recursive; and then

$$f(x) = (\overline{f}(x+1))_x. \qquad \dashv$$

Lemma 3I.14. *If $\langle\ \rangle_1$ and $\langle\ \rangle_2$ are primitive recursive number codings of tuples, then there exists a primitive recursive function $\pi : \mathbb{N} \to \mathbb{N}$ which computes one coding from the other, i.e. for all sequences,*

$$\pi(\langle x_0, \dots, x_{n-1}\rangle_1) = \langle x_0, \dots, x_{n-1}\rangle_2.$$

This result often allows us to establish results about the simple, standard, power coding of Lemma 3I.12 and then infer that they hold for all primitive recursive codings. The standard coding is very inefficient, and much better primitive recursive codings exist, cf. Problems 4A.6 – 4A.9; but we are not concerned with efficiency here, and so, to simplify matters, **we adopt the standard power coding of tuples** for these notes, so that we may use without mention its special properties listed in Lemma 3I.12.

3J. Further consistency proofs

We outline here the proof of (basically) the strongest consistency result which can be shown finitistically.

Definition 3J.1 (Primitive Recursive Arithmetic, I)**.** For each primitive recursive derivation

$$\vec{f} = (f_0, \dots, f_k),$$

we define a formal axiomatic system $\mathrm{PRA}(\vec{f})$ as follows.

(1) The signature of $\mathrm{PRA}(\vec{f})$ has the constant 0, the successor symbol S, the predecessor symbol Pd, function symbols for $f_1, \dots, f_k$ and the identity symbol $=$. (This is an $\mathbb{FOL}$ theory.) We assume the identity axioms for the function symbols in the signature, the two axioms for the successor,

$$S(x) \neq 0, \quad S(x) = S(y) \to x = y,$$

and the three axioms for the predecessor:

$$\mathrm{Pd}(0) = 0, \quad \mathrm{Pd}(S(x)) = x, \quad x \neq 0 \vee x = S(\mathrm{Pd}(x)).$$

(2) For each f_i we have its *defining equations* which come from the derivation as axioms. For example, if $f_3 = C_2^3$, then the corresponding axiom is

$$f_3(x, y, z) = S(S(0)).$$

If f_i is defined by primitive recursion from preceding functions f_l, f_m, we have the corresponding axioms

$$f_i(0, \vec{x}) = f_l(\vec{x}),$$
$$f_i(S(y), \vec{x}) = f_m(f_i(y, \vec{x}), y, \vec{x}).$$

(3) *Quantifier free induction scheme.* For each quantifier free formula $\phi(y, \vec{z})$ we take as axiom the universal closure of the formula

$$\phi(0, \vec{z}) \ \& \ (\forall y)[\phi(y, \vec{z}) \to \phi(S(y), \vec{z})] \ \to \ \forall x \phi(x, \vec{z}).$$

Notice that from the axiom

$$x = 0 \vee x = S(\mathrm{Pd}(x))$$

relating the successor and the predecessor functions, we can get immediately (by $\exists$-elimination) the Robinson axiom

$$x = 0 \vee (\exists y)[x = S(y)],$$

so that all the axioms of the Robinson system Q defined in **3.10** are provable in $\mathrm{PRA}(\vec{f})$, once the primitive recursive derivation $\vec{f}$ includes the defining equations for addition and multiplication.

The term **primitive recursive arithmetic** is used loosely for the "union" of all such $\mathrm{PRA}(\vec{f})$. More precisely, we say that a proposition can be *expressed and proved* in primitive recursive arithmetic, if it can be formalized and proved in some $\mathrm{PRA}(\vec{f})$.

Definition 3J.2 (Primitive Recursive Arithmetic, II)**.** For each primitive recursive derivation $\vec{f}$, let $\mathrm{PRA}^*(\vec{f})$ be the axiomatic system with the same signature as $\mathrm{PRA}(\vec{f})$ and with axioms (1) and (2) above, together with

(3)* For each of the function symbols h in the signature,

$$\{h(0, \vec{z}) = 0 \ \& \ (\forall y)[h(S(y), \vec{z}) = S(h(y, \vec{z}))]\} \to (\forall x)[h(x, \vec{z}) = x]. \tag{76}$$

Theorem 3J.3 (Key Lemma)**.** *For each primitive recursive derivation $\vec{f}$, the system* $\mathrm{PRA}^*(\vec{f})$ *is* (finitistically) *consistent.*

PROOF. First we replace the new axiom (77), for each function symbol h by its "Skolemized form"

$$(77)\quad (\forall x)\Big[\,\{h(0,\vec{z})=0\ \&\ [h(S(g_h(x,\vec{z})),\vec{z})=S(h(g_h(x,\vec{z}),\vec{z})]\}\\ \to h(x,\vec{z})=x\Big],$$

where g_h is a new function symbol. This axiom easily implies (77), by $\exists$-elimination: so it is enough to show that this system $\mathrm{PRA}^{**}(\vec{f})$ is consistent.

If the system $\mathrm{PRA}^{**}(\vec{f})$ is inconsistent, then it proves $0=1$, so by the Extended Hauptsatz we have a normal proof with endsequent

$$\phi_1,\dots,\phi_n \Rightarrow 0=1,$$

where each ϕ_i is either one of the basic axioms about the successor S and the predecessor Pd, a (universally quantified) defining equation for one of the primitive recursive functions in $\vec{f}$, or (78) for some $h=f_i$. The midsequent of this proof is of the form

$$\psi_1,\dots,\psi_m \Rightarrow 0=1,$$

where now each ψ_i is a (quantifier free) substitution instance of the matrix of some ϕ_j. *We now replace all variables above the midsequent by* 0; what we get is a propositional proof whose conclusion

$$\psi_1^*,\dots,\psi_m^* \Rightarrow 0=1$$

has on the left a sequence of closed, quantifier free sentences, each of them making a numerical assertion about S, Pd, the primitive recursive functions f_i and the (still unspecified) functions g_h. If we define

$$g_h(x,\vec{z})=\max\{y\le x \mid h(y,\vec{z})=y\},$$

then we can recognize immediately that for any x,

$$h(x,\vec{z})\neq x \Longrightarrow h(g_h(x,\vec{z}))\neq g_h(x,\vec{z}),$$

and from this it is immediate that all these numerical assertions in the midsequent are true: for example, a typical sentence in the left of the midsequent might be

$$f_2(f_5(S(0)),S(0)=f_1(S(0),0),$$

which can be verified by computing the numerical values of the functions involved from their (primitive recursive) definitions and then just checking. On the other hand, the right of the midsequent has the single false assertion $0=1$, which is absurd. ⊣

REMARK: In effect all we have done is to say that we have a model for $\mathrm{PRA}^{**}(\vec{f})$, and hence the theory must be consistent. The "finitistic" justification for the proof is that (1), the model is constructive—we can compute all the values of the functions involved, and we can verify numerical equations among them; and (2), we only need understand the truth of closed (numerical) quantifier free sentences about the model, not arbitrary sentences with quantifiers. The Extended Hauptsatz is used precisely to allow us to deal with quantifier free sentences rather than arbitrary ones.

Lemma 3J.4. *For each primitive recursive derivation $\vec{f}$ and each quantifier free formula $\phi(x, \vec{z})$ in its language, we can find a longer derivation $\vec{f}, h, \vec{g}$ such that the theory $T = \mathrm{PRA}^*(\vec{f}, h, \vec{g})$ proves the instance of quantifier free induction*

$$\phi(0, \vec{z}) \ \& \ (\forall y)[\phi(y, \vec{z}) \to \phi(S(y), \vec{z})] \to (\forall x)\phi(x, \vec{z}).$$

OUTLINE OF PROOF. We skip the parameters $\vec{z}$.

Consider again the Skolemized version of the given instance of quantifier free induction

$$\phi(0) \ \& \ [\phi(h(x)) \to \phi(S(h(x)))] \to \phi(x) \tag{78}$$

which implies easily the non-Skolemized form; so it suffices to find a primitive recursive derivation with a letter h in it so that the theory T proves (79). The idea is to take the function h defined by the following primitive recursion.

$$h(0) = 0,$$
$$h(S(y)) = \begin{cases} S(h(y)), & \text{if } \phi(h(y)) \ \& \ \phi(S(h(y))), \\ h(y), & \text{if } \phi(h(y)) \ \& \ \neg\phi(S(h(y))), \\ 0, & \text{if } \neg\phi(h(y)). \end{cases}$$

We omit the details of the proof that this h is primitive recursive, and that in the theory T which includes its primitive recursive derivation we can establish the following theorems, which express the cases in its definition.

$$\phi(h(y)) \ \& \ \phi(S(h(y))) \to h(S(y)) = S(h(y)), \tag{79}$$

$$\phi(h(y)) \ \& \ \neg\phi(S(h(y))) \to S(h(y)) = h(y), \tag{80}$$

$$\neg\phi(h(y)) \to h(S(y)) = 0. \tag{81}$$

Once we have these theorems from T, we assume the hypothesis

$$\phi(0), \phi(h(x)) \to \phi(S(h(x))) \tag{82}$$

of the implication to prove and we argue as follows, within T.

(1) $(\forall x)\phi(h(x))$. By Robinson's property, either $x = 0$, and then $h(0) = 0$ and $\phi(0)$ give the result, of $x = S(y)$ for some y, and then we can verify the conclusion taking cases in the hypothesis of (80) - (82).

(2) $(\forall y)[h(S(y)) = S(h(y))]$. This follows now from (80) – (82), since (82) cannot occur by (1) and (81) cannot occur by the hypothesis (83).

(3) $(\forall x)[h(x) = x]$, by $h(0) = 0$ and (2), together with the last axiom of T.

From (1) and (3) now we get the required $(\forall x)\phi(x)$. ⊣

REMARK: It is important, of course, that no induction is used in this proof, only the consideration of cases.

Theorem 3J.5 (Main Consistency Result)**.** *For each primitive recursive derivation $\vec{f}$, the system* PRA($\vec{f}$) *is* (finitistically) *consistent.*

Primitive recursive arithmetic is much more powerful than it might appear. As an example, here is one of its theorems.

Proposition 3J.6. *In the system* PRA(+) *(with the defining axioms for addition) we can prove that + is associative and commutative,*

$$x + (y + z) = (x + y) + z, \quad x + y = y + x.$$

This cannot be proved in Robinson's Q.