Notes on the Foundations of Constructive Mathematics

by Joan Rand Moschovakis

December 13, 2005

1 Background and Motivation

The constructive tendency in mathematics has deep roots. Most mathematicians prefer direct proofs to indirect ones, though some classical theorems have no direct proofs. For example, the proof that every limit point of $A \cup B$ is either a limit point of A or a limit point of B cannot be direct, since the hypothesis is insufficient to determine which of the two disjuncts of the conclusion must hold. What one actually proves is that if p has a neighborhood N_1 missing A and a neighborhood N_2 missing B, then p has a neighborhood missing $A \cup B$. This trivial argument is entirely constructive from the definition of "topological space," but classical logic is needed to interpret it as a proof of the original proposition.

Probably the most influential constructivist of the twentieth century was the intutionist L. E. J. Brouwer, who believed that the Aristotelian law of excluded middle (A or not A) held only in situations where the decision between the disjuncts could be made effectively. While Brouwer disapproved of formal reasoning, his student A. Heyting developed intuitionistic logic and arithmetic as subtheories of the corresponding classical theories; for this reason, intuitionistic arithmetic is called "Heyting arithmetic." Gödel showed by a translation that these intuitionistic theories are equiconsistent with the classical ones.

Other recognized varieties of constructive mathematics are finitism (Kronecker, Weyl), Russian recursive mathematics (Markov), and cautious constructivism (Bishop, Bridges, Richman). Markov and Bishop, like Brouwer, were especially interested in analysis. Bishop's constructive analysis is a subtheory of classical analysis; Markov's and Brouwer's are not. All are based on intuitionistic logic.

1.1 The B-H-K Interpretation

In order to recognize a statement as true, an intuitionist requires justification or proof. Tarski's "truth definition" for classical logic (see e.g. Kleene [1952] § 81) has an intuitionistic parallel, the Brouwer-Heyting-Kolmogorov interpretation, which clarifies the relationship between acceptable justification and logical structure.

1. To justify a prime sentence P is to recognize its truth.

2. To justify $A \;\&\; B$ is to justify A and B.

3. To justify $A \vee B$ is to justify a specific one of A, B.

4. To justify $A \rightarrow B$ is to provide a construction which transforms every justification of A into a justification of B.

5. To justify $\neg A$ is to justify $A \rightarrow \perp$, where $\perp$ is a known contradiction.

6. To justify $\forall x A(x)$ where D is the intended range of the variable x, is to provide a construction which associates with each $d \in D$ a justification of $A(d)$.

7. To justify $\exists x A(x)$ (with D as the range of x) is to justify $A(d)$ for a specific $d \in D$.

This is an explication, not a precise definition, as it relies on our intuitive understanding of words like "recognize," "construction" and "transforms." In applications the variable x ranges over a specific domain D, which need not be finite but must be structured so that a correct assertion of the form $d \in D$ is self-justifying. For arithmetic, D is the collection N of natural numbers, understood as generated from 0 by repeated application of the successor operation. For analysis, D is the collection of infinitely proceeding sequences of natural numbers.

Exercise 1.1. Assuming that every true statement can be justified (and that every recognizably true statement is true), use the B-H-K interpretation to prove that every justifiable statement is true according to the Tarski "definition" of classical truth.

1.2 Language and Logic

Brouwer expressed the view that mathematical objects (including proofs) are mental constructs, independent of language. Language is only a (sometimes untrustworthy) tool for communicating mathematical constructions. Logic is independent of language, but general logical principles which are always capable of justification may be formalized and used as shortcuts in mathematical reasoning.

The languages of pure intuitionistic propositional and predicate logic are the same as for classical logic. The language of intuitionistic (Heyting) arithmetic is the same as for classical (Peano) arithmetic. Only the logic is different.

The B-H-K interpretation gives each of the logical symbols &, $\vee$, $\to$, $\neg$, $\forall$, $\exists$ a distinct meaning. Classically, all the propositional connectives can be defined from & and $\neg$, while $\exists$ can be defined from $\forall$ and $\neg$, so $\vee$, $\to$ and $\exists$ are unnecessary. Intuitionistic logic, in contrast, makes full use of the expressive power of the formal language.

2 Formal Systems for Intuitionistic Logic

2.1 Intuitionistic Propositional Logic Pp

We begin with a Hilbert-style formalism **Pp**, from Kleene [1952], for intuitionistic propositional logic. The language $\mathcal{L}(\mathbf{Pp})$ has distinct proposition letters $P_0, P_1, P_2, \ldots$, logical symbols &, $\vee$, $\to$, $\neg$ and left and right parentheses (,).

Definition. The *prime formulas* of $\mathcal{L}(\mathbf{Pp})$ are the proposition letters. The *(well-formed) formulas* of $\mathcal{L}(\mathbf{Pp})$ are defined inductively as follows.

- Each prime formula is a *formula*.
- If A, B are *formulas* so are $(A \,\&\, B)$, $(A \vee B)$, $(A \to B)$ and $(\neg A)$.

In general, we use $A, B, C, \ldots$ as metavariables for well-formed formulas, omitting parentheses on the usual convention that $\neg$ binds closer than &, $\vee$ which bind closer than $\to$. Thus $\neg A \,\&\, B \to B \vee C$ abbreviates $(((\neg A) \,\&\, B) \to (B \vee C))$ and will be treated as well formed, while $A \to B \vee C \to A$ is ambiguous and hence not well formed.

Pp has one *rule of inference*:

R1 (*Modus Ponens*). From A and $A \to B$, conclude B.

The *axioms* of **Pp** are all formulas of the following forms:

X1. $A \to (B \to A)$.

X2. $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$.

X3. $A \to (B \to A \,\&\, B)$.

X4. $A \,\&\, B \to A$.

X5. $A \mathbin{\&} B \to B$.

X6. $A \to A \vee B$.

X7. $B \to A \vee B$.

X8. $(A \to C) \to ((B \to C) \to (A \vee B \to C))$.

X9. $(A \to B) \to ((A \to \neg B) \to \neg A)$.

X10. $\neg A \to (A \to B)$.

Definition. A *proof* in **Pp** is any finite sequence of formulas, each of which is an axiom or an immediate consequence, by the rule of inference, of two preceding formulas of the sequence. Any proof is said to *prove* its last formula, which is therefore a *theorem* of **Pp**. We write $\vdash_{\mathbf{Pp}} E$ (or in this subsection just $\vdash E$) to denote that E is a theorem of **Pp**.

Example. Here is a formal proof in **Pp** of $A \mathbin{\&} B \to B \mathbin{\&} A$, with the reasons for some of the steps omitted.

1. $A \mathbin{\&} B \to A$. [axiom by X4]
2. $(A \mathbin{\&} B \to A) \to ((A \mathbin{\&} B \to (A \to B \mathbin{\&} A)) \to (A \mathbin{\&} B \to B \mathbin{\&} A))$. [axiom by X2]
3. $(A \mathbin{\&} B \to (A \to B \mathbin{\&} A)) \to (A \mathbin{\&} B \to B \mathbin{\&} A)$. [by R1 from 1,2]
4. $B \to (A \to B \mathbin{\&} A)$.
5. $(B \to (A \to B \mathbin{\&} A)) \to (A \mathbin{\&} B \to (B \to (A \to B \mathbin{\&} A)))$.
6. $A \mathbin{\&} B \to (B \to (A \to B \mathbin{\&} A))$. [by R1 from 4,5]
7. $A \mathbin{\&} B \to B$. [axiom by X5]
8. $(A \mathbin{\&} B \to B) \to ((A \mathbin{\&} B \to (B \to (A \to B \mathbin{\&} A))) \to (A \mathbin{\&} B \to (A \to B \mathbin{\&} A)))$.
9. $(A \mathbin{\&} B \to (B \to (A \to B \mathbin{\&} A))) \to (A \mathbin{\&} B \to (A \to B \mathbin{\&} A))$.
10. $A \mathbin{\&} B \to (A \to B \mathbin{\&} A)$.
11. $A \mathbin{\&} B \to B \mathbin{\&} A$. [by R1 from 3,10]

Exercise 2.1. Provide reasons for steps 4, 5, 8, 9, 10 in the sample proof.

2.2 Deduction in Pp

The sample proof of $A \mathbin{\&} B \to B \mathbin{\&} A$ above suggests that formal proofs in **Pp** are slow and cumbersome. However, the pattern of lines 4-6 can be used to justify the *derived rule*

- From B conclude $A \to B$.

Using this rule, the sample proof could be shortened by one line. By considering *deductions* (or *derivations*) instead of just *proofs*, we can simplify the situation still further. A deduction is simply a proof from assumptions.

Definition. A *deduction* (or *derivation*) in **Pp** *of* a formula E *from* a collection Γ of formulas is a finite sequence of formulas, each of which is an axiom or a member of Γ or follows immediately by R1 from two formulas occurring earlier in the sequence. If such a deduction exists, E is said to be *deducible* or *derivable* in **Pp** from Γ, and we write $\Gamma \vdash_{\mathbf{Pp}} E$ (or in this section just $\Gamma \vdash E$).

Observe that if $\Gamma \vdash E$ then there is a finite subset $\Gamma' = \{G_1, \ldots, G_n\}$ of Γ such that $\Gamma' \vdash E$ (also written $G_1, \ldots, G_n \vdash E$). If $n = 0$ (so Γ' is empty) then $\vdash E$. Sometimes, as in the following theorem, it is convenient to write $\Gamma, A \vdash E$ instead of $\Gamma \cup \{A\} \vdash E$.

Theorem 2.1. (**The Deduction Theorem for Pp**) If $\Gamma, A \vdash B$ then $\Gamma \vdash (A \to B)$.

Proof. Fix Γ and A. We prove the theorem for every B, by induction on the length n of any given derivation $E_1, \ldots, E_n$ of B from Γ, A (so E_n is B).

If $n = 1$ then E_1 is an axiom, a member of Γ, or A. In the first two cases we construct a new deduction F_1, F_2, F_3 of $(A \to E_1)$ from Γ following the pattern of the derived rule suggested at the beginning of this subsection. If E_1 is A, construct a (five-line) proof of $(A \to A)$ in **Pp**.

Assuming the theorem holds for deductions of length $< n$ where $n > 1$, consider a given deduction $E_1, \ldots, E_n$ from Γ, A. If E_n is an axiom or a member of Γ, proceed as in the basis. If E_n comes from some E_j, E_k with $j, k < n$ by R1, where E_k is $(E_j \to E_n)$, then by the induction hypothesis there are deductions $F_1, \ldots, F_r$ of $(A \to E_j)$ from Γ, and $F_{r+1}, \ldots, F_{r+s}$ of $(A \to E_k)$ from Γ. Extend the deduction $F_1, \ldots, F_{r+s}$ by three lines to obtain a deduction of $(A \to E_n)$ from Γ.

Exercise 2.2. Complete the proof of the Deduction Theorem by providing $F_{r+s+1}, F_{r+s+2}, F_{r+s+3}$ for the induction step.

The next result is almost trivial, but useful nevertheless. We dignify it by calling it a theorem. Part (a) is the converse of the Deduction Theorem, and part (b) essentially says that $\vdash$ is transitive. As usual, Γ, Δ are collections of formulas and A, B are formulas; note that Γ, Δ may overlap.

Theorem 2.2. In **Pp**:
(a) If $\Gamma \vdash (A \to B)$ then $\Gamma, A \vdash B$.
(b) If $\Gamma \vdash A$ and $\Delta, A \vdash B$ then $\Gamma, \Delta \vdash B$.

Example. Here is a proof that $\vdash (A \to B)\ \&\ (B \to C) \to (A \to C)$. The proof is constructive, since the (constructive) proofs of the Deduction Theorem and Theorem 2.2 provide an algorithm for converting this outline into a formal proof in **Pp** of $(A \to B)\ \&\ (B \to C) \to (A \to C)$.

1. $(A \to B)\ \&\ (B \to C) \vdash (A \to B)$. [by Thm. 2.2(a) from X4]

2. $(A \to B)\ \&\ (B \to C) \vdash (B \to C)$. [by Thm. 2.2(a) from X5]

3. $(B \to C) \vdash (A \to (B \to C))$. [by Thm. 2.2(a) from X1]

4. $(A \to B), (A \to (B \to C)) \vdash (A \to C)$. [by Thm. 2.2(a) twice, from X2]

5. $(A \to B), (B \to C) \vdash (A \to C)$. [by Thm. 2.2(b) from 3,4]

6. $(A \to B)\ \&\ (B \to C), (B \to C) \vdash (A \to C)$. [by Thm. 2.2(b) from 1,5]

7. $(A \to B)\ \&\ (B \to C) \vdash (A \to C)$. [by Thm. 2.2(b) from 2,6]

8. $\vdash (A \to B)\ \&\ (B \to C) \to (A \to C)$. [by Thm. 2.1 from 7]

Exercise 2.3. Use Theorems 2.1 and 2.2 to prove that $\vdash ((A \to B) \to (\neg B \to \neg A))$.

Theorems 2.1 and 2.2 are *metatheorems* (theorems about the formal system, proved constructively). Another metatheorem which should be completely obvious is the fact that **Pp** has the *single substitution property*: If $\Gamma \vdash E$, and if Γ', E' come from Γ, E respectively by replacing *every* occurrence of a particular proposition letter P by an occurrence of the formula A, then $\Gamma' \vdash E'$.

Definition. Let E be a formula of $\mathcal{L}(\mathbf{Pp})$ containing at most the (distinct) proposition letters $P_1, \ldots, P_n$. Let $A_1, \ldots, A_n$ be (not necessarily distinct) formulas of $\mathcal{L}(\mathbf{Pp})$. It E' comes from E by simultaneously replacing each occurrence of P_i in E by an occurrence of A_i, for $i = 1, \ldots, n$, then E' is called a *substitution instance of* E *in* $\mathcal{L}(\mathbf{Pp})$.

Every such substitution instance of E can be viewed as the result of a finite sequence of single substitutions, as follows. Suppose the list $P_1, \ldots, P_{n+m}$ includes all the proposition letters occurring in $A_1, \ldots, A_n$. For $i = 1$ to n, let B_i come from A_i by successively replacing every occurrence of P_j by an occurrence of P_{n+m+j}, for $j = 1$ to n. Then none of $P_1, \ldots, P_n$ occurs in any of $B_1, \ldots, B_n$. Let F be the formula obtained from E by successively replacing every occurrence of P_i by an occurrence of

B_i, for $i = 1$ to n. Finally, E' comes from F by successively replacing every occurrence of P_{n+m+i} by an occurrence of P_i, for $i = 1$ to n.

Theorem 2.3. (**The Substitution Property for Pp**) If $\Gamma \ \vdash \ E$, and if Γ', E' come from Γ, E respectively by simultaneously replacing every occurrence of P_i by an occurrence of A_i, for $i = 1, \ldots, n$, then $\Gamma' \ \vdash \ E'$.

Exercise 2.4. Show that if Axiom Schema 10 is replaced by the classical law of double negation $\neg\neg A \to A$, then $A \vee \neg A$ becomes provable for every formula A. [*Hint*: First show how to construct a proof in **Pp** of $\neg\neg(A \vee \neg A)$.]

It follows from Exercise 2.4 that the formal system **cPp** which comes from **Pp** by strengthening Axiom Schema 10 to $\neg\neg A \to A$ (and defining $\vdash_{\mathbf{cPp}}$ accordingly) is classical propositional logic. Clearly **cPp** also has the substitution property, and the Deduction Theorem and Theorem 2.2 hold for **cPp** by essentially the same proofs as for **Pp**.

Exercise 2.5.* Suppose that E, F are formulas of $\mathcal{L}(\mathbf{Pp})$ such that for every substitution instance $(E' \to F')$ of $(E \to F)$: if $\vdash_{\mathbf{cPp}} E'$ then $\vdash_{\mathbf{cPp}} F'$. Show that $\vdash_{\mathbf{cPp}} (E \to F)$. [The * indicates a more difficult exercise.]

A rule of the form "From any substitution instance of E, conclude the corresponding substitution instance of F" which satisfies the hypothesis of this exercise with respect to a given formal theory is called an *admissible rule* of the theory. Exercise 2.5* shows that every admissible rule of **cPp** is *derivable* in **cPp**. The corresponding statement for **Pp** is false; in fact, the collection of admissible, nonderivable rules of **Pp** is recursively enumerable and infinite. A concrete enumeration proposed by de Jongh and Visser was recently proved by Iemhoff [2001] to be correct and complete.

2.3 The Natural Deduction System NPp

We have just observed that a few derived rules can save much time and effort in constructing (outlines of) formal proofs and derivations in **Pp**. One can go still further and abandon all axiom schemas in favor of rules as in the following *natural deduction* system **NPp** (essentially from Kleene [1952]), which differs from **N-IPC** of Troelstra and van Dalen [1988] only by having rules for $\neg$ instead of $\perp$. Formal derivations in a natural deduction system are labelled, rooted finite trees rather than finite sequences of formulas. This feature makes it easier to see how each step depends on the assumptions.

Definition. A *deduction* $\mathcal{D}$ *in* **Pp** *of* a formula E *from* assumptions Γ is a finite tree with a formula attached to each node (in particular, formulas from Γ attached to the leaves and E attached to the root), defined inductively as follows.

(i) If $E \in \Gamma$ then $\cdot E$ is a *deduction from* Γ *of* E.

(ii) If $\mathcal{D}_1$, $\mathcal{D}_2$ and $\mathcal{D}_3$ are *deductions from* Γ (and possibly the additional assumptions shown inside square brackets), *of* their last formulas (shown explicitly), then new *deductions from* Γ may be constructed using the following rules. Assumptions shown inside square brackets are *cancelled* when the indicated rule is applied. Each new deduction is a *deduction of* its last formula.

$$\&\mathrm{I}\ \dfrac{\begin{matrix}\mathcal{D}_1 & \quad \mathcal{D}_2\\ A & \quad B\end{matrix}}{A \,\&\, B} \qquad \&\mathrm{E}_r\ \dfrac{\begin{matrix}\mathcal{D}_1\\ A \,\&\, B\end{matrix}}{A} \qquad \&\mathrm{E}_l\ \dfrac{\begin{matrix}\mathcal{D}_1\\ A \,\&\, B\end{matrix}}{B}$$

$$\vee\mathrm{I}_r\ \dfrac{\begin{matrix}\mathcal{D}_1\\ A\end{matrix}}{A \vee B} \qquad \vee\mathrm{I}_l\ \dfrac{\begin{matrix}\mathcal{D}_1\\ B\end{matrix}}{A \vee B} \qquad \vee\mathrm{E}\ \dfrac{\begin{matrix} & [A] & [B]\\ \mathcal{D}_1 & \mathcal{D}_2 & \mathcal{D}_3\\ A \vee B & C & C\end{matrix}}{C}$$

$$\rightarrow \mathrm{I}\ \dfrac{\begin{array}{c}[A]\\ \mathcal{D}_1\\ B\end{array}}{A \rightarrow B} \qquad \rightarrow \mathrm{E}\ \dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2\\ A \rightarrow B & A\end{array}}{B}$$

$$\neg \mathrm{I}\ \dfrac{\begin{array}{cc}[A] & [A]\\ \mathcal{D}_1 & \mathcal{D}_2\\ B & \neg B\end{array}}{\neg A} \qquad \neg \mathrm{E}_i\ \dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2\\ A & \neg A\end{array}}{B}$$

If Γ is a list of formulas and E a formula in the language $\mathcal{L}(\mathbf{Pp})$, then $\Gamma \vdash_{\mathbf{NPp}} E$ means there is a deduction $\mathcal{D}$ in **NPp** of E from Γ. If Γ is empty then $\mathcal{D}$ is a *proof of* E in **NPp**.

It follows from the definition that if $\mathcal{D}$ is a deduction from Γ of E, and Γ' is the set of open assumption formulas occurring at the leaves of $\mathcal{D}$, then $\Gamma' \subseteq \Gamma$ and for each $\Delta \supseteq \Gamma'$: $\mathcal{D}$ is a deduction from Δ of E.

2.4 Equivalence of Pp with NPp

Theorem 2.4. If E is a formula, and Γ a collection of formulas, of $\mathcal{L}(\mathbf{Pp})$, then

$$\Gamma \vdash_{\mathbf{Pp}} E \ \text{ if and only if } \ \Gamma \vdash_{\mathbf{NPp}} E.$$

Proof for all Γ, E simultaneously, by induction on the definitions. If $E \in \Gamma$ there is nothing to prove in either direction. For $\Rightarrow$, we first construct a proof in **NPp** of each axiom E of **Pp**. As an example, observe that

$$\dfrac{A}{B \rightarrow A}\ \rightarrow \mathrm{I}$$

is a deduction of $(B \rightarrow A)$ from A, and hence

$$\dfrac{\dfrac{[A]}{B \rightarrow A}\ \rightarrow \mathrm{I}}{A \rightarrow (B \rightarrow A)}\ \rightarrow \mathrm{I}$$

is a proof of X1. There was no assumption B to cancel at the first $\rightarrow$ I. The assumption A was cancelled by the second $\rightarrow$ I.

Axioms X2-X10 are treated similarly, each using $\rightarrow$ I together with one other rule of **NPp**. Rule $\rightarrow$ E of **NPp** justifies the rule R1 of **Pp**. Hence every deduction in **Pp** can be transformed into a deduction in **NPp**, with the same assumptions and the same conclusion.

For $\Leftarrow$, we need to show that each rule of **NPp** is derivable in **Pp**. Theorem 2.1 takes care of $\rightarrow$ I, and Theorem 2.2 of $\rightarrow$ E. For $\vee$E, suppose $\mathcal{D}_1$ is an **NPp**-deduction from Γ, A of C; $\mathcal{D}_2$ is an **NPp**-deduction from Γ, B of C; and $\mathcal{D}_3$ is an **NPp**-deduction from Γ of $(A \vee B)$. By the induction hypothesis, in **Pp** there are deductions of C from Γ, A and of C from Γ, B, and also a deduction $G_1, \ldots, G_n$ of $(A \vee B)$ from Γ. By the Deduction Theorem for **Pp** there are deductions $E_1, \ldots, E_k$ of $A \rightarrow C$ from Γ, and $F_1, \ldots, F_m$ of $B \rightarrow C$ from Γ. Extend $E_1, \ldots, E_k, F_1, \ldots, F_m, G_1, \ldots, G_n$ by three lines H_1, H_2, H_3 to get a deduction of C from Γ in **Pp**, where H_1 is an axiom by X8, H_2 comes from E_k and H_1 by $R1$, and H_3 comes from F_m and H_2 by $R1$.

Exercise 2.6. Construct a labelled **NPp**-proof of Axiom X8 of **Pp**.

Exercise 2.7. Construct labelled **NPp**-proofs of Axioms X9 and X10 of **Pp**.

Exercise 2.8. Without using Theorem 2.4, prove that the rule $\neg$I of **NPp** can be derived in **Pp**.

2.5 Some Formal Theorems of Intuitionistic Propositional Logic

In intuitionistic as well as in classical logic, $A \leftrightarrow B$ abbreviates $(A \rightarrow B)$ & $(B \rightarrow A)$. Many classical equivalences fail intuitionistically; for example, as we shall see later, in parts (a),(b),(f)-(h) of the next theorem the main → cannot be replaced by ↔.

Theorem 2.5. In **Pp** (or equivalently, in **NPp**), for all formulas A, B:
(a) $\vdash (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$.
(b) $\vdash A \rightarrow \neg\neg A$.
(c) $\vdash \neg\neg\neg A \leftrightarrow \neg A$.
(d) $\vdash (A \rightarrow \neg B) \leftrightarrow (B \rightarrow \neg A)$.
(e) $\vdash \neg(A \vee B) \leftrightarrow (\neg A \,\&\, \neg B)$.
(f) $\vdash (\neg A \vee B) \rightarrow (A \rightarrow B)$.
(g) $\vdash (A \rightarrow B) \rightarrow \neg(A \,\&\, \neg B)$.
(h) $\vdash (\neg A \vee \neg B) \rightarrow \neg(A \,\&\, B)$.
(i) $\vdash (\neg\neg A \,\&\, \neg B) \leftrightarrow \neg(A \rightarrow B)$.

Proof of (b). $A, \neg A \vdash A$ and $A, \neg A \vdash \neg A$ trivially. Use the ¬I rule of **NPp** to conclude $A \vdash \neg\neg A$. Then use → I.

Proof of (e). We use **NPp**. By &I and → I we only need to derive $(\neg A \,\&\, \neg B)$ from $\neg(A \vee B)$, and conversely. Here are the two derivations:

$$\dfrac{\dfrac{\dfrac{[A]}{A \vee B}\,\vee\mathrm{I}_r \qquad \neg(A \vee B)}{\neg A}\,\neg\mathrm{I} \qquad \dfrac{\dfrac{[B]}{A \vee B}\,\vee\mathrm{I}_l \qquad \neg(A \vee B)}{\neg B}\,\neg\mathrm{I}}{(\neg A \,\&\, \neg B)}\,\&\,\mathrm{I}$$

$$\dfrac{[A \vee B] \qquad \dfrac{[A \vee B] \qquad \dfrac{[A] \qquad \dfrac{\neg A \,\&\, \neg B}{\neg A}\,\&\mathrm{E}_r}{\neg(A \vee B)}\,\neg\mathrm{E}_i \qquad \dfrac{[B] \qquad \dfrac{\neg A \,\&\, \neg B}{\neg B}\,\&\mathrm{E}_l}{\neg(A \vee B)}\,\neg\mathrm{E}_i}{\neg(A \vee B)}\,\vee\mathrm{E}}{\neg(A \vee B)}\,\neg\mathrm{I}\text{, cancelling } A \vee B \text{ (twice)}$$

Proof of (g). By → I it will be enough to derive $\neg(A \,\&\, \neg B)$ from $(A \rightarrow B)$ in **NPp**, as follows.

$$\dfrac{\dfrac{A \rightarrow B \qquad \dfrac{[A \,\&\, \neg B]}{A}\,\&\mathrm{E}_r}{B}\,\rightarrow\mathrm{E} \qquad \dfrac{[A \,\&\, \neg B]}{\neg B}\,\&\mathrm{E}_l}{\neg(A \,\&\, \neg B)}\,\neg\mathrm{I}$$

Exercise 2.9. Prove (c) and (f) of Theorem 2.5. [*Hint*: Exercise 2.3 established part (a), and part (b) is proved above. Hence in proving (c) you may use (a) and (b) (for any formulas A, B).]

A natural deduction system **NcPp** for classical propositional logic comes from **NPp** By changing the intuitionistic ¬-elimination rule $\neg\mathrm{E}_i$ to the following rule expressing the classical *law of double negation*:

$$\neg\mathrm{E}_c \; \dfrac{\begin{matrix}\mathcal{D}\\ \neg\neg A\end{matrix}}{A}$$

The proof of Theorem 2.4 can easily be adapted to show that derivability in **NcPp** is equivalent to derivability in **cPp**.

2.6 Intuitionistic First-Order Predicate Logic Pd

Again taking Kleene [1952] as a guide, we begin with a Hilbert-style formal system **Pd** which contains **Pp** as a subsystem. Formal theorems of **Pp** (such as the parts of Theorem 2.5) will hold in **Pd** for all formulas A, B of the extended language. The Deduction Theorem for **Pd** will need additional justification. Metatheorems whose hypotheses involve the deducibility relationship have to be reexamined whenever new axioms and/or rules are added to a formal theory.

The language $\mathcal{L}(\mathbf{Pd})$ has individual variables $a_1, a_2, a_3, \ldots$, and countably infinitely many distinct predicate letters of arity n for each $n = 0, 1, 2, 3, \ldots$. The 0-ary predicate letters are the proposition letters $P_1, P_2, \ldots$ of $\mathcal{L}(\mathbf{Pp})$. The unary predicate letters are $P_1(\cdot), P_2(\cdot), \ldots$, the binary ones are $P_1(\cdot,\cdot), P_2(\cdot,\cdot), \ldots$, and in general the n-ary ones are $P_i(\cdot, \ldots, \cdot)$ for $i = 1, 2, \ldots$ where $\cdot, \ldots, \cdot$ is a sequence of n placeholders. The logical symbols of $\mathcal{L}(\mathbf{Pd})$ are those of $\mathcal{L}(\mathbf{Pp})$, together with the universal quantifier $\forall$ and the existential quantifier $\exists$.

Definition. The *terms* of $\mathcal{L}(\mathbf{Pd})$ are the individual variables. If $P(\cdot, \ldots, \cdot)$ is an n-ary predicate letter and $t_1, \ldots, t_n$ are terms, then $P(t_1, \ldots, t_n)$ is a *prime formula* of $\mathcal{L}(\mathbf{Pd})$. The *(well-formed) formulas* of $\mathcal{L}(\mathbf{Pd})$ are defined inductively as follows:

- Each prime formula is a *formula.*
- If A, B are *formulas* so are $(A \mathbin{\&} B)$, $(A \vee B)$, $(A \rightarrow B)$ and $(\neg A)$.
- If A is a *formula* and x an individual variable, then $(\forall x A)$ and $(\exists x A)$ are *formulas.*

In general, $x, y, z, w, x_1, y_1, \ldots$ will be used as metavariables for individual variables, and $A, B, C, \ldots$ as metavariables for formulas. Anticipating applications (e.g. to arithmetic) where the terms may be more complicated, we use $t, u, v, t_1, \ldots$ as metavariables for terms. In omitting parentheses, $\forall x$ and $\exists x$ are treated like $\neg$, so $\exists x \neg A \rightarrow B$ abbreviates $((\exists x(\neg A)) \rightarrow B)$. If x is a variable and A a formula, we may write $A(x)$ for A (even if x does not actually occur in A), as in the following definition.

Definition. The *scope* of an outermost $\forall x$ or $\exists x$, in a formula of the form $(\forall x A(x))$ or $(\exists x A(x))$, is the subformula $A(x)$. An occurrence of a variable x in a formula B is *bound in B* if it is the x of a quantifier $\forall x$ or $\exists x$, or is within the scope of such a quantifier (with the same x). An occurrence of x in B which is not bound in B, is *free in B.* A bound occurrence of x in B is *bound by* the outermost quantifier of the smallest subformula of B of the form $(\forall x C(x))$ or $(\exists x C(x))$ (with the same x) to which it belongs. In **Pd** and all the applications to be considered in these notes, any occurrence of a variable x in a term t is *free in t.*

Example. In the formula $\forall a_1(\exists a_2(P_1(a_1, a_2) \rightarrow \exists a_1 P_2(a_1, a_2))) \mathbin{\&} P_1(a_1)$, the first and second occurrences of a_1 are bound by the $\forall a_1$. The third and fourth occurrences of a_1 are bound by the $\exists a_1$. The fifth occurrence of a_1 is free.

Definition. If $A(x)$ is a formula, x a variable, and t a term, then $A(t)$ is the result of substituting an occurrence of t for each free occurrence of x in $A(x)$. The substitution is *free* if no free occurrence in t of any variable becomes bound in $A(t)$, and in this case we say *t is free for x in $A(x)$.*

Example. Suppose $A(x, z)$ is $\forall y(P(x, y) \rightarrow \exists x Q(x, z))$ where $P(x, y)$ and $Q(x, z)$ are prime formulas with exactly the indicated variables free (where x, y, z are distinct individual variables). Then y is not free for x in $A(x, z)$, since the new occurrence of y in $A(y, z)$ will be bound by the $\forall y$. But z is free for x in $A(x, z)$, since $A(z, z)$ is $\forall y(P(z, y) \rightarrow \exists x Q(x, z))$ with the new occurrence of z free.

Exercise 2.10. For the $A(x, z)$ of the example, answer each of the following questions.
(a) What are the scopes of the quantifiers $\forall y$ and $\exists x$?
(b) Is x free for z in $A(x, z)$? Is y free for z in $A(x, z)$?

This use of the notations $A(x)$, $A(t)$ requires some care. If y is free for x in $A(x)$, $B(y)$ is (the same formula as) $A(y)$, and $B(x)$ is derived from $B(y)$ by substituting an occurrence of x for every free occurrence of y in $B(y)$, then $B(x)$ may differ from $A(x)$. For example, let $A(x)$ be $P_1(x, y)$ where x, y are distinct variables. Then y is free for x in $A(x)$, and $A(y)$ is $P_1(y, y)$. If $B(y)$ is $P_1(y, y)$ then x is free for y in $B(y)$, and $B(x)$ is $P_1(x, x)$.

However, if y *is* x, or if y is free for x in $A(x)$ *and does not occur free in* $A(x)$, then x is free for y in $A(y)$ and does not occur free in $A(y)$ (unless x is y). In either of these cases the sequence of substitutions $x \mapsto y \hookrightarrow x$ leads from $A(x)$ to $A(y)$ and back to $A(x)$. (Note that distinct metavariables $x, y, z, w, x_1, \ldots$ need not always denote distinct individual variables.)

In addition to R1, **Pd** has two new *rules of inference*:

R2. From $C \rightarrow A(x)$ where x does not occur free in C, conclude $C \rightarrow \forall x A(x)$.

R3. From $A(x) \rightarrow C$ where x does not occur free in C, conclude $\exists x A(x) \rightarrow C$.

In addition to X1 - X10, **Pd** has two new *axiom schemas*, where $A(x)$ may be any formula and t any term free for x in $A(x)$:

X11. $\forall x A(x) \rightarrow A(t)$.

X12. $A(t) \rightarrow \exists x A(x)$.

Definition. A *deduction* (or *derivation*) in **Pd** *of* a formula E *from* a collection Γ of formulas is a finite sequence of formulas, each of which is an axiom by X1 - X12, or a member of Γ, or follows immediately by R1, R2 or R3 from one or two formulas occurring earlier in the sequence. If such a deduction exists, we may write $\Gamma \vdash_{\mathbf{Pd}} E$ (or in this subsection just $\Gamma \vdash E$).

Definition. If $E_1, \ldots, E_n$ is a deduction from Γ and $G \in \Gamma$, then for each $k = 1, \ldots, n$ we say that E_k *depends on* G *in* the deduction if and only if one of the following holds:

- E_k is G, and is justified as an assumption formula from Γ, or
- E_k is a consequence by R1 of two formulas E_i, E_j with $i, j < k$, where one or both of E_i, E_j *depends on* G, or
- E_k is a consequence by R2 or R3 of some formula E_i which *depends on* G, where $i < k$.

If R2 or R3 is used in a deduction from Γ, with respect to a variable x which occurs free in at least one assumption from Γ on which the hypothesis of the rule depends, then x is *varied in* the deduction; otherwise x is *held constant in* the deduction. To indicate that a deduction of E from Γ exists in which $x_1, \ldots, x_k$ are varied, we sometimes write $\Gamma \vdash_{\mathbf{Pd}}^{x_1,\ldots,x_k} E$ (or in this subsection just $\Gamma \vdash^{x_1,\ldots,x_k} E$).

Exercise 2.11. Construct a deduction in **Pd** of $\exists x A(x)$ from $\forall x A(x)$, in which no variable is varied.

Exercise 2.12.* Let x be a variable, and $A(x)$ a formula containing x free. Suppose that y is a variable which does not occur free in $A(x)$, suppose y is free for x in $A(x)$, and let $A(y)$ be the result of substituting y for x in $A(x)$. Let C be a formula not containing y free.
(a) Construct a deduction in **Pd** of $(\exists x A(x) \rightarrow C)$ from $(A(y) \rightarrow C)$.
(b) Which, if any, variables were varied in your deduction?

The next lemma collects a few easy facts about deduction in **Pd**. Parts (b) and (c) correspond to Theorem 2.2(a) and (b).

Lemma 2.6. In **Pd**:
(a) If $\Gamma \vdash (A \rightarrow B)$ by a deduction in which only $x_1, \ldots, x_k$ are varied, then $\Gamma, A \vdash B$ by a deduction in which only $x_1, \ldots, x_k$ are varied.
(b) If $\Gamma, A \vdash B$ by a deduction $E_1, \ldots, E_k$ in which B does not depend on A and only $x_1, \ldots, x_n$ are varied, then some subsequence of $E_1, \ldots, E_k$ is a deduction of B from Γ in which no other variables are varied.
(c) If $\Gamma \vdash A$ and $\Delta, A \vdash B$ by deductions in which no variables other than $x_1, \ldots, x_k$ are varied, then $\Gamma, \Delta \vdash B$ by a deduction in which no other variables are varied.

Exercise 2.13. Prove that if $\Gamma \vdash_{\mathbf{Pd}} A(x)$ by a deduction in which none of $y_1, \ldots, y_m$ is varied, and x does not occur free in any assumption from Γ on which the conclusion $A(x)$ depends, then $\Gamma \vdash_{\mathbf{Pd}} \forall x A(x)$ by a deduction in which none of $y_1, \ldots, y_m$ is varied.

Exercise 2.14. [This is part of the proof of Theorem 2.7.] Prove that in **Pp**:
(a) $(A \to (C \to D)) \vdash (A \& C \to D)$ and
(b) $(A \& C \to D) \vdash (A \to (C \to D))$.

Theorem 2.7. (**The Deduction Theorem for Pd**) If $\Gamma, A \vdash_{\mathbf{Pd}} B$ by a deduction in which all variables occurring free in A are held constant, and only $x_1, \ldots, x_m$ are varied, then $\Gamma \vdash_{\mathbf{Pd}} (A \to B)$ by a deduction in which no variables except $x_1, \ldots, x_m$ (and possibly only some of these) are varied.

Proof. Fix Γ and A, and suppose $E_1, \ldots, E_n$ is a given deduction of B from Γ, A in which all variables occurring free in A are held constant and only $x_1, \ldots, x_m$ are varied. There are four new cases to add to the inductive proof of Theorem 2.1, and in the case for R1 we must consider which variables are varied.

For $n = 1$ the two new axiom schemas X11, X12 are treated exactly as X1 - X10 were before. If E_1 is a member of Γ then $(A \to E_1)$ is derivable from Γ by a three-line deduction in which no variables are varied.

Assuming the theorem holds for deductions of length $< n$ where $n > 1$, consider a given deduction $E_1, \ldots, E_n$ from Γ, A in which all variables free in A are held constant, and only $x_1, \ldots, x_m$ are varied. If E_n is an axiom or a member of Γ, proceed as in the basis, observing that no variables are varied in the resulting deduction of $(A \to E_n)$ from Γ. Now consider the three rules of inference.

Rule 1. If E_n comes from some E_j, E_k with $j, k < n$ by R1, recall the proof of Theorem 2.1. We may assume that no variables other than $x_1, \ldots, x_m$ were varied in the (independent) deductions $F_1, \ldots, F_r$ of $(A \to E_j)$ and $F_{r+1}, \ldots, F_{r+s}$ of $(A \to E_k)$ from Γ provided by the induction hypothesis. If y is another variable occurring free in some formula of Γ which appears as assumption F_i for some $1 \leq i \leq r$, then none of $F_{i+1}, \ldots, F_r$ was justified by applying R2 or R3 (with y as the variable) to any formula depending on F_i, and none of $F_{r+1}, \ldots, F_{r+s}$ depends on any of $F_1, \ldots, F_r$. Hence y is not varied in $F_1, \ldots, F_{r+s}$. Since the new steps $F_{r+s+1}, F_{r+s+2}, F_{r+s+3}$ use only propositional logic, no variables other than $x_1, \ldots, x_m$ are varied in the resulting deduction of $(A \to E_n)$ from Γ.

Rule 2. If E_n comes from some E_j with $j < n$ by R2, then E_n is of the form $(C \to \forall x D(x))$ where E_j is $(C \to D(x))$ and x does not occur free in C. There are two possibilities, depending on whether or not E_j depends on A in the given deduction.

Case 1. E_j depends on A. Then x is not free in A (otherwise it would have been varied in deriving E_n from E_j by R2). By the induction hypothesis there is a deduction $F_1, \ldots, F_r$ of $(A \to E_j)$ from Γ in which no variables other than $x_1, \ldots, x_m$ are varied. By the result of Exercise 2.14 this deduction can be extended to $F_1, \ldots, F_{r+s}$, using only X1-X10 and R1 in the new part, so that F_{r+s} is $(A \& C \to D(x))$. Since x is not free in $A \& C$, by R2 from F_{r+s} we conclude $(A \& C \to \forall x D(x))$, which is F_{r+s+1}. More propositional steps lead to $(A \to (C \to \forall x D(x)))$, which is $(A \to E_n)$. In the resulting deduction no variables have been varied which were not already varied in $E_1, \ldots, E_n$.

Case 2. E_j does not depend on A. Then neither does E_n, so by Lemma 2.6(b) from the induction hypothesis there is a deduction of E_n from Γ in which no variables other than $x_1, \ldots, x_m$ are varied. Extend this to a deduction of $(A \to E_n)$ from Γ in the usual way, using only X1 and R1.

Rule 3. If E_n comes from some E_j with $j < n$ by R3, then E_n is of the form $(\exists x D(x) \to C)$ where E_j is $(D(x) \to C)$, and x does not occur free in C. If E_j does not depend on A then neither does E_n, and we argue as in Case 2 for R2. If E_j depends on A then x is not free in A. By the induction hypothesis there is a deduction $G_1, \ldots, G_r$ of $(A \to E_j)$ from Γ in which no variables other than $x_1, \ldots, x_m$ are varied. Then $G_1, \ldots, G_r$ can be extended by propositional steps to $G_1, \ldots, G_{r+s}$ where G_{r+s} is $(D(x) \to (A \to C))$. Since x is not free in $(A \to C)$, by R3 from G_{r+s} we can conclude $(\exists x D(x) \to (A \to C))$, from which $(A \to E_n)$ follows by propositional logic.

2.7 The Natural Deduction System NPd

A rule-based formal system **NPd** equivalent to **Pd** begins by extending the framework and rules of **NPp** to $\mathcal{L}(\mathbf{Pd})$. Four new quantifier rules correspond to R2, X11, X12 and R3, with restrictions on the variables reflecting the fact that *dependence on* assumption formulas is determined by the tree form of a deduction.

Definition. A *deduction* $\mathcal{D}$ in **NPd** *of* a formula E *from* assumptions Γ is a finite tree with a formula attached to each node, as follows.

(i) If $E \in \Gamma$ then $\cdot E$ is a *deduction from* Γ *of* E.

(ii) If $\mathcal{D}_1$, $\mathcal{D}_2$ and $\mathcal{D}_3$ are *deductions from* Γ (and possibly the additional assumptions shown inside square brackets), *of* their last formulas (shown explicitly), then new *deductions from* Γ may be constructed using the rules of **NPp** and also the following rules, if the restrictions on their use are satisfied. Assumptions shown inside square brackets are *cancelled* when the indicated rule is applied. Each new deduction is a *deduction of* its last formula.

Restrictions: For $\forall$E and $\exists$I, t is a term free for x in $A(x)$. For $\forall$I, x is not free in any open assumption of $\mathcal{D}_1$. For $\exists$E, x is not free in C or in any open assumption of $\mathcal{D}_2$ except $A(x)$.

$$\forall\text{I}\ \dfrac{\begin{array}{c}\mathcal{D}_1\\ A(x)\end{array}}{\forall x A(x)} \qquad\qquad \forall\text{E}\ \dfrac{\begin{array}{c}\mathcal{D}_1\\ \forall x A(x)\end{array}}{A(t)}$$

$$\exists\text{I}\ \dfrac{\begin{array}{c}\mathcal{D}_1\\ A(t)\end{array}}{\exists x A(x)} \qquad\qquad \exists\text{E}\ \dfrac{\begin{array}{c}\mathcal{D}_1\\ \exists x A(x)\end{array} \qquad \begin{array}{c}[A(x)]\\ \mathcal{D}_2\\ C\end{array}}{C}$$

If Γ is a list of formulas and E a formula of $\mathcal{L}(\mathbf{Pd})$, then $\Gamma \vdash_{\mathbf{NPd}} E$ means that there is a deduction $\mathcal{D}$ in **NPd** of E from Γ. If Γ is empty then $\mathcal{D}$ is a *proof of* E in **NPd**.

It follows from the definition that if $\mathcal{D}$ is a deduction from Γ of E, and Γ' is the set of open assumption formulas occurring at the leaves of $\mathcal{D}$, then $\Gamma' \subseteq \Gamma$ and for each $\Delta \supseteq \Gamma'$: $\mathcal{D}$ is a deduction of E from Δ.

Example. Here is a proof in **NPd** of $\forall x A(x) \to \forall y A(y)$ if $A(x)$ is a formula such that y is free for x in $A(x)$, and y does not occur free in $A(x)$ (unless y is x). The second condition guarantees that y is not free in $\forall x A(x)$, justifying the $\forall$I.

$$\cfrac{\cfrac{\cfrac{[\forall x A(x)]}{A(y)}\ \forall\text{E}}{\forall y A(y)}\ \forall\text{I}}{\forall x A(x) \to \forall y A(y)}\ \to\text{I}$$

Exercise 2.15. Construct a proof in **NPd** of $\exists x A(x) \to \exists y A(y)$ if $A(x)$ is a formula such that y is free for x in $A(x)$, and y is not free in $\exists x A(x)$.

Definition. Two formulas A,B are *congruent* if (as strings of symbols) they differ only in the identity of their bound variables, in the sense that

(i) Every bound occurrence of a variable in either formula corresponds to an occurrence of a variable, bound by the same quantifier, in the other formula.

(ii) Every free occurrence of a variable in either formula corresponds to a free occurrence of the same variable in the other formula.

By the Replacement Theorem (in the next section) with the sample proof and Exercise 2.15, if A and B are congruent formulas then $\vdash_{\mathbf{Pd}} A \leftrightarrow B$. It follows that every formula has an equivalent congruent in which no variable occurs both bound and free.

2.8 Equivalence of Pd with NPd, and the Replacement Theorem for Pd

Theorem 2.8. If E is a formula, and Γ is a collection of formulas, of $\mathcal{L}(\mathbf{Pd})$, then the following are equivalent:

(a) $\Gamma \vdash_{\mathbf{Pd}} E$ by a deduction in which no variable is varied.

(b) $\Gamma \vdash_{\mathbf{NPd}} E$.

Proof of $(a) \Rightarrow (b)$, for all Γ, E simultaneously, by complete induction on the length of a given **Pd**-deduction of E from Γ in which no variable is varied. The proof of Theorem 2.4 ⇒ provides **NPd**-proof schemas for the propositional axioms X1-X10 of **Pd**. It is easy to construct **NPd**-proof schemas for X11 and X12, using the → rules with ∀E and ∃I (which have the same restrictions as X11 and X12 of **Pd**). The rules require more care.

Suppose $F_1, \ldots, F_n, F_{n+1}$ is a deduction in **Pd** from Γ in which no variable is varied, and F_{n+1} is a consequence by R1, R2 or R3 of one or two formulas occurring earlier in the deduction. Suppose the induction hypothesis holds for each **Pd**-deduction of length $\leq n$, so for each $j \leq n$ and each Δ: If $G_1, \ldots, G_j$ is a deduction in **Pd** from Δ in which no variable is varied, then $\Delta \vdash_{\mathbf{NPd}} G_j$. There are three possibilities.

Case 1. F_{n+1} is a consequence by R1 of F_i and F_j with $i, j \leq n$ where F_i is $F_j \to F_{n+1}$. By the induction hypothesis there are **NPd**-deductions $\mathcal{D}_1$, $\mathcal{D}_2$ of F_i, F_j respectively from Γ. Combine these using → E to get an **NPd**-deduction of F_{n+1} from Γ.

Case 2. F_{n+1} is $(C \to \forall x A(x))$, where x is not free in C, and F_{n+1} is a consequence by R2 of some F_i with $i \leq n$. Then F_i is $(C \to A(x))$, and x is not free in any assumption from Γ on which F_i depends (otherwise x would be varied by the use of R2). Then by Lemma 2.6(b) some subsequence of $F_1, \ldots, F_i$ is a **Pd**-deduction of $(C \to A(x))$ from a subcollection Γ' of Γ in which x does not occur free. By the induction hypothesis there is an **NPd**-deduction $\mathcal{D}_1$ of F_i from Γ'. Extend it as follows to an **NPd**-deduction of F_{n+1} from Γ' (hence also from Γ). The use of ∀I is justified because x is not free in C nor in any open assumption formula of $\mathcal{D}_1$, since every open assumption formula of $\mathcal{D}_1$ belongs to Γ'.

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\mathcal{D}_1\\ (C \to A(x))\end{array} \qquad [C]}{A(x)}\ {\to}\,\text{E}}{\forall x A(x)}\ \forall\text{I}}{(C \to \forall x A(x))}\ {\to}\,\text{I, cancelling } C$$

Case 3. F_{n+1} is $(\exists x A(x) \to C)$ where x is not free in C, and F_{n+1} is a consequence by R3 of some F_i with $i \leq n$. Then F_i is $(A(x) \to C)$, and x is not free in any assumption from Γ on which F_i depends (otherwise x would be varied by the use of R3). Then by Lemma 2.6(b) some subsequence of $F_1, \ldots, F_i$ is a **Pd**-deduction of $(A(x) \to C)$ from a subcollection Γ' of Γ in which x does not occur free, so by the induction hypothesis there is an **NPd**-deduction $\mathcal{D}_1$ of F_i from Γ'. Extend $\mathcal{D}_1$ to an **NPd**-deduction of F_{n+1} from Γ' (hence also from Γ) as follows.

$$\dfrac{\dfrac{[\exists x A(x)] \qquad \dfrac{\begin{array}{c}\mathcal{D}_1\\ (A(x) \to C)\end{array} \qquad [A(x)]}{C}\ {\to}\,\text{E}}{C}\ \exists\text{E, cancelling } A(x)\text{; no free } x \text{ in } \Gamma' \text{ or } C}{(\exists x A(x) \to C)}\ {\to}\,\text{I, cancelling } \exists x A(x)$$

Proof of $(b) \Rightarrow (a)$. Assume $\mathcal{D}$ is an **NPd**-deduction from Γ of E, and assume the induction hypothesis holds for the subdeduction(s) from Γ of the hypothesis (or hypotheses) of the last rule used to deduce E. If the last inference was by a propositional rule, proceed as in the proof of Theorem 2.4, using Lemma 2.6(a) and Theorem 2.7 to justify the → rules. If the last inference was by a quantifier rule, there are four possibilities.

Case 1. E is $\forall x A(x)$, which follows by $\forall$I from the conclusion $A(x)$ of a deduction $\mathcal{D}_1$ in which x is not free in any open assumption. Let Γ' be the collection of all assumptions from Γ which are open in $\mathcal{D}_1$, so x is not free in Γ' and $\mathcal{D}_1$ is a **NPd**-deduction from Γ' of $A(x)$. By the induction hypothesis, $\Gamma' \vdash_{\mathbf{Pd}} A(x)$ by a deduction in which no variable is varied, and x is not free in any assumption from Γ' on which $A(x)$ depends. Apply the result of Exercise 2.13.

Case 2. The last inference was by $\exists$E, so E is C without x free, and $\mathcal{D}$ has subdeductions $\mathcal{D}_1$ of $\exists x A(x)$ from Γ, and $\mathcal{D}_2$ of C from $\Gamma, A(x)$, such that x is not free in any open assumption of $\mathcal{D}_2$ other than $A(x)$. Let Γ' be the collection of all assumptions from Γ which are different from $A(x)$ and are open in $\mathcal{D}_2$, so $\mathcal{D}_2$ is a deduction of C from $\Gamma', A(x)$ and x is not free in Γ'. By the induction hypothesis $\Gamma', A(x) \vdash_{\mathbf{Pd}} C$ with no variables varied, so by the Deduction Theorem $\Gamma' \vdash_{\mathbf{Pd}} (A(x) \rightarrow C)$ with no variables varied. Since x is not free in C or in Γ', we can use R3 to conclude $\Gamma' \vdash_{\mathbf{Pd}} (\exists x A(x) \rightarrow C)$ with no variables varied.

Cases 3 and 4. The last inference was by $\forall$E or by $\exists$I. These cases are easy, using X11 and X12 with the induction hypothesis.

Theorems 2.7 and 2.8 provide flexibility in establishing facts about provability and deducibility in intuitionistic predicate logic. Propositional arguments carry over naturally to $\mathcal{L}(\mathbf{Pd})$, holding all variables constant, as in the following example. Quantifier arguments are often easier in **NPd** than in **Pd**, as in the next two exercises.

Example. The Replacement Theorem for **Pd** needs the lemma $(A \leftrightarrow B) \vdash_{\mathbf{Pd}} (A \vee C) \leftrightarrow (B \vee C)$, with no variables varied. Theorem 2.8 allows us to prove $(A \leftrightarrow B) \vdash_{\mathbf{NPd}} (A \vee C) \leftrightarrow (B \vee C)$ instead. Remember that $(A \leftrightarrow B)$ abbreviates $(A \rightarrow B)\ \&\ (B \rightarrow A)$, for any formulas A, B. The following deduction establishes $(A \leftrightarrow B), (A \vee C) \vdash_{\mathbf{NPd}} (B \vee C)$:

$$\dfrac{A \vee C \qquad \dfrac{\dfrac{\dfrac{A \leftrightarrow B}{(A \rightarrow B)}\;\&\mathrm{E}_r \qquad [A]}{B}\;\rightarrow \mathrm{E}}{B \vee C}\;\vee\mathrm{I}_r \qquad \dfrac{[C]}{B \vee C}\;\vee\mathrm{I}_l}{B \vee C}\;\vee\text{E, cancelling } A \text{ and } C$$

and $(A \leftrightarrow B), (B \vee C) \vdash_{\mathbf{NPd}} (A \vee C)$ by a similar deduction. Use $\rightarrow$ I (twice) and &I to complete the argument in **NPd**.

Exercise 2.16. Prove that $\forall x(A(x) \leftrightarrow B(x)) \vdash_{\mathbf{Pd}} (\exists x A(x) \leftrightarrow \exists x B(x))$ with all variables held constant. [*Hint*: Use Theorem 2.8.]

Exercise 2.17. Prove that if x, y are distinct, and E is any formula, then $\vdash_{\mathbf{Pd}} \forall x \forall y E \leftrightarrow \forall y \forall x E$.

Exercise 2.18.* Prove that if $x_1, \ldots, x_k$ all occur free in E, then $E \vdash_{\mathbf{Pd}}^{x_1,\ldots,x_k} \forall x_1 \ldots \forall x_k E$.

Definition. If $E(x_1, \ldots, x_k)$ is a formula of $\mathcal{L}(\mathbf{Pd})$ with exactly the distinct variables $x_1, \ldots, x_k$ free, where the first free occurrence of x_i precedes the first free occurrence of x_{i+1} for each $1 \leq i < k$, then the *universal closure* $\forall E$ *of* E is $\forall x_1 \ldots \forall x_k E(x_1, \ldots, x_k)$.

By Exercise 2.17, the order of the initial quantifiers in $\forall E$ is in some sense unimportant. That sense is made clearer by the following theorem, which is tedious to prove (by induction on the depth of the occurrence of A in C_A, using Theorem 2.8 with Exercise 2.18* and a lot of lemmas like the sample proof and Exercise 2.16). We state it correctly, following Kleene [1952], and move on.

Theorem 2.9. (**The Replacement Theorem for Pd**) Suppose A and B are formulas of $\mathcal{L}(\mathbf{Pd})$, and C_A and C_B are formulas which differ only in that C_B results from C_A by replacing a particular occurrence of the subformula A of C_A by an occurrence of B. Suppose $x_1, \ldots, x_k$ are all the distinct free variables of A or B which belong to a quantifier of C_A having the specified occurrence of A within its scope. Then

$$(A \leftrightarrow B) \vdash_{\mathbf{Pd}}^{x_1,\ldots,x_k} (C_A \leftrightarrow C_B).$$

2.9 Some Formal Theorems of Intuitionistic Predicate Logic

The next theorem lists some equivalences and implications which hold in intuitionistic predicate logic. The proofs of equivalences are simplified by the observation that if $E \vdash_{\mathbf{NPd}} F$ and $F \vdash_{\mathbf{NPd}} E$, then also $\vdash_{\mathbf{NPd}} (E \leftrightarrow F)$ by $\rightarrow$ I and &I. In parts (a), (d), (g) and (h) the $\rightarrow$ cannot be replaced by $\leftrightarrow$.

Theorem 2.10. In **Pd** (or equivalently, in **NPd**), for all formulas $A(x), B(x), C$ such that x is not free in C:

(a) $\vdash (\forall x A(x) \lor C) \rightarrow \forall x(A(x) \lor C)$.
(b) $\vdash (\exists x A(x) \lor \exists x B(x)) \leftrightarrow \exists x(A(x) \lor B(x))$.
(c) $\vdash \forall x(A(x) \,\&\, B(x)) \leftrightarrow (\forall x A(x) \,\&\, \forall x B(x))$.
(d) $\vdash \exists x(A(x) \,\&\, B(x)) \rightarrow (\exists x A(x) \,\&\, \exists x B(x))$.
(e) $\vdash \forall x(A(x) \rightarrow C) \leftrightarrow (\exists x A(x) \rightarrow C)$.
(f) $\vdash \forall x(C \rightarrow A(x)) \leftrightarrow (C \rightarrow \forall x A(x))$.
(g) $\vdash \exists x(A(x) \rightarrow C) \rightarrow (\forall x A(x) \rightarrow C)$.
(h) $\vdash \exists x(C \rightarrow A(x)) \rightarrow (C \rightarrow \exists x A(x))$.
(i) $\vdash (\exists x C \leftrightarrow C)$ and $\vdash (\forall x C \leftrightarrow C)$.

Proof of (a). By $\rightarrow$ I from the following **NPd**-deduction, which shows that $(\forall x A(x) \lor C) \vdash_{\mathbf{NPd}} \forall x(A(x) \lor C)$:

$$\dfrac{\dfrac{\forall x A(x) \lor C \qquad \dfrac{\dfrac{[\forall x A(x)]}{A(x)}\,\forall\mathrm{E}}{A(x) \lor C}\,\lor\mathrm{I}_r \qquad \dfrac{[C]}{A(x) \lor C}\,\lor\mathrm{I}_l}{A(x) \lor C}\,\lor\text{E, cancelling } \forall x A(x),\ C}{\forall x(A(x) \lor C)}\,\forall\text{I, no free } x \text{ in } \forall x A(x) \lor C$$

Proof of (e). Here is an informal argument that $\forall x(A(x) \rightarrow C) \vdash_{\mathbf{NPd}} (\exists x A(x) \rightarrow C)$. First, $\forall x(A(x) \rightarrow C) \vdash_{\mathbf{NPd}} (A(x) \rightarrow C)$ by $\forall$E. Hence by Theorem 2.8 there is a deduction in **Pd** of $(A(x) \rightarrow C)$ from $\forall x(A(x) \rightarrow C)$ in which no variable is varied. Extend this deduction using R3, so $\forall x(A(x) \rightarrow C) \vdash_{\mathbf{Pd}} (\exists x A(x) \rightarrow C)$ with all variables held constant. Now use Theorem 2.8. [Alternatively, use the prooftree given in Case 3 of the inductive proof of $(a) \Rightarrow (b)$ in Theorem 2.8, interpreting $\mathcal{D}_1$ as the immediate deduction of $A(x) \rightarrow C$ from $\forall x(A(x) \rightarrow C)$ by $\forall$E.]

We prove directly that $(\exists x A(x) \rightarrow C) \vdash_{\mathbf{NPd}} \forall x(A(x) \rightarrow C)$:

$$\dfrac{\dfrac{\dfrac{\exists x A(x) \rightarrow C \qquad \dfrac{[A(x)]}{\exists x A(x)}\,\exists\mathrm{I}}{C}\,\rightarrow\mathrm{E}}{A(x) \rightarrow C}\,\rightarrow\text{I, cancelling } A(x)}{\forall x(A(x) \rightarrow C)}\,\forall\text{I, no free } x \text{ in } \exists x A(x) \rightarrow C$$

Exercise 2.19. Prove (f) of Theorem 2.10.

Exercise 2.20. Prove (g) of Theorem 2.10.

The proof theory of **Pp** and **Pd** has been studied extensively, building on work of Gödel [1932] and Gentzen [1934-35] which established constructively that **Pp** (like **cPp**) is decidable, although **Pp** has no finite truth-table interpretation. Good references are Chapter 15 of Kleene [1952], Chapter 10 of (volume 2 of) Troelstra and van Dalen [1988], and Troelstra and Schwichtenberg [2000]. Gödel and Gentzen independently found negative translations of **cPp** into **Pp**, and of **cPd** into **Pd**, showing that in each case the intutionistic system is as strong as the classical one.

We have already considered in detail how to prove statements intuitionistically, and how to extend each intuitionistic system to the corresponding classical one by strengthening one axiom schema or one rule. Since the purpose of these notes is to provide a logical basis for the study of constructive mathematics, the next topic will be (not more proof theory, but) semantics for intuitionistic logic.

3 Semantics for Intuitionistic Logic

In order to show, for example, that $\vdash_{\mathbf{Pp}} \neg\neg A \to A$ does not hold for all formulas A of **Pp**, we need an interpretation with respect to which **Pp** is *sound* (so every theorem of **Pp** is verified by the semantics), and an instance of $\neg\neg A \to A$ which is not verified by the semantics. For similar reasons, we need a semantics for **Pd**. One solution is the "possible world" semantics of Kripke [1965]. An earlier solution found by Beth [1956, 1959] is discussed in Chapter 13 of Troelstra and van Dalen [1988]. We turn now to Kripke's semantics, giving first a simplified version for **Pp** and then the full interpretation for **Pd**.

3.1 Kripke Semantics for Pp

We first provide a Kripke semantics, based on finite rooted trees, with respect to which **Pp** is *sound* and *complete.* Using the decidability of **Pp**, this interpretation is constructive. From the classical viewpoint, on the other hand, the decidability of **Pp** is an easy corollary of the Kripke completeness theorem. Compactness considerations lead to a simple version of Kripke's interpretation for a language with finitely many symbols.

Definition. If E is a formula of $\mathcal{L}(\mathbf{Pp})$, then $\mathbf{sf}(E)$ is the (finite) set of all subformulas of E, including E itself. If Γ is a class of formulas of $\mathcal{L}(\mathbf{Pp})$, then $\mathbf{sf}(\Gamma)$ is the union of the sets $\mathbf{sf}(E)$ for all $E \in \Gamma$. The subset of $\mathbf{sf}(E)$ consisting of all *prime* subformulas of E is $\mathbf{psf}(E)$, and similarly for Γ. A class Δ of formulas of $\mathcal{L}(\mathbf{Pp})$ is *closed under subformulas* if $\mathbf{sf}(\Delta) \subseteq \Delta$.

Definition. A *tree* T is a set of finite sequences of natural numbers such that the *empty sequence* $\langle\ \rangle \in \mathrm{T}$, and if $\langle n_1, \ldots, n_{k+1}\rangle \in \mathrm{T}$ then $\langle n_1, \ldots, n_k\rangle \in \mathrm{T}$. In the second case, $\langle n_1, \ldots, n_k\rangle$ is called the *immediate predecessor of* $\langle n_1, \ldots, n_{k+1}\rangle$ in T, and $\langle n_1, \ldots, n_{k+1}\rangle$ is an *immediate successor of* $\langle n_1, \ldots, n_k\rangle$ in T. More generally, for each $i \leq k$, $\langle n_1, \ldots, n_i\rangle$ is a *predecessor of* $\langle n_1, \ldots, n_{k+1}\rangle$ in T and $\langle n_1, \ldots, n_{k+1}\rangle$ is a *successor of* $\langle n_1, \ldots, n_k\rangle$.

The elements of a tree are called *nodes.* A node which has no immediate successors (hence no successors) in T is a *leaf* of T, and $\langle\ \rangle$ is the *root.*

A tree T is *finitary* or *finitely splitting* if each $\langle n_1, \ldots, n_k\rangle \in \mathrm{T}$ has only finitely many immediate successors in T (possibly none). Note that a finitary tree may be finite or infinite.

We may use $w, u, v, w_1, \ldots$ as metavariables for finite sequences of natural numbers. If $k, l \geq 0$ and $n_1, \ldots, n_k, m_1, \ldots, m_l$ are natural numbers, the *concatenation* of $\langle n_1, \ldots, n_k\rangle$ with $\langle m_1, \ldots, m_l\rangle$ is

$$\langle n_1, \ldots, n_k\rangle * \langle m_1, \ldots, m_l\rangle = \langle n_1, \ldots, n_k, m_1, \ldots, m_l\rangle.$$

Using this notation, a tree is a set T of finite sequences of natural numbers such that $\langle\ \rangle \in \mathrm{T}$ and, for each w and n, if $w * \langle n\rangle \in \mathrm{T}$ then $w \in \mathrm{T}$. The tree is finitely splitting if for each $w \in \mathrm{T}$ there are only finitely many n (perhaps none) such that $w * \langle n\rangle \in \mathrm{T}$.

Note. Sometimes it is useful to interpret $\langle n_1, \ldots, n_k\rangle$ as a primitive recursive code for the sequence $n_1, \ldots, n_k$, for example

$$\langle n_1, \ldots, n_k\rangle \ = \ p_1^{n_1+1} \cdot \ldots \cdot p_k^{n_k+1}$$

where p_i is the ith prime, counting 2 as the first. Then if w and u code sequences, $w * u$ codes their concatenation.

Definition. A *propositional Kripke model* $\mathcal{K}$ *over* a finite list $P_1, \ldots, P_n$ of proposition letters is a pair

$$\mathcal{K} \ = \ ((\mathrm{K}, \leq), \kappa)$$

where K is a tree, $\leq$ is the partial ordering of the nodes of K determined by

$$u \leq v \ \text{ if and only if } u = v \text{ or } u \text{ is a predecessor of } v,$$

and κ is a function from K to the set of all subsets of $\{P_1, \ldots, P_n\}$ such that if $\langle x_1, \ldots, x_{j+1}\rangle \in \mathrm{K}$ then $\kappa(\langle x_1, \ldots, x_j\rangle) \subseteq \kappa\ (\langle x_1, \ldots, x_{j+1}\rangle)$.

The *forcing relation* $\Vdash$ on $\mathcal{K}$ is completely determined by κ and the structure of $(\mathrm{K},\leq)$. If $u \in \mathrm{K}$ and E is a formula such that $\mathbf{psf}(E) \subseteq \{P_1, \ldots, P_n\}$, then $u \Vdash E$ is defined as follows by induction on the logical form of E. (As always, the defined relation $\Vdash$ is the least fixed point of the induction.)

1. If E is prime, then $u \Vdash E$ if (and only if) $E \in \kappa(u)$.
2. $u \Vdash (A \,\&\, B)$ if $u \Vdash A$ and $u \Vdash B$.
3. $u \Vdash (A \vee B)$ if $u \Vdash A$ or $u \Vdash B$.
4. $u \Vdash (A \to B)$ if, for each $v \in \mathrm{K}$ with $u \leq v$: if $v \Vdash A$ then $v \Vdash B$.
5. $u \Vdash (\neg A)$ if, for each $v \in \mathrm{K}$ with $u \leq v$, it is *not* the case that $v \Vdash A$.

Lemma 3.1. (**Monotonicity**) If $\mathcal{K} = ((\mathrm{K},\leq),\kappa)$ is a propositional Kripke model over $P_1, \ldots, P_n$, and E is a formula with $\mathbf{psf}(E) \subseteq \{P_1, \ldots, P_n\}$, then for each $u, v \in \mathrm{K}$:

$$\text{if } u \Vdash E \text{ and } u \leq v \text{ then } v \Vdash E.$$

Exercise 3.1. Prove Lemma 3.1 by induction on the logical form of E.

Remark. By monotonicity, if $\langle\,\rangle \Vdash E$ then $u \Vdash E$ for every $u \in \mathrm{K}$. We say E is *valid in* $\mathcal{K}$, and write $\mathcal{K} \Vdash E$, if $\langle\,\rangle \Vdash E$.

Theorem 3.2. (**Soundness for Pp**) If E is a formula such that $\vdash_{\mathbf{Pp}} E$ by a proof $F_1, \ldots, F_m$ such that $\mathbf{psf}(F_i) \subseteq \{P_1, \ldots, P_n\}$ for each $i = 1, \ldots, m$, then for every propositional Kripke model $\mathcal{K}$ over $\{P_1, \ldots, P_n\}$: $\mathcal{K} \Vdash E$.

Proof, by complete induction on the length m of $F_1, \ldots, F_m$, where F_m is E. If $m = 1$ then E is an axiom of **Pp**. For example, if E is $A \to (B \to A)$ by X1, then for every $u \in \mathrm{K}$: if $u \Vdash A$ and $u \leq v$, then (whether or not $v \Vdash B$) also $v \Vdash A$ by monotonicity. The arguments for X2 and X3 also use monotonicity. Axiom schemas X4-X7 need only the definition of $\Vdash$. For X8, if $u \leq v \in \mathrm{K}$ and $u \Vdash (A \to C)$ and $v \Vdash (B \to C)$, then for every $w \in \mathrm{K}$ with $v \leq w$ such that $w \Vdash (A \vee B)$:
(a) $w \Vdash (A \to C)$ and $w \Vdash (B \to C)$ by monotonicity, and
(b) $w \Vdash A$ or $w \Vdash B$, so in either case
(c) $w \Vdash C$.
For X10, if $u \Vdash \neg A$ and $u \leq v \in \mathrm{K}$, then $v \nVdash A$ and so $u \Vdash (A \to B)$ vacuously.

If $m > 1$ and E is not an axiom of **Pp**, then E follows by R1 from two earlier formulas F_i, F_j where F_i is $(F_j \to E)$. By the induction hypothesis, $\langle\,\rangle \Vdash F_i$ and $\langle\,\rangle \Vdash F_j$, so by the definition of $\Vdash$ clearly $\langle\,\rangle \Vdash E$.

Exercise 3.2. Argue the case for X9 in the proof of Theorem 3.2.

Soundness gives us a way to show that a formula E is unprovable in **Pp**, by providing a *Kripke countermodel* (a Kripke model $\mathcal{K}$ over $\mathbf{psf}(E)$ such that $\mathcal{K} \nVdash E$). Completeness (the next theorem) will guarantee that every unprovable formula of **Pp** has such a countermodel.

Example. Here is a two-node Kripke countermodel $\mathcal{K}_1$ to $(P_1 \vee \neg P_1)$. Let $\mathrm{K}_1 = \{\langle\,\rangle, \langle\, 0 \,\rangle\}$, let $\kappa_1(\langle\, 0 \,\rangle) = \{P_1\}$ and $\kappa_1(\langle\,\rangle) = \emptyset$. Then $\langle\,\rangle \nVdash P_1$, but also $\langle\,\rangle \nVdash \neg P_1$ since $\langle\,\rangle \leq \langle\, 0 \,\rangle \in \mathrm{K}_1$ and $\langle\, 0 \,\rangle \Vdash P_1$. Note that this is also a countermodel to $\neg\neg P_1 \to P_1$, showing that the converse of Theorem 2.5(b) is unprovable in **Pp**.

Example. Let $\mathcal{K}_2 = ((\mathrm{K}_2,\leq),\kappa_2)$ where $\mathrm{K}_2 = \mathrm{K}_1 = \{\langle\,\rangle, \langle\, 0 \,\rangle\}$, but now $\kappa_2(\langle\, 0 \,\rangle) = \{P_1, P_2\}$ and $\kappa_2(\langle\,\rangle) = \{P_1\}$. Then $\mathcal{K}_2$ is a Kripke countermodel to $\neg(P_1 \,\&\, \neg P_2) \to (P_1 \to P_2)$, showing that the converse of Theorem 2.5(g) is unprovable in **Pp**.

Example. A three-node countermodel to $(P_1 \to (P_2 \vee P_3)) \to (P_1 \to P_2) \vee (P_1 \to P_3)$ is $\mathcal{K}_3 = ((\mathrm{K}_3,\leq),\kappa_3)$ where $\mathrm{K}_3 = \{\langle\,\rangle, \langle\, 0 \,\rangle \langle\, 1 \,\rangle\}$ and $\kappa_3(\langle\,\rangle) = \emptyset$, $\kappa_3(\langle\, 0 \,\rangle) = \{P_1, P_2\}$ and $\kappa_3(\langle\, 1 \,\rangle) = \{P_1, P_3\}$.

Exercise 3.3. Provide a Kripke countermodel for a formula of the form $(\neg B \to \neg A) \to (A \to B)$, showing that the converse of Theorem 2.5(a) is unprovable in **Pp**.

Exercise 3.4. Show that the converse of Theorem 2.5(f) is unprovable in **Pp**.

Definition. If Γ, Δ are collections of formulas of $\mathcal{L}(\mathbf{Pp})$, then Γ is Δ-*saturated* if

(i) Γ is consistent.

(ii) $\Gamma \subseteq \Delta$.

(iii) If $A, B \in \Delta$ and $\Gamma \vdash_{\mathbf{Pp}} (A \vee B)$ then $A \in \Gamma$ or $B \in \Gamma$.

Note that if Γ is a Δ-saturated collection of formulas and $\Gamma \vdash_{\mathbf{Pp}} A$ where $A \in \Delta$, then $A \in \Gamma$ by (iii) with $B = A$. Thus every Δ-saturated set is a deductively closed subset of Δ.

Lemma 3.3. (**Saturation Lemma for Pp**)

(a) If E is a formula of $\mathcal{L}(\mathbf{Pp})$ such that $\not\vdash_{\mathbf{Pp}} E$, then there is a (finite) $\Gamma_0 \subseteq \mathbf{sf}(E)$ such that Γ_0 is $\mathbf{sf}(E)$-saturated and $\Gamma_0 \not\vdash_{\mathbf{Pp}} E$.

(b) If E is a formula of $\mathcal{L}(\mathbf{Pp})$, and if $C \in \mathbf{sf}(E)$ and $\Delta \subseteq \mathbf{sf}(E)$ such that $\Delta \not\vdash_{\mathbf{Pp}} C$, then there is a (finite) $\Gamma \subseteq \mathbf{sf}(E)$ such that Γ is $\mathbf{sf}(E)$-saturated, $\Delta \subseteq \Gamma$, and $\Gamma \not\vdash_{\mathbf{Pp}} C$.

Proof of (a). List all the subformulas $F_1, \ldots, F_k$ of E (in any order, without repetitions). Consider F_1. If $F_1 \vdash_{\mathbf{Pp}} E$ define $\Gamma_0^1 = \emptyset$, and if $F_1 \not\vdash_{\mathbf{Pp}} E$ set $\Gamma_0^1 = \{F_1\}$.

Given Γ_0^i where $1 \leq i < k$, consider F_{i+1}. If $\Gamma_0^i \cup \{F_{i+1}\} \vdash_{\mathbf{Pp}} E$ define $\Gamma_0^{i+1} = \Gamma_0^i$, and if $\Gamma_0^i \cup \{F_{i+1}\} \not\vdash_{\mathbf{Pp}} E$ put $\Gamma_0^{i+1} = \Gamma_0^i \cup \{F_{i+1}\}$.

Finally, define $\Gamma_0 = \bigcup_{1 \leq i \leq k} \Gamma_0^i$. By construction with the assumption that E is unprovable, $\Gamma_0 \not\vdash_{\mathbf{Pp}} E$ and $\Gamma_0 \subseteq \mathbf{sf}(E)$, so (i) and (ii) of the definition of $\mathbf{sf}(E)$-saturated are satisfied.

For (iii), suppose $\Gamma_0 \vdash_{\mathbf{Pp}} (A \vee B)$ where $A, B \in \mathbf{sf}(E)$, but $A \notin \Gamma_0$ and $B \notin \Gamma_0$. Since both A, B appear in the list $F_1, \ldots, F_k$ but neither belongs to any Γ_0^i, it must be the case that $\Gamma_0 \cup \{A\} \vdash_{\mathbf{Pp}} E$ and $\Gamma_0 \cup \{B\} \vdash_{\mathbf{Pp}} E$. By $\vee$E (which holds for **Pp** as well as for **NPp** by Theorem 2.4): $\Gamma_0 \cup \{A \vee B\} \vdash_{\mathbf{Pp}} E$. But then $\Gamma_0 \vdash_{\mathbf{Pp}} E$, which is impossible.

Proof of (b). Similarly, except now $\Gamma^0 = \Delta$, and for $0 \leq i < k$: assuming $\Gamma^i \subseteq \mathbf{sf}(E)$ has been constructed so that $\Gamma^i \not\vdash_{\mathbf{Pp}} C$, consider F_{i+1}. If $\Gamma^i \cup \{F_{i+1}\} \vdash_{\mathbf{Pp}} C$, set $\Gamma^{i+1} = \Gamma^i$. Otherwise, set $\Gamma^{i+1} = \Gamma^i \cup \{F_{i+1}\}$. Define $\Gamma = \bigcup_{0 \leq i \leq k} \Gamma^i$.

By construction, $\Gamma \not\vdash_{\mathbf{Pp}} C$ and $\Delta \subseteq \Gamma \subseteq \mathbf{sf}(E)$. If $A, B \in \mathbf{sf}(E)$ and $\Gamma \vdash_{\mathbf{Pp}} A \vee B$, then not both $\Gamma \cup \{A\} \vdash_{\mathbf{Pp}} C$ and $\Gamma \cup \{B\} \vdash_{\mathbf{Pp}} C$, so since both A, B occur in the list $F_1, \ldots, F_k$ at least one of A, B must be a member of Γ. So Γ is $\mathbf{sf}(E)$-saturated.

Remark. Lemma 3.3 holds constructively because the relation $\{C_1, \ldots, C_j\} \vdash_{\mathbf{Pp}} D$ is effectively decidable. Thus (iii) can be proved by constructive cases: either $\Gamma_0 \cup \{A\} \vdash_{\mathbf{Pp}} E$, or $\Gamma_0 \cup \{B\} \vdash_{\mathbf{Pp}} E$, or neither holds (so both $A, B \in \Gamma_0$ by construction). The (classical) decidability of the relation $\vdash_{\mathbf{Pp}}$ can also be deduced from (the proof of) the following theorem.

Theorem 3.4. (**Completeness of Pp**) If E is any formula of $\mathcal{L}(\mathbf{Pp})$ such that $\not\vdash_{\mathbf{Pp}} E$, then E has a propositional Kripke countermodel.

Proof. Assume $\not\vdash_{\mathbf{Pp}} E$, and let Γ_0 be an $\mathbf{sf}(E)$-saturated subset of $\mathbf{sf}(E)$ given by Lemma 3.3(a). Let $\Gamma_1, \ldots, \Gamma_m$ be a list (without repetitions) of all the $\mathbf{sf}(E)$-saturated subsets of $\mathbf{sf}(E)$ such that $\Gamma_0 \subsetneq \Gamma_i$ for $1 \leq i \leq m$. Let K be the set of all sequences $\langle i_1, \ldots, i_n \rangle$ such that for $1 \leq j \leq n$: $1 \leq i_j \leq m$, and for $1 \leq j < n$: $\Gamma_{i_j} \subsetneq \Gamma_{i_{j+1}}$. Then K is a rooted finite tree with root $\langle\ \rangle$ (the empty sequence) representing Γ_0, and each node $u = \langle i_1, \ldots, i_n \rangle$ above $\langle\ \rangle$ represents an increasing sequence $\langle \Gamma_{i_1}, \ldots, \Gamma_{i_n} \rangle$ of $\mathbf{sf}(E)$-saturated supersets of Γ_0, with every possible such sequence included. We say that Γ_0 is *attached to* the root $\langle\ \rangle$, and Γ_{i_n} is *attached to* the node $\langle i_1, \ldots, i_n \rangle$ if $n \geq 1$.

We want to show that $\mathcal{K} = ((K, \leq), \kappa)$ is a Kripke countermodel to E, where $\kappa(\langle\ \rangle) = \Gamma_0 \cap \mathbf{psf}(E)$ and for each $n \geq 1$ and each $\langle i_1, \ldots, i_n \rangle \in$ K:

$$\kappa(\langle i_1, \ldots, i_n \rangle) = \Gamma_{i_n} \cap \mathbf{psf}(E).$$

The proof depends on the fact that each node forces exactly those subformulas of E which belong to the $\mathbf{sf}(E)$-saturated set attached to the node.

Claim. For each node $u = \langle i_1, \ldots, i_n \rangle$ of K, representing the increasing sequence $\langle \Gamma_{i_0}, \Gamma_{i_1}, \ldots, \Gamma_{i_n} \rangle$ of $\mathbf{sf}(E)$-saturated sets with $\Gamma_{i_0} = \Gamma_0$, and for each subformula C of E:

$$u \Vdash C \text{ if and only if } C \in \Gamma_{i_n}.$$

Exercise 3.5.* Prove this claim, and use it to complete the proof of Theorem 3.4. [*Hint.* For the case that C is $(A \to B)$ you will need Lemma 3.3(b). Note also that n may be 0, and then $u = \langle \, \rangle$.]

3.2 Consequences of the Kripke Soundness and Completeness of Pp

Theorem 3.5. For any distinct prime formulas P, Q, R of $\mathcal{L}(\mathbf{Pp})$, the following classically provable formulas are unprovable in **Pp**:

(a) $P \vee \neg P$.
(b) $\neg P \vee \neg\neg P$.
(c) $\neg\neg P \to P$.
(d) $(P \to Q) \to (\neg P \vee Q)$.
(e) $\neg(P \,\&\, \neg Q) \to (P \to Q)$.
(f) $\neg(P \,\&\, Q) \to (\neg P \vee \neg Q)$.
(g) $(\neg P \to \neg Q) \to (Q \to P)$.
(h) $(P \to Q \vee R) \to (P \to Q) \vee (P \to R)$.
(i) $(\neg P \to Q \vee R) \to (\neg P \to Q) \vee (\neg P \to R)$.
(j) $((P \to Q) \to P) \to P$ (Peirce's Law).

Proofs. Using Theorem 3.2 (Soundness), it will suffice to give a Kripke countermodel to each formula. Countermodels $\mathcal{K}_1$, $\mathcal{K}_2$ and $\mathcal{K}_3$ to (particular instances of) (a), (e) and (h) were given as examples in the previous subsection, while Exercises 3.3 and 3.4 asked for counterexamples to (g) and (d). Only (b), (c), (f), (i) and (j) remain.

The two-node countermodel $\mathcal{K}_1$ to (a) also works for (c). For a countermodel to (b), let $\mathcal{K}_4 = ((\mathrm{K}_4, \leq), \kappa_4)$ where $\mathrm{K}_4 = \mathrm{K}_3 = \{\langle \, \rangle, \langle \, 0 \, \rangle \langle \, 1 \, \rangle\}$ and $\kappa_4(\langle \, \rangle) = \kappa_4(\langle \, 0 \, \rangle) = \emptyset$, $\kappa_4(\langle \, 1 \, \rangle) = \langle P \rangle$. We leave the rest as exercises for the reader.

Exercise 3.6. Construct Kripke countermodels to (f), (i) and (j) of Theorem 3.5.

Without using the (recursive) decidability of **Pp**, we can deduce it from Theorems 3.2 and 3.4 as follows. The last sentence of the proof uses Markov's Principle, to be discussed in a later section.

Theorem 3.6. (**Decidability of Intuitionistic Propositional Logic Pp**) There is an effective (recursive) procedure for deciding, given a formula E of $\mathcal{L}(\mathbf{Pp})$, whether or not $\vdash_{\mathbf{Pp}} E$.

Proof. Given a formula E of $\mathcal{L}(\mathbf{Pp})$, there are only finitely many distinct subsets $\Delta_0, \ldots, \Delta_m$ of $\mathbf{sf}(E)$ (where $\Delta_0 = \emptyset$), and they are partially ordered by $\subseteq$. For each $0 \leq j \leq m$ there are only finitely many $\mathcal{H}^j \subseteq \{\Delta_0, \ldots, \Delta_m\}$ such that

(i) $\Delta_j \in \mathcal{H}^j$, and

(ii) $\Delta_j \subseteq \Delta_i$ for every $\Delta_i \in \mathcal{H}^j$.

Each such $\mathcal{H}^j$ can be completely described by a finite tree H^j whose root $\langle \, \rangle$ represents Δ_j, where $\langle i_1, \ldots, i_n \rangle \in \mathrm{H}^j$ if and only if $\Delta_{i_1}, \ldots, \Delta_{i_n} \in \mathcal{H}^j$ and $\Delta_j \subsetneq \Delta_{i_i} \subsetneq \ldots \subsetneq \Delta_{i_n}$. Let H^j_1, H^j_2,..., $\mathrm{H}^j_{k_j}$ be all the trees of this kind, with root representing Δ_j. Define $\kappa^j(\langle \, \rangle) = \Delta_j \cap \mathbf{psf}(E)$ and for $n > 0$ define $\kappa^j(\langle i_1, \ldots, i_n \rangle) = \Delta_{i_n} \cap \mathbf{psf}(E)$. Then for each $1 \leq j \leq m$, for each $1 \leq l \leq k_j$, the structure $\mathcal{H}^j_l = ((\mathrm{H}^j_l, \leq), \ \kappa^j)$ is a propositional Kripke model over $\mathbf{psf}(E)$. By the proof of Theorem 3.4, if $\nvdash_{\mathbf{Pp}} E$ then some $\mathcal{H}^j_l$ is a countermodel to E.

To check whether a given H^j_l is a countermodel to E, one needs to check finitely many forcing conditions over a finite tree, and this can be done effectively. There are only finitely many H^j_l to check. If some H^j_l is a countermodel to E, then $\nvdash_{\mathbf{Pp}} E$ by Theorem 3.2. Otherwise, $\vdash_{\mathbf{Pp}} E$, and a proof of E can be found by recursively enumerating all the proofs in **Pp**.

Theorem 3.7. For all formulas A, B, C of $\mathcal{L}(\mathbf{Pp})$:

(a) If $\vdash_{\mathbf{Pp}} (A \vee B)$, then $\vdash_{\mathbf{Pp}} A$ or $\vdash_{\mathbf{Pp}} B$.

(b) If $\vdash_{\mathbf{Pp}} (\neg A \rightarrow B \vee C)$, then $\vdash_{\mathbf{Pp}} (\neg A \rightarrow B) \vee (\neg A \rightarrow C)$.

Proof of (a). We show that if $\nvdash_{\mathbf{Pp}} A$ and $\nvdash_{\mathbf{Pp}} B$ then $\nvdash_{\mathbf{Pp}} (A \vee B)$. Theorem 3.6 (which is constructive except for the use of Markov's Principle) then justifies (a).

Assume $\nvdash_{\mathbf{Pp}} A$ and $\nvdash_{\mathbf{Pp}} B$. By Theorem 3.4, there are propositional Kripke countermodels $\mathcal{K}_1 = ((\mathrm{K}_1, \leq), \kappa_1)$ to A and $\mathcal{K}_2 = ((\mathrm{K}_2, \leq), \kappa_2)$ to B. Construct a new model $\mathcal{K} = ((\mathrm{K}, \leq), \kappa)$ as follows. The elements of K will be $\langle\ \rangle$ and all sequences of the forms $\langle 1 \rangle * u$ where $u \in \mathrm{K}_1$, and $\langle 2 \rangle * u$ where $u \in \mathrm{K}_2$. $\kappa(\langle\ \rangle)$ will be the intersection of $\kappa_1(\langle\ \rangle)$ with $\kappa_2(\langle\ \rangle)$, and $\kappa(\langle i \rangle * u) = \kappa_i(u)$ for $i = 1, 2$. Then $\mathcal{K}$ is a propositional Kripke countermodel to $A \vee B$.

*Exercise 3.7**. Prove Theorem 3.7(b).

3.3 Kripke Semantics for Pd

Definition. Let $R_1, \ldots, R_s$ be any distinct predicate letters of $\mathcal{L}(\mathbf{Pd})$, where R_i is n_i-ary $(1 \leq i \leq s)$. A *Kripke model* $\mathcal{K}$ *over* $R_1, \ldots, R_s$ is an $(s+3)$-tuple

$$\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{D}, \delta, \chi_1, \ldots, \chi_s)$$

where K is a tree, $\leq$ is the partial ordering of the nodes of K determined by

$$u \leq v \text{ if and only if } u = v \text{ or } u \text{ is a predecessor of } v,$$

D is a countable set with at least one element, δ is a function with domain K such that

(i) for each $u \in \mathrm{K}$ there is at least one $d \in \delta(u)$, and

(ii) if $u, v \in \mathrm{K}$ with $u \leq v$ then $\delta(u) \subseteq \delta(v) \subseteq \mathrm{D}$,

and for each $1 \leq i \leq s$: χ_i is an $(n_i + 1)$-ary function from $K \times \mathrm{D}^{n_i}$ to $\{0, 1\}$ such that for $u, v \in \mathrm{K}$ and all $x_i, \ldots, x_{n_i} \in \mathrm{D}$:

(iii) if $\chi_i(u, x_1, \ldots, x_{n_i}) = 1$ then $x_1, \ldots, x_{n_i} \in \delta(u)$, and

(iv) if $u \leq v$ and $\chi_i(u, x_1, \ldots, x_{n_i}) = 1$ then $\chi_i(v, x_1, \ldots, x_{n_i}) = 1$.

Remarks. There are good reasons for using characteristic functions χ_i instead of $(n_i + 1)$-ary relations to interpret the R_i. Most obviously, 0-ary relation symbols and $(k+1)$-ary relation symbols are interpreted in a uniform way. And from the constructive point of view, since (K and D are countable and) $\{0, 1\}$ is finite, the question whether $\chi_i(u, x_1, \ldots, x_{n_i}) = 0$ or 1 may be assumed to be effectively decidable, while arbitrary relations on countable sets may not be. Conditions (ii) and (iv) of the definition are the *monotonicity* requirements for a Kripke model over a predicate language with finitely many relation symbols; and D is the *domain* of the model.

Definition. If $\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{D}, \delta, \chi_1, \ldots, \chi_s)$ is a Kripke model over $R_1, \ldots, R_s$, then every function ϕ from $\{a_1, a_2, \ldots\}$ to D is a possible *assignment of values in* D to the distinct individual variables $a_1, a_2, \ldots$ of $\mathcal{L}(\mathbf{Pd})$. Each such assignment determines a *forcing relation* $\Vdash_\phi$ on $\mathcal{K}$, as follows.

Let $\mathcal{L}'(\mathbf{Pd})$ be the sublanguage of $\mathcal{L}(\mathbf{Pd})$ with only the distinct predicate letters $R_1, \ldots, R_s$ (but with all the individual variables $a_1, a_2, \ldots$). For each formula E in $\mathcal{L}'(\mathbf{Pd})$ and each $u \in \mathrm{K}$, we define $u \Vdash_\phi E$ by induction on the logical form of E.

1. If E is prime, E is $R_i(y_1, \ldots, y_{n_i})$ for some $1 \leq i \leq s$, where $y_1, \ldots, y_{n_i}$ are (not necessarily distinct) individual variables. Then $u \Vdash_\phi R_i(y_1, \ldots, y_{n_i})$ if (and only if) $\chi_i(u, \phi(y_1), \ldots, \phi(y_{n_i})) = 1$.

2. $u \Vdash_\phi (A \mathbin{\&} B)$ if $u \Vdash_\phi A$ and $u \Vdash_\phi B$.

3. $u \Vdash_\phi (A \vee B)$ if $\phi(y) \in \delta(u)$ for every variable y free in $(A \vee B)$, and $u \Vdash_\phi A$ or $u \Vdash_\phi B$.

4. $u \Vdash_\phi (A \to B)$ if $\phi(y) \in \delta(u)$ for every variable y free in $(A \to B)$, and for each $v \in \mathrm{K}$ with $u \leq v$: if $v \Vdash_\phi A$ then $v \Vdash_\phi B$.

5. $u \Vdash_\phi (\neg A)$ if $\phi(y) \in \delta(u)$ for every variable y free in A, and for each $v \in \mathrm{K}$ with $u \leq v$, it is *not* the case that $v \Vdash_\phi A$.

6. $u \Vdash_\phi \forall x A(x)$ if, for each $v \in \mathrm{K}$ with $u \leq v$ and every assignment ψ to the individual variables such that $\psi(x) \in \delta(v)$ and $\psi(y) = \phi(y)$ for every $y \neq x$: $v \Vdash_\psi A(x)$.

7. $u \Vdash_\phi \exists x A(x)$ if, for some assignment ψ to the individual variables which agrees with ϕ on all variables other than x: $u \Vdash_\psi A(x)$.

Exercise 3.8. Prove that if $u \Vdash_\phi E$ then $\phi(y) \in \delta(u)$ for every variable y free in E.

Exercise 3.9. Show that if ϕ and ψ are assignments which agree on all the variables free in E, then $u \Vdash_\phi E$ if and only if $u \Vdash_\psi E$.

Lemma 3.8. (**Monotonicity**) If $\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{D}, \delta, \chi_1, \ldots, \chi_s)$ is a Kripke model over $R_1, \ldots, R_s$, then for every formula E in the restricted language $\mathcal{L}'(\mathbf{Pd})$ with only the predicate letters $R_1, \ldots, R_s$, and every assignment ϕ of elements of D to the individual variables, for each $u, v \in \mathrm{K}$:

$$\text{if } \ u \Vdash_\phi E \ \text{ and } \ u \leq v \ \text{ then } v \Vdash_\phi E.$$

Proof, by induction on the logical form of E. If E is prime, monotonicity is guaranteed by (iv) of the definition. Cases 2 - 5 are like those for Lemma 3.1, using (ii) of the definition with Exercise 3.8.

Case 6. E is $\forall x A(x)$ where the induction hypothesis holds for $A(x)$. Assume $u, v \in \mathrm{K}$ with $u \leq v$, and $u \Vdash_\phi \forall x A(x)$. Suppose $w \in \mathrm{K}$ and $v \leq w$, and let ψ be any assignment such that $\psi(x) \in \delta(w)$ and $\psi(y) = \phi(y)$ for all $y \neq x$. Then $w \Vdash_\psi A(x)$ since $u \leq v \leq w$. So $v \Vdash_\phi \forall x A(x)$.

Case 7. E is $\exists x A(x)$ where the induction hypothesis holds for $A(x)$. Assume $u \leq v$ in K and $u \Vdash_\phi \exists x A(x)$, so there is an assignment ψ which agrees with ϕ on all variables other than x and satisfies $\psi(x) \in \delta(u)$ and $u \Vdash_\psi A(x)$. But then $v \Vdash_\psi A(x)$ by the induction hypothesis, and $\psi(x) \in \delta(v)$ by (ii) of the definition, so $v \Vdash_\phi \exists x A(x)$.

Definition. If $R_1, \ldots, R_s$ are distinct predicate letters including all those which occur in a formula E of $\mathcal{L}(\mathbf{Pd})$, and $\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{D}, \delta, \chi_1, \ldots, \chi_s)$ over $R_1, \ldots, R_s$ is a Kripke model over $R_1, \ldots, R_s$, then E is *valid in* $\mathcal{K}$ (written $\mathcal{K} \Vdash E$) if $\langle\, \rangle \Vdash_\phi E$ for every assignment ϕ of elements of D to the individual variables which assigns elements of $\delta(\langle\, \rangle)$ to all the variables free in E. If E is valid in *every* Kripke model over $R_1, \ldots, R_s$ then E is *Kripke-valid* (written $\Vdash E$).

Theorem 3.9. (**Soundness for Pd**) If E is a formula of $\mathcal{L}(\mathbf{Pd})$ such that $\vdash_{\mathbf{Pd}} E$ by a proof $F_1, \ldots, F_m$ in which no predicate letters but $R_1, \ldots, R_s$ may occur, then the universal closure $\forall E$ of E is valid in every Kripke model $\mathcal{K}$ over $R_1, \ldots, R_s$. Hence

$$\text{if } \ \vdash_{\mathbf{Pd}} E \ \text{ then } \ \Vdash E,$$

since the question whether $\mathcal{K} \Vdash E$ depends only on the interpretations of the predicate letters which actually occur in E.

Proof, by complete induction on the length m of $F_1, \ldots, F_m$, where F_m is E. Let $\mathcal{K}$ be a Kripke model over a list $R_1, \ldots, R_s$ of distinct predicate letters including all those occurring in $F_1, \ldots, F_m$. We must show that $\langle\, \rangle \Vdash_\phi \forall E$ for every assignment ϕ of elements of D to the individual variables, or equivalently that $u \Vdash_\phi E$ for every $u \in \mathrm{K}$ and every assignment ϕ such that

$$(\star): \quad \phi(y) \in \delta(u) \ \text{ for every } \ y \ \text{ free in } \ E.$$

If $m = 1$ then E is an axiom of **Pd**. The arguments for X1 - X10 are as for **Pp**. If E is an axiom by X11 then E is $\forall x A(x) \to A(y)$ where y is a variable free for x in $A(x)$. Suppose $u \in \mathrm{K}$, and ϕ is an assignment to the individual variables satisfying ($\star$) such that $u \Vdash_\phi \forall x A(x)$. Then if x is free in $A(x)$, $\phi(y) \in \delta(u)$ by ($\star$), and so $u \Vdash_\phi A(y)$. If x is not free in $A(x)$ then $A(y)$ is $A(x)$, and $u \Vdash_\phi A(x)$. In either case, $\forall E$ is valid in $\mathcal{K}$.

If E is an axiom by X12 then E is $A(y) \to \exists x A(x)$ where y is a variable free for x in $A(x)$. If x is free in $A(x)$ then y is free in $\exists x A(x)$ unless y is x. Hence, if $u \in \mathrm{K}$ and ϕ is an assignment to the individual variables satisfying ($\star$) such that $u \Vdash_\phi A(y)$, then either $u \Vdash_\phi \exists x A(x)$ (if $y = x$, for example, or if x is not free in $A(x)$), or by defining $\psi(x) = \phi(y)$ and letting ψ agree with ϕ on all the variables free in $\exists x A(x)$ we have $u \Vdash_\psi A(x)$. Therefore $\forall E$ is valid in $\mathcal{K}$.

If $m > 1$ and E is not an axiom of **Pd**, then E follows by R1, R2 or R3 from one or two earlier lines in the proof. If E follows from F_i, F_j by R1, where F_i is $(F_j \to E)$, then $\forall F_i$ and $\forall F_j$ are valid in $\mathcal{K}$ by the induction hypothesis. If $u \in \mathrm{K}$ and ϕ is an assignment to the variables such that $\phi(y) \in \delta(u)$ for all y free in F_i, and if $u \Vdash_\phi F_j$, then $u \Vdash_\phi E$. Therefore $\forall E$ is valid in $\mathcal{K}$.

If E follows from some F_i with $i < m$ by R2, then F_i is of the form $C \to A(x)$ where x is not free in C, $\forall F_i$ is valid in $\mathcal{K}$ by the induction hypothesis, and E is $C \to \forall x A(x)$. Suppose $u \in \mathrm{K}$ and ϕ is an assignment of elements of D to the variables satisfying ($\star$), and suppose $u \Vdash_\phi C$. Then for every $v \in \mathrm{K}$ with $u \leq v$, and every ψ which agrees with ϕ on all $y \neq x$ and satisfies $\phi(x) \in \delta(v)$: $u \Vdash_\psi C$, so $v \Vdash_\psi C$ by monotonicity, and $v \Vdash_\psi F_i$ by the induction hypothesis, so $v \Vdash_\psi A(x)$. So $\forall E$ is valid in $\mathcal{K}$.

If E follows from some F_j with $j < m$ by R3, then F_j is of the form $A(x) \to C$ where x is not free in C, $\forall F_j$ is valid in $\mathcal{K}$, and E is $\exists x A(x) \to C$. If $u \in \mathrm{K}$ and ϕ satisfies ($\star$) and $u \Vdash_\phi \exists x A(x)$, then for some assignment ψ which agrees with ϕ on all variables other than x: $u \Vdash_\psi A(x)$, so $u \Vdash_\psi C$ by the induction hypothesis (noting that $\psi(y) \in \delta(u)$ for each y free in F_j). But then $u \Vdash_\phi C$ also, since x is not free in C.

Example. To show that the converse of Theorem 2.10(h) is unprovable in **Pd** we search for a Kripke countermodel $\mathcal{K}_1 = ((\mathrm{K}_1, \leq), \mathrm{D}, \delta, \chi_1, \chi_2)$ to $(P_1 \to \exists x P_2(x)) \to \exists x(P_1 \to P_2(x))$, where P_1 is a 0-ary predicate letter and $P_2(\cdot)$ is a unary predicate letter (and x may be any variable) of $\mathcal{L}(\mathbf{Pd})$. The underlying tree of the model is $\mathrm{K}_1 = \{\langle\ \rangle, \langle 0\rangle\}$ and the domain of individuals is $\mathrm{D} = \{d_0, d_1\}$, with domain function $\delta(\langle\ \rangle) = \{d_0\}$, $\delta(\langle 0\rangle) = \{d_0, d_1\}$. The representing functions of $P_1, P_2(\cdot)$ in the model are χ_1, χ_2 where

$$\chi_1(\langle\ \rangle) = 0, \quad \chi_1(\langle 0\rangle) = 1, \quad \chi_2(\langle\ \rangle, d_0) = \chi_2(\langle\ \rangle, d_1) = 0, \quad \chi_2(\langle 0\rangle, d_0) = 0, \quad \text{and} \quad \chi_2(\langle 0\rangle, d_1) = 1.$$

Then for any assignment ϕ to the variables: $\langle\ \rangle \Vdash_\phi (P_1 \to \exists x P_2(x))$ since $\langle\ \rangle \not\Vdash_\phi P_1$ and $\langle 0\rangle \Vdash_\phi \exists x P_2(x)$, but $\langle\ \rangle \not\Vdash_\phi \exists x(P_1 \to P_2(x))$ because the only *witness* d_1 for $\exists x P_2(x)$ at node $\langle 0\rangle$ does not belong to the universe $\delta(\langle\ \rangle)$ of the root $\langle\ \rangle$. So $\mathcal{K}_1 \not\Vdash (P_1 \to \exists x P_2(x)) \to \exists x(P_1 \to P_2(x))$.

Example. Here is a Kripke countermodel to $\forall x \neg\neg P_1(x) \to \neg\neg\forall x P_1(x)$, showing that this formula is unprovable in **Pd**. Let $\mathrm{D} = \{d_0, d_1, d_2, \ldots\}$ and let K be the tree consisting of all finite sequences of 0s (so $\mathrm{K} = \{\langle\ \rangle, \langle 0\rangle, \langle 0, 0\rangle, \ldots\}$). If u is a sequence of 0s of length n, define $\delta(u) = \{d_0, \ldots, d_n\}$ and define $\chi_1(u, d_i) = 1$ if and only if $i < n$. Thus

(a) $\leq$ linearly orders K, and

(b) $\chi_1(\langle\ \rangle, d_i) = 0$ for all i, and

(c) for each $u \in \mathrm{K}$ there is exactly one $d_i \in \delta(u)$ for which $\chi_1(u, d_i) = 0$, and

(d) for each $d_i \in \mathrm{D}$ there is some $u \in \mathrm{K}$ such that $\chi_1(u, d_i) = 1$.

Let ϕ be any assignment of elements of D to the individual variables. By (a) and (c), $u \Vdash_\phi \neg\forall x P_1(x)$ for every $u \in \mathrm{K}$. By (a) and (d), $u \Vdash_\phi \forall x \neg\neg P_1(x)$. Hence $\langle\ \rangle \not\Vdash_\phi \forall x \neg\neg P_1(x) \to \neg\neg\forall x P_1(x)$.

Exercise 3.10. Show that the converse of Theorem 2.10(g) is unprovable in **Pd** by constructing a Kripke countermodel to $(\forall x P_1(x) \to P_2) \to \exists x(P_1(x) \to P_2)$, where $P_1(\cdot)$ is a unary predicate letter and P_2 is 0-ary.

3.4 Digression: Kripke Models with Constant Domain

Definition. A Kripke model $\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{D}, \delta, \chi_1, \ldots, \chi_s)$ over $R_1, \ldots, R_s$ has *constant domain* D if $\delta(u) = \mathrm{D}$ for *every* $u \in \mathrm{K}$. In this case, we may write $\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{D}, \chi_1, \ldots, \chi_s)$ and the definition of $\Vdash_\phi$ can be simplified accordingly.

Exercise 3.11. Show that $\forall x(A(x) \vee B) \to \forall x A(x) \vee B$ is valid in every Kripke model with constant domain, assuming x is not free in B. (You may need to use classical reasoning in your proof.)

Exercise 3.12. Construct a Kripke countermodel to $\forall x(P_1(x) \vee P_2) \to \forall x P_1(x) \vee P_2$, where $P_1(\cdot)$ is unary and P_2 is 0-ary. (This shows that the converse of Theorem 2.10(a) is not provable in **Pd**.)

These two exercises suggest that Kripke models with increasing domains are needed to prove e.g. that $\not\vdash_{\mathbf{Pd}} \forall x(P_1(x) \vee P_2) \to \forall x P_1(x) \vee P_2$. A simple but clever observation by D. H. J. de Jongh (from an unpublished manuscript *circa* 1970) suggests otherwise. In effect, de Jongh noticed that the domain of a countable Kripke model over a finite list of predicate letters can be described using a "fresh" unary predicate letter of the language. Some definitions are needed here.

Definition. If $\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{D}, \delta, \chi_1, \ldots, \chi_s)$ is a Kripke model over $R_1, \ldots, R_s$ and $u \in \mathrm{K}$, then $\mathcal{K}^u = ((\mathrm{K}^u, \leq^u), \mathrm{D}, \delta^u, \chi_1^u, \ldots, \chi_s^u)$ is the *submodel of* $\mathcal{K}$ defined as follows:

$(\mathrm{i})^u$ for each finite sequence v of natural numbers, $v \in \mathrm{K}^u$ if and only if $u * v \in \mathrm{K}$,

$(\mathrm{ii})^u$ if $v, w \in \mathrm{K}^u$, then $v \leq^u w$ if and only if $u * v \leq u * w$ in K,

$(\mathrm{iii})^u$ if $v \in \mathrm{K}^u$ then $\delta^u(v) = \delta(u * v)$, and

$(\mathrm{iv})^u$ if $v \in \mathrm{K}^u$ then for each $1 \leq i \leq s$ and all $x_1, \ldots, x_{n_i} \in \mathrm{D}$:

$$\chi_i^u(v, x_1, \ldots, x_{n_i}) = \chi_i(u * v, x_1, \ldots, x_{n_i}).$$

It is easy to check that $\mathcal{K}^u$ is also a Kripke model over $R_1, \ldots, R_s$, and so each assignment ϕ of elements of D to the individual variables determines a forcing relation $\Vdash_\phi^u$ on $\mathcal{K}^u$.

Lemma 3.10. If $\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{D}, \delta, \chi_1, \ldots, \chi_s)$ is a Kripke model over $R_1, \ldots, R_s$ and $u \in \mathrm{K}$, then for each formula E of the restricted language, each assignment ϕ of elements of D to the individual variables, and each $v \in \mathrm{K}^u$: $v \Vdash_\phi^u E$ in $\mathcal{K}^u$ if and only if $u * v \Vdash_\phi E$ in $\mathcal{K}$.

Lemma 3.11. To each Kripke model $\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{D}, \delta, \chi_1, \ldots, \chi_s)$ over $R_1, \ldots, R_s$ there corresponds a constant-domain Kripke model $\mathcal{K}^+ = ((\mathrm{K}, \leq), \mathrm{D}, \chi_1, \ldots, \chi_s, \chi_{s+1})$ over $R_1, \ldots, R_s, P$ where $P(\cdot)$ is a unary predicate symbol distinct from all of $R_1, \ldots, R_s$, such that for each $u \in \mathrm{K}$ and each positive integer i: $\chi_{s+1}(u, a_i) = 1$ if and only if the i^{th} element of D belongs to $\delta(u)$. Then $\mathcal{K}$ and $\mathcal{K}^+$ are equivalent in the following sense:

$$u \Vdash_\phi E(y_1, \ldots, y_k) \text{ if and only if } u \Vdash_\phi^+ P(y_1) \mathbin{\&} \ldots \mathbin{\&} P(y_k) \mathbin{\&} E^P(y_1, \ldots, y_k)$$

for every assignment ϕ to $a_1, a_2, \ldots$, every $u \in \mathrm{K}$ and every formula $E(y_1, \ldots, y_k)$ (with exactly the distinct variables $y_1, \ldots, y_k$ free) of the language $\mathcal{L}'(\mathbf{Pd})$ restricted to $R_1, \ldots, R_s$, where $\Vdash_\phi^+$ is the forcing relation in $\mathcal{K}^+$ and E^P comes from E by restricting every quantifier to P (i.e. by simultaneously replacing every subformula of E of the form $\forall x A(x)$ by $\forall x(P(x) \to A(x))$, and every subformula of E of the form $\exists y B(y)$ by $\exists y(P(y) \mathbin{\&} B(y))$).

Theorem 3.12. (**de Jongh's Observation**) A closed formula E is Kripke-valid if and only if $\exists x P(x) \to E^P$ is valid in every Kripke model with constant domain, where $P(\cdot)$ is a unary predicate symbol not occurring in E.

Proof, assuming Lemmas 3.10 and 3.11. Suppose E is closed and $\exists x P(x) \to E^P$ is valid in every Kripke model with constant domain. Given any Kripke model $\mathcal{K}$ for the language of E, let $\mathcal{K}^+$ be the corresponding constant-domain model (for the language expanded by a new unary relation symbol $P(\cdot)$) defined in the statement of Lemma 3.11. Then for each assignment ϕ to the individual variables, $\langle\,\rangle \Vdash_\phi^+ (\exists x P(x) \to E^P)$ by assumption. Hence by Lemma 3.11, $\langle\,\rangle \Vdash_\phi E$. So E is Kripke-valid.

Conversely, suppose E is closed and Kripke-valid, and let $\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{D}, \chi_1, \ldots, \chi_s, \chi_{s+1})$ be a constant-domain Kripke model for the language of E expanded by one new unary relation symbol $P(\cdot)$, which is interpreted in the model by χ_{s+1}. Suppose $u \in \mathrm{K}$ and ϕ is an assignment to the individual variables such that $u \Vdash_\phi \exists x P(x)$ in $\mathcal{K}$. For each $v \in \mathrm{K}$ define $\delta(v) = \{d \in \mathrm{D} \mid \chi_{s+1}(v, d) = 1\}$. Then $\mathcal{K}^- = ((\mathrm{K}, \leq), \mathrm{D}, \delta, \chi_1, \ldots, \chi_s)$ is a Kripke model for the language of E, with a corresponding forcing relationship $\Vdash_\phi^-$, so by assumption E is valid in $\mathcal{K}^-$. In particular, $u \Vdash_\phi^- E$, so by Lemma 3.10: $\langle\ \rangle \Vdash_\phi^{-u} E$ in the submodel $(\mathcal{K}^-)^u$ of $\mathcal{K}^-$ determined by u. But then $\langle\ \rangle \Vdash_\phi^u \exists x P(x) \rightarrow E^P$ in the submodel $\mathcal{K}^u$ of $\mathcal{K}$ determined by u, by Lemma 3.11, since $(\mathcal{K}^-)^+$ is $\mathcal{K}$. So $u \Vdash_\phi \exists x P(x) \rightarrow E^P$ by Lemma 3.10. Hence $\exists x P(x) \rightarrow E^P$ is valid in every Kripke model with a constant domain.

3.5 Completeness of the Kripke Semantics for Pd

Saturation for $\mathcal{L}(\mathbf{Pd})$ concerns existential formulas as well as disjunctions, and "fresh" variables (or constants) will be needed as witnesses. Instead of expanding the language to provide these witnesses, we consider sublanguages of $\mathcal{L}(\mathbf{Pd})$, as follows. In general, a set is *inhabited* if it has an element. (From the constructive viewpoint, being inhabited is a stronger requirement than being nonempty.)

Definition. Let V_0 be an inhabited subset of the set $\mathrm{V} = \{a_1, a_2, \ldots\}$ of individual variables of $\mathcal{L}(\mathbf{Pd})$. Let $R_1, \ldots, R_s$ be any distinct predicate letters of $\mathcal{L}(\mathbf{Pd})$, where R_i is n_i-ary $(1 \leq i \leq s)$. Then $\mathcal{L}(\mathrm{V}_0, \{R_1, \ldots, R_s\})$ is the *sublanguage* of $\mathcal{L}(\mathbf{Pd})$ consisting of all formulas involving only variables from V_0 and relation symbols from $\{R_1, \ldots, R_s\}$.

Definition. Let $\mathrm{V}_0 \subseteq W \subseteq \mathrm{V}_1$ be inhabited subsets of V. Let $R_1, \ldots, R_s$ be any distinct predicate letters of $\mathcal{L}(\mathbf{Pd})$, where R_i is n_i-ary $(1 \leq i \leq s)$. For $j = 0, 1$ let $\mathcal{L}'(\mathrm{V}_j) = \mathcal{L}(\mathrm{V}_j, \{R_1, \ldots, R_s\})$. Then a collection Γ of formulas of $\mathcal{L}'(\mathrm{V}_1)$ is $\mathcal{L}'(\mathrm{V}_0)$-*saturated with witnesses in* W if

(i) Γ is consistent.

(ii) If $A \vee B$ is a formula of $\mathcal{L}'(\mathrm{V}_0)$ such that $\Gamma \vdash_{\mathbf{Pd}} A \vee B$ with all variables held constant, then $A \in \Gamma$ or $B \in \Gamma$.

(iii) If $\exists x A(x)$ is a formula of $\mathcal{L}'(\mathrm{V}_0)$ such that $\Gamma \vdash_{\mathbf{Pd}} \exists x A(x)$ with all variables held constant, then $A'(y) \in \Gamma$ for some formula $A'(x)$ of $\mathcal{L}'(\mathrm{V}_1)$ congruent to $A(x)$ and some $y \in \mathrm{W}$ which is free for x in $A'(x)$.

If $\mathrm{V}_0 = \mathrm{W} = \mathrm{V}_1$, so Γ is a collection of formulas of $\mathcal{L}'(\mathrm{V}_1)$ which is $\mathcal{L}'(\mathrm{V}_1)$-saturated with witnesses in V_1, we say Γ is $\mathcal{L}'(\mathrm{V}_1)$-*saturated.*

Convention. For the rest of this section, "$\Gamma \vdash E$" abbreviates "$\Gamma \vdash_{\mathbf{Pd}} E$ with all variables free in Γ held constant," and "$\Gamma \nvdash E$" abbreviates "there is no derivation of E from Γ in **Pd** with all variables held constant."

Exercise 3.13. Show that if Γ is an $\mathcal{L}'(\mathrm{V}_0)$-saturated collection of formulas of $\mathcal{L}'(\mathrm{V}_1)$ with witnesses in W (where $\mathrm{V}_0 \subseteq \mathrm{W} \subseteq \mathrm{V}_1$), and if E is a formula of $\mathcal{L}'(\mathrm{V}_0)$ which has a congruent E' in $\mathcal{L}'(\mathrm{V}_1)$ such that $\Gamma \vdash E'$, then $E \in \Gamma$. [Congruence is discussed in Section 2.7 of these notes.]

Exercise 3.14. Show that if Γ is an $\mathcal{L}'(\mathrm{V}_1)$-saturated collection of formulas of $\mathcal{L}'(\mathrm{V}_1)$, then for all formulas E, E' of $\mathcal{L}'(\mathrm{V}_1)$:

(a) $\Gamma \vdash E$ if and only if $E \in \Gamma$.

(b) If E and E' are congruent, then $E \in \Gamma$ if and only if $E' \in \Gamma$.

Lemma 3.13. (**Saturation Lemma for Pd**) Let $R_1, \ldots, R_s$ be distinct predicate letters of $\mathcal{L}(\mathbf{Pd})$, where R_i is n_i-ary. Let $\mathrm{V}_0 \subset \mathrm{V}_1 \subseteq \mathrm{V}$ where V_0 is inhabited and V_1 - V_0 is countably infinite, let $\mathcal{L}'(\mathrm{V}_j) = \mathcal{L}(\mathrm{V}_j, \{R_1, \ldots, R_s\})$ for $j = 0, 1$, and suppose C is a formula of $\mathcal{L}'(\mathrm{V}_0)$ and Δ a collection of formulas of $\mathcal{L}'(\mathrm{V}_0)$ such that $\Delta \nvdash C$. Then

(a) There is a $\Gamma \subseteq \mathcal{L}'(\mathrm{V}_1)$ which is $\mathcal{L}'(\mathrm{V}_0)$-saturated with witnesses in V_1, such that $\Delta \subseteq \Gamma$ and $\Gamma \nvdash C$.

(b) There is a $\Gamma^* \subseteq \mathcal{L}'(\mathrm{V}_1)$ which is $\mathcal{L}'(\mathrm{V}_1)$-saturated, such that $\Delta \subseteq \Gamma^*$ and $\Gamma^* \nvdash C$.

Proof of (a). Let $F_1, F_2, F_3, \ldots$ be an enumeration of the formulas of $\mathcal{L}'(\mathrm{V}_0)$ without repetition. Define an increasing sequence $\{\Gamma_i\}$ of consistent subsets of $\mathcal{L}'(\mathrm{V}_1)$ as follows. Let $\Gamma_0 = \Delta$, so $\Gamma_0 \nvdash C$ by assumption. If $i \geq 0$ and $\Gamma_i \subseteq \mathcal{L}'(\mathrm{V}_1)$ has already been defined such that $\Gamma_i \nvdash C$, consider F_{i+1} and define Γ_{i+1} by cases:

Case 1. $\Gamma_i \cup \{F_{i+1}\} \vdash C$. Then $\Gamma_{i+1} = \Gamma_i$.

Case 2. $\Gamma_i \cup \{F_{i+1}\} \nvdash C$, and F_{i+1} is of the form $\exists x A(x)$. Then $\Gamma_{i+1} = \Gamma_i \cup \{F_{i+1}, A(y)\}$ where y is the first variable in V_1 which is free for x in $A(x)$ and does not occur free in $\Gamma_i \cup \{F_{i+1}\}$ or in C. Observe that if $\Gamma_{i+1} \vdash C$, then $\Gamma_i \cup \{F_{i+1}\} \vdash A(y) \to C$ by the Deduction Theorem for **Pd**, so $\Gamma_i \cup \{F_{i+1}\} \vdash \exists y A(y) \to C$ by R3 since y is not free in C or in $\Gamma_i \cup \{F_{i+1}\}$; hence $\Gamma_i \cup \{F_{i+1}\} \vdash C$ by R1 with Exercise 2.15. But this contradicts the case assumption, so $\Gamma_{i+1} \nvdash C$.

Case 3. $\Gamma_i \cup \{F_{i+1}\} \nvdash C$, and F_{i+1} is *not* of the form $\exists x A(x)$. Then $\Gamma_{i+1} = \Gamma_i \cup \{F_{i+1}\}$.

Finally, let $\Gamma = \bigcup_{i \geq 0} \Gamma_i$. Observe that $\Gamma \nvdash C$ and $\Delta \subseteq \Gamma \subseteq \mathcal{L}'(\mathrm{V}_1)$ by construction. We need to prove that Γ satisfies (ii) and (iii) of the definition of $\mathcal{L}'(\mathrm{V}_0)$-saturation with witnesses in V_1.

For (ii), suppose F_{i+1} is $A \vee B$ where $\Gamma \vdash A \vee B$. Both A and B are formulas of $\mathcal{L}'(\mathrm{V}_0)$, say A is F_{j+1} and B is F_{k+1}. If $\Gamma_j \cup \{A\} \nvdash C$ then $A \in \Gamma$ by construction. If $\Gamma_k \cup \{B\} \nvdash C$ then $B \in \Gamma$ by construction. And if both $\Gamma_j \cup \{A\} \vdash C$ and $\Gamma_k \cup \{B\} \vdash C$ then $\Gamma \cup \{A \vee B\} \vdash C$ and so $\Gamma \vdash C$, which is impossible. By classical reasoning, it follows that one of A, B must be in Γ.

For (iii), suppose F_{i+1} is $\exists x A(x)$ where $\Gamma \vdash \exists x A(x)$. Then $\Gamma \cup \{\exists x A(x)\} \nvdash C$, so $\Gamma_i \cup \{F_{i+1}\} \nvdash C$, so $A(y) \in \Gamma$ for some $y \in \mathrm{V}_1$ free for x in $A(x)$, by construction.

Proof of (b). Partition V_1 - V_0 into infinitely many infinite subsets, and use the partition to define $\{\mathrm{V}^*_j\}$ so that $\mathrm{V}_0 = \mathrm{V}^*_0$, $\mathrm{V}_1 = \bigcup_{j \in \omega} \mathrm{V}^*_j$ and for $j = 0, 1, 2, \ldots$: $\mathrm{V}^*_j \subseteq \mathrm{V}^*_{j+1}$ and V^*_{j+1} - V^*_j is infinite. Using (a), define by induction on j an increasing sequence $\{\Gamma^*_j\}$ of subsets of $\mathcal{L}'(\mathrm{V}_1)$ such that $\Delta \subseteq \Gamma^*_0$ and for each $j = 0, 1, \ldots$: Γ^*_j is a subset of $\mathcal{L}'(\mathrm{V}^*_{j+1})$ which is $\mathcal{L}'(\mathrm{V}^*_j)$-saturated with witnesses in V^*_{j+1}, and $\Gamma^*_j \nvdash C$. Let $\Gamma^* = \bigcup_{j \geq 0} \Gamma^*_j$. Then $\Delta \subseteq \Gamma^*$ by construction, $\Gamma^* \nvdash C$, and Γ^* is $\mathcal{L}'(\mathrm{V}_1)$-saturated because $\mathrm{V}_1 = \bigcup_{j \geq 0} \mathrm{V}^*_{j+1}$ and $\Gamma^*_0 \subseteq \Gamma^*_1 \subseteq \ldots \subseteq \Gamma^* \subseteq \mathcal{L}'(\mathrm{V}_1) = \bigcup_{j \geq 0} \mathcal{L}'(\mathrm{V}^*_j)$.

Lemma 3.14. Suppose $A(x_1, \ldots, x_m, x_{m+1})$ is a formula in which only the *distinct* variables $x_1, \ldots, x_m, x_{m+1}$ occur free, and $z_1, \ldots, z_m, z_{m+1}$ are any variables such that z_i is free for x_i in $\forall x_{m+1} A(x_1, \ldots, x_m, x_{m+1})$ (or equivalently in $\exists x_{m+1} A(x_1, \ldots, x_m, x_{m+1})$) for $1 \leq i \leq m$. Then

(a) If z_{m+1} is free for x_{m+1} in $A(z_1, \ldots, z_m, x_{m+1})$, then z_{m+1} is free for x_{m+1} in $A(x_1, \ldots, x_m, x_{m+1})$.

(b) If z_{m+1} is free for x_{m+1} in $A(x_1, \ldots, x_m, x_{m+1})$ and if $A'(x_1, \ldots, x_m, x_{m+1})$ is any congruent formula in which none of the variables $z_1, \ldots, z_m, z_{m+1}, x_{m+1}$ occur bound, then z_{m+1} is free for x_{m+1} in $A'(z_1, \ldots, z_m, x_{m+1})$, and $\exists x_{m+1} A'(z_1, \ldots, z_m, x_{m+1})$ is congruent to $\exists x_{m+1} A(z_1, \ldots, z_m, x_{m+1})$.

Theorem 3.15. (**Completeness for Pd**) Suppose E is a formula of $\mathcal{L}(\mathrm{V}, \{R_1, \ldots, R_s\})$ such that $\nvdash_{\mathbf{Pd}} E$. Then there is a Kripke model $\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{V}, \delta, \chi_1, \ldots, \chi_s)$ over $R_1, \ldots, R_s$, with domain V, such that $\langle\,\rangle \nVdash_\phi E$ where $\phi(y) = y$ for every $y \in \mathrm{V}$, and $\phi(x) \in \delta(\langle\,\rangle)$ for every x free in E.

Proof. Define an increasing sequence $\mathrm{V}_0 \subseteq \mathrm{V}_1 \subseteq \ldots$ of subsets of V such that each V_{j+1} - V_j is infinite, V_0 is infinite and contains all variables occurring in E, and $\mathrm{V} = \bigcup_{j \geq 0} V_j$. For each $j \geq 0$ let $F^j_1, F^j_2, \ldots$ be an enumeration without repetitions of all the formulas of $\mathcal{L}'(\mathrm{V}_j) = \mathcal{L}(\mathrm{V}_j, \{R_1, \ldots, R_s\})$. Since $\nvdash E$, by (b) of the Saturation Lemma there is an $\mathcal{L}'(\mathrm{V}_0)$-saturated $\Gamma_0 \subseteq \mathcal{L}'(\mathrm{V}_0)$ such that $\Gamma_0 \nvdash E$.

(K,$\leq$) is defined inductively, with nodes $u = \langle n_1, \ldots, n_k \rangle$ representing chains $\Gamma_0 \subseteq \ldots \subseteq \Gamma_k$ where each Γ_j is an $\mathcal{L}'(\mathrm{V}_j)$-saturated collection of formulas of $\mathcal{L}'(\mathrm{V}_j)$, and we say Γ_k *is attached to* the node u. First attach Γ_0 to the root $\langle\,\rangle$ of K. For each node u of length k with Γ_k attached, enumerate all the finite sequences $F^{k+1}_{i_1}, \ldots, F^{k+1}_{i_r}, F^{k+1}_{i_{r+1}}$ of formulas of $\mathcal{L}'(\mathrm{V}_{k+1})$ such that $r \geq 1$ and $\{F^{k+1}_{i_1}, \ldots, F^{k+1}_{i_r}\} \cap \Gamma_k = \emptyset$ and $\Gamma_k \cup \{F^{k+1}_{i_1}, \ldots, F^{k+1}_{i_r}\} \nvdash F^{k+1}_{i_{r+1}}$. For each m: If $F^{k+1}_{i_1}, \ldots, F^{k+1}_{i_r}, F^{k+1}_{i_{r+1}}$ is the m^{th} such sequence, by (b) of the Saturation Lemma there is an $\mathcal{L}'(\mathrm{V}_{k+1})$-saturated Γ_{k+1} such that $\Gamma_k \cup \{F^{k+1}_{i_1}, \ldots, F^{k+1}_{i_r}\} \subseteq \Gamma_{k+1}$ and $\Gamma_{k+1} \nvdash F^{k+1}_{i_{r+1}}$. Attach this Γ_{k+1} to $u * \langle m \rangle$.

The domain function δ assigns to each node $u = \langle n_1, \ldots, n_k \rangle$ of length k the set V_k; and for $1 \leq i \leq s$ we let $\chi_i(u, y_1, \ldots, y_{n_i}) = 1$ if and only if $R_i(y_1, \ldots, y_{n_i}) \in \Gamma_k$ where Γ_k is attached to u. By construction, $\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{V}, \delta, \chi_1, \ldots, \chi_s)$ is a Kripke model over $R_1, \ldots, R_s$ with domain V.

Suppose ϕ is an assignment to the variables which maps V_k into V_k and $C(x_1, \ldots, x_m)$ is a formula of $\mathcal{L}'(\mathrm{V}_k)$ with only the distinct variables $x_1, \ldots, x_m$ free. We call ϕ *free in* C if and only if $\phi(x_i)$ is free for x_i in C for each $1 \leq i \leq m$.

Claim. Suppose u is a node of K with Γ_k attached, $\phi(y) \in \mathrm{V}_k$ for every $y \in \mathrm{V}_k$, and $\phi(x_i) = z_i$ for $1 \leq i \leq m$. Then for every formula $C(x_1, \ldots, x_m)$ of $\mathcal{L}'(\mathrm{V}_k)$ in which ϕ is free and only the distinct variables $x_1, \ldots, x_m$ occur free:

$$(*) \quad u \Vdash_\phi C(x_1, \ldots, x_m) \quad \text{if and only if} \quad C(z_1, \ldots, z_m) \in \Gamma_k.$$

If C is prime, the claim is true by construction of the model. For the inductive cases, assume the claim holds (at all appropriate nodes, for all appropriate assignments) for all proper subformulas of $C(x_1, \ldots, x_m)$, and let u be a node of length k with Γ_k attached and ϕ be an assignment free in C such that $\phi(y) \in \mathrm{V}_k$ for all $y \in \mathrm{V}_k$, and $\phi(x_i) = z_i$ for $1 \leq i \leq m$. We must prove $(*)$ holds for C.

The propositional cases are exercises for the energetic reader. For the quantifier cases, if $z, x \in \mathrm{V}_k$ and ϕ is an assignment, then $\phi[z/x]$ is a standard abbreviation for the assignment ψ such that $\psi(x) = z$ and $\psi(y) = \phi(y)$ for all $y \neq x$.

Case 6. $C(x_1, \ldots, x_m)$ is $\forall x_{m+1} A(x_1, \ldots, x_m, x_{m+1})$ where $(*)$ holds for $A(x_1, \ldots, x_m, x_{m+1})$ at every node of length $\geq k$. If $u \Vdash_\phi C(x_1, \ldots, x_m)$, choose $z_{m+1} \in \mathrm{V}_{k+1} - \mathrm{V}_k$, so z_{m+1} is free for x_{m+1} in $A(z_1, \ldots, z_m, x_{m+1})$. If $\Gamma_k \nvdash A(z_1, \ldots, z_m, z_{m+1})$, by construction of the model u has an immediate successor v with some Γ_{k+1} attached such that $\Gamma_k \subsetneq \Gamma_{k+1}$ but $A(z_1, \ldots, z_m, z_{m+1}) \notin \Gamma_{k+1}$. By the induction hypothesis, $v \nVdash_\psi A(x_1, \ldots, x_m, x_{m+1})$ where $\psi = \phi[z_{m+1}/x_{m+1}]$. But $v \Vdash_\phi C(x_1, \ldots, x_m)$ by monotonicity, so $v \Vdash_\psi A(x_1, \ldots, x_m, x_{m+1})$, which is impossible. So $\Gamma_k \vdash A(z_1, \ldots, z_m, z_{m+1})$. Then $\Gamma_k \vdash C(z_1, \ldots, z_m)$ by Exercise 2.13, since z_{m+1} is not free in Γ_k, so $C(z_1, \ldots, z_m) \in \Gamma_k$ by Exercise 3.14(a).

Conversely, if $C(z_1, \ldots, z_m) \in \Gamma_k$ and $v \geq u$ is a node of length $h \geq k$ with Γ_h attached, then for every $z_{m+1} \in \mathrm{V}_h$ which is free for x_{m+1} in $A(z_1, \ldots, z_m, x_{m+1})$: $\Gamma_h \vdash A(z_1, \ldots, z_m, z_{m+1})$ so $A(z_1, \ldots, z_m, z_{m+1}) \in \Gamma_h$ by Exercise 3.14(a), and $\psi = \phi[z_{m+1}/x_{m+1}]$ is free in $A(x_1, \ldots, x_m, x_{m+1})$ so by the induction hypothesis $v \Vdash_\psi A(x_1, \ldots, x_m, x_{m+1})$, so $u \Vdash_\phi C(x_1, \ldots, x_m)$.

Case 7. $C(x_1, \ldots, x_m)$ is $\exists x_{m+1} A(x_1, \ldots, x_m, x_{m+1})$ where $(*)$ holds for $A(x_1, \ldots, x_m, x_{m+1})$ at every node of length $\geq k$. If $u \Vdash_\phi C(x_1, \ldots, x_m)$ then there is some $z_{m+1} \in \mathrm{V}_k$ which is free for x_{m+1} in $A(x_1, \ldots, x_m, x_{m+1})$ such that $u \Vdash_\psi A(x_1, \ldots, x_m, x_{m+1})$ where $\psi = \phi[z_{m+1}/x_{m+1}]$. Then ψ is free in $A(x_1, \ldots, x_m, x_{m+1})$, so $A(z_1, \ldots, z_m, z_{m+1}) \in \Gamma_k$ by the induction hypothesis. If z_{m+1} is free for x_{m+1} in $A(z_1, \ldots, z_m, x_{m+1})$ then $\Gamma_k \vdash C(z_1, \ldots, z_m)$ so $C(z_1, \ldots, z_m) \in \Gamma_k$ by saturation. Otherwise, choose a congruent $A'(x_1, \ldots, x_m, x_{m+1})$ of $A(x_1, \ldots, x_m, x_{m+1})$ in which none of the variables $z_1, \ldots, z_m, z_{m+1}, x_{m+1}$ occur bound, so z_{m+1} is free for x_{m+1} in $A'(z_1, \ldots, z_m, x_{m+1})$ and $A'(z_1, \ldots, z_m, z_{m+1}) \in \Gamma_k$ by Exercise 3.14(b). Then $\Gamma_k \vdash \exists x_{m+1} A'(z_1, \ldots, z_m, x_{m+1})$ and therefore $C(z_1, \ldots, z_m) \in \Gamma_k$ by Exercise 3.14(a) with Lemma 3.14(b).

Conversely, if $C(z_1, \ldots, z_m) \in \Gamma_k$ then $A'(z_1, \ldots, z_m, z_{m+1}) \in \Gamma_k$ for some $A'(x_1, \ldots, x_m, x_{m+1})$ congruent to $A(x_1, \ldots, x_m, x_{m+1})$ and some $z_{m+1} \in \mathrm{V}_k$ which is free for x_{m+1} in $A'(z_1, \ldots, z_m, x_{m+1})$, so if $\psi = \phi[z_{m+1}/x_{m+1}]$ then ψ is free in $A'(x_1, \ldots, x_m, x_{m+1})$ and by the induction hypothesis $u \Vdash_\psi A'(x_1, \ldots, x_m, x_{m+1})$. Hence $u \Vdash_\psi C(x_1, \ldots, x_m)$, and so $u \Vdash_\phi C(x_1, \ldots, x_m)$.

By the claim, $\langle\,\rangle \nVdash_\phi E$ if $\phi(x) = x$ for every $x \in \mathrm{V}$, since $E \notin \Gamma_0$ by construction. So the Kripke semantics is complete for **Pd**.

Exercise 3.15. Give the inductive argument for the claim $(*)$ in the proof of Theorem 3.15, for the case that C is of the form $A \vee B$.

Exercise 3.16. Give the inductive argument for the claim $(*)$ in the proof of Theorem 3.15, for the case that C is of the form $A \to B$.

Note the nonconstructive steps in the proof of the Soundness Theorem for **Pd**. These cannot be entirely eliminated. A constructive reformulation of the theorem would be something like this: If E is a Kripke-valid formula of $\mathcal{L}(\mathbf{Pd})$ then it is impossible that there is no proof in **Pd** of E. Hence by Markov's Principle, if $\Vdash E$ then $\vdash_{\mathbf{Pd}} E$.

3.6 Applications of Kripke Semantics for Pd

Theorem 3.16. For any distinct binary predicate letters $P(\cdot), Q(\cdot)$ and unary predicate letter R of $\mathcal{L}(\mathbf{Pd})$, the following classically provable formulas are unprovable in **Pd**:

(a) $\neg\neg\forall x(\neg P(x) \vee \neg\neg P(x))$.

(b) $\forall x(\neg\neg P(x) \to P(x))$.

(c) $\forall x(\neg\neg P(x) \to P(x)) \to \forall x(P(x) \vee \neg P(x))$.

(d) $\forall x\neg\neg P(x) \to \neg\neg\forall x P(x)$.

(e) $\neg\neg\exists x P(x) \to \exists x\neg\neg P(x)$.

(f) $\forall x(P(x) \vee \neg P(x))\ \&\ \neg\forall x\neg P(x) \to \exists x P(x)$.

(g) $\forall x(Q(x) \vee R) \to (\forall x Q(x) \vee R)$.

(h) $(\forall x Q(x) \to R) \to \exists x(Q(x) \to R)$.

(i) $(R \to \exists x Q(x)) \to \exists x(R \to Q(x))$.

(j) $(\neg R \to \exists x Q(x)) \to \exists x(\neg R \to Q(x))$.

Proof, in each case, is by providing a Kripke countermodel. The forms (d), (g)-(i) have already been treated in examples and exercises. A countermodel to (b) can be obtained from the propositional countermodel to part (c) of Theorem 3.5 by adding a one-element constant domain. That is, if $\mathcal{K}_5 = ((\mathrm{K}_5, \leq), \{d_0\}, \chi)$ where $\mathrm{K}_5 = \mathrm{K}_1 = \{\langle\ \rangle, \langle 0\rangle\}$, and $\chi(u, d_0) = 1$ if and only if $u = \langle 0\rangle$, then $\mathcal{K}_5$ is a countermodel to (b). We leave the rest as (sometimes challenging) exercises.

Exercise 3.17. Provide a Kripke countermodel to one of (a), (c), (e), (f), (j).

Unlike **Pp**, intuitionistic predicate logic **Pd** is not (recursively) decidable, so we have no analogue of Theorem 3.6. The completeness of Kripke semantics for **Pd** does give classical proofs of some interesting admissible rules of **Pd**, including the disjunction and existence properties (first established constructively, essentially by Gentzen in 1935) and a form of Markov's Rule. First we collect some easy facts in a lemma which holds constructively.

Lemma 3.17.

(a) If B is a closed formula of $\mathcal{L}'(\mathrm{V}) = \mathcal{L}(\mathrm{V},\{R_1, \ldots, R_s\})$ and $\mathcal{K}$ is a Kripke model over $R_1, \ldots, R_s$ with domain D such that $\langle\ \rangle \Vdash_\phi B$ for some assignment ϕ of elements of D to V, then $\langle\ \rangle \Vdash_\psi B$ for *every* assignment ψ of elements of D to V, so $\mathcal{K} \Vdash B$.

(b) Let $\mathcal{K}$ be a Kripke model over $R_1, \ldots, R_s$ with domain D, and $\mathrm{V}_0 = \{b_1, b_2, \ldots\}$ a countably infinite subset of V. Define $f(a_i) = b_i$ for each $i \geq 1$, and let $\mathcal{K}^f$ be the Kripke model over $\mathcal{L}'(\mathrm{V}_0)$ obtained from $\mathcal{K}$ by replacing δ by δ^f where $\delta^f(u) = \{f(x) : x \in \delta(u)\}$ and $\mathrm{D}^f = \cup_{u\in\mathrm{K}}\delta^f(u)$. Then for every formula E of $\mathcal{L}'(\mathrm{V}_0)$ and every assignment ϕ of elements of D to the variables in V_0:

$$\mathcal{K} \Vdash_\phi E \quad \text{if and only if} \quad \mathcal{K}^f \Vdash_{f\phi} E.$$

(c) Let $m \geq 1$ and for $1 \leq j \leq m$ let $\mathcal{K}_j = ((\mathrm{K}_j, \leq), \mathrm{D}_j, \delta_j, \chi_{j,1}, \ldots, \chi_{j,s})$ be a Kripke model over $R_1, \ldots, R_s$. Suppose $d_0 \in \bigcap_{1\leq j\leq m} \delta_j(\langle\ \rangle)$. Define a new Kripke model $\mathcal{K}' = ((\mathrm{K}', \leq), \mathrm{D}, \delta', \chi'_1, \ldots, \chi'_s)$ where

$$\mathrm{K}' = \{\langle\ \rangle\} \cup \bigcup_{1\leq j\leq m} \{\langle j\rangle * u : u \in \mathrm{K}_j\}, \quad \delta'(\langle\ \rangle) = \{d_0\} \ \text{ and } \ \delta'(\langle j\rangle * u) = \delta_j(u) \ \text{ if } \ u \in \mathrm{K}_j,$$

and if $1 \leq i \leq s$ then for all $x_1, \ldots, x_{i_n} \in \mathrm{V}$: $\chi'_i(\langle\ \rangle, x_1, \ldots, x_{n_i}) = 0$ and for every $1 \leq j \leq m$ and every $u \in \mathrm{K}_j$: $\chi'_i(\langle j\rangle * u, x_1, \ldots, x_{n_i}) = \chi_{j,i}(u, x_1, \ldots, x_{n_i})$. Suppose for each $1 \leq j \leq m$ there is a closed formula E_j of $\mathcal{L}'(\mathrm{V})$ such that $\mathcal{K}_j \not\Vdash E_j$. Then $\mathcal{K}' \not\Vdash E_1 \vee \ldots \vee E_m$.

Exercise 3.18. Prove Lemma 3.17(b).

The process of building $\mathcal{K}'$ from $\mathcal{K}_j$ $(1 \leq j \leq m)$ described in (c) of the lemma is due to Smorynski, and is used with considerable versatility in his Chapter 5 of Troelstra [1973]. We use it to give classical proofs of four admissible rules of **Pd**, two of which do not hold for classical predicate logic **cPd**. None of these rules is derivable in **Pd**.

Theorem 3.18. For all formulas $A(x), B, C$ of $\mathcal{L}(\mathbf{Pd})$ such that only x is free in $A(x)$, and B, C are closed:

(a) If $\vdash_{\mathbf{Pd}} B \vee C$ then $\vdash_{\mathbf{Pd}} B$ or $\vdash_{\mathbf{Pd}} C$.

(b) If $\vdash_{\mathbf{Pd}} \exists x A(x)$ then $\vdash_{\mathbf{Pd}} A(x)$ and hence $\vdash_{\mathbf{Pd}} \forall x A(x)$.

(c) If $\vdash_{\mathbf{Pd}} \neg B \rightarrow \exists x A(x)$ then $\vdash_{\mathbf{Pd}} \exists x(\neg B \rightarrow A(x))$.

(d) If $\vdash_{\mathbf{Pd}} \forall x(A(x) \vee \neg A(x))$ and $\vdash_{\mathbf{Pd}} \neg\forall x \neg A(x)$ then $\vdash_{\mathbf{Pd}} \exists x A(x)$ (and hence by (b), also $\vdash_{\mathbf{Pd}} \forall x A(x)$). (Markov's Rule for **Pd**).

Proof of (b). Assume $\vdash_{\mathbf{Pd}} \exists x A(x)$, so by soundness $\Vdash \exists x A(x)$, and suppose $\nvdash_{\mathbf{Pd}} A(x)$. Then by completeness there is a Kripke model $\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{D}, \delta, \chi_1, \ldots, \chi_s)$ over $R_1, \ldots, R_s$ and an assignment ϕ of elements of D to the individual variables such that $\phi(x) \in \delta(\langle\ \rangle)$ and $\langle\ \rangle \nVdash_{\phi} A(x)$. Without loss of generality, suppose $\phi(x) = d_0$. Apply Lemma 3.17(c) with $m = 1$ to get a new model $\mathcal{K}' = ((\mathrm{K}', \leq), \mathrm{D}, \delta', \chi_1', \ldots, \chi_s')$ such that $\delta'(\langle\ \rangle) = \{d_0\}$ and $\mathcal{K} = \mathcal{K}'^{(\langle 1 \rangle)}$ (see the definition of submodel in section 3.4). Let $\Vdash'$ be the forcing relation on $\mathcal{K}'$.

By Lemma 3.10, $\langle 1 \rangle \nVdash'_{\phi} A(x)$, so by monotonicity $\langle\ \rangle \nVdash'_{\phi} A(x)$. But $\langle\ \rangle \Vdash' \exists x A(x)$ by soundness, so $\langle\ \rangle \Vdash'_{\phi} A(x)$ because $\phi(x)$ is the only element in $\delta'(\langle\ \rangle)$. Contradiction.

Proof of (d). Assume $\vdash_{\mathbf{Pd}} \forall x(A(x) \vee \neg A(x))$ and $\vdash_{\mathbf{Pd}} \neg\forall x \neg A(x)$. Then $\vdash_{\mathbf{Pd}} \exists x(A(x) \vee \neg A(x))$ by Exercise 2.11, so $\vdash_{\mathbf{Pd}} (\exists x A(x) \vee \exists x \neg A(x))$ by Theorem 2.10(b). Hence $\vdash_{\mathbf{Pd}} \exists x A(x)$ or $\vdash_{\mathbf{Pd}} \exists x \neg A(x)$ by Part (a) of this theorem, whose proof is left as an exercise.

Suppose $\vdash_{\mathbf{Pd}} \exists x \neg A(x)$. Consider a one-node Kripke model $\mathcal{K}_0 = ((\{\langle\ \rangle\}, \leq), \mathrm{D}, \chi_1, \ldots, \chi_s)$ where $\mathrm{D} = \{d_0\}$. The only assignment of elements of D to the individual variables is the constant function ϕ such that $\phi(y) = d_0$ for every variable y, and by soundness $\langle\ \rangle \Vdash \exists x \neg A(x)$, so $\langle\ \rangle \Vdash_{\phi} \neg A(x)$. But then $\langle\ \rangle \Vdash \forall x \neg A(x)$, which is impossible because $\langle\ \rangle \Vdash \neg\forall x \neg A(x)$ by soundness. So $\nvdash_{\mathbf{Pd}} \exists x \neg A(x)$, and the only other possibility is $\vdash_{\mathbf{Pd}} \exists x A(x)$.

Exercise 3.19. Prove Theorem 3.18(a).

Exercise 3.20. Prove Theorem 3.18(c).

Question. It is known that the collection of admissible predicate logical rules of **Pd** is not recursively enumerable. Is there any coherent way to organize these rules? This vague question is apparently open.

4 Intuitionistic Logic in Mathematics: Cautious Constructivism

Any branch of mathematics can be studied using intuitionistic instead of classical logic, resulting in an intuitionistic subtheory of the classical theory. In fact, one cautious constructivist has said that constructive mathematics is just mathematics with intuitionistic logic. The first step in any such application is to axiomatize equality.

4.1 Intuitionistic Predicate Logic with Equality Pd[=]

It is possible to treat equality axiomatically within $\mathcal{L}(\mathbf{Pd})$, by choosing a particular binary predicate symbol (say $P_1(\cdot, \cdot)$) to express equality; alternatively, one can add a binary predicate constant to the language. We let $\mathcal{L}(\mathbf{Pd}[=])$ be $\mathcal{L}(\mathbf{Pd})$ with a special binary predicate symbol $\cdot = \cdot$, so if s, t are terms then $s = t$ is a *prime formula* in which all the variables free in s or t are free. Every prime formula of $\mathcal{L}(\mathbf{Pd})$ is also a *prime formula* of $\mathcal{L}(\mathbf{Pd}[=])$, and the *formulas* of $\mathcal{L}(\mathbf{Pd}[=])$ are built up from the prime formulas using $\&, \vee, \rightarrow, \neg, \forall$ and $\exists$ as before.

The axioms of **Pd**[=] are all formulas of $\mathcal{L}(\mathbf{Pd}[=])$ of the forms X1-X12 (the axiom schemas of **Pd**), the reflexivity axiom XE1 (where a is a particular individual variable), and the axiom schema XE2 (where a and b are distinct variables, $P(z)$ may be any prime formula of $\mathcal{L}(\mathbf{Pd})$ in which a and b are free for z, and $P(a)$, $P(b)$ are the results of substituting a and b respectively for all free occurrences of z in $P(z)$).

XE1. $a = a$.

XE2. $a = b \to (P(a) \to P(b))$.

The rules of inference of **Pd**[=] are R1-R3 extended to $\mathcal{L}(\mathbf{Pd}[=])$. A *deduction* (or *derivation*) in **Pd**[=] *of* a formula E *from* a collection Γ of formulas is a finite sequence of formulas, each of which is an axiom by X1-X12 or XE1-XE2, or a member of Γ, or follows by a rule of inference from one or two formulas earlier in the list. If such a deduction exists, we write $\Gamma \vdash_{\mathbf{Pd}[=]} E$. The notions of *dependence* and *variation* are defined just as for **Pd**, and a *proof* is a deduction from no assumptions.

Remarks. Alternatively, we could have replaced $P(z)$ in XE2 by an arbitrary formula $A(z)$ of $\mathcal{L}(\mathbf{Pd}[=])$. We choose this version because it asserts the substitutivity of equals for equals in prime formulas (e.g. $a = b \to (R_i(c, a) \to R_i(c, b))$, $a = b \to (R_i(a, c) \to R_i(b, c))$, $a = b \to (a = c \to b = c)$) and the general form follows by predicate logic. We follow Kleene [1952] in choosing open equality axioms, from which their universal closures can easily be proved.

Lemma 4.1. The Deduction Theorem holds for **Pd**[=].

Proof. Exactly as for **Pd**, with the new axioms XE1-2 treated using X1 and R1 as usual.

Lemma 4.2. **Pd**[=] proves that = is an equivalence relation. If x, y and z are distinct individual variables, then
(a) $\vdash_{\mathbf{Pd}[=]} \forall x(x = x)$.
(b) $\vdash_{\mathbf{Pd}[=]} \forall x \forall y(x = y \to y = x)$.
(c) $\vdash_{\mathbf{Pd}[=]} \forall x \forall y \forall z(x = y \;\&\; y = z \to x = z)$.

Exercise 4.1. Prove Lemma 4.2.

A natural deduction system **NPd**[=] equivalent to **Pd**[=] can be obtained by extending the rules of inference of **NPd** to $\mathcal{L}(\mathbf{Pd}[=])$ and adding two new rules, one (requiring no premises) expressing the reflexive property, and the other the substitutivity property, of =:

$$= \mathrm{I} \quad \cdot\ x = x \qquad\qquad = \mathrm{E}\ \ \frac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2 \\ A(s) & s = t\end{array}}{A(t)}$$

For (= I), x may be any individual variable. For (= E), $A(x)$ is a formula of $\mathcal{L}(\mathbf{Pd}[=])$, and $\mathcal{D}_1$ and $\mathcal{D}_2$ are given **NPd[=]**-deductions from Γ of $A(s)$ and $s = t$ respectively, where s and t are terms free for x in $A(x)$. Each resulting proof tree is a *deduction from* Γ *of* its last formula.

Theorem 4.3. **NPd[=]** and **Pd**[=] are equivalent in the sense that if E is a formula, and Γ a collection of formulas, of $\mathcal{L}(\mathbf{Pd}[=])$ then the following are equivalent:

(a) $\Gamma \vdash_{\mathbf{Pd}[=]} E$ by a deduction in which no variable is varied.

(b) $\Gamma \vdash_{\mathbf{NPd}[=]} E$.

Exercise 4.2. Add to the proof of Theorem 2.8 the additional cases needed for a proof of Theorem 4.3(a) and (b).

Corollary 4.4. Equality is a congruence relation on terms and formulas, in the following sense.

(a) $\vdash_{\mathbf{Pd}[=]} \forall x \forall y(x = y \to t(x) = t(y))$ if x, y are variables free for z in the term $t(z)$.

(b) $\vdash_{\mathbf{Pd}[=]} \forall x \forall y(x = y \to (A(x) \leftrightarrow A(y)))$ if $A(z)$ is a formula of $\mathcal{L}(\mathbf{Pd}[=])$ and x, y are distinct variables free for z in $A(z)$.

Exercise 4.3. Prove Corollary 4.4(a) and outline the proof of (b), treating completely the inductive cases for $\forall$ and $\exists$.

Note. Kleene [1952] gives the name "replacement theorem" to a pair of assertions, analogous to Theorem 2.9 but with $r = s$ in place of $A \leftrightarrow B$, and $t_r = t_s$ or $C_r \leftrightarrow C_s$ in place of $C_A \leftrightarrow C_B$, from which Corollary 4.4 follows. "Congruence" emphasizes the mathematical role of substitutivity of equality, which is important in applications.

4.2 Kripke Semantics for Pd[=]

A *Kripke model* $\mathcal{K}_= = ((\mathrm{K}, \leq), \mathrm{D}, \delta, \chi_1, \dots, \chi_s, \chi_=)$ *over* $R_1, \dots, R_s$ *with equality* is a Kripke model over $R_1, \dots, R_s$ with an additional ternary characteristic function $\chi_=$ interpreting $=$ by an equivalence relation on $\delta(u)$ for each $u \in \mathrm{K}$, with the usual monotonicity requirement so that if $u \leq v$ in K and $\chi_=(u, x, y) = 1$ then $x, y \in \delta(u)$ and $\chi_=(v, x, y) = 1$. A *normal* Kripke model is one in which $=$ is interpreted by identity at each node, so $\chi_=(u, x, y) = 1$ if and only if $x = y \in \delta(u)$.

It is not hard to show that monotonicity and soundness hold for Kripke models with equality, for the restricted language $\mathcal{L}'_= = \mathcal{L}_=(V, \{R_1, \dots, R_s\})$ which is like $\mathcal{L}(\mathbf{Pd}[=])$ but with only finitely many predicate letters $R_1, \dots, R_s$. Completeness holds as well. For theories with *decidable* equality (that is, theories such as Heyting arithmetic, in which $(x = y) \vee \neg(x = y)$ is provable for distinct individual variables x and y), completeness holds with respect to normal Kripke models. Leaving the justifications of these statements as optional, sometimes challenging, exercises for the reader, we turn to an important example of the use of intuitionistic logic in constructive mathematics.

4.3 Heyting Arithmetic HA

Heyting arithmetic **HA** is related to Peano arithmetic **PA** as **Pd** is related to **cPd**, that is, **HA** is arithmetic with intuitionistic logic. We follow Kleene [1952] in choosing an economical axiomatization with symbols and axioms for zero, successor, addition and multiplication, and the axiom schema of mathematical induction for all predicates of $\mathcal{L}(\mathbf{Pd}[=])$. The resulting theory will be strong enough to develop the theory of partial and general recursive functions and to prove Gödel's incompleteness theorem. The consistency question for intuitionistic arithmetic is constructively equivalent to that for classical arithmetic, by a negative interpretation due independently to Gödel and Gentzen.

The language $\mathcal{L}(\mathbf{HA})$ of **HA** has the distinct individual variables $a_1, a_2, a_3, \dots$, an individual constant 0, a unary function symbol $'$, two binary function symbols $+$ and $\cdot$, and the binary predicate symbol $=$. There are no other predicate symbols. *Terms* and *prime formulas* are defined inductively as follows:

- 0 is a *term.*
- Each individual variable is a *term.*
- If s and t are *terms* then s', $(s + t)$ and $(s \cdot t)$ are *terms.*
- If s and t are *terms* then $(s = t)$ is a *prime formula.*

Every occurrence of a variable x in a term s or t is *free in* $(s = t)$. Parentheses and the symbol $\cdot$ may be omitted according to the usual mathematical conventions when there is no chance of confusion. The terms 0, $0'$, $0''$, ... are the *numerals*, abbreviated by $0, 1, 2, \dots$.

Formulas are built from prime formulas as for $\mathcal{L}(\mathbf{Pd})$, using $\&, \vee, \to, \neg, \forall$ and $\exists$. The *scope* of a quantifier, and *free* and *bound* variables in a formula, are as for $\mathcal{L}(\mathbf{Pd})$ but with the current definition of *formula.*

The *axioms* of **HA** are of three kinds: the logical axiom schemas X1 - X12 (for formulas of $\mathcal{L}(\mathbf{HA})$), the axiom schema X13 of mathematical induction, and the particular arithmetical axioms X14-X21 (from which XE1-3 for $\mathcal{L}(\mathbf{HA})$ will follow). For X13, $A(x)$ may be any formula of $\mathcal{L}(\mathbf{HA})$ and x any variable. For X14 - X21 choose a, b, c to be three particular distinct individual variables (for example a_1, a_2, a_3), so these axioms (unlike X13) are formulas rather than schemas.

X13. $A(0) \;\&\; \forall x(A(x) \to A(x')) \to A(x)$.

X14. $(a' = b') \to (a = b)$.

X15. $\neg(a' = 0)$.

X16. $(a = b) \to ((a = c) \to (b = c))$.

X17. $(a = b) \to (a' = b')$.

X18. $(a + 0) = a$.

X19. $(a + b') = (a + b)'$.

X20. $(a \cdot 0) = 0$.

X21. $(a \cdot b') = (a \cdot b) + a$.

X22. $(a = b) \to (a + c = b + c)$.

X23. $(a = b) \to (c + a = c + b)$.

X24. $(a = b) \to (a \cdot c = b \cdot c)$.

X25. $(a = b) \to (c \cdot a = c \cdot b)$.

The only *rules of inference* are the predicate logical rules R1 - R3, for $\mathcal{L}(\mathbf{HA})$, with the usual restrictions on the variables. A *deduction* (or *derivation*) *of E from* Γ is a finite sequence $F_1, \ldots, F_n$ of formulas each of which is an axiom by one of the schemas X1-X13, or one of the particular arithmetical axioms X14-X25, or follows from one or more formulas earlier on the list by R1, R2 or R3. If such a deduction exists we write $\Gamma \vdash_{\mathbf{HA}} E$ and say that *E is deducible from* Γ *in* **HA**, and if $\vdash_{\mathbf{HA}} E$ then E is a *theorem* (or *provable formula*) of **HA**. The notions of *dependence* of one formula in a deduction on an earlier one, and *variation* of a variable in a deduction, carry over from **Pd**, as does the proof of the Deduction Theorem.

Observe that the universal closures of X14-X25 are provable by the method of Exercise 2.13, and hence *every* formula obtained by replacing a, b, c in X14-X25 by (not necessarily distinct) individual variables x, y, z is provable. After proving Lemma 4.5 we use this fact without comment. Also observe that the conclusion of X13 can be strengthened to $\forall x A(x)$ by R2, since x is not free in the hypothesis.[1]

If the intuitionistic negation-elimination axiom schema X10. $\neg A \to (A \to B)$ is replaced by the classical X10^c. $\neg\neg A \to A$, the result is a formal system **PA** for classical Peano arithmetic. We would like to know how much actual arithmetic can be done in **HA**, in particular whether **HA** is in some sense as strong as **PA**.

4.3.1 Primitive Recursive Functions

A number-theoretic function φ is *primitive recursive*, if φ can be defined by a finite sequence of applications of the following five operations:

I $\varphi(x) = x'$ (successor),

II $\varphi(x_1, \ldots, x_n) = q$ where $q \in \omega$ (constants),

III $\varphi(x_1, \ldots, x_n) = x_i$ where $1 \leq i \leq n$ (projections),

IV $\varphi(x_1, \ldots, x_n) = \psi(\chi_1(x_1, \ldots, x_n), \ldots, \chi_m(x_1, \ldots, x_n))$ (substitution),

Va $\varphi(0) = q$ and $\varphi(y') = \chi(y, \varphi(y))$,

Vb $\varphi(0, x_2, \ldots, x_n) = \psi(x_2, \ldots, x_n)$ and $\varphi(y', x_2, \ldots, x_n) = \chi(y, \varphi(y, x_2, \ldots, x_n), x_2, \ldots, x_n)$.

[1] This standard axiomatization is based on Kleene [1952]. Note that X18-X19 and X20-X21 are the primitive recursive definitions of $+$ and $\cdot$ respectively. We have added the "equality axioms" X22-X25 for $+$ and $\cdot$; these special cases of XE2 are provable by mathematical induction from the other axioms, so our axioms are not independent.

This is a recursive definition with I - III as basis; in IV and V, the ψ, χ_j, χ are assumed to be primitive recursive functions already derived. When the primitive recursion schema Va or Vb is used in conjunction with one or more of the explicit definition schemas I-IV, the explicit steps may be omitted if it is clear how to fill them in.

Example. To show that exponentiation is primitive recursive it is enough to observe that

$$x^0 = 0' \text{ and } x^{(y')} = (x^y) \cdot x,$$

where 0, $'$ and $\cdot$ are primitive recursive. A correct primitive recursive derivation of x^y is

1. $\varphi_0(x) = x'$ by (I)
2. $\varphi_1(x) = 0$ by (II)
3. $\varphi_2(x, y, z) = y$ by (III)
4. $\varphi_3(x, y, z) = z$ by (III)
5. $\varphi_4(x, y, z) = \varphi_2(x, y, z) \cdot \varphi_3(x, y, z)$ by (IV)
6. $\varphi_5(x) = \varphi_0(\varphi_1(x))$ by (IV)
7. $\varphi(0, x) = \varphi_5(x)$ and
   $\varphi(y', x) = \varphi_4(y, \varphi(y, x), x)$ by (Vb).

A relation is *primitive recursive* if and only if its characteristic function is. Gödel proved that every primitive recursive function is *arithmetical*, i.e. can be defined in **PA**. The same holds for **HA**; for example, the exponential function is *definable* in **HA** by a formula $A(a, b, c)$ of $\mathcal{L}(\mathbf{HA})$ for which

(ia) $\vdash_{\mathbf{HA}} \exists c A(a, b, c)$,

(ib) $\vdash_{\mathbf{HA}} A(a, b, c) \rightarrow (A(a, b, d) \rightarrow (c = d))$,

(ii) $\vdash_{\mathbf{HA}} A(a, 0, 0')$,

(iii) $\vdash_{\mathbf{HA}} A(a, b, c) \rightarrow A(a, b', (c \cdot a))$,

(iv) $\vdash_{\mathbf{HA}} a = d \rightarrow (A(a, b, c) \rightarrow A(d, b, c))$, and

(v) $\vdash_{\mathbf{HA}} b = d \rightarrow (A(a, b, c) \rightarrow A(a, d, c))$.

Then $r^s = t$ can be treated as an abbreviation of $A(r, s, t)$, if r, s, t are terms. Note that (ia) and (ib) can be replaced by the single condition (i) $\vdash_{\mathbf{HA}} \exists! c A(a, b, c)$ where in general:

$$\exists! y A(y) \text{ abbreviates } \exists y[A(y) \ \& \ \forall z(A(z) \rightarrow z = y)].$$

Exercise 4.4.* Outline a method for finding a particular formula $A(a, b, c)$ of $\mathcal{L}(\mathbf{HA})$ which defines the exponential function in the sense described above.

Alternatively, one can add a function symbol for exponentiation, with its primitive recursive definition and the corresponding equality axioms, to **HA** without increasing the class of provable formulas of the original language; such an extension of a theory is called an *inessential* or *conservative* extension.

There is a tradeoff between the proof-theoretic efficiency gained by restricting (as far as possible) the number of symbols and axioms, and the mathematical convenience provided by an adequate (finite) list of primitive recursive functions with their characteristic axioms. While Kleene's precise formal development of the theory of partial and general recursive functions from a minimal collection of mathematical axioms is close to optimal from the first standpoint, it is sometimes convenient to work in a conservative extension $\mathbf{HA}^{\#}$ of **HA** containing symbols and axioms for enough additional primitive recursive functions to make the arithmetization go smoothly. Unless otherwise stated, by $\mathbf{HA}^{\#}$ we will mean *any* conservative extension of **HA** obtained by adding constants and axioms for *finitely many* primitive recursive functions including the positivity test ($sg(a) = 1$ if $a > 0$, otherwise $sg(a) = 0$), the zero test ($\overline{sg}(a) = 1$ if $a = 0$, otherwise $\overline{sg}(a) = 0$), and

1. exponentiation: a^b
2. factorial: $a!$
3. predecessor: $pd(a)$ (where $pd(0) = 0$)
4. cutoff subtraction: $a \dot{-} b$
5. minimum: $min(a, b)$
6. maximum: $max(a, b)$
7. parity: $par(a)$
8. absolute value: $|a - b|$
9. remainder: $rm(a, b)$ (on dividing a by b)
10. quotient: $qn(a, b)$

Using these functions with sg and $\overline{sg}$ it is easy to show that the relations $a \leq b$, $a < b$, $a \,|\, b$ and $Pr(a)$ ("a is prime") are primitive recursive. For example, $a \leq b$ holds if and only if $\overline{sg}(b \dot{-} a) = 1$.

Exercise 4.5. Give primitive recursive defining equations for the other nine function constants (other than exponentiation, which was treated in the example) listed above. Using these, give explicit definitions for the characteristic functions of $a < b$, $a \,|\, b$ and $Pr(a)$.

Remark. The class of primitive recursive relations is closed under *definition by cases*: if $\chi(x_1, \ldots, x_n)$, $\eta(x_1, \ldots, x_n)$ and $\zeta(x_1, \ldots, x_n)$ are primitive recursive, so is

$$\varphi(x_1, \ldots, x_n) = \begin{cases} \eta(x_1, \ldots, x_n) & \text{if } \chi(x_1, \ldots, x_n) > 0, \\ \zeta(x_1, \ldots, x_n) & \text{otherwise.} \end{cases}$$

In fact, $\varphi(x_1, \ldots, x_n) = \eta(x_1, \ldots, x_n) \cdot sg(\chi(x_1, \ldots, x_n)) + \zeta(x_1, \ldots, x_n) \cdot \overline{sg}(\chi(x_1, \ldots, x_n))$. The next exercise summarizes other important closure properties of this class, and should not be skipped.

Exercise 4.6.* (a) Show that the class of primitive recursive relations is closed under the logical connectives $\&$, $\vee$, $\rightarrow$ and $\neg$.

(b) Show that the class of primitive recursive functions is closed under the following operations:

1. bounded sum: $\varphi(x, x_2, \ldots, x_n) = \Sigma_{y<x} \ \psi(y, x_2, \ldots, x_n)$
2. bounded product: $\varphi(x, x_2, \ldots, x_n) = \Pi_{y<x} \ \psi(y, x_2, \ldots, x_n)$
3. bounded maximum: $\varphi(x, x_2, \ldots, x_n) = max_{y<x} \ \psi(y, x_2, \ldots, x_n)$
4. bounded minimum: $\varphi(x, x_2, \ldots, x_n) = min_{y<x} \ \psi(y, x_2, \ldots, x_n)$
5. bounded least number operator: $\varphi(x, x_2, \ldots, x_n) = \mu y((y < x) \ \& \ (\psi(y, x_2, \ldots, x_n) = 1))$ if such a y exists, otherwise $\varphi(x, x_2, \ldots, x_n) = x$

in the sense that if ψ is primitive recursive, so is φ.

(c) Show that the class of primitive recursive relations $R(x_1, \ldots, x_n)$ is closed under the bounded quantifiers

$$\forall y_{y<x} R(y, x_2, \ldots, x_n) \text{ and } \exists y_{y<x} R(y, x_2, \ldots, x_n).$$

Exercise 4.7. Let p_i be the i^{th} prime, with $p_0 = 2$. Is p_i a primitive recursive function of i? Justify your answer. Include proofs of any mathematical facts you use.

4.3.2 Some Formal Theorems of HA

It is time to see what can be proved in Heyting arithmetic. Using the Deduction Theorem and the equivalence of **HA** with its natural deduction counterpart **NHA**, we can argue informally.

Lemma 4.5. **HA** proves that $=$ is an equivalence relation. If x, y, z are distinct variables, then
(a) $\vdash_{\mathbf{HA}} \forall x(x = x)$.
(b) $\vdash_{\mathbf{HA}} \forall x \forall y(x = y \to y = x)$.
(c) $\vdash_{\mathbf{HA}} \forall x \forall y \forall z(x = y \ \& \ y = z \to x = z)$.

Proofs. For (a), first use the method of Exercise 2.13 to prove the universal closures of X16 and X18. Then using X11 with R1, we have $(x+0) = x$ from X18, and $((x+0) = x) \to (((x+0) = x) \to (x = x))$ from X16, so $x = x$ by R1 twice, and $\forall x(x = x)$ follows by (the method of) Exercise 2.13. For (b), observe that $(x = y) \to ((x = x) \to (y = x))$ is an instance of the schema corresponding to X16, and use (a). For (c), use (b) with X16.

Theorem 4.6. Equality is a congruence relation on terms and formulas of **HA**. That is,
(a) $\vdash_{\mathbf{HA}} \forall x \forall y(x = y \to t(x) = t(y))$ if x, y are distinct variables free for z in the term $t(z)$.
(b) $\vdash_{\mathbf{HA}} \forall x \forall y(x = y \to (A(x) \leftrightarrow A(y)))$ if $A(z)$ is a formula of $\mathcal{L}(\mathbf{HA})$ and x, y are distinct variables free for z in $A(z)$.

Proofs. (a) uses Lemma 4.5 with X16, X17 and X22 - X25. (b) follows from (a) as in the proof of Corollary 4.4 (Exercise 4.3).

Theorem 4.7. If x, y, z are distinct variables, then
(a) $\vdash_{\mathbf{HA}} \forall x((x = 0) \vee \neg(x = 0))$.
(b) $\vdash_{\mathbf{HA}} \forall y((y = 0) \vee \exists z(y = z'))$.
(c) $\vdash_{\mathbf{HA}} \forall x \forall y((x = y) \vee \neg(x = y))$.

Proofs are by mathematical induction. (a) is proved by induction on x, using Lemma 4.5(a) for the basis and (the schema corresponding to) X15 for the induction step. (b) is by induction on y.

For (c) use induction on x to prove $\forall y((x = y) \vee \neg(x = y))$ as follows. By (a) with Lemma 4.5(b), $\forall y((0 = y) \vee \neg(0 = y))$. Assuming $\forall y((x = y) \vee \neg(x = y))$, to show $(x' = y) \vee \neg(x' = y)$ use (constructive) cases from (b). If $y = 0$ then $\neg(x' = y)$ by X15 with Lemma 4.5(c). If $y = z'$ then by the induction hypothesis: $(x = z) \vee \neg(x = z)$, so $(x' = z') \vee \neg(x' = z')$ by X17 and X14, so $(x' = y) \vee \neg(x' = y)$, and since this conclusion does not contain z free it follows from $\exists z(y = z')$.

Remark. Theorem 4.7(c) shows that prime formulas are decidable in **HA**. This is in contrast to pure intuitionistic logic, which obviously does not prove $P \vee \neg P$. Another nice feature is that both negation and disjunction are definable in **HA**, by

$$\neg A \ \equiv \ (A \to 0 = 1) \quad \text{and}$$

$$(A \vee B) \ \equiv \ \exists x((x = 0 \to A) \ \& \ (\neg(x = 0) \to B)) \ .$$

Exercise 4.8. Prove Theorem 4.7(b).

Exercise 4.9. Prove that for all formulas A and B of $\mathcal{L}(\mathbf{HA})$:
(a) $\vdash_{\mathbf{HA}} \neg A \leftrightarrow (A \to 0 = 1)$, and
(b) $\vdash_{\mathbf{HA}} (A \vee B) \leftrightarrow \exists x((x = 0 \to A) \ \& \ (\neg(x = 0) \to B))$, where x is not free in A or in B.

4.3.3 Other Varieties of Constructive Arithmetic

A theory based on (intuitionistic or classical) predicate logic is called *finitely axiomatizable* if it has only finitely many nonlogical axioms. **HA** is not finitely axiomatizable because it includes the induction schema X13 for arbitrary formulas $A(x)$.

Definition. Intuitionistic Robinson's Arithmetic **QA** is the finitely axiomatizable subtheory obtained from **HA** by replacing the induction schema X13 by the single axiom

XQ. $a = 0 \ \vee \ \exists b(a = b')$.

QA is consistent, provably in **HA**, and like **HA** it is essentially undecidable. That is, for any consistent theory **T** extending **QA**, there cannot fail to be sentences of $\mathcal{L}[\mathbf{T}]$ which are neither provable nor disprovable in **T**. In particular, **QA** itself is undecidable and cannot prove its own consistency.[2]

Intuitionistic Presburger arithmetic, the subtheory of **HA** obtained by omitting the symbol and axioms for multiplication, can be proved in **HA** to be consistent and complete, hence decidable.[3] The functions definable in Presburger arithmetic are of interest in model theory.

Another subtheory of **HA** which has been extensively studied in the literature resricts the schema of mathematical induction to instances in which the $A(x)$ is Π^0_2 without parameters. Beklemishev [1999] showed that this theory (call it $\mathbf{i\Pi^0_2}$**-IND**) proves that every primitive recursive function is total; and conversely, that only primitive recursive functions can be proved in $\mathbf{i\Pi^0_2}$**-IND** to be total. However, the gold standard for constructive arithmetic avoids quantifiers altogether.

Primitive recursive arithmetic **PRA** is the quantifier-free theory obtained from **HA** in the following way.[4] The language $\mathcal{L}(\mathbf{PRA})$ extends the quantifier-free part of $\mathcal{L}(\mathbf{HA})$ by adding a constant f_i for each primitive recursive function. The nonlogical axioms of **PRA** include the recursion and equality axioms for each f_i. The quantifier axioms X11, X12 and rules R2, R3 are replaced by the

Substitution Rule: From $A(x)$ conclude $A(t)$,

where $A(x)$ is quantifier-free and t may be any term; the x of the rule is varied in any deduction in which it is used, so for the natural deduction system one requires that the hypotheses of the given derivation of $A(x)$ do not contain x. Finally, the axiom schema X13 of mathematical induction is replaced by the following rule, for quantifier-free $A(x)$:

Induction Rule: From $A(0)$ and $(A(x) \to A(x'))$ conclude $A(x)$.[5]

The development of arithmetic in **PRA** is quite different from that in **HA**. Instead of the Robinson formula, which cannot be expressed without quantifiers, $\vdash_{\mathbf{PRA}} (y = 0 \;\vee\; y = (pd(y))')$ by induction using the definition of $pd(y)$.

The following rules are derivable in **PRA**, for $A(x, y)$ quantifier-free and $t(x, y)$ any term:

Subtle Induction: From $A(0, y)$ and $(A(x, t(x, y)) \to A(x', y))$ conclude $A(x, y)$.

Double Induction: From $A(x, 0)$, $A(0, y)$ and $(A(x, y) \to A(x', y'))$, conclude $A(x, y)$.

Hence $\vdash_{\mathbf{PRA}} (x = y \;\vee\; \neg(x = y))$. Since *every* quantifier-free $A(x_1, \ldots, x_n)$ is equivalent in **PRA** to a prime formula of the form $f_i(x_1, \ldots, x_n) = 0$, where f_i is a primitive recursive function constant, it follows that every formula is decidable. Hence it makes no difference whether the theory is based on classical or intuitionistic logic.

Exercise 4.10.* Outline proofs of the following facts:
(a) **PRA** is closed under the quantifier-free rule of subtle induction.
(b) **PRA** is closed under the quantifier-free rule of double induction.
(c) $\vdash_{\mathbf{PRA}} \; x = y \;\vee\; \neg(x = y)$.

[2] Classical Robinson's arithmetic, obtained from **QA** by the usual strengthening of the logical principle for negation, is often called **Q** in the literature. Kleene [1952] observes that the proof he gives of Rosser's form of Gödel's First Incompleteness Theorem for **PA** can be adapted to **QA** and to **Q**.

[3] Kleene [1952] observes that Joan Ross has verified that Hilbert and Bernays' adaptation of Presburger's original proof extends to the intuitionistic system.

[4] For a complete treatment of **PRA** see Chapter 3 of the first volume of TvD [1988].

[5] The theory obtained from **HA** by replacing X13 by the full Induction Rule (with no restriction on $A(x)$) is equivalent to **HA**, in the sense of proving the same formal theorems. Hence **PRA** is a conservative extension of **HA** with respect to quantifier-free formulas.

4.4 Kripke Semantics for HA

Since **HA** is an applied predicate logic with equality in which prime formulas are decidable (by Lemma 4.6(c)), we need only consider normal Kripke models in which $=$ is interpreted by identity. To satisfy the axioms, the individual constant 0 must be interpreted by a unique element of the domain and the function constants $'$, $+$, $\cdot$ must be interpreted at each node u by functions on $\delta(u)$ with the obvious monotonicity conditions. Thus we need an element $0_{\mathcal{K}}$ of D, a unary function γ_1 from D to D, and two binary functions γ_2, γ_3 from D$\times$D to D such that for each node $u \in$ K:

(i) $0_{\mathcal{K}} \in \delta(\langle\ \rangle)$.

(ii) $\gamma_1(x) \in \delta(u)$ for each $x \in \delta(u)$.

(iii) $\gamma_2(x, y) \in \delta(u)$ for each $x, y \in \delta(u)$.

(iv) $\gamma_3(x, y) \in \delta(u)$ for each $x, y \in \delta(u)$.

Then $\mathcal{K} = ((\mathrm{K}, \leq), \mathrm{D}, \delta, 0_{\mathcal{K}}, \gamma_1, \gamma_2, \gamma_3)$ is a *normal Kripke model for* $\mathcal{L}(\mathbf{HA})$ if (K,$\leq$) is a tree, δ is a monotone function from K into the class of all subsets of D such that $\mathrm{D} = \bigcup_{u \in \mathrm{K}} \delta(u)$, and $0_{\mathcal{K}}, \gamma_1, \gamma_2, \gamma_3$ satisfy (i) - (iv). Each assignment ϕ of values in D to the individual variables determines a *valuation function* Φ which assigns to each term s of $\mathcal{L}(\mathbf{HA})$ an element $\Phi(s)$ of D, such that $\Phi(0) = 0_{\mathcal{K}}$, $\Phi(s') = \gamma_1(\Phi(s))$, $\Phi(s + t) = \gamma_2(\Phi(s), \Phi(t))$ and $\Phi(s \cdot t) = \gamma_3(\Phi(s), \Phi(t))$. Forcing with respect to an assignment ϕ is defined for prime formulas so that $u \Vdash_{\phi} s = t$ if and only if $\phi(x) \in \delta(u)$ for every variable x free in s or t, and $\Phi(s) = \Phi(t) \in \delta(u)$. The induction for compound formulas follows the pattern of **Pd**.

A *normal Kripke model for* **HA** is a normal Kripke model for $\mathcal{L}(\mathbf{HA})$ which forces the universal closures of X13 - X25 at each node. The definition is justified by a soundness theorem, and completeness holds by the remarks in Section 4.2.

Theorem 4.8. (**Soundness for HA**) If $\mathcal{K}$ is a normal Kripke model for **HA** and E is a formula of $\mathcal{L}(\mathbf{HA})$ such that $\vdash_{\mathbf{HA}} E$, then $\mathcal{K} \Vdash E$.

Theorem 4.9. (**Completeness for HA**). If E is a formula of $\mathcal{L}(\mathbf{HA})$ such that $\nvdash_{\mathbf{HA}} E$, then there is a normal Kripke model $\mathcal{K}$ for **HA** such that $\mathcal{K} \nVdash E$.

The *numerals* of $\mathcal{L}(\mathbf{HA})$ are the terms $0, 0', 0'', \ldots$ representing the natural numbers $0, 1, 2, \ldots$ respectively. If $\mathcal{K}$ is a normal Kripke model for **HA** then $\delta(\langle\ \rangle)$ contains a distinct element $\mathbf{n}_{\mathcal{K}}$ for every numeral $\mathbf{n}$. These are the *standard natural numbers of* $\mathcal{K}$, and we call the set of them $\omega_{\mathcal{K}}$.

It is worth noticing that every leaf of a Kripke tree model for **HA** is a (possibly nonstandard) model of classical arithmetic. Conversely, if $\mathcal{M}_1, \ldots, \mathcal{M}_n$ are nonstandard models of **PA**, a Kripke model $(\Sigma_{i=1}^{n} \mathcal{M}_i)'$ of **HA** can be constructed by placing below all the $\mathcal{M}_i$ a root u_ω whose domain consists of the standard integers. This was Smorynski's original use of his gluing operation.[6]

Corollary 4.10. For all formulas $A(x)$, B, C and terms $s(x)$, $t(x)$ of $\mathcal{L}(\mathbf{HA})$ such that no variable other than x is free in $A(x)$ and B, C are closed:

(a) If $\vdash_{\mathbf{HA}} B \vee C$ then $\vdash_{\mathbf{HA}} B$ or $\vdash_{\mathbf{HA}} C$.

(b) If $\vdash_{\mathbf{HA}} \exists x A(x)$ then $\vdash_{\mathbf{HA}} A(\mathbf{n})$ for some numeral $\mathbf{n}$.

(c) If $\vdash_{\mathbf{HA}} \neg B \to \exists x A(x)$ then $\vdash_{\mathbf{HA}} \exists x(\neg B \to A(x))$.

(d) If $\vdash_{\mathbf{HA}} \neg\forall x \neg(s(x) = t(x))$ then $\vdash_{\mathbf{HA}} \exists x(s(x) = t(x))$ and hence, if no variable other than x is free in $s(x)$ or $t(x)$, also $\vdash_{\mathbf{HA}} s(\mathbf{n}) = t(\mathbf{n})$ for some numeral $\mathbf{n}$. (This is one form of Markov's Rule for **HA**.)

Exercise 4.11. Prove Corollary 4.10(d).

[6] See Section 3.6 of these notes.

4.5 Realizability Semantics for HA

A more constructive semantics for intuitionistic arithmetic was invented by Kleene around 1942 and published in 1945. His student David Nelson proved the soundness theorem and then formalized the semantics, making it possible to prove that **HA** is closed under various strong constructive rules which fail for **PA**. In 1973 Troelstra published a precise axiomatic characterization of the notion.

Kleene's idea was to interpret each sentence of **HA** as an incomplete communication, which could in principle be completed by providing certain recursive information. With hindsight, it is tempting to consider Kleene's realizability semantics as a precise implementation of the B-H-K interpretation, but Kleene himself attributed the idea to a combination of Church's Thesis and a passage from Hilbert and Bernays.

In order to state the definition efficiently we need a primitive recursive pairing operation $j(x, y)$ and its corresponding projections $j_0(z), j_1(z)$, as well as some version of the Kleene brackets notation for partial recursive function application. Details are left to the exercises.

Definition (*Number-Realizability*, or *1945-Realizability*). Following Kleene [1945] we define when a number n *realizes* a sentence of $\mathcal{L}(\mathbf{HA})$.

1. n *realizes* a prime sentence $r = t$, if $r = t$ is true.

2. n *realizes* A & B, if $j_0(n)$ *realizes* A and $j_1(n)$ *realizes* B.

3. n *realizes* $A \vee B$, if

   (a) if $j_0(n) = 0$ then $j_1(n)$ *realizes* A, and

   (b) if $j_0(n) \neq 0$ then $j_1(n)$ *realizes* B.

4. n *realizes* $A \to B$, if, for every m: if m *realizes* A then $\{n\}(m)$ is defined and *realizes* B.

5. n *realizes* $\neg A$, if no m *realizes* A.

6. n *realizes* $\forall x A(x)$, if, for every m: $\{n\}(m)$ is defined and *realizes* $A(\mathbf{m})$.

7. n *realizes* $\exists x A(x)$, if $j_1(n)$ *realizes* $A(\mathbf{m})$ where $m = j_0(n)$.

A sentence E of $\mathcal{L}(\mathbf{HA})$ is *realizable* if some number realizes E. A formula F of $\mathcal{L}(\mathbf{HA})$ is *realizable* if its universal closure $\forall F$ is realizable.

Exercise 4.12. Kleene used the (non-surjective) pairing operation

$$j(x, y) = 2^x \cdot 3^y.$$

Show there are primitive recursive functions $j_0(z)$ and $j_1(z)$ such that for all $x, y \in \omega$:

$$j_0(j(x, y)) = x \quad \text{and} \quad j_1(j(x, y)) = y.$$

Exercise 4.13. Prove that every closed term t of $\mathcal{L}(\mathbf{HA})$ is provably equal, in **HA**, to a numeral $\mathbf{n}$. We say that t, like $\mathbf{n}$, *expresses* the number n.

Lemma 4.11. For each formula $A(x)$ with at most x free, and each closed term t expressing the number corresponding to the numeral $\mathbf{t}$:

$$n \text{ realizes } A(t) \text{ if and only if } n \text{ realizes } A(\mathbf{t}).$$

Lemma 4.12. A formula $F(x_1, \ldots, x_m)$, in which only the distinct variables $x_1, \ldots, x_m$ may occur free, is realizable if and only if there is a recursive total function φ of m variables such that, for all $n_1, \ldots, n_m \in \omega$: $\varphi(n_1, \ldots, n_m)$ realizes $F(\mathbf{n}_1, \ldots, \mathbf{n}_m)$.

Proof. We prove the case $m = 3$; the general case is similar.

$\Rightarrow$: If f realizes $\forall x \forall y \forall z F(x, y, z)$ then $\varphi(x, y, z) = \{\{\{f\}(x)\}(y)\}(z)$ has the required property.

$\Leftarrow$: Let e be the gödel number of a recursive total function φ of three variables such that, for all $x, y, z \in \omega$: $\varphi(x,y,z) = \{e\}(x,y,z)$ realizes $F(\mathbf{x},\mathbf{y},\mathbf{z})$. We need the fact from recursion theory, that for each $m, n \in \omega$ there is a primitive recursive function $S^m_n(g, y_1, \ldots, y_m)$ of $m+1$ variables such that, if g is a gödel number of a recursive partial function $\psi(y_1,\ldots,y_m,x_1,\ldots,x_n)$ of $m+n$ variables, then for each $y_1 \ldots y_m$: $S^m_n(g, y_1, \ldots, y_m)$ is a gödel number of $\lambda x_1 \ldots x_n\, \psi(y_1,\ldots,y_m,x_1,\ldots,x_n)$. Kleene wrote $\Lambda x_1,\ldots,x_n\{g\}(y_1,\ldots,y_m,x_1,\ldots,x_m)$ or more generally $\Lambda x_1,\ldots,x_n\psi(y_1,\ldots,y_m,x_1,\ldots,x_m)$ for $S^m_n(g,y_1,\ldots,y_m)$. Then for each $y_1,\ldots,y_m$:

$$\{\Lambda x_1,\ldots,x_n\psi(y_1,\ldots,y_m,x_1,\ldots,x_m)\}(x_1,\ldots,x_n) \simeq \psi(y_1,\ldots,y_m,x_1,\ldots,x_m).$$

To complete the proof, observe that $\Lambda x \Lambda y \Lambda z\, \varphi(x,y,z) = \Lambda x\Lambda y\Lambda z\{e\}(x,y,z)$ realizes $\forall x\forall y\forall z F(x,y,z)$.[7]

Theorem 4.13 (Nelson's Theorem). If $C_1,\ldots,C_k \vdash_{\mathbf{HA}} A$, and $C_1,\ldots,C_k$ are all realizable, then A is realizable.

Proof is by induction on the given derivation of A from $C_1,\ldots,C_k$ in **HA**. Let $y_1,\ldots,y_m$ include all the distinct variables free in $A, C_1,\ldots,C_k$, and assume by Lemma 4.12 that $\psi_1,\ldots,\psi_k$ are recursive total functions such that for all $y_1,\ldots,y_m \in \omega$: $\psi_1(y_1,\ldots,y_m),\ldots,\psi_k(y_1,\ldots,y_m)$ realize $C_1(\mathbf{y_1},\ldots,\mathbf{y_m}),\ldots,C_k(\mathbf{y_1},\ldots,\mathbf{y_m})$ respectively. We need to provide a recursive realization function φ so that $\varphi(y_1,\ldots,y_m)$ is defined and realizes $A(\mathbf{y_1},\ldots,\mathbf{y_m})$ for all $y_1,\ldots,y_m \in \omega$.

For each propositional axiom the realization function is a constant function $\varphi(y_1,\ldots,y_m) = c$, so we just give the constant c, using Kleene's Λ notation.

X1. $\Lambda a\Lambda b\, a$ realizes $A \to (B \to A)$, since if a realizes $A(\mathbf{y_1},\ldots,\mathbf{y_m})$ and b realizes $B(\mathbf{y_1},\ldots,\mathbf{y_m})$ then $\{\{\Lambda a\Lambda b\, a\}(a)\}(b) = \{\Lambda b\, a\}(b) = a$ realizes $A(\mathbf{y_1},\ldots,\mathbf{y_m})$.

X2. $\Lambda d\Lambda e\Lambda a\,\{\{e\}(a)\}(\{d\}(a))$.

X3. $\Lambda a\Lambda b\, j(a,b)$.

X4. $\Lambda c\, j_0(c)$.

X5. $\Lambda c\, j_1(c)$.

X6. $\Lambda a\, j(0,a)$.

X7. $\Lambda b\, j(1,b)$.

X8. $\Lambda d\Lambda e\Lambda f[(1\dot{-}j_0(f))\cdot\{d\}(j_1(f)) + (j_0(f))\cdot\{e\}(j_1(f))]$.

X9. $\Lambda c\Lambda d\, 0$.

X10. $\Lambda c\, 0$ realizes $\neg A \to (A \to B)$ because if c realizes $\neg A$ then nothing can realize A.

The predicate axioms require Lemma 4.11. For each, suppose $t(x_1,\ldots,x_m)$ contains just the distinct variables shown, and $A(x,x_1,\ldots,x_m,y_1,\ldots,y_n)$ has free at most the variables shown, where we may assume $x \neq x_i$, $x \neq y_j$ and $x_i \neq y_j$ for all $1 \leq j \leq n$, $1 \leq i \leq m$. (If x happens to occur in t, first change the bound variable in the axiom.)

X11. $\varphi(x_1,\ldots,x_m,y_1,\ldots,y_n) = \Lambda b\,\{b\}(t(x_1,\ldots,x_m))$ is a realization function for any axiom of the form $\forall x A(x,x_1,\ldots,x_m,y_1,\ldots,y_n) \to A(t(x_1,\ldots,x_m),x_1,\ldots,x_m,y_1,\ldots,y_n)$, as follows. Fix $x_1,\ldots,x_m,y_1,\ldots,y_n$. If b realizes $\forall x A(x,\mathbf{x_1},\ldots,\mathbf{x_m},\mathbf{y_1},\ldots,\mathbf{y_n})$ then $\{b\}(t(x_1,\ldots,x_m))$ realizes $A(\mathbf{t},\mathbf{x_1},\ldots,\mathbf{x_m},\mathbf{y_1},\ldots,\mathbf{y_n})$ by definition, where $\mathbf{t}$ is the numeral expressing $t(x_1,\ldots,x_m)$. But then $\{b\}(t(x_1,\ldots,x_m))$ realizes $A(t(\mathbf{x_1},\ldots,\mathbf{x_m}),\mathbf{x_1},\ldots,\mathbf{x_m},\mathbf{y_1},\ldots,\mathbf{y_n})$ by Lemma 4.11.

[7] The primitive recursive functions $S^m_n(g,y_1,\ldots,y_m)$ are defined in Chapter XII of Kleene [1952], and in most elementary recursion theory courses. The theory of partial and general recursive functions will be covered more completely in a later edition of these notes. The Λ notation may hide the choice of g, so $\Lambda x\varphi(x,y)$ is not unique in general.

X12. Similarly, $\varphi(x_1, \ldots, x_m, y_1, \ldots, y_n) = \Lambda a\, j(t(x_1, \ldots, x_n), a)$ is a realization function for the axiom $A(t(x_1, \ldots, x_m), x_1, \ldots, x_m, y_1, \ldots, y_n) \to \exists x A(x, x_1, \ldots, x_m, y_1, \ldots, y_n)$.

Each of the mathematical axioms except the induction schema is realized by one of 0, $\Lambda t\, 0$, or (for X16) $\Lambda u\, \Lambda t\, 0$. For X13, if $A(x, y_1, \ldots, y_n)$ has free at most the distinct variables shown, then $\Lambda b\, \rho(x, b, y_1, \ldots, y_n)$ is a realization function for

$$A(0, y_1, \ldots, y_n) \ \&\ \forall x(A(x, y_1, \ldots, y_n) \to A(x', y_1, \ldots, y_n)) \to A(x, y_1, \ldots, y_n),$$

where ρ is the recursive partial function defined by the primitive recursion

$$\begin{cases} \rho(0, b, y_1, \ldots, y_n) = j_0(b) \\ \rho(x', b, y_1, \ldots, y_n) = \{\{j_1(b)\}(x)\}(\rho(x, b, y_1, \ldots, y_n). \end{cases}$$

Informal mathematical induction shows that if b realizes $A(0, \mathbf{y_1}, \ldots, \mathbf{y_n})$ & $\forall x(A(x, \mathbf{y_1}, \ldots, \mathbf{y_n}) \to A(x', \mathbf{y_1}, \ldots, \mathbf{y_n}))$ then $\rho(x, b, y_1, \ldots, y_n)$ is defined for all x and realizes $A(\mathbf{x}, \mathbf{y_1}, \ldots, \mathbf{y_n})$.

Now consider the rules of inference. If $\psi(y_1, \ldots, y_n)$ and $\chi(y_1, \ldots, y_n)$ are realization functions for the hypotheses $A(y_1, \ldots, y_n)$ and $A(y_1, \ldots, y_n) \to B(y_1, \ldots, y_n)$ of Rule R1, respectively, then $\varphi(y_1, \ldots, y_n) = \{\chi(y_1, \ldots, y_n)\}(\psi(y_1, \ldots, y_n))$ is a realization function for $B(y_1, \ldots, y_n)$.

If $\psi(x, y_1, \ldots, y_n)$ is a realization function for the hypothesis $C(y_1, \ldots, y_n) \to A(x, y_1, \ldots, y_n)$ of Rule R2, where $x \neq y_i$ for $1 \leq i \leq n$, then $\varphi(y_1, \ldots, y_n) = \Lambda c\, \Lambda x\, (\{\psi(x, y_1, \ldots, y_n)\}(c))$ is a realization function for the conclusion $C(y_1, \ldots, y_n) \to \forall x A(x, y_1, \ldots, y_n)$.

And if $\psi(x, y_1, \ldots, y_n)$ is a realization function for the hypothesis $A(x, y_1, \ldots, y_n) \to C(y_1, \ldots, y_n)$ of Rule R3, with the same condition on x, then $\varphi(y_1, \ldots, y_n) = \Lambda b\, (\{\psi(j_0(b), y_1, \ldots, y_n)\}(j_1(b)))$ is a realization function for the conclusion $\exists x A(x, y_1, \ldots, y_n) \to C(y_1, \ldots, y_n)$. This completes the proof.

Remark. Nelson's Theorem tells us that every extension of **HA** by realizable axioms is consistent. Not every sentence of the form $\forall x(\neg\neg A(x) \to A(x))$ is realizable (can you give a counterexample?), and as we shall see, not every realizable sentence is classically true. But before venturing into nonclassical extensions of **HA**, we take time to show that **HA** has some nice admissible rules.

An important variant of realizability is *realizability*($\vdash$), which changes the inductive clauses for $\vee$, $\to$, $\neg$ and $\exists$ as follows:

3. n *realizes*($\vdash$) $A \vee B$, if
   (a) if $j_0(n) = 0$ then $\vdash A$ and $j_1(n)$ *realizes*($\vdash$) A, and
   (b) if $j_0(n) \neq 0$ then $\vdash B$ and $j_1(n)$ *realizes*($\vdash$) B.
4. n *realizes*($\vdash$) $A \to B$, if, for every m: if $\vdash A$ and m *realizes*($\vdash$) A then $\{n\}(m)$ is defined and *realizes*($\vdash$) B.
5. n *realizes*($\vdash$) $\neg A$, if, if $\vdash A$, then no m *realizes*($\vdash$) A.
7. n *realizes*($\vdash$) $\exists x A(x)$, if $\vdash A(\mathbf{m})$ and $j_1(n)$ *realizes*($\vdash$) $A(\mathbf{m})$ where $m = j_0(n)$.

Assuming **HA** is consistent, Nelson's Theorem without the hypotheses $C_1, \ldots, C_k$ extends to realizability($\vdash$) by essentially the same proof. One only needs to check that the realizing objects for closed theorems are also realizing($\vdash$) objects for the same sentences.

Alternatively, hypotheses $C_1, \ldots, C_k$ (call them Γ) can be included in the definition, and the first clause changed to: n *realizes*($\Gamma \vdash$) a prime sentence $r = t$ if $\Gamma \vdash_{\mathbf{HA}} (r = t)$. Then Nelson's Theorem with hypotheses Γ extends also.

Theorem 4.14. (Kleene)

(a) If E is closed and $\vdash_{\mathbf{HA}} E$ then E is realizable($\vdash$).

(b) If E is closed, $\Gamma = \{C_1, \ldots, C_k\}$ where each C_i is realizable($\Gamma \vdash$), and $\Gamma \vdash_{\mathbf{HA}} E$, then E is realizable($\Gamma \vdash$).

Corollary 4.15. (Kleene) If $A(x,y)$ is a formula containing free only the distinct variables x,y such that $\vdash_{\mathbf{HA}} \forall x\exists y A(x,y)$, then there is a recursive choice function $\varphi(x)$ such that if $n \in \omega$ and $m = \varphi(n)$ then $\vdash_{\mathbf{HA}} A(\mathbf{n},\mathbf{m})$.

Corollary 4.16. For closed formulas A, B, $\exists x A(x)$ of $\mathcal{L}(\mathbf{HA})$:
(a) If $\vdash_{\mathbf{HA}} A \vee B$ then $\vdash_{\mathbf{HA}} A$ or $\vdash_{\mathbf{HA}} B$.
(b) If $\vdash_{\mathbf{HA}} \exists x A(x)$ then $\vdash_{\mathbf{HA}} A(\mathbf{m})$ for some numeral $\mathbf{m}$.

Definition. A formula E is *almost negative* if E contains no $\vee$, and no $\exists$ except in subformulas of the form $\exists x(r(x) = t(x))$.

Lemma 4.17. To each almost negative $E(x_1,\dots,x_n)$ with only the distinct variables $x_1,\dots,x_n$ free, there is a recursive partial function ε_E of n variables such that
(i) If $E(\mathbf{x_1}\dots,\mathbf{x_n})$ is true then $\varepsilon_E(x_1,\dots,x_n)$ realizes $E(\mathbf{x_1},\dots,\mathbf{x_n})$.
(ii) For each $e \in \omega$: if e realizes $E(\mathbf{x_1},\dots,\mathbf{x_n})$ then $E(\mathbf{x_1},\dots,\mathbf{x_n})$ is true.

Definition. A formula $B(y_1,\dots,y_k)$, with only the distinct variables $y_1,\dots,y_k$ free, *numeralwise expresses* (in $\mathbf{HA}$) the informal predicate $\mathcal{P}(y_1,\dots,y_k)$ if and only if, for each k-tuple $n_1,\dots,n_k$ of natural numbers:
(i) if $\mathcal{P}(n_1,\dots,n_k)$ holds then $\vdash_{\mathbf{HA}} B(\mathbf{n}_1,\dots,\mathbf{n}_k)$, and
(ii) if $\mathcal{P}(n_1,\dots,n_k)$ fails then $\vdash_{\mathbf{HA}} \neg B(\mathbf{n}_1,\dots,\mathbf{n}_k)$.

Remark. Every primitive recursive predicate is numeralwise expressible in $\mathbf{HA}$ by a decidable, almost negative formula. In particular, there are almost negative formulas $T(e,x,w)$ and $U(w,y)$ containing free only the variables shown, such that $T(e,x,w)$ numeralwise expresses "w is the smallest gödel number of a computation of $\{e\}(x)$," and $U(w,y)$ numeralwise expresses "y is the value computed by the computation with gödel number w if w codes a computation, otherwise $y = w$." Moreover,

(i) $\vdash_{\mathbf{HA}} \forall e\forall x\forall w[T(e,x,w) \vee \neg T(e,x,w)]$.

(ii) $\vdash_{\mathbf{HA}} \forall x\forall w[U(x,w) \vee \neg U(x,w)]$.

(iii) $\vdash_{\mathbf{HA}} \forall e\forall x\forall w\forall v[T(e,x,w) \;\&\; T(e,x,v) \rightarrow w = v]$.

(iv) $\vdash_{\mathbf{HA}} \forall x\forall w\forall v[U(x,w) \;\&\; U(x,v) \rightarrow w = v]$.

Church's Thesis, as a recursive choice principle, can then be expressed in $\mathbf{HA}$ by the schema CT_0:

$$\forall x\exists y A(x,y) \rightarrow \exists e\forall x\exists w\exists y[T(e,x,w) \;\&\; U(w,y) \;\&\; A(x,y)],$$

where $\forall x\exists y A(x,y)$ is any closed formula. Church's Thesis without choice can be expressed by the schema $\mathrm{CT}_0!$, which comes from CT_0 by replacing the hypothesis $\forall x\exists y A(x,y)$ by $\forall x\exists! y A(x,y)$, where in general $\exists! y B(y) \equiv \exists y[B(y) \;\&\; \forall z(B(z) \rightarrow z = y)]$. Since k-tuples can be coded and decoded primitive recursively, the analogue of CT_0 with hypothesis $\forall x_1 \dots \forall x_k \exists y A(x_1,\dots,x_k,y)$ and conclusion $\exists e\forall x_1 \dots \forall x_k \exists w\exists y[T_n(e,x_1,\dots,x_k,y) \;\&\; U(w,y) \;\&\; A(x_1,\dots,x_k,y)]$ is provable from CT_0 in $\mathbf{HA}$.

Exercise 4.14. Let C be the sentence obtained by taking the $A(x,y)$ in CT_0 to be the formula $(y = 0 \rightarrow \exists z T(x,x,z)) \;\&\; (y \neq 0 \rightarrow \forall z \neg T(x,x,z))$.
(a) Show that 0 realizes C.
(b) Show that C is inconsistent with classical arithmetic $\mathbf{PA}$.

Corollary 4.18 (to Nelson's Theorem). CT_0 (hence $\mathrm{CT}_0!$) is consistent relative to $\mathbf{HA}$.

Proof: Every instance of CT_0 is realizable. Let ε_T, ε_U be the partial recursive functions given by Lemma 4.17 for $T(e,x,w)$ and $U(w,y)$ respectively. Then

$$g = \Lambda m\, j(e_0, \Lambda x\, j(w_0, j(y_0, j(j(\varepsilon_T(e_0,x,w_0), \varepsilon_U(w_0,y_0)), j_1(\{m\}(x))))))$$

realizes CT_0, if $e_0 = \Lambda x\, j_0(\{m\}(x))$, $w_0 = \mu w\, T(e_0,x,w)$ and $y_0 = j_0(\{m\}(x))$. If $\mathbf{HA} + \mathrm{CT}_0$ were inconsistent, then by Nelson's Theorem $0 = 1$ would be realizable; but no n realizes $0 = 1$.

4.6 Formalized Realizability

Nelson formalized number-realizability in a conservative extension of **HA**, and Kleene used the formalization to prove for **HA** some very constructive admissible rules. For convenience, let $\mathbf{HA}^{\#}$ be a conservative extension of **HA** with symbols and axioms for additional primitive recursive functions including all those mentioned in Section 4.3.1, except that instead of just $j_0(x)$ and $j_1(x)$ we add a symbol and axioms for the primitive recursive function $j_n(x)$ of two variables (where $j_n(x)$ is the exponent of the n^{th} prime in the prime factorization of x). With this choice of coding there is no need to introduce a special symbol for $j(x,y)$ (or $j(x_0,\ldots,x_k)$) because $p_0^{x_0}\cdot\ldots p_k^{x_k}$ is a term of the language, but we may use "$j(x,y)$" as an abbreviation for $p_0^x\cdot p_1^y$, and similarly for $j(x_0,\ldots,x_k)$. We include in $\mathbf{HA}^{\#}$ the symbols and axioms for bounded sum and product and the bounded μ operator.

A symbol for the characteristic function of the primitive recursive predicate $T(e,x,w)$, and its axioms, belong to $\mathbf{HA}^{\#}$. We use "$T(e,x,w)$" to abbreviate the prime formula numeralwise expressing the predicate. Similarly, "$T(e,x_1,\ldots,x_k,w)$" abbreviates the prime formula $T(e,j(x_1,\ldots,x_k),w)$ numeralwise expressing the predicate $T(e,x_1,\ldots,x_k,w)$. Instead of the characteristic function of $U(w,y)$ we add a symbol and axioms for the primitive recursive function

$$u(w)=\begin{cases}\mu y<w\,U(w,y) & \text{if } \exists e<w\,\exists x<w\,T(e,x,w),\\ w & \text{otherwise.}\end{cases}$$

Every formula $E(x_1,\ldots,x_k)$ of $\mathcal{L}(\mathbf{HA}^{\#})$ with exactly the distinct variables $x_1,\ldots,x_k$ free is equivalent in $\mathbf{HA}^{\#}$ to a formula $E_{\#}(x_1,\ldots,x_k)$ of $\mathcal{L}(\mathbf{HA})$ with exactly the same free variables, and $\vdash_{\mathbf{HA}} E_{\#}(x_1,\ldots,x_k)$ if and only if $\vdash_{\mathbf{HA}^{\#}} E(x_1,\ldots,x_k)$.

Lemma 4.19. To each formula $E(x_1,\ldots,x_k)$ of $\mathcal{L}(\mathbf{HA}^{\#})$ with only the distinct variables $x_1,\ldots,x_k$ free, there is an almost negative formula $z\,\mathbf{r}\,E(x_1,\ldots,x_k)$ which expresses "z realizes $E(\mathbf{x_1},\ldots,\mathbf{x_k})$" under the natural interpretation of the language.

Partial Proof:

1. $z\,\mathbf{r}\,(s=t)$ is $(s=t)$.
2. $z\,\mathbf{r}\,(A\ \&\ B)$ is $(j_0(z)\,\mathbf{r}\,A)\ \&\ (j_1(z)\,\mathbf{r}\,B)$.
3. $z\,\mathbf{r}\,(A\vee B)$ is $(j_0(z)=0\to(j_1(z)\,\mathbf{r}\,A))\ \&\ (j_0(z)>0\to(j_1(z)\,\mathbf{r}\,B))$.
4. $z\,\mathbf{r}\,(A\to B)$ is $\forall f[(f\,\mathbf{r}\,A)\to[\exists wT(z,f,w)\ \&\ \forall w(T(z,f,w)\to(u(w)\,\mathbf{r}\,B))]]$.
5. $z\,\mathbf{r}\,(\neg A)$ is $\forall f\neg(f\,\mathbf{r}\,A)$.
6. $z\,\mathbf{r}\,\forall xA(x)$ is $\forall x[\exists wT(z,x,w)\ \&\ \forall w(T(z,x,w)\to(u(w)\,\mathbf{r}\,A(x)))]$.

Corollary 4.20. To each almost negative formula $E(x_1,\ldots,x_k)$ with none but the distinct variables $x_1,\ldots,x_k$ free, there is a number $n=\Lambda x_1\ldots x_k\,\varepsilon_E(x_1,\ldots,x_k)$ such that

$$\vdash_{\mathbf{HA}^{\#}}\forall x_1\ldots\forall x_k(E(x_1,\ldots,x_k)\leftrightarrow\{\mathbf{n}\}(x_1,\ldots,x_k)\,\mathbf{r}\,E(x_1,\ldots,x_k)),$$

where $\{n\}(x_1,\ldots,x_k)\,\mathbf{r}\,E(x_1,\ldots,x_k)$ abbreviates the formula

$$R_E(n,x_1,\ldots,x_k)\equiv\exists w\exists z[T(n,x_1,\ldots,x_k,w)\ \&\ (u(w)\,\mathbf{r}\,E(x_1,\ldots,x_k))].$$

Exercise 4.15. Complete the proof of Lemma 4.19 by giving case 7 ($z\,\mathbf{r}\,\exists xA(x)$) of the definition. Verify that the resulting formulas are almost negative.

Corollary 4.21. The schema

$$E\leftrightarrow\exists z(z\,\mathbf{r}\,E)$$

is consistent relative to $\mathbf{HA}^{\#}$ (and hence, with the appropriate translation of "$z\,\mathbf{r}\,E$," to **HA**).

Proof. For each formula $E(x_1,\ldots,x_n)$ with exactly the distinct variables $x_1,\ldots,x_n$ free, let $\varepsilon_E(x_1,\ldots,x_n)$ be the recursive partial function given by Lemma 4.17 for E and let $\varepsilon_{z\mathbf{r}E}(z,x_1,\ldots,x_n)$ be the recursive partial function given by Lemma 4.17 (with Lemma 4.19) for the predicate $(z\,\mathbf{r}\,E)$. Then

$$\varphi_1(x_1,\ldots,x_n)\simeq\Lambda e\, j(e,\varepsilon_{z\,\mathbf{r}E}(e,x_1,\ldots,x_n))$$

is a realization function for $E(x_1,\ldots,x_n)\to\exists z(z\,\mathbf{r}\,E(x_1,\ldots,x_n))$. Similarly (but more simply), $\varphi_2(x_1,\ldots,x_n)\simeq\Lambda f\varepsilon_E(x_1,\ldots,x_n)$ is a realization function for $\exists z(z\,\mathbf{r}\,E(x_1,\ldots,x_n))\to E(x_1,\ldots,x_n)$, so $\varphi(x_1,\ldots,x_n)\simeq j(\varphi_1(x_1,\ldots,x_n),\varphi_2(x_1,\ldots,x_n))$ is a realization function for the equivalence.

In [1971] Troelstra found a natural axiomatization of $\mathbf{HA}^\#$ + $(E\leftrightarrow\exists z(z\,\mathbf{r}\,E))$ by generalizing Church's Thesis to partial functions with almost negative domains. Here and in what follows, we use "$z\,\mathbf{r}\,E$" interchangeably for the formula of $\mathbf{HA}^\#$ defined above, or its translation into the language of $\mathbf{HA}$, noting that the translated formula (though clumsier than the original) is also almost negative. Thus Troelstra's characterization works also for $\mathbf{HA}$ + $(E\leftrightarrow\exists z(z\,\mathbf{r}\,E))$ over $\mathbf{HA}$.

Extended Church's Thesis ECT_0 is the following schema, where $A(x)$ must be almost negative and x,y,w are distinct variables:

$$\forall x[A(x)\to\exists yB(x,y)]\to\exists e\forall x[A(x)\to\exists w\exists y(T(e,x,w)\ \&\ U(w,y)\ \&\ B(x,y))]$$

where for $\mathbf{HA}^\#$, $U(w,y)$ abbreviates the prime formula $u(w)=y$, and $T(e,x,w)$ is also prime.

Theorem 4.22. (Troelstra's Characterization of Realizability)
(i) $\vdash_{\mathbf{HA}^\#+\mathrm{ECT}_0}(E\leftrightarrow\exists x(x\,\mathbf{r}\,E))$.
(ii) $\vdash_{\mathbf{HA}^\#+\mathrm{ECT}_0}E\iff\vdash_{\mathbf{HA}^\#}\exists x(x\,\mathbf{r}\,E)$.

Here is a nice application of Corollary 4.16 and Theorem 4.22. Call a formula $A(x)$ with only x free, or the predicate of x expressed by $A(x)$, a *Church domain* for an arithmetical theory $\mathbf{T}$ if for *every* arithmetical formula $B(x,y)$, if w,x,y are all distinct:

If $\mathbf{T}\vdash\forall x[A(x)\to\exists yB(x,y)]$ then $\mathbf{T}\vdash\exists e\forall x[A(x)\to\exists w\exists y(T(e,x,w)\ \&\ U(w,y)\ \&\ B(x,y))]$.

Every almost negative arithmetical predicate is obviously a Church domain for $\mathbf{HA}^\#$ + ECT_0. The converse holds too.

Corollary 4.23. (JRM) Let $A(x)$ be a Church domain for $\mathbf{HA}^\#$ + ECT_0. Then in $\mathbf{HA}^\#$ + ECT_0, $A(x)$ is provably almost negative.

Proof. Assume $A(x)$ is a Church domain for $\mathbf{HA}^\#$ + ECT_0. By Theorem 4.22(a):

$$(1)\quad\vdash_{\mathbf{HA}^\#+\mathrm{ECT}_0}\forall x[A(x)\leftrightarrow\exists y(y\,\mathbf{r}\,A(x))]$$

where $y\,\mathbf{r}\,A(x)$ is almost negative but $\exists y(y\,\mathbf{r}\,A(x))$ need not be. If we can find an almost negative formula $B(x)$, with only x free, such that $\mathbf{HA}^\#$ + ECT_0 proves $\forall x[A(x)\to B(x)]$ and $\forall x[B(x)\to\exists y(y\,\mathbf{r}\,A(x))]$, then (1) will give $\vdash_{\mathbf{HA}^\#+\mathrm{ECT}_0}\forall x[A(x)\leftrightarrow B(x)]$, proving the theorem. By (1),

$$(2)\quad\vdash_{\mathbf{HA}^\#+\mathrm{ECT}_0}\forall x[A(x)\to\exists y(y\,\mathbf{r}\,A(x))]\ \text{ and so}$$

$$(3)\quad\vdash_{\mathbf{HA}^\#+\mathrm{ECT}_0}\exists e\forall x[A(x)\to\exists w\exists y[T(e,x,w)\ \&\ U(w,y)\ \&\ (y\,\mathbf{r}\,A(x))]]$$

since $A(x)$ is a Church domain for $\mathbf{HA}^\#$ + ECT_0, and then by Theorem 4.22(b):

$$(4)\quad\vdash_{\mathbf{HA}^\#}\exists f[f\,\mathbf{r}\,\exists e\forall x[A(x)\to\exists w\exists y[T(e,x,w)\ \&\ U(w,y)\ \&\ (y\,\mathbf{r}\,A(x))]]].$$

By Corollary 4.16(b) (with the conservativity of $\mathbf{HA}^\#$ over $\mathbf{HA}$) there is an f so that

$$(5)\quad\vdash_{\mathbf{HA}^\#}\mathbf{f}\,\mathbf{r}\,\exists e\forall x[A(x)\to\exists w\exists y[T(e,x,w)\ \&\ U(w,y)\ \&\ (y\,\mathbf{r}\,A(x))]],\ \text{ and so}$$

$$(6)\quad\vdash_{\mathbf{HA}^\#}j_1(\mathbf{f})\,\mathbf{r}\,\forall x[A(x)\to\exists w\exists y[T(\mathbf{e},x,w)\ \&\ U(w,y)\ \&\ (y\,\mathbf{r}\,A(x))]]\ \text{ where } e=j_0(f).$$

From (6) by Theorem 4.22(b):

$$(7)\quad \vdash_{\mathbf{HA}^{\#}+\mathrm{ECT}_0} \forall x[A(x) \rightarrow \exists w \exists y[T(\mathbf{e},x,w) \ \& \ U(w,y) \ \& \ (y\,\mathbf{r}\,A(x))]].$$

Now let $B(x) \equiv \exists w T(\mathbf{e},x,w) \ \& \ \forall w \forall y[T(\mathbf{e},x,w) \ \& \ U(w,y) \rightarrow (y\,\mathbf{r}\,A(x))]$. In $\mathbf{HA}^{\#}$, $B(x)$ is almost negative and equivalent to the right hand side of (7). Hence

$$(8)\quad \vdash_{\mathbf{HA}^{\#}+\mathrm{ECT}_0} \forall x[A(x) \rightarrow B(x)] \ \text{ and } \ \vdash_{\mathbf{HA}^{\#}+\mathrm{ECT}_0} \forall x[B(x) \rightarrow \exists y(y\,\mathbf{r}\,A(x))],$$

so $\vdash_{\mathbf{HA}^{\#}+\mathrm{ECT}_0} \forall x[A(x) \leftrightarrow B(x)]$ as claimed.

One of the three main branches of constructive mathematics is Markov's *Russian recursive mathematics* **RM**, which works on the assumption that all real numbers are recursive. Troelstra has observed that **RM** = **HA** + ECT_0 + MP, where *Markov's Principle* MP is the schema

$$\forall x(A(x) \vee \neg A(x)) \wedge \neg\neg \exists x A(x) \rightarrow \exists x A(x).$$

One of the most important results of **RM** is the *Kreisel-Lacombe-Shoenfield-Tsejtin Theorem*, that every mapping from a complete separable metric space into a metric space is continuous. (It does *not* follow that every mapping from a compact metric space into a metric space is uniformly continuous!) Realizability provides a consistency proof for **RM** and a connection between **RM** and **PA**.

Corollary 4.24. **HA** + MP + ECT_0 is (classically) consistent relative to **HA**.[8]

Theorem 4.25. (Troelstra) For each formula E of the language of **HA**:

$$\vdash_{\mathbf{PA}} \exists x(x\mathbf{r}E) \ \Leftrightarrow \ \vdash_{\mathbf{HA}+\mathrm{MP}+\mathrm{ECT}_0} \neg\neg E.$$

Exercise 4.16. Prove Corollary 4.24.

Exercise 4.17.* Prove Theorem 4.25.

A much stronger result than Corollary 4.15 can be obtained using formalized **q**-realizability. Define $z\,\mathbf{q}\,E$, for $E(x_1,\ldots,x_k)$ any formula of $\mathcal{L}(\mathbf{HA}^{\#})$, by induction on E as $z\,\mathbf{r}\,E$ was defined in the proof of Lemma 4.19 but with the following changes:

3. $z\,\mathbf{q}\,(A \vee B)$ is $[j_0(z) = 0 \rightarrow (j_1(z)\,\mathbf{q}\,A) \ \& \ A] \ \& \ [j_0(z) > 0 \rightarrow (j_1(z)\,\mathbf{q}B) \ \& \ B]$.
4. $z\,\mathbf{q}\,(A \rightarrow B)$ is $\forall f[(f\,\mathbf{q}\,A) \ \& \ A \rightarrow [\exists w T(z,f,w) \ \& \ \forall w(T(z,f,w) \rightarrow (u(w)\,\mathbf{q}\,B))]]$.
5. $z\,\mathbf{q}\,(\neg A)$ is $\forall f \neg[(f\,\mathbf{q}\,A) \ \& \ A]$.
7. $z\,\mathbf{q}\,\exists x A(x)$ is $j_1(z)\,\mathbf{q}\,A(j_0(z)) \ \& \ A(j_0(z))$.

Lemma 4.26. (i) If A is almost negative, then

$$\vdash_{\mathbf{HA}^{\#}} \exists z(z\,\mathbf{q}\,A) \rightarrow A.$$

(ii) If $A(x)$ is almost negative with only x free, then there is a numeral $\mathbf{n}$ such that

$$\vdash_{\mathbf{HA}^{\#}} A(x) \rightarrow \exists w[T(\mathbf{n},x,w) \ \& \ u(w)\,\mathbf{q}\,A(x)].$$

(iii) If A is almost negative, then

$$\vdash_{\mathbf{HA}^{\#}} z\,\mathbf{r}\,A \leftrightarrow z\,\mathbf{q}\,A.$$

(iv) For every formula A of $\mathcal{L}(\mathbf{HA})$:

$$\vdash_{\mathbf{HA}^{\#}+\mathrm{ECT}_0} z\,\mathbf{r}\,A \leftrightarrow z\,\mathbf{q}\,A.$$

[8] Kreisel showed MP independent of **HA** + CT_0 using a typed variant of realizability, which we may have time to consider later.

(v) For closed A: If $\vdash_{\mathbf{HA}^{\#}+\mathrm{ECT}_0} A$ then there is an $\mathbf{n}$ such that

$$\vdash_{\mathbf{HA}^{\#}} \mathbf{n}\,\mathbf{r}\,A \quad \text{and} \quad \vdash_{\mathbf{HA}^{\#}+\mathrm{ECT}_0} \mathbf{n}\,\mathbf{q}\,A.$$

Exercise 4.18. Using Theorem 4.22, show how parts (iv) and (v) of Lemma 4.26 follow from parts (i) - (iii) and their consequence, that if A is almost negative then $\vdash_{\mathbf{HA}^{\#}} \exists z(z\,\mathbf{q}\,A) \leftrightarrow A$.

Exercise 4.19. Prove that the theories $\mathbf{T}_1 \equiv \mathbf{HA}^{\#} + \mathrm{ECT}_0$ and $\mathbf{T}_2 \equiv \mathbf{HA}^{\#} + \forall[E \leftrightarrow \exists z(z\,\mathbf{r}\,E)]$ are equivalent in the sense that they prove the same formal theorems in $\mathcal{L}(\mathbf{HA}^{\#})$.

Theorem 4.27 (Troelstra's Rule TR_0 for $\mathbf{HA}^{\#}$). If $A(x)$ is almost negative and contains only x free, if $B(x, y)$ contains free only the distinct variables x and y, and if $\vdash_{\mathbf{HA}^{\#}} \forall x[A(x) \to \exists y B(x, y)]$, then for some numeral s:

$$\vdash_{\mathbf{HA}^{\#}} \forall x[A(x) \to \exists y(T(\mathbf{s}, x, y)\ \&\ B(x, u(y))].$$

Corollary 4.28 (Church's Rule CR_0 for $\mathbf{HA}^{\#}$). If $B(x, y)$ has only x, y free and $\vdash_{\mathbf{HA}^{\#}} \forall x \exists y B(x, y)$, then for some numeral $\mathbf{s}$:

$$\vdash_{\mathbf{HA}^{\#}} \forall x \exists y(T(\mathbf{s}, x, y)\ \&\ B(x, u(y))).$$

Exercise 4.20. Write down the corresponding rules for $\mathbf{HA}$ and explain why they follow from Theorem 4.27 and Corollary 4.28 respectively.

5 Introduction to Intuitionistic Analysis

While arithmetic studies the natural numbers (and functions from numbers to numbers), mathematical analysis studies the real numbers (and functions from real numbers to real or natural numbers). The classical first-order theory of the rational numbers can be developed within Peano arithmetic, but in order to study the real numbers one needs a different or expanded context. Possibilities exploited in classical analysis include the

- algebraic representation of the real numbers as the unique (up to order-isomorphism) complete ordered field with a countable dense subset order-isomorphic to the rationals.
- geometric representation of the real numbers as the points of a Euclidean line.
- construction of the reals using Dedekind cuts in the rationals, with the convention that if the cut point is a rational number then it must belong to the left set of the cut.
- construction of the reals using Cauchy sequences $\{\rho_n\}_{n\in\omega}$ of rationals, with an equivalence relation identifying $\{\rho_n\}_{n\in\omega}$ with $\{\tau_n\}_{n\in\omega}$ if $\{|\rho_n - \tau_n|\}_{n\in\omega}$ converges to 0.

The last of these representations assumes an understanding of infinite sequences of rational numbers, i.e. of functions from ω into the set of all rationals. Since every non-zero rational number ρ has a unique integer code of the form $j(i, m, n)$ where i is 0 or 1 according as ρ is positive or negative, and where m and n are relatively prime natural numbers (and 0 codes itself), what is really needed is an understanding of the collection ${}^{\omega}\omega$ of all infinite sequences of natural numbers.

Classical *Baire space* is the *topological space* $({}^{\omega}\omega, \mathcal{T})$ whose *topology* (collection of *open sets*) is

$$\mathcal{T} = \{X \subseteq {}^{\omega}\omega \mid (\forall \alpha \in X)(\exists n \in \omega)(\forall \beta \in {}^{\omega}\omega)[(\forall m < n)[\beta(m) = \alpha(m)] \to \beta \in X]\}.$$

A function φ from ${}^{\omega}\omega$ to ω is *continuous* in the Baire topology if, for each $\alpha \in {}^{\omega}\omega$, the value $\varphi(\alpha) \in \omega$ is completely determined by some finite initial segment $\alpha(0), \ldots, \alpha(k)$ of α. Similarly, a functional $\Phi : {}^{\omega}\omega \to {}^{\omega}\omega$ is continuous if and only if, for each $\alpha \in {}^{\omega}\omega$ and $n \in \omega$, the value $(\Phi(\alpha))(n)$ is completely determined by some finite initial segment $\alpha(0), \ldots, \alpha(k_n)$ of α. Continuous functions and functionals play an important, but not an exclusive, role in classical analysis. Brouwer took a more radical view.

5.1 Brouwer's Intuitionistic Baire Space

Just as Heyting's arithmetic is a proper subtheory of classical Peano arithmetic, obtained by weakening the axiom schema of negation elimination, Baire space can be studied using intuitionistic rather than classical logic. Brouwer developed his intuitionistic analysis beginning with his doctoral dissertation [1907] and continuing for half a century. Heyting made an early attempt at formalization. Kleene and Vesley [1965] contains a correct and coherent axiomatization, together with a consistency proof, for Brouwer's analysis with a classically false principle of continuous choice (the analogue for analysis of CT_0 for arithmetic). We begin with an overview of Brouwer's informal theory of Baire space $({}^{\omega}\omega, \mathcal{T})$.

- *Elements* of intuitionistic Baire space are infinite sequences α of natural numbers, called "choice sequences." Brouwer accepted *arbitrary* choice sequences, not only those which can be defined or determined by an algorithm, as mathematical objects. Reasoning constructively about these required a new way of thinking about infinite sequences of natural numbers.

- *Neighborhoods* are determined by finite initial segments $\overline{\alpha}(n)$, where $\overline{\alpha}(0)$ is the empty sequence and $\overline{\alpha}(n+1)$ is $\langle \alpha(0), \ldots, \alpha(n) \rangle$. If $V_{\overline{\alpha}(n)} = \{\beta \in {}^{\omega}\omega \mid (\forall m < n)(\beta(m) = \alpha(m))\}$ is the neighborhood determined by $\overline{\alpha}(n)$, then $V_{\overline{\alpha}(n)} \in \mathcal{T}$. Since there are only countably many finite sequences of natural numbers, there are only countably many neighborhoods.

- *Open sets* (elements of $\mathcal{T}$) are countable unions of neighborhoods. Since finite sequences of natural numbers can be coded effectively by natural numbers, each countable union of neighborhoods can be coded by a choice sequence. In general, from a given representation of an open set X as a union of neighborhoods, one should *not* expect to be able to decide *effectively* whether or not a given choice sequence β belongs to X.

- The *countable axiom of choice* holds, for example: If for each n there is an m for which $A(n, m)$ holds, then there is a choice sequence β such that $A(n, \beta(n))$ holds for every n.

- *"Bar induction"* holds: If $A(w)$ and $B(w)$ are properties of finite sequences w of natural numbers such that

  (i) for each $\alpha \in {}^{\omega}\omega$ there is exactly one $n \in \omega$ such that $B(\overline{\alpha}(n))$,

  (ii) if $B(w)$ then $A(w)$, and

  (iii) if A holds at every sequence $w * \langle n \rangle$ obtained by extending w by one new number n, then $A(w)$ holds,

  then A holds at the empty sequence.

- *Every total function F from Baire space to the natural numbers is continuous!* Moreover, if for each α there is an m such that $A(\alpha, m)$, then there is a *neighborhood function* σ mapping the collection of finite sequences of natural numbers to ω such that for every $\alpha \in {}^{\omega}\omega$ there is exactly one n for which $\sigma(\overline{\alpha}(n)) > 0$, and if $\sigma(\overline{\alpha}(n)) = m + 1$ then $A(\alpha, m)$.

Brouwer justified the countable axiom of choice on the constructive meaning of the hypothesis "for each n there is an m." Bar induction, a powerful tool for which Brouwer gave an essentially circular justification (analyzed in Kleene and Vesley [1965]), is classically equivalent to transfinite induction up to any countable ordinal. Countable choice and bar induction would be accepted by most classical mathematicians.

Brouwer's continuity principle, however, is clearly inconsistent with classical analysis. We must remember that his logic was intuitionistic; he saw no need to prove his theory consistent because it was based on clear constructive principles. The key is his notion of choice sequence, which included sequences chosen one element at a time without any prior restriction on the numbers which may be chosen. A *total* function F must assign to each such sequence α a value $F(\alpha) \in \omega$; but this is possible only if $F(\alpha)$ is completely determined by some finite initial segment $\overline{\alpha}(n)$, and hence F must be continuous in the Baire topology.

Consider for example the function from ${}^{\omega}\omega$ to ω defined by cases:

$$\zeta(\alpha) = \begin{cases} 0 & \text{if } \forall x(\alpha(x) = 0), \\ n+1 & \text{if } \forall m < n(\alpha(m) = 0) \text{ but } \alpha(n) > 0. \end{cases}$$

Classically, ζ is total. Intuitionistically, $\zeta(\alpha)$ is defined if and only if either α is the identically zero sequence, or there is an x such that $\alpha(x) > 0$. Since the decision between the two cases cannot be made based on a finite initial segment of α (unless in fact there is an x such that $\alpha(x) > 0$), ζ is not continuous at $\lambda t\, 0$. Hence, according to Brouwer, ζ is *not* a total function!

We can imagine a free choice sequence β in which 0 is chosen consistently as the value of $\beta(n)$ for each n, but without any restriction on future choices. Then $\zeta(\beta)$ must be undefined, since $\zeta(\beta)$ cannot be different from 0 but if $\zeta(\beta) = 0$ then *all* choices of $\beta(n)$ must be 0, so β is no longer free.[9]

5.2 Kleene's Formalization of Intuitionistic Analysis: B and FIM

Kleene's basic formal system **B** expresses the classically correct part of Brouwer's analysis. We describe it briefly:

- Variables $x, y, z, \ldots$ for numbers and $\alpha, \beta, \gamma, \ldots$ for choice sequences. Type-0 variables are *terms* and type-1 variables are *functors*.

- Finitely many function constants $\mathrm{f}_0, \ldots, \mathrm{f}_p$, where each f_i expresses a primitive recursive function $f_i(x_1, \ldots, x_{k_i}, \alpha_1, \ldots, \alpha_{l_i})$ of k_i natural numbers and l_i choice sequences. The f_i include all the function symbols of $\mathbf{HA}^{\#}$; in particular, f_0 is 0 and f_1, f_2, f_3 are $'$, $+$ and $\cdot$ respectively. If $k_i = 1$ and $l_i = 0$ then f_i is a *functor*. If $t_1, \ldots, t_{k_i}$ are *terms* and $u_1, \ldots, u_{l_i}$ are *functors* then $f_i(t_1, \ldots, t_{k_i}, u_1, \ldots, u_{l_i})$ is a *term*.

- Church's λ, used to produce (type-1) *functors* $\lambda x.t$ from (type-0) *terms* t.

- Evaluation: If u is a *functor* and t is a *term* then $(u)(t)$ is a *term*. (Write $\alpha(t)$ for $(\alpha)(t)$.)

- *Prime formulas* are expressions of the form $s = t$ where s, t are (type-0) *terms*. For example, $(\beta(0))' + \beta(\alpha((0'))) = 5$ is a prime formula, but "$\alpha = \lambda t.5$" abbreviates a composite formula of the form $\forall x[\alpha(x) = (\lambda t.5)(x)]$. *Formulas* are built from prime formulas using the logical connectives $\&$, $\vee, \rightarrow, \neg$ and quantifiers $\forall, \exists$ of both types. Thus if $A(x, \alpha)$ is a formula then $\forall x \exists \alpha A(x, \alpha)$ is a formula.

- Axioms and rules of two-sorted intuitionistic predicate logic. These are obtained by extending the axiom schemas and rules for **Pd** to the language of analysis, renaming X11, X12, R2 and R3 as X11N, X12N, R2N and R3N respectively, and adding the axiom schemas and rules

X11F. $\forall \alpha A(\alpha) \rightarrow A(u)$ where u is any functor free for α in $A(\alpha)$.

X12F. $A(u) \rightarrow \exists \alpha A(\alpha)$ where u is any functor free for α in $A(\alpha)$.

R2F. From $C \rightarrow A(\alpha)$ where α does not occur free in C, conclude $C \rightarrow \forall \alpha A(\alpha)$.

R3F. From $A(\alpha) \rightarrow C$ where α does not occur free in C, conclude $\exists \alpha A(\alpha) \rightarrow C$.

- Axiom schema X13 of mathematical induction, extended to the two-sorted language.

- Axioms X14 - X21 of **HA**, additional axioms expressing the primitive recursive definitions of $f_4, \ldots, f_p$, and the "equality axiom" for sequence variables:

$$x = y \rightarrow \alpha(x) = \alpha(y)$$

from which X22 - X25 and the corresponding properties of $\mathrm{f}_4, \ldots, \mathrm{f}_p$ are derivable.

[9] In a formal context, such a free choice sequence could be represented by a function constant β_0^* for which $\beta_0^*(\mathbf{n}) = \mathbf{0}$ is an axiom for every n (where $\mathbf{n}$ is the numeral for n), but $\forall x\, (\beta_0^*(x) = 0)$ is unprovable.

- Axiom schema of λ-elimination or β-reduction:

$$(\lambda x.t(x))(s) = t(s) \text{ for any term } s \text{ free for } x \text{ in } t(x).$$

- Axiom of countable choice AC: $\forall x \exists \beta A(x, \beta) \rightarrow \exists \beta \forall x A(x, \lambda y.\beta(j(x,y)))$.

- Bar induction BI! (with a thin bar):

$$\forall \alpha \exists ! x R(\overline{\alpha}(x)) \ \& \ \forall w [Seq(w) \ \& \ (R(w) \vee \forall y A(w * \langle y \rangle)) \rightarrow A(w)] \rightarrow A(\langle \, \rangle),$$

  where $Seq(w)$, $*$ and $\langle \, \rangle$ express a primitive recursive coding of finite sequences of numbers, with the property that if $Seq(w)$ holds then the length $lh(w)$ of the sequence coded by w can be recovered primitive recursively from w. Kleene takes the code $\langle n_0, \ldots, n_k \rangle$ for $n_0, \ldots, n_k$ to be $j((n_0)', \ldots, (n_k)')$. If the *length* $lh(m)$ of any natural number m is the number of non-zero exponents in the prime factorization of m, then $lh(\overline{\alpha}(m)) = m$, and $Seq(w)$ holds if and only if $w = \overline{\alpha}(lh(w))$ for some α. If u and w code finite sequences then $u * v$ codes their concatenation.

Kleene's intuitionistic system **FIM** is **B** + CC$_1$ where CC$_1$ is a strong continuous choice principle:

$$\forall \alpha \exists \beta A(\alpha, \beta) \rightarrow \exists \sigma \forall \alpha [\forall x \exists y \{\sigma\}[\alpha](x) \simeq y \wedge A(\alpha, \{\sigma\}[\alpha])],$$

where $\{\sigma\}[\alpha](x) \simeq y$ abbreviates $\exists t[\sigma(\langle x \rangle * \overline{\alpha}(t)) = y' \ \& \ \forall z < t(\sigma(\langle x \rangle * \overline{\alpha}(z)) = 0)]$ and $A(\alpha, \{\sigma\}[\alpha])$ abbreviates $\forall \beta [\forall x \{\sigma\}[\alpha](x) \simeq \beta(x) \rightarrow A(\alpha, \beta)]$.

Variations on **FIM** replace AC by comprehension AC! (below), thin bar induction BI! by monotone or decidable bar induction BI$_M$ or BI$_D$, and CC$_1$ by CC$_0$ or weak continuity WC$_0$:

$$\forall \alpha \exists x A(\alpha, x) \rightarrow \forall \alpha \exists x \exists y \forall \beta [\overline{\alpha}(y) = \overline{\beta}(y) \rightarrow A(\beta, x)].$$

5.3 Some Formal Theorems of the Basic Theory B and the Intuitionistic Theory FIM

We first observe that **B** is closed under all the usual derived rules, including the $\forall$ and $\exists$ rules for both number and function quantifiers (with appropriate restrictions on the free variables). Since **HA** is a subtheory of **B**, the formal theorems established for **HA** in section 4.3.2 hold also for **B**. It is useful to consider some elementary properties of choice sequences which can be proved in **B**.

Theorem 5.1. If $y \not\equiv x \not\equiv z$ then
(a) $\vdash_{\mathbf{B}} \forall x \exists y (\alpha(x) = y)$.
(b) $\vdash_{\mathbf{B}} \forall x \forall z [(\alpha(x) = z) \vee \neg(\alpha(x) = z)]$.
(c) $\vdash_{\mathbf{B}} \forall y \exists \alpha \forall x (\alpha(x) = y)$.
(d) $\vdash_{\mathbf{B}} \forall \alpha \forall \beta \exists \gamma \forall x [\gamma(x) = j(\alpha(x), \beta(x))]$.
(e) $\vdash_{\mathbf{B}} \forall \alpha \forall n \exists \beta \forall x [\beta(x) = j_n(\alpha(x))]$.

Proofs. (a) follows from Lemma 4.5(a) and X12F by the $\forall$ rules and R1. $\forall y \forall z ((y = z) \vee \neg(y = z))$ holds by (a change of variables in) Theorem 4.7(c), so (b) follows by $\forall$-elimination. For (c), observe that $(\lambda x.y)(x) = y$ by λ-elimination, and use X12F with the quantifier rules. We leave (d) and (e) as exercises.

Exercise 5.1. Prove parts (d) and (e) of Theorem 5.1. Your proofs should be more detailed than the indications given for (a) - (c), but you may use the derived rules freely. Do *not* give complete formal proofs, please! (This remark applies to *all* the exercises in this section.)

Remarks. In general, by $j(\alpha, \beta)$ we mean the (unique) γ shown to exist by Theorem 5.1(d), and by $j_n(\alpha)$ we mean the (unique) β shown to exist by Theorem 5.1(e). We may also use the notation $j(\alpha_1, \ldots, \alpha_k)$ for the (unique) function δ satisfying $\delta(x) = j(\alpha_1(x), \ldots, \alpha_k(x))$ for every $x \in \omega$. These abbreviations are used both formally and informally, as in the previous section.

Equality between terms is primitive and decidable, but equality between functors is neither. By definition, "$\alpha = \beta$" abbreviates "$\forall x(\alpha(x) = \beta(x))$" and we should not expect this to be decidable in intuitionistic analysis because the relation of equality between choice sequences is not continuous.

Exercise 5.2. Prove that the relation $\mathcal{R}(\alpha) \equiv (j_0(\alpha) = j_1(\alpha))$ is not continuous in the Baire topology.

Exercise 5.3. Show that

$$\vdash_{\mathbf{B}} \forall x \exists y A(x,y) \rightarrow \exists \gamma \forall x A(x, \gamma(x)).$$

[*Hint*: Use Theorem 5.1(c) with AC and λ-elimination.]

Exercise 5.4.* Show that the axiom schema DC of dependent choices is provable in **B**, where DC is

$$\forall x \exists y A(x,y) \rightarrow \forall z \exists \alpha[\alpha(0) = z \ \& \ \forall x A(\alpha(x), \alpha(x'))].$$

As usual, $\exists ! x C(x)$ abbreviates $\exists x[C(x) \ \& \ \forall y(C(y) \rightarrow y = x)]$. All the results of this subsection (except Exercises 5.3 and 5.4) hold for the *minimal* subsystem **M** of **B**, where **M** omits the axiom schema of bar induction and replaces AC by the comprehension principle AC!:

$$\forall x \exists ! y A(x,y) \rightarrow \exists \alpha \forall x A(x, \alpha(x)).$$

Exercise 5.5. Show that $\vdash_{\mathbf{M}} \exists ! x C(x) \rightarrow \forall x (C(x) \vee \neg C(x))$.

Exercise 5.6.* Show that $\vdash_{\mathbf{M}} \forall x \exists ! \alpha A(x, \alpha) \rightarrow \exists \beta \forall x A(x, \lambda y.\beta(j(x,y)))$, where $\exists ! \alpha B(\alpha)$ is an abbreviation for $\exists \alpha[B(\alpha) \ \& \ \forall \gamma(B(\gamma) \rightarrow \forall x(\gamma(x) = \alpha(x)))]$.

Now we consider the principle of bar induction and its consequences in **B**. Although bar induction is stated for the "universal spread" ${}^{\omega}\omega$, it applies to every closed subset X of ${}^{\omega}\omega$ determined by a *spread law* σ satisfying the following conditions:

(i) $\sigma(\langle\,\rangle) = 0$, where $\langle\,\rangle$ codes the empty sequence.

(ii) For each $m \in \omega$:
$\sigma(m) = 0$ if and only if m codes a finite sequence and $\sigma(m * \langle y \rangle) = 0$ for some $y \in \omega$.

(iii) $\alpha \in X$ if and only if, for *every* $n \in \omega$: $\sigma(\overline{\alpha}(n)) = 0$.

A *finitary spread* or *fan* is a compact subset X of ${}^{\omega}\omega$ determined by a spread law σ which satisfies (i) - (iii) and also

(iv) For each $m \in \omega$:
If $\sigma(m) = 0$ then there is an $s \in \omega$ such that, for all $y \in \omega$: if $\sigma(m * \langle y \rangle) = 0$ then $y \leq s$.

In particular, the *binary fan* ${}^{\omega}2$ (with $2 = \{0,1\}$ as usual) is determined by setting $s = 1$ in (iv), for every $m \in \omega$, and strengthening the last "if ... then ..." to "... if and only if ...."

Classically, a fan is a tree with finite branching at each node, and no finite branches. Classical *König's Lemma* says that every tree with finite branching at each node, and arbitrarily long finite branches, has an infinite branch. Bar induction allows us to prove a constructive version of (the contrapositive of) König's Lemma. Continuous choice and bar induction together give Brouwer's classically false "Fan Theorem," which guarantees that every total function on a finitary spread is *uniformly* continuous.

Theorem 5.2. Let $F(\sigma)$ be a formula, with only σ free, expressing the conjunction of (i), (ii) and (iv) of the definition above; that is, $F(\sigma)$ expresses "σ is a finitary spread-law." Then for every formula $R(w)$ in which σ does not occur and α, x are free for w:

$$\vdash_{\mathbf{B}} F(\sigma) \ \& \ \forall \alpha[\forall x \sigma(\overline{\alpha}(x)) = 0 \rightarrow \exists ! x R(\overline{\alpha}(x))] \rightarrow \exists z \forall \alpha[\forall x \sigma(\overline{\alpha}(x)) = 0 \rightarrow \exists x[x \leq z \ \& \ R(\overline{\alpha}(x))]].$$

Theorem 5.3 (Brouwer's Fan Theorem). Let $F(\sigma)$ be as in the previous theorem, let $G(\alpha)$ abbreviate $\forall x\sigma(\overline{\alpha}(x)) = 0$, and let $A(\alpha, y)$ be a formula in which σ does not occur and in which γ is free for α. Then

$$\vdash_{\mathbf{FIM}} F(\sigma) \ \&\ \forall\alpha[G(\alpha) \to \exists y A(\alpha, y)] \to \exists z\forall\alpha[G(\alpha) \to \exists y\forall\gamma[G(\gamma) \ \&\ \overline{\gamma}(z) = \overline{\alpha}(z) \to A(\gamma, y)]].$$

5.4 Realizability Semantics for FIM

By 1959 Kleene had the idea of using number-theoretic functions, rather than numbers, as realizing objects for sentences of the two-sorted language. In [1965] and [1969] he developed function realizability and its variants, allowing him to prove the consistency of **FIM** and the analogues for intuitionistic analysis of many other results proved for intuitionistic arithmetic in the previous section. One difference is that the countable language of analysis does not contain a name for every choice sequence, so realizability has to be defined for formulas under an arbitrary assignment of choice sequences to the free function variables. Once this change is made, it is reasonable to assign natural numbers as values to the free number variables instead of substituting numerals for them.

Definition (Function realizability, Kleene 1959-65). For $E(\alpha_1, \ldots, \alpha_k, x_1, \ldots, x_n)$ any formula of $\mathcal{L}(\mathbf{FIM})$ in which only the distinct variables shown occur free, and any list $\Psi = (\psi_1, \ldots, \psi_k, m_1, \ldots, m_n)$ of choice sequences and natural numbers corresponding to $\alpha_1, \ldots, \alpha_k, x_1, \ldots, x_n$ respectively, we define when a number-theoretic function σ *realizes* E *under the assignment of* Ψ *to the free variables*, or briefly when σ *realizes*-Ψ E.

1. σ *realizes*-Ψ $r = t$, if $r = t$ is true-Ψ.

2. σ *realizes*-Ψ $A \wedge B$, if $j_0(\sigma)$ *realizes*-Ψ A and $j_1(\sigma)$ *realizes*-Ψ B.

3. σ *realizes*-Ψ $A \vee B$, if
   $(j_0(\sigma))(0) = 0 \Rightarrow j_1(\sigma)$ *realizes*-Ψ A, and
   $(j_0(\sigma))(0) \neq 0 \Rightarrow j_1(\sigma)$ *realizes*-Ψ B.

4. σ *realizes*-Ψ $A \to B$, if, for every τ:
   τ *realizes*-Ψ $A \Rightarrow \{\sigma\}[\tau]$ is totally defined and *realizes*-Ψ B.

5. σ *realizes*-Ψ $\neg A$, if no τ *realizes*-Ψ A.

6. σ *realizes*-Ψ $\forall x A$, if, for every m: $\{\sigma\}[m]$ is totally defined and *realizes*-Ψ, m A.

7. σ *realizes*-Ψ $\exists x A$, if $j_1(\sigma)$ *realizes*-$\Psi, (j_0(\sigma))(0)$ A.

8. σ *realizes*-Ψ $\forall\beta A$, if, for every β: $\{\sigma\}[\beta]$ is totally defined and *realizes*-Ψ, β A.

9. σ *realizes*-Ψ $\exists\beta A$, if $j_1(\sigma)$ *realizes*-$\Psi, j_0(\sigma)$ A.

A sentence E is *recursively realizable* if some recursive σ realizes E. A formula is recursively realizable if its universal closure is.

Theorem 5.4. (Kleene 1962) If $C_1, \ldots C_k$ are recursively realizable and $C_1, \ldots, C_k \vdash_{\mathbf{FIM}} E$, then E is recursively realizable.

Corollary 5.5. **FIM** is consistent. Classically, so is **FIM** + MP$_1$, where MP$_1$ is the sentence

$$\forall\alpha[\neg\neg\exists x(\alpha(x) = 0) \to \exists x(\alpha(x) = 0)]$$

expressing a form of Markov's Principle.

Exercise 5.7. Let MP be the schema

$$\forall x(A(x) \vee \neg A(x)) \ \&\ \neg\neg\exists x A(x) \to \exists x A(x),$$

where $A(x)$ may now be any formula of the two-sorted language.

(a) Prove that every instance of MP is provable in $\mathbf{B}$ + MP$_1$.

(b) Prove conversely that MP$_1$ is provable in $\mathbf{B}$ + MP.

Kleene used a typed variant of function-realizability to prove $\nvdash_{\mathbf{FIM}}$ MP, and formalized ordinary function-realizability and q-function-realizability to show:

Theorem 5.6. (Kleene 1969)

(i) If $\vdash_{\mathbf{FIM}} E$ then $\vdash_{\mathbf{B}} \exists\sigma(\sigma\,\mathbf{r}\,E)$. Hence if $\mathbf{B}$ is consistent, so is $\mathbf{FIM}$.

(ii) If $A \vee B$ is a sentence and $\vdash_{\mathbf{FIM}} A \vee B$ then $\vdash_{\mathbf{FIM}} A$ or $\vdash_{\mathbf{FIM}} B$. [10]

(iii) If $\exists x A(x)$ is a sentence and $\vdash_{\mathbf{FIM}} \exists x A(x)$ then $\vdash_{\mathbf{FIM}} A(\mathbf{m})$ for some numeral $\mathbf{m}$.

(iv) (Church's Rule) If $\vdash_{\mathbf{FIM}} \exists\alpha B(\alpha)$ where $B(\alpha)$ has only α free, then for a particular numeral $\mathbf{e}$:

$$\vdash_{\mathbf{FIM}} \exists\alpha[\forall x\exists y(T(\mathbf{e},x,y)\wedge u(y)=\alpha(x))\wedge B(\alpha)].$$

Church's Thesis CT$_1$ for analysis is $\forall\alpha GR(\alpha)$, where

$$GR(\alpha) \equiv \exists z\forall x\exists y[T(z,x,y)\wedge u(y)=\alpha(x)].$$

Theorem 5.7 (JRM). (CT$_1$ fails in $\mathbf{FIM}$, but) Weak Church's Thesis WCT$_1$:

$$\forall\alpha\neg\neg GR(\alpha)$$

is consistent with $\mathbf{FIM}$. In other words, intuitionistic analysis is consistent with the hypothesis that there are no non-recursive choice sequences.

The proof of the consistency of WCT$_1$ uses a modification of typed function-realizability. For example σ ^{G}realizes-Ψ $\forall\alpha B$, if $\{\sigma\}[\alpha]$ is totally defined (and of the right type to ^{G}realize-Ψ,α B) for every α, and ^{G}realizes-Ψ,α B when α is recursive.

Troelstra's *Generalized Continuity Principle* GC$_1$ is the schema:

$$\forall\alpha[A(\alpha)\rightarrow\exists\beta B(\alpha,\beta)]\rightarrow\exists\sigma\forall\alpha[A(\alpha)\rightarrow\forall x\exists y\{\sigma\}[\alpha](x)\simeq y\wedge B(\alpha,\{\sigma\}[\alpha])]$$

where $A(\alpha)$ must be almost negative. It extends Brouwer's principle of continuous choice to partial functions with almost negative domains (*domains of continuity*) and gives a precise characterization of function-realizability.[11]

Theorem 5.8 (Troelstra).

(i) $\vdash_{\mathbf{B}+\mathrm{GC}_1} (E \leftrightarrow \exists\sigma(\sigma\,\mathbf{r}\,E))$.

(ii) $\vdash_{\mathbf{B}+\mathrm{GC}_1} E \;\Leftrightarrow\; \vdash_{\mathbf{B}} \exists\sigma(\sigma\,\mathbf{r}\,E)$.

Kleene observed that $\forall x_1\ldots\forall x_n[A(x_1,\ldots,x_n)\vee\neg A(x_1,\ldots,x_n)]$ is classically function-realizable for every formula $A(x_1,\ldots,x_1)$ of $\mathcal{L}(\mathbf{HA})$ containing free only $x_1,\ldots,x_n$; hence $\mathbf{FIM}$ is consistent with classical arithmetic $\mathbf{PA}$. More generally, $\mathbf{FIM}$ is consistent with every classically realizable sentence of the two-sorted language.

Markov's Principle is classically realizable. So is every instance of "Kuroda's Principle" or "double negation shift" DNS$_0$:

$$\forall x\neg\neg A(x)\rightarrow\neg\neg\forall x A(x).$$

Let DNS$_1$ be the schema $\forall\alpha\neg\neg\exists x A(\overline{\alpha}(x))\rightarrow\neg\neg\forall\alpha\exists x A(\overline{\alpha}(x))$.

[10] Formalized q-realizability is needed for (ii) - (iv). Since arithmetic has a constant (numeral) for every natural number, the results for $\mathbf{HA}$ corresponding to (ii) and (iii) could be obtained using informal realizability($\vdash$). However, no countable theory can have a name for every choice sequence.

[11] An alert reader will note the similarity between Theorems 5.8 and 4.22. In arithmetic, recursive partial functions are coded by natural numbers. In analysis, continuous partial functions are coded by neighborhood functions, which are choice sequences. Troelstra's characterization theorems show that taking realizability seriously has mathematical consequences; in particular, an analogue of Theorem 4.23 holds for $\mathbf{B}$ + GC$_1$.

Lemma 5.9. Let $\mathbf{T}$ be any of the theories $\mathbf{B} + \mathrm{DNS}_1$, $\mathbf{B}+$ MP or $\mathbf{B} + \mathrm{DNS}_1+$ MP, and let $\mathbf{IT}$ be $\mathbf{T} + \mathrm{GC}_1$. Then for every sentence E of the two-sorted language:

$$\vdash_{\mathbf{IT}} E \;\Rightarrow\; \vdash_{\mathbf{T}} \exists\sigma(\sigma\,\mathbf{r}\,E).$$

Hence $\mathbf{IT}$ is consistent, and $\mathbf{T}$ is a proper subsystem of classical analysis $\mathbf{C}$.

Remark. Each of the theories $\mathbf{T}$ and $\mathbf{IT}$ of Lemma 5.9 has the disjunction and numerical existence properties (corresponding to Theorem 5.4(ii),(iii)) and is closed under Church's Rule and Troelstra's Rule (the rule corresponding to GC_1).

Lemma 5.10. For each formula E of the two-sorted language let E^g be its Gödel-Gentzen negative translation. Then
(i) $\vdash_{\mathbf{C}} E \Rightarrow \vdash_{\mathbf{B}+\mathrm{DNS}_0} E^g$.
(ii) $\vdash_{\mathbf{C}} E \leftrightarrow E^g$.

Theorem 5.11 (JRM). For each formula E of the two-sorted language:

$$\vdash_{\mathbf{C}} \exists\sigma(\sigma\,\mathbf{r}\,E) \;\Leftrightarrow\; \vdash_{\mathbf{B}+\mathrm{DNS}_0+\mathrm{MP}+\mathrm{GC}_1} \neg\neg E.$$

Corollary 5.12. DNS_1 is provable in $\mathbf{B} + \mathrm{DNS}_0+$ MP + GC_1.

Proof: Let E be any instance of DNS_1. Then $\vdash_{\mathbf{C}} \exists\sigma(\sigma\,\mathbf{r}\,E)$ by Lemma 5.7, so $\neg\neg E$ is provable in $\mathbf{B}$ + DNS_0 + MP + GC_1. But $\vdash_{\mathbf{B}} \neg\neg E \to E$ since E is of the form $F \to \neg\neg G$.